

Novell ZENworks® Desktop Management

7

www.novell.com

ADMINISTRATION GUIDE

July 14, 2006



Novell®

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Please refer to www.novell.com/info/exports/ for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2006 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.novell.com/company/legal/patents/> and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

For a list of Novell trademarks, see the [Novell Trademark and Service Mark \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html) list at <http://www.novell.com/company/legal/trademarks/tmlist.html>.

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide	29
Part I Understanding ZENworks 7 Desktop Management	31
1 Understanding the Novell Client	33
1.1 The Role of the Novell Client	33
1.1.1 The Novell Client and ZENworks Desktop Management Installation	33
1.1.2 The Novell Client and ConsoleOne Administration	34
1.1.3 Using the Novell Client in a ZENworks 7 Environment	34
2 Understanding the Desktop Management Agent	37
2.1 What is the Desktop Management Agent?	37
2.2 Getting Ready to Use the Desktop Management Agent	37
2.2.1 Desktop Management Agent Installation Considerations	38
2.2.2 Upgrading the Desktop Management Agent	38
2.2.3 Modifying the Desktop Management Agent Login	38
2.2.4 Setting Up AutoAdminLogon for Windows 2000/XP	39
3 Understanding the ZENworks Middle Tier Server and the Desktop Management Server	47
3.1 What Is the ZENworks Middle Tier Server?	47
3.2 Getting Ready to Use the ZENworks Middle Tier Server	47
3.2.1 Preparing for the Middle Tier Server	48
3.2.2 Installing ZENworks Middle Tier Server	48
3.2.3 Configuring the ZENworks Middle Tier Server with NSAdmin	48
3.3 What Is the Desktop Management Server?	57
3.4 Getting Ready to Use the Desktop Management Server	58
3.4.1 Preinstallation Considerations	58
3.4.2 Installing the Desktop Management Server	58
3.4.3 Configuring the Desktop Management Server	59
4 Understanding the ZENworks Multiple UNC Provider	61
4.1 What Is the ZENworks Multiple UNC Provider?	61
4.1.1 How Does ZENMUP Work?	62
4.1.2 ZENMUP Environments Overview	64
5 Process Flow in ZENworks Desktop Management	65
5.1 Authenticating to eDirectory	65
5.1.1 Logging in Using the Novell Client	65
5.1.2 Logging in Using the Desktop Management Agent	66
5.1.3 Logging in Locally to the Workstation	68
5.2 Reading Attributes from eDirectory	69
5.3 Accessing Policy and Application Files	69
5.3.1 Policy Files	69
5.3.2 Application Files	69

5.3.3	Accessing Files by Using a Client Inside the Firewall	70
5.3.4	Accessing Files by Using the Desktop Management Agent Outside the Firewall . . .	71
A	Implementing a DHCP Option for Delivering the Middle Tier Server Address	73
A.1	Overview	73
A.2	Creating a New DHCP Option	74
A.3	Changing the DHCP Option	74
A.4	Checking the Middle Tier Address in the Registry	74
B	Using a ZENworks Tree	75
B.1	Understanding the ZENworks Tree	75
B.2	The ZENworks Tree in an Active Directory Environment	75
B.3	The ZENworks Tree in an eDirectory Environment	76
B.3.1	Using the Novell Client	77
B.3.2	Using the Desktop Management Agent	77
C	E-Mail and Dotted Name Login Support	81
C.1	E-Mail Formatted Names	81
C.2	Non-E-Mail Formatted Names	82
C.3	Enabling E-Mail and Dotted Name Login Support	82
D	Using the Novell Kerberos KDC to Support ZENworks Dynamic Local Users	85
D.1	Kerberos Terms	85
D.2	Kerberos KDC Services	86
D.3	Things to Know Before Setting Up the Novell Kerberos KDC for ZENworks DLU	87
D.4	Setting Up the Novell Kerberos KDC for ZENworks DLU	87
D.4.1	Setting Up the Linux Server	88
D.4.2	Setting Up the KDC for Windows Workstations	89
D.4.3	Setup Options	90
E	Ports Used by ZENworks 7 Desktop Management	91
F	Documentation Updates	93
F.1	July 14, 2006 (Support Pack 1)	93
F.1.1	Appendix D: Using the Novell Kerberos KDC to Support ZENworks Dynamic Local Users	93
F.1.2	Understanding the ZENworks Middle Tier Server and the Desktop Management Server	94
F.2	January 31, 2006	94
F.2.1	Appendix E: Ports Used by ZENworks 7 Desktop Management	94
F.3	December 23, 2005	94
F.3.1	Understanding the ZENworks Middle Tier Server and the Desktop Management Server	94
F.4	December 9, 2005	95
Part II	Checking the ZENworks Desktop Management Installation	97

6	Checking the Installation of Desktop Management Components on Servers	99
6.1	Determining the Version of ZENworks Components Installed on a NetWare or Windows Server	99
6.1.1	Using Zenver.exe	99
6.1.2	Registry Entries Containing Version Information	99
6.2	Using Logging Methods to Check ZENworks on NetWare and Windows Servers	110
6.3	Identifying Processes Started by the Linux Installation	111
6.3.1	Controlling Individual ZENworks Processes	112
6.3.2	Starting and Stopping All ZENworks Processes	113
6.4	Determining the Version of ZENworks Components Installed on a Linux Server	113
G	Documentation Updates	115
G.1	July 14, 2006 (Support Pack 1)	115
G.2	December 23, 2005	115
G.2.1	Checking the Installation of Desktop Management Components on Servers	115
G.3	December 9, 2005	116
Part III	Automatic Workstation Import and Removal	117
7	Understanding Automatic Workstation Import and Removal	119
7.1	Understanding Workstation Import and Registration	119
7.1.1	Using the Import Service	120
7.1.2	Registering Imported Workstations	120
7.1.3	Removing Workstation Objects	120
7.2	Server Considerations	121
7.2.1	Selecting Servers for Deployment	121
7.2.2	Using DNS Names or Hosts Files	121
7.2.3	Scheduling Workstation Removal	122
8	Setting Up Automatic Workstation Import and Removal	123
8.1	Setting Up the Automatic Workstation Import and Removal Policies	124
8.1.1	Configuring the Automatic Workstation Import Policy	124
8.1.2	Configuring the Automatic Workstation Removal Policy	124
8.1.3	Associating the Server Package	124
8.2	Setting Up Automatic Workstation Import and Removal to Run on the Servers	124
8.3	Using the Novell Client and the ZENworks Desktop Management Agent	125
8.4	Verifying that Automatic Workstation Import and Removal are Working	125
9	Workstation Registration Files	127
9.1	Registration File Functions	127
9.2	Registration File Locations	127
9.3	Using Zwsreg.exe	127
9.4	Using Zenwsreg.dll	128
H	Documentation Updates	129
H.1	July 14, 2006 (Support Pack 1)	129
H.2	December 9, 2005	129

Part IV Workstation Management	131
10 Understanding Workstation Management	133
10.1 Workstation Management Components and Features	133
10.1.1 Components	134
10.1.2 Features	134
10.2 ZENworks Database	136
10.3 ZENworks Desktop Management Policies and Policy Packages	136
10.3.1 Policy Packages	137
10.3.2 ZENworks Desktop Management Policies	137
10.3.3 Plural Policies	138
10.3.4 Enabling Policies	138
10.3.5 Policy Scheduling	139
10.3.6 Policy Package Associations	139
10.3.7 Search Policy	140
10.3.8 Effective Policies	140
11 Creating Policy Packages	143
12 Setting Up the Search Policy in the Container Package	145
13 Setting Up Server Package Policies	149
13.1 Dictionary Update Policy	149
13.2 Imaging Server Policy	151
13.3 Inventory Roll-Up Policy	151
13.4 Workstation Import Policy	153
13.5 Workstation Removal Policy	159
13.6 ZENworks Database Policy	161
13.6.1 Configuring the ZENworks Database Object for Sybase	162
13.6.2 Configuring the ZENworks Database Object for Oracle	162
13.6.3 Setting Up the ZENworks Database Policy	163
13.7 Associating the Server Package	164
14 Setting Up Service Location Package Policies	165
14.1 SMTP Host Policy	165
14.2 SNMP Trap Targets Policy	166
14.3 XML Targets Policy	167
14.4 ZENworks Database Policy	168
14.5 Associating the Service Location Package	168
15 Setting Up User and Workstation Package Policies	169
15.1 Platform Pages	169
15.2 Computer/User Extensible Policies (Workstation/User Packages)	172
15.2.1 Understanding Extensible Policies	173
15.2.2 Configuring Extensible Policies	174
15.3 Dynamic Local User Policy (User Package)	177
15.4 Novell iPrint Policy (User and Workstation Packages)	182
15.5 Remote Control Policy (User and Workstation Packages)	187
15.6 Scheduled Action Policy (User and Workstation Packages)	187

15.7	User Extensible Policies (User Package)	190
15.8	Windows Desktop Preferences Policy (User Package)	190
15.9	Windows Group Policy (User and Workstation Packages)	192
15.9.1	Understanding the Windows Group Policy	193
15.9.2	Configuring the Windows Group Policy in the User Package	195
15.9.3	Configuring the Windows Group Policy in the Workstation Package	198
15.9.4	Editing Existing Windows Group Policies (User and Workstation Packages)	200
15.9.5	Importing Windows Group Policies (User and Workstation Packages)	202
15.10	Workstation Imaging Policy (Workstation Package)	204
15.11	Workstation Inventory Policy (Workstation Package)	204
15.12	ZENworks Desktop Management Agent Policy (Workstation Package)	204
15.13	Associating the User or Workstation Package	207
16	Generating Policy Reports	209
16.1	The Effective Policies Report	209
16.2	The Package Associations Report	209
17	Copying Policy Packages	211
17.1	Using the ConsoleOne Copy Policy Packages Utility	211
17.2	Using the Windows Copy Policy Packages Utility	211
18	Workstation Scheduler	213
18.1	Understanding Workstation Scheduler	213
18.1.1	Actions	213
18.1.2	Rights for Running Actions	214
18.1.3	Using the Scheduler in Windows 2000/XP	214
18.1.4	Microsoft SAGE Compatibility	214
18.2	Using Workstation Scheduler	214
18.2.1	Adding an Action	214
18.2.2	Adding an Action Item	216
18.2.3	Disabling or Enabling an Action	217
18.2.4	Disabling or Enabling an Action Item	217
18.2.5	Removing an Action	217
18.2.6	Removing an Action Item	217
18.2.7	Running an Action Immediately	217
18.2.8	Scheduling an Action to Run	218
18.2.9	Setting Advanced Action Properties	220
18.2.10	Viewing or Editing the Details or Properties of an Action	220
18.2.11	Viewing or Editing the Details or Properties of an Action Item	220
18.2.12	Viewing or Editing User-Defined Action Item Properties	221
I	Documentation Updates	223
I.1	July 14, 2006 (Support Pack 1)	223
I.1.1	Windows Group Policies	223
I.2	April 28, 2006	223
I.2.1	Dictionary Update Policy	224
I.2.2	Novell iPrint Policy (User and Workstation Packages)	224
I.3	February 28, 2006	224
I.3.1	ZENworks Windows Group Policy (User and Workstation Packages)	224
I.4	December 9, 2005	224
I.4.1	Setting Up User and Workstation Package Policies	224

Part V Application Management 227

19 Novell Application Launcher: Components Overview 229

19.1	Application Window	229
19.1.1	Application Window Description	230
19.1.2	What Users Can Do with the Application Window	230
19.1.3	Why Use the Application Window?	231
19.2	Application Explorer	231
19.2.1	Application Explorer Description	231
19.2.2	Why Use Application Explorer?	232
19.3	Application Browser	232
19.3.1	Application Browser Description	233
19.3.2	What Users Can Do with the Application Browser	233
19.3.3	Why Use the Application Browser?	234
19.3.4	Running the Application Browser Under Windows XP SP2 or Later	234
19.4	Application Launcher Engine	236
19.5	Application Launcher Service for Windows	236
19.6	Application Launcher Workstation Helper	237

20 Novell Application Launcher: Installing and Starting 239

20.1	Installing Application Launcher	239
20.2	Installing the Application Launcher Plug-In	239
20.3	Starting Application Launcher	240
20.3.1	Windows 2000/XP File System Rights	240
20.3.2	Manually Starting Application Launcher	240
20.3.3	Automating Application Launcher Startup	242
20.4	Using Application Launcher As the Windows Shell	243
20.4.1	Setting Up Application Launcher As the Shell on Windows 98	243
20.4.2	Setting Up Application Launcher As the Shell on Windows 2000/XP	243
20.5	Application Window Command Line Switches	244
20.6	Application Explorer Command Line Switches	251

21 Novell Application Launcher: Configuring Settings 255

21.1	How Configuration Settings Are Applied	255
21.2	Accessing the Application Launcher Configuration Settings	255
21.3	Configuring User Settings	258
21.4	Configuring Window Settings	263
21.5	Configuring Explorer Settings	265
21.6	Configuring Browser Settings	266
21.7	Configuring Workstation Settings	267
21.8	Designating the Top of a Configuration Tree	269

22 Novell Application Launcher: Customizing Views 271

22.1	Customizing the Application Window and Application Explorer Views	271
22.2	Customizing the Application Browser View	272
22.2.1	File Location	273
22.2.2	Modifying the Myapps.html and Axnalview.js Files	274
22.2.3	Creating a Refresh.html File	276
22.2.4	Creating an Hf_style.css File	277

23 Novell Application Launcher: Managing Authentication and File System Access	283
23.1 Novell eDirectory Authentication Overview	283
23.2 File System Access Overview	284
23.3 Authentication and File System Access for User-Associated Applications	285
23.3.1 Windows 98 (User-Associated Applications).	285
23.3.2 Windows 2000/XP (User-Associated Applications).	287
23.4 Authentication and File System Access for Workstation-Associated Applications	288
23.4.1 Windows 98 (Workstation-Associated Applications)	289
23.4.2 Windows 2000/XP (Workstation-Associated Applications)	290
 24 Novell Application Launcher: Managing the Cache	 293
24.1 NAL Cache Structure and Content	294
24.1.1 Launch Cache	294
24.1.2 Install Cache	296
24.2 File System Rights to the NAL Cache	296
24.3 Caching an Application	297
24.4 Changing the Cache Location	298
24.5 Disabling the Cache.	300
 25 Novell Application Launcher: Organizing Applications	 303
25.1 Types of Folders	303
25.2 Creating and Deleting Application Folders	304
25.3 Adding Applications to Application Folders	305
25.3.1 Using the Application Folder Object to Add Applications	306
25.3.2 Using the Application Object to Add the Application to a Folder	306
25.4 Adding Applications to Custom Folders.	307
 26 ZENworks Launch Gadget: Configuring Settings	 309
26.1 Modifying Gadget Configuration Settings	309
26.1.1 Configuring Gadget Settings on the ZENworks Application Page.	309
26.1.2 Configuring Gadget Settings on the Launch Gadget Object	310
26.1.3 ZENworks Launch Gadget (OD_ZENLaunchGadget) Settings.	310
26.2 Adding Citrix MetaFrame Servers to the Portal	311
 27 Distribution: Overview	 313
27.1 Application Types	313
27.2 User Associated vs. Workstation Associated.	313
 28 Distribution: Simple Applications	 315
28.1 Preparing a Simple Application	315
28.2 Configuring the Application in eDirectory.	316
28.3 Establishing File System Access	319
28.4 Establishing eDirectory Rights.	319
28.5 What's Next	320

29 Distribution: Complex Applications	321
29.1 Understanding Software Packages	321
29.1.1 Microsoft Windows Installer Packages	321
29.1.2 ZENworks snAppShot Packages	322
29.2 Preparing the Software Package	323
29.3 Configuring the Application in eDirectory	323
29.3.1 Creating an Application Object from a ZENworks snAppshot File	324
29.3.2 Creating the Application Object from a Windows Installer (.MSI) File	326
29.4 Establishing File System Access	329
29.5 Establishing eDirectory Rights	329
29.6 What's Next	329
30 Distribution: Terminal Server Applications	331
30.1 Preparing a Terminal Server Application	331
30.2 Configuring the Application in eDirectory	331
30.3 Establishing eDirectory Rights	334
30.4 What's Next	335
31 Distribution: Web Applications	337
31.1 Preparing a Web Application	337
31.2 Configuring the Application in eDirectory	337
31.3 Establishing eDirectory Rights	340
31.4 What's Next	340
32 Distribution: Applications to Terminal Servers	341
33 Advanced Distribution: Creating Distribution Rules	343
33.1 Types of Distribution Rules	343
33.2 AND/OR Boolean Operators and Groups	344
33.3 Distribution Rules vs. Legacy System Requirements	345
33.4 Distribution Rules Examples	346
33.4.1 Simple Rule Using an OR Operator	346
33.4.2 Simple Group	346
33.5 Creating Distribution Rules	347
33.6 Creating Distribution Rules by Importing Legacy System Requirements	348
33.6.1 Importing the Requirements When Opening the Distribution Rules Page	348
33.6.2 Importing the Requirements After Opening the Distribution Rules Page	350
33.7 Maintaining Legacy System Requirements	352
34 Advanced Distribution: Transferring Applications Using BITS	355
34.1 Understanding How Application Launcher Uses BITS	355
34.1.1 Application Launcher and BITS Process	356
34.1.2 Application Launcher Transfer vs. BITS Transfer	356
34.1.3 BITS Job Settings	356
34.1.4 BITS Maximum Bandwidth Setting	357
34.1.5 Scalability	357
34.2 Setting Up Workstations	357
34.3 Enabling Application Launcher to Use BITS	358
34.4 Configuring an Application to be Transferred by BITS	360

34.5	Changing the Default Settings for a BITS Job	361
34.6	Changing the BITS Maximum Network Bandwidth Setting	362
35	Advanced Distribution: Pre-Installing Applications	367
35.1	User-Associated Applications vs. Workstation-Associated Applications	367
35.2	Pre-Installing an Application Immediately	367
35.3	Scheduling an Application Pre-Install	370
36	Advanced Distribution: Configuring Fault Tolerance, Load Balancing, and Site Lists	377
36.1	Setting Up Fault Tolerance	377
36.1.1	Setting Up Fault Tolerance for MSI Applications	377
36.1.2	Setting Up Fault Tolerance for Simple or AOT/AXT Applications	378
36.2	Setting Up Load Balancing	381
36.2.1	Setting Up Load Balancing for MSI Applications	381
36.2.2	Setting Up Load Balancing for Simple or AOT/AXT Applications	383
36.3	Setting Up Site Lists	385
37	Advanced Distribution: Configuring Application Dependencies and Chains	389
37.1	Primary Applications vs. Dependent Applications	389
37.2	Application Chains	390
37.3	What Happens During the Distribution, Launch, and Uninstall of an Application That Has Dependencies	391
37.4	Adding an Application Dependency	392
37.5	Removing an Application Dependency	393
37.6	Deleting an Application That Has Dependencies	394
37.7	Creating an Application Chain	394
37.8	Viewing an Application Chain	395
38	Users: Supporting Terminal Server Users	397
38.1	Installing the RDP and ICA Clients	397
38.2	Determining Where Novell Application Launcher Runs	397
38.3	Managing Terminal Server User Accounts	398
38.4	Determining the Best Type of Application Objects and File Packages to Use When Distributing an Application	399
38.5	Ensuring Terminal Server Access Through a Firewall	400
39	Users: Supporting Disconnected Users	401
39.1	Disconnected Mode Overview	401
39.2	Configuring Applications as Disconnectable	403
39.3	Configuring Application Launcher to Start Automatically	404
39.4	Distributing Applications to Disconnected Workstations	404
40	Users: Supporting Remote Users	405
40.1	Configuring How Application Launcher Detects a Remote Connection	405
40.2	Disabling Applications	407
40.3	Establishing Alternate Applications	408

40.4	Distributing Applications	410
40.4.1	Adding Applications to the Cache	410
40.4.2	Distributing Applications Via Removable Media.	411
40.4.3	Enabling Checkpoint Restart for File Downloads.	411
41	Controlling Rogue Processes	415
41.1	What Rogue Process Management Does	415
41.2	How Rogue Process Management Works	415
41.3	Setting Up Rogue Process Management	416
41.3.1	Manually Modifying the Registry	416
41.3.2	Creating an Application Object to Distribute the Registry Modifications	418
42	Verifying Applications	423
42.1	How Application Launcher Detects Broken Applications	423
42.2	How Application Files are Verified	423
42.3	Why Automatic Verification Can Fail	423
42.4	Using Application Launcher to Verify an Application	424
43	Uninstalling Applications	425
43.1	Enabling an Application to be Uninstalled	425
43.2	Uninstalling Applications by Disassociating Users or Workstations	427
43.3	Uninstalling Unused Applications	428
43.4	Using Application Launcher to Uninstall an Application	429
43.5	Uninstalling Applications from Terminal Servers	430
44	Reporting Application Events	431
44.1	Setting Up Database Reporting	431
44.1.1	Installing the Sybase Database	432
44.1.2	Installing ODBC Drivers to Workstations	432
44.1.3	Creating a ZENworks Database Object	432
44.1.4	Configuring the Database's ODBC Information	434
44.1.5	Granting ODBC Property Rights to Users	435
44.1.6	Enabling the ZENworks Database Policy.	435
44.1.7	Configuring Application Objects to Use Database Reporting.	438
44.2	Setting Up SNMP Trap Reporting	438
44.2.1	Enabling Firewall Access	438
44.2.2	Enabling the SNMP Trap Targets Policy	438
44.2.3	Configuring Application Objects to Use SNMP Trap Reporting	441
44.3	Setting Up Log File Reporting	441
44.3.1	Setting Up a Common Log File Location	441
44.3.2	Configuring Application Objects to Use Log File Reporting	442
44.4	Setting Up XML Reporting	442
44.4.1	Meeting the Reporting Servlet Requirements	442
44.4.2	Installing the Reporting Servlet on Linux	443
44.4.3	Installing the Reporting Servlet on NetWare and Windows	443
44.4.4	Configuring the Reporting Servlet to be Used with an Apache Web Server	444
44.4.5	Configuring the Reporting Servlet to Write to the Database	444
44.4.6	Enabling the XML Targets Policy.	445
44.4.7	Configuring Application Objects to Use XML Reporting.	448
44.5	Configuring Applications to Use Reporting.	448
44.6	Generating Reports from a Database.	451

44.6.1	Predefined Reports	451
44.6.2	Custom Reports	451
44.6.3	Database Tables and Fields	452
44.7	Understanding Log File Reports	454
44.8	Enabling Windows Installer Verbose Logging	457
45	Metering Software Licenses	459
45.1	Installing Novell Licensing Services	459
45.2	Creating Metered Certificates	459
45.3	Installing the Novell Client and Licensing Files to Workstations	461
45.4	Configuring Applications to Use License Metering	461
46	Reference: AdminStudio ZENworks Edition	463
46.1	Installing AdminStudio ZENworks Edition	463
46.2	Using AdminStudio ZENworks Edition	464
47	Reference: ZENworks SnAppShot	465
47.1	Understanding SnAppShot	465
47.1.1	Application Object Templates	465
47.1.2	Application Source Files	466
47.1.3	Application File Definition File	466
47.1.4	SnAppShot Limitations	466
47.2	Preparing a SnAppShot Workstation	467
47.3	Creating an Installation Package	467
47.4	Command Line Switches	468
48	Reference: Application Object Settings	471
48.1	Identification Tab	471
48.1.1	Package Information Page	471
48.1.2	Icon Page	472
48.1.3	Description Page	475
48.1.4	Folders Page	475
48.1.5	Contacts Page	477
48.1.6	Administrator Notes Page	478
48.2	Distribution Options Tab	479
48.2.1	Icons/Shortcuts Page	479
48.2.2	Registry Page	482
48.2.3	Application Files Page	485
48.2.4	INI Settings Page	489
48.2.5	Text Files Page	493
48.2.6	Distribution Scripts Page	496
48.2.7	Pre-Install Schedule Page	499
48.2.8	Pre-Distribution Process Termination Page	503
48.2.9	Options Page	504
48.2.10	BITS Settings Page	507
48.3	Run Options Tab	509
48.3.1	Application Page	509
48.3.2	Environment Page	512
48.3.3	Launch Scripts Page	515
48.3.4	Environment Variables Page	518
48.3.5	Web URL	519
48.3.6	License/Metering Page	520

48.3.7	Application Dependencies Page	521
48.4	Associations Tab	524
48.4.1	Associations Page	524
48.5	Availability Tab	527
48.5.1	Distribution Rules Page	527
48.5.2	Schedule Page	543
48.5.3	Termination Page	546
48.6	Common Tab	548
48.6.1	Macros Page	549
48.6.2	Drives/Ports Page	551
48.6.3	File Rights Page	554
48.6.4	Reporting Page	556
48.6.5	Imaging Page	559
48.6.6	Sources Page	562
48.6.7	Uninstall Page	563
48.6.8	Uninstall Scripts Page	566
48.7	MSI Tab	568
48.7.1	Properties Page	569
48.7.2	Transforms Page	570
48.7.3	Verify Page	571
48.7.4	Patches Page	573
48.8	Terminal Server Client Tab	574
48.8.1	ICA Settings Page	574
48.8.2	RDP Settings Page	575
48.9	Fault Tolerance Tab	576
48.9.1	Fault Tolerance Page	576
48.9.2	Load Balancing Page	578
48.9.3	Site List Page	580
48.9.4	Remote Alternate App Page	582

49 Reference: Macros 585

49.1	Application Object Macros	585
49.1.1	Nesting Macros	586
49.1.2	Defining an Application Object Macro	586
49.2	Special Windows Macros	587
49.2.1	Windows 98 and Windows 2000/XP Macros	588
49.2.2	Windows 2000/XP Macros	589
49.3	Login Script Macros	590
49.3.1	Supported Login Script Identifier Variables	591
49.3.2	Unsupported Login Script Identifier Variables	592
49.4	eDirectory Attribute Macros	592
49.4.1	Syntax	592
49.4.2	Examples	593
49.5	Environment Variable Macros	594
49.6	Language Variable Macros	594
49.7	Macro Precedence	597
49.8	Application Object Properties Where Macros Can Be Used	597
49.8.1	Common Tab	597
49.8.2	Distribution Options Tab	598
49.8.3	MSI Tab	598
49.8.4	Run Options Tab	599
49.9	Refreshing Macro Information	599

50 Reference: Novell Application Launcher Tools	601
50.1 Export Application Object	601
50.2 Show Inherited Applications	601
50.3 Search and Replace	601
50.4 Manage Distribution GUIDs	602
50.5 AOT/AXT File Tools	603
50.6 Create Virtual CD	604
 51 Reference: Application Object Location	 609
51.1 Single Site	609
51.2 Multiple Sites	610
 52 Reference: Novell Application Launcher Authentication Hook	 611
52.1 Creating an Authentication Hook	611
52.2 Registering an Authentication Hook	612
52.3 Authentication Function (NWAPPAuthenticateExtern)	612
52.3.1 Syntax	612
52.3.2 Parameters	612
52.3.3 Return Values	613
52.3.4 Remarks	613
 J Documentation Updates	 615
J.1 July 14, 2006 (Support Pack 1)	615
J.1.1 Advanced Distribution: Transferring Applications Using BITS	615
J.1.2 Metering Software Licenses	616
J.1.3 Novell Application Launcher: Configuring Settings	616
J.1.4 Novell Application Launcher: Customizing Views	616
J.1.5 Novell Application Launcher: Installing and Starting	616
J.1.6 Novell Application Launcher: Managing the Cache	617
J.1.7 Reference: AdminStudio ZENworks Edition	617
J.1.8 Reference: Application Object Settings	617
J.1.9 Reference: ZENworks sNappShot	617
J.1.10 Reporting Application Events	618
J.2 February 28, 2006	618
J.2.1 Advanced Distribution: Pre-Installing Applications	618
J.2.2 Reference: Application Object Settings	618
J.2.3 Reporting Application Events	619
J.2.4 Setting Up Database Reporting	619
J.3 January 31, 2006	619
J.3.1 Configuring Applications to Use Reporting	620
J.3.2 Establishing File System Access	620
J.3.3 INI Settings	620
J.3.4 Installing Novell Licensing Services	620
J.3.5 Reference: Macros	620
J.3.6 Registry Settings	621
J.4 December 9, 2005	621
J.5 October 24, 2005	621
J.5.1 Reporting Application Events	621
J.6 September 30, 2005	621
J.6.1 Novell Application Launcher: Installing and Starting	621

Part VI Workstation and Server Imaging	623
53 Common Imaging Deployment Strategies	625
53.1 Installing a Standard Image Before Deploying New Workstations	625
53.2 Enabling Existing Workstations for Future Reimaging	626
53.3 Reimaging Corrupted Workstations	627
53.4 Restoring Lab or Classroom Workstations to a Clean State	627
54 Preparing a ZENworks Imaging Server	629
54.1 Imaging Server Prerequisites	629
54.2 Preparing an Imaging Server Where Automatic Workstation Import Is Not Installed	630
55 Preparing an Imaging Boot Method	631
55.1 Using Preboot Services (PXE)	631
55.1.1 If You Have Previously Installed a ZENworks partition	631
55.2 Preparing Imaging Boot CDs or DVDs	632
55.3 Using the ZENworks Imaging Floppy Boot Disk Creator	633
55.3.1 Starting the ZENworks Imaging Boot Disk Creator	633
55.3.2 Preparing a CD Boot Diskette	634
55.3.3 Configuring the Settings.txt File	634
55.3.4 Creating a PXE Disk	635
55.4 Creating an Imaging Hard-Disk Partition	635
56 Using ZENworks Desktop Management Preboot Services	637
56.1 Understanding Desktop Management Preboot Services	637
56.1.1 About Desktop Management Preboot Services	637
56.1.2 A Typical Preboot Services Operation	638
56.1.3 Illustrating the Preboot Services Processes for Linux Imaging Servers	639
56.1.4 Illustrating the Preboot Services Processes for NetWare and Windows Imaging Servers	646
56.2 Installing and Setting Up Desktop Management Preboot Services	649
56.3 Checking the Preboot Services Server Setup	649
56.3.1 Overview of Preboot Services Components	650
56.3.2 Checking Imaging Server Setup	651
56.3.3 Setting up Standard DHCP and Proxy DHCP Services on the Same Server	652
56.4 Deploying Desktop Management Preboot Services in a Network Environment	654
56.4.1 Server Configurations	655
56.4.2 Network Configuration	657
56.4.3 Configuring Filters on Switches and Routers	667
56.4.4 Spanning Tree Protocol in Switched Environments	667
56.5 Enabling PXE on a Workstation	668
56.5.1 Enabling PXE on a PXE-Capable Workstation	668
56.5.2 Verifying That PXE Is Enabled on a Workstation	669
56.5.3 If a Workstation Is Not PXE Capable	669
56.6 Administering Desktop Management Preboot Services	670
56.6.1 Configuring Preboot Services Servers in Linux	670
56.6.2 Configuring Preboot Services Servers in NetWare	671
56.6.3 Configuring Preboot Services Servers in Windows	673
56.6.4 Configuring IP Port Usage	676
56.7 Using the Desktop Management Preboot Services PXE-on-Disk Utility	677
56.7.1 What Is PXE-on-Disk Setup?	677

56.7.2	Creating a PXE-on-Disk Diskette	678
56.7.3	Booting with a PXE-on-Disk Diskette	681
56.7.4	If PXE-on-Disk Fails to Operate Correctly	681
56.8	Editing the Desktop Management Preboot Services Menu	681
56.8.1	Editing the Preboot Services Menu on Linux	682
56.8.2	Understanding the Windows-based Preboot Services Menu Editor	684
56.8.3	Editing the Preboot Services Menu on Windows	685
57	Setting Up Workstations for Imaging	693
57.1	Windows Workstation Requirements	693
57.2	Enabling a Windows Workstation for Auto-Imaging Operations	694
58	Setting Up Imaging Policies	697
58.1	Defining an Imaging Policy for Unregistered Workstations (Server Policy)	697
58.2	Defining an Imaging Policy for Registered Workstations (Workstation Policy)	699
58.3	Allowing Overwriting Filenames and Restricting the Save Location of Image Files (Imaging Server Settings)	701
59	Creating and Restoring Images	703
59.1	Creating a Workstation (Base) Image	703
59.2	Creating an Add-On Image	704
59.3	Using Image Explorer to Customize an Image	704
59.4	Making an Image Available for Automatic Imaging	706
59.4.1	Creating a Workstation Image Object	706
59.4.2	Associating an Add-On Image with a Base Image	707
59.4.3	Using a File Set of an Image	708
59.5	Performing an Automatic Imaging Creation or Restoration	709
60	Performing Manual Imaging Operations	711
60.1	Manually Taking an Image of a Workstation	711
60.1.1	Using the Bash Prompt to Manually Take an Image of a Workstation	711
60.1.2	Using the ZENworks Imaging Engine Menu to Manually Take an Image of a Workstation	713
60.2	Manually Putting an Image on a Workstation	715
60.2.1	Using the Bash Prompt to Manually Put an Image on a Workstation	715
60.2.2	Using the ZENworks Imaging Engine Menu to Manually Put an Image on a Workstation	717
61	Setting Up Disconnected Imaging Operations	719
61.1	Using a CD or DVD for Disconnected Imaging Operations	719
61.1.1	Using the Bash Prompt to Put Down an Image	719
61.1.2	Using the ZENworks Imaging Engine Menu to Put Down an Image	720
61.2	Using a Hard Disk or Jaz Drive for Disconnected Imaging Operations	721
61.2.1	Creating an Image on a Hard Disk or Jaz Drive	721
61.2.2	Putting Down an Image from a Hard Disk or Jaz Drive	723
62	Multicasting Images	725
62.1	Understanding Multicasting	725
62.1.1	Benefits of Multicasting Images	725

62.1.2	Limitations of Multicasting Images	726
62.2	Performing a Multicast Session	726
62.2.1	Initiating an Automatic Multicast Session in ConsoleOne	726
62.2.2	Performing a Manual Multicast Session	729

63 Imaging Utilities and Components 737

63.1	Image Explorer (imgexp.exe)	737
63.1.1	Starting Image Explorer (Imgexp.exe)	738
63.1.2	Opening an Image	739
63.1.3	Adding a File or Folder to an Open Image	739
63.1.4	Creating a Folder in an Open Image	739
63.1.5	Adding Specific Windows Registry Settings That Are to Be Applied After the Open Image Is Laid Down	739
63.1.6	Excluding a File or Folder from the Open Image	739
63.1.7	Marking a File or Folder for Deletion in the Open Image	739
63.1.8	Purging Files and Folders Marked for Deletion from the Open Image	740
63.1.9	Extracting a File or Directory from the Open Image to a Folder	740
63.1.10	Extracting a File or Directory from the Open Image as an Add-On Image	740
63.1.11	Viewing a File from the Open Image in its Associated Application	740
63.1.12	Saving Your Changes to the Open Image	740
63.1.13	Creating a Workstation Add-On Image	740
63.1.14	Adding a Partition to a New Add-On Image	741
63.1.15	Compressing an Image	741
63.1.16	Splitting an Image	742
63.1.17	Resizing a Partition in an Image	742
63.2	ZENworks Imaging Windows Agent (Ziswin.exe)	743
63.2.1	Understanding the ZENworks Imaging Windows Agent	743
63.2.2	Running the ZENworks Imaging Windows Agent in Interactive Mode	745
63.2.3	Running the ZENworks Imaging Windows Agent in Service Mode	750
63.2.4	Running the ZENworks Imaging Windows Agent in Installation Mode	753
63.2.5	Running the ZENworks Imaging Windows Agent in Uninstallation Mode	753
63.3	Image-Safe Data Viewer and Editor (Zisview and Zisedit)	754
63.3.1	Information Displayed by the Image-Safe Data Viewer	755
63.3.2	Image-Safe Data Viewer	756
63.3.3	Image-Safe Data Editor	757
63.4	Imaging Floppy Boot Disk Creator (zimboot.exe)	758
63.5	Imaging Configuration Parameters (Settings.txt)	758
63.6	Imaging Boot Parameters	761
63.7	Imaging Server (Imgserv.nlm or .dll or .dlm, or Linux Daemons)	761
63.7.1	Initiating the Imaging Processes on Linux Imaging Servers	762
63.7.2	Initiating the Imaging Processes on Windows or NetWare Imaging Servers	769
63.7.3	Viewing Information About Imaging Requests	769
63.7.4	Starting a Manual Multicast Session	770
63.8	Imaging Server Log (Zimglog.xml)	770

64 ZENworks Imaging Engine Commands 773

64.1	Help Mode (img help)	774
64.2	Auto Mode (img auto)	774
64.3	Make Mode (img make)	775
64.3.1	Make Locally (img makel)	776
64.3.2	Make on Proxy (img makep)	777
64.4	Restore Mode (img restore)	778
64.4.1	Restore from Local (img restorel)	779
64.4.2	Restore from Proxy (img restorep)	780

64.5	Session (Multicast) Mode (img session)	782
64.6	Partition Mode (img p)	784
64.6.1	Using the ZENworks Imaging Engine Menu	784
64.6.2	Using the Bash Prompt	785
64.7	ZENPartition Mode (img zenPartition)	786
64.8	Dump Mode (img dump)	786
64.9	Information Mode (img info)	787
65	Updating ZENworks Imaging Resource Files	789
65.1	The Linux Distribution for Imaging	789
65.2	Understanding Device Boot Processes in a ZENworks Imaging Environment	790
65.2.1	linuxrc	791
65.2.2	zenworks.s	792
65.3	Understanding ZENworks Partitions and Command Line Parameters	792
65.3.1	The ZENworks Partition	792
65.3.2	Command Line Parameters and Variables	792
65.4	Modifying ZENworks Imaging Resource Files	793
65.4.1	Adding Files to an Imaging Boot CD	794
65.4.2	Adding Files to the Initrd or Root File Systems	794
65.4.3	Using the Driverupdate File Method	796
65.5	Adding or Updating LAN Drivers	796
65.5.1	Obtaining Drivers	796
65.5.2	Building Drivers	796
65.5.3	Loading Drivers with Parameters	798
65.6	Using Uname	798
65.7	Variables and Parameters	799
65.7.1	Imaging Script Variables	800
65.7.2	Linuxrc Parameters Specified in Settings.txt	800
65.7.3	Image Engine Variables	801
65.8	Troubleshooting Linux Driver Problems	801
65.8.1	Troubleshooting During the Boot Process	801
65.8.2	Troubleshooting at the Bash Prompt	802
66	Supported Ethernet Cards	803
67	Accessing IP Addresses for Devices Running Dual NICs	805
K	Documentation Updates	807
K.1	July 14, 2006 (Support Pack 1)	807
K.1.1	Imaging Utilities and Components	808
K.1.2	Multicasting Images	808
K.1.3	Preparing an Imaging Boot Method	808
K.1.4	Preparing a ZENworks Imaging Server	809
K.1.5	Server Imaging	809
K.1.6	Updating ZENworks Imaging Resource Files	809
K.1.7	Using ZENworks Desktop Management Preboot Services	809
K.2	December 9, 2005	810
K.2.1	Updating ZENworks Imaging Resource Files	810
Part VII	Remote Management	811

68 Understanding Remote Management	813
68.1 Remote Management Terminology	813
68.2 Understanding the Remote Management Components	814
68.2.1 Understanding Remote Control	814
68.2.2 Understanding Remote View	814
68.2.3 Understanding Remote Execute	814
68.2.4 Understanding Remote Diagnostics	815
68.2.5 Understanding File Transfer	815
68.2.6 Understanding Remote Management Auditing	815
68.2.7 Understanding the Remote Management Events using Windows Event Viewer	815
68.2.8 Understanding Remote Wake Up	816
 69 Setting Up Remote Management	 817
69.1 Remote Management Deployment Strategies	817
69.1.1 Password-Based Remote Management	817
69.1.2 Directory-Based Remote Management	818
69.2 Configuring the Remote Management Policy for the Registered Workstations	819
69.3 Configuring the Remote Management Policy for Non-Registered Workstations	822
69.4 Setting Up the Remote Management Agent Password	822
69.5 Assigning Rights to the Remote Operator	822
69.5.1 Assigning Rights Using the Remote Operator Wizard	822
69.5.2 Assigning Rights Using the Remote Operators Tab	823
69.6 Operating with Windows XP Service Pack 2	823
69.7 Starting Remote Management Operations Using ConsoleOne	824
69.7.1 Initiating a Directory-Based Remote Management Session	824
69.7.2 Initiating a Password-Based Remote Management Session	825
69.7.3 Initiating Remote Management Session from the Remote Management Agent	827
69.8 Starting Remote Management Operations Without Using ConsoleOne	827
69.8.1 Launching User-Based Remote Management Using Desktop4.exe	829
69.9 Configuring Remote Management Ports	830
69.9.1 Configuring the Remote Management Agent Port	830
69.9.2 Configuring the Remote Control Listener Port	830
69.9.3 Customizing the Permission Message	831
 70 Managing Remote Workstations	 833
70.1 Managing a Remote View Session	833
70.1.1 Controlling the Display of the Viewing Window	833
70.1.2 Using the Viewing Window Accelerator Keys	834
70.1.3 Defining a Custom Accelerator Key Sequence	836
70.2 Managing a Remote Control Session	836
70.2.1 Controlling the Display of the Viewing Window	836
70.2.2 Using the Viewing Window Accelerator Keys	838
70.2.3 Using the Toolbar Buttons on the Viewing Window	839
70.2.4 Enabling the Wallpaper on the Managed Workstation	840
70.2.5 Obtaining Information About Remote Management Sessions	841
70.2.6 Obtaining General Information	841
70.2.7 Obtaining Security Information	841
70.3 Managing a Remote Execute Session	842
70.4 Managing a File Transfer Session	842
70.4.1 Using File Transfer Window Controls	842
70.5 Managing a Remote Wake Up Session	844
70.5.1 Prerequisites	844
70.5.2 Remotely Waking Up the Managed Workstations	844

70.5.3	Setting Up a Scheduled Remote Wake Up Using the Wake-on-LAN Policy	844
70.5.4	Starting and Stopping the Wake-on-LAN Service	845
70.6	Viewing the Audit Log of Remote Management Sessions Using the Windows Event Viewer	846
70.6.1	Understanding the Audit Log	847
70.7	Remote Operator Identification Display	849
70.8	Managing a Remote Management Audit Session	850
70.8.1	Viewing the Audit Logs from a Centralized Database	851
70.9	Generating Remote Management Reports	851
70.9.1	Prerequisites for Generating Remote Management Reports	852
70.9.2	Generating a Remote Management Report	852
70.9.3	Printing a Remote Management Report	853
70.9.4	Exporting a Remote Management Report to a File	853
70.10	Improving the Remote Management Performance	853
70.11	Using the Remote Management Agents	854
70.11.1	Shutting Down the Remote Management Agent	854
70.11.2	Restarting the Remote Management Agent	855
70.11.3	Using the Remote Management Agent Icon	855
71	Viewing the Diagnostic Information	857
71.1	Viewing Diagnostic Information for a Managed Workstation	858
71.2	Windows Memory Information	860
71.3	Environment Information	860
71.4	Event Log Information	861
71.5	Device Drivers Information	862
71.6	Services Information	862
71.7	WIN32 Process Information	862
71.8	WIN32 Modules Information	863
71.9	NetWare Connections Information	863
71.10	Novell Client Information	864
71.11	Network Protocols Information	864
71.12	Name Space Providers Information	865
71.13	Network Drives Information	865
71.14	Network Open Files Information	866
71.15	Print Capture Information	867
L	Documentation Updates	869
L.1	July 14, 2006 (Support Pack 1)	869
L.1.1	Setting Up Remote Management	869
L.2	December 9, 2005	870
Part VIII	Workstation Inventory	871
72	Understanding Workstation Inventory	873
72.1	Workstation Inventory Terminology	873
72.2	Overview of Inventory Components	874
72.2.1	Inventory Scanners	875
72.2.2	Inventory Components on Servers	875
72.2.3	Inventory Database	876
72.2.4	Management Console	876
72.3	Understanding Inventory Scanning Cycle	876
72.4	Understanding the Inventory Server Roles	876

72.4.1	Root Server	877
72.4.2	Root Server with Inventoried Workstations	878
72.4.3	Intermediate Server	878
72.4.4	Intermediate Server with Database	879
72.4.5	Intermediate Server with Inventoried Workstations	880
72.4.6	Intermediate Server with Database and Inventoried Workstations	881
72.4.7	Leaf Server.	882
72.4.8	Leaf Server with Database.	883
72.4.9	Standalone Server	884
72.4.10	Quick Reference Table of the Inventory Server Roles.	885
73	Setting Up Workstation Inventory	887
73.1	Deploying Workstation Inventory	887
73.1.1	Simple Deployment	887
73.1.2	Advanced Deployment.	890
73.1.3	Deploying the Inventory Agent.	910
73.1.4	Understanding the Effects of Workstation Inventory Installation	913
73.1.5	Starting and Stopping the Inventory Service	915
73.1.6	Checking the Status of the Workstation Inventory Components Installed on Linux.	917
73.1.7	Changing the Role of the Inventory Server	917
73.2	Setting Up the Inventory Database.	929
73.2.1	Setting Up the Sybase Inventory Database.	929
73.2.2	Setting Up the Oracle Inventory Database.	935
73.2.3	Setting Up the MS SQL Server 2000 or MS SQL Server 2005 Inventory Database.	945
73.3	Configuring the Inventory Service Object.	955
73.4	Changing the ScanDir Path for a Linux Inventory Server.	956
73.5	Configuring the Database Location Policy	957
73.6	Configuring the Workstation Inventory Policy.	958
73.7	Configuring the Roll-Up Policy	960
73.8	Configuring the Dictionary Update Policy.	961
73.9	Setting Up Distribution of Dictionary.	962
74	Understanding Workstation Inventory Components	965
74.1	Understanding the Inventory Service Manager	965
74.1.1	List of Services.	966
74.1.2	Services on NetWare Inventory Servers	966
74.1.3	Services on Windows Servers	967
74.1.4	Services on Linux Inventory Servers	967
74.2	Understanding the Server Configuration Service.	968
74.3	Understanding the Inventory Scanner	968
74.3.1	Inventory Scanning Process	969
74.3.2	Types of Scan	969
74.3.3	Scanning for the Hardware Inventory Information	970
74.3.4	Scanning for the Software Inventory Information.	971
74.3.5	Inventory Scanner Log Files	974
74.4	Understanding the Sender and Receiver	974
74.4.1	Understanding the Sender	975
74.4.2	Understanding the Receiver.	975
74.4.3	Understanding the Compressed Scan Data File	976
74.4.4	Sender-Receiver Directories	976
74.5	Understanding the TCP Receiver.	978
74.6	Understanding the Selector	979
74.7	Understanding the Storer	981
74.8	Understanding the Str Converter	981

74.9	Understanding the Inventory Sync Service	982
74.10	Understanding Dictionary Provider and Dictionary Consumer.	983
74.11	Understanding the Upgrade Service	983
74.11.1	Inventory Database Migration	984
74.11.2	Conversion and Movement of ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management Residue Files.	984
74.12	An Overview of the Inventory Components on an Inventory Server	985
74.13	Understanding the Inventory Database	986
75	Understanding the Inventory Database Schema	987
75.1	Overview	987
75.2	CIM Schema	988
75.2.1	CIM-to-Relational Mapping	991
75.2.2	Logical Schema.	992
75.2.3	Physical Schema.	994
75.3	Inventory Database Schema in ZENworks 7 Desktop Management.	995
75.3.1	Case Study of CIM Schema Implementation in ZENworks 7 Desktop Management	995
75.3.2	Legends for Schema Diagrams.	997
75.3.3	Schema Diagrams of CIM and the Extension Schema in ZENworks 7 Desktop Management	998
75.3.4	Custom Inventory Schema	1006
75.3.5	Software Inventory Schema	1008
75.3.6	Sample Inventory Database Queries	1012
76	Managing Your Inventory System	1021
76.1	Viewing the Servers Deployed for Inventory	1021
76.2	Customizing the Hardware Inventory Information To Be Scanned	1022
76.2.1	Customizing the Hardware Inventory Scanning of Inventoried Workstations	1022
76.2.2	Scanning for IBM Computer Models	1030
76.2.3	Customizing the Hardware Scanning Information of Jaz, Zip, and Floppy Drive Vendors.	1031
76.2.4	Scanning for Vendor-Specific Asset Information from DMI.	1032
76.2.5	Customizing the Hardware Information for Monitor Size.	1033
76.3	Customizing the Software Inventory Information To Be Scanned For ZENworks 7 Inventoried Workstations	1035
76.3.1	What is the ZENworks Software Dictionary?.	1036
76.3.2	What is a Software Dictionary Rule?.	1036
76.3.3	What is a Software Identifier?	1036
76.3.4	What is a Key Identifier?	1037
76.3.5	What is Unidentified Software?	1037
76.3.6	What is an Inherited Rule?	1037
76.3.7	What is an Overriding Rule?	1037
76.3.8	Understanding the Usage and Precedence of ZENworks Software Dictionary Rules.	1037
76.3.9	Understanding the Software Dictionary Pattern Types	1044
76.3.10	Configuring the Software Dictionary Rules	1045
76.3.11	Ignore Default File-Software Mapping Rules.	1048
76.3.12	Software Dictionary	1048
76.3.13	Report Files with These File Extensions As Unidentified Software.	1052
76.3.14	Manage Unidentified Software	1053
76.3.15	Report Multiple Software Versions	1054
76.3.16	Report Disk Space Used by File Extensions.	1056
76.3.17	Software Scanning Filters - Drives and Directories.	1057
76.3.18	Software Scanning Filters - File Extensions	1062
76.3.19	Software Scanning Filters - Files.	1064

76.3.20	Software Scanning Filters - Software	1065
76.3.21	Disk Usage Scanning Filters - Drives and Directories	1067
76.3.22	Disk Usage Scanning Filters - Files	1071
76.3.23	Vendor Name Aliases	1072
76.3.24	Software Name Aliases	1074
76.3.25	Reconcile Software	1075
76.3.26	Sorting Entries in the Table	1076
76.3.27	Filtering Entries in the Table	1076
76.3.28	Refreshing Entries in the Table	1077
76.3.29	Disabling File Scan	1077
76.3.30	Base-Lining the Software Dictionary Deployment	1078
76.3.31	Viewing Software Information in the Inventory Summary	1079
76.3.32	Generating Software Inventory Reports	1079
76.4	Customizing the Software Inventory Information To Be Scanned For ZENworks for Desktops 4.x and Earlier Versions of Inventoried Workstations	1081
76.5	Scanning for Workstations That Are Periodically Connected to the Network	1081
76.6	Scanning for Workstations That Are Never Connected to Your Network	1081
76.6.1	Prerequisites	1082
76.6.2	Collecting Inventory for Workstations That Are Not Connected to the Network	1082
76.6.3	Limitations	1084
76.7	Removing Redundant Inventoried Workstations from the Inventory Database	1084
76.7.1	Understanding the NDS Lookup for DB Utility	1086
76.8	Removing Duplicate Workstation Objects from the Inventory Database	1086
76.8.1	Running the Dupremove Utility	1087
76.8.2	Understanding the Dupremove Switches	1088
77	Viewing Inventory Information	1095
77.1	Viewing the Inventory Information Using ConsoleOne	1095
77.1.1	Configuring the Inventory Database	1096
77.1.2	Viewing the Inventory Summary of an Inventoried Workstation	1096
77.1.3	Viewing Inventory Information by Querying the Database	1109
77.1.4	Viewing the Minimal Inventory Information from an eDirectory Object	1112
77.1.5	Running Inventory Reports	1113
77.1.6	Quickly and Easily Viewing the Inventory Data Using Quick Reports	1127
77.2	Exporting the Inventory Information	1138
77.2.1	Procedure to Export the Inventory Information	1138
77.2.2	Loading an Existing Configuration File	1141
77.2.3	Running the Data Export Program From the Inventory Server	1142
77.2.4	An Overview of XML and the Contents of an XML File	1143
77.3	Viewing Inventory Information Without Using ConsoleOne	1145
77.4	Retrieving Inventory information from the Inventory Database Without Using the CIM Schema	1148
77.4.1	List of Inventory Views	1148
77.4.2	How to Use the Inventory Views	1174
78	Monitoring Workstation Inventory Using Status Logs	1177
78.1	Viewing the Scan History of an Inventoried Workstation	1177
78.2	Viewing the Scan Status of an Inventoried Workstation	1178
78.3	Viewing the Roll-Up History of the Server	1179
78.4	Viewing the Status of Inventory Components on a Server	1179
78.5	Viewing the Status of the Last Scan in the Workstation Scan Log	1180
78.6	Viewing the Roll-Up Log for Servers	1181
78.7	Status Logs and Scan Logs Overview	1182
78.8	Viewing the Status Log in XML Format	1182

M	Performance Tips	1185
M.1	Database Parameter Tuning Tips	1185
M.1.1	Sybase in the NetWare, Windows, or Linux Environment	1185
M.1.2	Oracle in the NetWare, Windows, or Linux Environment	1188
M.1.3	Optimizing the Performance of the Oracle Database	1189
M.1.4	MS SQL in the Windows Environment	1190
M.2	Improving the Throughput of the Inventory Storer	1191
M.2.1	Factors to be Considered Before Deployment	1191
M.2.2	Procedure to Improve the Throughput	1191
M.2.3	Recommendations for Administering the ZENworks Inventory Server	1193
M.2.4	Recommendations for Administering the Inventory Database	1194
M.3	Performance Tips for the Inventory Server (Support Pack 1).	1194
M.4	Performance Tips for the Inventory ConsoleOne Utilities	1196
M.4.1	Inventory Reports Performance Tips.	1197
M.4.2	Inventory Data Export Performance Tips	1197
M.4.3	Inventory Query Performance Tips	1197
M.5	References	1198
N	Hardware Information Collected by the Inventory Scanners	1199
O	ZENworks 7 Desktop Management Inventory Attributes	1211
P	Enumeration Values	1237
P.1	Enumeration Values for General-System Information-Management Technology	1237
P.2	Enumeration Values for General-Inventory Information-Scan Mode	1238
P.3	Enumeration Values for Software-Operating Systems-Windows - Name	1238
P.4	Enumeration Values for Installation Repository	1238
P.5	Enumeration Values for Hardware-Display Adapter-Video Architecture	1239
P.6	Enumeration Values for Hardware-Display Adapter-Video Memory Type	1239
P.7	Enumeration Values for Hardware-Pointing Device-Name	1239
P.8	Enumeration Values for Hardware-Battery-Chemistry	1239
P.9	Enumeration Values for Hardware-Processor-Processor Family	1240
P.10	Enumeration Values for Hardware-Processor-Upgrade Method	1240
P.11	Enumeration Values for Hardware-Chassis-Chassis Type	1240
P.12	Enumeration Values for Hardware-Bus-Protocol Supported	1241
P.13	Enumeration Values for Hardware-Processor-Role	1241
P.14	Enumeration Values for System-System Cache-Level	1241
P.15	Enumeration Values for System-System Cache-Cache Type	1241
P.16	Enumeration Values for System-System Cache-Replacement Policy	1241
P.17	Enumeration Values for System-System Cache-Read Policy	1242
P.18	Enumeration Values for System-System Cache-Write Policy	1242
P.19	Enumeration Values for System-System Cache-Associativity	1242
P.20	Enumeration Values for System-System IRQ-Availability	1242
P.21	Enumeration Values for System-System IRQ-IRQ Trigger Type	1242
P.22	Enumeration Values for System-System DMA-Availability	1243
P.23	Enumeration Values for Language	1243
Q	Documentation Updates	1247
Q.1	July 14, 2006 (Support Pack 1)	1247
Q.1.1	Appendix L: Performance Tips	1247

Q.1.2	Managing Your Inventory System	1248
Q.1.3	Setting Up Workstation Inventory	1248
Q.1.4	Viewing Inventory Information	1248
Q.2	December 23, 2005	1249
Q.2.1	Appendix L: Performance Tips	1249
Q.2.2	Deploying Workstation Inventory	1249
Q.2.3	Managing Your Inventory System	1249
Q.2.4	Viewing Inventory Information	1249
Q.3	December 9, 2005	1250
Q.3.1	Setting Up Workstation Inventory	1250
Q.3.2	Understanding Workstation Inventory Components	1250
Q.3.3	Viewing Inventory Information	1250
Q.4	September 30, 2005	1251
Q.4.1	Setting Up Workstation Inventory	1251

About This Guide

This *Administration* guide consists of comprehensive, conceptual information that you can use as you configure and use Novell® ZENworks® 7 Desktop Management components in your production environment. The sections include:

- Part I, “Understanding ZENworks 7 Desktop Management,” on page 31
- Part II, “Checking the ZENworks Desktop Management Installation,” on page 97
- Part III, “Automatic Workstation Import and Removal,” on page 117
- Part IV, “Workstation Management,” on page 131
- Part V, “Application Management,” on page 227
- Part VI, “Workstation and Server Imaging,” on page 623
- Part VII, “Remote Management,” on page 811
- Part VIII, “Workstation Inventory,” on page 871

Audience

This guide is intended for network administrators and IT professionals with responsibility for managing workstations in their corporate enterprise.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html (<http://www.novell.com/documentation/feedback.html>) and enter your comments there.

Documentation Updates

Check the [ZENworks 7 Desktop Management Documentation Web site](http://www.novell.com/documentation/beta/zenworks7/) (<http://www.novell.com/documentation/beta/zenworks7/>) for documentation updates.

Additional Documentation

For information about the installing, planning, setting up, testing, and upgrading processes that Novell ZENworks 7 Desktop Management customers typically encounter while implementing this product, see the *ZENworks 7 Desktop Management Installation Guide* (<http://www.novell.com/documentation/beta/zenworks7/dm7install/data/front.html>).

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux or UNIX, should use forward slashes as required by your software.

Understanding ZENworks 7 Desktop Management

This section of the Administration guide introduces the major parts of Novell® ZENworks® 7 Desktop Management and explains how they work together.

- Chapter 1, “Understanding the Novell Client,” on page 33
- Chapter 2, “Understanding the Desktop Management Agent,” on page 37
- Chapter 3, “Understanding the ZENworks Middle Tier Server and the Desktop Management Server,” on page 47
- Chapter 4, “Understanding the ZENworks Multiple UNC Provider,” on page 61
- Chapter 5, “Process Flow in ZENworks Desktop Management,” on page 65
- Appendix A, “Implementing a DHCP Option for Delivering the Middle Tier Server Address,” on page 73
- Appendix B, “Using a ZENworks Tree,” on page 75
- Appendix C, “E-Mail and Dotted Name Login Support,” on page 81
- Appendix D, “Using the Novell Kerberos KDC to Support ZENworks Dynamic Local Users,” on page 85
- Appendix E, “Ports Used by ZENworks 7 Desktop Management,” on page 91
- Appendix F, “Documentation Updates,” on page 93

Understanding the Novell Client

1

Since the first release of Novell® ZENworks® Desktop Management (formerly called “ZENworks for Desktops”), the Novell Client™ has been an integral part of delivering zero-effort networking (ZEN) to the user's desktop. The client enables the user's Windows* workstation to securely access network resources, including NetWare® and Windows 2000/2003 servers, security, and network printers. It also integrates NetWare services such as file and print, object management in the directory, drive mapping, browsing network servers and printers, user administration on network servers, establishing rights, login scripts, and so on.

With ZENworks 7 Desktop Management, the Novell Client is not mandatory on a user's workstation because the Desktop Management Agent performs all of the functions needed to manage a workstation. For more information about the Desktop Management Agent, see [Chapter 2, “Understanding the Desktop Management Agent,” on page 37](#)

This section includes the following information:

- [Section 1.1, “The Role of the Novell Client,” on page 33](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

1.1 The Role of the Novell Client

ZENworks 7 Desktop Management supports the Novell Client for Windows 98 workstations (version 3.4 and later) and the Novell Client for Windows 2000/XP workstations (version 4.9 SP1a and later). When installed on workstations, earlier versions of the Novell Client (that is, the client versions used prior to ZENworks for Desktops 4) included many of the ZENworks Desktop Management components, but that is no longer the case.

Beginning with ZENworks for Desktops 4, the ZENworks Desktop Management Agent has been responsible for installing ZENworks components on user workstations, making the Desktop Management Agent a required component for ZENworks Desktop Management.

The following sections provide information about the continuing role of the Novell Client in Desktop Management functionality.

- [“The Novell Client and ZENworks Desktop Management Installation” on page 33](#)
- [“The Novell Client and ConsoleOne Administration” on page 34](#)
- [“Using the Novell Client in a ZENworks 7 Environment” on page 34](#)

1.1.1 The Novell Client and ZENworks Desktop Management Installation

When you install the Desktop Management Server and the ZENworks Middle Tier Server, the installing workstation must have the required version of the Novell Client installed. The client establishes communication between the workstation and eDirectory™, making it possible for either of the two installation programs to recognize and display eDirectory trees and server objects that

help you visualize where to install Desktop Management software. For more information, see the *Novell ZENworks 7 Desktop Management Installation Guide*.

Upgrading from Earlier Versions of ZENworks

If you intend to perform an upgrade to ZENworks 7 from ZENworks 6.5 or ZENworks for Desktops 4.x, workstations in your environment already have the ZENworks Desktop Management Agent installed (even if users routinely use the Novell Client to log in) along with Novell Application Launcher™ components. This makes it simple to use the Application Launcher to upgrade the Desktop Management Agent. For more information, see “[Upgrading Workstations](#)” in the “[Upgrading from ZENworks for Desktops 4.x](#)” section of the *Novell ZENworks 7 Desktop Management Installation Guide*.

1.1.2 The Novell Client and ConsoleOne Administration

Novell ConsoleOne® is a Java*-based tool used to manage your network and its resources. By default, it lets you manage:

- eDirectory objects, schema, partitions, and replicas
- NetWare server resources

When you install the Desktop Management Server, the eDirectory schema is extended to include several directory objects unique to Desktop Management, including workstations, applications, databases, and policy packages. The capabilities to configure these objects are snapped in to the ConsoleOne structure.

You can install and run ConsoleOne locally on a Windows workstation or server, or you can install it remotely on a NetWare or Windows server and run it through a mapped or shared drive pointing to that server. The Novell Client must be installed on the Windows workstation or server where you will be running ConsoleOne for administering ZENworks Desktop Management. This is because ConsoleOne is dependent on the client's NetWare libraries. For more information, see the [ConsoleOne 1.3x User Guide \(http://www.novell.com/documentation/lg/console13/index.html?page=/documentation/lg/console13/c1_enu/data/hk42s9ot.html\)](http://www.novell.com/documentation/lg/console13/index.html?page=/documentation/lg/console13/c1_enu/data/hk42s9ot.html) at the Novell Product Documentation Web site.

1.1.3 Using the Novell Client in a ZENworks 7 Environment

With ZENworks 7 Desktop Management, the Novell Client is not mandatory on a user's workstation because the Desktop Management Agent makes it possible for users to authenticate to the Desktop Management Server and benefit from ZENworks functionality when outside the corporate firewall. For more information about the Desktop Management Agent, see [Chapter 2, “Understanding the Desktop Management Agent,” on page 37](#).

The Desktop Management Agent is not a replacement for the Novell Client. For more information about using the Novell Client in a NetWare environment, see the [Novell Client documentation Web site \(http://www.novell.com/documentation-index/index.jsp\)](http://www.novell.com/documentation-index/index.jsp).

If the Novell Client and the Desktop Management Agent are both installed on a workstation, the workstation login defaults to the Novell Client and all of the NetWare file system and eDirectory access is through the client.

NOTE: Users outside the firewall who have both the agent and the client installed on their workstations must use an alternative login method and will receive applications only, not Desktop Management policies. For more information about the alternative login method for authenticating to eDirectory outside the firewall when both the client and agent are installed, see [“Logging in Locally to the Workstation” on page 68](#).

Understanding the Desktop Management Agent

2

This section contains information you can use to help you gain a high-level understanding of the role of the Desktop Management Agent and how it works.

- [Section 2.1, “What is the Desktop Management Agent?” on page 37](#)
- [Section 2.2, “Getting Ready to Use the Desktop Management Agent,” on page 37](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

2.1 What is the Desktop Management Agent?

Novell® ZENworks® 7 Desktop Management requires the Desktop Management Agent. With this agent installed, users who log in directly with the Novell Client™ can use ZENworks 7 Desktop Management directly, while users in an all-Windows environment or users on workstations located outside of the corporate network firewall can log in and authenticate the workstation through the ZENworks Middle Tier Server to Novell eDirectory™ using port 80 over HTTP or port 443 over HTTPS.

IMPORTANT: The Desktop Management Agent must be installed on every workstation where you want to deploy ZENworks 7 Desktop Management functionality. This includes workstations where the Novell Client is already installed.

When authenticated with the proper credentials, the workstation receives the distributed applications, schedules, policies, and various workstation inventory, remote management, and Workstation Imaging enabling files as designated by you, the administrator.

The Desktop Management Agent includes functionality for login and authentication, packaging, sending, and receiving XML requests over HTTP or HTTPS.

2.2 Getting Ready to Use the Desktop Management Agent

This section includes information you need to know if you plan to deploy the Desktop Management Agent in your network environment:

- [“Desktop Management Agent Installation Considerations” on page 38](#)
- [“Upgrading the Desktop Management Agent” on page 38](#)
- [“Modifying the Desktop Management Agent Login” on page 38](#)
- [“Setting Up AutoAdminLogon for Windows 2000/XP” on page 39](#)

2.2.1 Desktop Management Agent Installation Considerations

Make sure that the workstations where you install the Desktop Management Agent meet the minimum requirements for hardware and installed software. For more information, see “[User Workstation Requirements](#)” in “[Preparation](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

The Desktop Management Agent installation lets you install various Desktop Management components on a one-time basis; that is, if you want to add or delete any of the components installed by the Agent in an earlier installation, you can use the Modify option that is available in the maintenance dialog box of the Desktop Management Agent setup.

2.2.2 Upgrading the Desktop Management Agent

The version of the Desktop Management Agent that shipped with the original *ZENworks for Desktops 4 Program* CD (`setup.exe`) is no longer supported. You must not attempt to upgrade from that version of the Desktop Management Agent.

You can upgrade the ZENworks for Desktops 4.0.1 Desktop Management Agent (and its functionality) and the ZENworks 6.5 Desktop Management Agent by installing the ZENworks 7 Desktop Management Agent.

Installing version 7 of the agent uninstalls older versions of the agent and enables ZENworks 7 functionality on your managed workstations.

For more information, see “[Upgrading Workstations](#)” in “[Upgrade](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

2.2.3 Modifying the Desktop Management Agent Login

If you want to modify the Desktop Management Agent for your network users, you can do so when you create the Desktop Management Agent installation for the workstations and after you import the workstations. This section includes information for both options:

- “[Modifying the Login Dialog](#)” on page 38
- “[Creating Custom Bitmaps for the Graphical Interface](#)” on page 38

Modifying the Login Dialog

If the Novell Client is not present on the installing workstation when you are installing the Desktop Management Agent, the installation program displays the Workstation Manager Settings dialog box. This dialog box can be customized. For more information about the customization options, see “[Customizing the Agent Login](#)” in “[Setting Up Authentication](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

Creating Custom Bitmaps for the Graphical Interface

If you deploy the Desktop Management Agent in your network environment, you can customize the login GINA (that is, the graphical interface used for authentication) and the Welcome dialog box with your own company identity. To replace the Novell bitmaps on the Desktop Management Agent Login dialog box or the Resident Workstation Welcome dialog box, use the Workstation Policy Package > Desktop Management Agent policy. For more information, see [Section 15.12](#),

“ZENworks Desktop Management Agent Policy (Workstation Package),” on page 204. The workstation must be imported into the eDirectory tree in order for these dialog boxes to access the customized bitmaps. When you change the bitmaps that are accessed through this policy, the new graphics are accessed when the scheduled system event occurs. The Login dialog box bitmap is sized at 390 x 75 pixels and the Welcome dialog box bitmap is sized at 320 x 195 pixels. The Welcome dialog box attribute is stored in the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\NWGINA
```

The Login dialog box attribute is stored in the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\LgnXtier
```

NOTE: You can also log in from the Application Explorer in the Windows system tray. The graphical interface of this login GINA cannot be customized. For more information, see “Logging in Locally to the Workstation” on page 68.

2.2.4 Setting Up AutoAdminLogon for Windows 2000/XP

You can automate the logon process for selected Windows 2000/XP users by using the Windows Registry Editor (`regedit.exe`) to enter user ID and password credentials in the Registry database. The result for the user is immediate access to the desktop and network resources without the need to pause to enter logon information.

NOTE: You can bypass the AutoAdminLogon process and log on as a different user by holding down the Shift key after a logout or after a workstation reboot.

Using AutoAdminLogon opens your network to a serious security risk. It exposes user IDs and passwords and it lets any user who starts the workstation use the embedded credentials to obtain access to the workstation and network files—even if the workstation is locked. We recommend that you review the Microsoft* recommendations regarding when to use AutoAdminLogon before you implement it. For more information, see [TID 10052847 \(http://support.novell.com/cgi-bin/search/tidfinder.cgi?10052847\)](http://support.novell.com/cgi-bin/search/tidfinder.cgi?10052847) at the [Novell Support Web site \(http://support.novell.com\)](http://support.novell.com).

IMPORTANT: If you install the Novell Client 4.9 SP1a for Windows 2000/XP on a workstation that already has the Desktop Management Agent installed and then set up AutoAdminLogon, you receive a login error because of a conflict between AutoAdminLogon and Novell Modular Authentication Services (NMAS™), installed by default by Novell Client 4.9 SP1a.

To work around the problem after the Client is installed, right-click the red N icon in the desktop system tray > click *Novell Client Properties* > *Advanced Login* > deselect *NMAS Authentication*.

This section contains the following information:

- “General Procedure for Setting Up AutoAdminLogon” on page 39
- “AutoAdminLogon Options” on page 40
- “Changing Passwords in NetWare Login with AutoAdminLogon” on page 45

General Procedure for Setting Up AutoAdminLogon

- 1 Start the Registry Editor (`regedit.exe`).

WARNING: Using the Registry Editor incorrectly can cause serious, system-wide problems that might require reinstalling Windows 2000/XP to correct them.

- 2 Locate the specified Registry keys and set the values as indicated.

If a value does not exist, click *Edit > New > String Value*, type the name of the value, then press Enter. All the values should be string values except for AutoAdminQueryNDS, which must be a DWORD value instead of a string value.

IMPORTANT: For a Windows logon only, if no DefaultPassword string is specified, the value of the AutoAdminLogon key automatically changes from 1 (True) to 0 (False), disabling the AutoAdminLogon feature after the first autoadminlogon session has occurred.

- 3 Exit the Registry Editor and log out of Windows 2000/XP.

AutoAdminLogon Options

This section lists the options you can choose from when you set up AutoAdminLogon.

- “Logon to Workstation Only: Client Only, Agent Only, or Both Client and Agent Installed” on page 40
- “Logon to Workstation and eDirectory: Client Only, or Both Client and Agent Installed” on page 41
- “Logon to Workstation and eDirectory: Agent Only Installed” on page 42
- “Login to NetWare Only Using Dynamic Local User (DLU) for Windows: Client Only, or Both Client and Agent Installed” on page 43
- “Logon to NetWare Only Using Dynamic Local User (DLU) for Windows: Agent Only Installed” on page 43
- “Logon to Windows and Query for NetWare: Client Only Installed” on page 44

In addition to these options for setting up AutoAdminLogon, you can also disable it. For more information, see “[Disable AutoAdminLogon](#)” on page 45. You should also be careful to use these options only for setting up user names and passwords if you want AutoAdminLogon to work properly. Be careful to caution users against resetting their own passwords. For more information, see “[Changing Passwords in NetWare Login with AutoAdminLogon](#)” on page 45.

Logon to Workstation Only: Client Only, Agent Only, or Both Client and Agent Installed

Use this option to allow users to go directly to the desktop when the workstation boots. Users are not authenticated to eDirectory. The effect is similar to the user authenticating by checking the *Workstation Only* check box in the Windows logon dialog box.

Table 2-1 *Settings for Using AutoAdminLogon: Logging on to the Workstation Only*

Registry Key	String Name	Enter This Value
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon	AutoAdminLogon	1
	DefaultDomain	Name of Domain
		or
		Name of Local Workstation
	DefaultUserName	Windows User Name
	DefaultPassword	Windows Password for the DefaultUserName specified above
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login	AutoAdminLogon	0

Logon to Workstation and eDirectory: Client Only, or Both Client and Agent Installed

Use this option to allow users to go directly to the desktop upon workstation bootup. No login prompts for Windows authentication or eDirectory authentication (Client or Agent) are displayed. Users are authenticated to eDirectory and to the Windows workstation. All Desktop Management policies and applications are delivered to the workstation.

Table 2-2 *Settings for using AutoAdminLogon: Logging in to the Workstation and eDirectory with the Novell Client Only Installed or with the Novell Client and ZENworks Agent Installed*

Registry Key	String Name	Enter This Value
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon	AutoAdminLogon	1
	DefaultDomain	Name of Domain
		or
		Name of Local Workstation
	DefaultUserName	Windows User Name
	DefaultPassword	Windows Password for the DefaultUserName specified above

Registry Key	String Name	Enter This Value
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login	AutoAdminLogon	1
	DefaultLocationProfile	Name of the Location Profile that contains the information about the Novell User to log in to the NetWare network such as Username, Tree, Context, Server, etc.
	DefaultPassword	Novell Password for the DefaultUserName specified in the Location Profile

Location profiles let you save a user's specific login information. The profile automatically sets up login information such as the user's name, server, tree, context, login script, and other applicable information so that the user does not need to type this information.

NOTE: The NT Credential information in the Location Profile is not used. The NT user information in the registry is used instead.

Logon to Workstation and eDirectory: Agent Only Installed

Use this option to allow users to go directly to the desktop upon workstation bootup. No login prompts for Windows authentication or eDirectory authentication are displayed. Users are authenticated to eDirectory and to the Windows workstation. All Desktop Management policies and applications are delivered to the workstation.

Table 2-3 Settings for using AutoAdminLogon: Logging in to the Workstation and eDirectory with the ZENworks Agent Only Installed

Registry Key	String Name	Enter This Value
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon	AutoAdminLogon	1
	DefaultDomain	Name of Domain or Name of Local Workstation
	DefaultUserName	Windows User Name
	DefaultPassword	Windows Password for the DefaultUserName specified above

Registry Key	String Name	Enter This Value
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login	AutoAdminLogon	1
	DefaultUserName	The fully-distinguished name (DN) or the common name (CN) portion of the DN that the Novell User uses to log in to eDirectory. Example: bjones or bjones.sales.novell
	DefaultPassword	Novell Password for the DefaultUserName specified in the DefaultUserName string.

Login to NetWare Only Using Dynamic Local User (DLU) for Windows: Client Only, or Both Client and Agent Installed

Use this option to allow users to go directly to the desktop upon workstation bootup. Users are authenticated to eDirectory according to the credentials entered in the registry, but they are authenticated to the Windows workstation according to the configuration of the DLU policy (no credentials for Windows are entered in the registry).

Table 2-4 Settings for using AutoAdminLogon: Logging in to NetWare Using DLU, Client Only or Both Client and Agent Installed

Registry Key	String Name	Enter This Value
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon	AutoAdminLogon	0
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login	AutoAdminLogon	1
	DefaultLocationProfile	Name of the Location Profile that contains the information about the Novell User to log in to the NetWare network, such as Username, Tree, Context, Server.
	DefaultPassword	Novell Password for the DefaultUserName specified in the Location Profile

Location profiles allow you to save a user's specific login information. The profile automatically sets up login information such as the user's name, server, tree, context, login script, and other applicable information so that the user does not need to type this information. In this case, the location profile must specify an eDirectory user with Dynamic Local User (DLU) privileges on the Windows 2000 workstation.

Login to NetWare Only Using Dynamic Local User (DLU) for Windows: Agent Only Installed

Use this option to allow users to go directly to the desktop upon workstation bootup. Users are authenticated to eDirectory according to the credentials entered in the registry, but they are

authenticated to the Windows workstation according to the configuration of the DLU policy (no credentials for Windows are entered in the registry).

Table 2-5 *Settings for using AutoAdminLogon: Logging in to NetWare Using DLU, Agent Only Installed*

Registry Key	String Name	Enter This Value
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon	AutoAdminLogon	0
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login	AutoAdminLogon	1
	DefaultUserName	The fully-distinguished name (DN) or the common name (CN) portion of the DN that the Novell User uses to log in to eDirectory. Example: bjones or bjones.sales.novell
	DefaultPassword	Novell Password for the DefaultUserName specified in the DefaultUserName string.

Logon to Windows and Query for NetWare: Client Only Installed

The following settings are applicable only if the workstation has only the Novell Client installed. They are not applicable if only the Desktop Management Agent is installed.

This option authenticates the user to the Windows workstation according to the credentials entered in the registry, but the login to NetWare requires the user to enter his or her eDirectory credentials.

Table 2-6 *Settings for using AutoAdminLogon: Logging on to Windows, Client Only Installed*

Registry Key	String Name	Enter This Value
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon	AutoAdminLogon	1
	DefaultDomain	Name of Domain
	or	or
	Local WorkstationName	Name of Local Workstation
	DefaultUserName	Windows User Name
	DefaultPassword	Windows Password for the DefaultUserName specified above

Registry Key	String Name	Enter This Value
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login	AutoAdminLogon	0
	AutoAdminQueryNDS	1
IMPORTANT: AutoAdminQueryNDS must be a DWORD value instead of a string value.		

Disable AutoAdminLogon

This is the behavior setting for logon to the Windows workstation and to eDirectory. The user is prompted for Windows workstation credentials and eDirectory credentials in order to authenticate.

Table 2-7 Settings for using AutoAdminLogon: Disabling for Logon

Registry Key	String Name	Enter This Value
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon	AutoAdminLogon	0
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login	AutoAdminLogon	0

Changing Passwords in NetWare Login with AutoAdminLogon

Novell Client Precautions

If AutoAdminLogon is enabled, be careful when running the NetWare Login utility from the icon in the NetWare (Common) group. When run as a standalone utility from the icon, NetWare Login does not recognize that the workstation is running AutoAdminLogon.

If the primary connection's password expires when running NetWare Login from the icon, the user is given the chance to synchronize all NetWare and Windows passwords. Make sure that users do not synchronize the Windows password, because NetWare Login does not update the Registry setting for AutoAdminLogon.

Desktop Management Agent Precautions

Although you can change the login password for the Desktop Management Agent using an applet in the Windows Control Panel, doing so doesn't affect the password setting in the Windows registry. If you change the password using the applet but you don't change it in the registry, AutoAdminLogon settings fail.

Understanding the ZENworks Middle Tier Server and the Desktop Management Server

This section contains information you can use to help you gain a high-level understanding of the role of the Novell® ZENworks® 7 Middle Tier Server and the Desktop Management Server and how to prepare to use them.

- [Section 3.1, “What Is the ZENworks Middle Tier Server?,” on page 47](#)
- [Section 3.2, “Getting Ready to Use the ZENworks Middle Tier Server,” on page 47](#)
- [Section 3.3, “What Is the Desktop Management Server?,” on page 57](#)
- [Section 3.4, “Getting Ready to Use the Desktop Management Server,” on page 58](#)

3.1 What Is the ZENworks Middle Tier Server?

The ZENworks Middle Tier Server is installed on a Windows server, a NetWare® server, or a Linux where a Web server (that is, Windows IIS on a Windows server or the Apache Web server on a NetWare server, OES Linux server, or a SLES 9 SP1 server) is already installed. The modules of the Middle Tier Server plug in to the Web server software and act as a Web service. The Middle Tier Server allows access to Novell eDirectory™ and the Windows file system (if running on a Windows server), the NetWare file system (if running on a NetWare server), or the Linux file system (if running on a SLES 9.x, SLES 10 (only on ZENworks 7 with SP1), or OES Linux server) for the users and workstations inside or outside the firewall.

Using ZENworks Desktop Management through the Desktop Management Agent and the Middle Tier Server, users can access their applications and policies through a Web server interface. For diagrams showing how the Middle Tier Server works, see [Chapter 5, “Process Flow in ZENworks Desktop Management,” on page 65](#).

3.2 Getting Ready to Use the ZENworks Middle Tier Server

The ZENworks Middle Tier Server can be installed on NetWare 6, NetWare 6.5, Windows 2000 servers, Windows Server 2003, SLES 9.x, SLES 10 (only on ZENworks 7 with SP1), or OES Linux platforms. The following sections provide details on where to find additional information about the prerequisites, installation steps, and configuration for the Middle Tier Server:

- [“Preparing for the Middle Tier Server” on page 48](#)
- [“Installing ZENworks Middle Tier Server” on page 48](#)
- [“Configuring the ZENworks Middle Tier Server with NSAdmin” on page 48](#)

3.2.1 Preparing for the Middle Tier Server

It is important that you understand the procedure for preparing to install the Middle Tier Server. We recommend that you review the following documentation:

- “[Platform Support for the Desktop Management Infrastructure](#)” in “[Overview](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.
- “[Prerequisites for the Workstation Running the Installation](#)” in “[Preparation](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.
- “[ZENworks Middle Tier Server Limitations](#)” in “[Preparation](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

This documentation includes information that details the limitations of the ZENworks Middle Tier Server, hardware and software requirements, and other installation prerequisites.

If you plan to install the ZENworks Middle Tier Server on a SLES 9.x server, a SLES 10 server (only on ZENworks 7 with SP1), or OES Linux server, see “[Preparing a Linux Server for ZENworks Functions](#)” in “[Preparation](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

3.2.2 Installing ZENworks Middle Tier Server

The procedure you should use for installing ZENworks Middle Tier Server software on a Windows or NetWare server is detailed in “[Installing the ZENworks Middle Tier Server](#)” and “[Installing the Desktop Management Server and the Middle Tier Server on the Same Machine](#)” in “[Windows-Based Installation](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

The options you can use for installing ZENworks Middle Tier Server software on a SLES 9.x, SLES 10 (used for ZENworks 7 with SP1 only), or OES Linux server are detailed in “[Installing ZENworks Desktop Management Services on Linux](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

3.2.3 Configuring the ZENworks Middle Tier Server with NSAdmin

When the ZENworks Middle Tier Server software is installed, it creates new registry entries on the machine where it is installed. If you want to edit or configure the configuration parameters, you can edit the registry of the NetWare or Windows server where the ZENworks Middle Tier server is installed, or you can use the NSAdmin utility to change the configuration.

IMPORTANT: Use caution when changing NetWare registry settings. Some NetWare registry entries should be changed only under direction from Novell. Changing the entries could adversely affect the Middle Tier Server, NetStorage, ZENworks Desktop Management, and your NetWare server.

You can invoke the interface of the NSAdmin utility by opening Internet Explorer and entering the NSAdmin URL in the Address box. For example:

`http://ip_address or dns_name/oneNet/nsadmin`

IMPORTANT: Do not use a browser other than Internet Explorer (for example, Mozilla Firefox) to run the NSAdmin utility. Other browsers cannot run NSAdmin successfully.

It is not necessary to restart Tomcat or Apache or any other service in order for the changes made in NSAdmin to take effect.

If you are running the server on a port number other than port 80, use the following syntax to run the utility:

`http://ip_address or dns_name:port/oneNet/nsadmin`

If you run the server on a port number other than port 80, make sure that when you install the Desktop Management Agent, you configure the IP address for the Middle Tier Server accordingly.

The NSAdmin Web page displays a list of links in the left column that are used to access the various pages for editing and viewing Middle Tier Server configuration information in the registry. Descriptions and information for each NSAdmin page are described in the following sections.

- “General” on page 50
- “Authentication Domains (Xtier 2.6.2 installation)” on page 52
- “Authentication Domains (Xtier 3.1x Installation)” on page 53
- “WebDav Provider” on page 54
- “iFolder Storage Provider” on page 55
- “NetWare Storage Provider” on page 55
- “Current Sessions” on page 55
- “Resource Usage” on page 56
- “Statistics” on page 57

IMPORTANT: The appearance and functionality of the NSAdmin *Authentication Domains* page varies according to the version of the ZENworks Middle Tier Server you install.

- ZENworks 7 Middle Tier Server installed on NetWare and Windows servers uses Xtier 2.6.2 (see “Authentication Domains (Xtier 2.6.2 installation)” on page 52)
- ZENworks 7 Middle Tier Server installed on Linux servers uses Xtier 3.1 (see “Authentication Domains (Xtier 3.1x Installation)” on page 53)
- ZENworks 7 Middle Tier Server with SP1 installed on NetWare, Windows, or Linux servers uses Xtier 3.1.4 (see “Authentication Domains (Xtier 3.1x Installation)” on page 53)

Please consult the appropriate documentation to understand the differences between these versions of the Middle Tier.

General

The General page of the NSAdmin utility is the default display.

Figure 3-1 The General Page of the NSAdmin Utility

The screenshot shows the NetStorage web interface in Microsoft Internet Explorer. The left sidebar contains the following links: Manage Middle Tier Server, Help, General, Authentication Domains, Manage NetStorage, WebDAV Provider, iFolder Storage Provider, NetWare Storage Provider, Sessions, Current Sessions, Middle Tier Server Usage, Resource Usage, and Statistics. The main content area displays a table of configuration settings with columns: Name, Type, Location, Default Value, and Value. The table contains the following rows:

Name	Type	Location	Default Value	Value
Proxy Username	NSADMIN_PASSWORD	XTier\Configuration\Xsrv		<input type="text"/>
Proxy Password	NSADMIN_PASSWORD	XTier\Configuration\Xsrv		<input type="text"/>
Location	REG_SZ	XTier\Configuration\Xsrv	/oneNet	<input type="text" value="/oneNet"/>
Certificate Name	REG_SZ	XTier\Configuration\Xsrv	SSL CertificateDNS	<input type="text" value="SSL CertificateDNS"/>
Session Timeout	REG_DEC_DWORD	XTier\Configuration\Xsrv	258	<input type="text" value="600"/>
Janitor Interval	REG_DWORD	XTier\Configuration\Xsrv	320	<input type="text" value="320"/>
Persistent Cookies	REG_DWORD	XTier\Configuration\Xsrv	0	<input type="text"/>
LDAP Port	REG_DEC_DWORD	XTier\Configuration\Xsrv	389	<input type="text"/>

At the bottom of the table are two buttons: Submit and Set Defaults.

This page lets you view or edit the following configuration settings:

Proxy Username and Proxy Password: This is the admin username and password that you entered when you installed your Middle Tier Server. If you want the Middle Tier Server to use a different username and password for administrator access, enter it in the fields provided.

If you click the *Set Defaults* button, the value is set to whatever value appears in the *Default Value* column. If there is no value in the *Default Value* column, the value is set to blank (no value).

Location: This is the registered location you want users to enter as part of the Middle Tier Server URL to access the ZENworks Middle Tier Server. The default is oneNet.

If you change this registry setting on a ZENworks Middle Tier Server installed on NetWare, you must also edit a configuration file for the change to take effect. Edit the `sys:\netstorage\xsrv.conf` file and change the `/oneNet` setting in the *Location* section (first section) to the same setting you specified in NSAdmin.

Certificate Name: NetIdentity is the default certificate name. It is created automatically during the Middle Tier Server installation. If you purchased a certificate that you want to use or if you just want to use a different certificate, enter the certificate name in this field.

Any certificates used by the Middle Tier Server should reside in the same eDirectory context.

Session Timeout: This is the amount of time in seconds that the session will remain idle before it is terminated. If there is no Middle Tier Server activity for this amount of time, the user is required to log in again to the Middle Tier Server before being allowed file access.

Janitor Interval: This setting should not be changed except under direction from Novell.

Persistent Cookies: The *Persistent Cookies* setting can be turned on or off. With the value set to 0, *Persistent Cookies* is turned off. *Persistent Cookies* is turned on (the default) if there is no value or if the value is set to anything other than 0.

With *Persistent Cookies* turned off, the NetStorage or ZENworks Desktop Management session ends when the user closes the current browser or Web folder. Also, if the user has a current instance of ZENworks Desktop Management or NetStorage up in a browser window or Web folder and starts up a new browser instance or Web folder, the user is required to reauthenticate.

Turning off *Persistent Cookies* can be beneficial if you have workstations that are shared because as long as the browser instance is closed down, the next user of the workstation cannot accidentally or intentionally obtain access to your network through ZENworks Desktop Management or NetStorage.

Leaving *Persistent Cookies* turned on can be beneficial if your workstations are not shared because it prevents users from having to unnecessarily re-authenticate.

If the user selects the *Logout* option in NetStorage or ZENworks Desktop Management, the session ends regardless of whether *Persistent Cookies* is turned on or off.

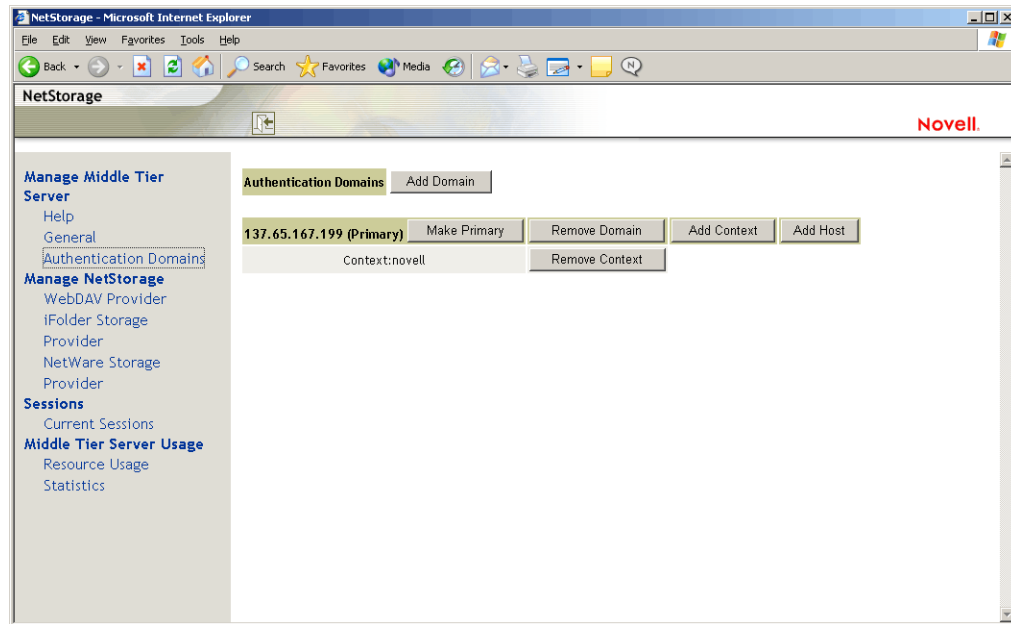
LDAP Port: Lets you change the LDAP port number if there is a conflict between Active Directory* and eDirectory for LDAP requests.

This conflict exists because the back end server is acting as a domain controller, which has Active Directory installed on it. The conflict is created by both eDirectory and Active Directory attempting to use the same default port (the default port number is 389). Active Directory normally wins the conflict. The Proxy User object type exists in eDirectory but not in Active Directory. Because of this, when the Middle Tier Server tries to bind as a Proxy User, the bind attempt fails. This is also the reason LDAP lookups fail.

Authentication Domains (Xtier 2.6.2 installation)

The Authentication Domains page lets you change or add the eDirectory server URLs and contexts that are required by the ZENworks Middle Tier Server. If you installed the ZENworks 7 Middle Tier Server on a Windows or NetWare server, it will look like this:

Figure 3-2 The Authentication Domains Page of the NSAdmin Utility when the Middle Tier Server's Xtier Kernel, version 2.6.2, is Installed



This page also lets you change the eDirectory server that is designated as the Primary. For more information about eDirectory server URLs and contexts, see the *NetStorage Administration Guide* (<http://www.novell.com/documentation/lg/nw6p/index.html?page=/documentation/lg/nw6p/netstor/data/h9izvdye.html>) at <http://www.novell.com/documentation/lg/nw6p>.

The following list identifies the functions of the buttons on the Authentication Domains page:

Add Domain: Lets you add another eDirectory server IP address or DNS name.

Make Primary: Makes the eDirectory server URL listed above the button the Primary.

Remove Domain: Removes the eDirectory server URL from the list of URLs used by the Middle Tier Server.

Remove Context: Removes the context (if there is one) from the eDirectory server URL.

Add Context: Lets you add a context to the eDirectory server URL.

Add Host: Lets you list additional hosts for an Authentication Domain. Clicking the *Add Hosts* button lets you create a list of alternative hosts for the domain.

If the ZENworks Middle Tier Server cannot reach the host specified in the domain, it searches the *Other Hosts* list specified in the value field to find another server to use for authentication.

Enter DNS names or IP addresses of alternate servers separated by a comma delimiter in the *Value* field. For example, you could enter a string similar to the following:

Zenmaster.provo.novell.com,Zenmaster1.provo.novell.com

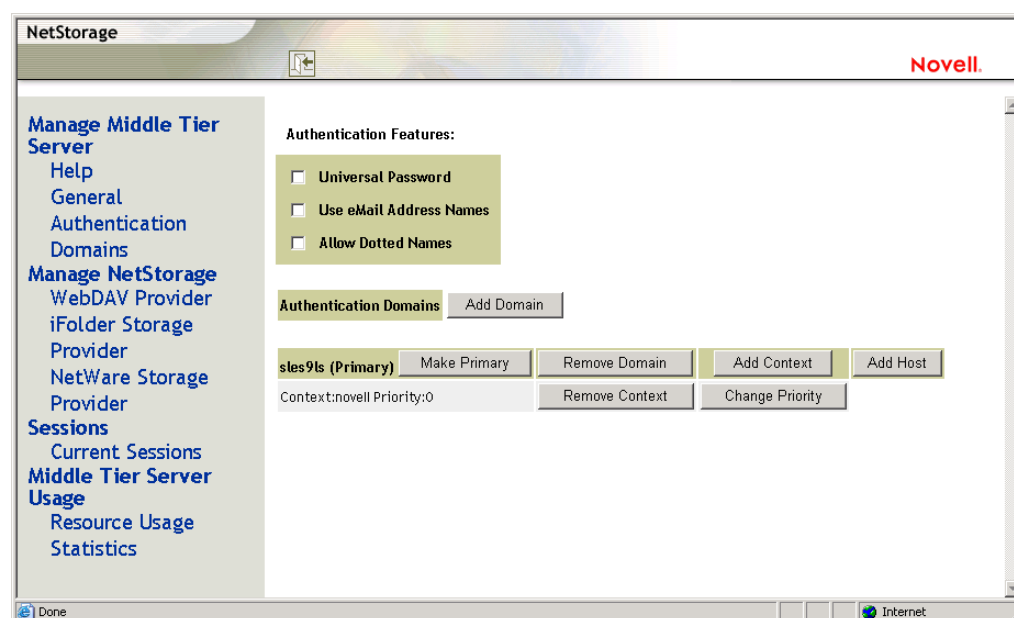
or

137.65.67.150,137.65.67.152

Authentication Domains (Xtier 3.1x Installation)

If you install the ZENworks 7 Middle Tier Server on a SLES 9.x server or on an OES Linux server, or if you install the ZENworks 7 with SP1 Middle Tier Server, the underlying Xtier kernel, version 3.1x (versus the Xtier version 2.6.2 installed with ZENworks 7 for Middle Tier installations on Windows and NetWare) displays an Authentication Domains page that looks like this:

Figure 3-3 Authentication Domains Page of the NSAdmin Utility when the Middle Tier Server's Xtier Kernel, version 3.1 and later, is Installed



The Authentication Domains page lets you change or add the eDirectory server URLs and contexts that are required by the ZENworks Middle Tier Server.

For more information about eDirectory server URLs and contexts, see the [NetStorage Administration Guide](http://www.novell.com/documentation/lg/nw6p/index.html?page=/documentation/lg/nw6p/netstor/data/h9izvdy.html) (<http://www.novell.com/documentation/lg/nw6p/index.html?page=/documentation/lg/nw6p/netstor/data/h9izvdy.html>) at <http://www.novell.com/documentation/lg/nw6p>.

The following list identifies the functions of the buttons on the Authentication Domains page:

Universal Password: Select this check box if you want to enable Universal Password.

Use eMail Address Names: Select this check box if you want to enable e-mail address names. This allows users to log in to the network through the ZENworks Middle Tier Server by using the same syntax they might be accustomed to when sending e-mail.

Although ZENworks 7 Desktop Management does not enable e-mail or dotted name logins by default (because of the complex process used by the Middle Tier Server to find the user and because

of the network traffic this process might generate), both login methods can be used for authentication when using the Desktop Management Agent.

Authentication contexts configured for the Middle Tier must not contain any embedded dots.

NOTE: In ZENworks 7 Desktop Management with SP1, this check box is still present, but is non-functional. E-mail address name support is automatically enabled with this release.

Allow Dotted Names: Select this check box if you want to enable dotted name support. This functionality (dotted-name support) applies for the user name only, not the user's context. The ZENworks Middle Tier Server does not support authentication to a dotted name in the root context of the eDirectory tree: that is, authentication contexts configured for the Middle Tier must not contain any embedded dots. For more information, see TID 10098582 in the [Novell Support Knowledgebase \(http://support.novell.com/search/kb_index.jsp\)](http://support.novell.com/search/kb_index.jsp).

NOTE: In ZENworks 7 Desktop Management with SP1, this check box is still present, but is non-functional. Dotted name support is automatically enabled with this release.

Add Domain: Lets you add another eDirectory server IP address or DNS name.

Make Primary: Designates the eDirectory whose URL is displayed as the primary eDirectory server.

Remove Domain: Removes the eDirectory server URL from the list of URLs used by the Middle Tier Server.

Add Context: Lets you add a context to the eDirectory server URL.

Add Host: Lets you list additional hosts for an Authentication Domain. Clicking the *Add Hosts* button lets you create a list of alternative hosts for the domain.

If the ZENworks Middle Tier Server cannot reach the host specified in the domain, it searches the *Other Hosts* list specified in the *Value* field to find another server to use for authentication.

Enter DNS names or IP addresses of alternate servers separated by a comma delimiter in the *Value* field. For example, you could enter a string similar to the following:

Zenmaster.provo.novell.com,Zenmaster1.provo.novell.com

or

137.65.67.150,137.65.67.152

Remove Context: Removes the context (if there is one) from the eDirectory server URL.

Change Priority: Lets you change the priority for the context to the eDirectory server URL.

WebDav Provider

This page is not used for administration of the ZENworks Middle Tier Server. Do not change the values on this page.

iFolder Storage Provider

This page is not used for administration of the ZENworks Middle Tier Server. Do not change the values on this page.

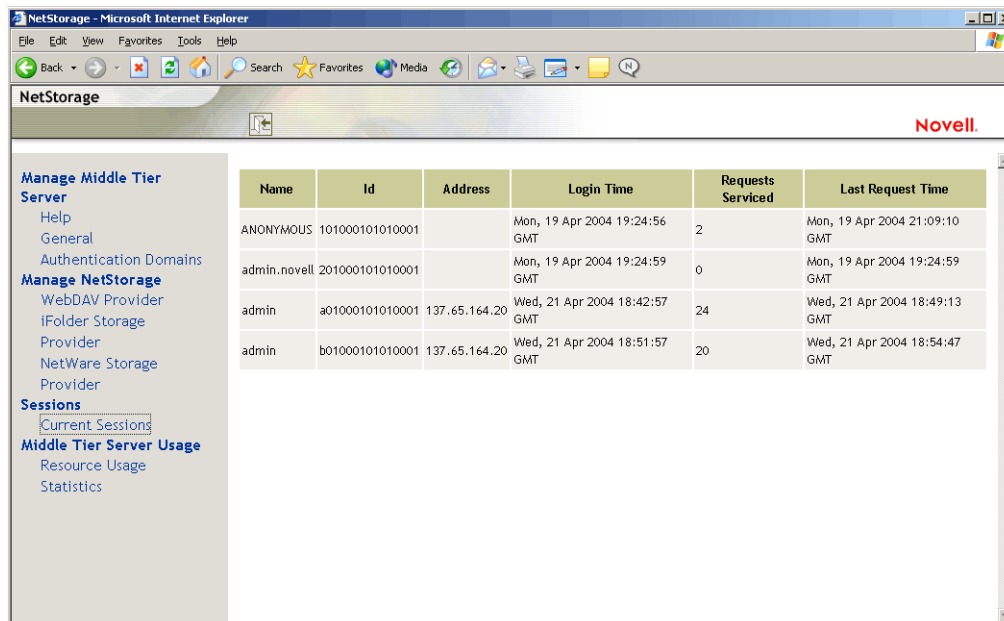
NetWare Storage Provider

This page is not used for administration of the ZENworks Middle Tier Server. Do not change the values on this page.

Current Sessions

The Current Sessions page displays a report with information on the current ZENworks Middle Tier Server sessions. The report is in XML format and can be customized with a parser to provide specific information.

Figure 3-4 The Current Sessions Page of the NSAdmin Utility

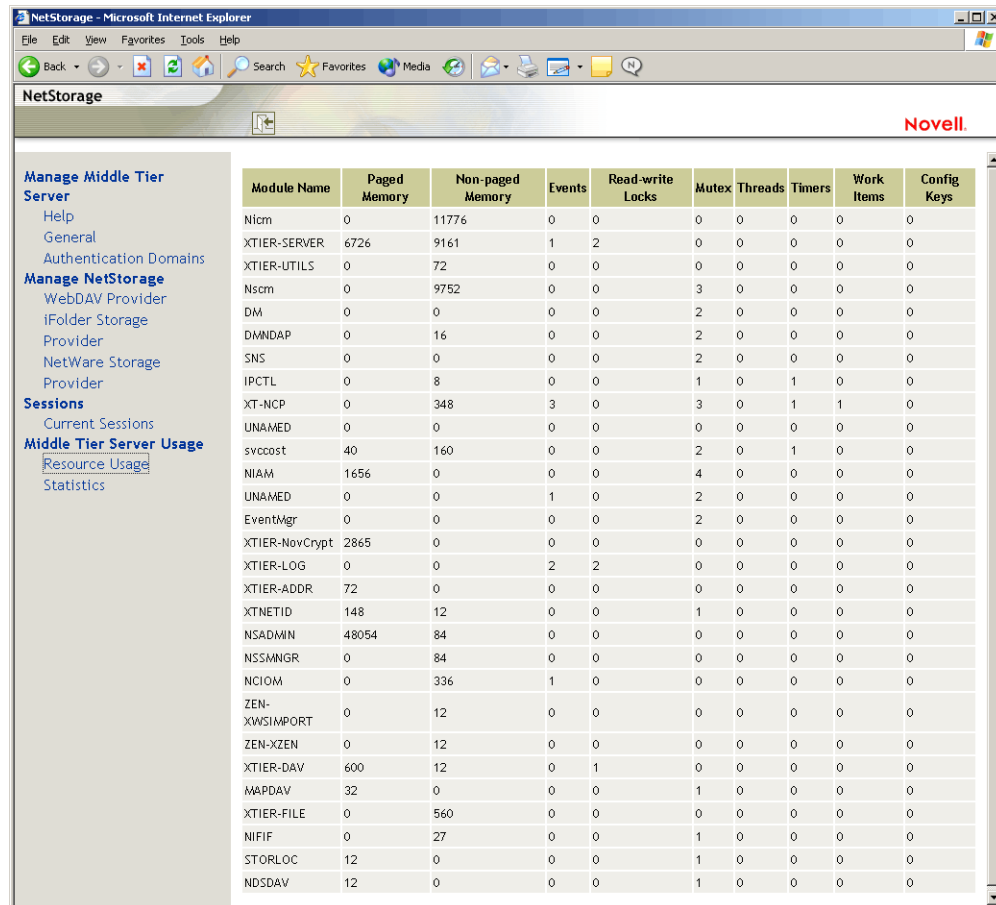


Name	Id	Address	Login Time	Requests Serviced	Last Request Time
ANONYMOUS	101000101010001		Mon, 19 Apr 2004 19:24:56 GMT	2	Mon, 19 Apr 2004 21:09:10 GMT
admin.novell	201000101010001		Mon, 19 Apr 2004 19:24:59 GMT	0	Mon, 19 Apr 2004 19:24:59 GMT
admin	a01000101010001	137.65.164.20	Wed, 21 Apr 2004 18:42:57 GMT	24	Wed, 21 Apr 2004 18:49:13 GMT
admin	b01000101010001	137.65.164.20	Wed, 21 Apr 2004 18:51:57 GMT	20	Wed, 21 Apr 2004 18:54:47 GMT

Resource Usage

The Resource Usage page displays a detailed report of resource utilization (memory, etc.) for the ZENworks Middle Tier Server. The report is in XML format and can be customized with a parser to provide specific information.

Figure 3-5 The Resource Usage Page of the NSAdmin Utility

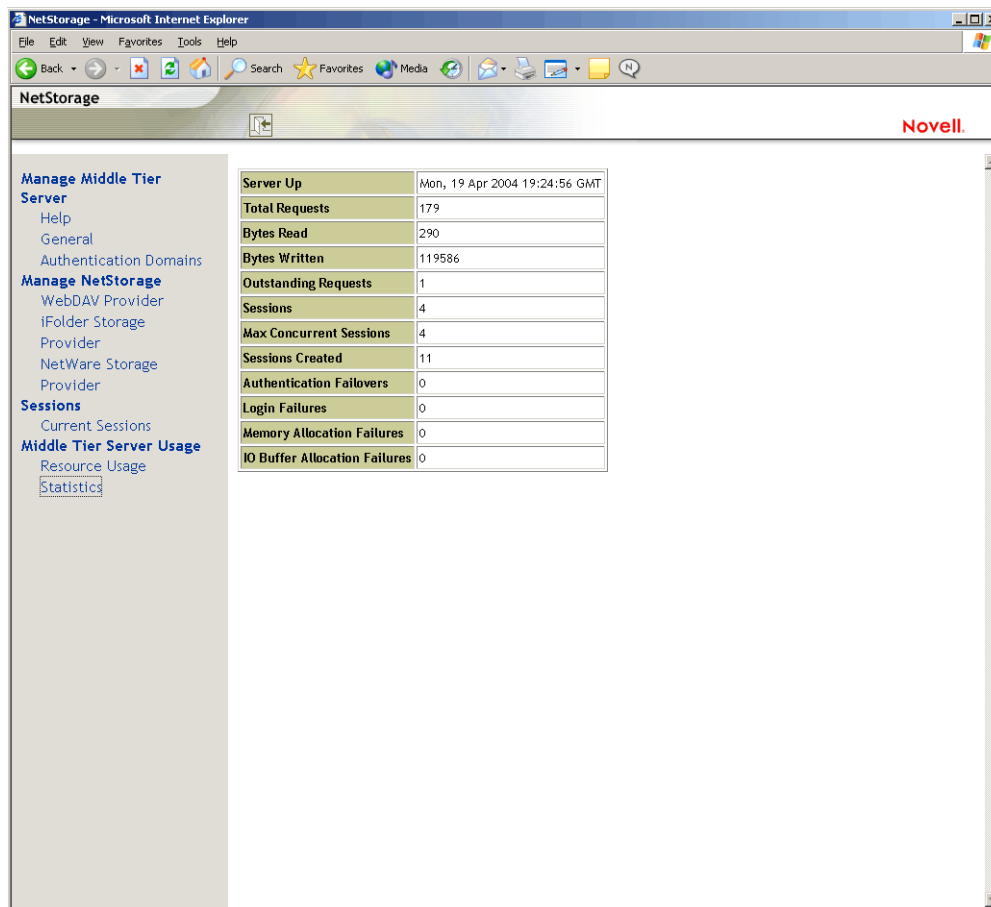


Module Name	Paged Memory	Non-paged Memory	Events	Read-write Locks	Mutex	Threads	Timers	Work Items	Config Keys
Nlcm	0	11776	0	0	0	0	0	0	0
XTIER-SERVER	6726	9161	1	2	0	0	0	0	0
XTIER-UTILS	0	72	0	0	0	0	0	0	0
Nscm	0	9752	0	0	3	0	0	0	0
DM	0	0	0	0	2	0	0	0	0
DMNDAP	0	16	0	0	2	0	0	0	0
SNS	0	0	0	0	2	0	0	0	0
IPCTL	0	8	0	0	1	0	1	0	0
XT-NCP	0	348	3	0	3	0	1	1	0
UNAMED	0	0	0	0	0	0	0	0	0
svccost	40	160	0	0	2	0	1	0	0
NIAM	1656	0	0	0	4	0	0	0	0
UNAMED	0	0	1	0	2	0	0	0	0
EventMgr	0	0	0	0	2	0	0	0	0
XTIER-NovCrypt	2865	0	0	0	0	0	0	0	0
XTIER-LOG	0	0	2	2	0	0	0	0	0
XTIER-ADDR	72	0	0	0	0	0	0	0	0
XTNETID	148	12	0	0	1	0	0	0	0
NSADMIN	48054	84	0	0	0	0	0	0	0
NSSMNGR	0	84	0	0	0	0	0	0	0
NCIOM	0	336	1	0	0	0	0	0	0
ZEN-XWSIMPORT	0	12	0	0	0	0	0	0	0
ZEN-XZEN	0	12	0	0	0	0	0	0	0
XTIER-DAV	600	12	0	1	0	0	0	0	0
MAPDAV	32	0	0	0	1	0	0	0	0
XTIER-FILE	0	560	0	0	0	0	0	0	0
NIFIF	0	27	0	0	1	0	0	0	0
STORLOC	12	0	0	0	1	0	0	0	0
NDSDAV	12	0	0	0	1	0	0	0	0

Statistics

The Statistics page displays a report with information like server up time, login failures, and number of sessions active on the ZENworks Middle Tier Server. The report is in XML format and can be customized with a parser to provide specific information.

Figure 3-6 The Statistics Page of the NSAdmin Utility



3.3 What Is the Desktop Management Server?

The ZENworks Desktop Management Server lets you centrally create and manage policies and profiles for users and workstations on a network. These policies and profiles enable you to distribute, manage, and update applications, perform advanced inventory and remote management functions, and automatically install operating systems on the Windows workstations in your network.

The ZENworks Desktop Management Server can be installed on a Windows 2000/2003 server, a NetWare 6/6.5 server, a SLES 9 SP1 server, or an OES Linux server.

The Desktop Management Server installation program installs selected components and necessary files to the server or servers you select. These components and files are what is sometimes referred to as the “back end” of the ZENworks Desktop Management setup. The back end also includes eDirectory, ZENworks policy and application files, various Desktop Management services, and designated NetWare or Windows servers that are either members of the same tree (if eDirectory is in

a NetWare environment) or members of the same Microsoft domain (if eDirectory is in a Windows environment) where the ZENworks files are located.

3.4 Getting Ready to Use the Desktop Management Server

The ZENworks Desktop Management Server can be installed on NetWare 6 SP4 servers, NetWare 6.5 SP3 servers, Windows 2000 SP2 servers, Windows Server 2003 machines, SLES 9 servers, or OES Linux servers. The following sections provide details on where to find additional information about the prerequisites, installation steps, and configuration for the Desktop Management Server:

- [“Preinstallation Considerations” on page 58](#)
- [“Installing the Desktop Management Server” on page 58](#)
- [“Configuring the Desktop Management Server” on page 59](#)

3.4.1 Preinstallation Considerations

It is important that you understand the procedure for preparing to install the Desktop Management Server. We recommend that you review the following documentation, which details the hardware and software requirements and other installation prerequisites of the Desktop Management Server installation.

- [“Platform Support for the Desktop Management Infrastructure” in “Overview” in the *Novell ZENworks 7 Desktop Management Installation Guide*.](#)
- [“Prerequisites for the Workstation Running the Installation” in “Preparation” in the *Novell ZENworks 7 Desktop Management Installation Guide*.](#)
- [“Prerequisites for Installing the ZENworks Desktop Management Server” in “Preparation” in the *Novell ZENworks 7 Desktop Management Installation Guide*.](#)
- [“Preparing a Linux Server for ZENworks Functions” in “Preparation” in the *Novell ZENworks 7 Desktop Management Installation Guide*.](#)

NOTE: If the Desktop Management Server is installed on a Windows 2000/2003 server, the server must have Microsoft Active Directory installed and it must be designated as a Primary Domain Controller (PDC).

If the server has the Novell Client installed, the client must be set up to work over the IP protocol, not IPX™.

If the ZENworks Middle Tier Server is installed on a Windows 2000/2003 server and it will communicate with the Desktop Management Server installed on a Windows 2000/2003 server, both of those servers must be members of the same Microsoft domain.

3.4.2 Installing the Desktop Management Server

The procedure you should use for installing the Desktop Management Server is detailed in [“Installing the ZENworks Desktop Management Server”](#) and [“Installing the Desktop Management Server and the Middle Tier Server on the Same Machine”](#) in [“Windows-Based Installation”](#) in the *Novell ZENworks 7 Desktop Management Installation Guide*.

The Desktop Management Server installation program lets you install the software to multiple servers, but because the ZENworks Middle Tier Server software installation allows for only one IP entry, not all of the Desktop Management Servers you set up can be used.

You can specify values in the *Add Host* field of the Authentication Domains page of the NSAdmin utility to add other Desktop Management Servers to which your users can background authenticate. If your primary Desktop Management Server goes down, these other servers are connected to the ZENworks Middle Tier Server without losing any ZENworks functionality. For more information, see [“Authentication Domains \(Xtier 2.6.2 installation\)” on page 52](#).

The options you can use for installing ZENworks Desktop Management Server software on a SLES 9 SP1 or OES Linux server are detailed in [“Installing ZENworks Desktop Management Services on Linux”](#) in the *Novell ZENworks 7 Desktop Management Installation Guide*.

3.4.3 Configuring the Desktop Management Server

The Desktop Management Server installation program installs selected `.jar` files to the `\consoleone` directory of the server or servers you also select. These files are the ZENworks 7 Desktop Management snap-ins that you use to manage the ZENworks objects in a directory tree.

The Desktop Management snap-ins are used by ConsoleOne[®], a graphical-interface management tool that can be installed and run either on a network server you are authenticated to or to your local workstation. ConsoleOne can view eDirectory objects of ZENworks (for example, workstation objects, application objects, policies, database objects, and so on) in trees to which you are authenticated.

When you manage or create a ZENworks object using ConsoleOne, you can define the path to the server location of application files and policy files. The location of these “ZENworks files” never changes, even though the policy or other eDirectory object that defines them might be replicated throughout the eDirectory tree.

If you want to configure any component of ZENworks 7 Desktop Management, you need to identify the object with which that component is associated and then make the adjustments you want.

For details about creating or configuring the components of Desktop Management, see the appropriate section in this guide:

- [Part IV, “Workstation Management,” on page 131](#)
- [Part III, “Automatic Workstation Import and Removal,” on page 117](#)
- [Part IV, “Workstation Management,” on page 131](#)
- [Part V, “Application Management,” on page 227](#)
- [Part VI, “Workstation and Server Imaging,” on page 623](#)
- [Part VII, “Remote Management,” on page 811](#)
- [Part VIII, “Workstation Inventory,” on page 871](#)

Understanding the ZENworks Multiple UNC Provider

4

In a Novell® ZENworks® for Desktops 4.x environment, accessing ZENworks policy and application files on a network server from a user desktop without using the Novell Client™ or mapped drives required the ZENworks Middle Tier Server, even if a Microsoft Client was available.

Now, in a ZENworks 7 environment, the ZENworks Multiple UNC Provider can use either the Novell Client or the Microsoft Client (through the CIFS/SMB protocol) to increase the speed of customer access to network policies and applications.

- [Section 4.1, “What Is the ZENworks Multiple UNC Provider?,” on page 61](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

4.1 What Is the ZENworks Multiple UNC Provider?

The Multiple UNC Provider (MUP) is a Windows service that assists in locating network resources identified using the Uniform Naming Convention (UNC). MUP receives commands containing UNC names from applications and sends the name to each registered UNC provider. When a provider identifies a UNC name as its own, MUP automatically redirects future instances of that name to that provider. Essentially, MUP determines which client the system must use to access the requested UNC name and hands off requests to that client's redirector. The redirector then directs the resource request from the workstation to the device on the network that can provide the resource.

The ZENworks Multiple UNC Provider (ZENMUP) lets workstations establish, on a per session basis, the fastest connection available to network policies and applications based on the customer's environment and what clients they are using. When requests for files (such as group policies, applications, and inventory requests) come from the ZENworks Desktop Management Agent, ZENMUP first attempts to access those files on the identified network volume by using any installed client (calling `_access` on the network volume to test for existence). If this succeeds, the file system provider registered with Windows claims this network name and native file system calls are used to access all files on that network volume. If no file system provider knows about that network name, the call fails and the ZENworks Middle Tier Server is used to access files on that volume. When the successful access method is determined, that information is stored in the Windows `mup.sys` file during that session. Subsequent file access to the same volume is accomplished with a lookup on that file.

ZENMUP is automatically installed and enabled as part of the ZENworks 7 Desktop Management Agent installation. It doesn't need to be configured and cannot be disabled.

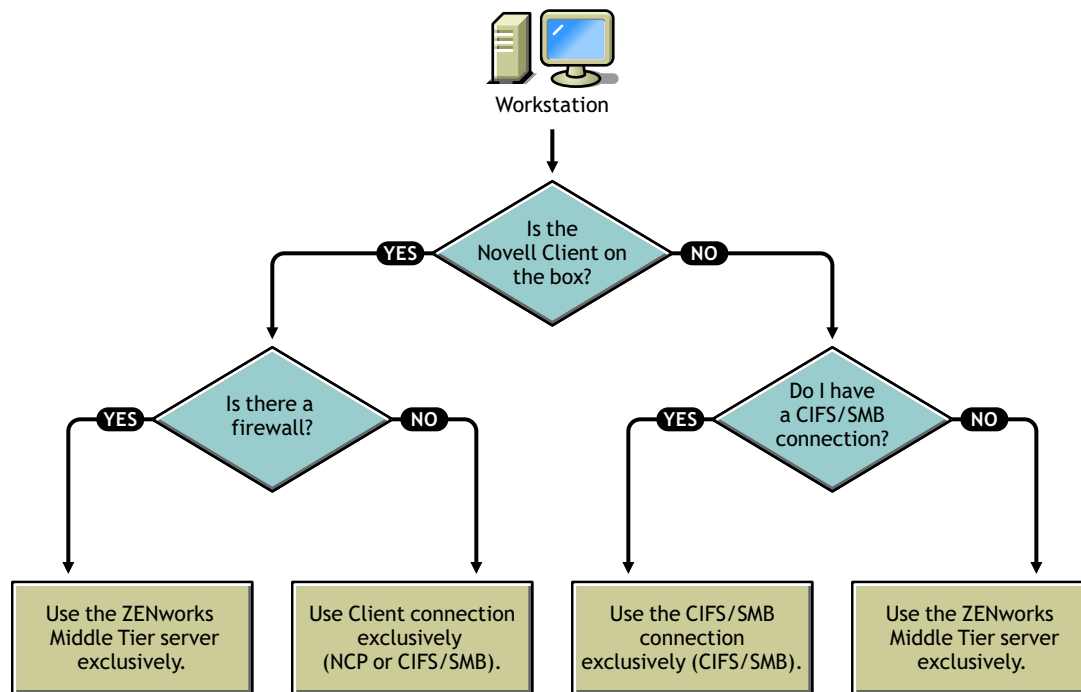
This section contains more specific information about ZENMUP in the following subsections:

- [Section 4.1.1, “How Does ZENMUP Work?,” on page 62](#)
- [Section 4.1.2, “ZENMUP Environments Overview,” on page 64](#)

4.1.1 How Does ZENMUP Work?

How ZENMUP works depends on the environment in which it is used, as outlined in the following diagram:

Figure 4-1 How ZENMUP Logic is Invoked when a Network Connection is Established



For more specific information about ZENMUP behavior in specific server environments, see the following sections:

- “ZENMUP in a NetWare Server Environment” on page 62
- “ZENMUP in a Windows-only Environment” on page 63
- “ZENMUP in a Linux Server Environment” on page 63
- “Other ZENMUP Considerations” on page 63

ZENMUP in a NetWare Server Environment

In a NetWare® server environment, when requests for files come from a workstation, ZENMUP first checks to see if the Novell Client is installed on the workstation. If it is installed, and if no firewall is present, the client uses either the NetWare Core Protocol™ (NCP™) or a CIFS/SMB connection to access the server, depending on the network operating system where the ZENworks files are stored.

IMPORTANT: Using ZENworks 7 with versions of the Novell Client prior to 4.9 SP2, a Middle Tier connection cannot be forced by right-clicking the Application Launcher/Explorer icon and selecting *ZENworks Middle Tier Server Login* (as it could be in ZENworks 4.0.1). Upgrading to Novell Client 4.9 SP2 allows a forced Middle Tier connection in ZENworks 7. If user logins hang, you can remove the ZENworks Middle Tier login option using the Launcher Configuration setting.

If ZENMUP detects that a firewall is present, all communication is done through the ZENworks Middle Tier Server.

If no firewall is present but CIFS is running on the NetWare servers, the NetWare server attaches a `-w` or `_w` (depending on the NetWare version) to the CIFS server name to differentiate the CIFS protocol from the NCP protocol, thereby avoiding conflicts. If resources are stored on a Windows server, those resources are accessed by the Microsoft Client using a CIFS/SMB connection.

If the Novell Client is not installed on the workstation, ZENMUP checks to see if there is a CIFS/SMB connection. If there is, ZENMUP uses the CIFS/SMB connection exclusively. If there is no CIFS/SMB connection, ZENMUP uses the ZENworks Middle Tier Server to access the files.

User support inside a firewall (using CIFS only) and continual support when outside a firewall (using HTTP) requires that the Middle Tier Server's host file is configured to recognize the CIFS server name with the `-w` or `_w`.

Workstation support is limited to the Middle Tier Server. When configuring the file location, you must specify the server's NetBios name (NetWare machine name), thus forcing the connection to go through the Middle Tier Server.

ZENMUP in a Windows-only Environment

In a Windows-only environment, you must use a domain controller, and each workstation must be a member of the domain. Inside the firewall, the MS Client (CIFS) is always used for connections. Outside the firewall, the Middle Tier Server is used. Because the CIFS/SMB protocol allows Guest authentication to a network volume (with no file rights required for workstations that are not in a Windows domain), all workstations in an agent-only environment must be members of a Windows domain. This allows ZENMUP to function as designed.

ZENMUP in a Linux Server Environment

In an OES Linux server environment using NetWare-style volumes, when requests for files come from a workstation, ZENMUP checks the preferred client protocol: if the Novell Client is installed, and if no firewall is present, ZENMUP uses the NetWare Core Protocol™ (NCP™) to access the Linux server; if the Desktop Management Agent is installed exclusively, ZENMUP uses a CIFS/SMB connection to access the Linux server (if the CIFS/SMB connection fails, ZENMUP attempts an HTTP connection). Essentially, the ZENMUP interacting with OES Linux works the same as it does on a NetWare server (including the behavior inside and outside the firewall).

In a SLES 9x or SLES 10 server environment, Samba shares must first be set up and configured. For more information, see “[Preparing a Linux Server for ZENworks Functions](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*. When this is accomplished, the ZENMUP interacting with SLES works the same as it does on a Windows server (including the behavior inside and outside the firewall). The exception to this is that it is not necessary to set up a domain controller nor to make the workstations members of a domain.

Other ZENMUP Considerations

For each network name (server name or IP address), an entry is stored in the Windows `mup.sys` file telling ZENMUP which connection to use. After a connection has been made, it is saved and used for that session.

NOTE: If your authentication environment changes (for example, if your CIFS server was down during the first access attempt, then you subsequently start it), you must reboot the workstation to refresh the file entries.

ZENMUP is session-based, so any connections made during a session are released when the workstation is rebooted.

4.1.2 ZENMUP Environments Overview

For a quick overview of how ZENMUP works in different environments, see the following table:

Table 4-1 *How ZENMUP Works in Different Network Environments*

Environment	Description
NetWare servers with workstations running the Novell Client	If no firewall is present, either the NetWare Core Protocol (NCP) is used (if accessing files on a NetWare server) or a CIFS/SMB connection is used (if accessing files on a Windows server).
NetWare servers running the CIFS protocol and workstations running the MS Client and the Desktop Management Agent	User support inside the firewall uses CIFS. If ZENMUP detects no direct file access (such as when a firewall is present), all communication is directed through the ZENworks Middle Tier Server (HTTP).
Windows servers with workstations running the Desktop Management Agent only or the Desktop Management Agent and the MS Client.	There must be a domain controller, and all workstations and users must be members of the domain with the appropriate file rights on the network share where the application and policy files are located. Inside the firewall, the MS Client (CIFS) is always used. Outside the firewall, the ZENworks Middle Tier Server is used to access files.
SLES 9 or SLES 10 servers with workstations running the Desktop Management Agent only or the Desktop Management Agent and the MS Client	Samba shares must be set up for file access. Workstations must have the appropriate file rights on the network share where the application and policy files are located. Inside the firewall, the MS Client (CIFS) is always used. To access files on a SLES server outside the firewall, workstations require a Windows Middle Tier Server.
OES Linux servers with workstations running the Novell Client	If no firewall is present, either the NetWare Core Protocol (NCP) is used (if using the Novell Client to access files on an OES or NetWare server) or a CIFS/SMB connection is used (if accessing files on a Windows or SLES server).
OES servers with workstations running the ZENworks Desktop Management Agent	All communication is directed through the ZENworks Middle Tier Server unless Samba is configured to allow direct file access.

Process Flow in ZENworks Desktop Management

5

This section includes information and diagrams that explain the following fundamental processes of Novell® ZENworks® Desktop Management:

- [Section 5.1, “Authenticating to eDirectory,” on page 65](#)
- [Section 5.2, “Reading Attributes from eDirectory,” on page 69](#)
- [Section 5.3, “Accessing Policy and Application Files,” on page 69](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

5.1 Authenticating to eDirectory

Before any applications or policies can be accessed by the user, the user must log in to the network (that is, log in to Novell eDirectory™) to verify login rights and to establish a connection to the network servers where the user needs to be authenticated.

IMPORTANT: LDAP authentication, which is launched when users log in and access ZENworks applications or policies, consumes two of the grace logins granted to a user when the user's password expires. Grace logins are set in ConsoleOne on the Restrictions page (password restrictions section) of the eDirectory User object.

For example, when eDirectory notifies a user that he or she has two grace logins left on a server, that user actually has no grace logins and will not be able to log in until the password is reset.

If you have installed the Novell Client™, the Desktop Management Agent, and the Middle Tier Server, there are three login scenarios:

- [“Logging in Using the Novell Client” on page 65](#)
- [“Logging in Using the Desktop Management Agent” on page 66](#)
- [“Logging in Locally to the Workstation” on page 68](#)

5.1.1 Logging in Using the Novell Client

When the Novell Client is used to authenticate, all communication to eDirectory and the server file system uses the traditional Novell NCP™ protocol. The client launches as the default login GINA (Graphical Identification and Authentication) user interface. For more information about authenticating with the Novell Client, see [“Using the Novell Client for Authentication”](#) in the *Novell ZENworks 7 Desktop Management Installation Guide*.

The process of authentication to eDirectory using the 32-bit client in this scenario is illustrated in the following diagram:

Figure 5-1 Authentication to eDirectory Using the 32-bit Novell Client

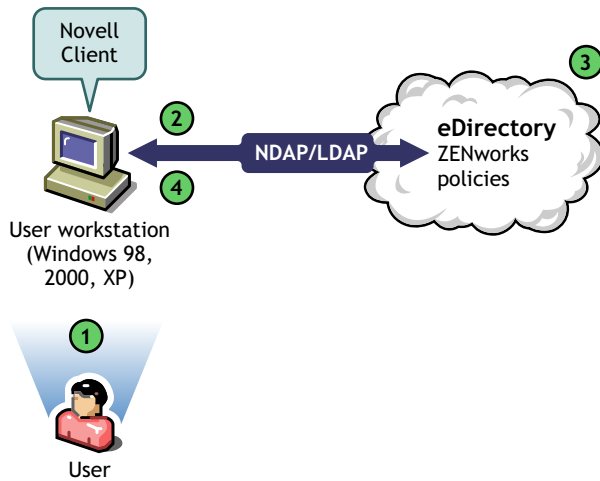


Table 5-1 Steps in the eDirectory Authentication Process Using the 32-bit Novell Client

Step	Explanation
①	A user with the appropriate rights enters eDirectory credentials in the login fields of Novell Client GINA.
②	The Novell Client sends the authentication request to eDirectory in an NDAP/LDAP packet.
③	eDirectory confirms that the login credentials are valid and sends the authentication response packet through NDAP/LDAP to the user workstation.
④	The Novell Client on the user workstation receives the response packet and confirms a successful authentication. The network connection is established.

However, if these same workstations are taken outside of the firewall, the client continues to launch as the default login GINA. Users can log in locally to their own Windows desktops, but they cannot authenticate to eDirectory through the ZENworks Middle Tier Server.

If users who have both the agent and the client installed on their machines want to authenticate and receive applications outside the firewall, they can still do so by using an alternative login method, but their workstations can receive only application files, not Desktop Management policies. For this reason, you should consider removing the client and installing only the agent on workstations that are to be used mainly outside the firewall.

For more information about the alternative login method used when the client and agent are installed together on a workstation outside the firewall, see [“Logging in Locally to the Workstation” on page 68](#).

5.1.2 Logging in Using the Desktop Management Agent

If you install the Desktop Management Agent and you want your users to log in to the network through the agent, you need to understand how the Desktop Management Agent authenticates to the

network. For more information about setting up the Desktop Management Agent for authentication, see “[Using the Desktop Management Agent and the ZENworks Middle Tier Server for Authentication](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

The diagram below shows the process occurring when a user authenticates to eDirectory using the Desktop Management Agent outside the firewall. The process is similar when the user is inside the firewall.

Figure 5-2 eDirectory Authentication Using the Desktop Management Agent Behind a Firewall

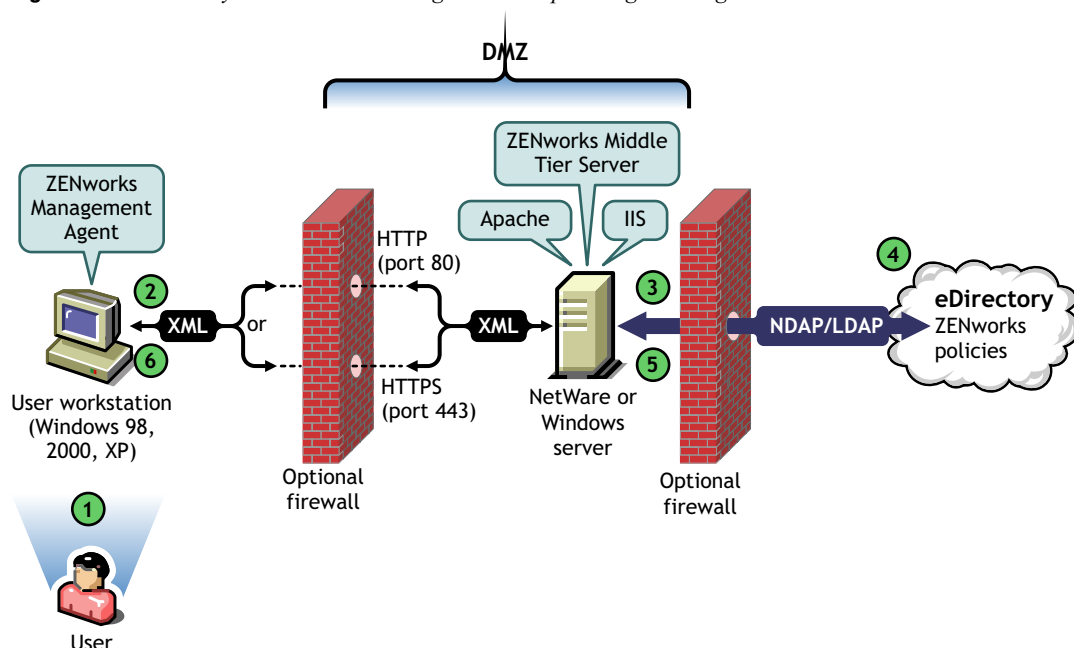


Table 5-2 Steps of eDirectory Authentication Using the Desktop Management Agent Behind a Firewall

Step	Explanation
1	A user accesses the ZENworks Management Agent and enters a user ID and password.
2	The agent collects the user credentials. Using public/private key and session key encryption methods, the credentials are securely passed to the ZENworks Middle Tier Server (through a corporate firewall) through HTTP or HTTPS.
NOTE: Credentials are always secured using the techniques mentioned above whether the transport mechanism is HTTP or HTTPS.	
3	The ZENworks Middle Tier Server Web service receives the credentials through the firewall, unparses them, converts them to an NDAP/LDAP packet, and then uses NDAP/LDAP to pass them through a port in the back-end firewall to eDirectory.
NOTE: No NetWare® licenses are consumed at the ZENworks Middle Tier Server. The licensed connections are consumed by the Desktop Management Server.	
4	eDirectory receives the NDAP/LDAP packet, confirms that the login credentials are valid, and sends the authentication response packet through NDAP/LDAP to the ZENworks Middle Tier Server.

Step	Explanation
5	The ZENworks Middle Tier Server encrypts the returned LDAP or NDAP packet to XML again, then sends the XML confirmation packet over HTTP or HTTPS to the ZENworks Management Agent.
6	The agent receives the XML packet, then unparses it and converts it to binary format, so the user at the workstation can recognize a successful login.

When eDirectory authenticates users, they are authenticated to any server in the tree where the system administrator has granted them rights.

The ZENworks Middle Tier Server uses LDAP/NDAP to authenticate to eDirectory because of the search capabilities of these protocols. If you select *Clear Text Passwords* during the installation of the ZENworks Middle Tier Server, the authentication request can use just the User ID (without its context) to search the entire tree for the authenticating user. Without a clear text password, the user must either log in using his or her fully distinguished name or you must restrict that user to an Authentication Domain, which is a particular context in the directory.

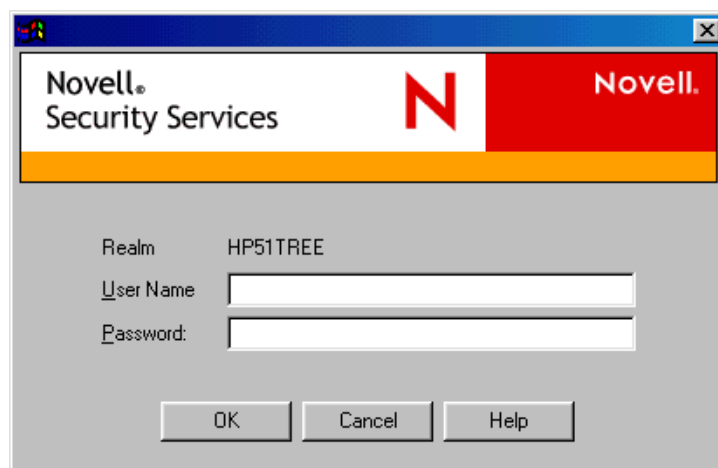
For more information about authentication and the role of the ZENworks Middle Tier Server in ZENworks file access, see [Section 3.3, “What Is the Desktop Management Server?” on page 57](#).

5.1.3 Logging in Locally to the Workstation

If users bypass the Desktop Management Agent login by logging in to the local workstation only, they still need to authenticate to eDirectory to access their applications.

If the Application Explorer icon is displayed on the user's desktop or system tray, the user has the option (by right-clicking the icon) to log in to the ZENworks Middle Tier Server. If the user chooses to log in, the Novell Security Services login GINA is displayed.

Figure 5-3 *The Novell Security Services Login Dialog Box*



When the user enters his or her user ID and password at the Security Services login GINA, these credentials are given to the ZENworks Middle Tier Server, which passes them to eDirectory for authentication. This login GINA uses the same authentication process used by the Desktop Management Agent login GINA. For more information, see [“Logging in Using the Desktop Management Agent” on page 66](#).

5.2 Reading Attributes from eDirectory

After the user is authenticated to eDirectory, Workstation Manager (or one of its helper `.dlls`) follows steps similar to those used to authenticate to eDirectory in order to access objects in eDirectory. The purpose of this second access is to read eDirectory for attributes; that is, settings that are configured in a directory object or container and intended for applying to the workstation.

For a simplified, step-by-step description of the authentication process, see [Section 5.1, “Authenticating to eDirectory,”](#) on page 65.

5.3 Accessing Policy and Application Files

After users are authenticated, the ZENworks Desktop Management can access the policy and application files that you have defined for their use, making it possible for their workstations to be configured, managed remotely, or inventoried, and the appropriate software applications pushed to their desktops.

5.3.1 Policy Files

Policies define the capabilities or configuration of a Windows workstation. You can manage these capabilities or configurations according to the user or workstation that is authenticated to eDirectory and associated to the policy. For the most part, when you configure a policy for a workstation or user, these configurations are stored in eDirectory as attributes. These attributes are read by various `.dlls` in the client or agent, and pulled to the workstation at login time by the Workstation Manager. These configurations are stored on the workstation in its registry.

Some workstation configurations, however, are not stored in eDirectory. The iPrint, Group Policies, and Desktop Preferences policies require a defined path to files that must be accessed by the client or Desktop Management Agent and applied to the workstation. For more information about the policies that require file access, see [Chapter 10, “Understanding Workstation Management,”](#) on page 133.

5.3.2 Application Files

ZENworks 7 Desktop Management lets you manage 32-bit Windows Application objects that are associated to users or workstations. Using ConsoleOne[®], you can configure numerous Application objects and associate them to users, workstations, groups, or containers.

The Novell Application Launcher[™] uses either the Novell Client or the ZENworks Middle Tier Server to access the application files on NetWare or Windows servers so the files can be distributed, launched, cached, or uninstalled. For more information, see [Chapter 23, “Novell Application Launcher: Managing Authentication and File System Access,”](#) on page 283.

5.3.3 Accessing Files by Using a Client Inside the Firewall

The process of using a client inside the firewall to access policy or application files (from a path defined in eDirectory) is illustrated in the following diagram:

Figure 5-4 Using the Novell Client Inside a Firewall to Access Policy or Application Files

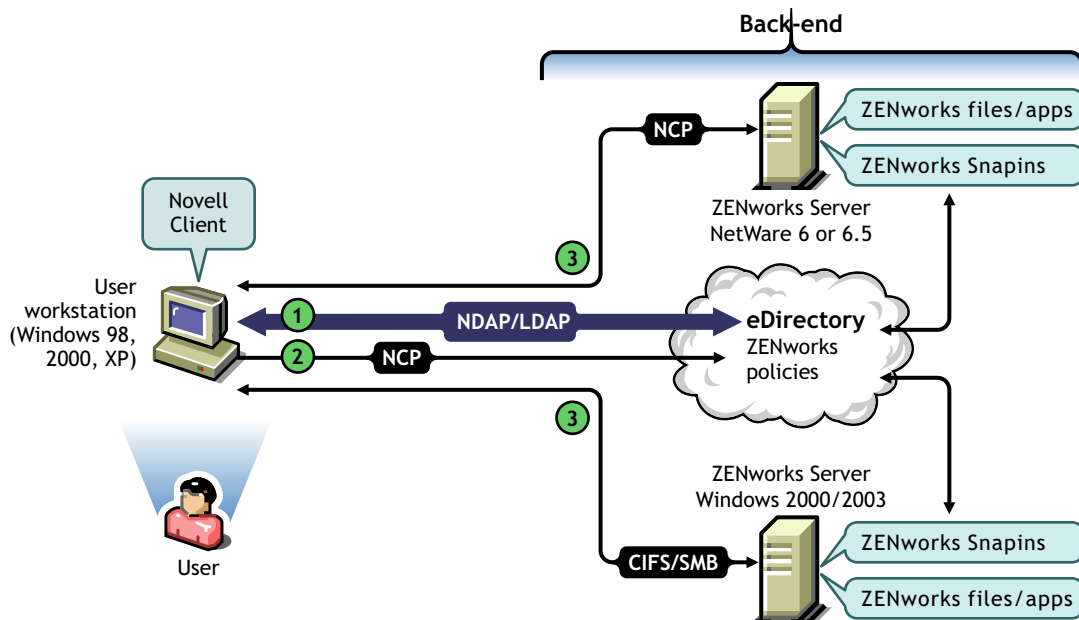


Table 5-3 Steps in the Process for Using the Novell Client Inside a Firewall to Access Policy or Application Files

Step	Explanation
①	A user with the appropriate rights enters eDirectory credentials in the login fields of Novell Client GINA and is authenticated to eDirectory through an NDAP/LDAP connection. For details, see Section 5.1, "Authenticating to eDirectory," on page 65.
②	The Workstation Manager or the Application Launcher installed on the workstation determines the need to access files and sends a request from the Novell Client to eDirectory in an NCP or CIFS packet.
③	The files are sent to the workstation through an NCP or CIFS packet.

5.3.4 Accessing Files by Using the Desktop Management Agent Outside the Firewall

The process of using the Desktop Management Agent outside the firewall to access policy or application files (from a path defined in eDirectory) is illustrated in the following diagram:

Figure 5-5 The Process of Using the Desktop Management Agent to Access Policy or Application Files Outside a Firewall

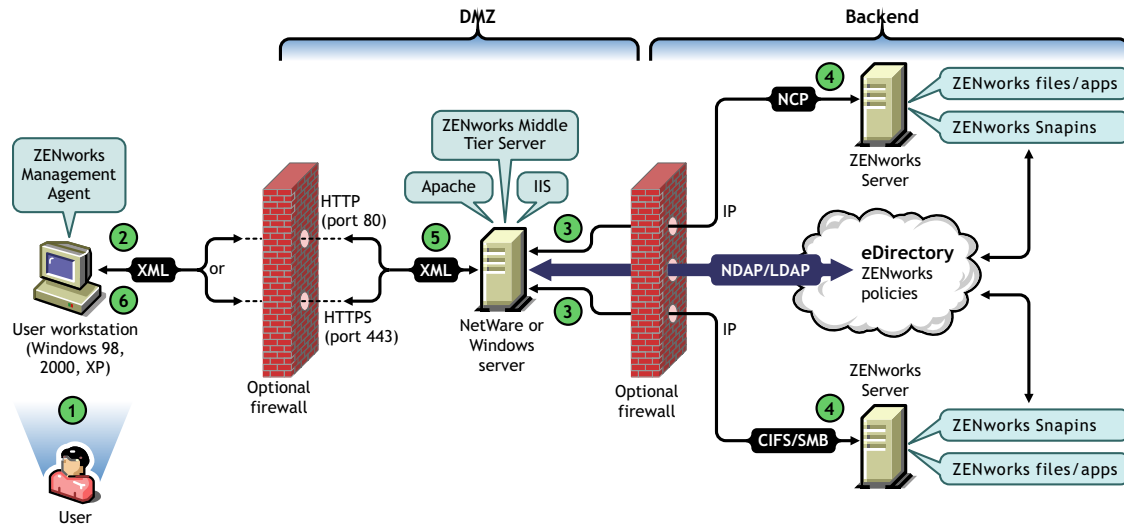


Table 5-4 Steps in the Process of Using the Desktop Management Agent to Access Policy or Application Files Outside a Firewall

Step	Explanation
1	A user with the appropriate rights enters eDirectory credentials in the login fields of the Novell Client GINA or the Microsoft Client GINA and is authenticated to eDirectory through an NDAP/LDAP connection. For details, see Section 5.1, "Authenticating to eDirectory," on page 65.
2	The Workstation Manager (or one of its helper .dlls) or the Application Launcher installed on the workstation determines the need to access files and sends a request to the ZENworks Middle Tier Server in an XML packet, using the HTTP or HTTPS protocol to pass it through a designated port in the corporate firewall to the ZENworks Middle Tier Server.
3	The ZENworks Middle Tier Server Web service receives the request, unparses it, converts it to an NDAP/LDAP packet, and then uses NDAP/LDAP to connect the request to eDirectory.
4	The file location is accessed and the files are sent back to the ZENworks Middle Tier Server in an NCP or CIFS packet. CIFS can be used only if the Middle Tier Server is running on a Windows server.
5	The ZENworks Middle Tier Server converts the returned NCP or CIFS packet containing the files to XML format again, then sends the XML packet over HTTP or HTTPS to the ZENworks Management Agent.
6	The Desktop Management Agent unparses the XML packet containing the files and converts them to binary format to be applied at the workstation.

For more information about users inside the firewall accessing files, see [Chapter 4, “Understanding the ZENworks Multiple UNC Provider,”](#) on page 61.

Workstation Management Does Not Use the Middle Tier if the Novell Client is Installed on the Workstation

If the Novell Client and the Desktop Management Agent are installed on a workstation (for example, a laptop workstation) and that workstation is taken outside the corporate firewall, only the traditional Novell Client login is displayed at login, and the user can log in locally by choosing *Workstation Only*.

In this scenario, Desktop Management Workstation Management does not utilize the Middle Tier to access eDirectory, and therefore Workstation Manager is in disconnected mode. This means that only cached policies are applied because Workstation Manager does not have an eDirectory connection for the User or the Workstation object. This is similar to the way Application Management works: if users log in *Workstation Only*, they see only the installed applications that are marked “disconnectable” or applications that were force-cached when they were connected.

There is one difference in this scenario between Application Management and Workstation Management. If both the Desktop Management Agent and the Novell Client are installed, and if the agent is configured with a Middle Tier Server address, users can log in to the Middle Tier through the Application Launcher after logging in *Workstation Only* using the Novell Client. In this case, the Application Launcher works in connected mode as it accesses eDirectory and the file system through the Middle Tier Server instead of the Novell Client. However, workstation associated applications do not work because Workstation Manager has already started the NAL Workstation Helper at system startup in order for cached applications to function.

NOTE: If a connection to eDirectory is established through the Novell Client after a user logs in using *Workstation Only*, within 60 seconds of the connection being made, Workstation Manager logs in as the Workstation Object and policies from the Workstation Package are retrieved.

Implementing a DHCP Option for Delivering the Middle Tier Server Address

Many corporate employees are often “on the road,” required to travel from worksite to worksite while maintaining contact and sharing information with other individuals in the corporation. Routinely, these roaming workers use their laptop computers to help them share information.

If Novell® ZENworks® is installed in the corporate network, and if the ZENworks Management Agent is installed on a roaming user's laptop, he or she can install and run applications that process e-mail and create documents by logging in through the ZENworks Middle Tier Server.

If the corporate network's DNS is not sub-zoned, however, the roaming user might find it necessary to log in through his or her “home” Middle Tier Server, which might be hundreds of miles away and which might require the use of a WAN link. Even in cases where the roaming user tries to log in to an off-site Middle Tier and is presented with a list of Middle Tier Server names to choose from, the inconvenience, loss of time and money make this a less-than-desirable scenario.

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

A.1 Overview

This section explains how to set up a local DHCP server to send out the address of the local Middle Tier Server, making it convenient for roaming users to quickly authenticate as a local node in the corporate network and making it possible to avoid authentication through a distant Middle Tier over a slow WAN link.

When this method is properly implemented, the user's local ZENworks Management Agent uses the configured-site DHCP option to get its Middle Tier information. Based on the information provided by the local DHCP server, the workstation communicates through the Middle Tier Server to the ZENworks Management Server and eDirectory.

IMPORTANT: This method does not work unless you select the *Workstation Management* feature when you install the ZENworks Desktop Management Agent. For more information about installing the agent, see “[Installing and Configuring the Desktop Management Agent](#)” in “[Windows-Based Installation](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

For example, if a user's home base is Toronto, his or her laptop computer uses the Toronto Middle Tier Server when authenticating at that office. If the user travels to São Paulo, Brazil, he or she receives São Paulo Middle Tier Server information when they receive an IP address from the São Paulo DHCP server.

A.2 Creating a New DHCP Option

You need to create and enable a new predefined DHCP Option 100 named “ZENworks” at each DHCP server you will be using in the network environment. The DHCP server sends this option with a configured string value you supply (the local Middle Tier Server address or DNS name) to the agent each time a workstation running in the subnet boots and requests an IP address.

NOTE: When you create the new DHCP option (on either NetWare[®], Windows, or SLES 9 SP1/OES Linux servers), make sure that you set the *Data* value as string. For more information, see [TID 10092121](http://support.novell.com/cgi-bin/search/searchtid.cgi?/10092121.htm) (<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10092121.htm>) in the Novell Knowledgebase.

A.3 Changing the DHCP Option

Although by default the DHCP option number sought by the ZENworks Desktop Management Agent is 100, you can change the option number by adding the following DWORD value to the HKLM\Software\Novell\ZENworks registry key at the workstation:

MiddleTierDhcpOptionNumber

You can set the numeric data (that is, the option number) for this value to any number, but you also need to make sure that the data matches the DHCP option string at the server.

A.4 Checking the Middle Tier Address in the Registry

You can verify that the DHCP option you have created is being used for the Middle Tier address by looking for the following STRING value in the HKLM\Software\Novell\ZENworks registry key at the workstation:

MiddleTierAddress

You can change the data for this value to the Middle Tier address being delivered from DHCP. If you delete the key, it is re-created with the address in DHCP option on the next reboot.

Using a ZENworks Tree

B

This section contains the following information:

- [Section B.1, “Understanding the ZENworks Tree,” on page 75](#)
- [Section B.2, “The ZENworks Tree in an Active Directory Environment,” on page 75](#)
- [Section B.3, “The ZENworks Tree in an eDirectory Environment,” on page 76](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

B.1 Understanding the ZENworks Tree

If you are concerned about creating change in your corporate directory structure (whether you use eDirectory® or Active Directory), you need to create a dedicated tree in eDirectory that can be used to hold the objects and configure the policies that are managed with Novell® ZENworks®. You use this dedicated “ZENworks tree” to deploy ZENworks Desktop Management without affecting the current tools, identity management processes, or authentication processes you currently have in place with your corporate tree.

After you create the ZENworks tree, you can install the ZENworks Desktop Management Server, the ZENworks Middle Tier Server there, and designate it in the ZENworks Desktop Management Agent installation program so that the ZENworks Desktop Management users and workstations are properly configured and ready to authenticate there.

Because you use the ZENworks tree exclusively for ZENworks, the Workstation objects created by ZENworks Automatic Workstation Import are to be found only in this tree. You create policies, Workstation Image objects, Database objects, and Application objects only in this tree. You can also use Nsure® Identity Manager (shipping with ZENworks 7) to synchronize User objects between your corporate tree and the ZENworks tree, making users available for association with desktop policies and applications, just as the imported workstations are available to be associated with policies and applications.

B.2 The ZENworks Tree in an Active Directory Environment

In order for ZENworks to function in a Windows (Active Directory) environment, you need to install eDirectory to synchronize with Active Directory and to manage your ZENworks objects. For more information, see “[Installing in a Windows Network Environment](#)” in “[Windows-Based Installation](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

If you don’t have Dynamic Local User requirements, you can configure the ZENworks Management Agent configured for pass through mode to display the Windows login when your users log in. If the Windows user credentials match those required by the ZENworks tree (after synchronizing User objects with Novell NSure® Identity Manager 2), users are authenticated to Active Directory and to the ZENworks tree. If the credentials don’t match, the user is prompted for credentials again, this time with a ZENworks Management Agent login dialog box.

The following illustration shows a simplified process of using a ZENworks tree in an Active Directory environment.

Figure B-1 Using a ZENworks Tree in an Active Directory Environment

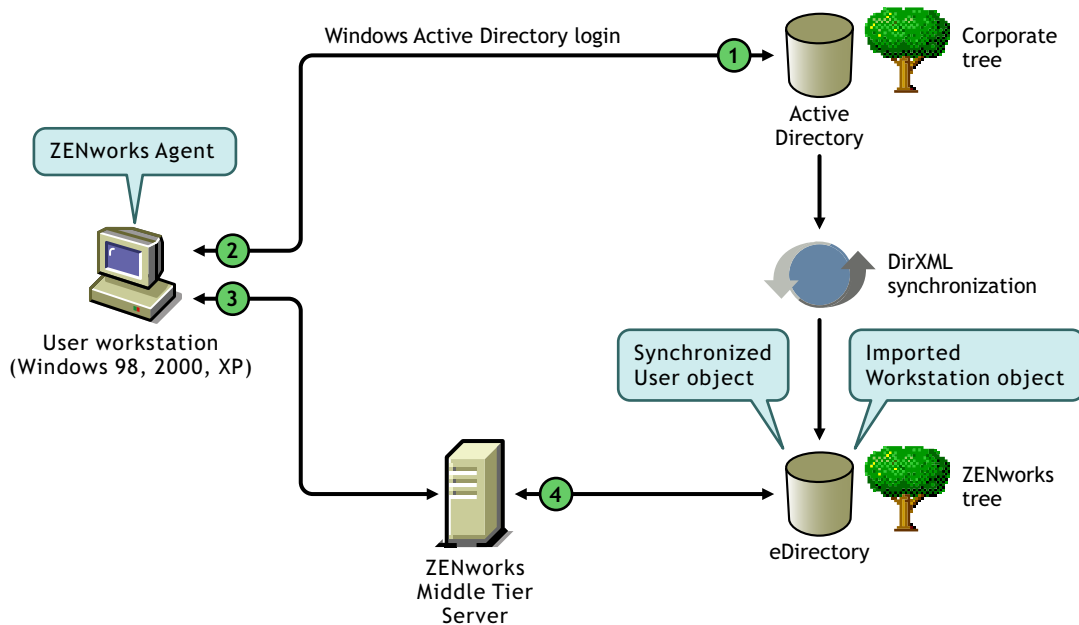


Table B-1 Steps in the Process of Using a ZENworks Tree in an Active Directory Environment

Step	Explanation
1	User authenticates to Active Directory.
2	The ZENworks Desktop Management Agent captures accepted user credentials.
3	The ZENworks Desktop Management Agent passes credentials to the ZENworks Middle Tier Server.
4	The user authenticates to the ZENworks tree through the ZENworks Middle Tier Server.

For more information about pass through login, see “[Synchronized Passthrough Login](#)” in “[Setting Up Authentication](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

B.3 The ZENworks Tree in an eDirectory Environment

If you have an eDirectory corporate tree, you can authenticate to a separate ZENworks Tree (with User objects synchronized with the corporate tree) whether you choose to use the Novell Client or the ZENworks Management Agent in combination with the ZENworks Middle Tier Server.

This section contains the following information:

- [Section B.3.1, “Using the Novell Client,” on page 77](#)
- [Section B.3.2, “Using the Desktop Management Agent,” on page 77](#)

B.3.1 Using the Novell Client

When users log in using the Novell Client, its login gathers user credentials and authenticates to the corporate tree and to the designated ZENworks tree.

The following illustration shows a simplified process of using the Novell Client to authenticate to a ZENworks tree while simultaneously authenticating to the corporate tree.

Figure B-2 Using the Novell Client to Authenticate to a ZENworks Tree

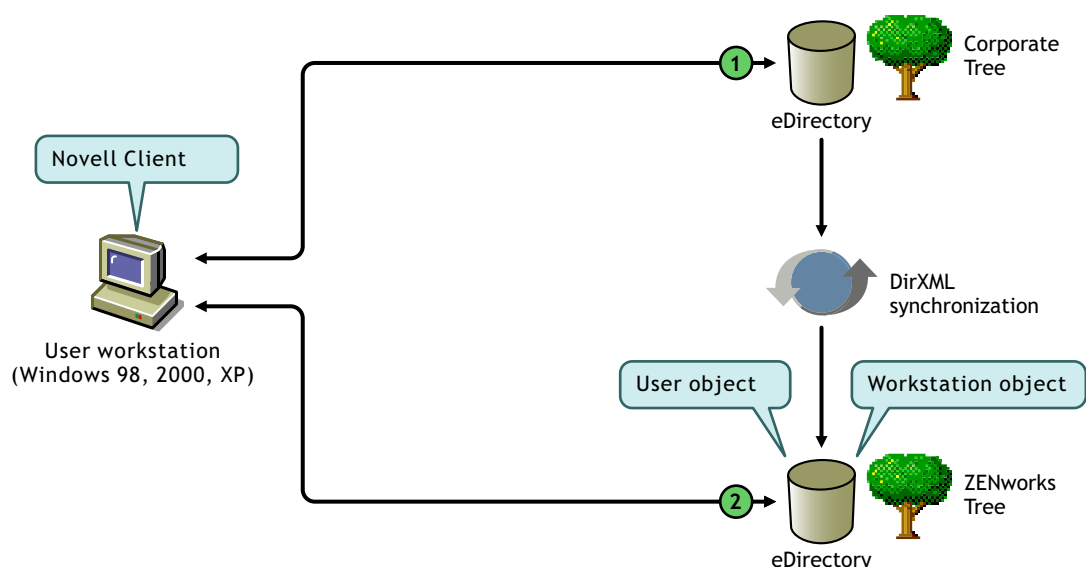


Table B-2 Steps in the Process of Using the Novell Client to Authenticate to a ZENworks Tree

Step	Explanation
1	The user authenticates to the corporate tree.
2	The user authenticates to the ZENworks tree.

B.3.2 Using the Desktop Management Agent

If only the ZENworks Desktop Management Agent is installed on workstations, depending on whether pass through is set up, the credentials supplied at the local login dialog box (or at the Agent login if pass through fails) are captured by the ZENworks login and are used to authenticate to both the corporate tree and to the ZENworks tree.

Authenticating to Primary and Secondary Domains

If you set up a ZENworks tree and you plan to use the Desktop Management Agent and the Middle Tier Server to authenticate, you can designate the ZENworks tree as the first authentication site or “primary authentication domain” and the corporate eDirectory tree as a subsequent authentication site, or “secondary authentication domain.” For more information about setting up authentication domains, see [“Authentication Domains \(Xtier 2.6.2 installation\)” on page 52](#).

If an eDirectory object exists in the primary domain and is successfully authenticated, the ZENworks Middle Tier Server looks for the presence of the same object in the secondary domain. If the object exists in the secondary domain there is a successful authentication to the secondary domain. If the object does not exist in the secondary domain, eDirectory fails the authentication to that domain only.

IMPORTANT: The context structure of the primary domain and the secondary domain must be identical (including leaf objects that might be authenticated, such as users or workstations) in order for the authentication to complete successfully.

The following illustration shows a simplified process of using the Desktop Management Agent to authenticate to a primary domain.

Figure B-3 Using the Desktop Management Agent to Authenticate to a Primary Domain

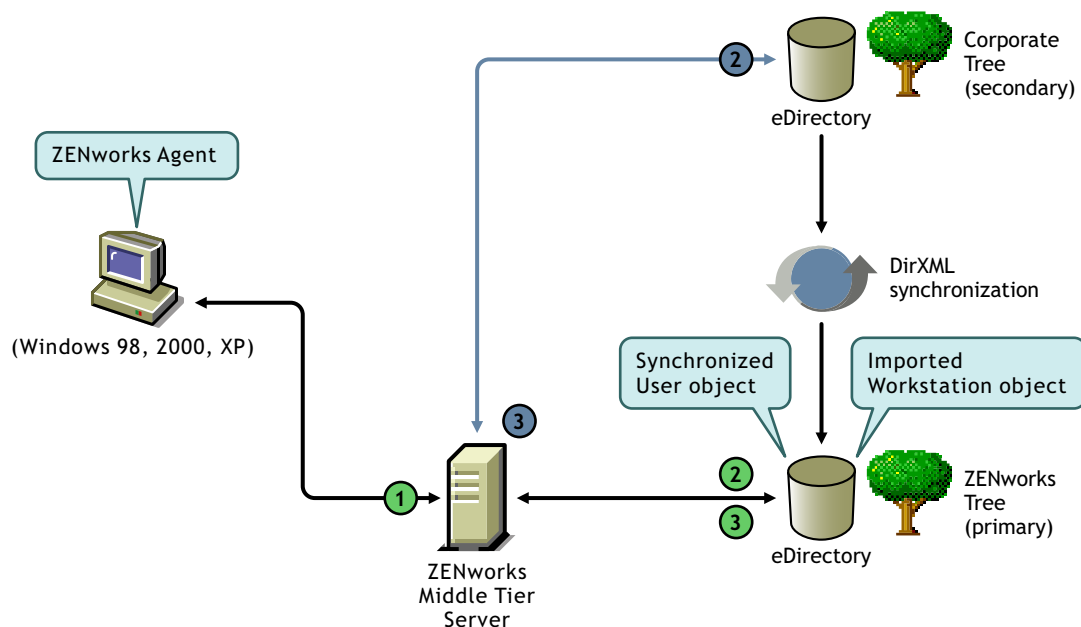


Table B-3 Steps in the Process of Using the Desktop Management Agent to Authenticate to a Primary Domain

Step	Explanation
①	The workstation attempts authentication.
②	The ZENworks Middle Tier Server passes credentials to the primary domain (the ZENworks tree).
②	The Middle Tier Server passes credentials to the secondary domain (the corporate tree).
③	The workstation authenticates to the ZENworks tree through the Middle Tier Server.
③	The workstation fails to authenticate through the Middle Tier Server.

The primary/secondary domain setup is particularly useful if, for example, all of your ZENworks objects, including workstations, are in the ZENworks tree, while other critical eDirectory objects (GroupWise objects, for example) are in the corporate tree. In this scenario, the primary

authentication would be to the ZENworks tree, where workstations exist, then to the corporate tree, where workstations do not exist. Many ZENworks applications and policies (Workstation Inventory policies, in particular) are associated to workstations only. If none of your policies or applications are associated with workstations, it is not necessary to designate the ZENworks tree as the primary authentication domain.

E-Mail and Dotted Name Login Support

C

If you want, you can allow users to log in to the network through the ZENworks Middle Tier Server using the same syntax they might be accustomed to when sending e-mail, or you might want them to log in with a more fully-qualified or perhaps a more simplified name that matches your authentication scheme.

Although ZENworks 7 Desktop Management does not enable e-mail or dotted name logins by default (because of the complex process used by the Middle Tier Server to find the user and because of the network traffic this process might generate), both login methods can be used for authentication when using the Desktop Management Agent.

IMPORTANT: This functionality (dotted-name support) applies for the user name only, not the user's context. The ZENworks Middle Tier Server does not support authentication to a dotted name in the root context of the eDirectory tree: that is, authentication contexts configured for the Middle Tier must not contain any embedded dots. For more information, see TID 10098582 in the [Novell Support Knowledgebase \(http://support.novell.com/search/kb_index.jsp\)](http://support.novell.com/search/kb_index.jsp).

This section explains these login methods and how to configure a workstation to use them. It includes the following information:

- [Section C.1, “E-Mail Formatted Names,” on page 81](#)
- [Section C.2, “Non-E-Mail Formatted Names,” on page 82](#)
- [Section C.3, “Enabling E-Mail and Dotted Name Login Support,” on page 82](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

C.1 E-Mail Formatted Names

E-mail formatted names have the following characteristics:

- They are considered short names, not partial contexts or distinguished names.
- They do not contain escaped (that is, “\.”) periods.
- They are found by the common name attribute in LDAP.

The following are some examples of e-mail formatted names:

tjones@example.com
tom.jones@example.com
tom.v.jones@example.com
tom@jones@miami.example.com

C.2 Non-E-Mail Formatted Names

Non-e-mail formatted names are those that:

- Begin or end with a period. Login names in this format are considered to be “fully qualified distinguished names” (FQDN).
- Include both a period and an escaped period (that is, “\.”). Login names in this format are considered to be “fully qualified names.”

The following are some examples of non-e-mail formatted names:

tom\.v\.jones.miami.example.acme_inc.(FQDN)

tom\.v\.jones.miami.example(FQDN)

tom.v.jones.miami.example

tom.v.jones

tom@jones

If a name includes a period, the Middle Tier Server attempts to authenticate it first as a FQDN. If that authentication fails, the Middle Tier attempts to authenticate the name with the periods escaped (“\.”) beginning from left to right. If that authentication fails, the Middle Tier attempts an LDAP search from each configured base distinguished name.

C.3 Enabling E-Mail and Dotted Name Login Support

At the authentication DNS or IP address entry under the authentication domains key, you can add DWORD values to control dotted name support and e-mail name support. The table below shows these values and their possible settings.

Table C-1 *DWORD Values and Settings Used to Control Dotted Name and e-Mail Name Support*

Type of Login Name Support	Setting
Dotted Name Support	1 or 0 (default)
E-Mail Name Support	1 or 0 (default)

At the context entry under the authentication DNS or IP address key, you can add DWORD values to control whether the entered name is attempted as an appendage to the context and whether to attempt an LDAP search from the context. The table below shows these values and their possible settings.

Table C-2 *DWORD Values and Settings Used to Control Dotted name and e-Mail Name Searches*

Type of Search Attempt	Setting
Append Context	1 (default) or 0
LDAP Search	1 (default) or 0

If you specify the Dotted Name Support value as 1 (enabled) at the authentication domain entry, then LDAP Search at the authentication context is always attempted.

NOTE: The registry does not allow a “\” in a key name. This means you cannot use a dotted context in the configuration.

Using the Novell Kerberos KDC to Support ZENworks Dynamic Local Users

D

Kerberos*, an authentication protocol developed at MIT, requires entities (for example, a user and a network service) that need to communicate over an insecure network to prove their identity to one another so that secure authentication can take place.

The Kerberos protocol has been proven to be highly trusted and valuable security tool for providing secure network authentication. Kerberos functionality is included natively in a Windows* Active Directory* environment, but there are administrators who want to use Kerberos with Novell® eDirectory® (in conjunction with the dynamic local user (DLU) accounts created by ZENworks® Desktop Management) in their NetWare® or Linux environments.

Kerberos requires the use of a Key Distribution Center (KDC) to act as a trusted third party between these entities. Novell has created a proprietary, Linux-based implementation of the KDC that makes eDirectory® its core authentication and identity authority and allows full Kerberos authentication of ZENworks DLU accounts. The Novell Kerberos KDC provides a single point of management, with the advantage of eDirectory replication and security capabilities. It moves Kerberos-specific data to eDirectory and provides Kerberos services using a KDC that accesses data stored in eDirectory.

The information in this section describes how to set up the Novell Kerberos KDC for use in a ZENworks DLU environment.

If you want more specific information about the Novell Kerberos KDC, see the [Novell Kerberos KDC documentation \(http://www.novell.com/documentation/kdc/\)](http://www.novell.com/documentation/kdc/) on the Novell product documentation Web site.

This section includes the following information:

- [Section D.1, “Kerberos Terms,” on page 85](#)
- [Section D.2, “Kerberos KDC Services,” on page 86](#)
- [Section D.3, “Things to Know Before Setting Up the Novell Kerberos KDC for ZENworks DLU,” on page 87](#)
- [Section D.4, “Setting Up the Novell Kerberos KDC for ZENworks DLU,” on page 87](#)

D.1 Kerberos Terms

The following table lists some of the terms that you need to understand as you set up the Novell Kerberos KDC.

Table D-1 *Important Kerberos Terms*

Kerberos Term	Definition
Key (also referred to as Secret Key)	An encryption key shared by a principal and the KDC, distributed outside the system, with a long lifetime. In the case of a user's principal, the key is derived from a password.
Principal	An entity in the network. Each entity corresponds to a principal.
Realm	A logical grouping of principals.
Service	A resource provided to network clients, such as a server holding a ZENworks policy or an application.
Service ticket	A record required to access services in the network.
Session key	A temporary encryption key used between two principals, with a lifetime limited to the duration of a single login session.
Ticket	A record that helps a client authenticate itself to a server. It contains information such as client's identity, a session key, a timestamp, and other information—all sealed using the server's secret key.
Ticket Granting Ticket (TGT)	The initial ticket obtained after a successful login. This ticket is used to get the service ticket to access a service.

D.2 Kerberos KDC Services

A KDC contains the identities and keys of every principal in the network that it must service within its realm. This principal information is stored in a local database within the KDC. In the Novell Kerberos KDC, the principal and realm information is stored in eDirectory.

The following tables list some of the services provided by a typical KDC (including the Novell Kerberos KDC):

- [Table D-2, “Basic KDC Services and Their Purpose,” on page 86](#)
- [Table D-3, “KDC Services Used to Manage KDC and Kerberos Principals,” on page 87](#)

Table D-2 *Basic KDC Services and Their Purpose*

Basic KDC Service	Purpose
Authentication Server (AS)	Issues authentication credentials known as Ticket Granting Tickets (TGT) to users while logging in.
Ticket Granting Server (TGS)	Issues service tickets to the users in response to their requests accompanied by TGT so that they can access various services in the realm.

Table D-3 KDC Services Used to Manage KDC and Kerberos Principals

KDC Service	Purpose
Kerberos Administration Server	Server component for maintaining Kerberos principals, policies, and service key tables (keytabs). This server responds to the requests from the <code>kadmin</code> and <code>kpasswd</code> utilities.
Kerberos Administration Utilities	Client component (such as <code>kadmin</code> , <code>kadmin.local</code> , and <code>kdb5_util</code>) for maintaining Kerberos realms, principals, policies, and service key tables.
Kerberos Password Server	Server component of the Kerberos Password utility for changing passwords of Kerberos principals.
Kerberos Client Utilities	Utilities such as <code>kinit</code> and <code>kpasswd</code> , which are used for various operations like login and changing passwords.

D.3 Things to Know Before Setting Up the Novell Kerberos KDC for ZENworks DLU

Before you begin the setup of the Novell Kerberos KDC for ZENworks DLU, you need to know the following:

- Time synchronization is required to be able to have a working Kerberos environment, make sure that the workstation time varies no more than five minutes from the server time.
- The Kerberos configuration file is located at `/etc/krb5.conf`.
- Kerberos credentials must stay in sync with eDirectory credentials in order to authenticate the user.
- Similar to Active Directory, there is a two step process used for preparing an end user account for Kerberos. Just as in Active Directory, you need to manually add the user principal to the server and then you need to add the workstation principal to the server. In Active Directory this is done when a workstation is added to the domain. With the Novell KDC, you need to use `ksetup.exe` to configure the workstation and then use `kadmin.local` (installed with the Novell KDC) to add it to the server using a process similar to adding a user principal.
- Commands are case sensitive. Make sure the commands are entered correctly.

D.4 Setting Up the Novell Kerberos KDC for ZENworks DLU

This section includes the following information:

- [Section D.4.1, “Setting Up the Linux Server,” on page 88](#)
- [Section D.4.2, “Setting Up the KDC for Windows Workstations,” on page 89](#)
- [Section D.4.3, “Setup Options,” on page 90](#)

NOTE: You need to know the following about the sample setup shown below:

- The Kerberos Realm name is `KERBEROS.YOURCOMPANY.COM`.
- The Kerberos username is `testuser`.

- Kerberos workstation is `testworkstation`.
 - The eDirectory root context is `Novell`.
 - The Kerberos user context is `Users.Novell`.
 - The supported encryption types are `des-cbc-crc` and `hmac`. These are exclusive.
 - Commands are case sensitive. Make sure that the commands are entered correctly.
-

D.4.1 Setting Up the Linux Server

Use the following sample procedure for setting up the KDC to run Kerberos authentication on a SLES 9 (or later) server:

- 1 Install Novell eDirectory 8.8.1 for Linux, available from the *ZENworks 7 Desktop Management with SPI Companion 1* CD.
- 2 Download (<http://download.novell.com/Download?buildid=SqdluPPy8KE~>) the Novell Kerberos KDC for Linux from the Novell Download site.
- 3 Using the [documentation for the Novell Kerberos KDC](http://www.novell.com/documentation/kdc/) (<http://www.novell.com/documentation/kdc/>), install the Novell Kerberos KDC for Linux.
- 4 Enter the following commands to set up the proper search paths, based on the installation location of the Novell Kerberos KDC:


```
export PATH=/opt/novell/kerberos/bin:/opt/novell/kerberos/sbin:$PATH
export LD_LIBRARY_PATH=/opt/novell/kerberos/lib:/opt/novell/lib:$LD_LIBRARY_PATH
```
- 5 Enter the following command to start the Kerberos daemon:


```
/etc/init.d/krb5kdc start
```
- 6 Run `kadmin.local` from the shell, then run the following commands for each user and workstation that you want to add to the Kerberos realm:

Command	Comments
<pre>addprinc -x userdn=cn=testuser,ou=Users,o=Novell -e des-cbc-crc:normal,rc4-hmac:normal -pw password testuser</pre>	<ul style="list-style-type: none"> • Type for each user (<code>testuser.Users.Novell</code>) in eDirectory, to create a corresponding Kerberos user principal • The command maps the eDirectory user (<code>testuser.Users.Novell</code>) to the kerberos user (<code>testuser</code>) • Make sure that the password for this newly created user principal is the same as the password for the user in eDirectory.

Command	Comments
<pre>addprinc -x containerdn=o=Novell -e rc4- hmac:normal,des-cbc-crc:normal -pw password host/ testworkstation.kerberos.yourcompany.com</pre>	<ul style="list-style-type: none"> • Type for each workstation (testworkstation). • Make sure that the password for this newly created workstation principal is the same as the password set with /SetComputerPassword in ksetup.exe on the Windows workstation.

- 7** From a new shell, run `tail -f /var/log/krb5kdc.log` before you attempt to connect to the Kerberos server. This command displays all messages or errors in the transaction.

NOTE: In this sample setup, `testuser.Users.Novell` is a user in eDirectory. The workstation (testworkstation) is a workstation to add to the Kerberos realm / domain, not necessarily in eDirectory.

D.4.2 Setting Up the KDC for Windows Workstations

Use the following sample procedure for setting up the KDC to run Kerberos authentication on Windows workstations:

- 1** Download (<http://download.microsoft.com/>) the `ksetup.exe` utility from Microsoft. The utility is included in the support tools for Windows workstations.
- 2** Set up the workstation's Kerberos information:
 - 2a** (Optional) Run the following commands from the Windows command line:

Command	Comment
<code>ksetup /SetRealm UPPERCASE_REALM_NAME</code>	Obtain the Realm Name from the <code>/etc/krb5.conf</code> file.
<code>ksetup.exe /AddKdc UPPERCASE_REALM_NAME KDC_DNS_name</code>	This command associates the Kerberos server to the Realm where the computer belongs so that the workstation recognizes the server that it needs to contact.
<code>ksetup.exe /AddKpasswd UPPERCASE_REALM_NAME Kerberos_Password_Server_DNS_name</code>	This command allows access to the Password Server so that you can change Kerberos user passwords from the workstation GINA.

Command	Comment
<code>ksetup.exe /SetComputerPassword computer_password_for_Kerberos_authentication</code>	This command sets the workstation password to authenticate to the Kerberos server. The password must be the same on both the workstation and the server.

- 2b** (Optional) Run a batch file with the following configuration (modified according to your Kerberos server) from the Windows command line:

```
@echo off
ksetup.exe /SetRealm KERBEROS.YOURCOMPANY.COM
ksetup.exe /AddKdc KERBEROS.YOURCOMPANY.COM
your_kerberos_server.your_company.com
ksetup.exe /SetComputerPassword password
ksetup.exe /AddKpasswd KERBEROS.YOURCOMPANY.COM novell
ksetup.exe /MapUser testuser@KERBEROS.YOURCOMPANY.COM testuser
ksetup.exe
```

- 3** Reboot the workstation.

D.4.3 Setup Options

Although ZENworks DLU can do so, you have the option of adding users to the Windows Kerberos registry mappings (local users to kerberos user). Use the following procedure to add users:

- 1** Run the following command:

```
ksetup.exe /MapUser testuser@KERBEROS.YOURCOMPANY.COM testuser
```

The functionality for enabling DLU on the workstation is set in the Windows Registry at HKLM\Software\Novell\NWGina\Security. The DWORD value is AllowKerberosLoginWithDLU. When enabled, the setting is 1.

Ports Used by ZENworks 7 Desktop Management



This appendix includes information regarding the IP ports used by Novell® ZENworks® Desktop Management, including those that should be open and available for use by various ZENworks components.

Table E-1 Ports Used by ZENworks 7 Desktop Management

ZENworks Component Using the Port(s)	Port(s) Used	Service	Protocols
ZENworks Middle Tier Server to Source File Server	524	NCP	TCP, UDP
ZENworks Middle Tier Server to Authentication Domain	389, 636	LDAP	TCP
ZENworks Middle Tier Server to Source File Server	445	CIFS	
ZENworks Middle Tier Server to Desktop Management Server - AWI	8039		
Novell Application Launcher™ using NCP (server and client)	524	NCP	TCP, UDP
Web Server (Middle Tier Server to the Internet)	80, 8080, 443, 8089	HTTP, HTTPS	TCP
Remote Control	80	HTTP	TCP, UDP
Remote Control	524	NCP	TCP, UDP
Remote Control Management Agent (client)	1761 (configurable)		TCP, UDP
Remote Control Listener Port (from ConsoleOne®)	1762 (configurable)		TCP
Service Location Protocol (server)	427		TCP, UDP
Service Location Protocol (client - ephemeral)	1024-1500		UDP
ZENworks Preboot Services: DHCP and Proxy DHCP Servers - PXE (server)	67		TCP, UDP
ZENworks Preboot Services: DHCP and Proxy DHCP Servers - Client Requests (server)	68		TCP, UDP
ZENworks PXE TFTP Server	69		UDP
PXE RPC Port Map Server (Sun RPC)	111		UDP
MTFTP Listener (server)	360		UDP
PXE (Windows Server)	524		

ZENworks Component Using the Port(s)	Port(s) Used	Service	Protocols
PXE Imaging Server Engine	997		
ZENworks Imaging Server	998		TCP
ZENworks Preboot Services: DHCP and Proxy DHCP Servers	4011		UDP
PXE Transaction Server	18753		UDP
Workstation Import Server (AWI server)	8039		TCP
MS SQL Inventory Database JDBC Driver (server)	1433		
Oracle Inventory Database JDBC Driver (server)	1521		
ZENworks Inventory Database (server)	2544		TCP
ZENworks Inventory Database (server)	2638 (configureable)	sybaseanywhere	TCP
ZENworks Inventory Sybase Database	2639 (configureable)		TCP
ZENworks Inventory Sybase Database	2640 (configureable)		TCP
ZENworks Inventory Service	8080	HTTP	TCP
ZENworks Inventory Proxy Port	65000		TCP

Documentation Updates

F

This section contains information on documentation content changes that have been made in this section of the *Administration* guide since the initial release of Novell® ZENworks® 7 (August 26, 2005). The information will help you to keep current on updates to the documentation.

All changes that are noted in this section were also made in the documentation. The documentation is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the documentation changes listed in this section.

The documentation update information is grouped according to the date the changes were published. Within a dated section, the changes are alphabetically listed by the names of the main table of contents sections for ZENworks 7 Personality Migration.

If you need to know whether a copy of the PDF documentation you are using is the most recent, the PDF document contains the date it was published on the front title page.

The documentation was updated on the following dates:

- [Section F.1, “July 14, 2006 \(Support Pack 1\),” on page 93](#)
- [Section F.2, “January 31, 2006,” on page 94](#)
- [Section F.3, “December 23, 2005,” on page 94](#)
- [Section F.4, “December 9, 2005,” on page 95](#)

F.1 July 14, 2006 (Support Pack 1)

The following note was added to each section:

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

Updates were also made to the following sections. The changes are explained below.

- [Section F.1.1, “Appendix D: Using the Novell Kerberos KDC to Support ZENworks Dynamic Local Users,” on page 93](#)
- [Section F.1.2, “Understanding the ZENworks Middle Tier Server and the Desktop Management Server,” on page 94](#)

F.1.1 Appendix D: Using the Novell Kerberos KDC to Support ZENworks Dynamic Local Users

The following changes were made in this section:

Location	Change
Appendix D, "Using the Novell Kerberos KDC to Support ZENworks Dynamic Local Users," on page 85	Newly-added appendix.

F.1.2 Understanding the ZENworks Middle Tier Server and the Desktop Management Server

The following changes were made in this section:

Location	Change
Section 3.2.3, "Configuring the ZENworks Middle Tier Server with NSAdmin," on page 48	Added the following sentence: "It is not necessary to restart Tomcat or Apache or any other service in order for the changes made in NSAdmin to take effect."

F.2 January 31, 2006

Updates were made to the following sections. The changes are explained below.

- Section F.2.1, "Appendix E: Ports Used by ZENworks 7 Desktop Management," on page 94

F.2.1 Appendix E: Ports Used by ZENworks 7 Desktop Management

The following changes were made in this section:

Location	Change
Appendix E, "Ports Used by ZENworks 7 Desktop Management," on page 91	Newly-added appendix.

F.3 December 23, 2005

Updates were made to the following sections. The changes are explained below.

- Section F.3.1, "Understanding the ZENworks Middle Tier Server and the Desktop Management Server," on page 94

F.3.1 Understanding the ZENworks Middle Tier Server and the Desktop Management Server

The following changes were made in this section:

Location	Change
Section 3.1, "What Is the ZENworks Middle Tier Server?," on page 47	Added information to reflect the installation of ZENworks Middle Tier Server on OES Linux and SLES 9 SP1 servers.

F.4 December 9, 2005

The page design in the guide was reformatted to comply with revised Novell documentation standards.

Checking the ZENworks Desktop Management Installation



The purpose of this section of the Novell® ZENworks® 7 Desktop Management documentation is to help you understand the methods you can use to help you check for a successful installation of ZENworks components and to help you change the configuration of some of those components. The section contains the following information:

- Chapter 6, “Checking the Installation of Desktop Management Components on Servers,” on page 99
- Appendix G, “Documentation Updates,” on page 115

Checking the Installation of Desktop Management Components on Servers

This section of the *Novell® ZENworks® 7 Desktop Management Administration Guide* includes information that can help you check the installed Desktop Management components on Windows, NetWare®, or Linux servers. The following items are included in this section:

- [Section 6.1, “Determining the Version of ZENworks Components Installed on a NetWare or Windows Server,” on page 99](#)
- [Section 6.2, “Using Logging Methods to Check ZENworks on NetWare and Windows Servers,” on page 110](#)
- [Section 6.3, “Identifying Processes Started by the Linux Installation,” on page 111](#)
- [Section 6.4, “Determining the Version of ZENworks Components Installed on a Linux Server,” on page 113](#)

6.1 Determining the Version of ZENworks Components Installed on a NetWare or Windows Server

If you need to be certain about which version of ZENworks Desktop Management or its components is installed on a Windows or NetWare server, use the following information included this section:

- [Section 6.1.1, “Using Zenver.exe,” on page 99](#)
- [Section 6.1.2, “Registry Entries Containing Version Information,” on page 99](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

6.1.1 Using Zenver.exe

The easiest way to determine the version of ZENworks Desktop Management that is running on the NetWare or Windows server is to run `zenver.exe` from the `\public` directory of the server where ZENworks has been installed. The major version and support pack version of ZENworks Desktop Management is displayed at the command line.

6.1.2 Registry Entries Containing Version Information

This section lists the registry entries (workstation and server) made by ZENworks 7 Desktop Management installation programs. These entries contain the product version information for this release. The Workstation Inventory scanner software uses these entries to determine and report the Desktop Management component and version that are installed. If you need to contact Novell

Support, you can convey this version information to support technicians who will use it to better understand and troubleshoot any problems you may be having.

The section contains the following information:

- “Version Information Available on Windows Workstations” on page 100
- “Version Information Available on a Windows Server” on page 102
- “Version Information Available on NetWare Servers” on page 107

NOTE: The format for build dates in the registry is *ymmdd*.

Version Information Available on Windows Workstations

Registry information in this section is organized according to the registry data available on Windows workstations for the following installed ZENworks agents:

- “One or More of the ZENworks Desktop Management Agents Installed to the Workstation” on page 100
- “Inventory Agent on a Windows Workstation” on page 101
- “Remote Management Agent on a Windows Workstation” on page 101
- “Application Management Agent on a Windows Workstation” on page 101
- “Imaging Agent on a Windows Workstation” on page 102
- “Workstation Manager Agent on a Windows Workstation” on page 102

One or More of the ZENworks Desktop Management Agents Installed to the Workstation

The registry keys and values indicating that one or more of the ZENworks 7 Desktop Management Agents have been installed to the workstation are listed in the table below.

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Version	<i>7.build.revision</i>
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Support Pack	0
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Display Name	ZENworks Desktop Management Agent
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\InstallPath	<i>Install Path - Install Root Directory</i> Example: C:\program files\novell\zenworks
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Langauge	<i>Language ID</i> Example: 1033 (for English)
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\ProductGUID	<i>MSI Product GUID</i>

Inventory Agent on a Windows Workstation

The registry keys and values indicating that the ZENworks 7 Desktop Management Inventory Agent has been installed are listed in the table below.

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Inventory\Version	<i>7.build.revision</i>
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Inventory\Support Pack	0
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Inventory\Display Name	Desktop Management Inventory Agent
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Inventory\InstallPath	<i>Install Path</i>

Remote Management Agent on a Windows Workstation

The registry keys and values indicating that the ZENworks 7 Desktop Management Remote Management Agent has been installed are listed in the table below.

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Remote Management\Version	<i>7.build.revision</i>
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Remote Management\Support Pack	0
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Remote Management\Display Name	ZENworks Desktop Management Remote Management Agent
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Remote Management\InstallPath	<i>Install Path</i>

Application Management Agent on a Windows Workstation

The registry keys and values indicating that the ZENworks 7 Desktop Management Application Management Agent has been installed are listed in the table below.

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Application Management\Version	<i>7.build.revision</i>
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Application Management\Support Pack	0

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Application Management\Display Name	ZDM Application Management Agent
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Application Management\InstallPath	<i>Install Path</i>

Imaging Agent on a Windows Workstation

The registry keys and values indicating that the ZENworks 7 Desktop Management Imaging Agent has been installed are listed in the table below.

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Imaging\Version	<i>7.build.revision</i>
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Imaging\Support Pack	0
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Imaging\Display Name	ZDM Imaging Agent
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Imaging\InstallPath	<i>Install Path</i>

Workstation Manager Agent on a Windows Workstation

The registry keys and values indicating that the ZENworks 7 Desktop Management Workstation Manager Agent has been installed are listed in the table below.

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Workstation Manager\Version	<i>7.build.revision</i>
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Workstation Manager\Support Pack	0
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Workstation Manager\Display Name	ZDM Workstation Manager Agent
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Agent\Workstation Manager\InstallPath	<i>Install Path</i>

Version Information Available on a Windows Server

Registry information in this section is organized according to the registry data available on a Windows server for the following installed ZENworks servers:

- “ZENworks Desktop Management Server Components Installed to the Windows Server” on page 103

- “Application Management Server Component on a Windows Server” on page 103
- “Remote Management Server Component on a Windows Server” on page 104
- “NAL Database Server Component on a Windows Server” on page 104
- “Inventory Database Server Component on a Windows Server” on page 104
- “Inventory Server Component on a Windows Server” on page 105
- “Inventory (XML) Proxy Server Component on a Windows Server” on page 105
- “Imaging Server Component on a Windows Server” on page 105
- “Preboot Services Server Component on a Windows Server” on page 106
- “Workstation Import/Removal Server Component on a Windows Server” on page 106
- “ZENworks Middle Tier Server on a Windows Server” on page 106

ZENworks Desktop Management Server Components Installed to the Windows Server

The registry keys and values used by all of the ZENworks 7 Desktop Management Server components when any of them have been installed on a Windows server are listed in the table below.

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Langauge	<i>Language ID</i> Example: 1033 (for English)
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Version	<i>7.build.revision</i>
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Support Pack	0

Application Management Server Component on a Windows Server

The registry keys and values indicating that the ZENworks 7 Desktop Management Application Management Server component has been installed on a Windows server are listed in the table below.

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\App Management Server\Version	<i>7.build.revision</i>
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\App Management Server\Support Pack	0
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\App Management Server\Display Name	ZENworks Application Management Server
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\App Management Server\Install Path	<i>Install Path</i>

Remote Management Server Component on a Windows Server

The registry keys and values indicating that the ZENworks 7 Desktop Management Remote Management Server component has been installed on a Windows server are listed in the table below.

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Remote Management Server\Version	<i>7.build.revision</i>
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Remote Management Server\Support Pack	0
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Remote Management Server\Display Name	ZENworks Desktop Management Remote Management Server
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\RMPPath	<i>Install Path</i>

NAL Database Server Component on a Windows Server

The registry keys and values indicating that the ZENworks 7 Desktop Management NAL Database Server component has been installed on a Windows server are listed in the table below.

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\NAL Database Server\Version	<i>7.build.revision</i>
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\NAL Database Server\Support Pack	0
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\NAL Database Server\Display Name	ZDM NAL Database Server
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\NALDBPath	<i>Install Path</i>

Inventory Database Server Component on a Windows Server

The registry keys and values that indicate that the ZENworks 7 Desktop Management Inventory Database Server component has been installed on a Windows server are listed in the table below.

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Inventory Database Server\Version	<i>7.build.revision</i>
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Inventory Database Server\Support Pack	0
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Inventory Database Server\Display Name	ZDM Inventory Database Server
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\InvDBPath	<i>Install Path</i>

Inventory Server Component on a Windows Server

The registry keys and values indicating that the ZENworks 7 Desktop Management Inventory Server component has been installed on a Windows server are listed in the table below.

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Inventory Server\Version	<i>7.build.revision</i>
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Inventory Server\Support Pack	0
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Inventory Server\Display Name	ZDM Inventory Server
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\InvSrvPath	<i>Install Path</i>

Inventory (XML) Proxy Server Component on a Windows Server

The registry keys and values indicating that the ZENworks 7 Desktop Management Inventory (XML) Proxy Server component has been installed on a Windows server are listed in the table below.

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\XMLProxy Server\Version	<i>7.build.revision</i>
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\XMLProxy Server\Support Pack	0
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\XMLProxy Server\Display Name	ZDM XML Proxy Server
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZWSPath	<i>Install Path</i>

Imaging Server Component on a Windows Server

The registry keys and values indicating that the ZENworks 7 Desktop Management Imaging Server component has been installed on a Windows server are listed in the table below.

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Imaging Server\Version	<i>7.build.revision</i>
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Imaging Server\Support Pack	0
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Imaging Server\Display Name	ZENworks Imaging Server
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Imaging Server\Install Path	<i>Install Path</i>

Preboot Services Server Component on a Windows Server

The registry keys and values indicating that the ZENworks 7 Desktop Management Preboot Services (PXE) Server component has been installed on a Windows server are listed in the table below.

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\PXE Server\Version	<i>7.build.revision</i>
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\PXE Server\Support Pack	0
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\PXE Server\Display Name	ZENworks PXE Server
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\PXE Server\Install Path	<i>Install Path</i>

Workstation Import/Removal Server Component on a Windows Server

The registry keys and values indicating that the ZENworks 7 Desktop Management Import/Removal Server component has been installed on a Windows server are listed in the table below.

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Workstation Import Server\Version	<i>7.build.revision</i>
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Workstation Import Server\Support Pack	0
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Workstation Import Server\Display Name	ZENworks Workstation Import Server
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Workstation Import Server\Install Path	<i>Install Path</i>

ZENworks Middle Tier Server on a Windows Server

The registry keys and values that indicate that the ZENworks 7 Middle Tier Server has been installed on a Windows server are listed in the table below.

Registry Key	Value
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Middle Tier Server\Version	<i>7.build.revision</i>
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Middle Tier Server\Support Pack	0
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Middle Tier Server\Display Name	ZENworks Middle Tier Server
HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\ZfD\Middle Tier Server\InstallPath	<i>Install Path</i>

Version Information Available on NetWare Servers

Registry information in this section is organized according to the registry data available on NetWare® servers for the following installed ZENworks servers:

- “ZENworks Desktop Management Server Components Installed to a NetWare Server” on page 107
- “Application Management Server Component on NetWare” on page 107
- “Remote Management Server Component on NetWare” on page 108
- “NAL Database Server Component on NetWare” on page 108
- “Inventory Database Server Component on NetWare” on page 108
- “Inventory Server Component on NetWare” on page 109
- “Inventory (XML) Proxy Server Component on NetWare” on page 109
- “Imaging Server Component on NetWare” on page 109
- “Preboot Services Server Component on NetWare” on page 109
- “Workstation Import/Removal Server Component on NetWare” on page 110
- “ZENworks Middle Tier Server on NetWare” on page 110

ZENworks Desktop Management Server Components Installed to a NetWare Server

The registry keys and values indicating that the ZENworks 7 Desktop Management Server has been installed on a NetWare server are listed in the table below.

Registry Key	Value
Software\Novell\ZENworks\ZfD\Language	<i>Language ID</i> Example: 1033 (for English)
Software\Novell\ZENworks\ZfD\Version	<i>7.build.revision</i>
Software\Novell\ZENworks\ZfD\Support Pack	0

Application Management Server Component on NetWare

The registry keys and values indicating that the ZENworks 7 Desktop Management Application Management Server component has been installed on a NetWare server are listed in the table below.

Registry Key	Value
Software\Novell\ZENworks\ZfD\App Management Server\Version	<i>7.build.revision</i>
Software\Novell\ZENworks\ZfD\App Management Server\Support Pack	0
Software\Novell\ZENworks\ZfD\App Management Server\Display Name	ZENworks Application Management Server
Software\Novell\ZENworks\ZfD\App Management Server\InstallPath	<i>Install Path</i>

Remote Management Server Component on NetWare

The registry keys and values indicating that the ZENworks 7 Desktop Management Remote Management Server component has been installed on a NetWare server are listed in the table below.

Registry Key	Value
Software\Novell\ZENworks\ZfD\Remote Management Server\Version	<i>7.build.revision</i>
Software\Novell\ZENworks\ZfD\Remote Management Server\Support Pack	0
Software\Novell\ZENworks\ZfD\Remote Management Server\Display Name	ZENworks Desktop Management Remote Management Server
Software\Novell\ZENworks\ZfD\RMPPath	<i>Install Path</i>

NAL Database Server Component on NetWare

The registry keys and values indicating that the ZENworks 7 Desktop Management NAL Database Server component has been installed on a NetWare server are listed in the table below.

Registry Key	Value
Software\Novell\ZENworks\ZfD\NAL Database Server\Version	<i>7.build.revision</i>
Software\Novell\ZENworks\ZfD\NAL Database Server\Support Pack	0
Software\Novell\ZENworks\ZfD\NAL Database Server\Display Name	ZDM NAL Database Server
Software\Novell\ZENworks\ZfD\NALDBPath	<i>Install Path</i>

Inventory Database Server Component on NetWare

The registry keys and values that indicate that the ZENworks 7 Desktop Management Inventory Database Server component has been installed on a NetWare server are listed in the table below.

Registry Key	Value
Software\Novell\ZENworks\ZfD\Inventory Database Server\Version	<i>7.build.revision</i>
Software\Novell\ZENworks\ZfD\Inventory Database Server\Support Pack	0
Software\Novell\ZENworks\ZfD\Inventory Database Server\Display Name	ZDM Inventory Database Server
Software\Novell\ZENworks\ZfD\InvDBPath	<i>Install Path</i>

Inventory Server Component on NetWare

The registry keys and values that indicate that the ZENworks 7 Desktop Management Inventory Server component has been installed on a NetWare server are listed in the table below.

Registry Key	Value
Software\Novell\ZENworks\ZfD\Inventory Server\Version	<i>7.build.revision</i>
Software\Novell\ZENworks\ZfD\Inventory Server\Support Pack	0
Software\Novell\ZENworks\ZfD\Inventory Server\Display Name	ZDM Inventory Server
Software\Novell\ZENworks\ZfD\InvSrvPath	<i>Install Path</i>

Inventory (XML) Proxy Server Component on NetWare

The registry keys and values that indicate that the ZENworks 7 Desktop Management Inventory Server component has been installed on a NetWare server are listed in the table below.

Registry Key	Value
Software\Novell\ZENworks\ZfD\XMLProxy Server\Version	<i>7.build.revision</i>
Software\Novell\ZENworks\ZfD\XMLProxy Server\Support Pack	0
Software\Novell\ZENworks\ZfD\XMLProxy Server\Display Name	ZDM XML Proxy Server
Software\Novell\ZENworks\ZfD\ZWSPath	<i>Install Path</i>

Imaging Server Component on NetWare

The registry keys and values indicating that the ZENworks 7 Desktop Management Imaging Server component has been installed on a NetWare server are listed in the table below.

Registry Key	Value
Software\Novell\ZENworks\ZfD\Imaging Server\Version	<i>7.build.revision</i>
Software\Novell\ZENworks\ZfD\Imaging Server\Support Pack	0
Software\Novell\ZENworks\ZfD\Imaging Server\Display Name	ZENworks Imaging Server
Software\Novell\ZENworks\ZfD\Imaging Server\InstallPath	<i>Install Path</i>

Preboot Services Server Component on NetWare

The registry keys and values indicating that the ZENworks 7 Desktop Management Preboot Services Server component has been installed on a NetWare server are listed in the table below.

Registry Key	Value
Software\Novell\ZENworks\ZfD\PXE Server\Version	<i>7.build.revision</i>

Registry Key	Value
Software\Novell\ZENworks\ZfD\PXE Server\Support Pack	0
Software\Novell\ZENworks\ZfD\PXE Server\Display Name	ZENworks PXE Server
Software\Novell\ZENworks\ZfD\PXE Server\InstallPath	<i>Install Path</i>

Workstation Import/Removal Server Component on NetWare

The registry keys and values indicating that the ZENworks 7 Desktop Management Workstation Import/Removal Server component has been installed on a NetWare server are listed in the table below.

Registry Key	Value
Software\Novell\ZENworks\ZfD\Workstation Import Server\Version	<i>7.build.revision</i>
Software\Novell\ZENworks\ZfD\Workstation Import Server\Support Pack	0
Software\Novell\ZENworks\ZfD\Workstation Import Server\Display Name	ZENworks Workstation Import Server
Software\Novell\ZENworks\ZfD\Workstation Import Server\InstallPath	<i>Install Path</i>

ZENworks Middle Tier Server on NetWare

The registry keys and values that indicate that the ZENworks 7 Middle Tier Server has been installed on a NetWare server are listed in the table below.

Registry Key	Value
Software\Novell\ZENworks\ZfD\Middle Tier Server\Version	<i>7.build.revision</i>
Software\Novell\ZENworks\ZfD\Middle Tier Server\Support Pack	0
Software\Novell\ZENworks\ZfD\Middle Tier Server\Display Name	ZENworks Middle Tier Server
Software\Novell\ZENworks\ZfD\Middle Tier Server\InstallPath	<i>Install Path</i>

6.2 Using Logging Methods to Check ZENworks on NetWare and Windows Servers

Information about the location of installation and debug logs for all of the ZENworks Desktop Management components installed on a NetWare or Windows server is included in [TID 10093312 \(http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093312.htm\)](http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093312.htm) in the Novell Knowledgebase. This information can be useful as you check and troubleshoot ZENworks components after they are installed.

6.3 Identifying Processes Started by the Linux Installation

The following processes—sometimes called “daemons” or “scripts”—are started by the ZENworks 7 Desktop Management installation on Linux servers, depending on what ZENworks components you have chosen to install. You can find these processes in the storage area for ZENworks scripts, which is the `/etc/init.d` directory.

Many of these processes also has a `.conf` file or a `.properties` file that you can use to configure its execution. The information included in the log file includes parameters you can use while running the process from the command line.

One such process is the creation of log files. Each `.conf` or `.properties` file includes information about the location of its log file and the logging levels you can set. The logging levels settings are explained in the list below:

The following table is a summary of some helpful information about the ZENworks processes.

Table 6-1 Summary of ZENworks Processes on Linux

Name of Process Script	ZENworks Service or Daemon	Configuration File	Log File
novell-zdm-aws	ZENworks Auto Workstation Import/ Removal	<code>/etc/opt/novell/zenworks/zdm/novell-zdm-aws.conf</code>	<code>/var/opt/novell/log/zenworks/aws.log</code> and <code>awsr.log</code> (Logging levels 0-3 are available)
novell-proxydhcp	ZENworks Preboot Services	<code>/etc/opt/novell/novell-proxydhcp.conf</code>	<code>/var/opt/novell/log/novell-proxydhcp.log</code> (Logging levels 0-4 are available)
novell-tftp	ZENworks Preboot Services	<code>/etc/opt/novell/novell-tftp.conf</code>	<code>/var/opt/novell/log/novell-tftp.log</code> (Logging levels 0-4 are available)
novell-zmgprebootpolicy	ZENworks Preboot Services	<code>/etc/opt/novell/zenworks/preboot/novell-zmgprebootpolicy.conf</code>	<code>/var/opt/novell/log/zenworks/preboot/novell-zmgprebootpolicy.log</code> (Logging levels 0-4 are available)
novell-zimgserv ¹	ZENworks Imaging Service	<code>/etc/opt/novell/zenworks/preboot/novell-zimgserv.conf</code>	<code>/var/opt/novell/log/zenworks/preboot/novell-zimgdbg.log</code>
novell-zdm-wol	ZENworks Remote Management	<code>/etc/opt/novell/zenworks/rm/*.properties</code>	<code>/var/opt/novell/log/zenworks/rm/novell-zdm-wol.log</code>
novell-tomcat4	ZENworks Middle Tier Server	<code>/etc/opt/novell/novell-tomcat4.conf</code>	<code>/var/opt/novell/tomcat4/catalina.out</code>

Name of Process Script	ZENworks Service or Daemon	Configuration File	Log File
apache2	ZENworks Middle Tier Server	/etc/apache2/httpd.conf	/var/log/apache2/error_log
novell-xregd	ZENworks Middle Tier Server	no .conf file other configuration utilities ³	/var/log/messages ²
novell-xsrvd	ZENworks Middle Tier Server	/etc/opt/novell/xtier/xsrvd/xsrvd.conf other configuration utilities ³	/var/log/messages and /var/opt/novell/xtier/xterrornn.log (The <i>nn</i> variable in the log file name represents a number between 1-10)
novell-zdm-sybase	ZENworks Inventory Service	n/a	n/a
novell-zfs	ZENworks Inventory Service	/etc/opt/novell/zenworks/zws.properties	n/a
novell-zdm-inv	ZENworks Inventory Service	/etc/opt/novell/zenworks/inv/*.properties	/var/opt/novell/log/zenworks/inv/novell-zdm-inv.log

¹novell-zimgserv is not a daemon in ZENworks 7 Desktop Management Services on Linux. It is loaded by Novell eDirectory™ and is run as a subprocess of eDirectory.

²The messages log is a general log used by the novell-xregd and the novell-xsrvd daemons.

³You can launch novell-xregd and novell-xsrvd by invoking the regedit and xsrvcfg utilities from an SSH session. Among other things, these utilities can be used to configure authentication domains. You must have the appropriate rights to use the regedit utility (the registry service), which is found in /opt/novell/xtier/bin/regedit. For more information about the xsrvcfg utility, see the [Novell NetStorage \(http://www.novell.com/documentation/oes/oes_readme/data/oes_readme.html#bu7fccc\)](http://www.novell.com/documentation/oes/oes_readme/data/oes_readme.html#bu7fccc) section of the Novell Open Enterprise Server (Linux) readme.

6.3.1 Controlling Individual ZENworks Processes

You can use some command line parameters for each of these processes when you change the directory to the location of the process and type the following command:

```
./process_script -parameter_name
```

The following command line parameters are available for these processes. Their purpose is self-explanatory.

```
start
stop
```

status
restart

6.3.2 Starting and Stopping All ZENworks Processes

You can use `./ZDMstart` to start and `./ZDMstop` to stop all of the ZENworks processes at once. Both of these utilities are found in the `/opt/novell/zenworks/bin` directory. You can also use the `./ZDMstart -status` command to show status for all of the ZENworks processes.

6.4 Determining the Version of ZENworks Components Installed on a Linux Server

You can list the version of the ZENworks components installed on your Linux server by running the version utility located in the `/opt/novell/zenworks/bin` directory called `novell-zdm-version`. For a list of the available parameters you can use with this utility, enter one of the following commands:

```
./novell-zdm-version -h  
./novell-zdm-version -help
```

The help for this utility lists the following:

```
Usage:  novell-zdm-version [options]Options:  
-l[list]: List component names with their display names  
-c[omponent] <c> : Show version information for component <c> only  
-p[ackages]      : Show package versions for each specified component  
-d[etails]      : Display all ZENworks-installable packages per  
component  
-s[howcommon]    : Show information about common components  
-h[elp]          : Display this help messageNotes:  
    1) Use the -l[list] option to get a mapping from component names  
to display names. The component names are used with the -c[omponent]  
option.  
    2) The -d[etails] option shows additional package dependency  
information for each component displayed.It implies the -p[ackages]  
option.  
    3) The -s[howcommon] option displays information about  
components (or packages) that are not directly selectable from the  
installer.
```


Documentation Updates



This section contains information on documentation content changes that have been made in this section of the *Administration* guide since the initial release of Novell® ZENworks® 7 (August 26, 2005). The information will help you to keep current on updates to the documentation.

All changes that are noted in this section were also made in the documentation. The documentation is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the documentation changes listed in this section.

The documentation update information is grouped according to the date the changes were published. Within a dated section, the changes are alphabetically listed by the names of the main table of contents sections for ZENworks 7 Personality Migration.

If you need to know whether a copy of the PDF documentation you are using is the most recent, the PDF document contains the date it was published on the front title page.

The documentation was updated on the following dates:

- [Section G.1, “July 14, 2006 \(Support Pack 1\),” on page 115](#)
- [Section G.2, “December 23, 2005,” on page 115](#)
- [Section G.3, “December 9, 2005,” on page 116](#)

G.1 July 14, 2006 (Support Pack 1)

The following note was added to each section:

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

G.2 December 23, 2005

Updates were made to the following sections. The changes are explained below.

- [Section G.2.1, “Checking the Installation of Desktop Management Components on Servers,” on page 115](#)

G.2.1 Checking the Installation of Desktop Management Components on Servers

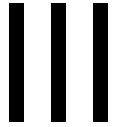
The following changes were made in this section:

Location	Change
Section 6.4, “Determining the Version of ZENworks Components Installed on a Linux Server,” on page 113	Moved the information in this section into a more generically named chapter so that all methods for determining versioning, for all server platforms are in the same chapter.

G.3 December 9, 2005

The page design in the guide was reformatted to comply with revised Novell documentation standards.

Automatic Workstation Import and Removal



The Automatic Workstation Import and Automatic Workstation Removal features of Novell® ZENworks® Desktop Management provide simplified, hands-off management of users' workstations.

Automatic Workstation Import imports workstations into Novell eDirectory™ and integrates them automatically. Automatic Workstation Removal removes obsolete workstation data from the directory and from the Inventory database.

The Workstation objects created by Automatic Workstation Import provide you with a way to push software and computer settings down to the workstations by using the Novell Application Launcher™ and Workstation Management policies. For more information about the Novell Application Launcher, see [Part V, “Application Management,” on page 227](#). For more information about Workstation Management policies, see [Part IV, “Workstation Management,” on page 131](#).

The following sections help you to understand, deploy, and use Automatic Workstation Import and Removal:

- [Chapter 7, “Understanding Automatic Workstation Import and Removal,” on page 119](#)
- [Chapter 8, “Setting Up Automatic Workstation Import and Removal,” on page 123](#)
- [Chapter 9, “Workstation Registration Files,” on page 127](#)
- [Appendix H, “Documentation Updates,” on page 129](#)

Understanding Automatic Workstation Import and Removal

7

Novell® ZENworks® Desktop Management Automatic Workstation Import includes Automatic Workstation Removal and provides management of the entire life cycle of a workstation, from the creation of its object to its removal.

The following sections help you to understand Automatic Workstation Import and Removal:

- [Section 7.1, “Understanding Workstation Import and Registration,” on page 119](#)
- [Section 7.2, “Server Considerations,” on page 121](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

7.1 Understanding Workstation Import and Registration

After you have installed Automatic Workstation Import using the ZENworks Desktop Management Server installation, importing workstations is a one-step process. The Workstation Registration program in the Desktop Management Agent accesses the Automatic Workstation Import service, which creates the Workstation object in Novell eDirectory™ and registers the workstation. For more information about using ZENworks Desktop Management with either the Novell Client™ or with the Desktop Management Agent, see [Part I, “Understanding ZENworks 7 Desktop Management,” on page 31](#). For more information about installing Automatic Workstation Import, see [“Installing the ZENworks Desktop Management Server” in the *Novell ZENworks 7 Desktop Management Installation Guide*](#).

The actual process of importing unregistered workstations into eDirectory depends on the physical location of the workstation (whether it is located inside or outside of the firewall).

If the workstation is located inside the firewall, the workstation accesses the Automatic Workstation Import service directly. In this scenario, the hostname (zenwsimport) must resolve to the Import Service as in previous versions of ZENworks.

If the workstation is located outside the firewall, the workstation accesses the ZENworks Desktop Management Middle Tier Server via HTTP using the Desktop Management Agent. The Middle Tier Server then acts as a proxy to pass the request on to the Automatic Workstation Import service. In this scenario, the hostname on the Middle Tier Server (zenwsimport) must resolve to the server running the import service. You should ping the server from the Middle Tier Server to make sure that it is pointing to the correct address.

The following sections provide additional information:

- [“Using the Import Service” on page 120](#)
- [“Registering Imported Workstations” on page 120](#)
- [“Removing Workstation Objects” on page 120](#)

7.1.1 Using the Import Service

The Automatic Workstation Import service creates network traffic; however, the import service is used only when one of the following occurs:

- A workstation boots and a corresponding Workstation object does not exist.

This is normally the first time the workstation is registered. The Automatic Workstation Import service initially creates the Workstation object in the tree, populates the object with default values, and updates the properties with the current registration information.

The Workstation Import policy is used to determine where the Workstation object is created and how it is named.

- A workstation attempts to log in to the tree and its Workstation object was either moved or renamed.

The registration program calls the import service to synchronize the workstation with its Workstation object.

At all other times when a workstation is logged in to the network, the Workstation Registration program registers the workstation and updates the Workstation object. The import service is not contacted for these operations, so network traffic to and from the Workstation Import service is not an issue. Workstations that authenticate and update Workstation objects still generate some network traffic.

For more information, see [Section 13.4, “Workstation Import Policy,” on page 153](#).

7.1.2 Registering Imported Workstations

After a workstation has been imported into the directory, it only needs to be registered each time it logs in to the tree. The Workstation Registration program updates the Workstation object when one of the following occurs:

- The Workstation Manager program starts
- A user logs in to the tree
- A Windows 2000/XP user logs out

The Workstation Registration program updates the workstation's registration time, network address, last server, and last user information.

Network traffic is minimized because the Workstation Registration program doesn't need to access the import service.

7.1.3 Removing Workstation Objects

You should periodically remove unused Workstation objects from the directory so that inventory reporting is more accurate.

Automatic Workstation Removal uses the Workstation Removal policy to determine when Workstation objects are considered to be unused so that they can automatically be removed from the directory.

Workstation objects can be automatically removed when a workstation has not been registered within the time frame you specify in the effective Workstation Removal policy.

You can specify any number of days for how long a workstation can go without registering before it is considered unused.

For more information, see [Section 13.5, “Workstation Removal Policy,” on page 159](#).

7.2 Server Considerations

Consider the following when setting up the server portion of Automatic Workstation Import and Removal:

- [“Selecting Servers for Deployment” on page 121](#)
- [“Using DNS Names or Hosts Files” on page 121](#)
- [“Scheduling Workstation Removal” on page 122](#)

7.2.1 Selecting Servers for Deployment

Generally, more workstations are imported than are removed. Therefore, you should have more servers set up with the Automatic Workstation Import service than with the Automatic Workstation Removal service.

To minimize network traffic, you should install the Automatic Workstation Import service on at least one server per WAN location. Automatic Workstation Removal does not generally produce a lot of network traffic, so it can be used across WAN links.

If you create a Server package in ZENworks Desktop Management 4.x or later, you cannot associate the package with a ZENworks for Desktops 3.x import server. You must associate it with a ZENworks Desktop Management 4.x or later import server.

7.2.2 Using DNS Names or Hosts Files

In setting up Automatic Workstation Import, you should use DNS for TCP/IP addresses so that hostnames can be found automatically, instead of setting up and maintaining a `hosts` file on every workstation.

Using DNS names in your network provides you with automated management of workstation importing. You should coordinate with your DNS administrator to set up IP addresses for your workstation import services according to physical location in order to allow workstations to contact the import service locally, rather than across WAN links.

You can differentiate IP addresses according to domain or zone by using multiple domains or by using primary and secondary zones. For example, you could have a DNS entry for Automatic Workstation Import using the following syntax:

```
zenwsimport.context_string.com
```

`Hosts` files can be used to handle exceptions, such as when you want a specific workstation to resolve to a specific workstation import service. A `hosts` file is useful for manually importing a workstation, such as in a test environment. For information about setting up a `hosts` file on a local workstation, see [“Setting Up a Hosts File on a Local Workstation” on page 122](#).

Setting Up a Hosts File on a Local Workstation

To set up workstation import on a local workstation, open and edit the `hosts` file on the local workstation.

For Windows 98, the `hosts` file's location should be:

```
Win98_drive:\Win98_directory\hosts
```

IMPORTANT: The default `hosts` file in Windows is named `hosts.sam`. Do not use the `.sam` extension with your filename. Rename `hosts.sam` to `hosts`, or make a copy and rename the copy. By default, Windows 98 hides filename extensions that are of a known type, so you should make sure that filename extensions are being displayed so that you can correctly rename the `hosts.sam` file to `hosts`.

For Windows 2000/XP, the `hosts` file's location should be:

```
Win_drive:\Win_directory\SYSTEM32\drivers\etc\hosts
```

Hosts as shown above is a filename, not a folder name.

The following is an example of the text you would add in a `hosts` file for Automatic Workstation Import:

```
151.155.155.55 zenwsimport
```

In this example, the TCP/IP address is for the server where you are running the Automatic Workstation Import service. “zenwsimport” is not the name of a server, but a DNS name that resolves to this TCP/IP address. In other words, `zenwsimport` is a label to identify the server as the one running the Automatic Workstation Import service.

7.2.3 Scheduling Workstation Removal

You should schedule workstation removal so that it is performed periodically when the network is least busy, such as during non-work hours.

Setting Up Automatic Workstation Import and Removal

8

When installing Novell® ZENworks® Desktop Management, you can specify import and removal roles for selected servers. Therefore, before running the ZENworks Desktop Management installation program, you should determine which servers you want to run the import service, the removal service, or both. For further information on selecting servers to run each service, see [“Selecting Servers for Deployment” on page 121](#).

To deploy Automatic Workstation Import and Removal, we recommend the following sequence:

1. Install the Automatic Workstation Import and Removal service software. For more information, see [“Installing the ZENworks Desktop Management Server”](#) in the *Novell ZENworks 7 Desktop Management Installation Guide*.
2. Set up the Automatic Workstation Import and Removal policies. For more information, see [Section 8.1, “Setting Up the Automatic Workstation Import and Removal Policies,” on page 124](#).
3. Set up DNS names and customize logging.
Using DNS names is preferable to using `hosts` files for registering workstations because `hosts` files must be managed manually at each workstation.
4. Install the Novell Client™ and/or the Desktop Management Agent on the workstations. For more information, see [“User Workstation Hardware Requirements”](#) and [“User Workstation Software Requirements”](#) in the *Novell ZENworks 7 Desktop Management Installation Guide*.

After you have completed this sequence, Automatic Workstation Import and Removal is functional.

Before completing the tasks in the following sections, you should have already installed the Automatic Workstation Import and Removal software during your installation of ZENworks Desktop Management. For more information, see [“Installing the ZENworks Desktop Management Server”](#) in the *Novell ZENworks 7 Desktop Management Installation Guide*.

The following sections contain steps to help you set up Automatic Workstation Import and Removal:

- [Section 8.1, “Setting Up the Automatic Workstation Import and Removal Policies,” on page 124](#)
- [Section 8.2, “Setting Up Automatic Workstation Import and Removal to Run on the Servers,” on page 124](#)
- [Section 8.3, “Using the Novell Client and the ZENworks Desktop Management Agent,” on page 125](#)
- [Section 8.4, “Verifying that Automatic Workstation Import and Removal are Working,” on page 125](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

8.1 Setting Up the Automatic Workstation Import and Removal Policies

The following sections help you to configure and associate the necessary policies:

- “Configuring the Automatic Workstation Import Policy” on page 124
- “Configuring the Automatic Workstation Removal Policy” on page 124
- “Associating the Server Package” on page 124

8.1.1 Configuring the Automatic Workstation Import Policy

For Automatic Workstation Import to work, you must configure the Workstation Import policy. This policy determines how the workstation objects are named and where they are placed in Novell eDirectory™.

For conceptual and step-by-step information about configuring the Workstation Import policy, see [Section 13.4, “Workstation Import Policy,” on page 153](#).

8.1.2 Configuring the Automatic Workstation Removal Policy

For Automatic Workstation Removal to work, you must configure the Workstation Removal policy. This policy determines when unused Workstation objects are removed from eDirectory.

For conceptual and step-by-step information about configuring the Workstation Removal policy, see [Section 13.5, “Workstation Removal Policy,” on page 159](#).

8.1.3 Associating the Server Package

The Import and Removal policies you configured and enabled cannot be in effect until you associate their Server package with a server. For further information, see [Section 13.7, “Associating the Server Package,” on page 164](#).

8.2 Setting Up Automatic Workstation Import and Removal to Run on the Servers

The steps in the following sections assume that you selected the *Import*, *Removal*, or *Import/Removal* option as part of Automatic Workstation Import installation. For further information, see “[Installing the ZENworks Desktop Management Server](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

The most important item to remember when deploying Automatic Workstation Import is to use DNS for TCP/IP addresses so that DNS names can be found automatically. This is preferable to setting up and maintaining `hosts` files on every workstation.

To set up Automatic Workstation Import, do the following for each import service server:

- 1 Set up a DNS name for Automatic Workstation Import to use.

This can be either a DNS entry or an entry in a local `hosts` file. An example of a DNS name is `www.novell.com`.

The following is an example of the text you would add in a `hosts` file for Automatic Workstation Import:

```
151.155.155.55 zenwsimport
```

In this example, the TCP/IP address is for the server where you are running the Automatic Workstation Import service. “Zenwsimport” is not the name of a server, but a DNS name that resolves to this TCP/IP address. In other words, zenwsimport is a label to identify the server as the one running the Automatic Workstation Import service.

For Windows 98, the `hosts` file's location should be:

```
Win98_drive:\Win98_directory\hosts
```

IMPORTANT: The default `hosts` file in Windows is named `hosts.sam`. Do not use the `.sam` extension with your filename. Rename `hosts.sam` to `hosts`, or make a copy and rename the copy. By default, Windows 98 hides filename extensions that are of a known type, so you should make sure that filename extensions are being displayed so that you can correctly rename the `hosts.sam` file to `hosts`.

For Windows 2000/XP, the `hosts` file's location should be:

```
Win_drive:\Win_directory\SYSTEM32\drivers\etc\hosts
```

Hosts as shown above is a filename, not a folder name.

- 2 To verify the DNS name or TCP/IP address, enter the following at the workstation command prompt:

```
ping zenwsimport
```

8.3 Using the Novell Client and the ZENworks Desktop Management Agent

You must update each workstation that you want to import with the latest ZENworks Desktop Management Agent. This is required to place Workstation Manager on the workstations. For further information, see [Part I, “Understanding ZENworks 7 Desktop Management,” on page 31](#).

8.4 Verifying that Automatic Workstation Import and Removal are Working

At this point, if the scheduler is working, workstation import should happen automatically when any of these events occur, depending on the Import policy:

- Scheduler service startup (98/2000/XP)
- User login (98/2000/XP)

Verifying That Automatic Workstation Import and Removal Are Working

To verify that Automatic Workstation Import and Removal are working:

- For each NetWare[®] import or removal service server, press Ctrl+Esc and look for a ZENworks Workstation Import screen.

- For each Windows 2000/XP import or removal service server, check services for:
ZENworks Workstation Import
or
ZENworks Workstation Removal
- For each SLES 9 SP1 or OES Linux server, run `/etc/init.d/novell-zdm-aws status` at the bash prompt. The import service returns a message as to whether it is currently running.

If Automatic Workstation Import or Removal is not running on the Windows server or on the NetWare server, restart the server. If they are not running on the Linux server, restart the service as explained below.

Forcing Workstation Import at the Workstation

You can force workstation import or registration to occur by running `zwsreg.exe`, located on the workstation at:

```
drive:\program files\novell\zenworks\zwsreg.exe
```

Stopping the Import/Removal Service on NetWare Servers

To stop an import or removal service on a NetWare server, use the following commands in place of using the process IDs displayed by the `java -show` command. Enter the following at the server console:

```
java -killzenwsimp
java -killzenwsrem
```

These commands are also contained in the `sys:\system\zfdstop.ncf` file.

Stopping and Restarting the Import/Removal Service on Linux Servers

To stop the import/removal service on a SLES 9 SP1 server or on an OES Linux server:

- 1 At the Linux server prompt, go to `/etc/init.d`.
- 2 Enter `./novell-zdm-aws stop`.

To start the service, run `/etc/init.d/novell-zdm-aws start` or `/etc/init.d/novell-zdm-aws restart` at the bash prompt.

To restart the service while it is currently running, run `/etc/init.d/novell-zdm-aws restart` at the bash prompt.

Workstation Registration Files

9

Workstation registration in Novell® ZENworks® 7 Desktop Management involves three executable files: `zwsreg.exe`, `zenwsreg.dll`, and `zenwsrgr.dll`.

The following sections provide information on these files:

- [Section 9.1, “Registration File Functions,” on page 127](#)
- [Section 9.2, “Registration File Locations,” on page 127](#)
- [Section 9.3, “Using Zwsreg.exe,” on page 127](#)
- [Section 9.4, “Using Zenwsreg.dll,” on page 128](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

9.1 Registration File Functions

Zwsreg.exe: Calls `zenwsreg.dll`.

zenwsreg.dll: Performs workstation registration tasks.

zenwsrgr.dll: Contains strings used by `zenwsreg.dll`. These strings are available for language translation.

9.2 Registration File Locations

Windows 98 Client Workstation:

```
drive:\program files\novell\zenworks\zwsreg.exe
drive:\program files\novell\zenworks\zenwsreg.dll
drive:\program files\novell\zenworks\nls\english\zenwsrgr.dll
```

Windows 2000/XP Client Workstation:

```
drive:\program files\novell\zenworks\zwsreg.exe
drive:\program files\novell\zenworks\zenwsreg.dll
drive:\program files\novell\zenworks\nls\english\zenwsrgr.dll
```

9.3 Using Zwsreg.exe

In previous versions of ZENworks for Desktops, `wsreg32.exe` and `unreg32.exe` handled workstation import and removal functions. In ZENworks Desktop Management 4.x or later, `zwsreg.exe` replaces both files.

The syntax for `zwsreg` is as follows:

```
zwsreg option
```

You can use the following options with `zwsreg`:

Table 9-1 *Zwsreg.exe Startup Options*

Option	Explanation
-importserver <i>server_ip_address</i>	Specifies the IP address of the import server. If you specify None or 0 for the import server, you can import workstations without setting up an import server. To do this, however, the user must have sufficient rights and the Novell Client™ must be installed on the workstation.
-importpolicy <i>policy_DN</i>	Specifies the DN of the effective Workstation Import policy.
-importtws <i>new_workstation_DN</i>	Specifies the DN of the workstation to be imported. You can specify a custom workstation DN to override the effective Workstation Import policy.
-version 3_or_4	Specifies whether the workstation to be imported is a ZENworks for Desktops 3 or a ZENworks for Desktops 4 workstation. The 4 setting is the default and works for ZENworks for Desktops 4 and newer.
-unreg	Clears the registry.

9.4 Using Zenwsreg.dll

`zenwsreg.dll` is called by Workstation Manager's Scheduler when one of the following events occurs:

- Workstation startup
- User login
- User logout
- Registration service shutdown

When one of the above events is detected, the sequence of file calls is as follows:

Windows 98: `wm95.exe > wm98sast.exe > zenwsreg.dll`.

Windows 2000/XP: `wm.exe > wmrundll.exe > zenwsreg.dll`.

Documentation Updates



This section contains information on documentation content changes that have been made in this section of the *Administration* guide since the initial release of Novell® ZENworks® 7 (August 26, 2005). The information will help you to keep current on updates to the documentation.

All changes that are noted in this section were also made in the documentation. The documentation is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the documentation changes listed in this section.

The documentation update information is grouped according to the date the changes were published. Within a dated section, the changes are alphabetically listed by the names of the main table of contents sections for ZENworks 7 Personality Migration.

If you need to know whether a copy of the PDF documentation you are using is the most recent, the PDF document contains the date it was published on the front title page.

The documentation was updated on the following dates:

- [Section H.1, “July 14, 2006 \(Support Pack 1\),” on page 129](#)
- [Section H.2, “December 9, 2005,” on page 129](#)

H.1 July 14, 2006 (Support Pack 1)

The following note was added to each section:

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

H.2 December 9, 2005

The page design in the guide was reformatted to comply with revised Novell documentation standards.

Workstation Management

IV

Much of the functionality of the Workstation Management component of Novell® ZENworks® Desktop Management depends on the preliminary administrative work you do in ConsoleOne® as you import user workstations into the directory and set up the policies that can be associated with User and Workstation objects.

Before you can manage your network's workstations, you must understand Workstation Management and set up policies. After deploying Workstation Management, you can perform periodic maintenance operations, such generating reports of effective policies and policy package associations, copying policy packages from one container in the directory to another container, and more.

Refer to the following sections for further information:

- [Chapter 10, “Understanding Workstation Management,” on page 133](#)
- [Chapter 11, “Creating Policy Packages,” on page 143](#)
- [Chapter 12, “Setting Up the Search Policy in the Container Package,” on page 145](#)
- [Chapter 13, “Setting Up Server Package Policies,” on page 149](#)
- [Chapter 14, “Setting Up Service Location Package Policies,” on page 165](#)
- [Chapter 15, “Setting Up User and Workstation Package Policies,” on page 169](#)
- [Chapter 16, “Generating Policy Reports,” on page 209](#)
- [Chapter 17, “Copying Policy Packages,” on page 211](#)
- [Chapter 18, “Workstation Scheduler,” on page 213](#)
- [Appendix I, “Documentation Updates,” on page 223](#)

Understanding Workstation Management

10

The following sections help you to understand and plan a full deployment of the Workstation Management component of Novell® ZENworks® 7 Desktop Management on your network:

- [Section 10.1, “Workstation Management Components and Features,” on page 133](#)
- [Section 10.2, “ZENworks Database,” on page 136](#)
- [Section 10.3, “ZENworks Desktop Management Policies and Policy Packages,” on page 136](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

10.1 Workstation Management Components and Features

Workstation Management helps you reduce the overall cost and complexity of configuring and maintaining workstation desktops in your network. Desktop Management policies provide you with automatic management of server, user, and workstation configurations, processes, and behaviors. You set up these policies using ConsoleOne®, which means that you do not need to visit each workstation in your site to configure user and workstation settings.

Using Workstation Management, you can:

- Enable roaming profiles and set default desktop preferences for users
- Use extensible policies (for Windows 98) and Group policies (for Windows 2000/XP) to control any application function that is configured in the Windows registry
- Set parameters such as remote control and remote view for remotely managing users' workstations
- Set parameters for imaging workstations
- Configure users created on Windows 2000/XP workstations after they have authenticated to the directory
- Set parameters to specify what inventory information to collect
- Set parameters to automatically import new workstations into the tree and to remove workstations when they are no longer in use
- Set user parameters for printing using the Novell iPrint client, which lets users print to any iPrint printer, regardless of the printer's physical location
- Configure users' Terminal Server connections

The following sections provide basic information on Workstation Management components and features:

- [“Components” on page 134](#)
- [“Features” on page 134](#)

10.1.1 Components

Workstation Management has the following components:

- “Workstation Resident Modules” on page 134
- “ConsoleOne Snap-Ins” on page 134

Workstation Resident Modules

The workstation resident modules authenticate the user to the workstation (Windows 2000/XP only) and network, and transfer configuration information to and from the directory. Under Windows 2000/XP, Workstation Management runs with administrative privileges that allow it to dynamically create and delete user accounts, provided it can communicate with the directory.

ConsoleOne Snap-Ins

The ConsoleOne snap-ins are Java files that are used to create, view, and configure the various Workstation Management directory objects through ConsoleOne. For more information about ConsoleOne, see the [ConsoleOne Documentation Web site \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

10.1.2 Features

Workstation Management features let you store and configure Windows 98/2000/XP desktop policies in the directory and push them to the client. The client workstation can be thought of as an extension of the user.

Workstation Management has the following features:

- “Multiple Platform Support” on page 134
- “Windows 2000/XP Support” on page 135
- “Workstation Profile Management” on page 135
- “Scheduled Actions” on page 135
- “Server and Client Policies” on page 135
- “Directory Storage for Extensible Policies” on page 135
- “ZENworks Desktop Management Reports” on page 135

Multiple Platform Support

Workstation Management software allows all user account and desktop information for Windows 98/2000/XP to be centrally managed within the directory using ConsoleOne as the single administrative utility.

Configuration information is stored in policy package objects. For example, there are policy package objects containing policies for Windows 98, Windows 2000, Windows XP, and Microsoft Terminal Servers that can be downloaded to the workstations.

For more information about Desktop Management support for the Windows NT* platform, see “[Interoperability with Windows NT 4 Workstations](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

Windows 2000/XP Support

For Windows 2000/XP environments, Workstation Management also eliminates the need for domains or for a large number of user accounts to reside in the local Security Access Manager (SAM) of each workstation.

The Windows Group policy is an extension of extensible policies for Windows 2000/XP and Active Directory.

Workstation Management stores user information, desktop configuration, OS configuration, and workstation information in the directory. For 2000/XP users, this means that when a user's directory account is associated with this configuration information, the user can access the network using any 2000/XP workstation configured with Workstation Management.

If the user does not have an account on the workstation at the time of login, Workstation Management can automatically create an account according to the associated user information. After the user is attached to the network, associated policies are downloaded to the workstation to provide a consistent desktop on each workstation used.

Workstation Profile Management

You can create and manage mandatory user profiles, and you can control user interface options, such as the command console and display control attributes. After you have set these attributes, users cannot modify these settings unless they are given the appropriate rights.

Scheduled Actions

This feature lets you schedule actions to occur at a specific time, such as during the evening when the workstation is not in use. These actions can be done without requiring users to be logged in to the network from the workstation. As long as the workstation is powered on, Workstation Management can authenticate the workstation to the directory and perform the action.

Server and Client Policies

Desktop Management uses policies for hands-off management of server and client processes. Policies can be set for automating workstation import and removal, managing users and workstations, and providing workstation inventory information.

Directory Storage for Extensible Policies

Workstation Management lets you create extensible policies using ConsoleOne instead of the Microsoft POLEDIT utility. This approach to creating policies provides three specific benefits:

- It eliminates the requirement that you copy the policy file to the `sys:\public` directory of each server on the network, thus reducing your initial setup workload.
- Because the policy is stored in the directory, you only need to make changes once.
- Any change you make to a policy is automatically replicated across the network in a multiple-partition network, thus providing automatic fault tolerance.

ZENworks Desktop Management Reports

Desktop Management provides predefined reports for effective policies and policy package associations. The scope of both reports is for a selected container and, optionally, its subcontainers.

The Effective Policies report provides the following information:

- Version
- Tree
- Container
- Object DN
- Platform
- Effective Policy DN

The Package Associations report provides the following information:

- Tree
- Container
- Package DN
- Association

The report results are displayed in Notepad and are automatically saved as text files on the workstation where you are running ConsoleOne. For further information, see [Chapter 16, “Generating Policy Reports,” on page 209](#).

10.2 ZENworks Database

The ZENworks database is used for logging report information for Desktop Management. Therefore, to run reports on Workstation Management, you need a configured Database object with an associated ZENworks Database policy.

If you selected to install the Sybase* database management system during installation of Desktop Management, you should configure and enable the ZENworks Database policy to identify the location of the database object, which knows the location of the database file (`mgmt.db`).

If you are using a Sybase database, the Database object is created during installation if you selected the Inventory option. The Database object then contains default values.

If you are using an Oracle* or Microsoft SQL database, you need to create and configure the Database object and the database.

For more information on configuring the Database object for both Sybase and Oracle, as well as information on configuring the ZENworks Database policy, see [Section 13.6, “ZENworks Database Policy,” on page 161](#).

10.3 ZENworks Desktop Management Policies and Policy Packages

To fully deploy the Workstation Management component of Desktop Management, you must configure, enable, and associate the necessary policies and policy packages in ConsoleOne.

A policy is a set of rules that defines how workstations, users, and servers can be configured and controlled, including application availability and access, file access, and the appearance and contents of individual desktops. Policies are contained within policy packages, where they are also administered and customized.

A policy package is a Novell eDirectory™ object containing one or more individual policies. A policy package groups policies according to function, making it easier to administer them. It also provides the means for the administrator to change policy settings and to determine how they affect other eDirectory objects.

Review the following sections for an understanding of Desktop Management policies and policy packages:

- “Policy Packages” on page 137
- “ZENworks Desktop Management Policies” on page 137
- “Plural Policies” on page 138
- “Enabling Policies” on page 138
- “Policy Scheduling” on page 139
- “Policy Package Associations” on page 139
- “Search Policy” on page 140
- “Effective Policies” on page 140
- “Extensible Policies” on page 141

10.3.1 Policy Packages

Desktop Management policies are grouped into policy packages for ease of administration. You create and manage policy packages using ConsoleOne.

The property page for each policy package contains one or more platform-specific tabs that list one or more policies specific to that platform and package. These pages each identify an operating platform, such as General, NetWare, Windows (9x/NT/2000/XP), or Windows Terminal Server (2000/XP). Any policy that you enable on a General page applies to all platforms indicated by the other pages. However, any policy configurations you set on a specific platform page override similar settings on the General page.

The Desktop Management policy packages are:

- Container Package
- Server Package
- Service Location Package
- User Package
- Workstation Package

The Container Package and Service Location Package are identical to the policy packages used in ZENworks Server Management. The Server Package also exists in ZENworks Server Management; however, in ZENworks Desktop Management it contains different policies. The User Package and Workstation Package are unique to Desktop Management. For more information, see [Chapter 11, “Creating Policy Packages,” on page 143](#).

10.3.2 ZENworks Desktop Management Policies

A policy is a set of rules that defines how workstations, users, and servers can be configured and controlled, including application availability and access, file access, and the appearance and contents of individual desktops. Policies are contained within policy packages, where they are also

administered and customized. Desktop Management policies provide you with automated management of server, user, and workstation configurations, processes, and behaviors. For example, you could set up a user policy that determines how a certain user's desktop looks, regardless of the machine that users logs in from. Or, you could set up a workstation policy that determines how a certain machine's desktop looks, regardless of which user logs in.

You can use policies to define the following:

- Parameters for importing workstation objects to the tree
- How far in the tree to search for effective policies
- Parameters for collecting hardware and software inventory
- Parameters for remotely controlling a workstation
- Event and action scheduling

Each policy's properties contains one or more tabs where you can specify settings or configurations related to User, Workstation, Group, or container objects, depending on the type of policy. For more information, see [Chapter 11, “Creating Policy Packages,” on page 143](#).

10.3.3 Plural Policies

Plural policies allow you to have multiple instances of the same policy type within the same policy package or as effective policy. Desktop Management has one plural policy in both the User and Workstation Policy packages with the default name of Scheduled Action.

Because you can have several different actions that you might want to run on different schedules, when you add a Scheduled Action policy to the policy package you should name it to reflect the action being scheduled.

For Desktop Management, the Scheduled Action plural policy is available for all platforms in the User Package and Workstation Package. For more information about the Scheduled Action policy in the User Package, see [Section 15.6, “Scheduled Action Policy \(User and Workstation Packages\),” on page 187](#).

10.3.4 Enabling Policies

As your Workstation Management needs change, you can enable, disable, or modify a policy using any of the three states for policy settings:

Table 10-1 *States for Policy Settings*

State	Description
Enabled	Activates the policy's settings; however, settings are not enforced unless the policy package is also associated with an object.
Disabled	Clears a policy. However, disabling a policy in ConsoleOne does not immediately clear its effect at the workstation. The workstation runs the policy with the cleared settings because the settings for each policy are saved in the workstation's registry.
Ignored	Does not guarantee the clearing or enabling of a policy, because it allows the workstation to continue with whichever policy setting it previously had.

When you create a policy package, its policies are disabled by default. After you enable a policy, some default settings are still in place.

A policy can be enabled when you:

- Create a policy package
- Modify a policy package

A policy can also be enabled anytime from within most of the lists where the policy is displayed.

10.3.5 Policy Scheduling

Some policies can be scheduled to run at a certain time. During creation, all policy packages are given a default run schedule. This means that all applicable policies in this package run according to the default schedule. However, you can change the entire policy package schedule, or you can set a policy within the package to run at a different time from the rest of the package.

If you enable a policy but fail to schedule it, it runs according to the schedule currently defined in the Default Package Schedule.

10.3.6 Policy Package Associations

When you have enabled a policy, you must then associate it to make it effective. Configuring, enabling, and scheduling a policy only sets it up. A policy is enforced through its association with a directory object, such as a Server, Container, User, Group, or Workstation object.

Because policy package associations flow down a tree like inherited rights flow in the directory, you can associate a policy package directly with an object. You can also associate a policy package indirectly, such as with the object's parent container.

When you view the associated policy packages for an object, Desktop Management starts at the object and searches up the tree in the following order for the associated policy packages to be displayed (unless the search order has been changed with a Search policy):

1. The object itself
2. Any Group where the object has membership
3. Any container above the object up to [Root]

Similar to assigning different rights for different users in the directory, you can set a general policy for most users and unique policies for unique users.

You must have the Write right to both the policy package and the object in order to associate one with the another.

You can associate a policy package with Server, Container, User, Group, or Workstation objects when you:

- Create or modify the policy package
- Create or modify the Server, Container, User, Group, or Workstation object
- Associate a policy package with a group or container where the User or Workstation objects have membership

IMPORTANT: Do not associate the policy packages with Alias objects. Alias objects are not supported.

10.3.7 Search Policy

The Search policy is used to prevent tree-walking. Unless specified differently in a Search policy, when Desktop Management starts searching for an object's associated policy packages, it starts at the object and works its way up the tree. If Desktop Management does not have any Search policies defined, it walks the tree until it finds the root object. This can cause unnecessary network traffic. Therefore, plan to use Search policies wherever needed.

Unless otherwise specified in a Search policy, all enabled policies in a policy package that is associated directly with an object have precedence over contradicting policies in policy packages higher in the tree.

For more information about configuring the Search policy, see [“Setting Up the Search Policy in the Container Package” on page 145](#).

10.3.8 Effective Policies

Effective policies for a directory object are those that have been configured, enabled, and associated with the object. Just as the effective rights in the directory flow down the tree, policy package associations also flow down the tree.

The following sections provide more information on effective policies:

- [“How Effective Policies Are Determined” on page 140](#)
- [“How Package Associations Are Resolved to Determine Effective Policies” on page 140](#)

How Effective Policies Are Determined

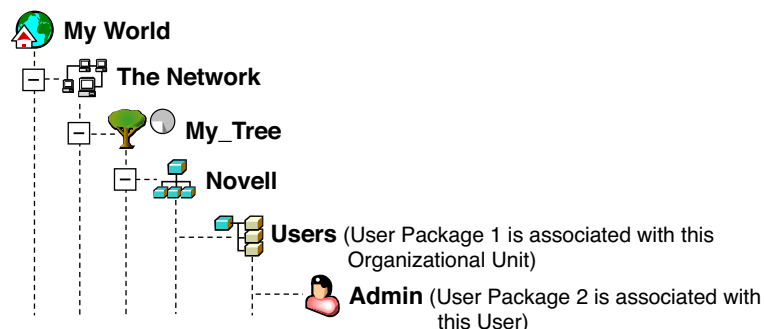
When Desktop Management calculates the effective policies for an object, it starts with all policy packages assigned to that object. It then looks up the tree for policy packages associated to Group objects and then for policy packages associated to Containers (assuming that the search order starts at the leaf object and goes up towards the root of the tree).

How Package Associations Are Resolved to Determine Effective Policies

Because Desktop Management policies provide management-by-exception through policy package associations, a lower package association overrides an upper package association. In other words, a package associated to a User object overrides any similar settings in a package associated to the user's container object.

The following illustrates policy package associations:

Figure 10-1 Directory Tree Showing Policy Package Associations



Suppose that in this illustration, User Package 1 contains three enabled policies: Windows Desktop Preferences, Inventory, and Remote Control. User Package 2 contains one enabled policy: Windows Desktop Preferences. For the User object, the Windows Desktop Preferences policy settings in User Package 2 overrides the similar policy settings in User Package 1.

The effective policies for the user are the Windows Desktop Preferences policy in Policy Package 2 and the Inventory and Remote Control policies in Policy Package 1. The *Associations* tab for this User object lists the one policy in User Package 2 that has been enabled. The two enabled policies in User Package 1 are also listed on the User object's *Associations* tab. In other words, effective policies are the sum of all enabled policies in all policy packages associated directly or indirectly to an object.

Extensible Policies

For any Windows-compatible software program, an extensible policy allows you to control any application function that is configured in the Windows registry. Desktop Management lets you easily customize and deploy extensible policies across your network to accommodate your specific business practices.

Extensible policies are not supported on Windows XP. You should use Windows Group policies to configure policies for Windows XP systems. Additionally, we recommend that you use Windows Group policies instead of extensible policies for Windows 2000 or newer. You should continue using extensible policies for the Windows 9.x platforms.

For more information, see [Section 15.2.1, “Understanding Extensible Policies,”](#) on page 173.

Creating Policy Packages

11

For Novell® ZENworks® 7 Desktop Management to function properly, you must create the policy packages so that you can configure, enable, schedule, and associate your planned policies.

Many of the Desktop Management policies are available only if you select the *Workstation Management* installation option. For installation steps, refer to “[Installing the ZENworks Desktop Management Server](#)” in the “[Novell ZENworks 7 Desktop Management Installation Guide](#)”.

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

A policy package is a Novell eDirectory™ object containing one or more individual policies. A policy package groups policies according to function, making it easier to administer them. It also provides the means for the administrator to change policy settings and to determine how they affect other eDirectory objects.

You should create an Organizational Unit (OU) to hold the policy packages. Consider the following when determining where to place this OU:

- If you have partitions in your tree
- The 256-character limit in eDirectory for the full distinguished name
- The Search policy that is used to determine the search order and the search level ceiling for the policy package

To minimize tree walking, it is best to create this policy package OU at the root of the partition that contains the objects with which the policy package is associated and to configure the Search policy to stop searching at the container in which the policy package is located. In doing so, the following benefits are realized:

- Tree walking is minimized with the root of the partition and the Search policy being used
- Placing the OU at the partition’s root maximizes the number of characters that are available for naming plural policies

To create an OU and then a policy package:

- 1 In ConsoleOne®, right-click the container where you want the container for the policy packages placed, click *New*, then click *Organizational Unit*.
- 2 Give the container a short name, then click *OK*.

Because you can have ZENworks Desktop Management, ZENworks Handheld Management, and ZENworks Server Management policies in the same tree, make sure you use a name that distinguishes your Desktop Management policies container, for example, Desktop Policies.

- 3 Right-click the new container that will hold your policy packages, click *New*, then click *Policy Package*.



- 4 Select one of the following policy packages:

Container Package
Server Package
Service Location Package
User Package
Workstation Package

To see a list of policies that are contained in each policy package, select the desired policy package in the *Policy Packages* list on the left side to display the available policies in the *Policies* list on the right.

- 5 Click *Next*, give the package a short name, click *Next*, click *Create Another Policy Package* (unless this is the last one being created), then click *Finish*.

Short package name suggestions include:

Container
Server
Location
User
Workstation

- 6 Repeat **Step 4** through **Step 5** for each policy package to be created.

Setting Up the Search Policy in the Container Package

12

The Container Package contains only the Search policy. The Search policy is used to limit how far up the tree Desktop Management searches for the effective policies.

The Search policy provides the following benefits:

- Improved security
- The ability to reorder a search
- Better search performance by limiting the search levels traversed in Novell® eDirectory™ and by avoiding unnecessary LAN traffic

The Search policy locates policy packages that are associated with containers. To make a Search policy effective, you associate it with a container.

You can specify the number of levels above or below the location to begin the search:

Table 12-1 Search Policy Levels

Number	Description
0	Limits the search to the selected level.
1	Limits the search to one level above the selected level. For example, if you selected the server's parent container, this limits the search to one level above the parent level.
-1	Limits the search to one level below the selected level. For example, if you selected [Root], -1 would limit the search to one level below [Root].

Without a Search policy in effect, the default is to search from the parent container to [Root]. The search checks each container up the tree towards [Root] for policy packages associated with those containers.

The default Search policy recognizes the policy package associated with the User or Workstation object before it looks in any group or container where such an object resides.

The default search order, *Object > Group > Container > Root*, can be reordered and can include as few as one of the locations. For instance, you can exclude Group objects by setting the search order to *Object > Container > Root*.

You can avoid unnecessary LAN traffic by searching to an associated or selected container instead of [Root].

When you view the associated policy packages for an object, by default Desktop Management starts at the object and searches up the tree to [Root] for all policy packages associated with:

- The object

- Any Group where the object has membership
- Any of the object's parent containers

The Search policy is required to limit the range which is being used to find other policies. You set up Search policies at a container level. Set up as many Search policies as you need to help minimize network traffic.

To set up a Search policy:

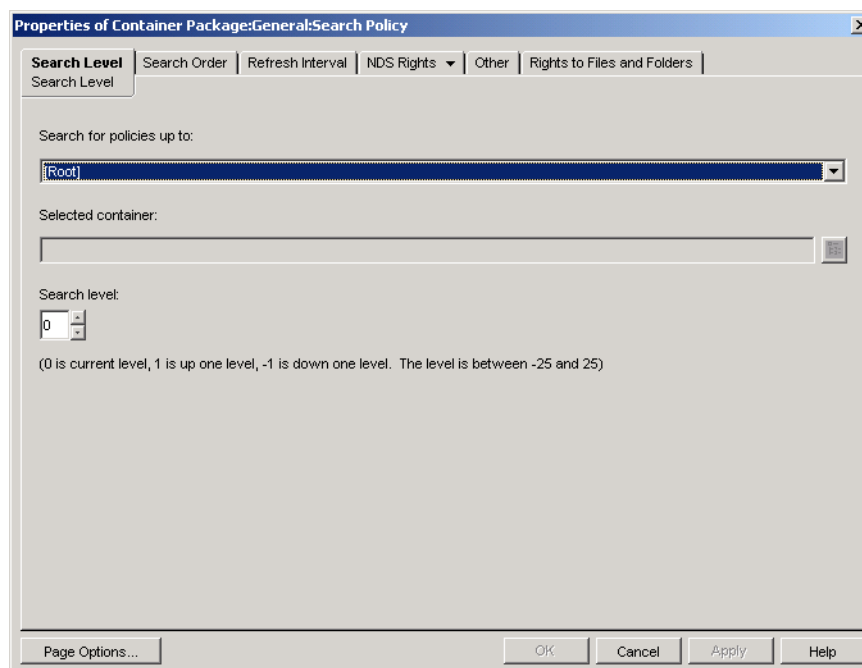
- 1 In ConsoleOne®, right-click the Container Package, then click *Properties*.

If you have not yet created the Container Package, see [“Creating Policy Packages” on page 143](#).

- 2 Select the check box under the *Enabled* column for the Search policy.

This both selects and enables the policy.

- 3 Click *Properties* to display the Search Level Page.



- 4 Using the drop-down list, select the level to search up to:

[Root]: Searches from the object to the root of the tree.

Object Container: Searches to the parent container of the Server, User, or Workstation object.

Associated Container: Searches to the associated container that this Search policy is associated with. The Associated Container level replaces Partition in earlier versions of ZENworks® for Desktops.

If you are upgrading from a previous version, and you use Partition in your Search policy, make sure that the Container Package is associated only to the partition root.

Selected Container: Searches from the object to the selected container.

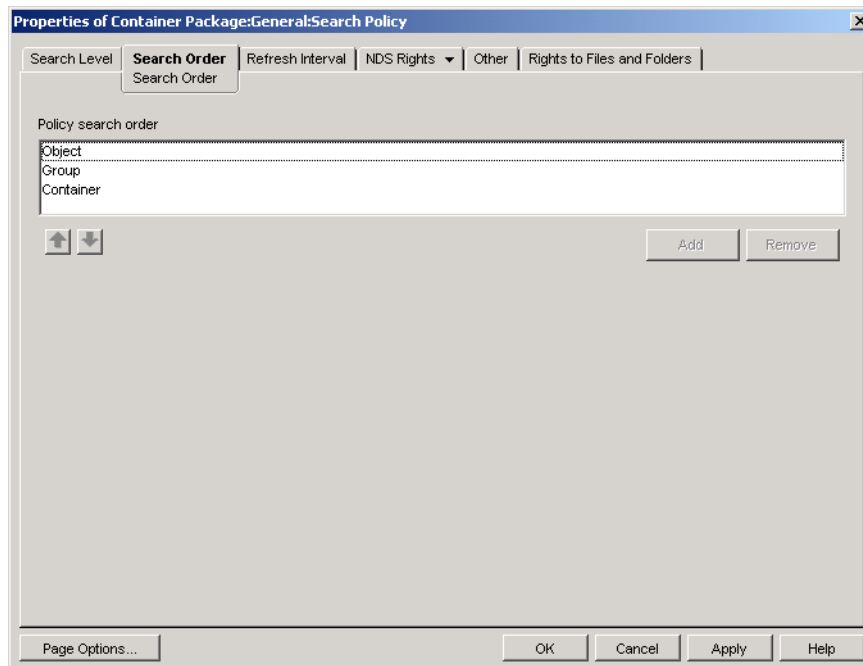
- 5 (Conditional) If you chose Selected Container, browse for and select the container.

- 6 To determine the searching limits in either direction, specify a number in the Search Level box:

Number	Description
0	Limits the search to the selected level. This is the default setting.
1	Limits the search to one level above the selected level. For example, if you selected the server's parent container, this would limit the search to one level above the parent level.
-1	Limits the search to one level below the selected level. For example, if you selected [Root], -1 limits the search up to one level below [Root].

You can specify any number between -25 and 25, but using the default setting of 0 is a good administrative practice.

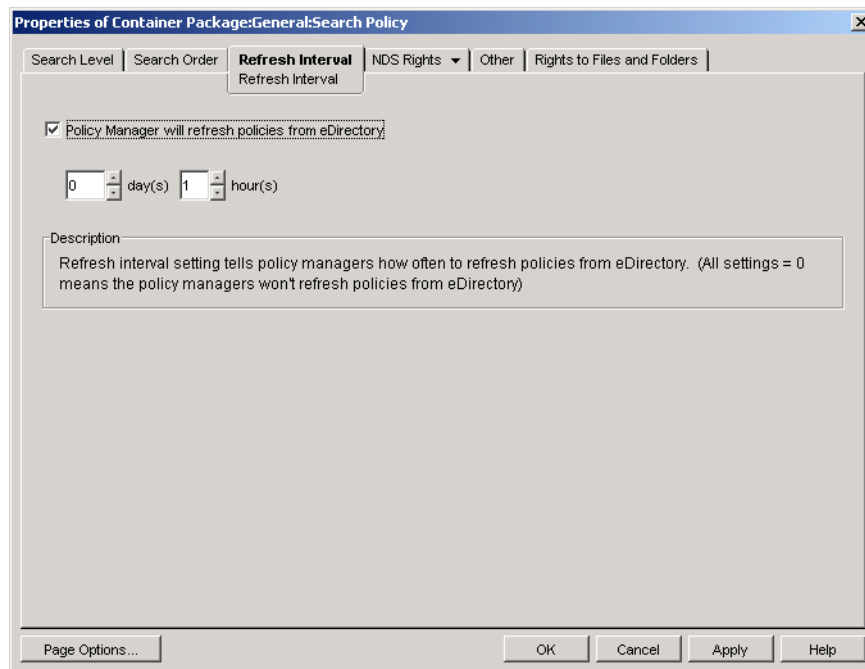
- 7 Click the *Search Order* tab.



- 8 Specify the policy searching order using the arrow keys, the *Add* button, and the *Remove* button as necessary.

The default search order is *Object > Group > Container*.

- 9 Click the *Refresh Interval* tab.



- 10 Specify the frequency for how often the server should refresh its policies.

By default, the *Policy Manager Will Refresh Policies from eDirectory* option is enabled and the refresh interval is set to one hour. If you set both time increments to zero (0), policies are never refreshed, even if you have the *Policy Manager Will Refresh Policies from eDirectory* option enabled.

- 11 Click *OK*.
- 12 Click the *Associations* tab, then click *Add*.
- 13 Browse for and select the container object for association to the Search policy.
- 14 Click *OK* when finished.

Setting Up Server Package Policies

The Server Package has six policies that are used for ZENworks® Desktop Management server functions. The policies you configure and enable are not in effect until you associate their policy package with a container or server object. For further information on configuring the available policies and associating them, see the following sections:

- [Section 13.1, “Dictionary Update Policy,” on page 149](#)
- [Section 13.2, “Imaging Server Policy,” on page 151](#)
- [Section 13.3, “Inventory Roll-Up Policy,” on page 151](#)
- [Section 13.4, “Workstation Import Policy,” on page 153](#)
- [Section 13.5, “Workstation Removal Policy,” on page 159](#)
- [Section 13.6, “ZENworks Database Policy,” on page 161](#)
- [Section 13.7, “Associating the Server Package,” on page 164](#)

NOTE: The Distributed Server Package is not used by ZENworks Desktop Management. It is only used by Policy and Distribution Services in ZENworks Server Management.

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

13.1 Dictionary Update Policy

This policy allows you to specify where the source for the software dictionary list is located. A software dictionary contains a list of files that, when found on the drive, constitute a known software package. The software dictionary is stored on each individual workstation as it performs its scanning process for it to determine the software packages present on the workstation.

Occasionally, you might want to update the dictionary to include additional, internal software package files. This policy tells the workstation agents where to find the source and how often to update their individual dictionary files.

To configure the Dictionary Update policy:

- 1 In ConsoleOne®, right-click the *Server Package*, click *Properties*, then click the appropriate platform page.

Policies set on a specific platform override policies set on the *General* tab.

2 Select *Dictionary Update Policy*, then click *Properties*.

The screenshot shows the 'Properties of Server Package:General:Dictionary Update Policy' dialog box. The 'Dictionary Update Policy' tab is selected. The 'Use the Rollup Server as the update source' checkbox is unchecked. The 'Source Server Configuration' section includes a 'Source Service Object' text box with a 'Browse' button and a 'Server IP Address / DNS Name' dropdown menu. The 'Proxy Server Configuration' section includes an 'IP Address / DNS Name' text box and a 'Port' text box. The bottom of the dialog features a 'Page Options...' button and 'OK', 'Cancel', 'Apply', and 'Help' buttons.

3 Fill in the fields:

Use the Rollup Server as the update source: Select this option if you want the Dictionary Update Service to use the Inventory server configured in the Roll-Up policy as the source for dictionary updates. If you do not select this option, the Dictionary Update Service will use the following settings.

NOTE: Do not select this option for a Standalone server. You must manually configure the following settings of the policy.

Source Server Configuration

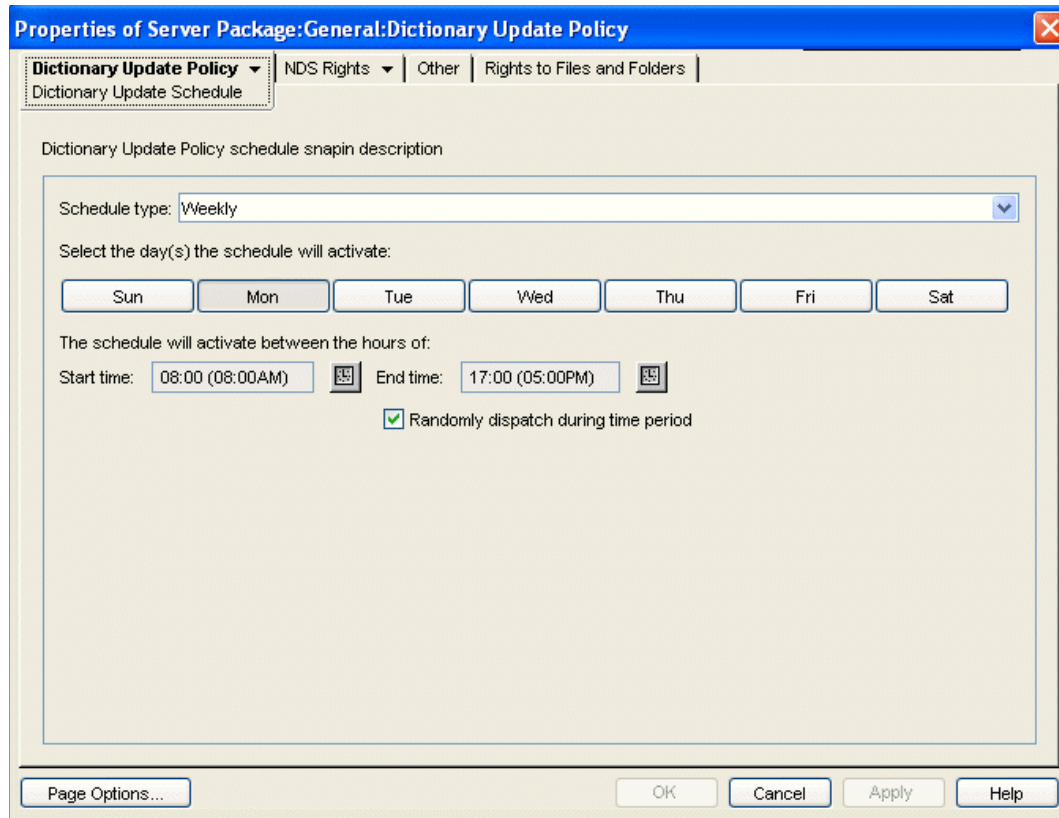
- **Source Service Object:** Browse to select the DN of the Inventory server, which provides the dictionary updates.
- **Server IP Address / DNS Name:** Select the IP address or the DNS name of the Inventory server, which provides the dictionary updates.

Proxy Server Configuration: If the Inventory server, which provides the dictionary updates, is across a firewall, specify the IP address port number of the proxy server.

- **IP Address / DNS Name:** Specify the IP address or the DNS name of the proxy server.
- **Port:** Specify the port number of the proxy server.

Page Options: Click to specify your preferences for arranging the property pages for this type of object. These preferences are saved and used the next time you start Novell® ConsoleOne® on this computer.

- 4 Click the down-arrow on the *Dictionary Update Policy* tab and click *Dictionary Update Schedule*.



- 5 Select the schedule using the *Schedule Type* drop-down list:

Daily
Monthly
Yearly
Never

- 6 Select the days the schedule will activate.

- 7 Click *Apply*.

13.2 Imaging Server Policy

If you will be imaging workstations, configure and enable this policy. This policy sets rules that determine which images to put on workstations that are imaged by this policy. For more detailed information, see [Chapter 58, “Setting Up Imaging Policies,” on page 697](#).

13.3 Inventory Roll-Up Policy

If you want to track workstation inventory information, configure and enable the Inventory Roll-Up policy. For more detailed information on Inventory, see [Part VIII, “Workstation Inventory,” on page 871](#).

While performing the following steps, you can get detailed information about each dialog box by clicking the *Help* button.

To set up the Inventory Roll-Up policy:

- 1 In ConsoleOne, right-click the Server Package, click *Properties*, then click the appropriate platform page.

Policies set on a specific platform override policies set on the General page.

- 2 Select the check box under the *Enabled* column for the Inventory Roll-Up policy.

This both selects and enables the policy.

- 3 Click *Properties*.

Properties of Server Package:General:RollUp Policy

Roll-Up Policy | NDS Rights | Other | Rights to Files and Folders

Destination Server Configuration

Select the service object of the next level destination server.

Destination Service Object: Browse

Server IP Address / DNS Name:

Proxy Server Configuration

IP Address / DNS Name:

Port:

Page Options... OK Cancel Apply Help

- 4 Fill in the fields:

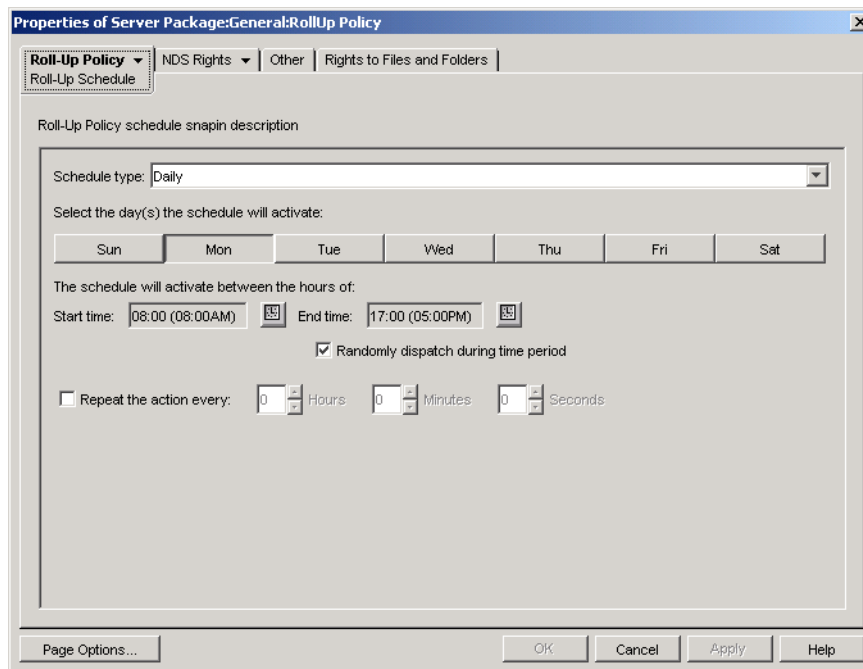
Destination Service Object: Browse to and select the DN of the next-level server for the selected Inventory server.

Server IP Address / DNS Name: Select the IP address or DNS name of the next-level Inventory server.

IP Address / DNS Name: If the Inventory server is outside of the firewall, specify the IP address or DNS name of the proxy server.

Port: If the Inventory server is outside of the firewall, specify the port number of the proxy server.

- 5 Click the down-arrow on the *Roll-Up Policy* tab, then click *Roll-Up Schedule*.



- 6 Select the schedule using the *Schedule Type* drop-down list:

Daily
Monthly
Yearly
Never

Click the *Help* button on the Roll-Up Schedule page for detailed information about each schedule type and its options.

- 7 Click *OK* to save the policy.
- 8 Repeat **Step 1** through **Step 7** for each platform where you want to set an Inventory Roll-Up policy.
- 9 When you have finished configuring all of the policies for this package, continue with the steps under **Section 13.7, “Associating the Server Package,” on page 164** to associate the policy package.

13.4 Workstation Import Policy

The Workstation Import policy sets parameters to control automatic workstation importing. It must be enabled for Automatic Workstation Import to function. For more detailed information, see **Section 7.1, “Understanding Workstation Import and Registration,” on page 119**.

You can set rules on how Workstation objects are named and where they are created. You should decide if you want to create Workstation objects in their own containers or in the container where the User objects reside.

You might find it easiest to manage Workstation objects in a common container if your User objects are scattered among various containers in the tree.

You might also find it easiest to keep User and Workstation objects in the same container.

While performing the following steps, you can get detailed information about each dialog box by clicking the *Help* button.

To set up the Workstation Import policy:

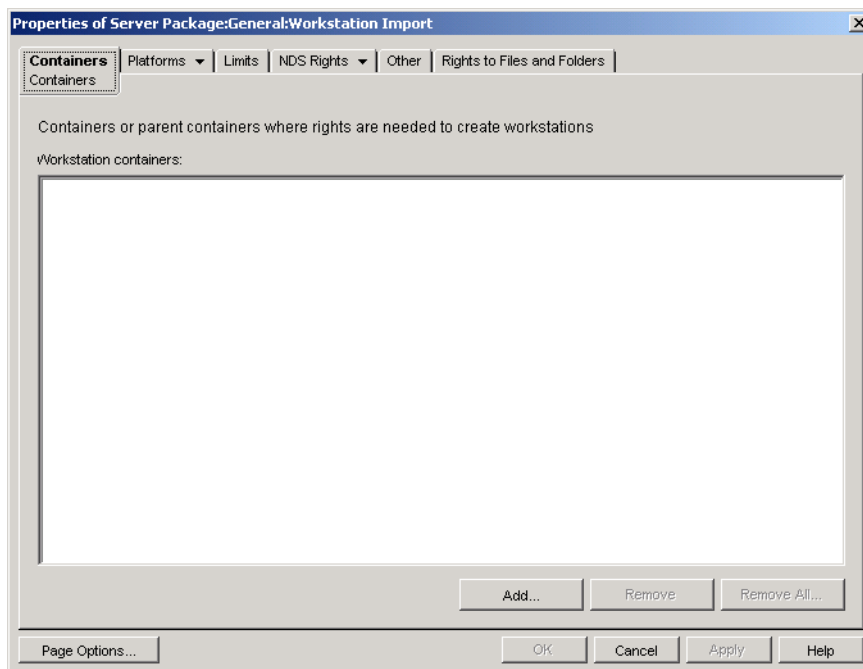
- 1 In ConsoleOne, right-click the Server Package, click *Properties*, then click the appropriate platform page.

Policies set on a specific platform override policies set on the *General* tab.

- 2 Select the check box under the *Enabled* column for the Workstation Import policy.

This both selects and enables the policy.

- 3 Click *Properties* to display the Containers page.



- 4 Click *Add*, select the eDirectory™ containers where rights are needed for creating Workstation objects, then click *OK*.

5 Click the *Limits* tab.

The screenshot shows a Windows-style dialog box titled "Properties of Server Package:General:Workstation Import". It has several tabs: "Containers", "Platforms", "Limits", "NDS Rights", "Other", and "Rights to Files and Folders". The "Limits" tab is selected and highlighted. Inside the dialog, there are several settings:

- "User login number:" with a spin box set to "3".
- "Number of times user logs in before creating a workstation if policy needs user information" (this text is below the spin box).
- A checkbox labeled "Disable user history" which is currently unchecked.
- A checkbox labeled "Limit number of workstations imported" which is currently unchecked.
- "Workstations created per hour:" with a spin box set to "10000".
- "Maximum number of workstations created per hour for each import service" (this text is below the spin box).

At the bottom of the dialog, there are buttons for "Page Options...", "OK", "Cancel", "Apply", and "Help".

6 Fill in the fields:

User Login Number: If the Workstation Import policy requires user information, this number represents the number of times the user needs to log in before the user's Workstation object is created.

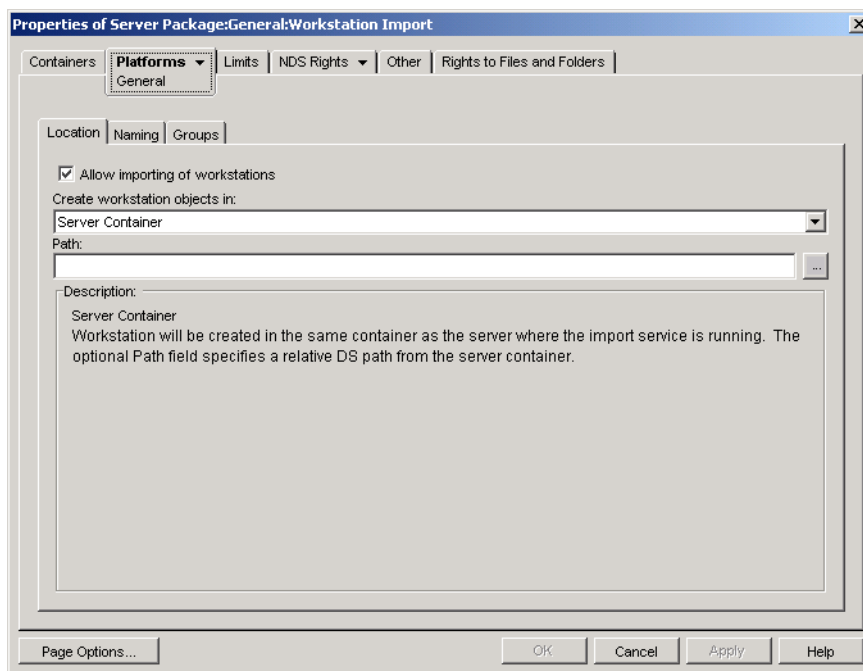
Disable User History: Each time a user logs in to a workstation, the Workstation object's User History page is updated so that an administrator can view a complete list of all users who have logged in to that workstation. If you do not want user history to be collected for workstations, you should enable this option.

This option lets you disable the collection of user history for all workstations imported after you enable this option. To disable user history collection on workstations that were imported before you enabled this option, right-click the appropriate Workstation object, click *Properties*, click the *User History* tab, then select the *Do Not Add to History* check box.

Limit Number of Workstations Imported: To help balance server workload, enable this option to limit how many workstations are imported. When you select this option, the *Workstations Created Per Hour* box is available.

Workstations Created Per Hour: Specify the limit for how many Workstation objects can be created per hour.

7 Click the *Platforms* tab, then click *General*, *WinNT*, *Win2000*, *WinXP*, or *Win9x*, as applicable.



8 Fill in the fields:

Enable Platform Settings to Override General Settings: This check box appears only on the WinNT, Win2000, WinXP, and Win9x platform pages; it does not appear on the General page. Select this check box to override the settings on the General page with the setting you configure on one of the four specific platform pages.

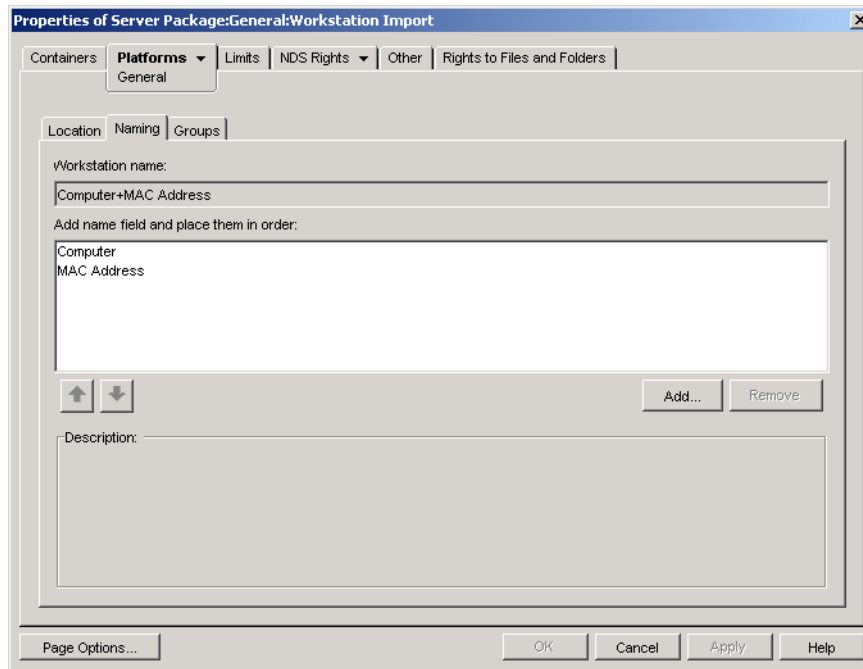
Allow Importing of Workstations: Enable this option to allow registered workstations to be imported.

Create Workstation Objects In: Select an option from the drop-down list:

- **Selected Container:** The Workstation object is created in the container specified in the Path field. This is an absolute path.
- **Server Container:** The Workstation object is created in the same container as the server running the import service. You can specify a relative path from the server container.
- **User Container:** The Workstation object is created in the container where the User object resides for the logged-in user. You can specify a relative path from the user container.
- **Associated Object Container:** The Workstation object is created in the container that is associated with the Workstation Import policy. You can specify a relative path from the associated container.

Path: If you are using a relative path, specify a string. The number of periods you end the path with determines the number of relative levels. If you are using an absolute path, select the container.

9 Click the *Naming* tab.



10 Fill in the fields:

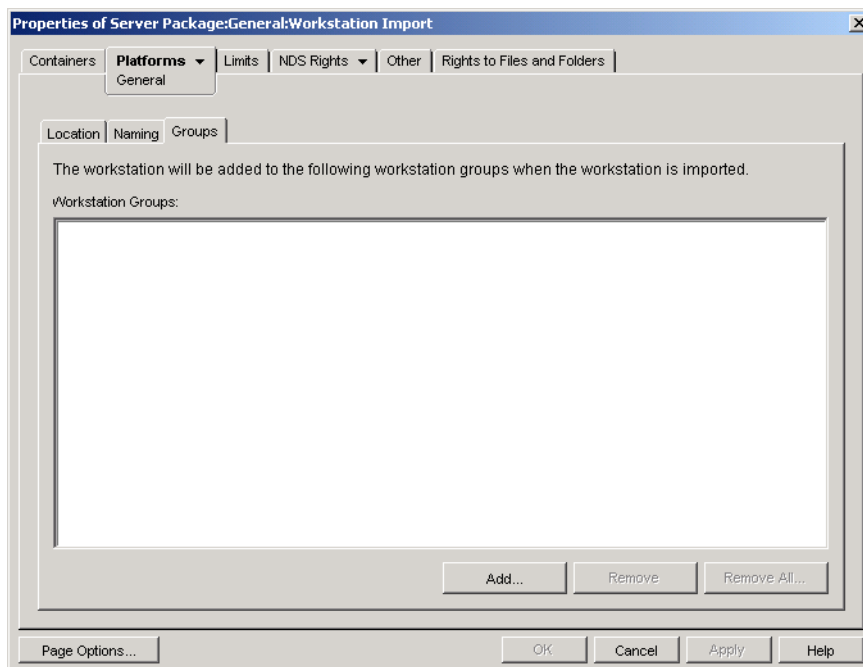
Workstation Name: Displays the workstation naming convention currently defined in the *Add Name Fields and Place Them in Order* list. Whenever there is a potential name conflict (such as two Workstation objects in the same container named after the User object), the system appends a 3-digit number on the end of the name that you enter here.

Add Name Fields and Place Them in Order: You must have at least one option in this list. By default, *Computer + Network Address* is displayed in the list. Click *Add* to select from the following list of name fields. After creation of the Workstation object, this information is static and does not change.

Name Field	Description
Computer	The Windows computer name, usually as it was named during the Windows installation process.
MAC Address	The workstation's MAC address. This address is unique to the workstation's network card.
Container	The container where the User object resides.

Name Field	Description
<User Defined>	<p>You can type your own information here. You must use characters that are valid in a DS object name. Do not use the following characters:</p> <ul style="list-style-type: none"> • Underscore (_) • Asterisk (*) • Less than symbol (<) • Greater than symbol (>) • Semicolon (;) • Pound sign (#)
User	The name of the user that is logged in.
IP Address	The workstation's Internet Protocol (IP) address.
DNS	The Domain Name System name (the logical name related to the IP address).
Server	The workstation's preferred server.
OS	The workstation's operating system (Windows 98, Windows NT, Windows 2000, Windows XP).
CPU	The type of central processing unit in the workstation (386, 486, Pentium*, and so forth).

11 Click the *Groups* tab.



12 Click *Add*, then browse for and select the workstation groups you want this Workstation object to belong to when it is imported.

13 Click *OK* to save the policy.

- 14 Repeat [Step 1](#) through [Step 13](#) for each platform where you want to set a Workstation Import policy.
- 15 When you have finished configuring all of the policies for this package, continue with the steps under [Section 13.7, “Associating the Server Package,” on page 164](#) to associate the policy package.

13.5 Workstation Removal Policy

If you want Workstation objects to be automatically removed after they have not been used for a specified period of time, configure and enable the Workstation Removal policy. For more detailed information on workstation removal, see [Part III, “Automatic Workstation Import and Removal,” on page 117](#).

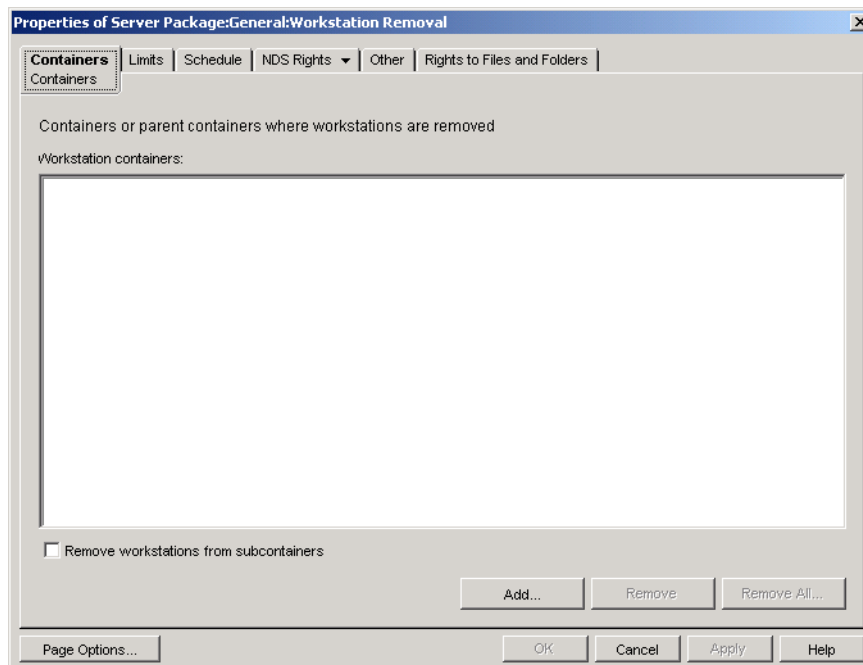
While performing the following steps, you can get detailed information about each dialog box by clicking the *Help* button.

To set up the Workstation Removal policy:

- 1 In ConsoleOne, right-click the Server Package, click *Properties*, then click the appropriate platform page.

Policies set on a specific platform override policies set on the *General* tab.
- 2 Select the check box under the *Enabled* column for the Workstation Removal policy.

This both selects and enables the policy.
- 3 Click *Properties* to display the Containers page.



- 4 Click *Add*, select the containers where workstations to be removed reside, then click *OK*.

Select the *Remove Workstations From Subcontainers* check box, if desired.

- 5 Click the *Limits* tab.

The screenshot shows the 'Properties of Server Package:General:Workstation Removal' dialog box with the 'Limits' tab selected. The 'Limits' sub-tab is also active. The 'Days before removing unused workstations:' is set to 60. Below it, the text reads 'Number of days workstation has not registered before being removed'. The bottom of the dialog has buttons for 'Page Options...', 'OK', 'Cancel', 'Apply', and 'Help'.

- 6 Specify the number of days a Workstation object should remain in the tree without registering before its object is removed.

- 7 Click the *Schedule* tab.

The screenshot shows the 'Properties of Server Package:General:Workstation Removal' dialog box with the 'Schedule' tab selected. The 'Schedule' sub-tab is also active. The 'The year to begin workstation removal (usually the current year)' is set to 2006. The 'Select the day of the year you want the policy to run on' is set to May 01. The 'Start the policy between the hours of:' is set to 23:00 (11:00PM) with a duration of 04:00. The 'Repeat interval in days:' is set to 7. The 'Repeat this action after a specified number of days (1 = Daily, 7 = Weekly)' is checked. The 'Limit number of workstations removed' checkbox is unchecked. The 'Workstations removed per session:' is set to 10000. The 'Maximum number of workstations removed per removal session for each removal service' is also set to 10000. The bottom of the dialog has buttons for 'Page Options...', 'OK', 'Cancel', 'Apply', and 'Help'.

- 8 Fill in the fields:

Year: The year to begin workstation removal.

Date: The day of year that you want the policy to run on.

Start Time: The beginning time of when the policy can run.

Duration: Length of the time window.

Repeat Interval In Days: Beginning from the starting date, Workstation object removal is performed at this interval.

Limit Number of Workstations Removed: To help balance server workload, enable this option to limit how many workstations are removed in a session. When you select this option, the *Workstation Removed Per Session* option becomes available.

Workstations Removed Per Session: Specify a number to set the limit for how many Workstation objects can be removed per session.

9 Click *OK* to save the policy.

10 Repeat **Step 1** through **Step 9** for each platform where you want to set a Workstation Removal policy.

11 When you have finished configuring all of the policies for this package, continue with the steps under **Section 13.7, “Associating the Server Package,” on page 164** to associate the policy package.

13.6 ZENworks Database Policy

This policy identifies the location of the ZENworks Database object. If you selected to install the ZENworks database, you should configure and enable this policy.

NOTE: In previous versions of ZENworks for Desktops, you configured and enabled the ZENworks Database policy using the Service Location Package. In ZENworks for Desktops 4.x and later, you can also configure and enable this policy in the Server Package.

The ZENworks Database policy in the Server Package lets you configure only the Inventory database. The ZENworks Database policy in the Service Location Package lets you configure both the Inventory database and the Application Management databases.

If backward compatibility with an existing ZENworks Database policy for ZENworks for Desktops 3.x is important, you might want to configure this policy in the Service Location Package. However, there is improved manageability if you configure this policy in the Server Package. Configuring the ZENworks Database policy in the Server Package allows you to associate the policy with individual servers rather than with containers.

Sybase: If you are using a Sybase database, the Database object might have been installed with default property values, depending on whether you selected to install Desktop Management Inventory. In either case, follow the applicable steps under **“Configuring the ZENworks Database Object for Sybase” on page 162**, then continue with **“Setting Up the ZENworks Database Policy” on page 163**.

Oracle: If you are using an Oracle database, you need to create the Database object and enter the required property values. In this case, follow the steps under **“Configuring the ZENworks Database Object for Oracle” on page 162**, then continue with **“Setting Up the ZENworks Database Policy” on page 163**.

13.6.1 Configuring the ZENworks Database Object for Sybase

While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

- 1 In ConsoleOne, right-click the Database object, then click *Properties*.

The *ZENworks Database* tab should be displayed.

- 2 Fill in the applicable fields, keeping the user name and password pairs together:

Database (Read-Write) User Name: Secures read and write access to the database file.

Database (Read-Write) Password: Secures read and write access to the database file.

Database (Read Only) User Name: Secures only read access to the database file.

Database (Read Only) Password: Secures only read access to the database file.

Database (Write Only) User Name: Secures only write access to the database file.

Database (Write Only) Password: Secures only write access to the database file.

- 3 To change any default JDBC* driver type information, click the *JDBC Driver Information* tab, then edit the fields:

Driver

Protocol

Subprotocol

SubName

Port

Flag

Database Service Name

- 4 If you will use an ODBC driver for the database file, click the *ODBC Driver Information* tab, then fill in the fields:

Driver Filename

Data Source Name

Connection Parameters

- 5 Click *OK* to save the database property changes.

Continue with “[Setting Up the ZENworks Database Policy](#)” on page 163.

13.6.2 Configuring the ZENworks Database Object for Oracle

While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

- 1 In ConsoleOne, right-click the container where the Database object is to be created, click *New*, click *Object*, click *ZENworks Database*, then click *OK*.
- 2 Specify a name for the Database object, click *Define Additional Properties*, then click *OK*.
The *ZENworks Database* tab should be displayed.
- 3 Select the DN of the server where the database files are to be stored.
- 4 (Optional) Specify the IP address of the server.

- 5 Fill in the applicable fields, keeping the user name and password pairs together:
 - Database (Read-Write) User Name:** Secures read and write access to the database file.
 - Database (Read-Write) Password:** Secures read and write access to the database file.
 - Database (Read Only) User Name:** Secures only read access to the database file.
 - Database (Read Only) Password:** Secures only read access to the database file.
 - Database (Write Only) User Name:** Secures only write access to the database file.
 - Database (Write Only) Password:** Secures only write access to the database file.
- 6 To specify the JDBC driver type, click the *JDBC Driver Information* tab, click the *Populate Fields With Default Values For An Oracle Database* button, then click *Populate Now*.
- 7 To change any default JDBC driver type information, edit the fields:

Driver

Protocol

SubProtocol

SubName

Port

- 8 If you will use an ODBC driver for the database file, click the *ODBC Driver Information* tab, then fill in the fields:

Driver Filename

Data Source Name

Connection Parameters

- 9 Click *OK* to save the database property changes.

Continue with “[Setting Up the ZENworks Database Policy](#)” on page 163.

13.6.3 Setting Up the ZENworks Database Policy

While performing the following steps, you can get detailed information about each dialog box by clicking the Help button.

- 1 In ConsoleOne, right-click the Server Package or the Service Location Package, then click *Properties*.
The *General* tab is displayed.
- 2 Select the check box under the *Enabled* column for the ZENworks Database policy.
This both selects and enables the policy.
- 3 Click *Properties*.
- 4 Select the database DN, then click *OK*.
- 5 When you have finished configuring all of the policies for this package, continue with the steps under [Section 14.5, “Associating the Service Location Package,” on page 168](#) to associate the policy package.

13.7 Associating the Server Package

The policies you configured and enabled are not in effect until you associate their policy package with a container or server object.

- 1 In ConsoleOne, right-click the Server Package, then click *Properties*.
- 2 Click the *Associations* tab > *Add*.
- 3 Browse for and select the container or server for associating the package, then click *OK*.

Setting Up Service Location Package Policies

14

The Service Location Package includes four policies on the General platform page. The policies you configure and enable are not in effect until you associate their policy package with a container object. For further information on configuring the available policies and associating them, see the following sections:

- [Section 14.1, “SMTP Host Policy,” on page 165](#)
- [Section 14.2, “SNMP Trap Targets Policy,” on page 166](#)
- [Section 14.3, “XML Targets Policy,” on page 167](#)
- [Section 13.6, “ZENworks Database Policy,” on page 161](#)
- [Section 14.5, “Associating the Service Location Package,” on page 168](#)

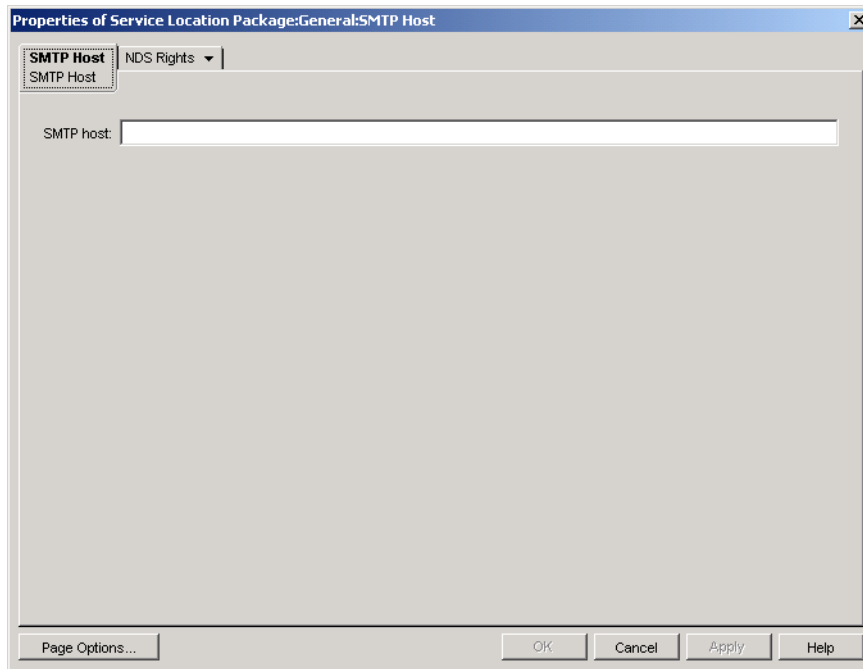
14.1 SMTP Host Policy

While performing the following steps, you can get detailed information about each dialog box by clicking the *Help* button.

To set up the SMTP Host policy:

- 1 In ConsoleOne®, right-click the Service Location Package, then click *Properties*.
The *General* tab is displayed.
- 2 Select the check box under the *Enabled* column for the SMTP Host policy.
This both selects and enables the policy.

- 3 Click *Properties* to display the SMTP Host page.



- 4 Specify the TCP/IP address or DNS name of the relay host server, then click *OK*.
- 5 When you have finished configuring all of the policies for this package, continue with the steps under [Section 14.5, “Associating the Service Location Package,” on page 168](#) to associate the policy package.

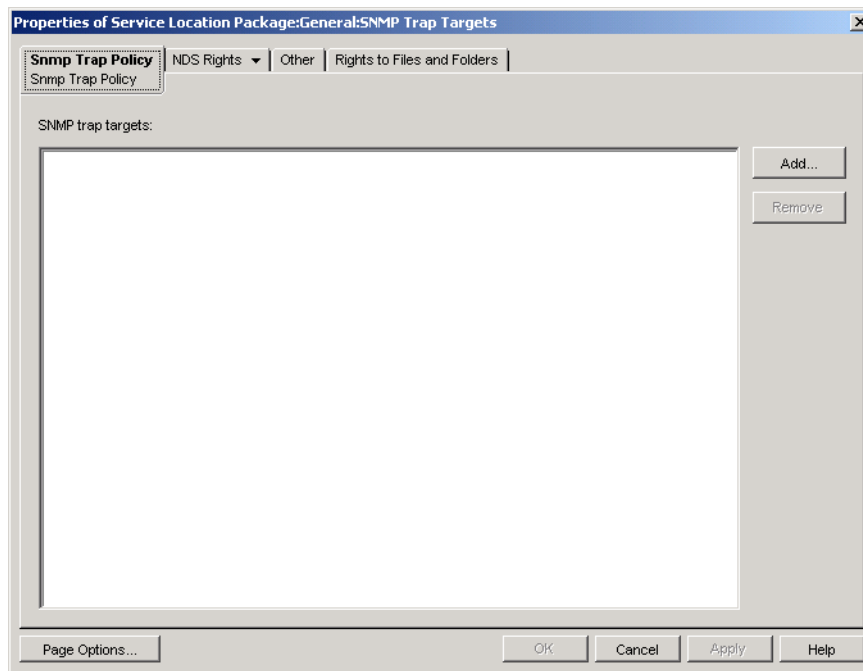
14.2 SNMP Trap Targets Policy

If you are using SNMP, you should configure and enable this policy. You use this policy to establish the targets (or locations) where you want SNMP traps sent. Each target must be a valid TCP/IP address or DNS name.

To set up the SNMP Trap Targets policy:

- 1 In ConsoleOne, right-click the Service Location Package, then click *Properties*.
The *General* tab is displayed.
- 2 Select the check box under the *Enabled* column for the SNMP Trap Targets policy.
This both selects and enables the policy.

3 Click *Properties*.



- 4 Click *Add*, enter a new target, then click *OK*.
- 5 Repeat **Step 4** for each trap target you need.
- 6 Click *OK* to save the policy.
- 7 When you have finished configuring all of the policies for this package, continue with the steps under **Section 14.5, “Associating the Service Location Package,” on page 168** to associate the policy package.

14.3 XML Targets Policy

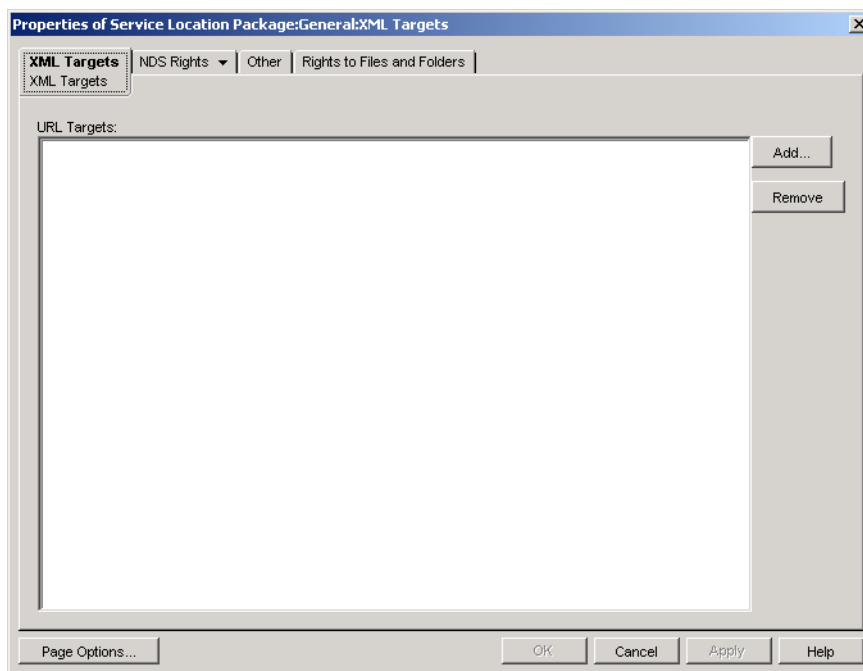
Extensible Markup Language (XML) is a flexible way to create common information formats and share both the format and the data on the Internet, intranets, and elsewhere. If you choose to export and view Application Management information in XML format via the Internet, you should configure and enable this policy. The XML Targets policy lets you assign the URL that you'll use to view this information.

While performing the following steps, you can get detailed information about each dialog box by clicking the *Help* button.

To set up the XML Targets policy:

- 1 In ConsoleOne, right-click the Service Location Package, then click *Properties*.
The *General* tab is displayed.
- 2 Select the check box under the *Enabled* column for the XML Targets policy.
This both selects and enables the policy.

3 Click *Properties*.



- 4 Click *Add*, type the URL, then click *OK*.
- 5 Click *OK* to save the policy.
- 6 When you have finished configuring all of the policies for this package, continue with the steps under [Section 14.5, “Associating the Service Location Package,” on page 168](#) to associate the policy package.

14.4 ZENworks Database Policy

In previous versions of ZENworks[®] for Desktops, you configured and enabled the ZENworks Database policy using the Service Location Package only. You can now also configure and enable this policy in the Server Package. For more information see, [Section 13.6, “ZENworks Database Policy,” on page 161](#).

14.5 Associating the Service Location Package

The policies you configured and enabled are not in effect until you associate their policy package with a container object.

- 1 In ConsoleOne, right-click the Service Location Package, then click *Properties*.
- 2 Click the *Associations* tab, then click *Add*.
- 3 Browse for and select the container for associating the package, then click *OK*.

Setting Up User and Workstation Package Policies

15

Review the following sections for information to help you set up and associate the User and Workstation Package policies:

- [Section 15.1, “Platform Pages,” on page 169](#)
- [Section 15.2, “Computer/User Extensible Policies \(Workstation/User Packages\),” on page 172](#)
- [Section 15.3, “Dynamic Local User Policy \(User Package\),” on page 177](#)
- [Section 15.4, “Novell iPrint Policy \(User and Workstation Packages\),” on page 182](#)
- [Section 15.5, “Remote Control Policy \(User and Workstation Packages\),” on page 187](#)
- [Section 15.6, “Scheduled Action Policy \(User and Workstation Packages\),” on page 187](#)
- [Section 15.7, “User Extensible Policies \(User Package\),” on page 190](#)
- [Section 15.8, “Windows Desktop Preferences Policy \(User Package\),” on page 190](#)
- [Section 15.9, “Windows Group Policy \(User and Workstation Packages\),” on page 192](#)
- [Section 15.10, “Workstation Imaging Policy \(Workstation Package\),” on page 204](#)
- [Section 15.11, “Workstation Inventory Policy \(Workstation Package\),” on page 204](#)
- [Section 15.12, “ZENworks Desktop Management Agent Policy \(Workstation Package\),” on page 204](#)
- [Section 15.13, “Associating the User or Workstation Package,” on page 207](#)

NOTE: The information in this section also applies to ZENworks® 7 Desktop Management with Support Pack 1.

15.1 Platform Pages

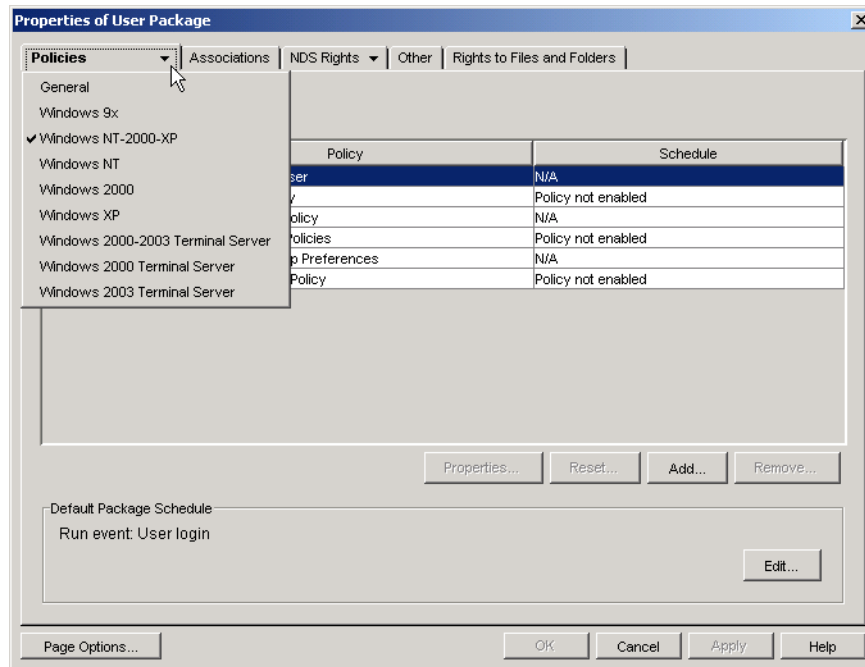
Desktop Management provides policies that apply to various individual computer platforms, to a combination of platforms, and to a General platform, which lets you configure policies that apply to all platforms.

To display a platform page:

- 1 In ConsoleOne®, right-click the User Package or Workstation Package, then click *Properties*.

- 2 Click the down-arrow on the *Policies* tab, then select the desired platform.

Figure 15-1 *The User Package Properties Page*



The following table lists each platform page, the package that contains each platform page, and a brief description:

Table 15-1 *Platform Pages and the Packages They Contain*

Platform Page	Package	Description
General	User and Workstation Packages	<p>Lists the available policies for the General page.</p> <p>Policies set on this page apply to all platforms unless you configure the same policy on a specific platform page; policies set on a specific platform page override policies set on the General page.</p>
Windows 9x	User and Workstation Packages	<p>Lists the available policies for Windows 9.x machines.</p> <p>Although Microsoft no longer supports Windows 95, existing Windows 95/98 policies from a previous installation of ZENworks that are associated with Windows 95 machines or users will continue to function. Desktop Management does not allow you to create new policies for Windows 95 machines or users.</p>

Platform Page	Package	Description
Windows NT-2000-XP	User and Workstation Packages	<p>Lists the available policies for Windows NT/2000/XP machines.</p> <p>Use this page if you do not want to treat Windows NT/2000/XP machines as separate platforms. You can also use this page to set policies for users and workstations that are using earlier versions of ZENworks for Desktops.</p> <p>If you are using the Novell Client™ without the Desktop Management Agent, you must configure and enable policies on this page rather than on the individual platform pages listed below (Windows NT, Windows 2000, or Windows XP).</p> <p>If you are upgrading from a previous version of ZENworks for Desktops, your existing policies are listed on this platform page. New platform pages that separate the Windows NT/2000/XP platforms into individual platform pages were new enhancements to ZENworks for Desktops 4. You can continue to manage your policies from a previous version of ZENworks for Desktops on this page or you can configure and enable new policies that apply to individual platforms by using one of the specific platform pages listed below.</p> <p>For more information about Desktop Management support for the Windows NT platform, see “Interoperability with Windows NT 4 Workstations” in the <i>Novell ZENworks 7 Desktop Management Installation Guide</i>.</p>
Windows NT	User and Workstation Packages	<p>Lists the available policies for Windows NT machines¹.</p> <p>For more information about Desktop Management support for the Windows NT platform, see “Interoperability with Windows NT 4 Workstations” in the <i>Novell ZENworks 7 Desktop Management Installation Guide</i>.</p>
Windows 2000	User and Workstation Packages	<p>Lists the available policies for Windows 2000 machines¹.</p>
Windows XP	User and Workstation Packages	<p>Lists the available policies for Windows XP machines¹.</p>

Platform Page	Package	Description
Windows 2000-2003 Terminal Server	User Package only	Lists the available policies for Windows 2000 or Windows 2003 Terminal Servers ² . You should use this page if you want to set policies that apply to both platforms to make managing Terminal Servers easier. If you want to treat Windows 2000 and Windows 2003 Terminal Servers as separate platforms, use one of the specific platform pages.
Windows 2000 Terminal Server	User Package only	Lists the available policies for Windows 2000 Terminal Servers ² .
Windows 2003 Terminal Server	User Package only	Lists the available policies for Windows 2003 Terminal Servers ² .

¹ Policies enabled on this page are applied only on workstations that have been upgraded to ZENworks for Desktops 4 or newer. To set policies for workstations using earlier versions of ZENworks for Desktops, use the Windows NT-2000-XP page.

² Because earlier versions of ZENworks did not support Terminal Servers, policies enabled on this page are applied only on workstations that have been upgraded to ZENworks for Desktops 4 or newer.

You must be running the Desktop Management Agent to configure and enable policies for Terminal Servers.

Terminal Servers do not support the Scheduled Action and Remote Control policies.

15.2 Computer/User Extensible Policies (Workstation/User Packages)

For any Windows-compatible software program, an extensible policy allows you to control any application function that is configured in the Windows registry. Desktop Management lets you easily customize and deploy extensible policies across your network to accommodate your specific business practices.

NOTE: Computer Extensible policies are contained in the Workstation Package; User Extensible policies are contained in the User Package. The information in this section applies to both packages; however, there are differences between the two packages. When you set Computer Extensible policies in the Workstation Package, the policies apply to all users who log in to an associated workstation. When you set User Extensible policies in the User Package, the policies apply to all associated users regardless of the workstation they use.

The following sections contain additional information:

- [Section 15.2.1, “Understanding Extensible Policies,” on page 173](#)
- [Section 15.2.2, “Configuring Extensible Policies,” on page 174](#)

15.2.1 Understanding Extensible Policies

Desktop Management leverages Microsoft desktop enhancements by doing the following to provide extensible policies that are enabled in the directory:

- Moving the policy editor functionality into the directory
- Moving Windows registry information for applications into the directory
- Enabling the directory to point to extensible policy files

Review the following sections for more information:

- [“How Extensible Policies Work” on page 173](#)
- [“.Adm Files” on page 173](#)

How Extensible Policies Work

When you install a software application that is compatible with Windows, the application's installation program uses the Microsoft policy editor (`poledit.exe`) to read the application's `.adm` file and create a `.pol` file that updates the workstation's Windows registry. However, when you install an application on a workstation under the umbrella of Desktop Management, the Desktop Management policy editor (`wmpolshp.exe`) is used to read the `.adm` file and make the necessary changes to the workstation's Windows registry.

The Microsoft policy editor lets you make changes to the policies created by the `.adm` files, but only per workstation. If an application is installed using the Application Management component of Desktop Management, the Desktop Management policy editor ensures that the application's directory-enabled policies are automatically applied across the network, rather than manually to one workstation at a time.

Extensible policies are not supported on Windows XP. You should use Windows Group policies to configure policies for Windows XP systems. Additionally, we recommend that you use Windows Group policies instead of extensible policies for Windows 2000 or newer. You should continue using extensible policies for the Windows 9.x/NT platforms.

Extensible policies are not cumulative. Unless specified differently in a Search policy, when Desktop Management starts searching for an object's associated policy packages, it starts at the object and works its way up the tree. Because extensible policies are not cumulative, Desktop Management walks the tree until it finds the first effective policy for the object and applies that policy's settings.

.Adm Files

Files with the `.adm` extension provide customizable attributes for users and workstations. You can add existing `.adm` files and configure their settings to create extensible policies. Depending on whether you are configuring User Extensible policies or Computer Extensible policies, the attributes you can customize will vary.

The `.adm` files are static templates for creating policies in the ZENworks database. When you edit a policy in Desktop Management, the changes are made in the database rather than in the `.adm` file. Even so, you should not delete an `.adm` file from a directory after it has been used in Desktop Management because it is needed to undo registry changes if you should remove the policy from Desktop Management.

When you have .adm files that you want to use, you should place them in a location where you can easily browse for them. You should save them on a server, because after the .adm file has been used to create a policy, it is not needed again until you modify the policy.

Because Desktop Management automatically displays any policies listed in the following location when you view an Extensible Policies page, we recommend that you use it:

```
sys:\public\mgmt\consoleone\1.2\bin\zen\adm files
```

This is the default location where .adm files shipped with Desktop Management are placed if you run ConsoleOne from the server. If you run ConsoleOne from a workstation, .adm files are placed in the consoleone\1.2\bin\zen directory on the workstation.

15.2.2 Configuring Extensible Policies

The Computer Extensible/User Extensible policies are not found on the General or Windows XP platform pages.

To set up the Computer Extensible or User Extensible policies:

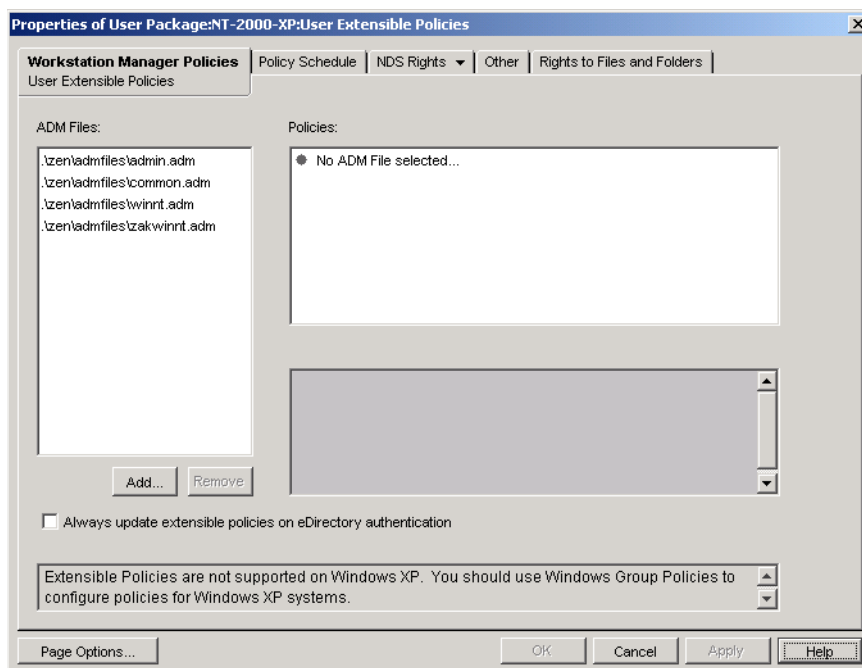
- 1 In ConsoleOne, right-click the User Package or the Workstation Package, click *Properties*, then click the appropriate **platform page**.

For more information about Desktop Management support for the Windows NT platform, see “**Interoperability with Windows NT 4 Workstations**” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

- 2 Select the check box under the *Enabled* column for the Computer Extensible or User Extensible policies.

This both selects and enables the policy.

- 3 Click *Properties* to display the User Extensible/Computer Extensible Policies page.



The User Extensible/Computer Extensible Policies page is divided into three areas.

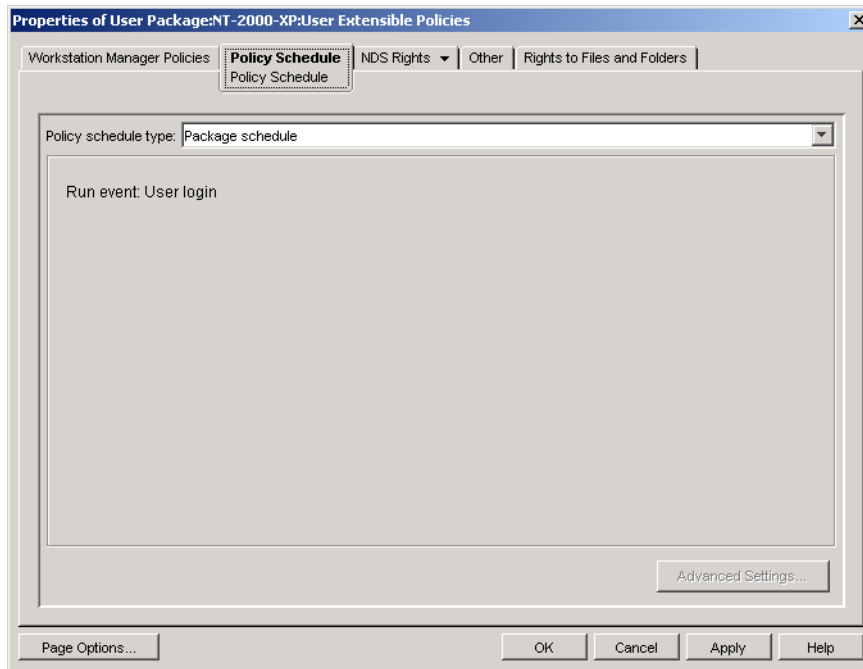
- **ADM Files:** The *ADM Files* list box displays, by default, the four .adm files that are automatically pulled into ConsoleOne by the Desktop Management plug-in: admin.adm, common.adm, winnt.adm, and zakwinnt.adm. You can use the *Add* button to add .adm files for applications that you have installed using ZENworks Application Management to the list. You can use the *Remove* button to remove .adm files from the list. Do not manually delete an .adm file from its directory without first removing it in ConsoleOne from the *ADM Files* list. If you first delete the .adm file from the directory, registry changes that enable the policy are still in effect.
 - **Policies:** When you select an .adm file in the *ADM Files* list box, its registry contents are displayed in the *Policies* list box. You can expand and traverse the policy tree to enable or disable each policy attribute.
 - **Settings:** The policy-specific *Settings* box at the bottom right of the page displays other attribute options with check boxes that can be enabled or disabled. It can also provide fields for information entry or drop-down lists for selecting attribute options.
- 4 To edit the properties of a policy, click the policy in the *ADM Files* box, then browse and edit the policy settings in the *Policies* and *Settings* list boxes.

The check box states are as follows:

Check Box	State	Description
<input checked="" type="checkbox"/>	Enabled	The attribute is enabled in the client. Any values you enter for it are applied.
<input type="checkbox"/>	Disabled	The attribute is disabled in the client.
<input type="checkbox"/> or <input checked="" type="checkbox"/>	Ignored	The attribute is ignored (not changed in the client). If the attribute is already enabled in the client, it remains enabled. If it is already disabled in the client, it remains disabled.

- 5 (Optional) Select the *Always Update Extensible Policies on eDirectory Authentication* check box if you want extensible policies to be pushed when the user or workstation is authenticated.
- 6 Repeat **Step 4** and **Step 5** for each extensible policy to be added.

7 Click the *Policy Schedule* tab.



When you create an extensible policy, you must schedule it to run before it can take effect. Some hard-coded policies are run explicitly at login. Such policies are not scheduled.

8 Select a schedule type:

Package Schedule

Event

Daily

Weekly

Monthly

Yearly

Click the *Help* button on the *Schedule* tab for more information about each schedule.

For a Windows 98 User Extensible policy, even if you select *User Login* on the Policy Schedule page, the *Color Scheme* settings are not applied until the user logs out. When the user logs in again, the settings are correct. However, if you first create a user profile on the workstation under *Control Panel > Users*, the settings are applied when the user logs in the first time.

9 Click *Apply*.

Until you click *Apply*, policy changes are kept in a temporary location. Because of this, if two .adm files have the same check box item attribute (the same Windows registry entry), a change made in one .adm file is seen in the other.

10 Repeat **Step 1** through **Step 9** for each platform where you want to set a User Extensible/Computer Extensible policy.

11 When you have finished configuring all of the policies for this package, continue with the steps under **Section 15.13, “Associating the User or Workstation Package,” on page 207** to associate the policy package.

15.3 Dynamic Local User Policy (User Package)

A dynamic local user (DLU) is a User object that is temporarily or permanently created in the workstation's Security Access Manager (SAM) database.

A temporary user or account is known as a volatile user, and the duration is determined by the administrator. This type of account prevents the SAM from becoming too large.

If your environment has several users who log on to a shared workstation or Terminal Server, you can configure and enable the Dynamic Local User (DLU) policy. After you have configured and enabled this policy, Desktop Management dynamically creates user accounts on the local workstation or Terminal Server while the user is logging in to the system.

For Windows NT/2000/XP workstations and Windows 2000/2003 Terminal Servers, the Dynamic Local User policy lets you configure users created on Windows NT/2000/XP workstations and Windows 2000/2003 Terminal Servers after they have authenticated to the directory. After a user has been associated with a Configuration object, NetWare® Graphical Identification and Authentication (NWGINA) can retrieve information from the Configuration object to create a user account on the workstation.

If a user is not defined as a DLU and does not have an account on the workstation, the user's account cannot be created. Therefore, the user cannot log in to the workstation, unless there is a previous account, or the administrator manually creates the user's account on the workstation. If the user is not defined as a DLU, the user's credentials from the *Windows NT/2000/XP* tab of the login dialog box are used to authenticate to the workstation.

If the user is defined as a DLU, the user's credentials from the directory or from the User Package, depending on how the administrator sets it up, are used.

If you configure a DLU in a User Policy Package to administer user access to NT/2000/XP workstations or Windows 2000/2003 Terminal Servers, and if you use a credential set other than the NetWare credential set, the workstation user accounts created have a random, unknown password and are created as volatile user accounts. If volatile user caching is also enabled, the user accounts persist on the workstation for the duration of the cache life. However, these accounts are inaccessible because they have an unknown password.

If you use volatile user caching for users with non-NetWare credential sets, those user accounts are not accessible unless the users log in to the directory concurrently and have the *Manage Existing User Account* option set.

You can allow or restrict DLU login access to certain workstations by using the Login Restrictions page. Workstations and containers listed in the *Excluded Workstation* list cannot use DLU access; workstations listed or workstations that are part of containers listed in the *Included Workstations* list can use DLU access.

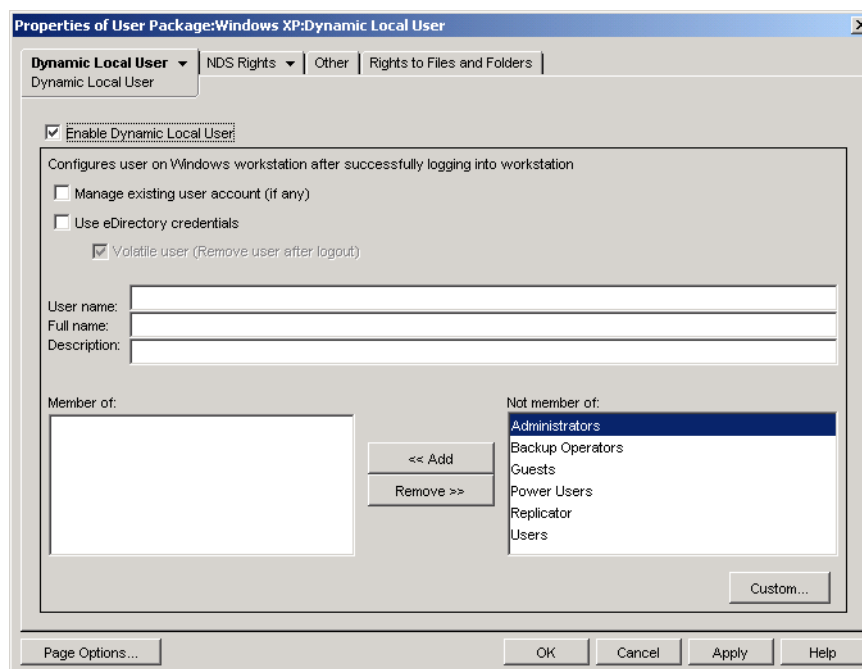
To properly manage group priorities, do not allow users associated with DLUs to be members of multiple groups.

To set up the Dynamic Local User policy:

- 1 In ConsoleOne, right-click the User Package, click *Properties*, then click the appropriate [platform page](#).

For more information about Desktop Management support for the Windows NT platform, see “[Interoperability with Windows NT 4 Workstations](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

- 2 Select the check box under the *Enabled* column for the Dynamic Local User policy.
This both selects and enables the policy.
- 3 Click *Properties*.



- 4 Fill in the fields:

Enable Dynamic Local User: Enables creation of a User object that resides either temporarily or permanently in the workstation’s Security Access Manager (SAM) database.

NWGINA requires that you specify whether a local user is to be created.

If this check box is not selected, NWGINA does not create a user in the local SAM. Instead, NWGINA attempts to find an existing user with the credentials indicated in the NWGINA login interface.

If the *Enable Dynamic Local User* check box is selected, NWGINA gets the Username from the Configuration object and queries the local SAM to see if the Username already exists. If it does exist, NWGINA authenticates the user to the workstation or Terminal Server and access is granted. If the Username does not exist, NWGINA creates the user in the local workstation’s or Terminal Server’s SAM.

If password restriction policies are set on the local workstation or Terminal Server, Dynamic Local User is not used. The password that the DLU uses for the local account must meet local workstation password restrictions.

Manage Existing User Account (If Any): Allows management through the existing user account. Enable this option if the User object you want to manage already exists. Workstation group assignments specified by Workstation Management are implemented, including changing the account from nonvolatile to volatile when the user logs in to the account. The account is also removed from the workstation after the user logs out.

If this check box and the *Volatile User* check box are both selected, and the user has a permanent local account that uses the same credentials specified in eDirectory™, the permanent account is changed to a volatile (temporary) account. The account is managed, but is removed when the volatile user cache age is reached or the user logs out.

Any settings you change here overwrite the current account settings at the workstation or Terminal Server. If this option is not enabled, Workstation Management cannot manage the existing User object.

Use eDirectory Credentials: Enables logging in through the user's eDirectory credentials instead of NT/2000/XP credentials. When creating the user account, NWGINA can use either the same credential set used for eDirectory authentication or a predetermined credential set specified in the Configuration object. When using eDirectory credentials to create the workstation user account, NWGINA queries the user's eDirectory account for the login name, full name, and description. The password for the NT/2000/XP user account is the same as that for the eDirectory user account.

If eDirectory credentials are not used, the account is always volatile and is not accessible. *Full Name* and *Description* can also be included to provide a complete user description.

If you don't use eDirectory credentials and the user account does not already exist (as indicated by the *Manage Existing User Accounts* check box), the user account is created as a volatile user account, which means that the user account is automatically deleted at logout. This is apparent because the *Volatile User* check box is automatically enabled if the *Use eDirectory Credentials* check box is not enabled.

Volatile User (Remove User After Logout): Specifies the use of a volatile user account for login. The user account that NWGINA creates on the local workstation can be either a volatile or a nonvolatile account.

Be aware that if you select both the *Volatile User (Remove User After Logout)* and *Manage Existing User Account (If Any)* check boxes, the volatile user account is removed when the user logs out, even if the account existed before the user logged in using DLU.

User Name: The NT/2000/XP user name. The user name (not including the context) must contain fewer than 20 characters for a dynamic local user to log in.

A user that is manually created via User Manager can't have a longer name.

Full Name: The user's full name.

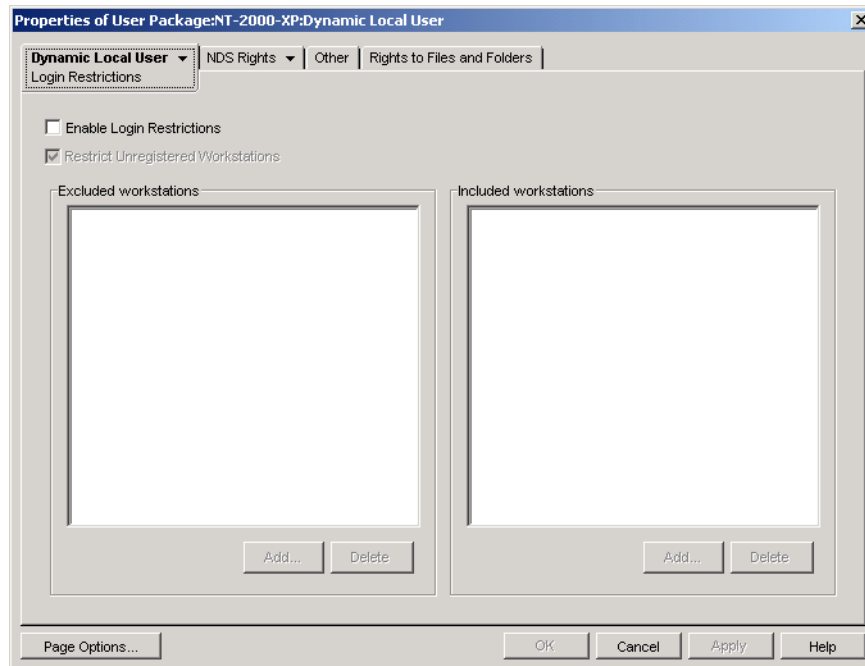
Description: Enter any additional information that helps you to further identify this user account.

Member Of: Lists the groups where this user has membership. When NWGINA creates the workstation user, it can provide group membership to any user groups. The groups that the user is added to are listed in the *Members Of* list. The default configuration is for the user to be added to the Users group. Other groups can be added by selecting the group and clicking *Add*. Groups can be removed by selecting the group and clicking *Remove*.

Not Member Of: Lists available groups where this user has not been assigned as a member.

Custom: Opens the Custom Groups page, where you can add a new custom group, delete an existing custom group, and view or modify properties of an existing custom group. Click the *Help* button on the Custom Group Properties dialog box for more information about the available options.

- 5 (Optional) If you want to restrict DLU access to certain workstations, click the down-arrow on the *Dynamic Local User* tab > click *Login Restrictions*.



- 5a Select the *Enable Login Restrictions* check box to restrict DLU access to certain workstations.

When you select the *Enable Login Restrictions* check box, the *Add* and *Delete* buttons are available.

- 5b Select the *Restrict Unregistered Workstations* check box if you want to restrict DLU access to unregistered workstations

In previous releases of ZENworks for Desktops, workstations that had not registered in eDirectory could not be given DLU access because they could not be listed in the *Included Workstation* list. If you enable this option, all unregistered workstations cannot be granted DLU access (as in previous versions of ZENworks for Desktops). If you do not select the *Restrict Unregistered Workstations* check box, all unregistered workstations can be granted DLU access even if they do not appear in the *Included Workstations* list.

- 5c Use the *Add* and *Delete* buttons under the *Excluded Workstations* list box as appropriate.

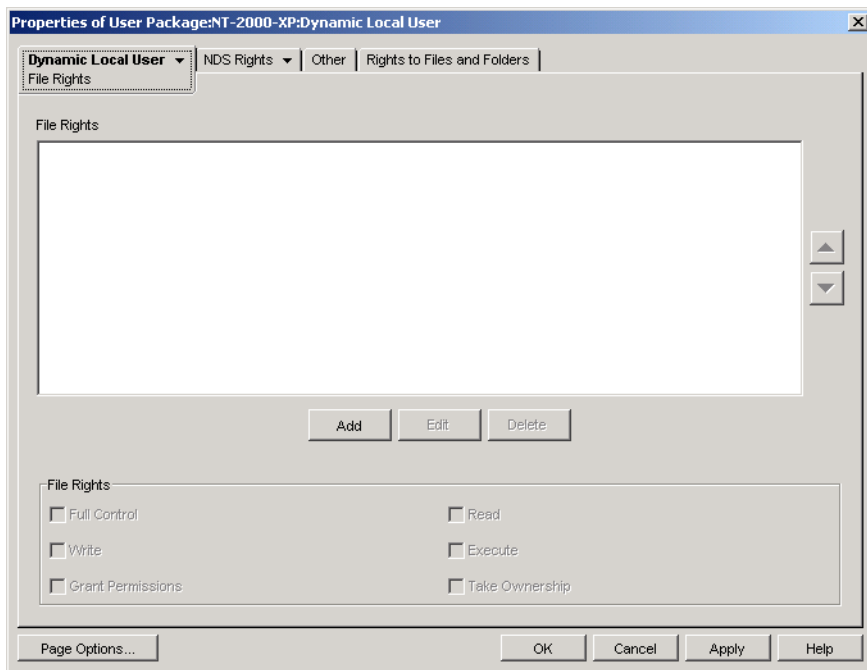
The *Excluded Workstation* box lists the workstations and containers that you want to exclude DLU access to. Workstations listed or workstations that are part of containers listed in this box cannot use DLU access. You can make exceptions for individual workstations by listing them in the *Included Workstation* list. This allows DLU access to those workstations only, while excluding DLU access to the remaining workstations in the container.

- 5d Use the *Add* and *Delete* buttons under the *Included Workstations* list box as appropriate.

The *Included Workstations* box lists the workstations and containers that you want to allow DLU access to. Workstations listed or workstations that are part of containers listed in this box can use DLU access. You can make exceptions for individual workstations by listing them in the *Excluded Workstation* list. This excludes DLU access to those

workstations only, while allowing DLU access to the remaining workstations in the container.

- 6 (Optional) Click the down-arrow on the *Dynamic Local User* tab > click *File Rights* if you want to manage DLU file system access on Windows NT/2000/XP workstations and Terminal Servers.



You can control access to entire directories or to individual files. For example, if the Dynamic Local User policy creates the user as a member of a group that does not give access to a directory required to run an application, you can use this page to explicitly grant the required directory rights. Or, if the user has Full Control rights to a directory, you can use this page to limit rights to any of the directory's files.

- 6a Use the *Add* button to modify the directories and files to which the user has been explicitly assigned file system rights.

You are prompted to enter or select the directory or file. The directory or file path must be from the perspective of the workstation or Terminal Server where the rights will be assigned. After you add a directory or file to the list, select the directory or file, then use the *File Rights* box to assign the appropriate file rights (Full Control, Read, Write, Execute, Grant Permissions, and Take Ownership).

The *File Rights* list displays the directories and files to which the user has been explicitly assigned file system rights. When you select a directory or file in the list, the assigned rights are shown in the *File Rights* box below the list. For an explanation of each of these rights (Full Control, Read, Write, Execute, Grant Permissions, and Take Ownership), refer to the Microsoft Windows operating system documentation.

- 6b Use the Arrow buttons on the right side of the *File Rights* list box to reposition the entries as appropriate.

Directory rights are assigned in the order the directories are listed, from top to bottom. Because of directory rights inheritance, if a directory and its subdirectory are listed, the

subdirectory must be listed after its parent directory. This ensures that the subdirectory's explicitly assigned rights are not overridden by rights inherited from its parent directory.

File rights always take precedence over directory rights, regardless of their position in the list. For example, if you assign Full Control rights to the `c:\program files` directory and Read and Execute rights to the `c:\program files\sample.txt` file, the user is assigned Read and Execute rights to the file regardless of whether the file is listed before or after the directory.

It is possible to block the inheritance of rights on the NTFS files system, and under Windows XP, by default, the Windows directory does not allow rights to be inherited.

- 7 Click *OK* to save the policy.
- 8 Repeat **Step 1** through **Step 7** for each platform where you want to set a Dynamic Local User policy.
- 9 When you have finished configuring all of the policies for this package, continue with the steps under **Section 15.13, "Associating the User or Workstation Package," on page 207** to associate the policy package.

15.4 Novell iPrint Policy (User and Workstation Packages)

The Novell® iPrint policy lets you configure a Novell iPrint client that can be placed on workstations. Using the Novell iPrint client, users can use the Internet to print to iPrint printers just like any other printer, regardless of the printer's physical location.

NOTE: The Novell iPrint policy is contained in both the User Package and in the Workstation Package. The information in this section applies to both packages; however, there are differences between the two packages. When you configure the Novell iPrint policy contained in the User Package, the policy applies to all associated users regardless of the workstation they use. When you configure the Novell iPrint policy contained in the Workstation Package, the policy applies to all users who log in to an associated workstation.

IMPORTANT: Unless you are running NetWare 6.5 SP2 or later, you must download the latest Novell iPrint utility file from **TID 2968629** (<http://support.novell.com/cgi-bin/search/searchtid.cgi?/2968629.htm>). See **Step 4 on page 184** for more information.

Novell iPrint ships with NetWare 6 (Support Pack 2 or newer) and Open Enterprise Server Linux, or it can be purchased separately. Novell iPrint also runs on NetWare 5.1 (Support Pack 5 or newer). The Novell iPrint policy in Desktop Management replaces all previous ZENworks printer policies. If you are upgrading from a previous version of ZENworks for Desktops and are running previous printer policies, Desktop Management supports them. For further information about iPrint, see the **iPrint Product Web page** (<http://www.novell.com/products/netware/printing/index.html>).

In order to use the Novell iPrint policy, be aware of the following:

- **NetWare/Open Enterprise Server Linux:** To use the iPrint client, you must have at least one NetWare or Open Enterprise Server Linux server in your system. If you choose to not use the iPrint client, you can still use your existing Microsoft printing setup outside of Desktop Management.

- **Desktop Management Agent:** You must also install the Desktop Management Agent on each workstation where you want to run the iPrint client; the policy does not run on a workstation that uses only the Novell Client.
- **Using the Novell iPrint Policy for the Windows NT/2000/XP Platforms Contained in the User Package:** If you configure the Novell iPrint policy as part of a User package to be pushed to Windows NT/2000/XP workstations, you must change the *AllowUserPrinters* value in the `iprint.ini` file (refer to [Step 4 on page 184](#) for the default location of the `iprint.ini` file) from the default value of 0 to 1.
- **Using the Novell iPrint Policy in Conjunction with the Dynamic Local User or Windows Desktop Preferences Policies:** If you are managing user profiles using the [Dynamic Local User](#) or [Windows Desktop Preferences](#) policy, you must rename the native Microsoft Internet Print Provider (`inetpp.dll`) registry reference. Renaming this registry reference ensures that user profiles are properly closed or deleted when users log out. If user profiles remain open, when users log back in to workstations, the profile remains locked, causing multiple user accounts to be created.

To prevent this situation, you should change the following registry value:

```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Print\Providers\Internet Print Provider\Name
from inetpp.dll to inetpp.old.
```

You can also use ZENworks Application Management to deliver the iPrint client to users' workstations. For more information, see [Chapter 28, "Distribution: Simple Applications," on page 315](#). If you choose to distribute the iPrint client with a simple Application object, follow the instructions under [Path to the Novell iPrint Client Install](#) in [Step 4 on page 184](#) to make sure that the iPrint client install file (`nipp-s.exe`) is in its own directory location on your server.

To set up the Novell iPrint policy:

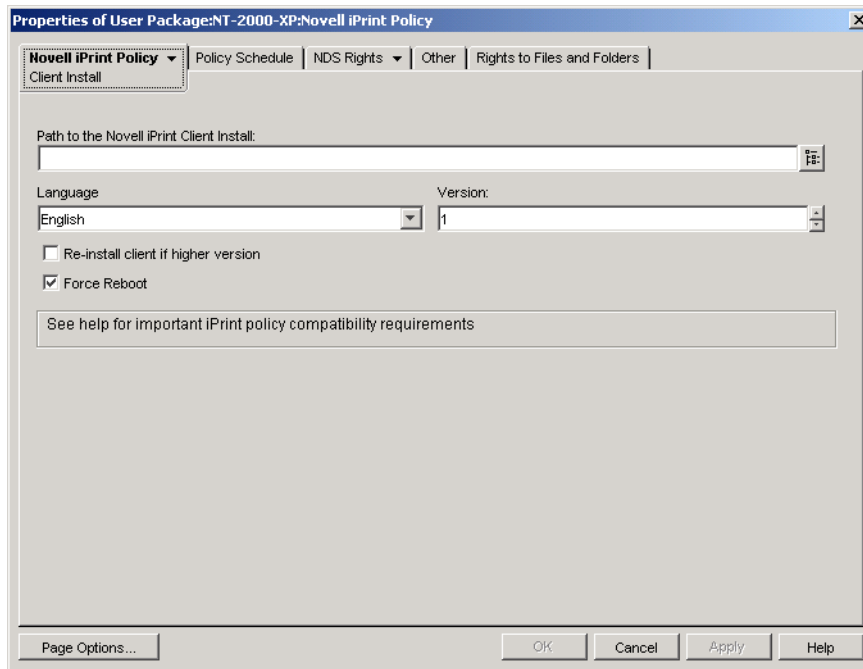
- 1 In ConsoleOne, right-click the User Package or Workstation Package, click *Properties*, then click the appropriate [platform page](#).

NOTE: For more information about Desktop Management support for the Windows NT platform, see "[Interoperability with Windows NT 4 Workstations](#)" in the *Novell ZENworks 7 Desktop Management Installation Guide*.

- 2 Select the check box under the *Enabled* column for the Novell iPrint policy.

This both selects and enables the policy.

3 Click *Properties* to display the Client Install page.



4 Fill in the fields:

Path to the Novell iPrint Client Install: Specify the path to the iPrint client install file (`nipp-s.exe`). This file must be the only file in its own directory location on your server. Make sure that users have rights to this directory.

Unless you are running NetWare 6.5 SP2 or later, you must download the latest Novell iPrint client install file from TID 2968629 in the [Novell Knowledgebase](http://support.novell.com/search/kb_index.jsp?sourceidint=hdr_support_kb) (http://support.novell.com/search/kb_index.jsp?sourceidint=hdr_support_kb).

The downloadable iPrint client install file is a self-extracting utility that places the `nipp-s.exe` file and other files in the directory that it is executed in.

After the latest `nipp.exe` is extracted, copy the `nipp-s.exe` (on NetWare 6.5 SP 2 it is already extracted to `sys:\apache2\htdocs\ippdocs`) to an empty directory where users have rights. For example, create an `iprint` directory under `sys:\login` and then copy the file to `sys:\login\iprint\`.

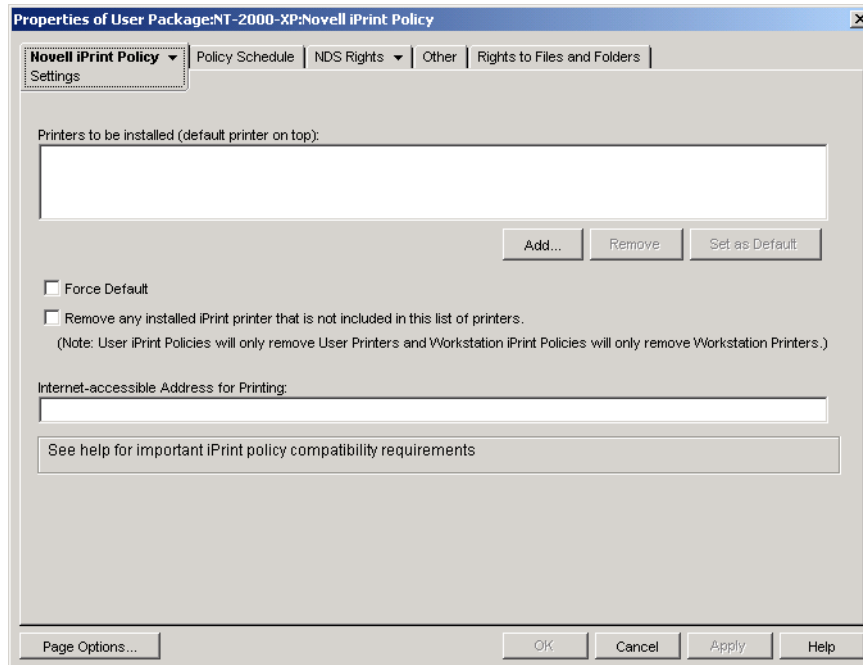
Language: Select a language from the drop-down list. If you are using the latest Novell iPrint client install file, the language that is installed is detected automatically, based on the configuration of the workstation. The English language is the default. If you push the iPrint client to a workstation that is configured for a non-localized language (Japanese, for example), the English version of the iPrint client is installed.

Version: Specify a version number for this iPrint policy. The version number you provide in this field does not reflect the actual version of the iPrint client. If you want to force a new iPrint policy to workstations or users to upgrade the iPrint client, you should increment the version number (from 1 to 2, for example). This version number is stored in the Windows registry. If the version number stored in the registry is lower than the number in the *Version* field, the iPrint client is installed if the *Re-install client if higher version* check box is selected.

Re-install client if higher version: Select this check box to re-install the iPrint client if the iPrint client listed in the *Path to the Novell iPrint Client Install* is newer than that installed on the workstation.

Force Reboot: Enable this option to force a reboot on each workstation after the iPrint client has been installed. We recommend that you use the default setting (enabled) for this option. You should use the default setting if you are performing a silent install after working hours. Also, you should use the default setting to avoid possible errors if you should uninstall the iPrint client from a workstation or reinstall the iPrint client to a workstation.

- 5 Click the down-arrow on the *Novell iPrint Policy* tab > click *Settings*.



- 6 Click *Add* to browse to a printer to add to the *Printers to be installed* list box.

or

Select a printer to be removed from the *Printers to be installed* list box, then click *Remove*.

Depending on users' driver signing settings, user workstations might display a "This driver is not digitally signed" message when the printer is installed. If you do not want users to see this message and be forced to choose to install the driver, you can change this setting in the Control Panel of each workstation (*Start > Settings > Control Panel > System > Hardware > Driver Signing*) or you can change this setting using a Windows Group policy in Desktop Management.

- 7 To select a default printer, select a printer in the *Printers to be installed* list box, then click *Set as Default*.

The user can also select another printer to use as the default.

- 8 Select the *Force Default* check box to force the selection of the default printer.

If a user changes the default printer, the default printer that you choose is set as the default each time this policy is run, according to its schedule.

The *Force Default* printer setting can only be set when a user is logged in. This setting does not work when the policy is scheduled to run at system startup.

- 9 (Optional) Select the *Remove any installed iPrint printer that is not included in this list of printers* check box.

If you selected the *Re-install client if higher version* check box in step **Step 4 on page 184**, any iPrint printers that were pushed by a previous version of the Novell iPrint policy to the workstation are removed, unless they are listed in the *Printers to be installed* list box.

Consider the following platform-specific information about using the *Remove any installed iPrint printer that is not included in this list of printers* check box:

- **Windows NT/2000/XP and Windows 2000/2003 Terminal Servers Platforms Contained in the User Package:** For the Windows NT/2000/XP platforms and Windows 2000/2003 Terminal Servers, if you are configuring the Novell iPrint policy contained in the User Package, enabling this option removes only those iPrint printers that were pushed to the workstation or Terminal Server using the Novell iPrint policy in the User Package.
- **Windows NT/2000/XP Platforms Contained in the Workstation Package:** For the Windows NT/2000/XP platforms, if you are configuring the Novell iPrint policy contained in the Workstation Package, enabling this option removes only those iPrint printers that were pushed to the workstation using the Novell iPrint policy in the Workstation Package. Additionally, if you enable this option in the Novell iPrint policy contained in the Workstation Package, and if the user of that workstation is locked down, that user does not have sufficient rights for that iPrint printer to be removed.
- **Windows 9x Platform in the User or Workstation Package:** For the Windows 9x platform, if you are configuring the Novell iPrint policy contained in either the User Package or the Workstation Package, the printers are installed as workstation printers, regardless of which type of package they were installed from. Enabling this option removes any iPrint printers that were pushed to the workstation using the Novell iPrint policy in either package.

- 10 (Optional) If you have workstations that are physically located outside the firewall, use the *Internet accessible Address for Printing* field to specify the proxy, firewall, or Network Address Translation (NAT) address followed by a colon (:) and the port number.

If you have workstations outside the firewall and they use Novell iPrint printers, you must open port 631. If you have workstations outside the firewall and they use secure printers that are not Novell iPrint printers, you must open port 443 (the standard port number for secure printers coming through a firewall).

If workstations are not located outside of the firewall, you should leave this field empty.

If you are using NetWare 6.5 and have workstations outside of the firewall, you must have a server proxy set up in order to use the Novell iPrint policy.

- 11 (Optional) Click the Policy Schedule page to schedule the Novell iPrint policy.

If you configure the Novell iPrint policy as part of a Workstation Package and schedule the package to run at system startup, the iPrint policy runs; however, printers cannot be pushed at system startup. For printers to be pushed to the workstation, a user must be logged in to the workstation. This is not an issue if you configure the Novell iPrint policy as part of a User Package because you cannot schedule User Package policies to run at system startup.

If you normally schedule Workstation Packages to run at system startup, you should create a schedule for the iPrint policy to run at user login or some other time when the user is logged in to the workstation. If you schedule an iPrint policy in a Workstation Package to run at user login, make sure that the *Impersonation* remains at the default: *System Impersonation* (*Advanced Settings > Impersonation*). If you set the policy to run at user login and interactive user, the policy fails to run.

- 12 Click *OK* to save the policy.
- 13 Repeat [Step 1](#) through [Step 12](#) for each platform where you want to set a Novell iPrint policy.
- 14 When you have finished configuring all of the policies for this package, continue with the steps under [Section 15.13, “Associating the User or Workstation Package,” on page 207](#) to associate the policy package.

NOTE: On Windows 98, the iPrint client installation applies to all user profiles on the workstation. If you set up different user profiles on a Windows 98 workstation before installing the iPrint client, *Novell iPrint Client* appears on the default user's Start Menu rather than on the logged-in user's Start Menu. For this reason, if you want to uninstall the iPrint client from a Windows 98 workstation using the *Novell iPrint Client Uninstall* option on the Start Menu, you need to log in as the default user. On Windows NT/2000/XP workstations, after installation of the iPrint client, *Novell iPrint Client* appears on the logged in user's Start menu.

15.5 Remote Control Policy (User and Workstation Packages)

Sets parameters for remote management sessions. This policy is available on each of the platform pages. For more detailed information, see [Part VII, “Remote Management,” on page 811](#).

15.6 Scheduled Action Policy (User and Workstation Packages)

The Scheduled Action policy sets up schedules for specific actions that you specify. As many as 15 items can be placed in an action.

NOTE: The Scheduled Action policy is contained in both the User Package and in the Workstation Package. The information in this section applies to both packages; however, there are differences between the two packages. When you configure the Scheduled Action policy contained in the User Package, the policy applies to all associated users regardless of the workstation they use. When you configure the Scheduled Action policy contained in the Workstation Package, the policy applies to all users who log in to an associated workstation.

Because scheduled actions do not apply to Terminal Server sessions, the Add button has been disabled on the Windows 2000-2003 Terminal Server, Windows 2000 Terminal Server, and Windows 2003 Terminal Server platform pages. Only those policies that are run before the Terminal Server's desktop is started apply to Terminal Server sessions.

The Scheduled Action policy is a plural policy, meaning it can be added many times to the policy package. Plural policies allow you to have multiple instances of the same policy type within the same policy package.

Because you can have several different actions that you might want to run on different schedules, when you add a Scheduled Action policy to the policy package you should name it to reflect the action being scheduled.

The Scheduled Action policy is available for each of the platform pages.

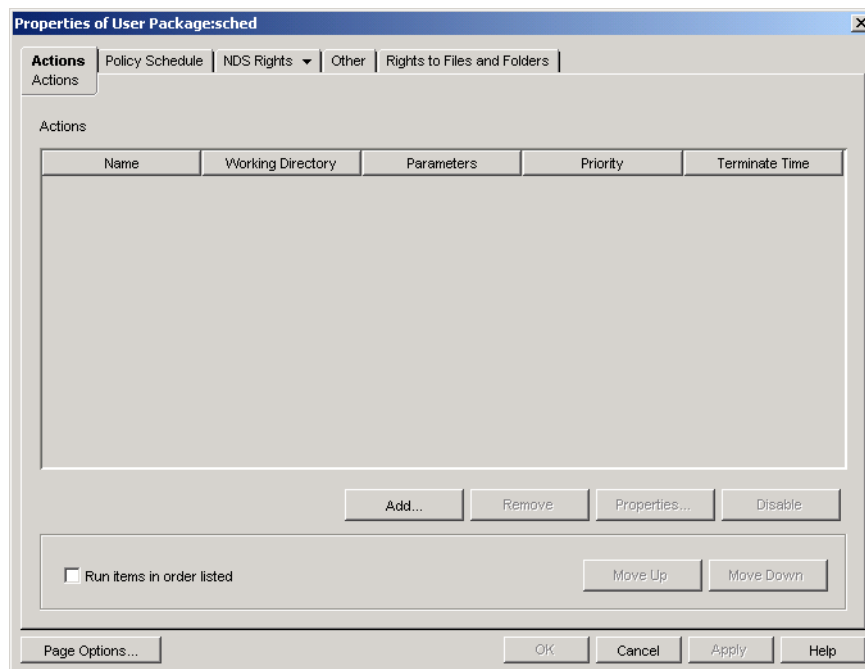
To set up the Scheduled Action policy:

- 1 In ConsoleOne, right-click the User Package or Workstation Package, click *Properties*, then click the appropriate **platform page**.

Policies set on a specific platform override policies set on the General page.

For more information about Desktop Management support for the Windows NT platform, see “**Interoperability with Windows NT 4 Workstations**” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

- 2 To add the Scheduled Action policy, click *Add*, give the policy a descriptive name, then click *OK*.
- 3 Select the check box under the *Enabled* column for the newly created Scheduled Action policy. This both selects and enables the policy.
- 4 Click *Properties* to display the Actions page.



- 5 Click *Add*.

- 6 Fill in the fields:

Name: The name of the action item.

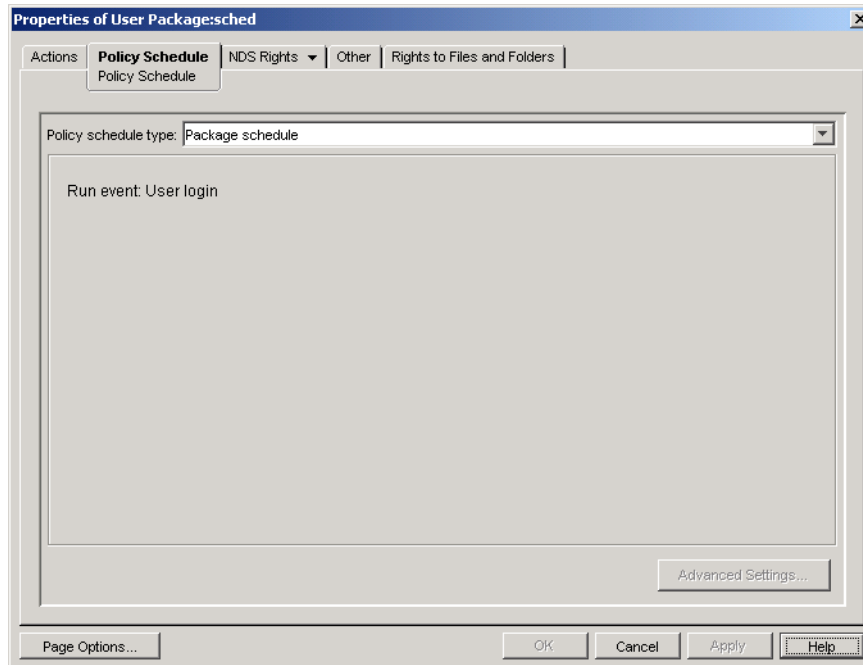
Working Directory: This is usually the path where the executable file for this action is located. It can be a different path if the program requires it.

Parameters: The parameters to pass to the action item. For more information, see the documentation associated with the executable file specified in the *Working Directory* field.

Priority: The importance assigned to this action in relation to the user’s access to the workstation.

Terminate Time: The length of time this action can run before the system stops it. The assumption is that if it takes longer than a specified time to run, there might be a problem associated with running this action and the action should be terminated.

- 7 Click *OK*.
- 8 Select the *Run items in order listed* check box if you want the items to run in the order they display in the list. You can reorder the list with the *Move Up* and *Move Down* buttons.
- 9 Click the *Policy Schedule* tab.



- 10 Select a schedule type:

Package schedule

Event

Daily

Weekly

Monthly

Yearly

Click the *Help* button on the Schedule tab for more information about each schedule.

If you select the *Event* schedule type and then select *User Logout* or *System Shutdown*, some actions cannot occur before the user is logged out or the system shuts down. If actions that are scheduled at user logout or system shutdown do not function as expected, try changing the schedule to another event.

- 11 Click *OK* to save the policy.
- 12 Repeat **Step 1** through **Step 11** for each platform where you want to set a Scheduled Action policy.
- 13 When you have finished configuring all of the policies for this package, continue with the steps under **Section 15.13, “Associating the User or Workstation Package,” on page 207** to associate the policy package.

15.7 User Extensible Policies (User Package)

For information about User Extensible policies, see [Section 15.2, “Computer/User Extensible Policies \(Workstation/User Packages\),”](#) on page 172.

15.8 Windows Desktop Preferences Policy (User Package)

Allows you to enable roaming profiles and apply desktop settings.

A user’s profile contains information that defines the way the screen works, such as desktop colors and patterns, desktop icons, and so forth.

Normally, a user profile works on just one workstation or Terminal Server. However, a profile stored on the network (called a roaming profile) follows the user regardless of where the user logs in from, so each network workstation or Terminal Server where the user logs in always has the same appearance. If the applications are stored on the network, the user also has access to the same applications.

You can enable a roaming profile or a mandatory profile and specify where the profile is to be stored. How changes to that profile are handled depends on the profile type.

In ZENworks for Desktops 4.x, if a slow link was detected that would require significant time to download a roaming profile, you could set registry keys to automatically download the roaming profile, use the locally stored profile, or display an instructional dialog box to let the user choose to either continue the download or to use the locally stored profile. This functionality is no longer supported in ZENworks 7 Desktop Management. All roaming profile processing is now handled by Microsoft.

This functionality is provided by the Microsoft native support for slow link detection. The Microsoft Group Policy Editor should now be used to configure slow link detection.

IMPORTANT: If roaming profiles are to be stored on a NetWare file system, either the Novell Client is required or CIFS needs to be installed on the NetWare server; CIFS lets workstations access the NetWare file system without needing the Novell Client.

You can store roaming profiles on a Windows server if the workstations are not running the Novell Client but are running the Microsoft SMB client.

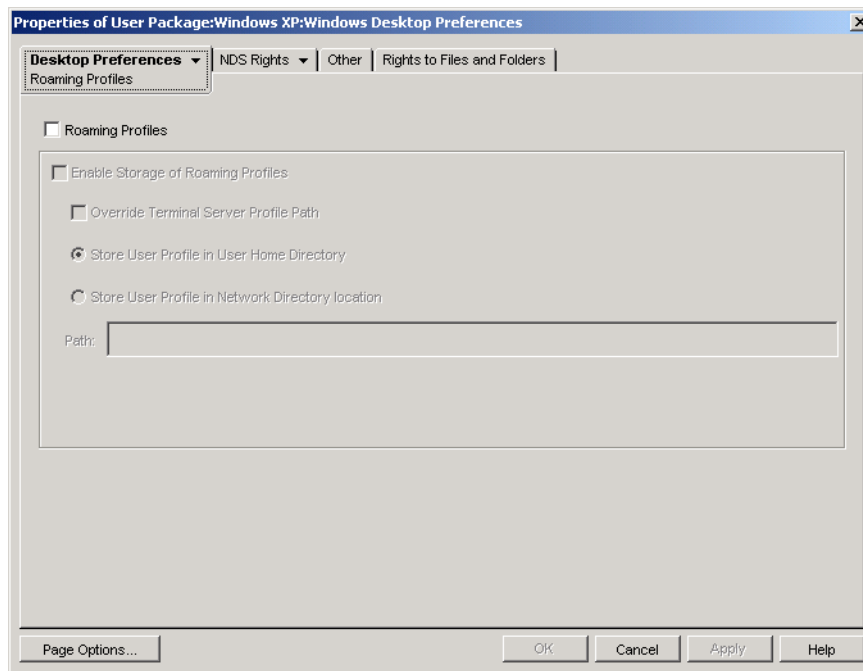
To set up the Windows Desktop Preferences policy:

- 1 In ConsoleOne, right-click the User Package, click *Properties*, then click the appropriate [platform page](#).

For more information about Desktop Management support for the Windows NT platform, see “[Interoperability with Windows NT 4 Workstations](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

- 2 Select the check box under the *Enabled* column for the Windows Desktop Preferences policy.
This both selects and enables the policy.

3 Click *Properties* to display the Roaming Profiles page.



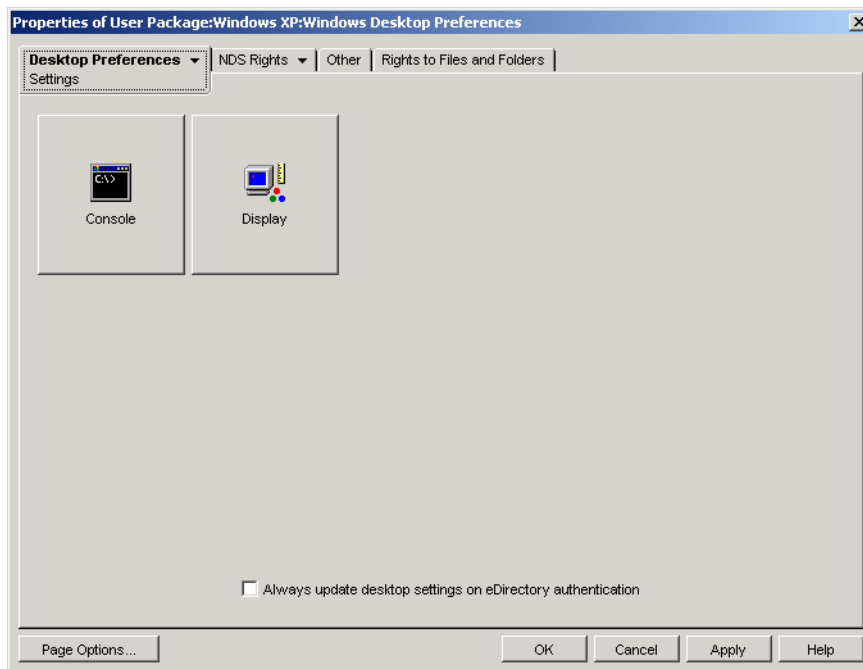
4 To enable roaming profiles, set the desired parameters in the following fields:

Roaming Profiles: Select this check box to enable roaming profiles. When you enable this check box, the other options on this page become available.

Enable Storage of Roaming Profiles: Select this check box to enable the storage of roaming profiles. This option allows profiles to be stored on a network server where they can be accessed from any workstation. Choose from the following options to specify how you want roaming profiles managed:

- **Override Terminal Server Profile Path:** If the user is accessing a Terminal Server that has its own profile, enable this option to override the Terminal Server's profile and use the roaming profile stored in the user's home directory or the profile stored in the network directory location specified in the Path field.
- **Store User Profile in User's Home Directory:** Stores the roaming profile on the network in the user's home directory. This allows the user to utilize the same desktop environment on all workstations throughout the network. Any changes made to the user's environment on one workstation are saved to the profile stored in the user's home directory on the network. The environment specified in the profile is then available on any workstation where the user subsequently logs in.
- **Store User Profile in Network Directory Location:** Stores the user profile in a network directory. When you choose this option, the user profile is stored on the network and users who have their roaming profiles pointed to this location share this profile. Any changes that users make to the profile are saved in the network directory location.
- **Path:** Specify the UNC path to the user's profile.

- 5 Click the down-arrow on the *Desktop Preferences* tab, then click *Settings*.



- 6 Click either the *Console* or *Display* button to display a dialog box that shows the options available for each feature.

This page displays icons matching the equivalent desktop features in Windows 98 or Windows NT/2000/XP.

See your Microsoft Windows documentation for help on these features and their options.

- 7 (Optional) Select the *Always update desktop settings on eDirectory authentication* check box.
- 8 Click *OK* to save the policy.
- 9 Repeat **Step 1** through **Step 8** for each platform where you want to set desktop preferences.
- 10 When you have finished configuring all of the policies for this package, continue with the steps under **Section 15.13, “Associating the User or Workstation Package,” on page 207** to associate the policy package.

15.9 Windows Group Policy (User and Workstation Packages)

You can specify and edit group policies for Windows 2000/XP workstations (User and Workstation Package) and for Windows 2000/2003 Terminal Servers (User Package only).

NOTE: The Windows Group policy is contained in both the User Package and in the Workstation Package. When you configure the Windows Group policy in the User Package, the policy applies to all associated users regardless of the workstation they use. When you configure the Windows Group policy in the Workstation Package, the policy applies to all users who log in to an associated workstation.

The following sections contain additional information:

- [Section 15.9.1, “Understanding the Windows Group Policy,” on page 193](#)
- [Section 15.9.2, “Configuring the Windows Group Policy in the User Package,” on page 195](#)
- [Section 15.9.3, “Configuring the Windows Group Policy in the Workstation Package,” on page 198](#)
- [Section 15.9.4, “Editing Existing Windows Group Policies \(User and Workstation Packages\),” on page 200](#)
- [Section 15.9.5, “Importing Windows Group Policies \(User and Workstation Packages\),” on page 202](#)

15.9.1 Understanding the Windows Group Policy

The Windows Group policy is an extension of extensible policies for Windows 2000/XP and Active Directory. There is some cross-over in policy settings between the Windows Group policy and Desktop Management extensible policies, such as under *User Configuration > Administrative Templates*. For more information about extensible policies, see [Section 15.2, “Computer/User Extensible Policies \(Workstation/User Packages\),” on page 172](#).

NOTE: You should not configure group policies on a Windows 2000 Domain Controller using ConsoleOne. To edit group policies through ConsoleOne, you should use a Windows 2000 workstation to edit Windows 2000 group policies and a Windows XP workstation to edit Windows XP group policies.

If a workstation is a member of an Active Directory domain but is disconnected from the domain, Windows Group policies contained in both the User and Workstation packages do not apply.

Using ZENworks Desktop Management to distribute Group policies to workstations or users where Group policies are already distributed by Active Directory (or vice versa) is not supported because of the unpredictable behavior that occurs. ZENworks Desktop Management does support distributing Active Directory settings. For more information, see [Section 15.9.5, “Importing Windows Group Policies \(User and Workstation Packages\),” on page 202](#).

For the following reasons, you must use UNC paths rather than mapped drives for importing this policy to Desktop Management:

- Users could change their login scripts, altering drive mappings
- Workstation objects are often logged in before users are, so there are no drive mappings available

With UNC paths, as long as the server is available, the policy is found.

Group policies have changed significantly since the ZENworks for Desktops 3 initial release. Review the following sections for more information:

- [“Additive Group Policies” on page 194](#)
- [“Revision Checking” on page 194](#)
- [“Group Policy Caching” on page 194](#)
- [“Persistent and Volatile Settings” on page 194](#)
- [“Using Group Policies on Terminal Servers” on page 194](#)

Additive Group Policies

Group policies are now additive. This means that settings from multiple Windows Group policies are cumulatively effective, rather than individually. Settings from multiple Windows Group policies can affect users and workstations. Policies start with the local Windows Group policy settings and are applied in reverse of the policy search order. This means that a setting in a policy applied first has lowest priority and its value is overwritten by any other policy with the same setting.

Security settings are not additive; they are set by the last effective policy.

Revision Checking

Windows Group policies now track the revision of the policies in effect. As long as the list of effective policies and their revisions remains the same, Windows Group policies are not processed, but use the cached Group policy.

NOTE: Each time the *Edit Policies* button is clicked, the revision of a Windows Group policy changes, causing the policies to be reprocessed.

Group Policy Caching

The last-processed Windows Group policy is cached locally. This helps reduce network traffic by processing Windows Group policies only if necessary. If UserA logs in on a new machine, his or her effective Group policies are processed and then cached.

If UserA logs out and UserB logs in, and if UserB has the same effective Group policies as UserA, the locally-cached Group policy is restored instead of reprocessing Windows Group policies. If the list of effective policies is different or if the revision is changed on any policy, the Windows Group policies are reprocessed.

New functionality has been added to the Desktop Management Windows Group policy implementation. The Windows Group policy settings in both the User Package and in the Workstation Package can remain in effect even when the workstation is disconnected from the network.

Persistent and Volatile Settings

The administrator determines if Windows Group policies are persistent or volatile. The persistent setting indicates that when the Windows Group policies are set, they remain set—even if a user happens to log in only to a workstation and not to the network.

The volatile setting indicates that the original local Windows Group policy settings will be restored when:

- The user logs out (the user Group policy settings are removed)
- The system shuts down (the workstation Group policy settings are removed)

Using Group Policies on Terminal Servers

You can configure Windows Group policies in a User Package for Windows 2000 and Windows 2003 Terminal Servers. You can also use the Windows 2000-2003 Terminal Server platform page if you want to set policies that apply to both platforms to make managing Terminal Servers easier.

When configuring Windows Group policies for Terminal Servers, consider the following:

- **Applied Settings Types:** Only the *User Configuration* settings under *Applied Settings Types* apply to Terminal Servers. The *Computer Configuration* and *Security Settings* options are not available for Terminal Servers.
- **Logoff Scripts:** Logoff scripts are not supported in a Terminal Server environment.

15.9.2 Configuring the Windows Group Policy in the User Package

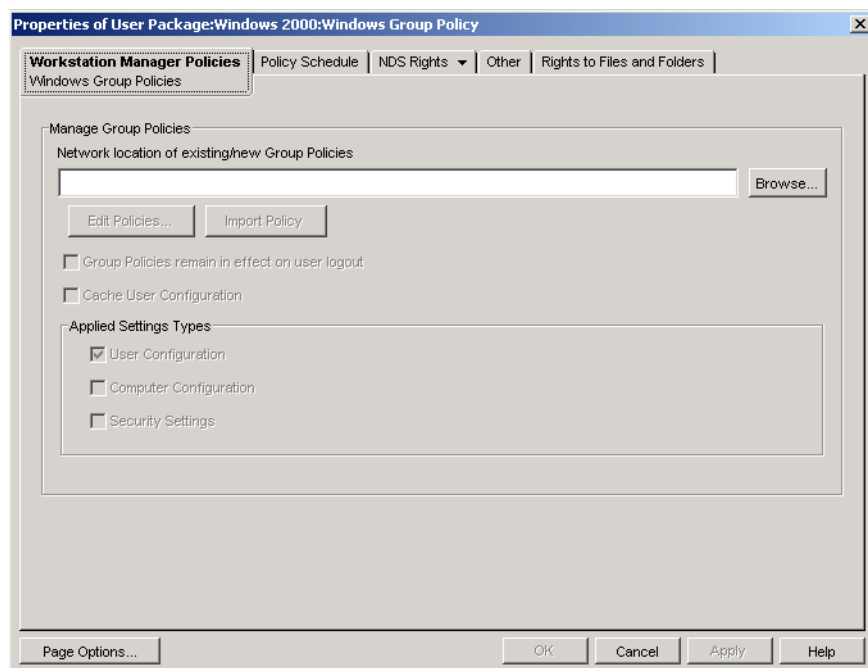
- 1 In ConsoleOne, right-click the User Package, click *Properties*, then click the appropriate **platform page**.

When choosing the appropriate platform page, take the following into account:

- **Windows NT:** For more information about Desktop Management support for the Windows NT platform, see “**Interoperability with Windows NT 4 Workstations**” in the *Novell ZENworks 7 Desktop Management Installation Guide*.
- **Windows NT-2000-XP platform page:** Because of the differences between Windows 2000 and Windows XP in regards to how security settings are saved, you cannot use the Windows NT-2000-XP platform page to edit the Windows Group policy. For Windows 2000, security settings are saved in the `gpptml.inf` file; for Windows XP, security settings are saved in the `xpsec.dat` file. Both files are located in the `\group policies\machine\microsoft\windows nt\secedit` directory.

In ZENworks 7, the *Edit* option on the Windows NT-2000-XP platform page has been disabled; you must use one of the specific platform pages to edit group policies.

- 2 Select the check box under the *Enabled* column for the Windows Group policy.
This both selects and enables the policy.
- 3 Click *Properties* to display the Windows Group Policies page.



- 4 Specify the network location for new or existing group policies.

Make sure that users have sufficient rights to access this network location.

If you use an environment variable in the *Network location of existing/new group policies* field, you must first set the environment variable on the management workstation on which you are running ConsoleOne and on any workstations that receive the group policy. You must also exit and restart ConsoleOne before the variable is recognized.

- 5 (Conditional) If you want to import group policies from Active Directory, click *Import Policy*.

For more information, see [Section 15.9.5, “Importing Windows Group Policies \(User and Workstation Packages\),” on page 202](#).

- 6 (Conditional) If you want to edit existing group policies, click *Edit Policies*.

For more information, see [Section 15.9.4, “Editing Existing Windows Group Policies \(User and Workstation Packages\),” on page 200](#).

- 7 (Optional) Select the *Group Policies remain in effect on user logout* check box to indicate that the pushed group policies remain in effect on the local Windows desktop after the user logs out.

IMPORTANT: We do not recommend using both the *Group policies remain in effect on user logout* settings and the *Cache User Configuration* settings in an environment in which the user Group policies are pushed to different users on common workstations.

- 8 (Optional) Select the *Cache User Configuration* check box.

Caching user configuration settings is different than enabling the *Group Policies remain in effect on user logout* check box.

Setting the *Group policies remain in effect on user logout* option enables the administrator to retain the group policy settings of the last logged-in user. The limitation with this approach is that any user who logs in locally (workstation only) receives the Group policy settings of the last person who logged in to the network on that workstation. If an administrator was the last user to log in to the network on a particular workstation, any subsequent local logins result in the user receiving the administrator's policy settings.

To avoid this situation, you can enable the *Cache User Configuration* check box to allow each user's settings to be cached.

Consider the following before you enable caching of settings in the User Package's Windows Group policy:

- The cache user settings functionality works with both NetWare or Windows on the back end. If you are using a Windows server on the back end, consider the following:
 - The user must be logged in with a local user account, not a cached domain account. Windows Group policy settings apply to domain accounts as long as the user is logging in to the domain. When the user does not log in to the domain, but uses a cached domain account, the Desktop Management Windows Group policy settings do not apply.
 - If you store Group policy files on an Active Directory server, the Active Directory username and password must match the eDirectory credentials.
- Users must have unique local user accounts. The Windows Group policy settings are cached in the local user's profile, so users with different effective Windows Group policies must have different local user accounts.
- Each user must have a profile on the machine in which to cache the settings. You can provide this profile by using local user accounts or by using Dynamic Local User (DLU)

accounts; however, the account cannot be removed. If the DLU policy removes the local user account (either by using a volatile user account or by using an expired cached volatile user account), the user cannot log in locally.

- Only the settings contained in the `\user\registry.pol` file are cached. This is roughly equivalent to the *User Settings* in the Group Policy editor with the exception of the logon/logoff scripts (they are stored in the Scripts folder under `\user`, and therefore not cached).

Selecting the *Cache User Configuration* check box causes the user configuration settings of each user's effective Windows Group policies to be stored in each user's local profile. When each user logs in locally, the user settings are read from the cached copy of the `registry.pol` in that user's profile and are applied. The only settings cached are those stored in the `registry.pol` file in the `\user` folder. Other settings are not cached, including logon/logoff scripts, computer settings, and security settings.

IMPORTANT: We do not recommend using both the *Group Policies remain in effect on user logout* settings and the *Cache User Configuration* settings in an environment in which the user Group policies are pushed to different users on common workstations.

- 9** In the *Applied Settings Types* group box, enable the desired options.

These options allow Windows user, computer, and security settings to be pushed with a User or Workstation policy. This differs from earlier releases in which user settings were pushed with User Packages and computer and security settings were pushed with Workstation Packages.

User Configuration: Select to push settings under *User Configuration* with the Windows Group policy.

Computer Configuration: Select to push settings under *Computer Configuration* (except *Security Settings*) with the Windows Group policy.

Security Settings: Select to push Windows security settings with the Windows Group policy. Selecting this option applies all security settings under *Computer Configuration > Windows Settings > Security Settings*, including *Account Policies*, *Local Policies*, *Public Key Policies*, and *IP Security Policies on Local Machine*. You cannot choose to push individual policies and policies are not additive.

Only the *User Configuration* settings under *Applied Settings Types* apply to Terminal Servers. The *Computer Configuration* and *Security Settings* options are not available for Terminal Servers.

- 10** Click the *Policy Schedule* tab > select a schedule type:

Package Schedule

Event

Daily

Weekly

Monthly

Yearly

You can click *Advanced Settings* to set additional settings such as *Completion*, *Fault*, *Impersonation*, *Priority*, and *Time Limit*. For detailed information on each of these settings, click the *Help* button on each page.

- 11** Click *OK* to save the policy.

- 12 When you have finished configuring all of the policies for this package, continue with the steps under [Section 15.13, “Associating the User or Workstation Package,” on page 207](#) to associate the policy package.

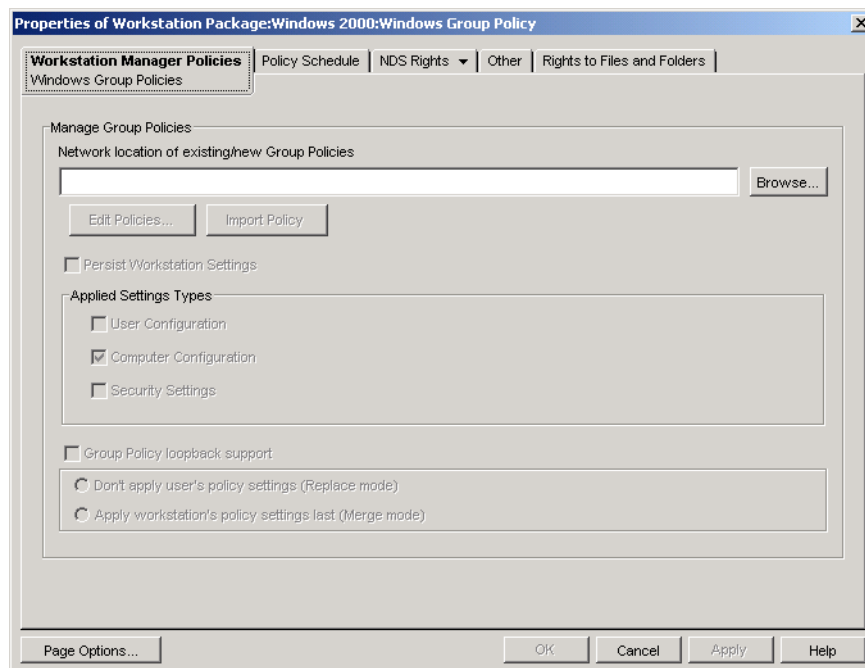
15.9.3 Configuring the Windows Group Policy in the Workstation Package

- 1 In ConsoleOne, right-click the Workstation Package, click *Properties*, then click the appropriate [platform page](#).

When choosing the appropriate platform page, take the following into account:

- **Windows NT:** For more information about Desktop Management support for the Windows NT platform, see “[Interoperability with Windows NT 4 Workstations](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.
- **Windows NT-2000-XP platform page:** Because of the differences between Windows 2000 and Windows XP in regards to how security settings are saved, you cannot use the Windows NT-2000-XP platform page to edit the Windows Group policy. For Windows 2000, security settings are saved in the `gphtml.inf` file; for Windows XP, security settings are saved in the `xpsec.dat` file. Both files are located in the `\group policies\machine\microsoft\windows nt\secdit` directory.
In ZENworks 7, the *Edit* option on the Windows NT-2000-XP platform page has been disabled; you must use one of the specific platform pages to edit group policies.

- 2 Select the check box under the *Enabled* column for the Windows Group policy.
This both selects and enables the policy.
- 3 Click *Properties* to display the Windows Group Policies page.



- 4 Specify the network location for new or existing group policies.
Make sure that users have sufficient rights to access this network location.

If you use an environment variable in the *Network location of existing/new Group Policies* field, you must first set the environment variable on the management workstation on which you are running ConsoleOne and on any workstations that receive the group policy. You must also exit and restart ConsoleOne before the variable is recognized.

- 5 (Conditional) If you want to import group policies from Active Directory, click *Import Policy*.

For more information, see [Section 15.9.5, “Importing Windows Group Policies \(User and Workstation Packages\),” on page 202.](#)

- 6 (Conditional) If you want to edit existing group policies, click *Edit Policies*.

For more information, see [Section 15.9.4, “Editing Existing Windows Group Policies \(User and Workstation Packages\),” on page 200.](#)

- 7 (Optional) Select the *Persist workstation settings* check box.

Selecting this option specifies that all workstation settings that Desktop Management supports (user, machine, and security settings) in the Workstation Package's Windows group policy can remain in effect (are cached) regardless of network connectivity.

Consider the following before you enable caching of settings in the Workstation Package's Windows group policy:

- The persistent workstation settings functionality works with both NetWare or Windows on the back end. If you are using a Windows server on the back end and you store Windows Group policy files on a Windows server, the workstation must be a member of that domain.
- In order to use persistent workstation settings, you cannot enable the *Group Policy LoopBack Support* option in the Windows Group policy associated to the workstations for which you want to cache settings (this includes either the *Replace Mode* or the *Merge Mode* options). By not enabling loopback support, the configuration in the user's policy always takes precedence over the configuration in the Workstation Package's Windows Group policy if conflicting settings exist.

Selecting the *Persist Workstation Settings* check box causes the workstation's effective Windows Group policy settings that are already stored in `windows_directory\system32\group_policy.wkscache` to be applied, even if that workstation is unable to log in to the network as the Workstation object (for example, when the workstation is disconnected from the network).

- 8 In the *Applied Settings Types* group box, enable the desired options.

These options allow Windows user, computer, and security settings to be pushed with a User or Workstation policy. This differs from earlier releases in which user settings were pushed with User Packages and computer and security settings were pushed with Workstation Packages.

User Configuration: Select this option to push settings under *User Configuration* with the Windows Group policy.

Computer Configuration: Select this option to push settings under *Computer Configuration* (except *Security Settings*) with the Windows Group policy.

Security Settings: Select this option to push Windows security settings with the Windows Group policy. Selecting this option applies all security settings under *Computer Configuration > Windows Settings > Security Settings*, including *Account Policies*, *Local Policies*, *Public Key Policies*, and *IP Security Policies on Local Machine*. You cannot choose to push individual policies and policies are not additive.

- 9 (Optional) Select the *Group Policy Loopback Support* check box, then select a mode.

Enabling this option gives precedence to Workstation Package policies over User Package policies. Loopback support has two modes, replace and merge:

Don't Apply User's Policy Settings (Replace Mode): Select this option to ignore all User policy settings; Workstation policy settings are applied.

Apply Workstation's Policy Settings Last (Merge Mode): Select this option to apply User policy settings first and then Workstation policy settings. This lets you apply user settings but override conflicting settings with workstation settings. If a user setting does not conflict, it remains in effect.

- 10 Click the *Policy Schedule* tab > select a schedule type:

Package Schedule

Event

Daily

Weekly

Monthly

Yearly

Because the Windows desktop files finish loading before group policy settings are loaded, some group policies in the Workstation Package might exhibit odd behavior if they are scheduled to run at user login. Specifically, any changes to desktop settings (for example, hide My Network Place, hide all icons on desktop, etc.) do not occur, and programs won't run if you have scheduled them to run at user login through use of a login script. If the user logs off and back on, the settings display correctly.

To prevent this behavior, do not configure group policies in the Workstation Package to run at user login. Instead, configure them to run at system startup, on a daily basis, or on some other regular schedule.

If you configure group policies to run startup scripts and you schedule those policies to run at system startup, you should select the *Persist Workstation Settings* option in [Step 7 on page 199](#). Because Windows 2000/XP looks for and runs startup scripts before Workstation Manager authenticates and applies policies, group policies that you configure to run startup scripts might fail to run when scheduled to run at system startup. If you select the *Persist Workstation Settings* option, the Workstation Package group policy settings (and startup scripts) are cached and can be applied correctly at the next system startup.

You can click *Advanced Settings* to set additional settings such as *Completion*, *Fault*, *Impersonation*, *Priority*, and *Time Limit*. For detailed information on each of these settings, click the *Help* button on each page.

- 11 Click *OK* to save the policy.
- 12 When you have finished configuring all of the policies for this package, continue with the steps under [Section 15.13, "Associating the User or Workstation Package," on page 207](#) to associate the policy package.

15.9.4 Editing Existing Windows Group Policies (User and Workstation Packages)

- 1 In ConsoleOne, right-click the User or Workstation Package, click *Properties*, then click the appropriate [platform page](#).
- 2 Select the check box under the *Enabled* column for the Windows Group policy.

This both selects and enables the policy.

- 3 Click *Properties* to display the Windows Group Policies page.
- 4 Specify the network location for new or existing group policies.
- 5 Click *Edit Policies*.

When you click the *Edit Policies* button, the Microsoft Management Console editor is launched, where you can edit a User Package policy or a Workstation Package policy. For more information, click *Help* in the dialog boxes. After you have finished editing the policy, click the *Close* button.

When you edit group policies, be aware of the following:

- **Directory Path:** Make sure you have selected the correct directory path because you could destroy data. All of the files in the selected directory as well as the `\adm`, `\user`, and `\machine` subdirectories are deleted before the Active Directory group policy is copied to it.

NOTE: If the Network Location of Existing/New Group Policies path is set to a Linux file server, permission must be set from a Linux machine to allow read rights for users and workstations.

- **Security Settings that Cannot be Edited in Windows XP:** Because of changes in Windows XP, you cannot currently edit the following Windows XP Security settings using Desktop Management:
 - Under *Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy*:
Password Must Meet Complexity Requirements
Store Password Using Reversible Encryption
 - Under *Security Settings > Local Policies > Security Options*:
Network Access: Allow Anonymous SID/Name Translation
Accounts: Administrator Account Status
Accounts: Guest Account Status
- **Operating System Version and Service Pack Level Checking in ZENworks 7:** New functionality has been added to ZENworks 7 to check the operating system version and service pack level while editing group policies on all platforms on which you can edit group policies (Windows 2000, Windows XP, and Windows Server 2003). For example, if a group policy was created on a Windows XP SP1 or earlier workstation and you attempt to edit it on a Windows XP SP2 workstation, ZENworks displays a warning dialog box. ZENworks also prohibits you from editing a group policy that was created on a Windows XP SP2 workstation if you are using a workstation with either Windows XP or Windows XP SP1 installed.
- **Disabling Group Policy Settings using ZENworks 7:** In ZENworks 7, new functionality has been included to let you disable certain group policy settings without preventing future editing of the policy.

In previous versions of ZENworks, disabling certain settings disabled the group policy editor, preventing you from editing that policy in the future. These settings include the following (depending on the OS and service pack level, not all settings might be present):

- Under *User Configuration > Administrative Templates > Windows Components > Microsoft Management Console*:

Restrict the user from entering author mode
Restrict users to the explicitly permitted list of snap-ins

- Under *User Configuration > Administrative Templates > Windows Components > Microsoft Management Console > Restricted/Permitted Snap-ins > Group Policy*:
Group Policy Management
Group Policy Object Editor
- Under *User Configuration > Administrative Templates > Windows Components > Microsoft Management Console > Restricted/Permitted Snap-ins > Group Policy > Group Policy snap-in extensions*:
Administrative Templates (Computers)
Administrative Templates (Users)
Folder Redirection
Internet Explorer Maintenance
Remote Installation Services
Scripts (Logon/Logoff)
Scripts (Startup/Shutdown)
Security Settings
Software Installation (Computers)
Software Installation (Users)
Wireless network (IEEE 802.11) Policies

If you disable any of these settings and then attempt to edit the policy, an error message displays stating that the snap-in has been restricted by policy. In addition, the group policy editor does not open.

To avoid this problem in ZENworks 7, these settings are removed from the group policy and saved in a temporary local location. When you close the editor, the settings in the temporary file are merged with the settings in the newly configured group policy. If you made any changes to these settings while using the editor and they conflict with those settings that were saved in the temporary file, the new settings take precedence over the original settings that were moved to the temporary file.

- 6 Click *OK* to save the policy.

15.9.5 Importing Windows Group Policies (User and Workstation Packages)

- 1 In ConsoleOne, right-click the User or Workstation Package, click *Properties*, then click the appropriate **platform page**.
- 2 Select the check box under the *Enabled* column for the Windows Group policy.
This both selects and enables the policy.
- 3 Click *Properties* to display the Windows Group Policies page.
- 4 Specify the network location for new or existing group policies.
- 5 If you want to import group policies from Active Directory, click *Import Policy*, then fill in the fields.
 - 5a Select an import option:

Import Whole Active Directory Folder: Lets you import all group policies in the Active Directory folder. If you select this option, use the *Source Location* field to specify the UNC path to the folder containing group policies created by Active Directory that you

want to migrate to the directory listed in the *Destination location of migrated group policies* field. You must know or browse for the Unique Name of the directory from where you import the Active Directory group policy. You can find the Unique Name by examining the properties of the Active Directory Group policy.

Import Security Settings: Lets you import security settings from a file. If you select this option, use the *Source Location* field to specify the UNC path to the file containing the security settings created by Active Directory that you want to migrate to the directory listed in the *Destination location of migrated group policies* field. You must know or browse for the Unique Name of the file that you import into the group policy.

Imported security settings let administrators set only certain security settings without affecting all remaining security settings. Security settings can be imported from an Active Directory Group policy or can be created with the Security Templates snap-in in the Microsoft Management Console (MMC). For more information, see “[Creating Security Settings Using the Security Templates Snap-In in the Microsoft Management Console \(MMC\)](#)” on page 203.

When you import an Active Directory Group policy containing security settings or import a security settings file, the imported settings are saved in a new file called `zensec.inf`.

The security settings in `zensec.inf` are used instead of the regular security settings displayed when editing the Group policy in MMC. The security settings shown in MMC are not accurate and any changes made are not applied. If imported security settings are detected while editing a Group policy, a message box informs the user that the security settings in `zensec.inf` will be used in place of the regular security settings and give the user the option of displaying the settings in the `zensec.inf` file.

IMPORTANT: You should use UNC paths rather than mapped drives for group policies.

5b Click *Import*.

This copies the Active Directory group policy or file to the directory specified in the Destination Location of Migrated Group Policies field. If the specified directory does not exist, it is created.

WARNING: Make sure you have selected the correct directory path in the Destination Location of Migrated Group Policies field because you could destroy data. All of the files in the selected directory as well as the `\adm`, `\user`, and `\machine` subdirectories are deleted before the Active Directory group policy is copied to it.

6 Click *OK* to save the policy.

Creating Security Settings Using the Security Templates Snap-In in the Microsoft Management Console (MMC)

We recommend that you create new security settings rather than editing existing settings in the MMC. If you edit existing security settings, they might contain default settings that you do not need and might take a significant amount of time to process. You can avoid this problem by generating new settings.

NOTE: You must be logged on as an administrator or a member of the Administrators group to create security templates. Network policy settings might also prevent you from creating security templates.

To create new security settings using the Security Templates snap-in:

- 1 Click the *Start* button, then click *Run*.
- 2 Type `mmc`, then click *OK*.
- 3 Click *File > Add/Remove Snap-in* to display the Add/Remove Snap-in dialog box.
- 4 In the Standalone page, click *Add*.
- 5 In the Add Standalone Snap-in dialog box, click *Security Templates*, click *Add*, then click *Close* to close the Add Standalone Snap-in dialog box.
- 6 In the Add Remove Snap-in dialog box, click *OK*.
- 7 (Optional) In the console tree, right-click Security Templates, click *New Template Search Path*, then select the new location.
A folder with the path of the new location appears in the console tree.
- 8 Right-click the folder where you want to store the new template, then click *New Template*.
- 9 Type a template name and description, then click *OK*.
- 10 In the console tree, double-click the new security template to display the security areas and navigate until the security setting you want to configure is in the right pane.
- 11 Double-click the security setting you want to configure, select the *Define This Policy* setting in the *Template* check box, edit the settings, then click *OK*.

15.10 Workstation Imaging Policy (Workstation Package)

Sets the parameters for imaging workstations. This policy is found on each of the platform pages. For general imaging information, see [Part VI, “Workstation and Server Imaging,” on page 623](#).

The setup procedure that is applicable to you depends on your imaging deployment strategy. For more information, see [Chapter 58, “Setting Up Imaging Policies,” on page 697](#).

15.11 Workstation Inventory Policy (Workstation Package)

Sets what hardware and software inventory data you want to view for each workstation. For more detailed information, see [Part VIII, “Workstation Inventory,” on page 871](#).

15.12 ZENworks Desktop Management Agent Policy (Workstation Package)

The ZENworks Desktop Management Agent policy lets you configure the Desktop Management Agent, which lets you use Desktop Management without using the Novell Client. The Desktop Management Agent lets users access the Desktop Management Middle Tier server using a DNS name or IP address. In order to use the ZENworks Desktop Management Agent policy, you must have the Desktop Management Agents installed; you cannot use this policy in an environment that has only the Novell Client installed. For more information, see [Part I, “Understanding ZENworks 7 Desktop Management,” on page 31](#).

To set up the ZENworks Desktop Management Agent policy:

- 1 In ConsoleOne, right-click the Workstation Package, click *Properties*, then click the appropriate **platform page**.

For more information about Desktop Management support for the Windows NT platform, see “**Interoperability with Windows NT 4 Workstations**” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

- 2 Select the check box under the *Enabled* column for the ZENworks Desktop Management Agent policy.

This both selects and enables the policy.

- 3 Click *Properties* to display the Settings page.

The screenshot shows the 'Properties of Workstation Package: General: ZENworks Desktop Management Agent' dialog box. The 'Settings' tab is active. The 'Global Settings' section has an unchecked checkbox for 'Apply Middle Tier Address' and a text field for 'DNS name or IP address of the ZENworks Middle Tier Server'. The 'Workstation Manager Specific Settings' section has a spin box for 'eDirectory Refresh Rate (Minutes)' set to 1380. The 'Login Settings' section has an unchecked checkbox for 'Display ZENworks authentication dialog (Note: Client32 login displayed if installed)', an unchecked checkbox for 'Allow users to change ZENworks Middle Tier server address on authentication dialog', and three empty text fields for 'Resident workstation welcome bitmap', 'Welcome caption', and 'Login window bitmap'. The 'Dynamic Local User Policy Settings' section has an unchecked checkbox for 'Enable Volatile User cache' and a spin box for 'Cache Volatile User time period (Days)' set to 5. At the bottom are buttons for 'Page Options...', 'OK', 'Cancel', 'Apply', and 'Help'.

- 4 Select the *Apply Middle Tier address* check box, then fill in the fields:

DNS Name or IP Address of the ZENworks Management Middle Tier Server: Specify the DNS name or IP address of the Middle Tier Server.

The DNS name or IP address you specify in this location identifies the access point that all Desktop Management components (Workstation Inventory, Workstation Management, Application Management, and Remote Management) use to function outside of the firewall.

Only non-blank values are passed on to the associated workstations. If you leave the *DNS name or IP address of the Middle Tier Server* field blank, this setting is not affected on the associated workstations.

If you change the DNS name or IP address in this location, this setting is applied to all associated workstations the next time they start up. Therefore, in a clientless environment, be sure to provide adequate time for associated workstations to transition to the new DNS name or IP address before removing access to the previous location.

eDirectory Refresh Rate (Minutes): Use the arrows to set the refresh rate for eDirectory. The rate you set determines how often the agent looks for updated information in eDirectory, such as new or edited policies.

Display ZENworks Authentication Dialog: Select this check box if you want the ZENworks authentication dialog box to display during startup.

Allow Users to Change ZENworks Middle Tier Server Address on Authentication Dialog: Select this check box if you want to allow users to change the Middle Tier Server address to point to another Middle Tier Server. If this box is selected, users can click the *Options* button in the ZENworks authentication dialog box and specify another Middle Tier server's address.

Resident Workstation Welcome Bitmap: Specify the name of the bitmap file that appears on the welcome screen when you start Windows NT/2000/XP. You can specify any file located in the associated workstations' Windows NT/2000/XP directory. You can also leave this field blank if you do not want to use a bitmap.

Welcome Caption: Specify the text that appears in the header on the welcome screen when you start Windows NT/2000/XP.

Login Window Bitmap: Specify the name of the bitmap file that appears in the login window. You can specify any file located in the associated workstations' Windows NT/2000/XP directory. You can also leave this field blank if you do not want to use a bitmap.

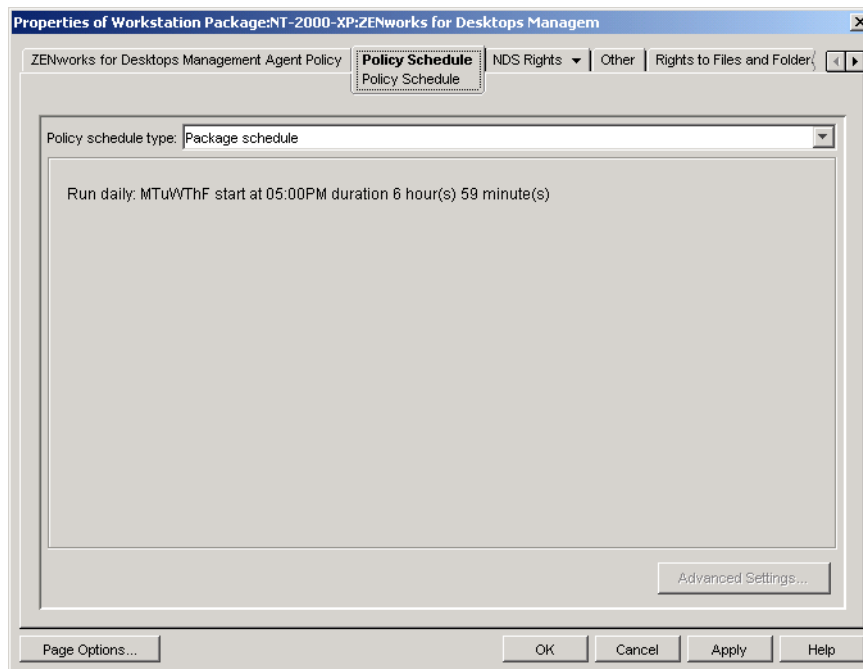
Enable Volatile User Cache: Select this check box to enable the volatile user cache. This option allows for volatile user information that has previously been cached on a workstation to remain on the workstation for a specified period. Therefore, volatile users are not created or removed at every login or logout. This promotes faster logins for volatile users because NWGINA does not need to spend cycles re-creating the user desktop.

The Dynamic Local User (DLU) policy settings configure users created on Windows NT/2000/XP workstations after they have authenticated to eDirectory.

The cache makes it possible for a user to continue using the workstation even when the workstation is disconnected from the network and the user is not a registered user on the workstation.

Cache Volatile User Time Period (Days): Use the arrows to select how often you want to remove volatile user information. When the time limit expires and if the user has not authenticated to eDirectory within the specified time period, all volatile user information is removed from the workstation. However, if the user authenticates to eDirectory within the specified time period, the countdown begins again according to the number of days you specify using this option.

5 Click the *Policy Schedule* tab.



6 Select a schedule type:

Package Schedule

Event

Daily

Weekly

Monthly

Yearly

Click the *Help* button on the Schedule tab for more information about each schedule.

7 Click *OK* to save the policy.

8 Repeat **Step 1** through **Step 7** for each platform where you want to set a ZENworks Desktop Management Agent policy.

9 When you have finished configuring all of the policies for this package, continue with the steps under **Section 15.13, “Associating the User or Workstation Package,” on page 207** to associate the policy package.

15.13 Associating the User or Workstation Package

The policies you configured and enabled are not in effect until you associate their policy package with a container object.

1 In ConsoleOne, right-click the User Package or Workstation Package, then click *Properties*.

2 Click the *Associations* tab > *Add*.

- 3** Browse for and select the container, group, user, or workstation object for associating the package, then click *OK*.

Generating Policy Reports

16

Novell® ZENworks® 7 Desktop Management provides two predefined reports through ConsoleOne® for effective policies and policy package associations.

You can run either report based on a selected container, and you can include its subcontainers.

Report results are automatically displayed in Notepad and are saved as text files in the `\temp` directory of the workstation where you are running ConsoleOne.

The following sections provide information on Desktop Management reporting:

- [Section 16.1, “The Effective Policies Report,” on page 209](#)
- [Section 16.2, “The Package Associations Report,” on page 209](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

16.1 The Effective Policies Report

The Effective Policies report shows which policies are currently in effect for the listed objects. It provides the following information:

Version
Tree
Container
Object DN
Platform
Effective Policy DN

To run a report on the effective policies:

- 1 In ConsoleOne, click *Tools > ZENworks Utilities > Report Policies and Packages*.
- 2 In the *Report From* field, browse for a context for the report.
- 3 To include all subcontainers in that context, click *Include Subcontainers*.
- 4 Click *Effective Policies Report*, then click *OK*.

The report results are displayed in Notepad and are automatically saved to `\temp\effectivepolicies.txt` on the user's workstation.

16.2 The Package Associations Report

The Package Associations report shows which policy packages are associated with the listed containers, subcontainers, and objects. It provides the following information:

Tree
Container
Package DN

Association

To run a report on policy package associations:

- 1** In ConsoleOne, click *Tools > ZENworks Utilities > Report Policies and Packages*.
- 2** In the *Report From* field, browse for a context for the report.
- 3** To include all subcontainers in that context, click *Include Subcontainers*.
- 4** Click *Package Association Report*, then click *OK*.

The report results are displayed in Notepad and are automatically saved to `\temp\packageassociations.txt` on the user's workstation.

Copying Policy Packages

17

Novell® ZENworks® 7 Desktop Management provides a utility to help you copy policy packages from one directory container to another. You can run the Copy Policy Packages utility via a ConsoleOne® snap-in or you can use a version of the utility based on Windows.

The following sections contain step-by-step instructions to help you run the Copy Policy Packages utility:

- [Section 17.1, “Using the ConsoleOne Copy Policy Packages Utility,” on page 211](#)
- [Section 17.2, “Using the Windows Copy Policy Packages Utility,” on page 211](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

17.1 Using the ConsoleOne Copy Policy Packages Utility

The Copy Policy Packages utility can be run via a ConsoleOne snap-in. The snap-in consists of the `zencopypol.jar` and `zencopypolreg.jar` files.

To run the Copy Policy Packages utility from ConsoleOne:

- 1 In ConsoleOne, click *Tools > ZENworks Utilities > Copy Policy Packages*.
- 2 Browse to and select a policy package or container that contains policy packages.
- 3 Browse to and select a container where you want to copy this policy package.
- 4 Click *Add* to add the container to the *Selected Container* list.
To copy the policy package or container to multiple containers, repeat [Step 3](#) and [Step 4](#).
- 5 Click *OK*.

17.2 Using the Windows Copy Policy Packages Utility

The Windows-based Copy Policy Packages utility is found in the `windows_drive\sys\public\mgmt\consoleone\1.2\bin` directory.

To run the Copy Policy Packages utility from Windows:

- 1 Double-click `copypol.exe`.
- 2 Specify the name of a policy package or container that contains policy packages that you want to copy from one Novell eDirectory™ container to another.
- 3 Specify a container name.
- 4 Click *Add* to add the container name to the *Selected Container* list.
To copy the policy package or container to multiple containers, repeat [Step 3](#) and [Step 4](#).
- 5 Click *OK*.

The Windows-based Copy Policy Packages utility can also run from the Windows command line. You can copy a policy package from one container to another or you can copy all of the policy packages from one container to another container.

To copy a policy package from one container to another, use the following syntax:

```
copypol policy_package_DN /d destination_container
```

To copy all of the policy packages from one container to a different container, use the following syntax:

```
copypol container_DN /d destination_container
```

You can use the following command line switches:

Table 17-1 *List of Command Line Switches for Use with the Windows Copy Policy Packages Utility*

Switch	Description
/d	Specifies the destination container where the policy packages will be copied
/h	Runs the Copy Policy Packages utility in hidden mode
/r	Replaces the policy package in the destination container if a policy package with the same name already exists in that container
/t	Specifies the tree to copy the policy packages to
/v	Lets you view a log file to verify the results of the copy process

The Novell® ZENworks® 7 Desktop Management Scheduler allows you to set up different actions to run on a workstation. You can run actions on a workstation using policies or manually using the Scheduler. In previous versions of ZENworks for Desktops, the Scheduler was available on the Windows taskbar. Because many system administrators do not want users to be able to access the Scheduler, it is no longer displayed in the taskbar. The Scheduler (`wmsched.exe`), however, is installed as part of the Workstation Client installation.

This section contains the following topics to help you understand and use the workstation Scheduler manually; for further information on how to manage the workstation scheduler using policies, see [Section 15.6, “Scheduled Action Policy \(User and Workstation Packages\),” on page 187](#):

- [Section 18.1, “Understanding Workstation Scheduler,” on page 213](#)
- [Section 18.2, “Using Workstation Scheduler,” on page 214](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

18.1 Understanding Workstation Scheduler

This section contains the following topics:

- [“Actions” on page 213](#)
- [“Rights for Running Actions” on page 214](#)
- [“Using the Scheduler in Windows 2000/XP” on page 214](#)
- [“Microsoft SAGE Compatibility” on page 214](#)

18.1.1 Actions

An action is an object that contains a list of one or more action items (for example, `.exe` files `.dll` files, ActiveX*, and JavaScript*). The action applies only to the workstation from which you are running the workstation Scheduler.

Actions and action items can be given a priority, allowing you to specify which action or action item should run first, second, and so forth. You can also schedule actions to automatically run when a workstation event occurs or periodically at a certain time.

You determine the amount of time each action or action item has to complete. If the action cannot occur at the specified time, you can indicate whether to discontinue it, retry it every minute, or have it rescheduled.

If the action does not complete within a specified amount of time, you can indicate that the action should be terminated. If the action does complete successfully, you can indicate that the action should not be run again.

You can also specify if an action should dial a number before any action item runs.

If you have the necessary rights, you can view and edit details or properties associated with an action. You can also delete an action, disable or enable an action, or run an action immediately even if it was scheduled to run at a later date or time or upon the occurrence of a given event.

You can remove, disable or enable, reorder, and view or modify properties associated with action items.

18.1.2 Rights for Running Actions

For actions to have the proper rights to modify the workstation's environment, you must have the appropriate workstation access rights.

18.1.3 Using the Scheduler in Windows 2000/XP

In Windows 2000/XP, a user does not need to be logged in to the workstation or the network for the action to happen. The action takes place even when no one is at the workstation. However, the workstation must be powered on for the action to occur. If the workstation is not on when an action starts, Scheduler reschedules the action within a block of time called the startup block of time. If the workstation is not turned on within this time, you can indicate that the action be retried every minute, rescheduled to occur during the next interval, or dropped.

18.1.4 Microsoft SAGE Compatibility

The Scheduler is compatible with Microsoft SAGE for Windows 98 and can run SAGE-aware programs.

18.2 Using Workstation Scheduler

This section contains the following topics:

- “Adding an Action” on page 214
- “Adding an Action Item” on page 216
- “Disabling or Enabling an Action” on page 217
- “Disabling or Enabling an Action Item” on page 217
- “Removing an Action” on page 217
- “Removing an Action Item” on page 217
- “Running an Action Immediately” on page 217
- “Scheduling an Action to Run” on page 218
- “Setting Advanced Action Properties” on page 220
- “Viewing or Editing the Details or Properties of an Action” on page 220
- “Viewing or Editing the Details or Properties of an Action Item” on page 220
- “Viewing or Editing User-Defined Action Item Properties” on page 221

18.2.1 Adding an Action

Setting up an action item requires that you add the action item to the list of action items. The network administrator (or other user with the Supervisor right) can do this in ConsoleOne® and then

push the action item to one or more user workstations. Users can also set up action items to run on their individual workstations by using the workstation Scheduler.

- 1 Load the Scheduler (run `wmsched.exe`).
- 2 Click *Add* to display the Action Properties dialog box.
- 3 On the General page, fill in the fields:

Name: The name of the action. In ConsoleOne, the name includes the action object's full context. In the workstation Scheduler, the name is whatever you enter in this field.

Priority: The order in which the action is run. Higher priority actions run first. If two actions have the same priority, the first one encountered in the action list (contained in the window that is first displayed when the Scheduler is loaded) runs first. The priority selected applies to all action items contained in this action, unless the action item overrides it.

Impersonation: The workstation access rights to grant to all action items contained by this action. (Windows NT/2000/XP only.)

Action Remains Persistent after Reboot: The action is saved to the workstation, allowing the Scheduler to reactivate the action at the appointed time when the workstation is rebooted. If this option is not selected, the action is lost when you exit Windows NT/2000/XP.

- 4 On the Actions page, click *Add*.
- 5 In the Item Properties dialog box, fill in the fields:

Name: Specify the name of the program to run. This program must exist on the user's path to be run as an action item.

Working Directory: The working directory is automatically set when you specify an action item. It is set to the directory that the action item is in. You can specify a different working directory by entering the path in this field.

Parameters: The information the system can use for command line arguments to be sent to the application. For example, if you want to launch `notepad.exe` and have it automatically open the `readme.txt` file, put `readme.txt` in the Parameters field.

Priority: Both actions and action items have four priorities available: *Action Default*, *Above Normal*, *Normal*, and *Below Normal*. Action items can assume the same priority as the Action object that contains them; in other words, they take on the action's default priority. Alternatively, they can override the default by using one of the three other priority settings.

If the action occurs during normal business hours, it should be assigned a *Below Normal* priority so it does not affect the user's workstation performance.

If two or more actions or action items have the same priority, the first one defined (the one that appears first in the list) has precedence over the others.

- 6 Select the *Terminate action if still running after ? minutes* check box, then select the desired number of minutes.

This option terminates the action if it is still running after the number of minutes you specify. The action is then rescheduled to run at the next scheduled time.

The number of minutes you specify in the *Minutes* field should be the total time required by the action itself as well as by all action items associated with the action, where applicable. If you do not specify sufficient time for the action and all associated action items to run, your action items might not have enough time to complete their tasks.

- 7 Click *OK* twice.

The action is added to the *Action* list on the Scheduler. You can now do any of the following:

- Specify when this action should take place (Schedule page).
- Add items to this action (Items page).
- Specify what happens if this action cannot occur (Advanced page).

18.2.2 Adding an Action Item

This process assumes that you have previously created an action to contain the action items. If you have not yet created an action, see [“Adding an Action” on page 214](#).

- 1 In the Scheduler, select an action, click *Properties*, click *Items*, then click *Add*.
- 2 In the Item Properties dialog box, fill in the fields:

Name: Browse to or enter the name of the program to run. This program must exist on the user's path to run as an action item.

Working Directory: The working directory is automatically set when you browse for an action item. It is set to the directory that the action item is in. You can specify a different working directory by providing the path in this field.

The *Working Directory* field must specify a local device. Network paths cannot be used as working directories.

Parameters: The information the system can use for command line arguments to be sent to the application. For example, if you want to launch `notepad.exe` and have it automatically open the `readme.txt` file, put `readme.txt` in the *Parameters* field.

If you are adding an action item that is a DOS batch file, a DOS window must be opened to run it. The DOS window closes when the batch file has finished running if you include the `/c` parameter. You must add the `/c` parameter, followed by a space, in front of the name of the batch file in the *Parameters* field.

For example, to run a DOS batch file called `test_c.bat`, make the following entries in the Item Properties dialog box for the action item when you add the action item:

- *Name:* `CMD.exe` (the name of the Windows NT/2000/XP command that opens a DOS window) or `START` (the name of the Windows 98 command that opens a DOS window).
- *Working Directory:* Leave this field blank unless you need to specify where either `cmd.exe` or `start` is located.
- *Parameters:* `/c test_c.bat`. You must include the full filename with its extension, and you must use the `/c` parameter if you want the DOS window to close as soon as the batch file has finished running.
- *Priority:* Leave at Action Default, or choose one of the other settings.

Priority: Both actions and action items have four priorities available: *Action Default*, *Above Normal*, *Normal*, and *Below Normal*. Action items can assume the same priority as the Action object that contains them; in other words, they take on the action's default priority. Alternatively, they can override the default by using one of the three other priority settings.

If the action occurs during normal business hours, it should be assigned a *Below Normal* priority so it does not affect the user's workstation performance.

If two or more actions or action items have the same priority, the first one defined (the one that appears first in the list) has precedence over the others.

- 3 Select the *terminate action if still running after ? minutes* check box, then select the desired number of minutes.

This option terminates the action if it is still running after the number of minutes you specify. The action is then rescheduled to run at the next scheduled time.

The number of minutes you specify in the *Minutes* field should be the total time required by the action itself as well as by all action items associated with the action, where applicable. If you do not specify sufficient time for the action and all associated action items to run, your action items might not have enough time to complete their tasks.

- 4 To save the settings and continue editing the action, click *Apply*.

or

When you are done with the action item's properties, click *OK*.

The action item now appears in the *Action item* list.

If any action items are scheduled to run now and you click *OK* or *Apply*, they run.

- 5 Repeat **Step 2** through **Step 4** until you have finished adding items.

18.2.3 Disabling or Enabling an Action

- 1 Load the Scheduler (run `wmsched.exe`).
- 2 Click an action.
- 3 Click *Enable/Disable*.

18.2.4 Disabling or Enabling an Action Item

- 1 Load the Scheduler (run `wmsched.exe`).
- 2 Click an action, then click *Properties*.
- 3 Click the *Items* page, select an action item, then click *Disable/Enable*.

18.2.5 Removing an Action

This procedure cannot be undone. When you click *Remove*, you are not prompted to verify the removal of the action. If you remove an action that you need later, you must add it again.

- 1 Click an action.
- 2 Click *Remove*.

18.2.6 Removing an Action Item

This procedure cannot be undone. When you click *Remove*, you are not prompted to verify the removal of the action item. If you remove an action item that you need later, you must add it again.

- 1 Click an action, then click *Properties*.
- 2 Click *Items*, select an action item, then click *Remove*.

18.2.7 Running an Action Immediately

- 1 Click an Action.

- 2 Click *Run Now*.

18.2.8 Scheduling an Action to Run

Use the fields on the Schedule page to specify when the action should run and to provide details that the system needs about when the action runs.

The Schedule page contains five scheduling options: *Event*, *Daily*, *Weekly*, *Monthly*, and *Yearly*. The option you choose and the settings you associate with it determine when the action is run.

You can use only one scheduling option at a time. For example, if the *Daily* option is selected, all other options are ignored unless you use the options found on the *Advanced* tab.

Time units are shown according to a 24-hour clock (for example, 9:00 for 9 a.m. and 13:30 for 1:30 p.m.).

The Scheduler ignores the scheduling information until the action can be started successfully.

To schedule an item:

- 1 Select the action you want to schedule.
- 2 Click *Properties > Schedule*.
- 3 Select the desired scheduling option:
 - **Event:** Event scheduling allows you to determine what kind of workstation event causes your action to run. To schedule the action based on an event, click *Event* and choose from the following list of recognized events:
 - Scheduler Service Startup:** Runs the action when the Scheduler starts up. You cannot choose the *Scheduler Service Startup* event to start the action if you are going to run the action with the rights of an interactive user. When these events take place, the interactive user is not yet authenticated. *Scheduler Service Startup* requires System rights.
 - User Login:** Runs the action after the user has successfully logged in but before the login scripts are executed.
 - User Desktop Is Active:** Runs the action after the login scripts have completed (does not apply to Windows 98).
 - Workstation Is Locked:** Runs the action when the workstation is locked (does not apply to Windows 98).
 - Workstation Is Unlocked:** Runs the action when the workstation is unlocked (does not apply to Windows 98).
 - Screen Saver Is Activated:** Runs the action when the screen saver is activated.
 - User Logout:** Runs the action before logout is completed.
 - System Shutdown:** Runs the action after all other applications have successfully closed, but before the system shuts down. You cannot choose the *System Shutdown* event to start the action if you are going to run the action with the rights of an interactive user. When these events take place, the interactive user is no longer authenticated. *System Shutdown* requires System rights.
 - **Daily:** Lets you schedule an action to occur on one or more days between the specified start and end times. Optionally, it allows you to repeat the action at regular intervals after the action successfully starts. For example, on Monday, Wednesday, and Friday, you

could start the action between 12:30 and 13:00 and run it every 10 minutes. To schedule the action based on a daily basis, click *Daily* and choose from the following options:

Run this Action on the Following Days: Specify the days of the week when the action is to run.

Start the Action Between the Hours of ? (HH:MM): Specify a range of time within which this action can be started.

Repeat the Action Every ? (HH:MM:SS): Specify the length of time the system is to wait before it repeats this action.

- **Weekly:** Lets you schedule an action on a particular day of the week. To schedule an action on a weekly basis, click *Weekly* and choose from the following options:

Run this Action Once a Week On: Identifies day of the week when you want the action to run.

Start this Action Between the Hours of ? (HH:MM): Identifies the exact hour (HH) and minute (MM) to start this action.

- **Monthly:** Lets you choose the day of the month when this action runs, as well as the time to start this action. For example, you can choose to run this action on every fourth day of the month, between the hours of 8:00 and 10:15. You specify the time range using a 24-hour clock. If you prefer, you can choose to have the action run on the last day of the month, regardless of how many days there are in the month. To schedule the action on a monthly basis, click *Monthly* and choose from the following options:

Run this Action Once a Month on Day __ of the Month: Specify the day of the month on which the system is to automatically run this action. Click one of the available option buttons:

- **On Day _ of the Month:** This action runs on the specified day.
- **On the Last Day of the Month:** This action runs on the last day of the month regardless of how many days there are in the month.

Start this Action Between the Hours of ? (HH:MM): Specify the exact hour (HH) and minute (MM) this action is to start.

- **Yearly:** Lets you determine the time and the day of the month to perform the action. To schedule the action on a yearly basis, click *Yearly* and choose from the following options:

Run the Action Once a Year on Day ? of ?: Specify the day of the month and the month of the year for the action to run.

Start the Action between the Hours of ? and ?: Using a 24-hour clock, specify the hour and minute of the earliest time this action is to be started, and then the hour and minute of the latest time this action is to be started. For example, choose 17:30 to begin the action no earlier than 5:30 p.m. and 20:00 to begin the action no later than 8:00 p.m.

4 Click *OK*.

The schedule you define applies to every action item contained in the action and overrides the package schedule.

18.2.9 Setting Advanced Action Properties

Use the fields on the Advanced page to determine what happens to the action's schedule if it did not complete or run within the given time, or when it successfully completes.

- 1 Click an action > *Properties* > *Advanced*.
- 2 Specify what should happen if the system cannot run the action:
 - **Disable the Action:** Disables the action so it does not run again (unless you enable it again).
 - **Retry Every Minute:** Causes the system to keep trying to run this action every 60 seconds.
 - **Ignore the Error and Reschedule Normally:** Causes any error that occurred while the action was running to be ignored and the action to be rescheduled for a later date/time.
- 3 Select the *Disable the action after completion* check box to disable the rescheduling mechanism for this action after all action items have started successfully.
- 4 Select the *Terminate action if still running after ? minutes* check box, then select the number of minutes.

This feature terminates the action if it is still running after the number of minutes you specify. The action is then rescheduled to run at the next scheduled time.

To set a time limit on how long the action should run, select the check box. The number of minutes that you specify in the *Minutes* field should be the total time required by the action itself as well as by all action items associated with the action, where applicable. If you do not specify sufficient time for the action and all associated action items to run, your action items might not have enough time to complete their tasks.

This feature prevents an action that has stopped responding or running without completing from continuously tying up the system. However, selecting this option only affects actions that are not currently running. You cannot use this check box to terminate an action that has already been loaded by the Scheduler and is currently running. Also, if the action you are running (such as a DOS batch file) opened a DOS window, the DOS window is not automatically closed after the action has completed, unless you added the */c* parameter in the *Parameters* field when you originally added the action item.

18.2.10 Viewing or Editing the Details or Properties of an Action

- 1 Click an action, then click *Properties*.
- 2 Click one of the pages containing the details or properties associated with this action.
- 3 Make the necessary changes.
- 4 Click *OK*.

18.2.11 Viewing or Editing the Details or Properties of an Action Item

- 1 Click an action, then click *Properties*.
- 2 Click *Item*, select an action item, then click *Properties*.

- 3 Make the necessary changes.
- 4 Click *OK*.

18.2.12 Viewing or Editing User-Defined Action Item Properties

- 1 Open the Scheduler on a workstation.
- 2 Select an action item > click *Properties*.
- 3 Make the necessary changes.
- 4 Click *OK*.

Documentation Updates

This section contains information on documentation content changes that have been made in this section of the *Administration* guide since the initial release of Novell® ZENworks® 7 (August 26, 2005). The information will help you to keep current on updates to the documentation.

All changes that are noted in this section were also made in the documentation. The documentation is provided on the Web in two formats: .html and .pdf. The HTML and PDF documentation are both kept up-to-date with the documentation changes listed in this section.

The documentation update information is grouped according to the date the changes were published. Within a dated section, the changes are alphabetically listed by the names of the main table of contents sections for ZENworks 7 Workstation Management.

If you need to know whether a copy of the PDF documentation you are using is the most recent, the PDF document contains the date it was published on the front title page.

The documentation was updated on the following dates:

- [Section I.1, “July 14, 2006 \(Support Pack 1\),” on page 223](#)
- [Section I.2, “April 28, 2006,” on page 223](#)
- [Section I.3, “February 28, 2006,” on page 224](#)
- [Section I.4, “December 9, 2005,” on page 224](#)

I.1 July 14, 2006 (Support Pack 1)

Updates were made to the following section:

- [Section 15.9.4, “Editing Existing Windows Group Policies \(User and Workstation Packages\),” on page 200](#)

I.1.1 Windows Group Policies

The following updates were made to this section:

Location	Change
Section 15.9.4, “Editing Existing Windows Group Policies (User and Workstation Packages),” on page 200	Added a note to warn users that if the Network Location of Existing/New Group Policies path is set to a Linux file server, permission must be set from a Linux machine to allow read rights for users and workstations.

I.2 April 28, 2006

Updates were made to the following sections. The changes are explained below.

- [Section 13.1, “Dictionary Update Policy,” on page 149](#)
- [Section 15.4, “Novell iPrint Policy \(User and Workstation Packages\),” on page 182](#)

I.2.1 Dictionary Update Policy

The following updates were made in this section:

Location	Change
Section 13.1, "Dictionary Update Policy," on page 149	Added a section documenting the Dictionary Update Policy.

I.2.2 Novell iPrint Policy (User and Workstation Packages)

The following updates were made in this section:

Location	Change
Section 15.4, "Novell iPrint Policy (User and Workstation Packages)," on page 182	Deleted outdated information on using the Novell iPrint Policy on Windows 2000 terminal servers.

I.3 February 28, 2006

Updates were made to the following sections. The changes are explained below.

- Section I.3.1, "ZENworks Windows Group Policy (User and Workstation Packages)," on page 224

I.3.1 ZENworks Windows Group Policy (User and Workstation Packages)

The following updates were made in this section:

Location	Change
Section 15.9.1, "Understanding the Windows Group Policy," on page 193	Added a paragraph to warn users that using ZENworks Group Policies and Group Policies configured in Active Directory in the same environment is not supported.

I.4 December 9, 2005

The page design of the entire guide was reformatted to comply with revised Novell documentation standards.

Updates were made to the following sections. The changes are explained below.

- Section I.4.1, "Setting Up User and Workstation Package Policies," on page 224

I.4.1 Setting Up User and Workstation Package Policies

The following updates were made in this section:

Location	Change
Section 15.9.4, "Editing Existing Windows Group Policies (User and Workstation Packages)," on page 200	One of the subsections in this part of the documentation, entitled "Using Windows XP SP2 and ZENworks 7" was deleted because the scenario is no longer viable because of a fix in the code.

Application Management



The following sections provide information on the Application Management features in Novell® ZENworks® Desktop Management and the tasks you might need to perform to manage your applications:

- Chapter 19, “Novell Application Launcher: Components Overview,” on page 229
- Chapter 20, “Novell Application Launcher: Installing and Starting,” on page 239
- Chapter 21, “Novell Application Launcher: Configuring Settings,” on page 255
- Chapter 22, “Novell Application Launcher: Customizing Views,” on page 271
- Chapter 23, “Novell Application Launcher: Managing Authentication and File System Access,” on page 283
- Chapter 24, “Novell Application Launcher: Managing the Cache,” on page 293
- Chapter 25, “Novell Application Launcher: Organizing Applications,” on page 303
- Chapter 26, “ZENworks Launch Gadget: Configuring Settings,” on page 309
- Chapter 27, “Distribution: Overview,” on page 313
- Chapter 28, “Distribution: Simple Applications,” on page 315
- Chapter 29, “Distribution: Complex Applications,” on page 321
- Chapter 30, “Distribution: Terminal Server Applications,” on page 331
- Chapter 31, “Distribution: Web Applications,” on page 337
- Chapter 32, “Distribution: Applications to Terminal Servers,” on page 341
- Chapter 33, “Advanced Distribution: Creating Distribution Rules,” on page 343
- Chapter 34, “Advanced Distribution: Transferring Applications Using BITS,” on page 355
- Chapter 35, “Advanced Distribution: Pre-Installing Applications,” on page 367
- Chapter 36, “Advanced Distribution: Configuring Fault Tolerance, Load Balancing, and Site Lists,” on page 377
- Chapter 37, “Advanced Distribution: Configuring Application Dependencies and Chains,” on page 389
- Chapter 38, “Users: Supporting Terminal Server Users,” on page 397
- Chapter 39, “Users: Supporting Disconnected Users,” on page 401
- Chapter 40, “Users: Supporting Remote Users,” on page 405
- Chapter 41, “Controlling Rogue Processes,” on page 415
- Chapter 42, “Verifying Applications,” on page 423
- Chapter 43, “Uninstalling Applications,” on page 425
- Chapter 44, “Reporting Application Events,” on page 431
- Chapter 45, “Metering Software Licenses,” on page 459
- Chapter 46, “Reference: AdminStudio ZENworks Edition,” on page 463
- Chapter 47, “Reference: ZENworks SnAppShot,” on page 465
- Chapter 48, “Reference: Application Object Settings,” on page 471

- Chapter 49, “Reference: Macros,” on page 585
- Chapter 50, “Reference: Novell Application Launcher Tools,” on page 601
- Chapter 51, “Reference: Application Object Location,” on page 609
- Chapter 52, “Reference: Novell Application Launcher Authentication Hook,” on page 611
- Appendix J, “Documentation Updates,” on page 615

Novell Application Launcher: Components Overview

19

Novell® ZENworks® Desktop Management includes Novell Application Launcher™, workstation-based software that is used to deliver applications to the workstation.

Application Launcher is a 32-bit application that supports Windows 98 SE, Windows 2000, and Windows XP. When run on a workstation, Application Launcher reads Novell eDirectory™ to provide access to the applications the logged-in user and the workstation have been given rights to. If the user or workstation is not authenticated to eDirectory, Application Launcher uses the eDirectory information cached on the local workstation. It then controls every aspect of an application's use, from installing the application files, to mapping required drives, to uninstalling the application.

Application Launcher consists of three different user views that can be used to display, manage, and launch applications on user workstations: Application Window, Application Explorer, and Application Browser. If desired, all three views can be used at the same time on the same machine.

In addition to the three user views, Application Launcher includes the engine application, a Windows service, and a ZENworks Workstation Manager plug-in.

The following sections provide information to help you understand each of these components:

- [Section 19.1, “Application Window,” on page 229](#)
- [Section 19.2, “Application Explorer,” on page 231](#)
- [Section 19.3, “Application Browser,” on page 232](#)
- [Section 19.4, “Application Launcher Engine,” on page 236](#)
- [Section 19.5, “Application Launcher Service for Windows,” on page 236](#)
- [Section 19.6, “Application Launcher Workstation Helper,” on page 237](#)

19.1 Application Window

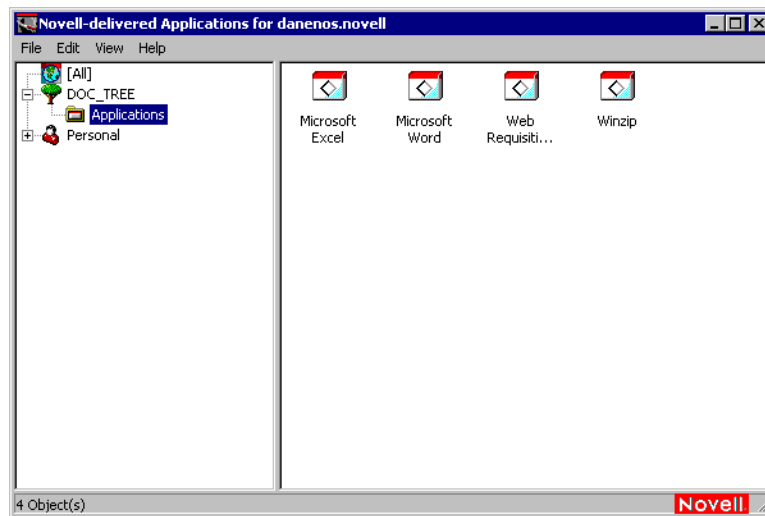
The Application Window is a standalone desktop window that provides greater administrative control of the user desktop than the other Application Launcher views.

The following sections contain additional information:

- [Section 19.1.1, “Application Window Description,” on page 230](#)
- [Section 19.1.2, “What Users Can Do with the Application Window,” on page 230](#)
- [Section 19.1.3, “Why Use the Application Window?,” on page 231](#)

19.1.1 Application Window Description

Figure 19-1 *Application Window*



The Application Window is divided into two panes. The left pane, referred to as the folder view, displays the following:

- **[All] folder:** Contains all applications that have been associated with the user or the workstation. This is an administrator-controlled feature. By default, it is enabled, which means the folder appears. You can disable the feature if desired. For instructions, see [Section 21.3, “Configuring User Settings,” on page 258](#).
- **eDirectory trees:** Each tree contains the applications, located within the tree, that have been associated with the user or workstation. The Application Window displays only the trees to which the user and workstation are authenticated.
- **Personal folder:** Provides a location for the user to create personal folders for organizing applications. This is an administrator-controlled feature. By default, it is disabled, which means the folder does not appear. For information about enabling personal folders, see [Section 21.3, “Configuring User Settings,” on page 258](#).

When a user selects a tree or folder in the left pane, the right pane displays the items (folders or applications) that are contained within the tree or folder.

You can also configure the Application Window to not include the folder view (the left pane).

19.1.2 What Users Can Do with the Application Window

Using the Application Window, users can do the following:

- Run an application by double-clicking the application's icon in the right pane. Depending on the application and how it is configured in eDirectory, the Application Launcher might install files to the workstation, map drives, or change workstation configuration files or settings.
- View the properties of an application. The properties include a description of the application, information about people to contact for help with the application, the times when the application is available for use, and the workstation requirements established for the application.

- Verify (fix) problems with an installed application. Verifying an application causes Application Launcher to redistribute the application to the workstation.
- Uninstall an application. This is an administrator-controlled feature. By default, it is disabled. You can enable it on a per-application basis. For information, see [Section 43.1, “Enabling an Application to be Uninstalled,” on page 425](#).
- Create personal folders to organize applications. This is an administrator-controlled feature. By default, it is disabled. For information about enabling personal folders, see [Section 21.3, “Configuring User Settings,” on page 258](#).
- Log in to eDirectory through the Novell Client™ or the ZENworks Middle Tier Server. This is an administrator-controlled feature. By default, it is disabled.
- Disconnect Application Launcher from eDirectory so that the user can work offline. Disconnecting Application Launcher from eDirectory does not log the user out of eDirectory.

19.1.3 Why Use the Application Window?

The Application Window provides greater administrative control of the user desktop than either of the other two views. You should use this view if you want to partially or completely lock down user workstations.

For example, the Application Window lets you ensure that all distributed applications are located only in the Application Window. At the same time, you can also determine the way the applications are organized in the window.

Or, if you want even greater control, you can replace the Windows desktop with the Application Window. This lets you restrict user access to only the applications in the Application Window. For instructions, see [Section 20.4, “Using Application Launcher As the Windows Shell,” on page 243](#).

19.2 Application Explorer

Application Explorer integrates with Windows Explorer to make applications available through a standalone window, similar to the Application Window, and from the Windows desktop, the Start menu, the system tray, and the Quick Launch bar.

The following sections contain additional information:

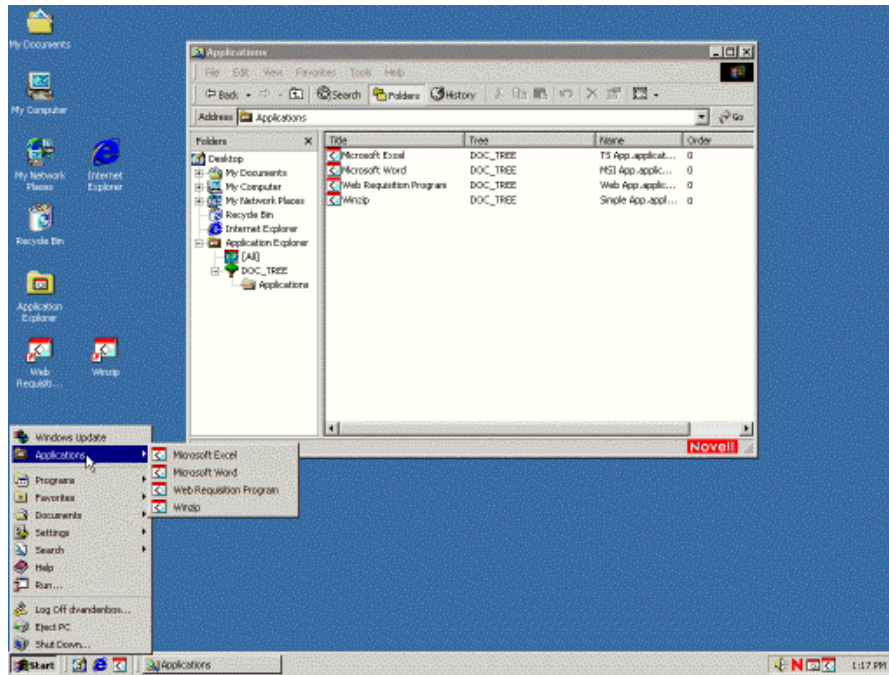
- [Section 19.2.1, “Application Explorer Description,” on page 231](#)
- [Section 19.2.2, “Why Use Application Explorer?,” on page 232](#)

19.2.1 Application Explorer Description

In the following example screen, the Application Explorer window displays the applications contained in the DOC_TREE. In addition, these same four applications are also displayed on the

Start menu, and two of the applications also appear on the desktop, one in the Quick Launch bar, and another in the system tray.

Figure 19-2 *Application Explorer Window*



The Application Explorer window contains the same features and functionality as the Application Window (see [Section 19.1, “Application Window,” on page 229](#)). In addition, because the Application Explorer window is an extension to Windows Explorer, it also includes functionality native to Windows Explorer, such as showing or hiding the folder view (left pane).

19.2.2 Why Use Application Explorer?

You should use Application Explorer if you don't require complete control of user desktops and you want take advantage of all the locations (Start menu, Windows desktop, and so forth) where application shortcuts can be placed.

19.3 Application Browser

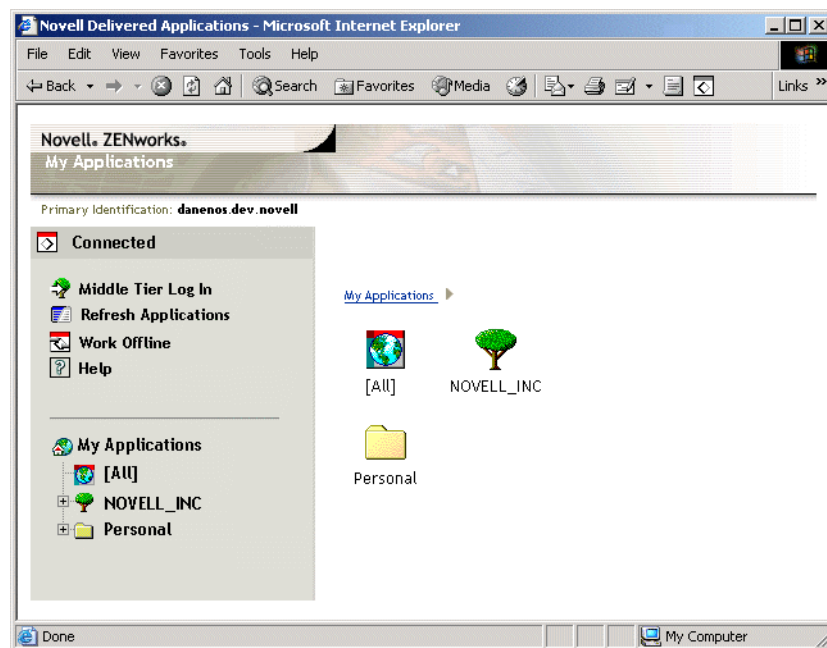
Application Browser, shown below, is a Web browser view similar to the Application Window and the Application Explorer window.

The following sections contain additional information:

- [Section 19.3.1, “Application Browser Description,” on page 233](#)
- [Section 19.3.2, “What Users Can Do with the Application Browser,” on page 233](#)
- [Section 19.3.3, “Why Use the Application Browser?,” on page 234](#)
- [Section 19.3.4, “Running the Application Browser Under Windows XP SP2 or Later,” on page 234](#)

19.3.1 Application Browser Description

Figure 19-3 Application Browser View



The Application Browser functionality is limited compared to the Application Window and Application Explorer. The view displays the following:

- **[All] folder:** Contains all applications that have been distributed to the user. This is an administrator-controlled feature. By default, it is enabled, which means the folder appears. You can disable the feature if desired. For instructions, see [Section 21.3, “Configuring User Settings,” on page 258](#).
- **eDirectory trees:** Each tree contains the applications, located within the tree, that have been distributed to the user or workstation. Application Launcher displays only the trees to which the user is authenticated.
- **Personal folder:** Provides a location for the user to create personal folders for organizing applications. This is an administrator-controlled feature. By default, it is disabled, which means the folder does not appear. For information about enabling personal folders, see [Section 21.3, “Configuring User Settings,” on page 258](#).

In the Application Browser, the Personal folder structure is for viewing and launching only. If users want to create or delete subfolders, add applications, or remove applications, they must use the Application Window or Application Explorer.

19.3.2 What Users Can Do with the Application Browser

Using the Application Browser, users can do the following:

- Run an application by double-clicking the application's icon in the right pane. Depending on the application and how it is configured in eDirectory, the Application Launcher might install files to the workstation, map drives, or change workstation configuration files or settings.

- View the properties of an application. The properties include a description of the application, information about people to contact for help with the application, the times when the application is available for use, and the workstation requirements established for the application.
- Verify (fix) problems with an installed application. Verifying an application causes Application Launcher to redistribute the application to the workstation.
- Uninstall an application. This is an administrator-controlled feature. By default, it is disabled. You can enable it on a per-application basis. For information, see [Section 43.1, “Enabling an Application to be Uninstalled,” on page 425](#).

19.3.3 Why Use the Application Browser?

The primary purpose of the Application Browser is to provide applications in a Web browser environment. You can enable users to launch the Application Browser independently, or you can integrate it into a Web portal, such as Novell Portal Services or Novell exteNd Director™, so that your applications are presented alongside Web content you've made available to users.

19.3.4 Running the Application Browser Under Windows XP SP2 or Later

Because of security changes in Windows XP Service Pack 2 (SP2), the Application Browser behaves differently on Windows XP SP2 or later workstations. As an administrator, you should communicate these changes to affected users.

The following sections contain additional information:

- [“Internet Explorer Information Bar and Add-On Installs” on page 234](#)
- [“Internet Explorer Local Machine Zone Lockdown and Active Content Blocking” on page 235](#)

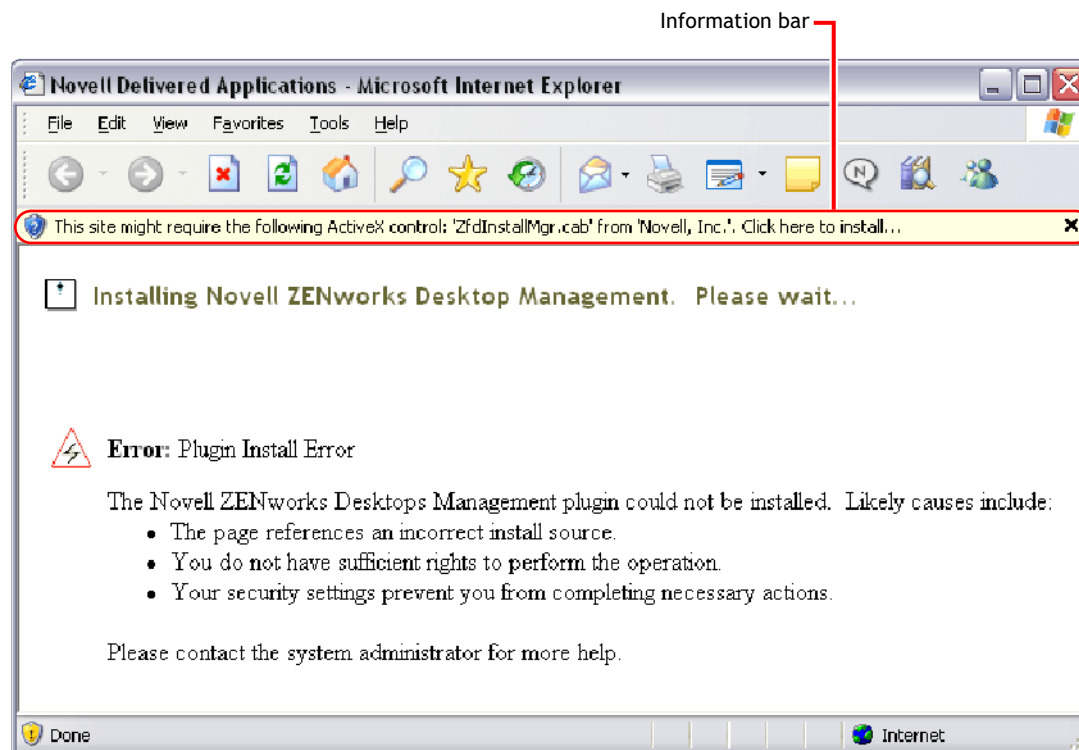
Internet Explorer Information Bar and Add-On Installs

When a Web page refers to an ActiveX control that is not currently on the workstation, users are asked whether or not they want the ActiveX control to be downloaded. In Windows XP SP2, this prompt is displayed in the information bar. The information bar displays in between the Internet Explorer toolbars and the Web page when a notification is present, and disappears on the next navigation.

NOTE: Displaying the information bar is enabled by default; however, the user can change the default setting so that the information bar does not display. Additionally, the ActiveX controls are installed automatically, without the information bar being displayed, if the publisher of the control (such as Novell) has been previously marked by the user as trusted.

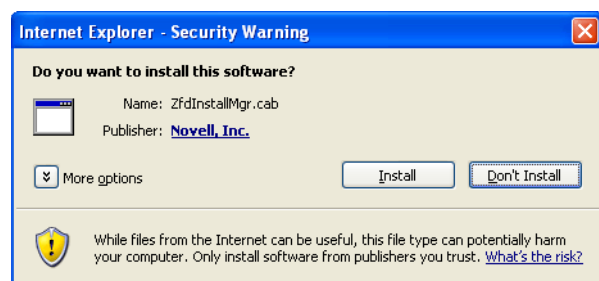
When a user running Windows XP SP2 or later accesses the Application Browser for the first time (assuming that the user is using the default settings and has not marked Novell as trusted), the following error message displays in the Web page and the information bar displays directly above it.

Figure 19-4 Information Bar Displayed In Internet Explorer



Clicking the information bar, then clicking Install ActiveX Control displays the following dialog box, from which the user installs the ActiveX control.

Figure 19-5 Internet Explorer - Security Warning Dialog Box



Internet Explorer Local Machine Zone Lockdown and Active Content Blocking

When Internet Explorer attempts to open a Web page, it places restrictions on what the page can do, based on the page's Internet Explorer security zone (in Internet Explorer, Tools > Internet Options). In Windows XP SP2 or later, the Local Machine Lockdown is more restrictive than in earlier versions of Windows XP.

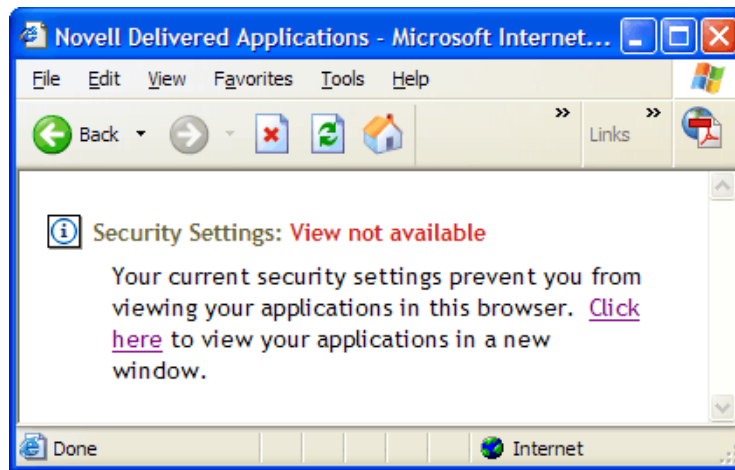
Because the ZENworks Application Browser is a locally installed HTML control containing ActiveX controls, the Local Machine Lockdown feature, when combined with the new active

content blocking feature, causes the Application Browser to behave differently on Windows XP SP2 or later workstations.

When a user types the URL to the Application Browser in the Address box or clicks a link to the Application Browser in the Favorites list, Internet Explorer shows an unformatted HTML page with the information bar showing the text “To help protect your security, Internet Explorer has restricted this file from showing active content that could access your computer. Click here for options.”

To avoid this situation and make it easier for users to access ZENworks Application Browser, the Application Browser view automatically detects if the Local Machine Lockdown feature is enabled on the workstation. If so, the following intermediate page displays:

Figure 19-6 Internet Explorer Security Warning Page



The user can then execute the link in this page, causing the Application Browser view to display in a new window, from which the user can access applications.

If the user accesses the Application Browser by clicking the *Application Browser* icon on the Standard Buttons toolbar in Internet Explorer, the intermediate page does not display and the Application Browser view displays without problems.

19.4 Application Launcher Engine

The Application Launcher engine, referred to simply as Application Launcher, performs the tasks required to manage applications associated with users or workstations. This includes such tasks as distributing, running, verifying, uninstalling, and caching applications.

Regardless of which view (Application Window, Application Explorer, or Application Browser) the user launches, Application Launcher is started in the background. It then accesses eDirectory (or the workstation's local cache directory if the user or workstation is not authenticated to eDirectory) to determine which applications to display to the user and to perform any other preconfigured tasks.

19.5 Application Launcher Service for Windows

On Windows 98, Application Launcher can perform all the tasks required to manage an application. On Windows 2000/XP, a user might not have all the workstation rights required by Application Launcher to perform its tasks. To ensure that it always has the necessary rights, Application

Launcher includes a Windows service (`nalntsrv.exe`), referred to as the NAL Service, that does the following:

- **Distribution, Caching, Uninstalling:** Ensures that applications can be distributed to, cached to, and uninstalled from the workstation regardless of the logged-in user's file system access. For example, if you've restricted user rights to specific local directories, the user might not have the file system and registry rights required to install an application to the workstation. The NAL Service, running in the system space, ensures that the application can be installed.
- **Launching:** Enables you to configure applications to launch and run under the System user's credentials rather than the logged-in user's credentials. This gives an application full rights to the file system and the registry, regardless of the logged-in user's rights.

You can choose from two security modes when launching the application as the System user: secure System user mode and unsecure System user mode.

Secure System user mode can be used if the user does not need to interact with the application (for example, you are applying a Service Pack); no interface is displayed to the user.

Unsecure System user mode can be used if the user requires interaction with the program (for example, a word processor); the normal interface is displayed to the user.

19.6 Application Launcher Workstation Helper

Application Launcher and the NAL Service manage all tasks for applications associated with the logged-in user. However, in addition to associating applications with users, you can associate applications with workstations. This requires that workstations be included in eDirectory as Workstation objects and that Workstation Manager be running on the workstations (see [Part III, “Automatic Workstation Import and Removal,” on page 117](#)).

When Workstation Manager starts, it loads the Application Launcher Workstation Helper (`zenappws.dll`). The Workstation Helper authenticates to eDirectory as the workstation (through the Workstation object). The Workstation Helper finds any applications associated with the workstation and performs any preconfigured management tasks associated with the applications. For example, if you've scheduled an application to be pre-installed in the middle of the night (also referred to as a “lights out” distribution), the application is distributed to the workstation by the Workstation Helper. Or, if you've configured an application to be launch immediately, the Workstation Helper launches the application.

The Workstation Helper does not have a user interface. Workstation-associated applications are only displayed when Application Launcher is running. When Application Launcher starts, it receives the list of workstation-associated applications from the Workstation Helper. Application Launcher then displays the workstation-associated applications just as it does the user-associated applications.

The Workstation Helper refreshes—that is, rereads eDirectory for changes to Application objects associated with the workstation—when 1) Application Launcher is started, 2) Application Launcher is manually refreshed, or 3) the Workstation Helper's scheduled refresh time occurs (see [Section 21.7, “Configuring Workstation Settings,” on page 267](#)).

Novell Application Launcher: Installing and Starting

20

The following sections provide information to help you install and start Novell® Application Launcher™:

- [Section 20.1, “Installing Application Launcher,” on page 239](#)
- [Section 20.2, “Installing the Application Launcher Plug-In,” on page 239](#)
- [Section 20.3, “Starting Application Launcher,” on page 240](#)
- [Section 20.4, “Using Application Launcher As the Windows Shell,” on page 243](#)
- [Section 20.5, “Application Window Command Line Switches,” on page 244](#)
- [Section 20.6, “Application Explorer Command Line Switches,” on page 251](#)

For additional information about Application Launcher, see [Chapter 19, “Novell Application Launcher: Components Overview,” on page 229](#).

20.1 Installing Application Launcher

The ZENworks® Desktop Management Agent installation program installs Application Launcher. All three Application Launcher views (Application Window, Application Explorer, and Application Browser) are installed, as well as the NAL Service for Windows and the Application Launcher Workstation Helper.

The Desktop Management Agent installation program must be run on each user's workstation. For instructions, see [“Installing and Configuring the Desktop Management Agent”](#) in the *Novell ZENworks 7 Desktop Management Installation Guide*.

NOTE: If you plan to use the Novell Client™ to enable Application Launcher to authenticate to Novell eDirectory™ and access NetWare® servers, you need to install it on your user workstations. For Novell Client requirements and installation instructions, see [“User Workstation Requirements”](#) in the *Novell ZENworks 7 Desktop Management Installation Guide*. If you plan to use the ZENworks Middle Tier Server rather than the Novell Client, and the Middle Tier Server is not already installed, see [“Installing the ZENworks Middle Tier Server”](#) in the *Novell ZENworks 7 Desktop Management Installation Guide*.

20.2 Installing the Application Launcher Plug-In

The Novell Application Launcher plug-in is a simplified version of Novell Application Launcher that can be used in place of the ZENworks Desktop Management Agent on workstations that only require distribution of user-associated applications. Or, it can be used to provide a Web-based roll-out of the Management Agent to workstations.

The Application Launcher plug-in includes only the Application Explorer and Application Browser views. It does not include the Application Window view, Application Launcher Service for Windows (nalntsrv.exe), or Application Launcher Workstation Helper (zenappws.dll). It

also does not include any other Desktop Management components, such as Workstation Manager, Workstation Inventory, Remote Management, or Workstation Imaging.

For information about installing the Application Launcher plug-in, see “[Installing the Novell Application Launcher Plug-In](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

20.3 Starting Application Launcher

The following sections explain how to manually start Application Launcher and how to automate starting the applications:

- [Section 20.3.1, “Windows 2000/XP File System Rights,” on page 240](#)
- [Section 20.3.2, “Manually Starting Application Launcher,” on page 240](#)
- [Section 20.3.3, “Automating Application Launcher Startup,” on page 242](#)

20.3.1 Windows 2000/XP File System Rights

To ensure that Application Launcher has the local file system access that it needs to distribute applications, make sure the user has the following rights on the workstation:

- At least Read access to the NAL cache directory (typically, `c:\nalcache`). For more information, see [Section 24.2, “File System Rights to the NAL Cache,” on page 296](#).
- Full Control access to the user's temp directory (typically, `c:\documents and settings\username\local settings\temp`).
- Full Control access to the user's data encryption directory (typically, `c:\documents and settings\username\application data\microsoft\crypto`). This is required only if the user is using the Desktop Management Agent without a network client.
- Read\Write rights to the `HKEY_CURRENT_USER\Software\NetWare\NAL\1.0` registry key.
- Read rights to the `HKEY_LOCAL_MACHINE\Software\NetWare\NAL\1.0` registry key
- Read rights to the `HKEY_LOCAL_MACHINE\Software\Novell\ZENworks` registry key.

If you have not locked down the workstation, the appropriate rights can be granted through membership in the Users group.

In addition, the System user requires full access to all areas of the workstation so that the NAL Service (a component of Application Launcher) can distribute applications and launch applications configured to run in the “system” space. By default, this access is granted to the System user as a member of the Administrators group. Do not limit the default rights given to the Administrators group or the System user account.

For more information about Application Launcher file system access requirements, see [Chapter 23, “Novell Application Launcher: Managing Authentication and File System Access,” on page 283](#).

20.3.2 Manually Starting Application Launcher

The view (Application Window, Application Explorer, or Application Browser) you want to use determines how you start Application Launcher.

The following sections contain additional information:

- “Application Window” on page 241
- “Application Explorer” on page 241
- “Application Browser” on page 242

Application Window

To start Application Launcher so that the Application Window view is displayed:

- 1 Click the *Start* menu > *Programs* > *Novell ZENworks Desktop Management* > *Application Window*.

or

Run `nalwin.exe` or `nalwin32.exe` from the `c:\program files\novell\zenworks` directory.

or

Run `nal.exe` from the `sys:\public` directory on the ZENworks Desktop Management Server.

In previous releases, `nal.exe` copied the Novell Application Launcher files to the workstation and then started the Application Window. Beginning with ZENworks for Desktops 4, `nal.exe` does not copy the files to the workstation; it only starts the Application Window if the Novell Application Launcher files are installed on the workstation. The primary purpose of the `nal.exe` file on the ZENworks Desktop Management Server is to maintain backward compatibility with login scripts created for previous versions.

IMPORTANT: You must ensure that you are not executing `nal.exe` from a server that has ZENworks for Desktops version 4.x or earlier installed. Running the ZENworks for Desktops 3.x `nal.exe` downgrades the Novell Application Launcher components on your workstation and causes error in the Application Launcher processes.

IMPORTANT: If you run `nal.exe` from the `sys:\public` directory and receive an error stating “The ordinal 6625 could not be located in the dynamic link library MFC42.DLL,” you need to update your server's `sys:\public\mfc42.dll` file. The correct version of `mfc42.dll` is installed to workstations by the ZENworks Desktop Management Agent. You can copy the file from a workstation's `c:\winnt\system32` directory to the server's `sys:\public\mfc42.dll` directory.

For information about command line switches that can be used when starting the Application Window, see [Section 20.5, “Application Window Command Line Switches,” on page 244](#).

Application Explorer

To start Application Launcher so that the Application Explorer view is displayed:

- 1 Click the *Start* menu > *Programs* > *Novell ZENworks Desktop Management* > *Application Explorer*.

or

Run `nalview.exe` or `naldesk.exe` from the `c:\program files\novell\zenworks` directory.

or

Run `naexpld.exe` from the `sys:public` directory on the ZENworks Desktop Management Server.

In previous releases, `naexpld.exe` copied the Novell Application Launcher files to the workstation and then started the Application Explorer. Beginning with ZENworks for Desktops 4, `naexpld.exe` does not copy the files to the workstation; it only starts the Application Explorer if the Novell Application Launcher files are installed on the workstation. The primary purpose of the `naexpld.exe` file on the Desktop Management Server is to maintain backward compatibility with login scripts created for previous versions.

IMPORTANT: You must ensure that you are not executing `nal.exe` from a server that has ZENworks for Desktops version 4.x or earlier installed. Running the ZENworks for Desktops 3.x `nal.exe` downgrades the Novell Application Launcher components on your workstation and causes error in the Application Launcher processes.

IMPORTANT: If you run `naexpld.exe` from the `sys:\public` directory and receive an error stating “The ordinal 6625 could not be located in the dynamic link library MFC42.DLL,” you need to update your server's `sys:\public\mfc42.dll` file. The correct version of `mfc42.dll` is installed to workstations by the ZENworks Desktop Management Agent. You can copy the file from a workstation's `c:\winnt\system32` directory to the server's `sys:\public\mfc42.dll` directory.

For information about command line switches that can be used when starting the Application Window, see [Section 20.6, “Application Explorer Command Line Switches,” on page 251](#).

Application Browser

To start Application Launcher so that the Application Browser view is displayed:

- 1 Launch the Web browser, then click the *Application Browser* icon on the Standard Buttons toolbar.

20.3.3 Automating Application Launcher Startup

There are several ways to automatically start Application Launcher, including the following:

- Include the appropriate Application Window, Application Explorer, or Application Browser startup commands in the user's Windows or network login script.
- Add the Application Window or Application Explorer shortcut to the Windows Startup folder. The Desktop Management Agent installation program includes options to let you add either shortcut to the Startup folder.

20.4 Using Application Launcher As the Windows Shell

You can use Application Launcher in place of Windows Explorer (the default Windows shell) to further restrict user access to applications on workstations. When you do so, the Application Window view replaces the standard Windows desktop.

- [Section 20.4.1, “Setting Up Application Launcher As the Shell on Windows 98,” on page 243](#)
- [Section 20.4.2, “Setting Up Application Launcher As the Shell on Windows 2000/XP,” on page 243](#)

20.4.1 Setting Up Application Launcher As the Shell on Windows 98

- 1 Open the workstation's `system.ini` file (typically, `c:\windows\system.ini`) with a text editor.
- 2 Replace the `shell=explorer.exe` line with the following line:
`shell=c:\program files\novell\zenworks\nalwin.exe`
If you want the Application Window to be maximized when it comes up, add the `/max` switch to `nalwin.exe` (for example, `nalwin.exe /max`).
- 3 Save and close the `system.ini` file.
- 4 Restart Windows.

IMPORTANT: Starting Application Launcher under the Application Window shell is not supported. On a Windows 98 machine, doing so can cause general fault protection errors.

You should ensure that Application Launcher is not accidentally started. For example, remove the Application Explorer and Application Window shortcuts from the Start menu (*Start > Programs > ZENworks Desktop Management*), disable the user's ability to browse to the `c:\program files\novell\zenworks` directory, and verify that `nalwin.exe`, `nal.exe`, `nalwin32.exe`, and `naldesk.exe` are not being executed in the user's login scripts (Windows login script, Novell login script, etc.).

20.4.2 Setting Up Application Launcher As the Shell on Windows 2000/XP

- 1 On the Windows 2000/XP workstation, run `regedit.exe` and locate the following setting:
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`
- 2 Change the `SHELL` value from `explore.exe` to:
`c:\program files\novell\zenworks\nalwin.exe`
If you want the Application Window to be maximized when it comes up, add the `/max` switch to `nalwin.exe` (for example, `nalwin.exe /max`).
- 3 Close `regedit.exe`.
- 4 Restart Windows.

20.5 Application Window Command Line Switches

The following command line switches can be used when starting the Application Window.

The Application Window can be started by using the `nalwin.exe` or `nalwin32.exe` files, located in the workstation's `c:\program files\novell\zenworks` directory, or the `nal.exe` file, located in the ZENworks Desktop Management Server's `sys:public` directory. These switches work with all three files.

IMPORTANT: When you use a command line switch to distribute (`/a`), uninstall (`/l`), or verify (`/v`) an application, Application Launcher performs the action in the user space, not in the workstation space (even if the application is associated with the workstation). Therefore, the logged-in user must have the eDirectory rights and file system rights required to perform the distribution, uninstall, or verification of the application.

Table 20-1 Application Window Command Line Switches

Switch	Description
<code>:</code>	Skips the initial splash screen.
EXAMPLE: <code>nalwin :</code>	
<code>/a="tree:.app_object_dn"</code>	Distributes and launches the specified Application object, regardless of whether or not it has been associated with the user or workstation, as long as the user has the file system rights needed to distribute and launch the application and the rights to read Application object properties.
EXAMPLE: <code>nalwin /a="nov:.ms word.app"</code>	In addition to distributing and launching the specified application, Application Launcher continues running and displays the user and workstation-associated applications in the Application Window. If you don't want Application Launcher to do this, you can use the <code>/f</code> switch to instruct it not to read eDirectory for associations and the <code>/h</code> switch to hide the Application Window.
	<i>Tree</i> is the eDirectory tree where the Application object resides. The default tree is assumed if no tree name is specified.
	<i>App_object_dn</i> is the fully distinguished name of the Application object.
	NOTE: The quotation marks are required only if a space is used in the tree name or Application object name.

Switch	Description
<p><code>/c="window_title"</code></p> <p>EXAMPLE: <code>nalwin /c="%cn%'s Apps"</code></p>	<p>Uses the specified text as the title for the Application Window. The default window title is "Novell-delivered Applications for <i>User</i>," where <i>User</i> is the distinguished name of the user.</p> <p>The text specified can contain macros (variables) to display eDirectory information. The example, <code>/c="%cn%'s Apps"</code> substitutes the user's common name in the title (for example, JSmith's Apps).</p> <hr/> <p>NOTE: The quotation marks are required only if a space is used in the window title.</p> <hr/> <p>For information about macros, see Chapter 49, "Reference: Macros," on page 585.</p>
<p><code>/f</code></p> <p>EXAMPLE: <code>nalwin /f /h</code></p>	<p>Instructs Application Launcher not to read eDirectory to get the list of applications that have been associated with the logged-in user or the workstation. This is useful when using the <code>/a</code>, <code>/v</code>, or <code>/l</code> switches to simply distribute, verify, or uninstall a specific application. The example causes Application Launcher to start with the Application Window hidden (<code>/h</code>) not read eDirectory for all of the applications associated to the logged-in user or workstation (<code>/f</code>), and then distribute and launch the Word application (<code>/a=.word.apps</code>).</p> <p>This switch also requires you to use the <code>/h</code> switch.</p>
<p><code>/h</code></p> <p>EXAMPLE: <code>nalwin /h</code></p>	<p>Hides the Application Window.</p> <p>This switch is required when using the <code>/f</code> switch and is useful with the <code>/a</code>, <code>/v</code>, and <code>/l</code> switches.</p>
<p><code>/l="tree:.app_object_dn"</code></p> <p>EXAMPLE: <code>nalwin /l="nov:.msword.app"</code></p>	<p>Uninstalls the specified Application object.</p> <p>In addition to uninstalling the specified application, Application Launcher continues running and displays the user and workstation-associated applications in the Application Window. If you don't want Application Launcher to do this, you can use the <code>/f</code> switch to instruct it not to read eDirectory for associations and the <code>/h</code> switch to hide the Application Window.</p> <p><i>Tree</i> is the name of the tree where the Application object resides. The default tree is assumed if no tree name is specified.</p> <p><i>App_object_dn</i> is the fully distinguished name of the Application object.</p> <hr/> <p>NOTE: The quotation marks are required only if a space is used in the tree name or Application object name.</p> <hr/>
<p><code>/max</code></p> <p>EXAMPLE: <code>nalwin /max</code></p>	<p>Displays the Application Window maximized when first loaded, overriding the window state (size and position) that was saved when exiting the previous Application Window session.</p>
<p><code>/min</code></p> <p>EXAMPLE: <code>nalwin /min</code></p>	<p>Displays the Application Window minimized when first loaded, overriding the window state (size and position) that was saved when exiting the previous Application Window session.</p>

Switch	Description
<p>/nd</p> <p>EXAMPLE:</p> <pre>nalwin /nd</pre>	<p>Skips the warning dialog box that appears when a dial-up connection is detected.</p>
<p>/norm</p> <p>EXAMPLE:</p> <pre>nalwin /norm</pre>	<p>Displays the Application Window in its original state (size and position) when first loaded, as long as the Save Window Size and Position setting (<i>User object > ZENworks tab > Launcher Configuration page > Add button > Window tab</i>) is turned off. By default, the Save Window Size and Position setting is turned off.</p>
<p>/nq</p> <p>EXAMPLE:</p> <pre>nalwin.exe /a=.word.app / p="file 1.txt" /nq</pre>	<p>Used only with the /p switch, instructs Application Launcher to remove the enclosing quotes from the parameter string. In the example, if /nq is not used, the parameters passed to the application would be "file 1.txt". With the /nq switch, the parameter is passed as file 1.txt.</p>

Switch	Description
<p><code>/p=param</code> <code>/p="param1 param2 param3"</code></p> <p>EXAMPLE: <code>nalwin /a=.word.app /</code> <code>p=file.txt</code></p>	<p>Passes the specified parameters to the launched application. It is only effective when used with <code>/a</code> or <code>/v</code>. The specified parameters are added to any that are already defined in the Application object (<i>Run Options</i> tab > <i>Application</i> page > <i>Parameters</i> field). The following rules apply when using the switch:</p> <ul style="list-style-type: none"> • Application Launcher reads everything after <code>/p=</code> until the first space. At that point, it assumes the end of the parameter string. If the parameter string includes spaces, you must enclose the entire string in quotes. <p>Example 1: <code>nalwin.exe /a=.word.app /p=file.txt</code> Passed to word.app: <code>file.txt</code></p> <p>Example 2: <code>nalwin.exe /a=.word.app /p="/</code> <code>f=file.txt /m / w"</code> Passed to word.app: <code>"/f=file.txt /m /w"</code></p> <p>Example 3: <code>nalwin.exe /a=.word.app /p=file 1.txt</code> Passed to word.app: <code>file</code></p> <p>In Example 1, the parameter string does not include spaces so no quotes are required. In Example 2, the parameter string includes three parameters, separated by spaces, so quotes are required. In Example 3, the parameter string includes a filename with spaces, but no quotes have been used, so only the first part of the filename is passed to the application.</p> <ul style="list-style-type: none"> • Use the <code>/nq</code> (no quotes) switch if you don't want the enclosing quotes to be passed to the application. <p>Example 4: <code>nalwin.exe /a=.word.app /p="file</code> <code>1.txt" /nq</code> Passed to word.app: <code>file 1.txt</code></p> <p>Example 5: <code>nalwin.exe /a=.word.app /p="/</code> <code>f=file.txt /m / w" /nq</code> Passed to word.app: <code>/f=file.txt /m /w</code></p> <p>Example 5 is the same as Example 2. However, Example 5 includes <code>/nq</code> so that the enclosing quotes are not passed.</p> <ul style="list-style-type: none"> • Use escaped quotes (<code>\"</code>) for any parameters that must include quotes in order to be accepted by the application. <p>Example 6: <code>nalwin.exe /a=word.app /p="/f=\"file</code> <code>1.txt\" /r /q" /nq</code> Passed to word.app: <code>/f="file 1.txt" /r /q</code></p> <p>Example 7: <code>nalwin.exe /a=word.app /p="/f=file</code> <code>1.txt /r /q" /nq</code> Passed to word.app: <code>/f=file 1.txt /r /q</code></p> <p>Example 6 assumes that the application requires file <code>1.txt</code> to be enclosed in quotes because the filename includes spaces. Example 7 assumes that the application does not require filenames with spaces to be enclosed in quotes.</p> <ul style="list-style-type: none"> • The total characters allowed for all parameters is 256.

Switch	Description
/r EXAMPLE: nalwin /r	Resets the Application Launcher launch flag to 0. This occurs automatically when Application Launcher terminates normally, However, if Application Launcher terminates abnormally (for example, a user uses Ctrl+Alt+Del to shut down <code>nalwin.exe</code>), the launch flag is not reset and Application Launcher cannot be restarted until the workstation is rebooted or this switch is used.

Switch	Description
<pre>/restrictonline=0 1 2 3</pre> <p>EXAMPLE: <pre>nalwin /restrictonline=1</pre></p>	<p>Determines the Application Launcher state (online or offline) as eDirectory connections become available. This switch is supported only when eDirectory authentication occurs directly through the ZENworks Desktop Management Agent; it is not supported when eDirectory authentication occurs through the ZENworks Middle Tier Server.</p> <p>The switch's four possible values are described below, with each value having both a startup behavior and a running behavior. The running behavior applies when, after initial startup, Application Launcher detects a change in eDirectory connections.</p> <p><code>/restrictonline=0</code></p> <ul style="list-style-type: none"> • At startup: Application Launcher goes into online mode if it detects an eDirectory connection, unless the connection is through dial-up. In that case, Application Launcher prompts the user whether to go online or stay offline. • Running: Regardless of the connection type (direct or dial-up), Application Launcher automatically goes into online mode if it detects an eDirectory connection. <p>The <code>/restrictonline=0</code> value results in the same behavior as Application Launcher's default behavior. In other words, using the 0 value is the same as not using the switch at all.</p> <p><code>/restrictonline=1</code></p> <ul style="list-style-type: none"> • At startup: Application Launcher goes into online mode if it detects an eDirectory connection, unless the connection is through dial-up. In that case, Application Launcher stays in offline mode. • Running: Same as the startup behavior. Application Launcher goes into online mode if it detects an eDirectory connection, unless the connection is through dial-up. In that case, Application Launcher stays in offline mode. <p><code>/restrictonline=2</code></p> <ul style="list-style-type: none"> • At startup: Value not used at this time. • Running: Value not used at this time. <p><code>/restrictonline=3</code></p> <ul style="list-style-type: none"> • At startup: Application Launcher goes into online mode if it detects an eDirectory connection, otherwise, Application Launcher stays in offline mode. • Running: If Application Launcher started in online mode, it remains in online mode as long as an eDirectory connection is available. If Application Launcher started in offline mode, it remains in offline mode even if an eDirectory connection becomes available.

Switch	Description
<p><code>/singletree="tree"</code></p> <p>EXAMPLE: <code>nalwin /singletree=nov</code></p>	<p>Reads the specified eDirectory tree only, regardless of any other trees the user might be authenticated to. This option applies only to user-associated applications, not workstation-associated applications. For example, assume that the workstation has a Workstation object in TREE1. The user authenticates to TREE2 and starts Application Launcher against TREE2 (<code>nalwin /singletree=TREE2</code>). Application Launcher displays the user-associated application from TREE2 and the workstation-associated applications from TREE1.</p> <hr/> <p>NOTE: The quotation marks are required only if a space is used in the tree name.</p> <hr/>
<p><code>/s</code></p> <p>EXAMPLE: <code>nalwin /s</code></p>	<p>Makes the Application Window act like the Windows shell. For example, on the File menu, the Exit Application Launcher option changes to Shutdown and gives the user the standard Windows shutdown options.</p> <p>This is not a true replacement for the Windows shell. If users minimize the Application Window, they have access to the normal desktop. If you want the Application Window to replace the Windows shell, see Section 20.4, "Using Application Launcher As the Windows Shell," on page 243.</p> <hr/> <p>NOTE: On a Windows 98 workstation, when a user selects Shutdown > Close All Programs and Log On as a Different User, the user's Windows desktop remains displayed while the login dialog box is displayed; normally, the desktop is removed.</p> <hr/>
<p><code>/time=n</code></p> <p>or</p> <p><code>/timen</code></p> <p>EXAMPLE: <code>nalwin /time=30</code></p>	<p>Delays starting of Application Launcher for the specified number of seconds.</p> <p>Use this switch only if you want Application Launcher to wait extra time before loading. For example, if several other programs are starting from the login script and they all display splash screens, you might not want all of them displayed at the same time. Or, if you are using the <code>/a</code> switch to launch an application from a login script, you might want to delay the start until all other commands in the login script have been executed.</p> <hr/>
<p><code>/u</code></p> <p>EXAMPLE: <code>nalwin /u</code></p>	<p>Terminates all applications, exits the Application Window, and unloads Application Launcher from memory.</p> <hr/>

Switch	Description
<code>/v="app_object_dn"</code>	Verifies and launches the specified application.
<p>EXAMPLE: <code>nalwin /v="nov:.snap.apps"</code></p>	<p>In addition to verifying and launching the specified application, Application Launcher continues running and displays the user and workstation-associated applications in the Application Window. If you don't want Application Launcher to do this, you can use the <code>/f</code> switch to instruct it not to read eDirectory for associations and the <code>/h</code> switch to hide the Application Window.</p> <p><i>Tree</i> is the name of the tree where the Application object resides. The default tree is assumed if no tree name is specified.</p> <p><i>Application_object_dn</i> is the fully distinguished name of the Application object.</p>
<p>NOTE: The quotation marks are required only if a space is used in the tree name or Application object name.</p>	

20.6 Application Explorer Command Line Switches

The following command line switches can be used when starting Application Explorer.

Application Explorer can be started by using the `nalview.exe` or `naldesk.exe` files, located in the workstation's `c:\program files\novell\zenworks` directory, or the `nalexpld.exe` file, located in the ZENworks Desktop Management Server's `sys:public` directory. These switches work with all three files.

Table 20-2 Application Explorer Command Line Switches

Switch	Description
<code>/nd</code>	Skips the warning dialog box that appears when a dial-up connection is detected.
<p>EXAMPLE: <code>nalview /nd</code></p>	
<code>/ns</code>	Skips the initial splash screen.
<p>EXAMPLE: <code>nalview /ns</code></p>	

Switch	Description
<pre>/restrictonline=0 1 2 3</pre> <p>EXAMPLE: <pre>nalview /restrictonline=1</pre></p>	<p>Determines the Application Launcher state (online or offline) as eDirectory connections become available. This switch is supported only when eDirectory authentication occurs directly through the ZENworks Desktop Management Agent; it is not supported when eDirectory authentication occurs through the ZENworks Middle Tier Server.</p> <p>The switch's four possible values are described below, with each value having both a startup behavior and a running behavior. The running behavior applies when, after initial startup, Application Launcher detects a change in eDirectory connections.</p> <p><code>/restrictonline=0</code></p> <ul style="list-style-type: none"> • At startup: Application Launcher goes into online mode if it detects an eDirectory connection, unless the connection is through dial-up. In that case, Application Launcher prompts the user whether to go online or stay offline. • Running: Regardless of the connection type (direct or dial-up), Application Launcher automatically goes into online mode if it detects an eDirectory connection. <p>The <code>/restrictonline=0</code> value results in the same behavior as Application Launcher's default behavior. In other words, using the 0 value is the same as not using the switch at all.</p> <p><code>/restrictonline=1</code></p> <ul style="list-style-type: none"> • At startup: Application Launcher goes into online mode if it detects an eDirectory connection, unless the connection is through dial-up. In that case, Application Launcher stays in offline mode. • Running: Same as the startup behavior. Application Launcher goes into online mode if it detects an eDirectory connection, unless the connection is through dial-up. In that case, Application Launcher stays in offline mode. <p><code>/restrictonline=2</code></p> <ul style="list-style-type: none"> • At startup: Value not used at this time. • Running: Value not used at this time. <p><code>/restrictonline=3</code></p> <ul style="list-style-type: none"> • At startup: Application Launcher goes into online mode if it detects an eDirectory connection, unless the connection is through dial-up. In that case, Application Launcher stays in offline mode. Same startup behavior as <code>/restrictonline=1</code>. • Running: If Application Launcher started in online mode, it remains in online mode as long as an eDirectory connection is available. If Application Launcher started in offline mode, it remains in offline mode even if an eDirectory connection becomes available.

Switch	Description
<code>/singletree="tree"</code> EXAMPLE: <code>nalview /singletree=nov</code>	<p>Reads the specified eDirectory tree only, regardless of any other trees the user might be authenticated to. This option applies only to user-associated applications, not workstation-associated applications. For example, assume that the workstation has a Workstation object in TREE1. The user authenticates to TREE2 and starts Application Launcher against TREE2 (<code>nalview /singletree=TREE2</code>). Application Launcher displays the user-associated application from TREE2 and the workstation-associated applications from TREE1.</p> <hr/> <p>NOTE: The quotation marks are required only if a space is used in the tree name.</p>

Novell Application Launcher: Configuring Settings

21

You can use the Novell® Application Launcher™ settings to configure how Application Launcher works. The following sections provide information and instructions for using the configuration settings:

- [Section 21.1, “How Configuration Settings Are Applied,” on page 255](#)
- [Section 21.2, “Accessing the Application Launcher Configuration Settings,” on page 255](#)
- [Section 21.3, “Configuring User Settings,” on page 258](#)
- [Section 21.4, “Configuring Window Settings,” on page 263](#)
- [Section 21.5, “Configuring Explorer Settings,” on page 265](#)
- [Section 21.6, “Configuring Browser Settings,” on page 266](#)
- [Section 21.7, “Configuring Workstation Settings,” on page 267](#)
- [Section 21.8, “Designating the Top of a Configuration Tree,” on page 269](#)

21.1 How Configuration Settings Are Applied

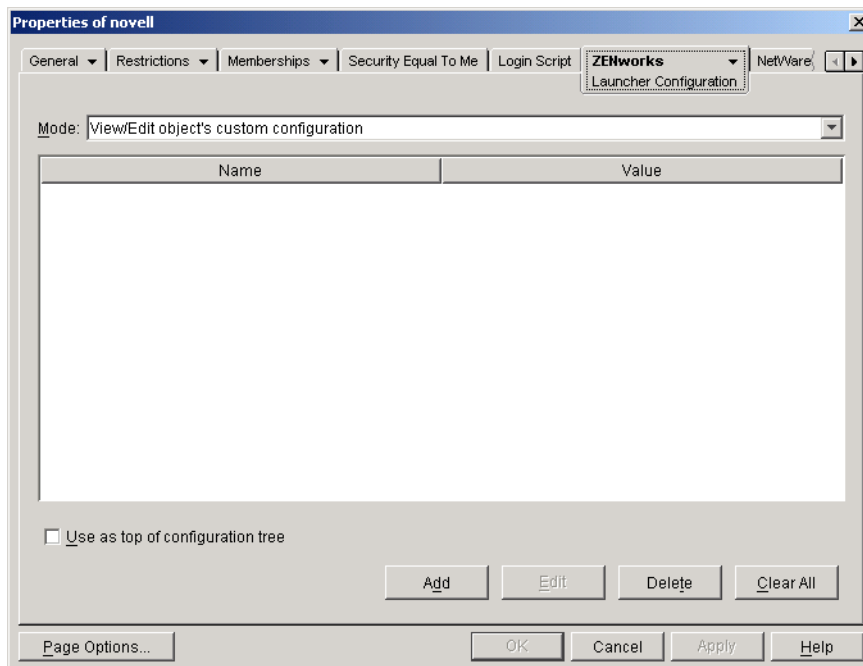
You can configure settings at the object or container level. When Application Launcher starts, it searches the Novell eDirectory™ tree, starting with the User object, for the settings that should be applied to the logged-in user. If a setting has not been defined at the User object, Application Launcher looks at the User object's parent container to see if the setting has been defined at that level. If not, Application Launcher continues up the eDirectory tree until it reaches the container object that has been designated as the top of the configuration tree (see [Section 21.8, “Designating the Top of a Configuration Tree,” on page 269](#)). If the setting is still not defined, it is considered undefined, or “unset,” and the preset default value is applied. Every configuration setting has a preset default value.

Application Launcher and the Application Launcher Workstation Helper follow the same process for determining configuration settings for the workstation, starting with the Workstation object.

21.2 Accessing the Application Launcher Configuration Settings

- 1 In ConsoleOne®, right-click the User, Workstation, or container object to which you want to apply new settings, then click *Properties*.

- 2 Click the *ZENworks* tab, then click *Launcher Configuration* to display the Launcher Configuration page.



The Launcher Configuration page provides three modes you can use to view the configuration settings for the current object. By default, the *View/edit object's custom configuration* mode is selected.

- 3 Make sure the *View/edit object's custom configuration* mode is selected. This is the mode that lets you set configuration options for the object. All three modes are described below.

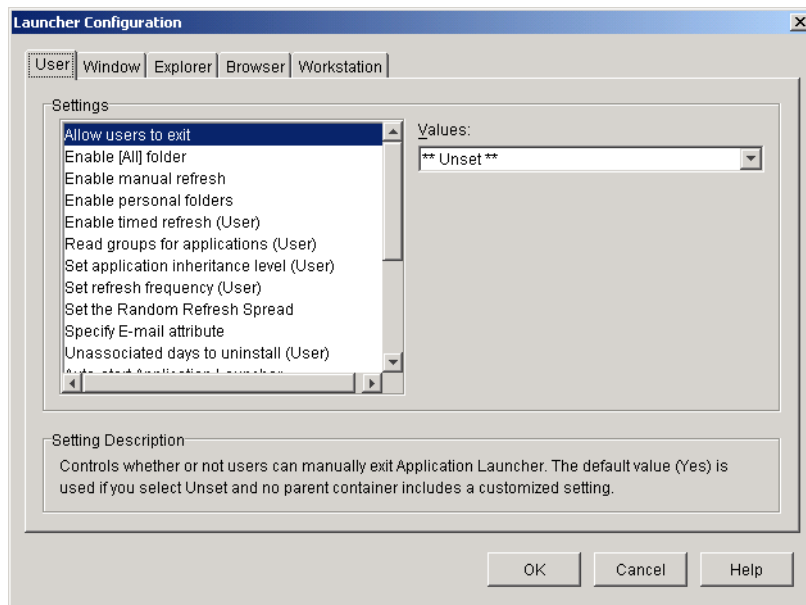
View/edit object's custom configuration (default mode): In this mode, the window lists all custom configuration settings that have been added and lists the settings values. Only customized settings are displayed; settings that are using the default or are receiving their value from their parent container (or higher) are not displayed.

This is the mode you must use to customize a configuration setting or edit a customized configuration setting.

View object's effective settings: In this mode, the window lists all configuration options with their effective settings. Effective settings might be from custom settings applied directly to the object, from settings inherited from a parent container, or from settings determined by the default settings values. This mode is useful when you want to see all settings that are being applied to the object.

View configuration tree: In this mode, the window displays the portion of the eDirectory tree that is being used to determine the configuration settings for the option. Only configuration options that are using a custom setting (either from the current object or from its parent container) are displayed. This mode is useful when you want to see where a setting is being inherited from.

- 4 Click *Add* to display the Launcher Configuration dialog box.



The Launcher Configuration dialog box has four or five tabs, depending on the type of object:

User: The User settings apply to Application Launcher regardless of the view (Application Window, application Explorer, Application Browser) that the user has open.

Window: The Window settings apply to the Application Window view.

Explorer: The Explorer settings apply to the Application Explorer view.

Browser: The Browser settings apply to the Application Browser view.

Workstation: The Workstation settings apply to the Application Launcher Workstation Helper. These settings are only used when the workstation has been imported into eDirectory as a Workstation object and Workstation Manager is running on the workstation.

- 5 To configure general settings for Application Launcher, see [Section 21.3, “Configuring User Settings,” on page 258](#).

or

To configure settings for the Application Window view, see [Section 21.4, “Configuring Window Settings,” on page 263](#).

or

To configure settings for the Application Explorer view, see [Section 21.5, “Configuring Explorer Settings,” on page 265](#).

or

To configure settings for the Application Browser view, see [Section 21.6, “Configuring Browser Settings,” on page 266](#).

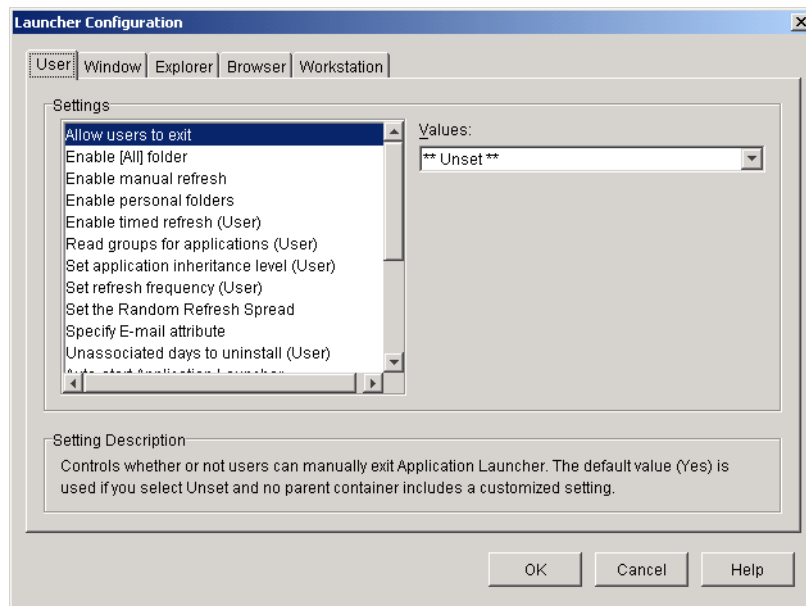
or

To configure settings for the Workstation Helper, see [Section 21.7, “Configuring Workstation Settings,” on page 267](#).

21.3 Configuring User Settings

The User settings are general configuration settings that apply to Application Launcher regardless of the view (Application Window, Application Explorer, Application Browser) the user has open.

- 1 Make sure the Launcher Configuration dialog box is open. If it is not, see [Section 21.2, “Accessing the Application Launcher Configuration Settings,”](#) on page 255.
- 2 Click *User* to display the general configuration settings that apply to Application Launcher.



- 3 Configure the following settings:

Allow users to exit: Specify whether or not to allow the user to exit Application Launcher. If you choose *No*, the Exit Application Launcher option is removed from the File menu in the Application Window and the Application Explorer window.

The setting values are *Yes*, *No*, and *Unset*. The default value (*Yes*) is used if you select *Unset* and no parent container includes a customized setting.

Enable [All] folder: Specify whether or not the user can see the [All] folder. The [All] folder displays all applications the user has access to, regardless of the application's eDirectory tree or folder.

The setting values are *Yes*, *No*, and *Unset*. The default value (*Yes*) is used if you select *Unset* and no parent container includes a customized setting.

Enable manual refresh: By default, when Application Launcher starts on a user's workstation it reads the eDirectory information for all applications associated with the user. If an application's eDirectory information changes after Application Launcher starts, Application Launcher must refresh its information before the changes show up on the user's workstation.

Specify whether or not users can manually refresh Application Launcher to distribute any changes made to application information since the last time Application Launcher read eDirectory.

The *Enable manual refresh* option and *Enable timed refresh* option are not connected in any way except that they both control refresh. One option does not need to be selected for the other to work.

The setting values are *Yes*, *No*, and *Unset*. The default value (*Yes*) is used if you select *Unset* and no parent container includes a customized setting.

Enable personal folders: Specify whether or not Application Launcher displays the Personal folder. If the Personal folder is displayed, users can organize their most used applications by moving them into the folder. They can even create subfolders.

When this option is enabled, the Application Window, Application Explorer window, and Application Browser all display the Personal folder. However, the Application Browser does not support creating personal folders. Personal folders created in the Application Window or the Application Explorer window display in the Application Browser, but the user cannot create additional personal folders.

The setting values are *Yes*, *No*, and *Unset*. The default value (*No*) is used if you select *Unset* and no parent container includes a customized setting.

Enable timed refresh: By default, when Application Launcher starts it reads the eDirectory information for all applications associated with the user. If an application's eDirectory information changes after Application Launcher starts, Application Launcher must refresh its information before the changes show up on the user's workstation.

Specify whether or not Application Launcher automatically refreshes applications so the user doesn't need to manually refresh them.

The setting values are *Yes*, *No*, and *Unset*. The default value (*No*) is used if you select *Unset* and no parent container includes a customized setting. If you set the option to *Yes*, the *Set refresh frequency* option determines how often Application Launcher refreshes applications.

Read group objects for applications: Specify whether or not you want Application Launcher to read Group objects to see if the user has been associated with any applications through membership in a group. Although groups are a convenient way of indirectly associating the user with applications, requiring Application Launcher to read Group objects can also decrease performance.

The setting values are *Yes*, *No*, and *Unset*. The default value (*Yes*) is used if you select *Unset* and no parent container includes a customized setting.

Set application inheritance level: Specify how many parent containers Application Launcher searches for applications associated with the user.

The setting values are *-1*, *1* through *999*, and *Unset*. Entering *-1* instructs Application Launcher to search to the root of the eDirectory tree. The default value (*1*) is used if you select *Unset* and no parent container includes a customized setting.

Set refresh frequency: This option applies only if Application Launcher is configured to perform a timed refresh (see the *Enable timed refresh* option).

Specify how often you want Application Launcher to search eDirectory for new or changed Application objects associated with the user. A short timed refresh interval is very useful in situations where you want changes to refresh quickly. However, a short timed refresh interval can cause higher network traffic.

The setting values are *0* through *999,999,999* seconds and *Unset*. The default value (*43200* seconds or 12 hours) is used if you select *Unset* and no parent container includes a customized setting.

Set the random refresh spread: By default, when Application Launcher starts it immediately reads eDirectory to get information about the applications associated with the user. You can use this option to instruct Application Launcher to retrieve its application information from the user's local cache directory during startup and then refresh that information from eDirectory at

a later time. This allows you to reduce network traffic (generated by Application Launcher reading eDirectory) during peak times such as the morning login period.

The setting values are *Custom* and *Unset*. If you select *Custom*, specify a range from which Application Launcher determines the initial refresh time. For example, if you specify *3600* seconds (1 hour), Application Launcher randomly selects a number between 0 and 3600 and does the initial refresh that long after starting. Entering 0 in the range field causes Application Launcher to refresh immediately upon starting.

If you select *Unset* and no parent container includes a customized setting, the default value (0) is used, which means that Application Launcher refreshes at startup.

Specify e-mail attribute: Specify the eDirectory attribute you want to use to display e-mail names on the Help Contacts tab of the Application object's Properties dialog box. If the user has problems with applications, he or she can contact people by e-mail to get help. The e-mail name that appears is pulled from the eDirectory attribute you specify here. Users must have the eDirectory rights required to read the selected attribute for all users defined as contacts.

The setting values include all the eDirectory attributes and *Unset*. The default value (*Internet e-mail address*) is used if you select *Unset* and no parent container includes a customized setting.

Unassociated days to uninstall: Specify the number of days after which you want Application Launcher to uninstall an application that is no longer associated with the user.

The setting values are *-1* through *730* and *Unset*. Specify *0* if you want the application to be uninstalled as soon as the user is no longer associated with it. You should use *0* only for users who are located in a high-availability environment such as a LAN environment. You should not use this setting for users whose workstations are using a wireless network connection or a LAN environment that is unreliable. Using *0* as the setting in either of these environments can result in applications being uninstalled if the workstation loses its network connection during an application refresh; the best practice is to use the *-1* setting or a setting of 1 or greater.

Specify *-1* if you don't want the application uninstalled when unassociated with the user. The default value (*-1*) is used if you select *Unset* and no parent container includes a customized setting.

NOTE: This option requires you to have enabled the application to be uninstalled. For information, see [Chapter 43, "Uninstalling Applications,"](#) on page 425.

Auto-start Application Launcher: This setting applies only to pre-ZENworks 6.5 versions of Application Launcher. Beginning with ZENworks 6.5, this setting is replaced by the ability to designate a startup option in the ZENworks Desktop Management Agent installation program.

If you have pre-ZENworks 6.5 versions of Application Launcher, specify whether or not you want Application Launcher to be included in the user's Startup folder so that it automatically starts when the user logs on to the Windows workstation. When Application Launcher starts, it displays the same view (Application Window or Application Explorer) that was being used at the time it was added to the Startup folder.

The setting values are *Yes*, *No*, and *Unset*. The default value (*No*) is used if you select *Unset* and no parent container includes a customized setting.

Enable reading from removable cache: Specify whether or not you want to enable Application Launcher's ability to read information from the cache directory on removable media such as a CD, Jaz*, or Zip* drive.

If you set this option to *No*, you disable a user's ability to launch applications or install applications from removable media only. Application Launcher continues to read the cache on the local hard drive.

The setting values are *Yes*, *No*, and *Unset*. The default value (*Yes*) is used if you select *Unset* and no parent container includes a customized setting.

Enable writing to the cache: Specify whether or not you want to enable Application Launcher's ability to write information to the cache directory.

The primary purpose of the cache directory is to enable users to work offline, disconnected from eDirectory. Setting this option to *No* disables the local cache, forcing users to be connected to eDirectory or a removable cache in order to access applications. To ensure that users don't manually go offline, the *Work offline* feature in Application Launcher is also disabled.

The setting values are *Yes*, *No*, and *Unset*. The default value (*Yes*) is used if you select *Unset* and no parent container includes a customized setting.

Enable the checkpoint restart postpone button: Distribution of a large application across a slow link can require a significant amount of time. Specify whether you want Application Launcher to display a *Postpone* button that enables the user to postpone the distribution of an application to his or her workstation. If you enable the *Postpone* button, it is only displayed when Application Launcher detects that the user's workstation is running in remote mode (see the [Configure remote access detection method](#) option).

The setting values are *Yes*, *No*, and *Unset*. The default value (*Yes*) is used if you select *Unset* and no parent container includes a customized setting.

Always evaluate referrals: Specify whether you want Application Launcher, when making a call to eDirectory, to evaluate the location of the eDirectory replicas and use the most accessible one at the time, or to force all eDirectory calls to go the first eDirectory replica found.

The setting values are *Yes*, *No*, and *Unset*. The default value (*No*) forces all eDirectory calls to the same replica and is used if you select *Unset* and no parent container includes a customized setting.

Enable automatic icon cleanup: This setting applies only when Application Launcher is running on a terminal server (Microsoft Windows Terminal Server or Citrix* MetaFrame*).

Specify whether or not you want Application Launcher, when exited, to remove application icons from the user's terminal server session desktop. Generally, you would set this option to *Yes* to have Application Launcher clean up. However, if you have multiple terminal server users who log in with the same username to run applications, you should disable this option. Otherwise, when one user exits Application Launcher, the application icon's disappears from all users' terminal server session desktops.

The setting values are *Yes*, *No*, and *Unset*. The default value (*Yes*) is used if you select *Unset* and no parent container includes a customized setting.

Configure remote access detection method: If Application Launcher detects an active dial-up connection, it starts in remote mode. In the case where an active dial-up connection is not detected, you can specify how you want Application Launcher to detect if the user's workstation is running in local or remote mode. The setting values are:

- **User will always be local:** Application Launcher functions as if the user is local.
- **User will always be remote:** Application Launcher functions as if the user is remote.
- **Prompt:** Application Launcher prompts the user to select local or remote.
- **Auto detect using max interface speed:** Application Launcher detects the maximum speed of the network interface card and determines from that speed whether or not the user

is local or remote. If you select this option, you must establish the connection speed (threshold) that determines local or remote status.

IMPORTANT: This functionality uses the Windows `sensapi.dll`. On Windows NT 4, this DLL is installed only with Internet Explorer 6. If this functionality is not working on Windows NT 4 workstations, make sure the DLL exists by updating to IE 6.

- **Detect using network ID:** Application Launcher uses the workstation's network ID (also known as the network address) to establish whether or not the user is local or remote.

If you select this option, you must enter the network ID used to establish whether the user is local or remote. To determine the network ID, take the bit-wise logical AND comparison of the 32-bit IP address and 32-bit subnet mask, then convert the resulting 32-bit network ID to dotted decimal notation. In an AND comparison, the result of the two bits being compared is true (1) only when both bits are 1; otherwise, the result is false (0). For example:

10000001 00111000 10111101 00101001	(129.56.189.41 IP address)
11111111 11111111 11110000 00000000	(255.255.240.0 subnet mask)
10000001 00111000 10110000 00000000	(129.56.176.0 network ID)

If you want workstations whose network IDs match the specified network ID to be considered local, select *Network ID is equal to this network ID*.

If you want workstations whose network IDs do not match the specified network ID to be considered local, select *Network ID is not equal to this network ID*.

- **Unset:** The default value (*User will always be local*) is used if you select *Unset* and no parent container includes a customized setting.

Bring all popup windows to the front: Specify whether or not you want Application Launcher to ensure that a launched application appears in front of any other currently-opened desktop windows. The setting values are *Yes*, *No*, and *Unset*. The default value (*Yes*) is used if you select *Unset* and no parent container includes a customized setting.

This setting has no affect on Windows 98 workstations because the default system configuration already forces pop-up windows to the front. However, the default system setting for Windows 2000 and Windows XP causes all pop-up windows to appear behind the current application's active window. With Application Launcher, this causes the launched application to appear behind the Application Launcher window. Enabling this option changes the Windows registry setting so that all pop-up windows, even the ones not generated by launching an application, appear as the front window. This is similar to using the Microsoft Tweak UI utility (`tweakui.exe`) to change the registry setting.

Enable Middle Tier login: Specify whether or not you want to add an Application Launcher menu item to enable users to log in through a ZENworks Middle Tier server (if they don't already have a Middle Tier session running). The setting values are *Yes*, *No*, and *Unset*. The default setting (*Yes*) is used if you select *Unset* and no parent container includes a customized setting.

Enable BITS: Specify whether or not you want Application Launcher to be able to use the Microsoft Background Intelligent Service (BITS) to transfer a user's applications to the workstation. Unlike Application Launcher's standard transfer method which competes with other applications for available network bandwidth, BITS uses idle network bandwidth to transfer files, increasing or decreasing the rate at which files are transferred based on the

amount of idle network bandwidth available. For example, if a network application begins to consume more bandwidth, BITS decreases its transfer rate.

The setting values are *Yes*, *No*, and *Unset*. The default setting (*No*) is used if you select *Unset* and no parent container includes a customized setting.

For additional configuration tasks you must complete to enable Application Launcher to use BITS, see [Chapter 34, “Advanced Distribution: Transferring Applications Using BITS,” on page 355](#).

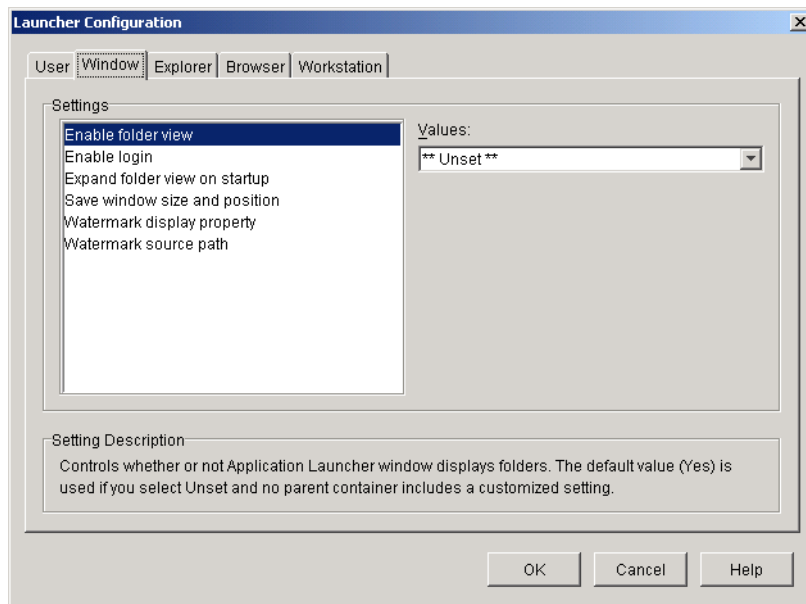
Allow User to Override BITS Transfer: Because BITS uses idle network bandwidth to transfer applications, an application might not be available when a user attempts to launch it. Specify the action you want to occur in this case:

- *Yes* (default): Causes Application Launcher to cancel the BITS job and immediately transfer the application itself.
- *No*: Causes BITS to maintain control of the transfer; the user is unable to launch the application until the transfer is complete.
- *Prompt*: Prompts the user as to whether or not to interrupt the BITS transfer and have Application Launcher immediately download the application.

21.4 Configuring Window Settings

The Window settings are configuration settings that apply only to the Application Window view. When a user opens the Application Window view, these settings, along with any settings configured on the User page (see [Section 21.3, “Configuring User Settings,” on page 258](#)), are applied.

- 1 Make sure the Launcher Configuration dialog box is open. If it is not, see [Section 21.2, “Accessing the Application Launcher Configuration Settings,” on page 255](#).
- 2 Click *Window* to display the configuration settings that apply to the Application Window view.



- 3 Configure the following settings:

Enable folder view: Specify whether or not to display a folder list in the Application Window. When this option is enabled, the Application Window is divided into two panes: the right pane contains the folder list and the left pane displays the applications located in the selected folder. When this option is disabled, the Application Window consists of one pane only with all applications displayed in that pane.

Changes to this setting do not take effect until after a user exits and restarts the Application Window.

The setting values are *Yes*, *No*, and *Unset*. The default value (*Yes*) is used if you select *Unset* and no parent container includes a customized setting.

Enable log in: Specify whether or not you want to add a Client32 Login option on the File menu in the Application Window so the user can run the Novell Client™ to log in to eDirectory. Before you enable the Log In option, make sure that Application Launcher can find the login program (`loginw32.exe`) on the user's workstation. For example, you could make sure that the login program's directory (typically `c:\winnt\system32`) is included in the PATH environment variable.

The setting values are *Yes*, *No*, and *Unset*. The default value (*No*) is used if you select *Unset* and no parent container includes a customized setting.

Expand folder view on startup: This option applies only if the folder view is enabled (see the *Enable folder view* option).

Specify whether or not you want to expand the entire folder tree when the Application Window opens.

The setting values are *Yes*, *No*, and *Unset*. The default value (*No*) is used if you select *Unset* and no parent container includes a customized setting.

Save window size and position: Specify whether or not to save the Application Window size and position settings.

The setting values are *Yes*, *No*, and *Unset*. The default value (*Yes*) is used if you select *Unset* and no parent container includes a customized setting.

Watermark display property: This setting applies only if you've specified a watermark (see the *Watermark source path* option). Select *Default* to have the watermark placed in the upper left corner in the Application Window. Select *Tile* to have the watermark repeated to cover the entire window. The default setting is *Default*.

Watermark source path: Specify the location of the graphic file you want to use as the background wallpaper in the Application Launcher window. Graphics files larger than 172 Kb cannot be used as the background wallpaper. You can use any valid file path convention (for example, URL, mapped drive, or UNC path) and wallpaper graphics type (for example, `.bmp`, `.gif`, or `.jpg`).

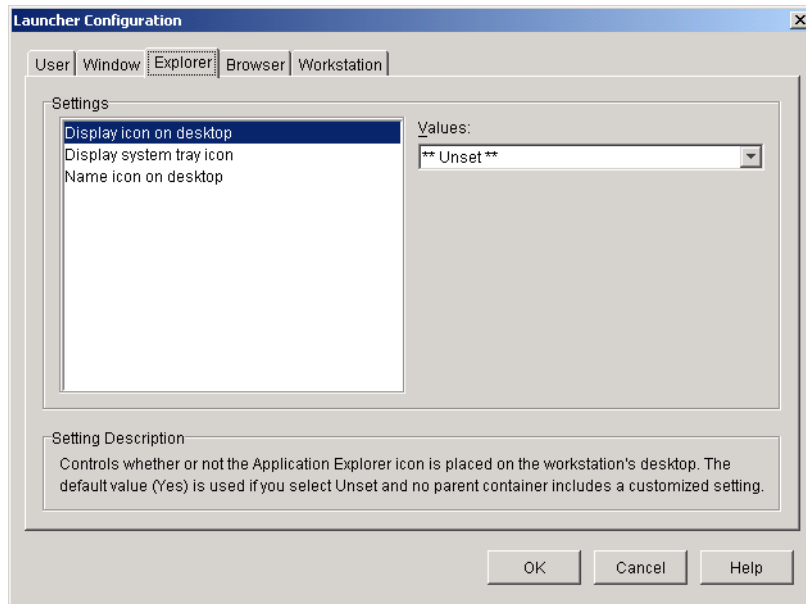
The ZENworks Desktop Management Agent does not support network drive mappings or UNC paths. You should only use these mapping types if users have a network client installed that enables access to the watermark source files. If this is not possible, you can also use an Application object to distribute the watermark to each workstation and use this Watermark Source Path field to enter the path to the local source.

The setting values are *Unset* and *Custom*. The default value (*Unset*) causes the setting to be inherited from the user's container. To override this setting, select *Custom* and then specify the appropriate file path.

21.5 Configuring Explorer Settings

The Explorer settings are configuration settings that apply only to the Application Explorer view. When a user opens the Application Explorer view, these settings, along with any settings configured on the User page (see [Section 21.3, “Configuring User Settings,” on page 258](#)), are applied.

- 1 Make sure the Launcher Configuration dialog box is open. If it is not, see [Section 21.2, “Accessing the Application Launcher Configuration Settings,” on page 255](#).
- 2 Click *Explorer* to display the configuration settings that apply to the Application Explorer view.



- 3 Configure the following settings:

Display icon on desktop: Specify whether or not you want the Application Explorer icon displayed on the user's desktop. The Application Explorer icon lets users open the Application Explorer window.

The setting values are *Yes*, *No*, and *Unset*. The default value (*Yes*) is used if you select *Unset* and no parent container includes a customized setting.

Display system tray icon: Specify whether or not you want the Application Explorer icon displayed in the Windows system tray. The Application Explorer icon lets users open the Application Explorer window.

The setting values are *Yes*, *No*, and *Unset*. The default value (*Yes*) is used if you select *Unset* and no parent container includes a customized setting.

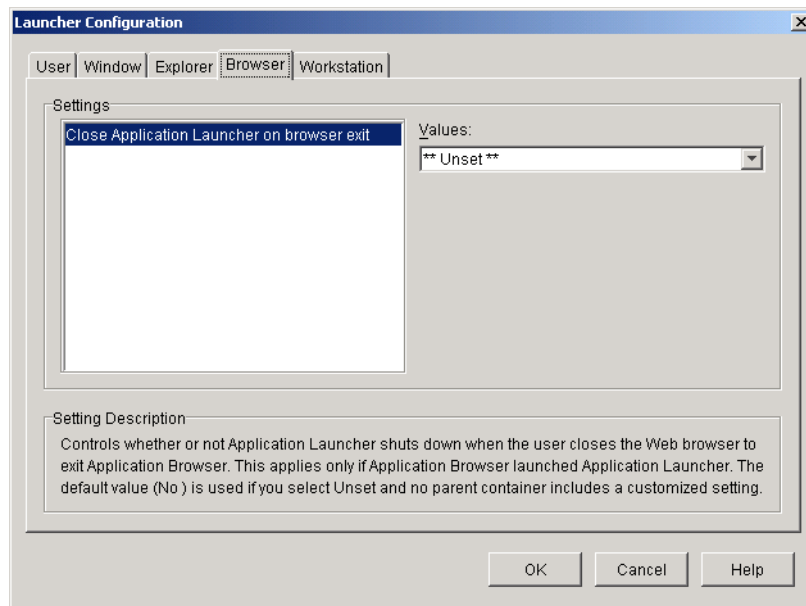
Name icon on desktop: Use this setting to change the name of the Application Explorer icon. The default name is Application Explorer.

The setting values are *Custom* and *Unset*. The default value (*Application Explorer*) is used if you select *Unset* and no parent container includes a customized setting. To use a different name, select *Custom* and enter the icon title.

21.6 Configuring Browser Settings

The Browser settings are configuration settings that apply only to the Application Browser view. When a user opens the Application Browser view, these settings, along with any settings configured on the User page (see [Section 21.3, “Configuring User Settings,” on page 258](#)), are applied.

- 1 Make sure the Launcher Configuration dialog box is open. If it is not, see [Section 21.2, “Accessing the Application Launcher Configuration Settings,” on page 255](#).
- 2 Click *Browser* to display the configuration settings that apply to the Application Browser view.



- 3 Configure the following settings:

Close Application Launcher on browser exit: This setting applies only to pre-ZENworks 7 versions of Application Launcher. Beginning with ZENworks 7, Application Launcher does not use this setting. Instead, it keeps track of the number of times its been called and shuts down only after the last view (Application Explorer, Application Window, or Application Browser) is exited.

With pre-ZENworks 7 versions, when a user opens the Application Browser view in his or her Web browser, Application Launcher is started if necessary. Specify whether or not you want Application Launcher to shut down when the user closes the Web browser to exit the Application Browser.

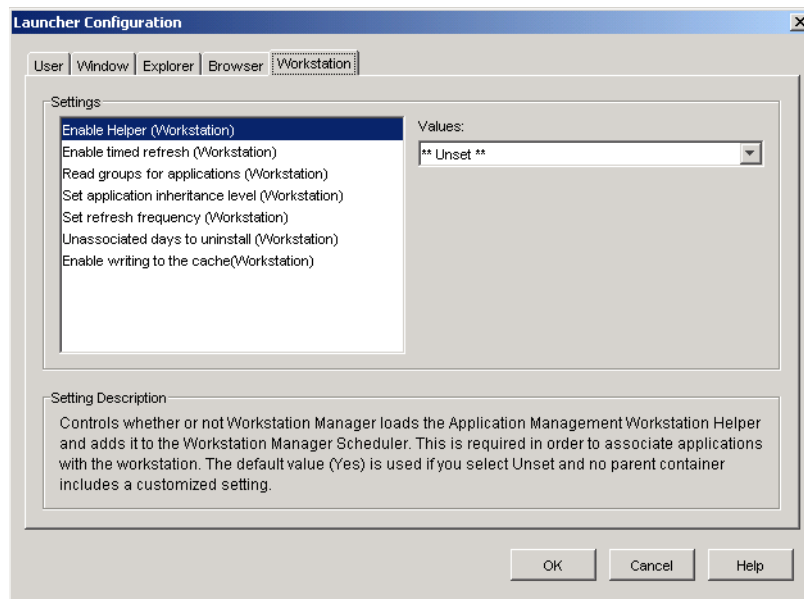
You should set this option to *Yes* only when users are using the Application Browser and neither of the other views (Application Window or Application Explorer). If users are also using the Application Window view or Application Explorer view, having Application Launcher close when the Web browser is exited also causes the Application Window and Application Explorer views to close.

The setting values are *Yes*, *No*, and *Unset*. The default value (*No*) is used if you select *Unset* and no parent container includes a customized setting.

21.7 Configuring Workstation Settings

The Workstation settings are configuration settings that apply to the Application Launcher Workstation Helper.

- 1 Make sure the Launcher Configuration dialog box is open. If it is not, see [Section 21.2, “Accessing the Application Launcher Configuration Settings,”](#) on page 255.
- 2 Click *Workstation* to display the configuration settings that apply to the Application Launcher Workstation Helper.



- 3 Configure the following settings:

Enable Helper: Specify whether or not you want to enable the Workstation Helper. Application Launcher reads eDirectory on behalf of logged-in users, but the Workstation Helper, running under Workstation Manager Scheduler, reads eDirectory on behalf of the workstation and passes the application information to Application Launcher. You must enable the Workstation Helper if you want to be able to distribute workstation-associated applications and have Application Launcher display them.

The setting values are *Yes*, *No*, and *Unset*. The default value (*Yes*) is used if you select *Unset* and no parent container includes a customized setting.

Enable Timed Refresh: Specify whether or not you want the Workstation Helper to periodically refresh application information from eDirectory. This enables the Workstation Helper to know about any new Application objects associated with the workstation or any updated information for currently-associated objects.

The setting values are *Yes*, *No*, and *Unset*. The default value (*Yes*) is used if you select *Unset* and no parent container includes a customized setting. The *Set refresh frequency* option determines how often Workstation Helper refreshes applications.

NOTE: A Workstation Helper timed refresh does not cause Application Launcher to display new workstation-associated applications discovered by the Workstation Helper timed refresh. If Application Launcher is running on the workstation, Application Launcher only displays the newly discovered workstation-associated applications after the user performs a manual refresh

or after Application Launcher performs its own timed refresh as defined by the Enable Time Refresh (User) setting on the User tab (see [Enable Timed Refresh](#) under [Section 21.3](#), “[Configuring User Settings](#),” on page 258). During its refresh, Application Launcher gets information about workstation-associated applications from Workstation Helper.

Read group objects for applications: Specify whether or not you want Workstation Helper to read Group objects to see if the workstation has been associated with any applications through membership in a group. Although groups are a convenient way of indirectly associating workstations with applications, reading Group objects can also decrease performance.

The setting values are *Yes*, *No*, and *Unset*. The default value (*No*) is used if you select *Unset* and no parent container includes a customized setting.

Set application inheritance level: Specify how many parent containers you want Workstation Helper to search for applications associated with the workstation.

The setting values are *-1* through *999* and *Unset*. The default value (*1*) is used if you select *Unset* and no parent container includes a customized setting.

Set refresh frequency: This setting applies only if Workstation Helper is configured to perform a timed refresh (see the [Enable timed refresh](#) option).

Specify how often you want the Workstation Helper to search eDirectory for new or changed Application objects associated with the workstation. A short timed refresh interval is very useful in situations where you want changes to refresh quickly. However, a short timed refresh interval can cause higher network traffic.

The setting values are *0* through *999,999,999* (seconds) and *Unset*. The default value (*43200*, which equates to 12 hours) is used if you select *Unset* and no parent container includes a customized setting.

Unassociated days to uninstall: Specify the number of days after which you want to uninstall an application that is no longer associated with the workstation.

The setting values are *-1* through *730* and *Unset*. Specify *0* if you want the application to be uninstalled as soon as the workstation is no longer associated with it. You should use *0* only for workstations that are located in a high-availability environment such as a LAN environment. You should not use this setting for workstations that are using a wireless network connection or a LAN environment that is unreliable. Using *0* as the setting in either of these environments can result in applications being uninstalled if the workstation loses its network connection during an application refresh; the best practice is to use the *-1* setting or a setting of *1* or greater.

Specify *-1* if you don't want the application uninstalled when unassociated with the workstation. The default value (*-1*) is used if you select *Unset* and no parent container includes a customized setting.

Enable writing to the cache: Specify whether or not you want to enable Workstation Helper's ability to write information to the cache directory. The main purpose of this option is to disable the local cache, forcing users to access their applications through eDirectory or a cache directory on removable media.

The setting values are *Yes*, *No*, and *Unset*. The default value (*Yes*) is used if you select *Unset* and no parent container includes a customized setting.

Enable BITS: Specify whether or not you want to be able to use the Microsoft Background Intelligent Service (BITS) to transfer a user's applications to the workstation. Unlike Application Launcher's standard transfer method which competes with other applications for available network bandwidth, BITS uses idle network bandwidth to transfer files, increasing or decreasing the rate at which files are transferred based on the amount of idle network

bandwidth available. For example, if a network application begins to consume more bandwidth, BITS decreases its transfer rate.

The setting values are *Yes*, *No*, and *Unset*. The default setting (*No*) is used if you select *Unset* and no parent container includes a customized setting.

For additional configuration tasks you must complete to enable Application Launcher to use BITS, see [Chapter 34, “Advanced Distribution: Transferring Applications Using BITS,” on page 355](#).

21.8 Designating the Top of a Configuration Tree

When Application Launcher searches the eDirectory tree for a user's Application Launcher configuration settings, it starts with the User object. If the option has not been set for the User object, Application Launcher looks at the object's parent container to see if the option has been set at that level. If not, Application Launcher continues up the eDirectory tree searching for the option's setting until it reaches an object that has been designated as the top of the tree or the [ROOT]. The Application Launcher Workstation Helper follows the same process, starting at the Workstation object, to discover the configuration settings for the workstation.

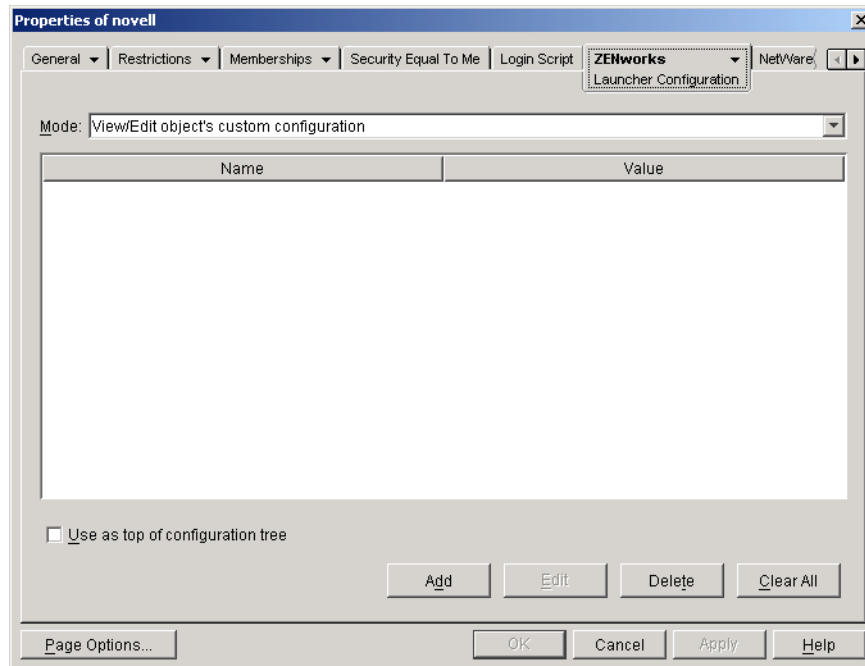
You can designate User, Workstation, or container objects as the top of a configuration tree. For example, if you want Application Launcher to read only the user's object for its configuration settings, you would designate the User object as the top of the configuration tree. Or, if you want Application Launcher to read the user's object and its parent container object for its configuration settings, you would designate the parent container object as the top of the configuration tree.

Not all users and workstations must use the same top for the configuration tree. For example, for one user you might want Application Launcher to read the user's configuration settings only, but you want to use the parent container as the top of the configuration tree for all other users in the container. In this case, you would specify the User object as the top of the configuration tree for the one user, and specify the parent container as the top of the configuration tree for the other users.

To designate an object as the top of the configuration tree:

- 1 In ConsoleOne, right-click the User, Workstation, or container object you want to designate as the top of a configuration tree, then click *Properties*.

- 2 Click the *ZENworks* tab, then click *Launcher Configuration* to display the Launcher Configuration page.



- 3 Select the *Use as top of configuration tree* check box to designate this object as the top of a configuration tree.
- 4 Click *OK*.

Novell Application Launcher: Customizing Views

22

The following sections provide information about changes you can make to the Application Window, Application Explorer, and Application Browser views to customize their appearance:

- [Section 22.1, “Customizing the Application Window and Application Explorer Views,” on page 271](#)
- [Section 22.2, “Customizing the Application Browser View,” on page 272](#)

22.1 Customizing the Application Window and Application Explorer Views

You can customize the appearance of the Application Window and Application Explorer views by replacing the following graphics elements:

- The startup screen (Application Window and Application Explorer)
- The Application Explorer desktop icons used to represent connected mode and disconnected mode
- The Application Explorer system tray icons used to represent idle, offline, and refreshing
- The AVI file used during the distribution and caching processes (Application Window and Application Explorer)
- The AVI file used during the uninstall process (Application Window and Application Explorer)
- The Novell® banner in the lower-right corner of the Application Window and Application Explorer window
- The 12 system tray icons used to animate a refresh (Application Window and Application Explorer)

Each graphics file must have a specific name and must be placed in the `c:\program files\novell\zenworks\graphics` directory.

- 1 Create the new graphics elements you want, using the information in the following table.

Element	File Name
Startup screen	splash.bmp
Desktop icon - connected mode	desktop.ico
Desktop icon - disconnected mode	offlinedesktop.ico
System tray icon - idle	systray.ico
System tray icon - disconnected mode	offlinesystray.ico
Distribution and caching process	progress.avi
Uninstall process	uninstall.avi

Element	File Name
Novell banner	minibanner.bmp
System tray icons - refresh animation	refresh1.bmp - refresh12.bmp

- 2 Create a `\graphics` directory under the `c:\program files\novell\zenworks` directory on each user's workstation (for example, `c:\program files\novell\zenworks\graphics`).
- 3 Copy the new graphics files to the `\graphics` directory.

TIP: To avoid manually creating the directory and copying the files to each user's workstation, create a simple Application object that creates the `\graphics` directory and copies the files to it. Then associate the Application object with each user (or workstation) and mark it as *Force run*.

22.2 Customizing the Application Browser View

You can use the `myapps.html`, `axnalview.js`, `refresh.html`, and `hf_style.css` files to customize the functionality and look of the Application Browser view. The following table lists what each file controls:

Table 22-1 Application Browser Files

File	Controls...
<code>myapps.html</code> <code>axnalview.js</code>	<ul style="list-style-type: none"> • Which ZENworks® Middle Tier Server is accessed • Whether the view is Web portal enabled or not • The banner graphic • The banner height • Whether or not the view includes the folder tree • How the application icons are displayed • The navigation elements that are displayed
<code>refresh.html</code>	<ul style="list-style-type: none"> • The message displayed in the Application Browser view while Application Launcher starts and retrieves application information
<code>hf_style.css</code>	<ul style="list-style-type: none"> • All styles that are applied to the view's HTML elements (heading, text, etc.)

The following sections provide information to help you use the files to customize the Application Browser view:

- [Section 22.2.1, “File Location,” on page 273](#)
- [Section 22.2.2, “Modifying the Myapps.html and Axnalview.js Files,” on page 274](#)
- [Section 22.2.3, “Creating a Refresh.html File,” on page 276](#)
- [Section 22.2.4, “Creating an Hf_style.css File,” on page 277](#)

22.2.1 File Location

The `myapps.html`, `axnalview.js`, `refresh.html`, and `hf_style.css` files reside, or can reside, in two locations, as shown in the following table:

Table 22-2 Application Browser File Locations

File	Location
<code>myapps.html</code> <code>axnalview.js</code>	<ul style="list-style-type: none">• <code>web_server_root\nwdocs</code> directory on the ZENworks Middle Tier Server• <code>c:\program files\novell\zenworks\nls\language</code> directory on the local workstation
<code>refresh.html</code>	This file does not exist until you create it. You must then place it in one of the following directories: <ul style="list-style-type: none">• <code>web_server_root\nwdocs\nal_html</code> directory on the ZENworks Middle Tier Server• <code>c:\program files\novell\zenworks\nal_html</code> directory on the local workstation
<code>hf_style.css</code>	This file does not exist until you create it. You must then place it in one of the following directories: <ul style="list-style-type: none">• <code>web_server_root\nwdocs\nal_html</code> directory on the ZENworks Middle Tier Server• <code>c:\program files\novell\zenworks\nal_html</code> directory on the local workstation

Myapps.html and Axnalview.js Files

The `myapps.html` and `axnalview.js` files contain the parameter settings that determine the appearance and functionality of the Application Browser view. They are installed with either of the following components:

- **Desktop Management Agent:** The files are installed by the Desktop Management Agent installation program as part of Application Launcher. For information about installing the Desktop Management Agent, see “[Installing and Configuring the Desktop Management Agent](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.
- **NAL plug-in:** The NAL plug-in is a simplified version of Application Launcher that includes only the Application Explorer and Application Browser views. The NAL plug-in, including the `myapps.html` and `axnalview.js` files, is installed to the ZENworks Middle Tier Server. When a user accesses the `myapps.html` file on the Web server for the first time, the NAL plug-in installation manager (`zfdwebinstallmgr.dll`), which is installed to the Middle Tier Server along with the `myapps.html` file, installs the NAL plug-in (including `myapps.html` and `axnalview.js`) to the user's workstation.

For information about installing the Middle Tier Server, see “[Installing the ZENworks Middle Tier Server](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*. For information about installing and using the NAL plug-in, see “[Installing the Novell Application Launcher Plug-In](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

If you modify the `myapps.html` file and `axnalview.js` file on the Middle Tier Server, users who access the Application Browser from the server have the modified files downloaded to the

c:\program files\novell\zenworks\nls\language directory on their workstations. This ensures that the same Application Browser settings are used regardless of whether a user accesses the Application Browser from the Middle Tier Server or the local drive.

If you have users who only launch the Application Browser by accessing the `myapps.html` file on the workstation, you need to modify the `myapps.html` file and `axnalview.js` file on their workstations. You might want to modify single copies of the files and then use an Application object to push them to each user's workstation.

Refresh.html and Hf_style.css Files

The `refresh.html` and `hf_style.css` files do not exist until you create them. After you create them and place them in the appropriate directory, they are used in place of the Application Browser's internal settings.

If you add the `refresh.html` and `hf_style.css` files to the ZENworks Middle Tier Server, when a user accesses the `myapps.html` file on the server, the files are downloaded to the user's workstation to maintain consistency.

If users are not accessing the `myapps.html` file from a ZENworks Middle Tier Server, you need to add the files to each user's workstation. You might want to distribute them through Application Launcher at the same time you distribute the `myapps.html`.

22.2.2 Modifying the Myapps.html and Axnalview.js Files

Both the `myapps.html` file and `axnalview.js` files include the same nine parameters, shown below.

```
<!--param name="SingleTree\" value="ZENWORKS_TREE"-->
<!--param name="PortalView\" value="false"-->
<!--param name="BannerURL\" value="http://www.company.com/
banner.html"-->
<!--param name="BannerHeight\" value="80"-->
<!--param name="ShowTree\" value="true"-->
<!--param name="ShowTasks\" value="false"-->
<!--param name="AppDisplayType\" value="0"-->
<!--param name="ShowAppFrameNavigation\" value="true"-->
<!--param name="ShowIEToolbarButton\" value="true"-->
```

Even though the files contain the same parameters, you need to modify both files. This ensures that Internet Explorer can successfully launch the Application Browser with the correct settings, regardless of its Local Machine Lockdown and Active Content Blocking security settings.

If you install the Application Browser from a Middle Tier Server (see “[Installing the Novell Application Launcher Plug-In](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.) rather than through the ZENworks Desktop Management Agent installation, you can customize two additional `myapps.html` parameters that are used by the installation manager:

```
<!--param name="MiddleTierAddress\" value=\"$ $IPADDR$\"-->
<!--param name="Nt4PluginVersion\" value="4,0,1,0"-->
```

By default, the parameters are commented out, which results in the Application Browser using its preset internal values.

To modify a parameter:

- 1 Open the `myapps.html` file and `axnalview.js` files in an editor.

For information about the location of these files, see [Section 22.2.1, “File Location,” on page 273](#).

- 2 Remove the `!--` (beginning comment) and the `--` (ending comment) to activate the parameter.
For example:

```
<param name=\"SingleTree\" value=\"novell_tree\"
```

- 3 Modify the parameter's VALUE. Each parameter is described below.

SingleTree: This parameter lets you specify a single Novell eDirectory™ tree from which to read application information. If this parameter is used, Application Launcher ignores any other trees to which the user authenticates.

This parameter applies only at installation time. After installation, changes to this parameter have no affect.

PortalView: This parameter lets you better support portals by removing the banner section of the Application Browser view. The VALUE settings are *True* or *False*. *True* removes the banner section.

BannerURL: This parameter applies only if the PortalView parameter is set to *False*.

You can use this parameter to specify an alternate banner. For example, you could use a banner that contains your company's logo instead of the Novell logo. The VALUE setting must be a URL to an HTML page or graphics file (GIF, JPEG, etc.). If you specify an HTML page, the page is cropped to the height specified by the BannerHeight parameter. If you specify a graphics file, the banner section scrolls to fit the entire graphics file. Unless you want the banner section to be scrollable, you should ensure that the graphic's height is not greater than the height specified in the BannerHeight parameter.

BannerHeight: This parameter applies only if PortalView parameter is set to *False* and the default Novell banner is being overridden by the *BannerView* parameter.

You can use this parameter to determine the height of the banner section. The VALUE setting must be from 5 to 200. Any number less than 5 is rounded up to 5. Any number greater than 200 is rounded down to 200.

ShowTree: This parameter determines whether or not the Application Browser view includes the left pane (referred to as the folder view). The VALUE settings are *True* and *False*. *True* causes the folder view to display, and *False* causes it to be removed.

ShowTasks: This parameter determines whether or not the folder view (left pane) includes the *Work online/work offline*, *MiddleTier log in/Middle Tier log out*, *Refresh applications*, and *Help* options. The VALUE settings are *True* and *False*. *True* causes the options to display, and *False* causes them to be removed.

AppDisplayType: This parameter determines how the applications are displayed in the right pane of the Application Browser view. The VALUE settings are *0* and *1*. The default setting, *0*, causes the application icons to display as large icons, similar to the Large Icons view in Windows Explorer. The *1* setting causes the applications to be listed in table format, similar to the List view in Windows Explorer.

ShowAppFrameNavigation: This parameter determines whether or not the right pane of the Application Browser view includes navigation. The VALUE settings are *True* and *False*. *True*

causes the right pane to include navigation. The type of navigation depends on the setting for the `AppDisplayType` parameter:

- When the `AppDisplayType` parameter is set to *0* (large icons), navigation is displayed as a breadcrumb trail (for example, ZENworks Tree > Application Folder > Application A).
- When the `AppDisplayType` parameter is set to *1* (small icons), navigation is displayed as an Up arrow at the top of the applications list.

Setting this parameter's value to *False* causes the Application Browser view to start with the All folder open, meaning that all application icons are displayed in the right pane. If the All folder is disabled in the user's Launcher Configuration settings in ConsoleOne, this parameter is ignored (in other words, the default value of *True* is used).

ShowIEToolbarButton: This parameter determines whether or not the Application Browser button is added to the Internet Explorer toolbar. The Application Browser button launches the local version of the `myapps.html` file. The *VALUE* settings are *True* and *False*. The *True* setting is the default setting and causes the Application Browser button to be added to the toolbar. The *False* setting causes the Application Browser button to be removed from the toolbar. Whenever this setting is changed, the user must close Internet Explorer and then reopen it for the change to take affect.

MiddleTierAddress: This parameter applies only if you've configured a ZENworks Middle Tier Server for access to eDirectory.

The `MiddleTierAddress` parameter lets you specify the IP address of the Middle Tier Server that the user authenticates to. It is used only if a Middle Tier Server address is not included in the Windows registry; the registry includes the address if the user entered it when running the ZENworks Desktop Management Agent installation program.

Nt4PluginVersion: The ZENworks 7 NAL plug-in is not supported on Windows NT 4 workstations (see “[Interoperability with Windows NT 4 Workstations](#)” in “[Interoperability with ZENworks for Desktops 4.x](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide* for more information about Windows NT 4 support). You can, however, continue to use the ZfD 4.0.1 NAL plug-in on those workstations. This parameter specifies the minimum version of the ZfD 4.0.1 NAL plug-in that runs on Windows NT workstations.

For example, the default parameter setting (4,0,1,0) requires only that the original ZENworks for Desktops 4.0.1 NAL plug-in be installed on the workstation. If you place an updated ZENworks for Desktops 4.0.1 NAL plug-in (`zfd40.cab`) with a version number higher than 4,0,1,0 (for example, 4,0,1,1 or 4,0,1,2) on the Middle Tier Server, workstations that have the 4.0.1.0 NAL plug-in are upgraded to the new version only if you change this parameter to the new version. In other words, upgrades do not happen automatically when you place a newer NAL plug-in version on the Middle Tier Server; if you want workstations upgraded, you must force the upgrade by bumping up the version number specified in this parameter.

- 4 Save the file.

22.2.3 Creating a Refresh.html File

When Application Launcher first starts, it reads eDirectory and the local cache for information about the applications it needs to display. If Application Launcher is started by opening the Application

Browser view, the following message is displayed in the view while Application Launcher retrieves its application information:

Figure 22-1 *Application Progress Message*



In Progress: Your application list is being generated.

You can replace this message by creating a `refresh.html` file that contains the message and graphics you want displayed during startup.

- 1 Create the file you want to use. Be aware of the following guidelines:
 - The file can contain text, graphics, and other standard HTML elements.
 - Make sure referenced files are available. If the `refresh.html` file is being accessed from a workstation rather than the ZENworks Middle Tier Server, use an absolute URL rather than a relative URL. For example, when referencing an image, use `` rather than ``. Any files referenced from the `refresh.html` file, regardless of the location, are downloaded to user's workstations along with the `refresh.html` file. In addition, the references are modified to point to the files on the workstation. Only referenced files one level deep are downloaded. For example, if `refresh.html` references `message.html`, which references `banner.jpg`, `message.html` is downloaded but not `banner.jpg`.
- 2 Name the file `refresh.html`.
- 3 Create a `nal_html` directory in one of the following two locations:
 - Under the `web_server_root\nwdocs` directory on the ZENworks Middle Tier Server (for example, `apache\nwdocs\nal_html`). The `nal_html` directory and its contents are copied to each user's workstation the same way the `myapps.html` file is copied. For information, see [“File Location” on page 273](#).
 - Under the `c:\program files\novell\zenworks` directory on each user's workstation, if users won't access the `myapps.html` page from the Middle Tier Server.
- 4 Copy the `refresh.html` file to the `nal_html` directory.

22.2.4 Creating an `Hf_style.css` File

The Application Browser uses an internal default cascading style sheet (`.css`) to determine the look of elements such as headings and paragraph text. You can replace the default style sheet by creating an `hf_style.css` file that contains the style definitions you want used.

- 1 Create the cascading style sheet. You can use the default Application Browser cascading style sheet, shown below, as an example or template.
- 2 Name the file `hf_style.css`.
- 3 Create a `nal_html` directory in one of the following two locations:
 - Under the `web_server_root\nwdocs` directory on the ZENworks Middle Tier Server (for example, `apache\nwdocs\nal_html`). The `\nal_html` directory, and its contents, is copied to each user's workstation the same way the `myapps.html` file is copied. For information, see [“File Location” on page 273](#).

- Under the c:\program files\novell\zenworks directory on each user's workstation, if users won't access the myapps.html page from the ZENworks Middle Tier Server.

4 Copy the hf_style.css file to the \nal_html directory.

Default Application Browser Cascading Style Sheet

```
a { color: #039; font-family: "Trebuchet MS", Arial, Helvetica,
Geneva, Swiss, SunSans-Regular; text-decoration: underline }
body { font family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss,
SunSans-Regular }
p, option, li, ol, ul { color: black; font-size: 0.9em; font-family:
"Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-Regular }
th { font-family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss,
SunSans-Regular }
.datalink { color: #039; text-decoration:underline; margin-top: 2px }
.errorlink { color: #c82727; text-decoration: underline; margin-top:
2px }
.errorhead { color: #c82727; font-style: normal; font-weight: 800;
font-size: 1.2em; line-height: 1.5em; margin-bottom: 1.5em }
.formcolumnhead1 { color: #556c79; font-weight: bold; font-size:
0.7em; text-align: center }
.formhead1 { color: white; font-weight: bold; font-size: 1em; line-
height: 1.2em; background-color: #6b8899; text-align: left; text-
indent: 0.5em; letter-spacing: 0.1em; vertical-align: middle }
.formhead1b { color: white; font-weight: bold; font-size: 1em; line-
height: 1.2em; background-color: #6b8899; text-align: left; text-
indent: 0.5em; letter-spacing: 0.1em; vertical-align: middle }
.formhead2 { color: black; font-weight: bold; font-size: 1em; line-
height: 1.2em; text-align: left; vertical-align: middle }
.formdescriptext { color: #355263; font-size: 0.8em; margin-left:
1em }
.head1 { color: black; font-weight: bold; font-size: 1.3em; line-
height: 1.3em; font-family: "Trebuchet MS", Arial, Helvetica, Geneva,
Swiss, SunSans-Regular; margin-bottom: 0.6em }
.head1a { color: #663; font-weight: bold; font-size: 1.3em; line-
height: 1.3em; font-family: "Trebuchet MS", Arial, Helvetica, Geneva,
Swiss, SunSans-Regular; margin-bottom: 0.6em; margin-left: 1em }
.head1b { color: black; font-weight: bold; font-size: 1.3em; line-
height: 1.3em; font-family: "Trebuchet MS", Arial, Helvetica, Geneva,
Swiss, SunSans-Regular }
.head1w { color: white; font-weight: bold; font-size: 1.3em; line-
height: 1.3em; font-family: "Trebuchet MS", Arial, Helvetica, Geneva,
Swiss, SunSans-Regular }
.head2 { color: black; font-weight: bold; font-size: 1.2em;
font-family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss,
SunSans-Regular; margin-top: 0.4em }
.head2a { color: #663; font-weight: bold; font-size: 1.2em; font-
family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-
Regular; margin-top: 0.4em }
.head2b { color: black; font-weight: 600; font-size: 1.2em; font-
family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-
Regular; letter-spacing: 0.1em; margin-top: 0.4em; margin-bottom:
```

```

0.3em; border-bottom: 2px solid #6c8899 }
.head2tm6 { color: black; font-weight: bold; font-size: 1.2em; font-
family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-
Regular; margin-top: 0.6em }
.head2w { color: #fff; font-weight: bold; font-size: 1.2em; font-
family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-
Regular }
.head2indent { color: black; font-weight: bold; font-size: 1.2em;
font-family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-
Regular; margin-top: 0.4em; margin-left: 0.5em }
.head3 { color: black; font-weight: bold; font-size: 1em; font-
family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-
Regular; margin-top: 0.3em }
.head3a { color: #663; font-weight: bold; font-size: 1em; font-
family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-
Regular; margin-top: 0.3em }
.head3b { color: black; font-weight: bold; font-size: 1em; font-
family: "Trebuchet MS", Arial, Helvetica, Geneva, "Trebuchet MS",
Arial, Helvetica, Geneva, Swiss, SunSans-Regular; }
.head3center { color: black; font-weight: bold; font-size: 1em; font-
family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-
Regular; text-align: center }
.head3indent { color: black; font-weight: bold; font-size: 1em; font-
family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-
Regular; margin-top: 0.3em; margin-left: 1em }
.head3tm6 { color: black; font-weight: bold; font-size: 1em; font-
family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-
Regular; margin-top: 0.6em }
.head3w { color: #fff; font-weight: bold; font-size: 1em; font-
family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-
Regular }
.head4 { color: black; font-weight: bold; font-size: 0.85em; font-
family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-
Regular; margin-top: 0.2em }
.head4b { color: #663; font-weight: bold; font-size: 0.85em; font-
family: "Trebuchet MS", Arial, Helvetica, Geneva, "Trebuchet MS",
Arial, Helvetica, Geneva, Swiss, SunSans-Regular; margin-top: 0.2em }
.head4tm6 { color: black; font-weight: bold; font-size: 0.85em; font-
family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-
Regular; margin-top: 0.6em }
.head5 { color: black; font-weight: 600; font-size: 0.75em; font-
family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-
Regular; margin-top: 0.2em }
.head5b { color: #663; font-weight: 600; font-size: 0.75em; font-
family: "Trebuchet MS", Arial, Helvetica, Geneva, "Trebuchet MS",
Arial, Helvetica, Geneva, Swiss, SunSans-Regular; margin-top: 0.2em }
.head5tm6 { color: black; font-weight: 600; font-size: 0.75em; font-
family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-
Regular; margin-top: 0.6em; margin-left: 2em }
.hint1 { color: #663; font-size: 12px; line-height: 14px; font-
family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-
Regular }
.hint1centered { color: #663; font-size: 12px; line-height: 14px;
font-family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-

```

```

Regular; text-align: center }
.hintlright { color: #663; font-size: 12px; line-height: 14px; font-
family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-
Regular; text-align: right }
.inactive { color: #738c9c }
.indent1 { margin-top: 0.3em; margin-left: 1em }
.indent1b { line-height: 18pt; margin-top: 0.5em; margin-left: 1em }
.indent1c { margin-top: 0.8em; margin-left: 1em }
.iconindent1 { margin-left: 18px }
.iconindent2 { margin-left: 34px }
.indent2 { margin-top: 0.3em; margin-left: 2em }
.indent3 { margin-top: 0.3em; margin-left: 3em }
.indentall { margin-left: 0.5em }
.listhead1 { color: black; font-style: normal; font-weight: 800;
font-size: 12pt; text-indent: .3em; }
.mainnavlink { font-weight: bold; font-size: 15pt; line-height: 18pt;
}
.margintop1 { margin-top: 0.3em }
.margintop2 { margin-top: 0.5em }
.margintop3 { margin-top: 1em }
.marginleft1 { margin-left: 1em }
.marginleft1b { font-size: 0.85em; margin-left: 1em }
.marginleft2 { margin-left: 2em }
.marginleft3 { margin-left: 3em }
.marginleft4 { margin-left: 4em }
.navlink { color: #030; font-weight: normal; text-decoration:
underline }
.nonproportional { color: black; font-size: 12pt; font-family:
"Courier New", Courier, Monaco }
.rowaltcolor { color: #efeee9 }
.serverhead1 { color: #c82727; font-weight: 800; font-size: 1.3em;
font-family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-
Regular }
.smalltext { font-size: 0.7em; line-height: 1em; font-family:
"Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-Regular }
.mediumtext { font-size: 0.85em; line-height: 1em; font-family:
"Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-Regular }
.smalltext2c { color: #355263; font-size: 0.7em; line-height: 1.1em;
font-family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-
Regular; width: 400px }
.textblue1 { color: #355263; font-size: 1em; font-family: "Trebuchet
MS", Arial, Helvetica, Geneva, Swiss, SunSans-Regular }
.smalltext2a { color: #663; font-size: 0.9em; line-height: 1.1em;
font-family: "Trebuchet MS", Arial, Helvetica, Geneva, Swiss, SunSans-
Regular }
.smalltext2b { color: black; font-weight: bold; font-size: 0.8em;
line-height: 1.1em; font-family: "Trebuchet MS", Arial, Helvetica,
Geneva, Swiss, SunSans-Regular }
.subtitle1 { color: black; font-weight: bold; font-size: 14px; line-
height: 14px; font-family: "Trebuchet MS", Arial, Helvetica, Geneva,
Swiss, SunSans-Regular }
.subtitle2 { color: white; font-weight: bold; font-size: 14px; line-
height: 14px; font-family: "Trebuchet MS", Arial, Helvetica, Geneva,
Swiss, SunSans-Regular }

```

```

.headpb { color: black; font-weight: bold; font-size: 15px; text-align: left; vertical-align: top; letter-spacing: 2px; }
.tab1s { color: white; font-weight: bold; font-size: 12px; line-height: 17px; text-decoration: none; background-color: #6b8899; text-align: center }
.tab1u { color: black; background-color: #DFDDD5; font-size: 12px; text-decoration: none; font-weight: bold; text-align: center }
.tab2s { color: white; font-weight: bold; font-size: 11px; text-decoration: none; background-color: #6b8899 }
.tab2u { color: white; font-weight: normal; font-size: 11px; text-decoration: none; background-color: #6b8899 }
span.tab1u { color: black }
span.tab2u { text-decoration: underline }
span.tab2s { text-decoration: underline }
.tablecolumnhead1 { color: #663; font-weight: bold; font-size: 0.7em; text-align: center }
.tablecolumnhead2 { color: #663; font-weight: 600; font-size: 0.75em }
.tablehead1 { font-weight: bold; font-size: 1em; line-height: 1.1em; background-color: #cc9; text-align: left; text-indent: 0.5em; letter-spacing: 0.1em }
.tablehead1b { font-weight: bold; font-size: 1em; line-height: 1.1em; background-color: #cc9; text-align: left; text-indent: 0.5em }
.tablesubhead1 { color: black; font-weight: bold; font-size: 0.85em; background-color: #efeee9; text-align: left; text-indent: 0.5em }
.tablehead3 { color: black; font-weight: bold; margin-left: .5em }
.tabb { font-weight: bold; font-size: 14pt; }
.tabw { color: white; font-weight: bold; font-size: 14pt; }
.task1 { margin-top: 0.3em; margin-left: 1em; font-size: 0.8em }
.task2 { margin-top: 0.3em; margin-left: 2em; font-size: 0.8em }
.windowheadgrey { color: #5a5958; font-weight: bold; font-size: 18pt; line-height: 18pt; letter-spacing: 1px }
.windowheadblack { color: #5a5958; font-weight: bold; font-size: 18pt; line-height: 18pt; letter-spacing: 1px }
.windowheadwhite { color: white; font-weight: bold; font-size: 18pt; line-height: 18pt; letter-spacing: 1px }
.width350 { width: 350px }
.width400 { width: 400px }
.width450 { width: 450px }
.width500
width: 500px }

```


Novell Application Launcher: Managing Authentication and File System Access

23

In order to manage applications, Novell® Application Launcher™ requires access to Novell eDirectory™, the workstation's local file system, and, in some cases, a network server's file system.

The following sections provide information to help you manage the authentication and file system rights required by Application Launcher to distribute, launch, cache, and uninstall applications:

- [Section 23.1, “Novell eDirectory Authentication Overview,” on page 283](#)
- [Section 23.2, “File System Access Overview,” on page 284](#)
- [Section 23.3, “Authentication and File System Access for User-Associated Applications,” on page 285](#)
- [Section 23.4, “Authentication and File System Access for Workstation-Associated Applications,” on page 288](#)

23.1 Novell eDirectory Authentication Overview

Application Launcher authenticates to eDirectory to get information about the applications available to the logged-in user or the workstation.

Application Launcher can use the Novell Client™ to authenticate to eDirectory. Because the Novell Client uses NCP™ (NetWare® Core Protocol™) to access eDirectory, it works best for workstations that are running on a local area network inside a firewall.

If you do not have the Novell Client rolled out to workstations in your local area network, or you have users who must authenticate to eDirectory through a firewall, Application Launcher can also use the ZENworks Middle Tier Server. Novell Application Launcher uses the standard HTTP or HTTPS protocol to communicate with the ZENworks Middle Tier Server inside your firewall, which then accesses eDirectory on behalf of the user. For information about setting up a Middle Tier server, see [“Installing the ZENworks Middle Tier Server”](#) in the *Novell ZENworks 7 Desktop Management Installation Guide*.

A Note About the Application Launcher Cache

To enable users to run applications while disconnected from eDirectory, Application Launcher creates a cache directory, referred to as the NAL cache, on the local workstation.

The NAL cache contains the information required to display and launch applications. When the user is not authenticated to eDirectory, Application Launcher uses the information in the NAL cache. This means that after a user installs an application to his or her workstation, the application is available to the user regardless of whether or not he or she is authenticated to eDirectory.

You can force cache an application to the user's workstation to ensure that the application is available to the user when disconnected from eDirectory, even if it has not yet been installed. In this situation, the cache contains all the information and files required to install the application.

For more information about the cache, see [Chapter 24, “Novell Application Launcher: Managing the Cache,” on page 293](#).

23.2 File System Access Overview

During distribution, launching, caching, or uninstalling of an application, Application Launcher requires access to the local file system and might require access to network file systems such as NetWare, Linux, or Windows servers.

Local File System Access

Local file system access is provided through the logged-in Windows user account and through the Windows System user account.

For Application Launcher to work properly, the logged-in user requires the following rights:

- At least Read access to the NAL cache directory (typically, `c:\nalcache`). For more information, see [Section 24.2, “File System Rights to the NAL Cache,” on page 296](#).
- Full Control access to the user's temp directory (typically, `c:\documents and settings\username\local settings\temp`).
- Full Control access to the user's data encryption directory (typically, `c:\documents and settings\username\application data\microsoft\crypto`). This is required only if the user is using the Desktop Management Agent without a network client.
- Read\Write rights to the `HKEY_CURRENT_USER\Software\NetWare\NAL\1.0` registry key.
- Read rights to the `HKEY_LOCAL_MACHINE\Software\NetWare\NAL\1.0` registry key
- Read rights to the `HKEY_LOCAL_MACHINE\Software\Novell\ZENworks` registry key.

In addition, the System user requires full access to all areas of the workstation. By default, this access is granted to the System user as a member of the Administrators group. Do not limit the default rights given to the Administrators group or the System user account.

Network File System Access

File system access to NetWare, Linux, and Windows servers is provided through a network client, such as the Novell Client or the Client for Microsoft Networks, that supports the file system protocols (CIFS, Samba, NCP, etc.) used by the server. In general, network clients work well in a local area network environment.

If Application Launcher must access a file system through a firewall, or if you don't want to use a network client, you can use the ZENworks Middle Tier Server. The Middle Tier Server provides limited file system access to network servers. For information about setting up a Middle Tier server, see [“Installing the ZENworks Middle Tier Server”](#) in the *Novell ZENworks 7 Desktop Management Installation Guide*.

File System Access Limitations in a Clientless Environment

The ZENworks Middle Tier Server does not include the same file system access capabilities as a full network client such as the Novell Client and Microsoft Client. Although the Middle Tier Server can copy files from a network server location to a user's workstation, it does not provide the ability to

open or execute files located on a network server. Because of this limitation, the following distribution and launch issues exist when running Application Launcher in a clientless environment or an environment where the network client cannot establish the appropriate network server connection (for example, through a firewall):

- Application Launcher is not able to launch applications that reside on a network server (in other words, when the *Path to file* field on the *Run Options > Application* page points to a network location).
- Application Launcher requires MSI applications to be marked Force Cache in order to distribute them. Application Launcher copies the force cached applications to the workstation's NAL cache directory. Microsoft Windows Installer then installs the applications to the workstation from the cache.

File Path Syntax

When specifying a network file path for distributing or launching an application, you can use either mapped drives or UNC paths. The following path syntaxes are valid:

```
server\volume:path  
\\server_name\volume\path  
\\IP_address\volume\path  
volume_object_name:path  
directory_map_object_name:path  
driveletter:\path
```

If you use a mapped drive, the user's workstation must have the same drive mapping as the server from which you are running ConsoleOne.

If you use a UNC path, applications running on Windows 2000 servers might launch slowly because of the way Windows resolves UNC paths. For more information, see [Microsoft Knowledge Base Article Q150807](http://support.microsoft.com/support/kb/articles/Q150/8/07.asp) (<http://support.microsoft.com/support/kb/articles/Q150/8/07.asp>).

23.3 Authentication and File System Access for User-Associated Applications

The Application Launcher components, authentication methods, and file system access used when managing user-associated applications differ from a Windows 98 operating system to a Windows 2000/XP operating system, as explained in the following sections.

- [Section 23.3.1, “Windows 98 \(User-Associated Applications\),” on page 285](#)
- [Section 23.3.2, “Windows 2000/XP \(User-Associated Applications\),” on page 287](#)

23.3.1 Windows 98 (User-Associated Applications)

The following table lists the components, authentication method, and file system access used by Application Launcher when managing a user-associated application on a Windows 98 workstation.

Table 23-1 *Windows 98 (User-Associated Applications)*

Event	Responsible Component	eDirectory Authentication	Workstation File System Access	Network Server File System Access
Distribution	Application Launcher	eDirectory user (User object)	Windows user ¹	NetWare: Folder and file rights assigned to eDirectory user ² Windows: Permissions assigned to Active Directory user ³ Linux: Rights assigned to Samba user ⁴
Launch (normal)	Same as Distribution			
Launch (force run ⁵)	Same as Distribution			
Caching	Same as Distribution			
Uninstall	Application Launcher	eDirectory user (User object)	Windows user	Not applicable

¹ The Windows 98 operating system, unlike Windows 2000/XP, does not provide file system security for individual users. Each Windows 98 user account has full access to the local file system, which means that Application Launcher has all the file system access it requires.

² NetWare server file rights can be assigned through the Application object (*Common* tab > *File Rights* page). Any object that is associated with the Application object receives these rights. You can also directly assign rights to users through their User objects (*Rights to Files and Folder* tab > *Trustee File System Rights* page) or some other method, such as adding them to a group that has been assigned the appropriate rights.

³ Windows server file permissions must be assigned through the user's Active Directory account, which must have the same username and password as the user's eDirectory account. The user, workstation, Middle Tier Server (if used), and Windows server must be members of the same Windows domain. For information about using Novell DirXML to synchronize user account information between eDirectory and Active Directory, see “[Installing Nsure Identity Manager 2.02 Bundle Edition](#)” in “[Installing ZENworks 7 Desktop Management in a Windows Network Environment](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

⁴ Linux server file rights are assigned through Samba. The procedures for doing this depend on the Linux distribution (Open Enterprise Server Linux, SUSE Linux Enterprise Server, etc.) being used. For OES Linux and SUSE Linux Enterprise Server, see “[Configuring a Linux Server for ZENworks File Access](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*. For additional information, refer to the OES Linux and SUSE Linux Enterprise Server documentation available on the [Novell Documentation Web site \(http://www.novell.com/documentation\)](http://www.novell.com/documentation) or refer to the documentation for your Linux distribution.

⁵ The Force Run setting causes the application to automatically distribute after it becomes available. For information about configuring an application as Force Run, see “[Associations Page](#)” on [page 524](#).

23.3.2 Windows 2000/XP (User-Associated Applications)

The following table lists the components, authentication method, and file system access used by Application Launcher when managing a user-associated application on a Windows 2000/XP workstation.

Table 23-2 *Windows 2000/XP (User-Associated Applications)*

Event	Responsible Component	eDirectory Authentication	Workstation File System Access	Network Server File System Access
Distribution	NAL Service	eDirectory user	Windows System user ¹	NetWare: Folder and file rights assigned to eDirectory user ² Windows: Permissions assigned to Active Directory user ³ Linux: Rights assigned to Samba user ⁴
Launch (normal)	Application Launcher or NAL Service (when run as secure/unsecure System user ⁵)	eDirectory user	Windows user or Windows System user (when run as secure/unsecure System user)	NetWare: Folder and file rights assigned to eDirectory user Windows: Permissions assigned to Active Directory user Linux: Rights assigned to Samba user
Launch (force run ⁶)	Same as Launch (normal)			
Caching	NAL Service	eDirectory user	Windows System user	NetWare: Folder and file rights assigned to eDirectory user Windows: Permissions assigned to Active Directory user Linux: Rights assigned to Samba user
Uninstall	NAL Service	eDirectory user	Windows System user	Not applicable

¹ For Application Launcher and its associated programs (NAL Service and Workstation Helper) to work properly, the Windows System user account must have full rights to all areas of the workstation. By default, this access is granted to the System user as a member of the Administrators group. Do not limit the default rights given to the Administrators group or the System user account.

In addition, Application Launcher requires that the user's Windows account provide the following rights:

- At least Read access to the NAL cache directory (typically, `c:\nalcache`). For more information, see [Section 24.2, “File System Rights to the NAL Cache,” on page 296](#).
- Full Control access to the user's temp directory (typically, `c:\documents and settings\username\local settings\temp`).

- Full Control access to the user's data encryption directory (typically, `c:\documents and settings\username\application data\microsoft\crypto`). This is required only if the user is using the Desktop Management Agent without a network client.
- Read\Write rights to the `HKEY_CURRENT_USER\Software\NetWare\NAL\1.0` registry key.
- Read rights to the `HKEY_LOCAL_MACHINE\Software\NetWare\NAL\1.0` registry key
- Read rights to the `HKEY_LOCAL_MACHINE\Software\Novell\ZENworks` registry key.

² NetWare file system rights can be assigned through the Application object (*Common* tab > *File Rights* page). Any user who is associated with the Application object receives these rights. You can also directly assign rights to users through their User objects (*Rights to Files and Folder* tab > *Trustee File System Rights* page) or some other method, such as adding them to a group that has been assigned the appropriate rights.

³ Windows server file permissions must be assigned through the user's Active Directory account, which must have the same username and password as the user's eDirectory account. The user, workstation, Middle Tier Server (if used), and Windows server must be members of the same Windows domain. For information about using Novell DirXML to synchronize user account information between eDirectory and Active Directory, see “[Installing Nsure Identity Manager 2.02 Bundle Edition](#)” in “[Installing ZENworks 7 Desktop Management in a Windows Network Environment](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

⁴ Linux server file rights are assigned through Samba. The procedures for doing this depend on the Linux distribution (OES Linux, SUSE Linux Enterprise Server, etc.) being used. For OES Linux and SUSE Linux Enterprise Server, see “[Configuring a Linux Server for ZENworks File Access](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*. For additional information, refer to the OES Linux and SUSE Linux Enterprise Server documentation available on the [Novell Documentation Web site](#) (<http://www.novell.com/documentation>) or refer to the documentation for your Linux distribution.

⁵ The Secure System User and Unsecure System User settings apply to applications running on Windows 2000/XP only. These settings cause the application to run in the “system” space as the Windows System user rather than in the “user” space as the logged-in user. These settings are intended to ensure that users can run the application even if they have limited access rights to the workstation's file system. For more information, see “[Environment Page](#)” on [page 512](#).

⁶ The Force Run setting causes the application to automatically distribute after it becomes available. For information about configuring an application as Force Run, see “[Associations Page](#)” on [page 524](#).

23.4 Authentication and File System Access for Workstation-Associated Applications

The Application Launcher components, authentication methods, and file system access used when managing workstation-associated applications differ from a Windows 98 operating system to a Windows 2000/XP operating system, as explained in the following sections:

- [Section 23.4.1, “Windows 98 \(Workstation-Associated Applications\),” on page 289](#)
- [Section 23.4.2, “Windows 2000/XP \(Workstation-Associated Applications\),” on page 290](#)

23.4.1 Windows 98 (Workstation-Associated Applications)

The following table lists the components, authentication method, and file system access used by Application Launcher when managing a workstation-associated application on a Windows 98 workstation.

Table 23-3 *Windows 98 (Workstation-Associated Applications)*

Event	Responsible Component	eDirectory Authentication	Workstation File System Access	Network Server File System Access
Distribution	Workstation Helper	eDirectory workstation (Workstation object)	Windows user ¹	NetWare: Folder and file rights assigned to eDirectory workstation ² Windows: Permissions assigned to Active Directory user ³ Linux: Rights assigned to Samba user ⁴
Launch (normal)	Same as Distribution.			
Launch (force run ⁵)	Workstation Helper	eDirectory workstation (Workstation object)	Windows user	NetWare: Folder and file rights assigned to eDirectory workstation Windows: Permissions assigned to Active Directory user Linux: Rights assigned to Samba user
Caching	Same as Launch (force run).			
Uninstall	Workstation Helper	eDirectory workstation (Workstation object)	Windows user	Not applicable

¹ The Windows 98 operating system, unlike Windows 2000/XP, does not provide file system security for individual users. Each Windows 98 user account has full access to the local file system, which means that Application Launcher and Workstation Helper have all the file system access they require.

² NetWare file system rights can be assigned through the Application object (*Common* tab > *File Rights* page). Any workstation that is associated with the Application object receives these rights. You can also directly assign rights to workstations through their Workstation objects (*Rights to Files and Folder* tab > *Trustee File System Rights* page) or some other method, such as adding them to a workstation group that has been assigned the appropriate rights.

³ Windows server file permissions must be assigned through the user's Active Directory account, which must have the same username and password as the user's eDirectory account. The user, Middle Tier Server (if used), and Windows server must be members of the same Windows domain. For information about using Novell DirXML to synchronize user account information between eDirectory and Active Directory, see [“Installing Nsure Identity Manager 2.02 Bundle Edition”](#) in

“Installing in a Windows Network Environment” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

Note that this is different than for a workstation-associated application distributed to a Windows 2000/XP workstation (see “Windows 2000/XP (Workstation-Associated Applications)” on page 290). Windows 98 does not differentiate between the user and the workstation (system), so the user credentials must be used for login, not the workstation credentials. If access to the Windows server is being provided through the ZENworks Middle Tier Server, the Domain User account used by the Middle Tier Server must be assigned the appropriate permissions.

⁴ Linux server file rights are assigned through Samba. The procedures for doing this depend on the Linux distribution (OES Linux, SUSE Linux Enterprise Server, etc.) being used. For OES Linux and SUSE Linux Enterprise Server, see “Configuring a Linux Server for ZENworks File Access” in the *Novell ZENworks 7 Desktop Management Installation Guide*. For additional information, refer to the OES Linux and SUSE Linux Enterprise Server documentation available on the [Novell Documentation Web site \(http://www.novell.com/documentation\)](http://www.novell.com/documentation) or refer to the documentation for your Linux distribution.

⁵ The Force Run setting causes the application to automatically distribute after it becomes available. For information about configuring an application as Force Run, see “Associations Page” on page 524.

23.4.2 Windows 2000/XP (Workstation-Associated Applications)

The following table lists the components, authentication method, and file system access used by Application Launcher when managing a workstation-associated application on a Windows 2000/XP workstation.

Table 23-4 *Windows 2000/XP (Workstation-Associated Applications)*

Event	Responsible Component	eDirectory Authentication	Workstation File System Access	Network Server File System Access
Distribution	NAL Service	eDirectory workstation (Workstation object)	Windows System user ¹	NetWare: Folder and file rights assigned to eDirectory workstation ² Windows: Permissions assigned to Active Directory workstation ³ Linux: Rights assigned to workstation through Samba ⁴

Event	Responsible Component	eDirectory Authentication	Workstation File System Access	Network Server File System Access
Launch (normal)	Application Launcher or NAL Service (when run as secure/unsecure System user ⁵)	eDirectory workstation (Workstation object)	Windows user or Windows System user (when run as secure/unsecure System user)	NetWare: Folder and file rights assigned to eDirectory user or folder and file rights assigned to eDirectory workstation (when run as secure/unsecure System user) Windows: Permissions assigned to Active Directory user or permissions assigned to Active Directory workstation (when run as secure/unsecure System user) Linux: Rights assigned to Samba user or rights assigned to workstation (when run as secure/unsecure System user)
Launch (force run ⁶)	NAL Service	eDirectory workstation (Workstation object)	Windows System user	NetWare: Folder and file rights assigned to eDirectory workstation Windows: Permissions assigned to Active Directory workstation Linux: Rights assigned to workstation through Samba
Caching	NAL Service	eDirectory workstation (Workstation object)	Windows System user	NetWare: Folder and file rights assigned to eDirectory workstation Windows: Permissions assigned to Active Directory workstation Linux: Rights assigned to workstation through Samba
Uninstall	NAL Service	eDirectory workstation (Workstation object)	Windows System user	Not applicable

¹ For Application Launcher and its associated programs (NAL Service and Workstation Helper) to work properly, the Windows System user account must have full rights to all areas of the workstation. By default, this access is granted to the System user as a member of the Administrators group. Do not limit the default rights given to the Administrators group or the System user account.

In addition, Application Launcher requires that the Windows user account provide the following rights:

- At least Read access to the NAL cache directory (typically, `c:\nalcache`). For more information, see [Section 24.2, “File System Rights to the NAL Cache,” on page 296](#).
- Full Control access to the user's temp directory (typically, `c:\documents and settings\username\local settings\temp`).
- Full Control access to the user's data encryption directory (typically, `c:\documents and settings\username\application data\microsoft\crypto`). This is required only if the user is using the Desktop Management Agent without a network client.

- Read\Write rights to the HKEY_CURRENT_USER\Software\NetWare\NAL\1.0 registry key.
- Read rights to the HKEY_LOCAL_MACHINE\Software\NetWare\NAL\1.0 registry key
- Read rights to the HKEY_LOCAL_MACHINE\Software\Novell\ZENworks registry key.

² NetWare server file rights can be assigned through the Application object (*Common* tab > *File Rights* page). Any workstation that is associated with the Application object receives these rights. You can also directly assign rights to workstations through their Workstation objects (*Rights to Files and Folder* tab > *Trustee File System Rights* page) or some other method, such as adding them to a workstation group that has been assigned the appropriate rights.

³ Windows server file permissions must be assigned through the workstation's Active Directory account. The workstation, Middle Tier Server (if used), and Windows server must be members of the same Windows domain. Note that this is different than for a workstation-associated application distributed to a Windows 98 workstation (see “[Windows 98 \(Workstation-Associated Applications\)](#)” on page 289). Windows 98 does not differentiate between the user and the workstation (system), so the user credentials must be used for login, not the workstation credentials. If access to the Windows server is being provided through the ZENworks Middle Tier Server, the Domain User account used by the Middle Tier Server must be assigned the appropriate permissions.

⁴ Linux server file rights are assigned through Samba. The workstation (not the logged-in user) must have rights to read files from the Linux server's Samba share. The procedures for assigning rights depend on the Linux distribution (OES Linux, SUSE Linux Enterprise Server, etc.) being used. For OES Linux and SUSE Linux Enterprise Server, see “[Configuring a Linux Server for ZENworks File Access](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*. For additional information, refer to the OES Linux and SUSE Linux Enterprise Server documentation available on the [Novell Documentation Web site \(http://www.novell.com/documentation\)](http://www.novell.com/documentation) or refer to the documentation for your Linux distribution.

⁵ The Secure System User and Unsecure System User settings cause the application to run in the "system" space as the Windows System user rather than in the "user" space as the logged-in user. These settings are intended to ensure that users can run the application even if they have limited access rights to the workstation's file system. For more information, see “[Environment Page](#)” on page 512.

⁶ The Force Run setting causes the application to automatically distribute after it becomes available. For information about configuring an application as Force Run, see “[Associations Page](#)” on page 524.

Novell Application Launcher: Managing the Cache

24

Novell® Application Launcher™ creates a cache directory, referred to as the NAL cache, on the workstation's Windows system drive (the drive containing the `system32` directory). The NAL cache enables Application Launcher to do the following:

- Display, launch, install, and fix applications when the user or workstation is not authenticated to Novell eDirectory™.
- Uninstall applications it has installed to the workstation.
- Delay reading eDirectory during startup in order to minimize network traffic during peak user login times.
- Resume downloading of an application's files and information while in remote mode, rather than starting over on the download.
- Reduce network traffic by minimizing the number of times it accesses eDirectory for application information.

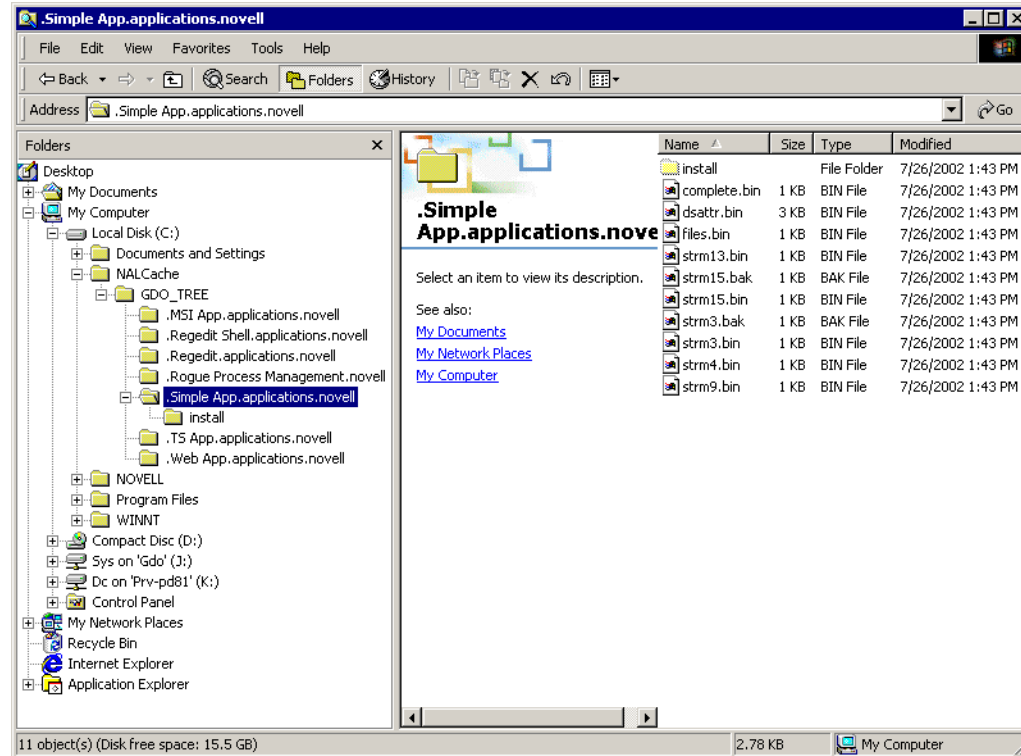
The following sections provide detailed information about the contents of the NAL cache and tasks to help you manage the NAL cache:

- [Section 24.1, “NAL Cache Structure and Content,” on page 294](#)
- [Section 24.2, “File System Rights to the NAL Cache,” on page 296](#)
- [Section 24.3, “Caching an Application,” on page 297](#)
- [Section 24.4, “Changing the Cache Location,” on page 298](#)
- [Section 24.5, “Disabling the Cache,” on page 300](#)

24.1 NAL Cache Structure and Content

By default, the NAL cache directory is created as a hidden `\nalcache` directory at the root of the drive, as shown in the following example.

Figure 24-1 NAL Cache Directory on a Local Drive



When an application is associated with the user or workstation, Application Launcher creates a directory for the application under the `\nalcache` directory. The application's directory is named the same as the Application object's eDirectory distinguished name (for example, Simple App.applications.novell) and contains the files that make up the launch cache and install cache. These two caches are described in the following sections:

- [Section 24.1.1, "Launch Cache," on page 294](#)
- [Section 24.1.2, "Install Cache," on page 296](#)

24.1.1 Launch Cache

The files in an application's launch cache contain the information Application Launcher needs to launch, run, and uninstall the application. Application Launcher automatically creates the application's launch cache when the application is distributed to the workstation. If Application Launcher has not yet distributed the application to the workstation, the launch cache contains only the information needed to display the application's icon on the workstation's desktop.

The launch cache files are located directly under the application directory (`\nalcache\edirectory_tree\app_object` directory). The following table describes the launch cache files. Depending on the Application object's settings, some of the files might not be necessary, in which case they are not included in the launch cache.

Table 24-1 *Launch Cache*

File	Description
complete.bin	Contains the Application object's complete eDirectory name. If this file does not exist, Application Launcher assumes that the cache is bad and recreates the cache.
dsattr.bin	Contains all of the Application object's eDirectory attributes.
delta.bin	Flags the cache as a delta cache. This means the cache contains only the information required by Application Launcher to display the application's icon on the desktop, and exists only if Application Launcher has not yet distributed the application to the workstation. After Application Launcher distributes the application, it removes this file.
files.bin	Contains the file vitals for the cache files.
folders.bin	Contains the list of Application Launcher window folders and Start menu folders where the Application object displays.
strm1.bin	Contains the Application object's icon.
strm2.bin	Contains all text file modifications.
strm3.bin ¹	Contains all files to be copied to the workstation.
strm4.bin ¹	Contains registry modifications that are made during initial distribution.
strm5.bin ¹	Contains INI modifications that are made during initial distribution.
strm6.bin ¹	Contains shortcut modifications that are made during initial distribution.
strm7.bin	Contains macro information.
strm8.bin	Contains schedule information.
strm9.bin	Contains system requirements information.
strm10.bin	Contains Administrator notes.
strm11.bin	Contains the shutdown script.
strm12.bin	Contains the startup script.
strm13.bin ¹	Contains registry modifications to be made each time the application is launched.
strm14.bin ¹	Contains INI modifications to be made each time the application is launched.
strm15.bin ¹	Contains files to be copied to the workstation each time the application is launched.
strm16.bin	Contains text file modifications to be made each time the application is launched.
strm17.bin ¹	Contains icons to be modified each time the application is launched.
strm18.bin	Contains environment variable settings to be made.
strm19.bin	Contains the pre-distribution script.
strm20.bin	Contains the post-distribution script.

File	Description
strm21.bin	Contains the pre-install schedule information.

¹ All files except those containing application files, INI settings, shortcut icons, and registry settings are refreshed each time Application Launcher performs a timed or manual refresh. The non-refreshed files remain the same until the version number (Application object > *Distribution Options* tab > *Options* page) is changed. This allows Application Launcher to successfully uninstall the application (including the files, INI settings, shortcuts, and registry settings) if necessary.

24.1.2 Install Cache

The install cache contains the application source files needed to install or verify (fix) the application. Application Launcher creates an install cache for an application in the following two situations:

- The application is marked as Force Cache. Application Launcher retains the install cache for a Force Cache application as long as the application is associated with the user or workstation.
- The application is not marked as Force Cache, but Application Launcher is running in Remote Mode and the application is launched. In this case, Application Launcher first copies the application to the install cache and then distributes it (which populates the launch cache). After the application is launched, Application Launcher removes its install cache.

The install cache is created in the `nalcache\edirectory_tree\app_object\install` directory.

Although the files in the install cache are compressed, they can still require a large amount of disk space on the workstation's local drive, so an application should only be cached if users need to install or verify the application while disconnected from eDirectory.

An application can still run in disconnected mode without being cached to the install cache. To run in disconnected mode, an application needs only to have been distributed (installed) on the workstation. Caching an application to the install cache only enables the application to be installed or verified (fixed) while in disconnected mode.

24.2 File System Rights to the NAL Cache

Prior to ZENworks 6.5 Support Pack 1 (SP1), the ZENworks Desktop Management Agent installation program created the NAL cache directory (typically, `c:\nalcache`) and automatically assigned the user Full Control access.

As a result, if you installed the Desktop Management Agent on a workstation, even a locked-down workstation, the installation program created the NAL cache directory and assigned Full Control access, which allowed Novell Application Launcher to access the NAL cache without further modifications to file system rights.

Beginning with ZENworks 6.5 SP1, the ZENworks Desktop Management Agent installation program no longer assigns the user any file system rights to the NAL cache directory (typically, `c:\nalcache`). Instead, the NAL cache directory inherits whatever rights are assigned to the root of the drive, assuming you use the default location (`c:\nalcache`). In order for users to be able to access the NAL cache, they need at least Read rights to the NAL cache directory.

As a result of this change, consider the following:

- When you install the ZENworks 7 Desktop Management Agent on workstations that had the ZENworks 6.5 (or earlier) Desktop Management Agent installed at one time, you should not experience any NAL cache file system access problems. The original installation created the NAL cache directory with Full Control rights, and the upgrade continues using these same rights.
- When you install the ZENworks 7 Desktop Management Agent on a workstation that has not had the ZENworks 6.5 (or earlier) Desktop Management Agent installed at one time, the installation program does not assign any file system rights to the NAL cache directory; it inherits whatever rights are assigned to the root of the drive.

As a result, users might experience problems accessing the NAL cache on locked-down workstations. For example, if users do not have at least Read rights to the root of the drive, they cannot access the NAL cache directory and Novell Application Launcher cannot use the cache.

- If you manually created the NAL cache directory and assigned rights before installing the ZENworks 7 Desktop Management Agent or if you changed rights to an existing directory, these rights remain in effect after installation. Be aware that the user needs at least Read rights to the NAL cache, or Novell Application Launcher cannot use the cache.

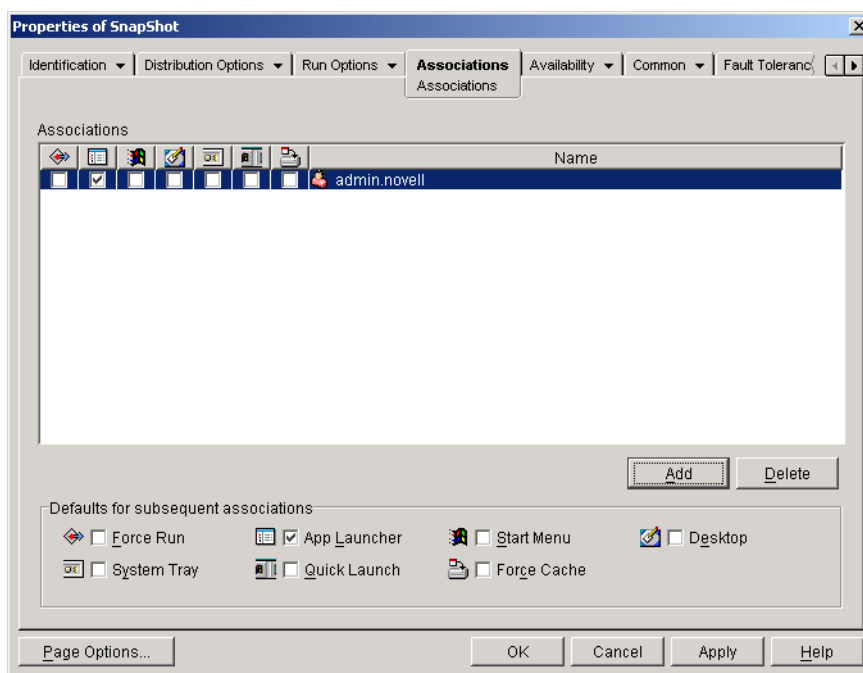
24.3 Caching an Application

Applications are not cached by default. If you want to enable a user to install or verify an application while disconnected from eDirectory, you must configure the application to be cached.

- 1 In ConsoleOne®, right-click the Application object, then click *Properties*.
- 2 Click the *Identification* tab to display the Icon page.
- 3 Make sure the *Disconnectable* box is selected.

In order to cache an application, it must be marked as Disconnectable. If the application is not marked as Disconnectable, the Force Cache option is not available.

- 4 Click the *Associations* tab to display the Associations page.



- 5 In the Associations list, select the *Force cache* box for the user whose workstation you want to cache the application to.

NOTE: If the application is marked as Distribute Always (Distribution Options tab > Options page) and Application Launcher is running in remote mode, Application Launcher behaves as if the Force Cache and Check Point Restart options are enabled regardless of their actual settings.

- 6 Click *OK* to save the changes.

The application is cached to the user's local drive the next time Application Launcher restarts or refreshes.

The same task can be accomplished through the *ZENworks* tab > *Applications* page on a User, Workstation, Group, Workstation Group, or container object.

24.4 Changing the Cache Location

As mentioned in [Section 24.1, “NAL Cache Structure and Content,” on page 294](#), the default cache is created as a hidden directory (`\nalcache`) on the root of the workstation's Windows drive.

You can change the cache location by modify the workstation's registry. The next time Application Launcher refreshes (either a timed refresh, a manual refresh, or a restart), the cache is created in the new location. The old cache directory is not removed automatically.

To change the location of the cache directory:

- 1 Use `regedit.exe` to open the Windows registry.
- 2 Locate the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\NetWare\NAL\1.0
```

- 3 Add a new String value to the key using the following information:

Value type: String

Value name: MasterCache

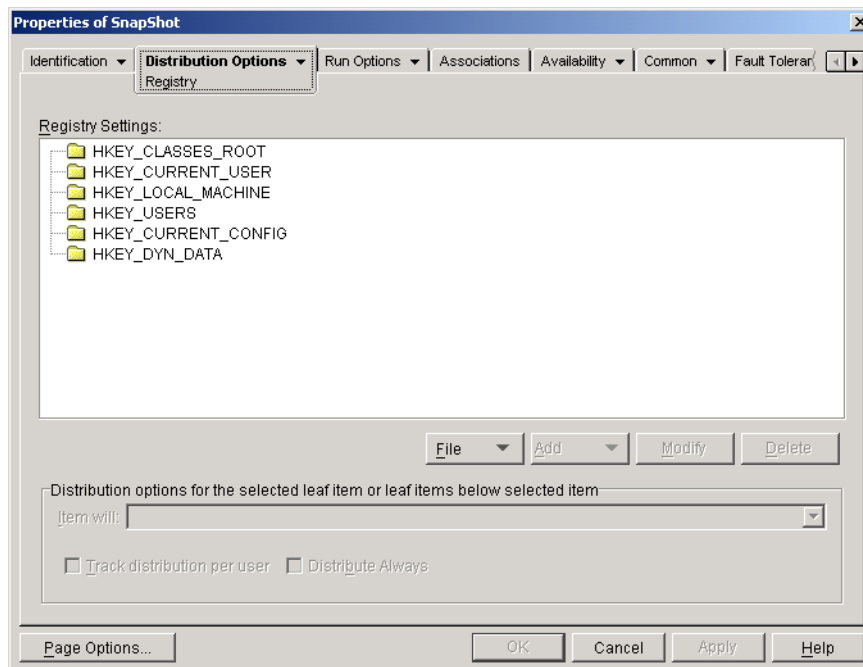
Value data: Specify the directory you want to use for the cache. To avoid having the cache files and subdirectories mixed in with other files and directories, you might want to specify an empty directory. For example, if you want the cache located under the `c:\novell` directory, you might want to specify `c:\novell\nalcache` rather than just `c:\novell`. Do not use macros in this field; macros are not supported.

- 4 Save the registry changes.
- 5 Refresh or restart Application Launcher.

Using Application Launcher to Change the Cache Location

You can also use Application Launcher to change the cache location. To do so:

- 1 In ConsoleOne, create a simple Application object. For instructions, see [Chapter 28, "Distribution: Simple Applications,"](#) on page 315.
- 2 Right-click the Application object, then click *Properties* to display the object's property pages.
- 3 Click *Distributions Options > Registry* to display the Registry page.



- 4 Add the following registry key:
`HKEY_LOCAL_MACHINE\SOFTWARE\NetWare\NAL\1.0`
- 5 Add a new String value to the key using the following information:

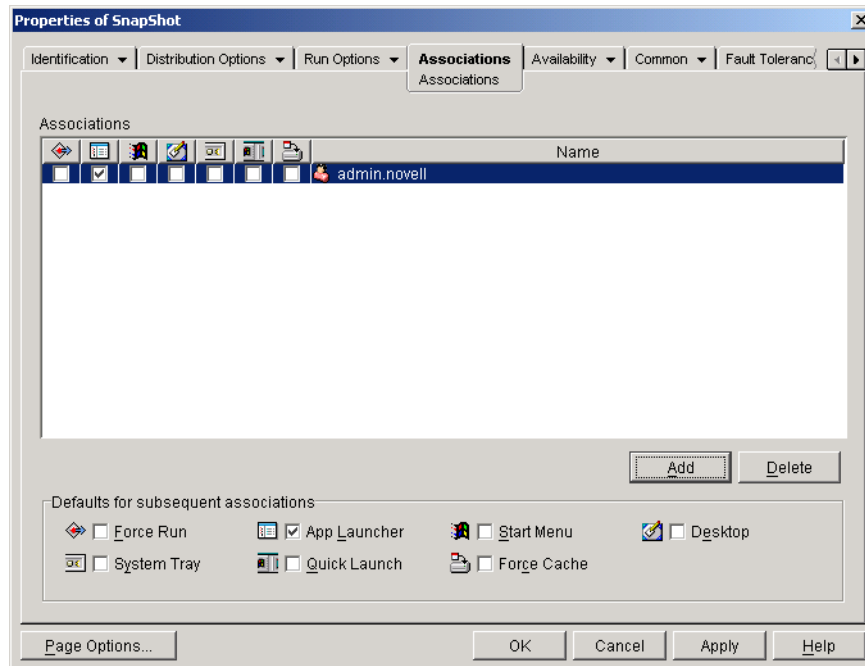
Value type: String

Value name: MasterCache

Value data: Specify the directory you want to use for the cache. To avoid having the cache files and subdirectories mixed in with other files and directories, you might want to specify an

empty directory. For example, if you want the cache located under the `c:\novell` directory, you might want to specify `c:\novell\ナルcache` rather than just `c:\novell`. Do not use macros in this field; macros are not supported.

- 6 Click *Associations* to display the Associations page.



- 7 Add the users who you want the changes distributed to.
- 8 For each user association, select the *Force run* option to have the change made without requiring user intervention.
- 9 Click *OK* to save the information.

24.5 Disabling the Cache

You can disable the cache by turning off Application Launcher's ability to write application information to it. If you choose to disable the cache, please be aware of the following:

- The primary purpose of the cache is to enable users to work offline, disconnected from eDirectory. Disabling the cache forces users to be connected to eDirectory or a removable cache in order to access applications. To ensure that users don't manually go offline, the Work Offline feature in Application Launcher is disabled when the cache is disabled.
- The uninstall, random refresh, and checkpoint restart features do not work. These features rely on Application Launcher having access to the cache.

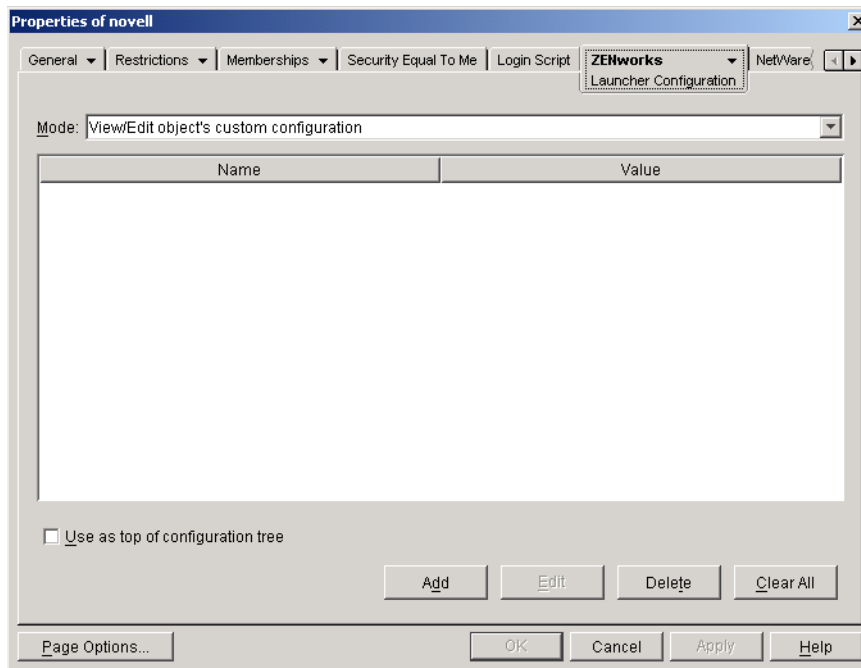
To disable the cache:

- 1 In ConsoleOne, select a container object if you want to disable the cache for all users in the container.

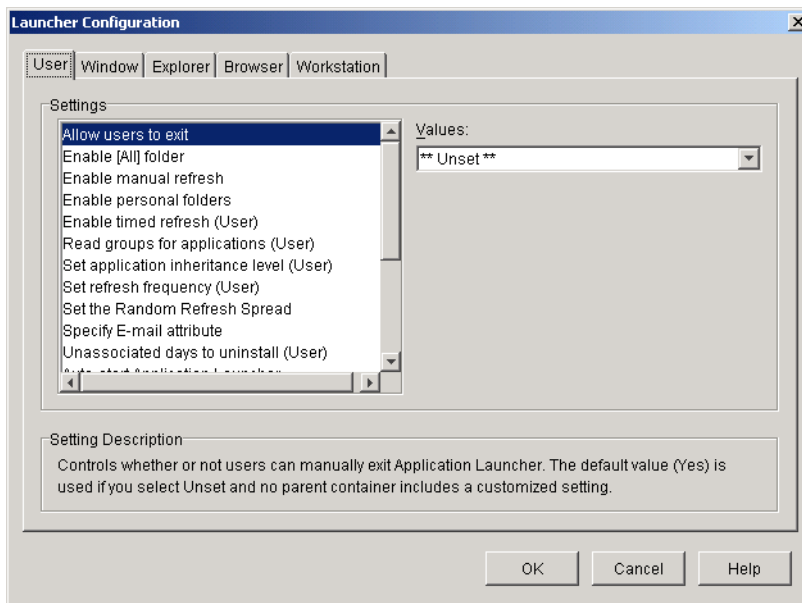
or

Select a User object if you want to disable the cache for an individual user.

- 2 Right-click the object, then click *Properties* to display the object's property pages.
- 3 Click the *ZENworks* tab, then click *Launcher Configuration* to display the Launcher Configuration page.



- 4 Click *Add* to display the Launcher Configuration Settings page.



- 5 In the Settings list on the User or Workstation tab, select the *Enable writing to the cache* option.

NOTE: The *Enable writing to the cache* option is available on both the User and Workstation tabs. You should use the appropriate tab, depending on whether you want to disable writing to

the cache for user-associated applications or for workstation-associated applications. If you want to disable the cache for both user-associated and workstation-associated applications, you should perform the steps in this section on both the User and Workstation tabs.

6 In the *Values* field, select *No*.

7 Click *OK* to save the change.

The change is applied the next time Application Launcher restarts or refreshes.

Novell Application Launcher: Organizing Applications

25

Novell® ZENworks® Desktop Management enables you to organize Application objects into folders. Folders show up in the Novell Application Launcher™ windows (Application Window, Application Explorer window, and Application Browser window) and on the Windows Start menu.

The following sections provide information about the different types of folders available for organizing applications, instructions for creating an Application Folder object, and instructions for adding Application objects to application folders or custom folders:

- [Section 25.1, “Types of Folders,” on page 303](#)
- [Section 25.2, “Creating and Deleting Application Folders,” on page 304](#)
- [Section 25.3, “Adding Applications to Application Folders,” on page 305](#)
- [Section 25.4, “Adding Applications to Custom Folders,” on page 307](#)

25.1 Types of Folders

There are four types of folders used to organize applications:

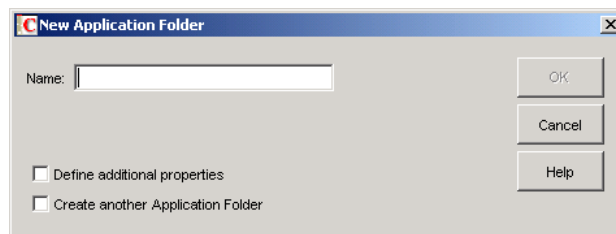
- **Application folder (administrator created):** An application folder is created as a Novell eDirectory™ object. A single Application Folder object can consist of one folder or multiple folders (a multi-level folder structure). After you create an Application Folder object, you can add any number of Application objects to the folder (or folders). Application Folder objects are the recommended folder type if you want to maintain consistent folders from user to user. For information about creating Application Folder objects, see [Section 25.2, “Creating and Deleting Application Folders,” on page 304](#). For information about adding applications to an application folder, see [Section 25.3, “Adding Applications to Application Folders,” on page 305](#).
- **Custom folder (administrator created):** A custom folder is created specifically for a single Application object in eDirectory. No other Application objects can be included in the folder. Custom folders support folders within folders, which means that you can create a custom folder structure. For example, although you could not have Calculator and Notepad in the same custom folder, you could create two subfolders within the same custom folder and place the two programs in the two subfolders (in other words, `winapps\calculator\calc.exe` and `winapps\notepad\notepad.exe`). For information about creating custom folders for an application, see [Section 25.4, “Adding Applications to Custom Folders,” on page 307](#).
- **Personal folder (user created):** A personal folder is created in Application Launcher by individual users. Users can move Application objects from other folders into the personal folder. By default, the ability to create personal folders is disabled. For information about enabling this feature, see [“Novell Application Launcher: Configuring Settings” on page 255](#).
- **System folder (system created):** A system folder is automatically created by Application Launcher to store an Application object if the object has not been added to an application folder or a custom folder.

If the Application object is associated with a user, the Application object's system folder is given the name specified in the User object's Full Name field (for example, John Smith). If the

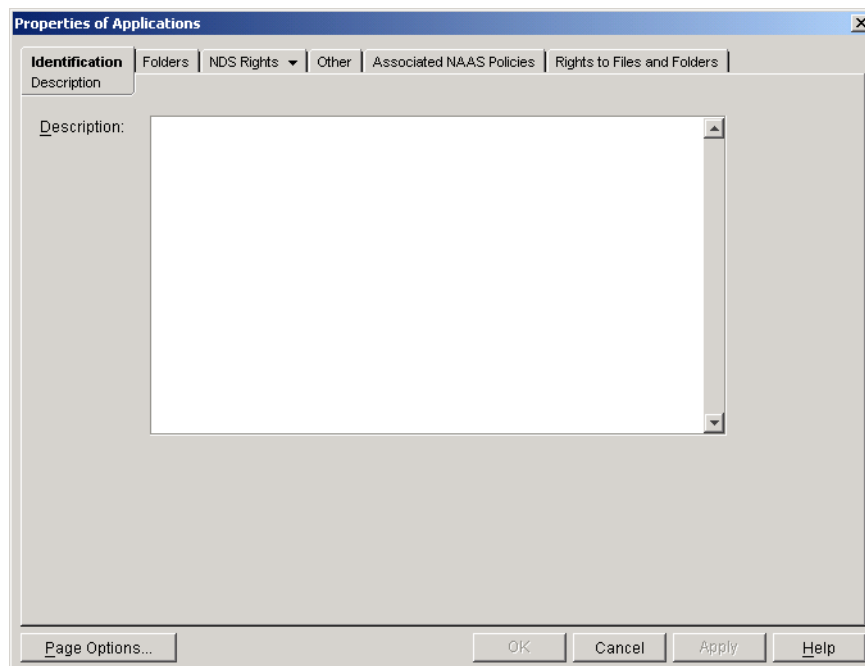
Application object is associated with another eDirectory object (Group, Workstation, container, and so forth), the system folder is given the name specified in the object's Description field (for example, System Test Group). If nothing is specified in the Full Name or Description field, the system folder is given the object's fully distinguished name. For example, an Application object associated with a user through his or her User object would be placed in a system folder that has the user's fully distinguished name, but an Application object associated with a user through a group would be placed in a folder that has the group's fully distinguished name.

25.2 Creating and Deleting Application Folders

- 1 In ConsoleOne®, right-click the container where you want to create the Application Folder object, click **New**, then click **Object** to display the New Object dialog box.
- 2 Select *Application folder*, then click **OK** to display the New App:Folders dialog box.

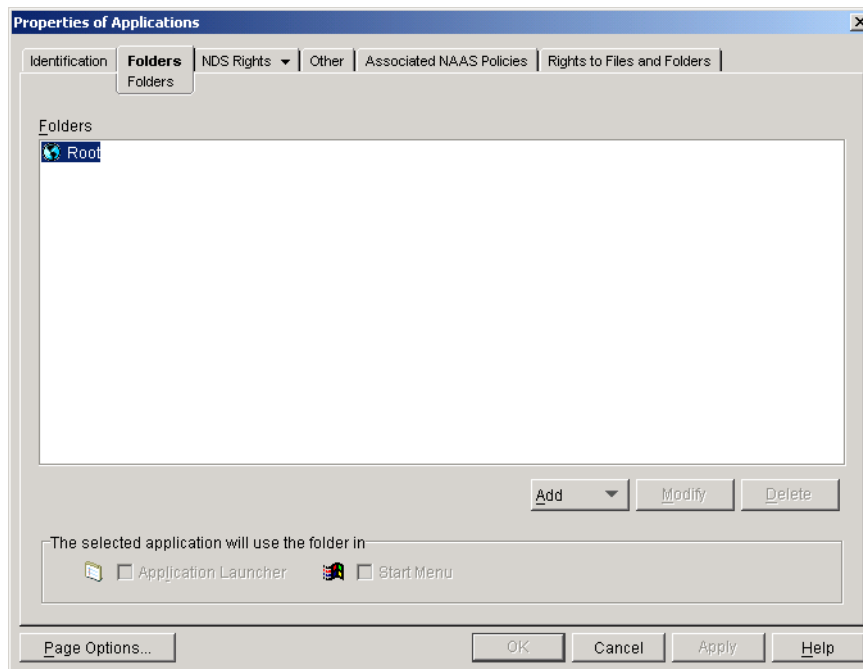


- 3 In the *Name* field, specify a name for the object. The name is displayed only in eDirectory and does not need to be the same name as the one you want to appear in the Application Launcher window and on the Start menu on the users' workstations.
- 4 Select the *Define additional properties* check box, then click **OK** to display the Application Folder object's Description page.



- 5 If desired, enter a description in the Description box.

- 6 Click the *Folders* tab to display the Folders page.



The Folders tree contains one entry called Root. Root represents the Windows Start menu and the Application Launcher window.

- 7 Use the *Add*, *Modify*, and *Delete* options to create the folder structure you want.

Add: To add a folder, select the folder (or Root) where you want to create a new folder, click *Add*, click *Folder*, type the name for the new folder, then press Enter.

The following characters are invalid when used in Windows folder and file names:

\ / : * ? " < > |

If you use any of these characters in the folder name, they are replaced by an underscore (_).

Modify: To change the name of a folder, select the folder in the Folders tree, click *Modify*, type the new folder name, then press Enter.

Delete: To remove a folder, select the folder in the Folders tree, then click *Delete*. The change is applied the next time Application Launcher restarts.

- 8 Click *OK* when you are finished creating the folder structure.
- 9 To add applications to your folders, continue with [Section 25.3, “Adding Applications to Application Folders,”](#) on page 305.

25.3 Adding Applications to Application Folders

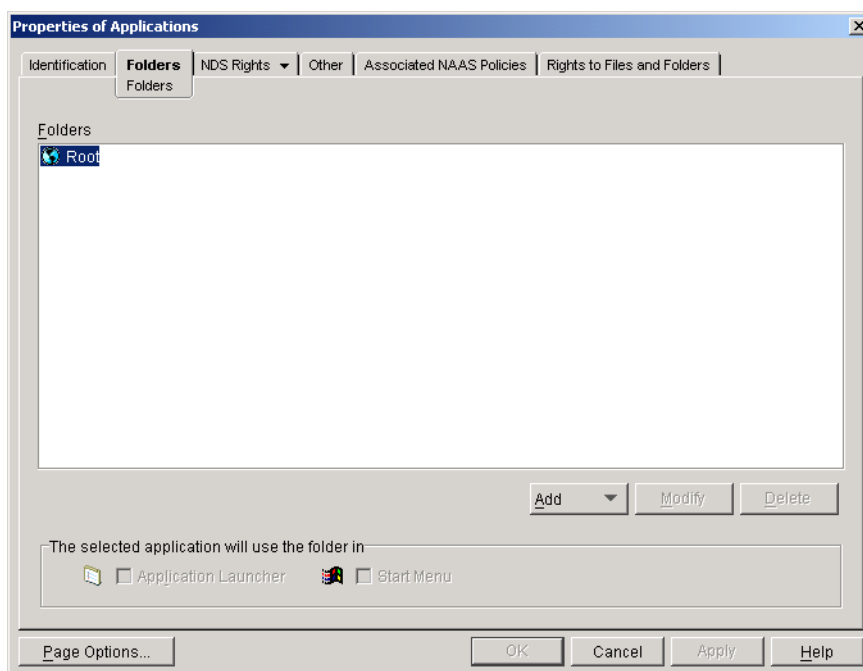
There are two ways you can add Application objects to application folders. You can add Application objects through the Folders page on the Application Folder object, or you can link individual Application objects through the Folders page on the Application object. Using the Application Folder object enables you to add multiple Application objects to the application folder at one time. Using the Application object enables you to add the single Application object only.

- [Section 25.3.1, “Using the Application Folder Object to Add Applications,”](#) on page 306

- [Section 25.3.2, “Using the Application Object to Add the Application to a Folder,”](#) on page 306

25.3.1 Using the Application Folder Object to Add Applications

- 1 In ConsoleOne, right-click the Application Folder object you want to add the Application object to, then click *Properties*.
- 2 Click the *Folders* tab to display the Folders page.

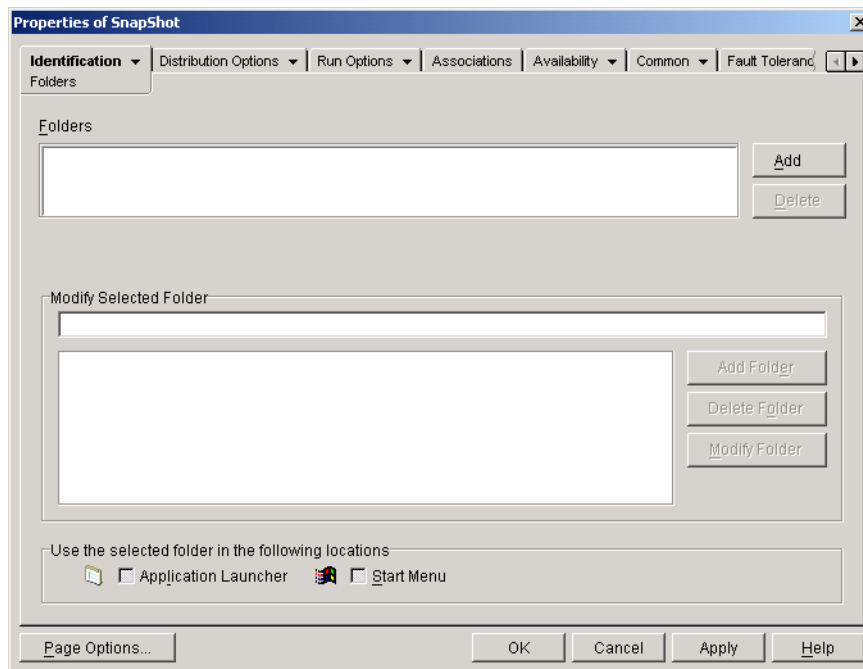


- 3 In the Folders tree, select the folder where you want to add the Application object.
- 4 Click *Add*, click *Application*, browse for and select the desired Application object, then click *OK* to add it to the folder in the folders list.
- 5 When finished adding Application objects, click *OK* to save your changes.

25.3.2 Using the Application Object to Add the Application to a Folder

- 1 In ConsoleOne, right-click the Application object you want to add to a folder, then click *Properties*.

- 2 Click the *Identification* tab > *Folders* to display the Folders page.



- 3 Click the *Add* button > *Linked folder* to display the Select Object dialog box.
- 4 Browse for and select the Application Folder object you want to add the Application object to, then click *OK* to display the Folder Object Structure dialog box.
- 5 Select the folder you want to add the Application object to, then click *OK* to add it to the Folders list.

If you select the Root folder, the Application object is displayed directly on the Start menu and at the root of the Application Launcher window.

By default, the Application object is displayed in the selected folder on the Start menu and the Application Launcher window.

- 6 In the Use the Selected Folder in the Following Locations box, deselect Application Launcher if you don't want the Application object included in that folder in the Application Launcher window and deselect Start Menu if you don't want the Application object included in that folder on the Windows Start menu.

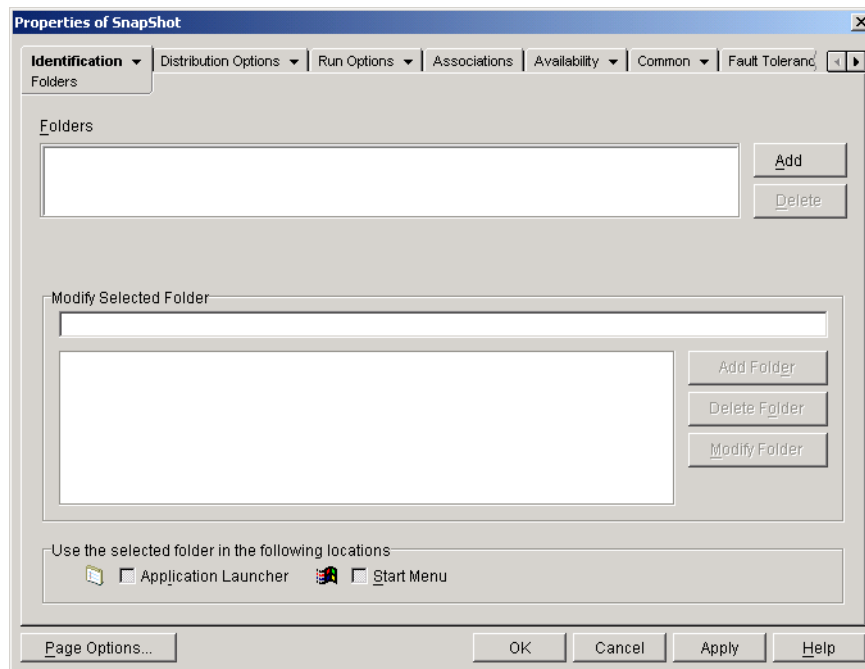
A folder displays in the Application Launcher window and on the Start menu only if it contains an Application object. If no Application objects have been linked to the folder, it is not displayed.

- 7 Click *OK* to save the changes.

25.4 Adding Applications to Custom Folders

- 1 In ConsoleOne, right-click the Application object you want to add to a folder, then click *Properties*.

- 2 Click the *Identification* tab > *Folders* to display the Folders page.



- 3 Click the *Add* button > *Custom folder* to add a New Folder entry to the Folders list.
- 4 In the Modify Selected Folder list, select the New Folder entry, click *Modify Folder*, type a name for the folder, then press Enter.
- 5 If you want to add subfolders, select the folder, click *Add Folder*, type a name for the subfolder, then press Enter.
When you add subfolders, the Application object is displayed in the lowest-level folder.
- 6 Click *OK* to save the changes.

ZENworks Launch Gadget: Configuring Settings

26

Novell® ZENworks® Desktop Management includes the ZENworks Launch gadget that can be used to launch user-associated applications from within a Novell exteNd Director™ 4.1 SE portal. If you have not installed the Launch gadget but are interested in using it, see “[Installing the ZENworks Launch Gadget](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

The Launch gadget includes several settings you can use to configure how the gadget works. To configure the settings:

- [Section 26.1, “Modifying Gadget Configuration Settings,” on page 309](#)
- [Section 26.2, “Adding Citrix MetaFrame Servers to the Portal,” on page 311](#)

26.1 Modifying Gadget Configuration Settings

Within the exteNd Director portal administration utility, there are two places that you can modify the Launch gadget configuration settings: the ZENworks Applications page and the ZENworks Launch gadget object.

- **ZENworks Applications page:** The Launch gadget installation creates a ZENworks Applications page and assigns the Launch gadget (OD_ZenLaunchGadget) to the page. You can modify the gadget configuration settings for the ZENworks Application page, the modifications apply only to the gadget on that page. If you assign the gadget to another page, the modifications are not applied to that page. For instructions, see “[Configuring Gadget Settings on the ZENworks Application Page](#)” on page 309.
- **Launch gadget object:** You can modify configuration settings on the Launch gadget object if you want the settings applied to all pages the gadget is assigned to. For instructions, see “[Configuring Gadget Settings on the Launch Gadget Object](#)” on page 310.

26.1.1 Configuring Gadget Settings on the ZENworks Application Page

- 1 Log in to the portal as a portal administrator.
- 2 Click *Administer the portal*.
- 3 Click *Pages*.
- 4 Select the ZENworks Application page, then click *Edit*.
- 5 In the gadget assignments list, select *ZENworks applications*, then click *Edit* to display the Gadget Assignment Configuration page.
- 6 Modify the configuration settings. For a description of each setting, see “[ZENworks Launch Gadget \(OD_ZENLaunchGadget\) Settings](#)” on page 310.

26.1.2 Configuring Gadget Settings on the Launch Gadget Object

- 1 Log in to the portal as a portal administrator.
- 2 Click *Administer the portal*.
- 3 Click *Gadgets*.
- 4 Select *OD_ZENLaunchGadget*, then click *Edit*.
- 5 Click *Configuration* to display the Gadget Configuration page.
- 6 Modify the configuration settings. For a description of each setting, see “ZENworks Launch Gadget (OD_ZENLaunchGadget) Settings” on page 310

26.1.3 ZENworks Launch Gadget (OD_ZENLaunchGadget) Settings

The Launch gadget has the following configuration settings:

Display name: Specifies the name used when displaying the gadget on the portal page. This field is available only if you are editing a gadget assignment rather than the gadget object.

Window height: Specifies the height of the window that lists the applications. If the application list is too long to fit in the window, the window provides a vertical scroll bar. The default setting is 198 pixels.

Novell Client authentication host server: Specifies the IP address or DNS host name of the server to be used when authenticating to eDirectory through the Novell Client™. This setting overrides (and changes) the user's current Novell Client configuration setting.

XTier authentication host server: Specifies the IP address or DNS host name of the server where the ZENworks Middle Tier server is installed. The Middle Tier servers enables access to Novell eDirectory without the Novell Client. This setting overrides (and changes) the user's current Middle Tier server configuration setting.

XTier port: Specifies the number of the Middle Tier server. This setting overrides (and changes) the user's current Middle Tier server configuration setting.

Display thin-client applications: Specifies whether or not to display terminal server applications in the list. The default is *TRUE*.

Display workstation installed applications: Specifies whether or not to display desktop applications in the list. The default is *TRUE*.

Display large icons: Specifies whether application icons are displayed in the Windows small icon format or in large icon format. The default is *FALSE*, which means small icon format is used.

Number of columns: This setting applies only if *Display large icons* is set to *TRUE*. It specifies the number of columns to use when displaying the icons. The default is 4.

ICA template file: Specifies the file that contains default initialization information for the Citrix ICA Client program. The settings in the file are overwritten with information from IMA database, *NFuse.conf*, and gadget settings. The default file is *OnDemandTemplate.ica*, located in the *tomcat\webapps\nps\portal\gadgets\com.novell.ondemand.gadgets.ZenLaunchGadget* directory.

ICA window type: Specifies the type of window used by the ICA client when launching applications. The default is seamless. Other possible values are: percent, pixels, fullscreen. If you specify percent, you must use the **ICA Percent** setting to specify the size. If you specify pixels, you must use the **ICA Width** and **ICA Height** settings to specify the size.

ICA width: This setting applies only when ICA Window Type is set to pixels. Specify the width of the ICA client window in pixels. The default is 640 pixels.

ICA height: This setting applies only when ICA Window Type is set to pixels. Specify the height of the ICA client window in pixels. The default is 480 pixels.

ICA percent: This setting applies only when ICA Window Type is set to percent. Specify the percentage of the user's screen to be used by the ICA client window. The default is 25 percent.

ICA color depth: Specifies the color settings used by the ICA client when launching applications. Possible values are:

- 1 — 16 colors
- 2 — 256 colors
- 4 — high color (16-bit)
- 8 — true color (24 -bit)

The default is 2.

ICA audio: Specifies whether ICA client support for audio is turned on or off. The default is off.

Production context attribute: This setting applies only in an environment with multiple eDirectory trees. Typically, in this type of environment, one tree is used for authentication and is synchronized with the production tree via Nsure™ Identity Manager.

In order for the Launch gadget to authenticate to the production tree, you must use the ConsoleOne® Schema Manager to create a new attribute (for example ProductionContext) and assign it to the User object (class). Create the attribute as a single valued string. After you create and assign it to the User object, set the attribute's value to the base context of the users in the production tree, formatted as Typeless Dot notation. For example: users.department.company.

After setting up the attribute in ConsoleOne, use this setting to specify the attribute name (for example, ProductionContext).

26.2 Adding Citrix MetaFrame Servers to the Portal

During installation of the ZENworks Launch gadget to a portal, you specified the DNS name or IP address of the server where the Citrix IMA database resides. If you have multiple Citrix farms, you should have specified addresses of each server where an IMA database resides.

If you need to define additional servers, you can do so through the portal configuration:

- 1 Log in to the portal as a portal administrator.
- 2 Click *Administer the portal*.
- 3 Click *Portal* to display the Edit Portal page.
- 4 Under the Configuration heading, click *Configuration* to display the Portal Configuration page.

- 5** In the *XML_SERVER_PORT* field, add the DNS names or IP addresses of the new servers, using a semicolon (;) to separate each address. For example:

123.456.79.90;123.456.78.91;123.456.78.92

- 6** Click *Save* to save your changes.

Novell® ZENworks® Desktop Management lets you distribute applications to users on Windows 98 and Windows 2000/XP workstations.

The distribution process for an application might be as simple as creating a shortcut to an already installed network application, Web application, or terminal server application, or it might be as complex as installing the application files on the workstation, modifying the workstation's registry and configuration settings, and mapping drive paths. The following sections provide basic information you should understand before configuring applications for distribution:

- [Section 27.1, “Application Types,” on page 313](#)
- [Section 27.2, “User Associated vs. Workstation Associated,” on page 313](#)

After you've familiarized yourself with the information in these sections, you should refer to the following for detailed instructions about configuring applications for distribution:

- [Chapter 28, “Distribution: Simple Applications,” on page 315](#)
- [Chapter 29, “Distribution: Complex Applications,” on page 321](#)
- [Chapter 30, “Distribution: Terminal Server Applications,” on page 331](#)
- [Chapter 31, “Distribution: Web Applications,” on page 337](#)

27.1 Application Types

Applications you distribute are categorized into four types:

- **Simple application:** Distribution requires Novell Application Launcher™ to copy no (or few) files to the workstation and make no (or few) changes to the workstation's registry, INI files, environment variables, and so forth. An example is Windows Notepad.
- **Complex application:** Distribution requires Application Launcher to copy many files and make many configuration changes to the workstation. This type of application also includes (or uses) .msi files. An example is Novell GroupWise® or Microsoft Office.
- **Web application:** Distribution requires Application Launcher to display an application icon that, when launched, opens the workstation's Web browser and displays the Web-based application (or other Web content). No files need to be copied to the workstation and no configuration settings are modified.
- **Terminal server application:** Distribution requires Application Launcher to display an application icon that, when launched, opens a client session to the terminal server and starts the application (or displays the desktop). An example is Novell GroupWise or Microsoft Office running on a terminal server rather than the user's local workstation.

27.2 User Associated vs. Workstation Associated

When configuring an application for distribution, you can associate the application with both users and workstations.

With a user-associated application, the application is available to the user regardless of the workstation from which the user logs in to eDirectory.

With a workstation-associated application, the application is available on that workstation only. If the user moves to another workstation that is not associated with the application, the application is not available to the user.

If you choose to associate applications with workstations, you should be aware of the following:

- Each workstation associated with applications must be imported into eDirectory™ as a Workstation object. For details about importing workstations, see [Part III, “Automatic Workstation Import and Removal,” on page 117](#).
- If you associate an application with a Windows 98 workstation, any users of that workstation must be added as trustees of the Application object. Unlike Windows 2000/XP, Windows 98 does not differentiate between the user and workstation, so Application Launcher always uses the user's eDirectory credentials when distributing or launching workstation-associated applications on a Windows 98 workstation. Trustee rights are not granted automatically; you must use ConsoleOne® to manually give default trustee rights to each user who runs the application on the workstation. If you don't assign trustee rights to the user, the distribution or launch fails.
- The Application Launcher Workstation Helper, running under Workstation Manager, is responsible for authenticating the workstation to eDirectory and retrieving information about workstation-associated applications. However, the Workstation Helper does not have a user interface. For users to see workstation-associated applications, they must run Application Launcher, but they do not need to be logged in to eDirectory. The Workstation Helper passes the list of workstation-associated applications to Application Launcher, which then displays the applications.
- Application Launcher displays applications that are associated with the workstation and applications that are associated with the user logged in to eDirectory. This enables you to configure applications you want on the workstation regardless of the user who logs in, while still providing individual users with access to their specific applications.

Distribution: Simple Applications

28

Novell® ZENworks® Desktop Management lets you distribute simple applications to users on Windows 98 and Windows 2000/XP workstations.

A simple application requires no (or few) files to be copied to the workstation and no (or few) changes to the workstation's registry, INI files, environment variables, and so forth.

The following table gives some examples of simple application distributions.

Table 28-1 *Simple Application Distributions*

Example	Distribution Requirement
New application run from user's workstation	Copy an application, consisting of three files, to the user's workstation; no workstation configuration settings need to be changed.
Existing application run from user's workstation	Make an existing application (for example, Windows Notepad) accessible through Application Launcher.
Software patch	Copy a software patch to the user's workstation and automatically apply it.
Database application run from the network	Make a network database application available on the user's workstation. No files need to be copied to the workstation; it simply requires a shortcut that points to the database application's executable.

The following sections help you distribute a simple applications:

- [Section 28.1, “Preparing a Simple Application,” on page 315](#)
- [Section 28.2, “Configuring the Application in eDirectory,” on page 316](#)
- [Section 28.3, “Establishing File System Access,” on page 319](#)
- [Section 28.4, “Establishing eDirectory Rights,” on page 319](#)
- [Section 28.5, “What's Next,” on page 320](#)

28.1 Preparing a Simple Application

In general, the following rules apply when preparing a simple application for distribution:

- If the distribution requires Application Launcher to copy files to the workstation, place the files on a NetWare®, Linux, or Windows server that is available to Application Launcher. For more information about what is required for Application Launcher to access a network resource, see [“Novell Application Launcher: Managing Authentication and File System Access” on page 283](#).
- If the application runs from the network, make sure the application is installed on a NetWare, Linux, or Windows server that is available to Application Launcher. For more information about what is required for Application Launcher to access a network resource, see [“Novell Application Launcher: Managing Authentication and File System Access” on page 283](#).

After creating the eDirectory object for the simple application (see [Section 28.2, “Configuring the Application in eDirectory,” on page 316](#)), you can configure the Application object so that Application Launcher copies the files to the workstation, creates the shortcut to the application executable, or does whatever else is needed to properly distribute the application. If necessary, you can also configure the Application object to modify any workstation settings (registry settings, INI settings, and so forth) required by the application.

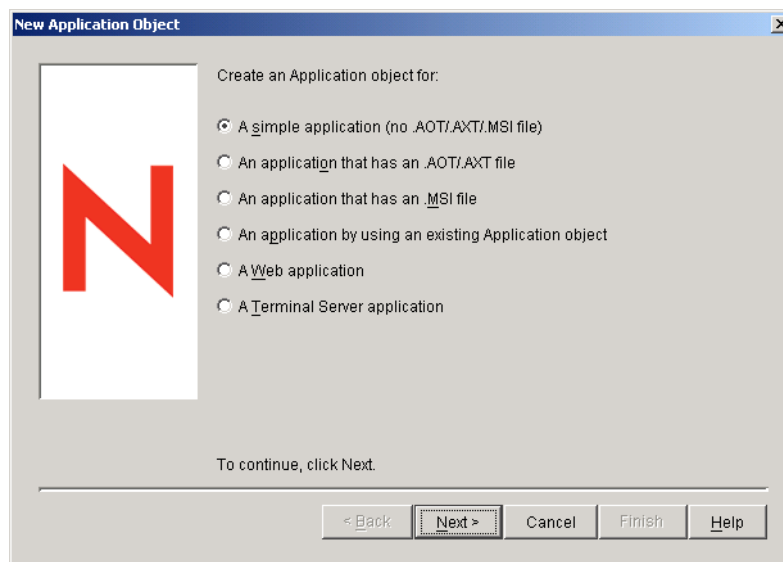
28.2 Configuring the Application in eDirectory

After you have prepared the application for distribution (see [Section 28.1, “Preparing a Simple Application,” on page 315](#)), you are ready to create the application as an Application object in eDirectory™, define its distribution rules, and associate it with users and workstations.

You can create the Application object in any container you want. Because Application Launcher accesses the object on behalf of the logged-in user or workstation, you should place it in a container whose partition (or a replica of the partition) is available to the user or workstation over a local area connection rather than a wide area connection. For more information, see [Chapter 51, “Reference: Application Object Location,” on page 609](#).

To create the Application object in eDirectory and configure it:

- 1 In ConsoleOne®, right-click the container where you want to create the Application object, click *New*, then click *Application* to display the New Application Object dialog box.



- 2 In the New Application Object dialog box, select the *Simple application (No .AOT/.AXT/.MSI file)* option, then click *Next*.
- 3 In the Object Name field, type a name for the Application object.

The Application object's name must conform to the following rules:

- The name must be unique in the container.
- Special characters are allowed. However, plus (+), equals (=), and period (.) must be preceded by a backslash (\) if used.

- The following characters are valid in Application object names but are invalid when used in Windows folder and file names:

\ / : * ? " < > |

If you use these characters in the Application object name, they are replaced by an underscore (_) when displayed in locations controlled by Windows and not Novell Application Launcher (for example, on the Windows desktop).

- Uppercase and lowercase letters, as well as underscores and spaces, are displayed as you first entered them, but they aren't distinguished. For example, ZENworks_Desktop_Management and ZENWORKS DESKTOP MANAGEMENT are considered identical.

The Application object's name is visible in eDirectory. By default, the name is also used as the Application object's icon title when displayed by Application Launcher on a user's workstation. You can, if necessary, change the icon title after the Application object has been created (Application object > Identification tab > Icon page).

- 4 Click *Next* to display the Path to File field, then enter the path to the location from which the application's executable file runs.

As you specify the path, be aware of the following:

- Include the executable file in the path.
- If, as part of the distribution process, Application Launcher copies the executable file to a target directory on the workstation, specify that location as the path.
- For Application Launcher to launch an application from a network server, the workstation must have the appropriate network client (Novell Client™ or Client for Microsoft Networks) installed. This is because the ZENworks Desktop Management Agent and Middle Tier Server do not support opening or executing of files from a network server; only copying of files is supported. In a clientless environment, the alternative to launching the application from a network server is to have Application Launcher first copy the application files to the local workstation and then launch the application locally. For more information about file system access in a clientless environment, see [Section 23.2, "File System Access Overview," on page 284](#).
- When specifying a path to a network server, you can use a mapped drive or UNC path (with server name or IP address). If you use a UNC path and your workstations have multiple network clients, applications might launch more slowly than with a mapped drive because the Windows Multiple UNC Provider (MUP) must resolve the UNC paths to the appropriate network client. For more information, see [Microsoft Knowledge Base Article Q150807 \(http://support.microsoft.com/support/kb/articles/Q150/8/07.asp\)](http://support.microsoft.com/support/kb/articles/Q150/8/07.asp).

- 5 Click *Next*, then define the rules used by Application Launcher to determine if a workstation meets the requirements for the application.

The distribution rules ensure that Application Launcher does not distribute the application to workstations that cannot support the application. For example, if the application runs on Windows 2000/XP only, you can create an operating system rule that prohibits distribution to Windows 98 workstations.

NOTE: The requirement for an operating system to be defined before an application is available has been removed.

In previous ZENworks versions, an OS platform had to be defined in the System Requirements before an application was available for distribution and launching. This requirement has been removed.

The new behavior uses the following logic: If an application runs only on a specific operating system, define an operating system distribution rule. If an application does not require a specific operating system, there is no need to define a distribution rule. By default, applications without a defined operating system distribution rule are available on all supported platforms (Windows 98, Windows 2000, and Windows XP).

To add a distribution rule:

5a Click *Add*, then select the type of rule you want to define.

5b Fill in the information for the requirement (click *Help* for information about the requirement or refer to “[Distribution Rules Page](#)” on page 527), then click *OK* to add the requirement to the list.

If you want to create additional distribution rules for the application at a later time, you can use the Distribution Rules page on the Application object. For information, see “[Distribution Rules Page](#)” on page 527.

6 Click *Next*, then associate the Application object with the users or workstations that you want to distribute the application to. To do so:

6a Click *Add*, then browse for and select User or Workstation objects.

Each workstation that you want to associate with applications must first be imported into eDirectory as a Workstation object. If a workstation with which you want to associate the application has not been imported as a Workstation object, see [Part III, “Automatic Workstation Import and Removal,”](#) on page 117.

You can also select Group objects, Workstation Group objects, and container objects (Organizational Unit, Organization, or Country). If you select a container object, you are given the choice of associating all the container's User and/or Workstation objects with the application.

Associating an Application object with a Group, Workstation Group, or other container object is the preferred method of associating the Application object in eDirectory.

Associating the application to a large number of User or Workstation objects (for example, more than 250) might cause increased server utilization.

IMPORTANT: Do not associate the Application object with Alias objects. Alias objects are not supported.

6b After you add the user or workstation to the list, select the appropriate check boxes for the user or workstation to set the characteristics (*Force run*, *App Launcher*, *Start menu*, *Desktop*, *System tray*, *Quick launch*, and *Force cache*) you want applied to the application. Click *Help* for a description of each of these characteristics, or refer to “[Associations Page](#)” on page 524.

If you want to associate the application with additional users or workstations at a later time, you can use the Associations page on the Application object. For information, see “[Associations Page](#)” on page 524.

7 Click *Next*, review the Application object settings, then click *Finish* to create the Application object.

8 If, as part of the distribution process for the application, Application Launcher needs to copy files to the workstation, right-click the Application object, click *Properties*, then complete the remaining steps.

or

If the application runs from the network or is already located on the workstation, skip the remain steps and continue with [Section 28.3, “Establishing File System Access,” on page 319](#).

- 9 Click the *Distribution Options* tab, then click *Application files*.

You need to add the files to the Application Files list in order for Application Launcher to copy them to the workstation.

- 10 Click *Add*, click *File*, then fill in the following fields.

Source file: Select the file you want copied to the workstation (for example, `\\server1\sys\public\notepad\notepad.exe`).

Target file: Enter the full path, including the file name, of where you want the file copied (for example, `c:\notepad\notepad.exe`).

- 11 Click *OK* to add the file to the list.
- 12 Repeat [Step 10](#) and [Step 11](#) for each file to be copied.
- 13 When finished adding files, click *OK* to save the Application object information.
- 14 Continue with then next section, [Establishing File System Access](#).

28.3 Establishing File System Access

For Application Launcher to be able to distribute or launch an application from a NetWare, Linux, or Windows server, it must have the appropriate rights to the server's file system. If you have not already established file system access for users and/or workstations you've associated the application to, see [Chapter 23, “Novell Application Launcher: Managing Authentication and File System Access,” on page 283](#).

28.4 Establishing eDirectory Rights

By default, when a user or workstation is associated with an Application object, the User object or Workstation object is assigned trustee rights to the object. This provides Application Launcher with sufficient eDirectory rights to distribute and launch the application on the user's workstation.

However, for workstation-associated applications that are installed on Windows 98 workstations, you need to also manually assign trustee rights to any users who distribute or launch the application. Windows 98 does not differentiate between the user and workstation, so Application Launcher always uses the user's eDirectory credentials when distributing or launching workstation-associated applications on a Windows 98 workstation. If you don't assign trustee rights to the user, the distribution or launch fails.

To assign trustee rights to a user:

- 1 In ConsoleOne, right-click the Application object, then click *Properties*.
- 2 Click the *NDS Rights* tab, then click *Trustees of this object*.
- 3 Click *Add trustee*, select the user you want to add as a trustee, then click *OK* to add the user to the trustee list. Repeat this step for all users you need to add.
- 4 Click *OK* to save the changes.

28.5 What's Next

To better manage the application you've distributed, you can configure the Application object to:

- Automatically cache the application's files to the local workstation (if the distribution requires installation of the application). This enables users to install or fix problems with the application when they are disconnected from eDirectory and your network. See [Chapter 24, “Novell Application Launcher: Managing the Cache,”](#) on page 293.
- Add the Application object to a folder in the Application Window, Application Explorer window, Application Browser window, or on the Windows Start menu. See [Chapter 25, “Novell Application Launcher: Organizing Applications,”](#) on page 303.
- Automatically distribute and run other applications on which it is dependent. See [Chapter 37, “Advanced Distribution: Configuring Application Dependencies and Chains,”](#) on page 389.
- Report on the success or failure of events such as distributing, caching, and uninstalling the application on workstations. See [Chapter 44, “Reporting Application Events,”](#) on page 431.
- Track the number of licenses being used for the application. See [Chapter 45, “Metering Software Licenses,”](#) on page 459.
- Determine the schedule of when the application is available to users. See [“Schedule Page”](#) on page 543.
- Set up backup copies of the application's file package to enable fault tolerance. See [“Setting Up Fault Tolerance for Simple or AOT/AXT Applications”](#) on page 378.
- Define multiple Application objects for the same application and enable load balancing. See [Section 36.2, “Setting Up Load Balancing,”](#) on page 381.
- Set up site lists to enable users who travel from site to site to continue to have access to their applications. See [Section 36.3, “Setting Up Site Lists,”](#) on page 385.
- Define many additional Application object properties to control the behavior of the application. For information about all Application object properties, see [Chapter 48, “Reference: Application Object Settings,”](#) on page 471.

Distribution: Complex Applications

29

Novell® ZENworks® Desktop Management lets you distribute complex applications to users on Windows 98 and Windows 2000/XP workstations.

A complex application is one that requires Application Launcher to copy many files and make many configuration changes to the workstation during distribution of the application. An example is Novell GroupWise® or Microsoft Office.

The following sections help you set up a complex application for distribution:

- [Section 29.1, “Understanding Software Packages,” on page 321](#)
- [Section 29.2, “Preparing the Software Package,” on page 323](#)
- [Section 29.3, “Configuring the Application in eDirectory,” on page 323](#)
- [Section 29.4, “Establishing File System Access,” on page 329](#)
- [Section 29.5, “Establishing eDirectory Rights,” on page 329](#)
- [Section 29.6, “What's Next,” on page 329](#)

29.1 Understanding Software Packages

A complex application such as Novell GroupWise or Microsoft Office requires many files to be installed and many configuration changes to be made to the workstation. To ensure that complex application are distributed and installed correctly, ZENworks Desktop Management supports the use of software packages.

Software packages contain the files, configuration settings, and instructions required to install the application. The following sections describe the two types of software packages that ZENworks Desktop Management supports:

- [Section 29.1.1, “Microsoft Windows Installer Packages,” on page 321](#)
- [Section 29.1.2, “ZENworks snAppShot Packages,” on page 322](#)

In addition to the information provided in the sections listed above, the following articles contain excellent information about software packages and the ZENworks utilities provided to create them:

- [Novell snAppShot versus FLEXnet AdminStudio's Repackager \(http://www.macrovision.com/company/news/newsletter/tips/novell_vs_adminstudio.shtml\)](http://www.macrovision.com/company/news/newsletter/tips/novell_vs_adminstudio.shtml)
- [Consistently Consistent \(http://www.novell.com/connectionmagazine/2004/11/tech_talk_2.html\)](http://www.novell.com/connectionmagazine/2004/11/tech_talk_2.html)

29.1.1 Microsoft Windows Installer Packages

The Microsoft Windows Installer is an installation and configuration service that ships as part of the Windows 2000 and Windows XP operating systems, and is provided in a service pack to Windows 98.

The software packages used by Windows Installer are called Windows Installer packages or MSI packages (because of their `.msi` file extension). Windows Installer packages are the common and accepted standard for Windows applications. Because of the benefits associated with using the native Windows Installer, Novell recommends that you use Windows Installer packages whenever possible.

Vendor-Supplied MSI Packages

Many software vendors provide Windows Installer packages that include the files and configuration settings required by the Windows Installer to install the application to a workstation. In this case, unless you want to customize the package, the package is ready to distribute.

Customized MSI Packages

Different groups within an organization often use the same application, but that doesn't mean they require the same feature set. One of the benefits of Windows Installer is that if you have 10 groups needing 10 different feature sets or other alterations for the same application, you can deploy the same MSI package to all 10 user groups, but with a different transform file (MST) applied for each group.

A transform file is a collection of changes applied to an MSI installation. It contains all modification information, such as whether features are installed; how they are installed; which files, shortcuts, and registry entries are included; and Add/Remove Programs applet information.

If you have vendor-supplied MSI packages, you can use FLEXnet AdminStudio 7.5 ZENworks Edition to create and manage transforms. For information about using AdminStudio ZENworks Edition, see [Chapter 46, “Reference: AdminStudio ZENworks Edition,” on page 463](#).

Non-Windows Installer Installations

Not all Windows applications are designed to be installed by Windows Installer. Many applications use other software installers such as MacroVision InstallShield.

AdminStudio ZENworks Edition includes a Repackaging Wizard that lets you create MSI packages for non-Windows Installer applications. For information about using AdminStudio ZENworks Edition, see [Chapter 46, “Reference: AdminStudio ZENworks Edition,” on page 463](#).

29.1.2 ZENworks snAppShot Packages

Windows Installer packages are the recommended package format for distributing applications. If you cannot create a Windows Installer package for an application, you can use the ZENworks snAppShot utility to create a software package.

ZENworks snAppShot was created prior to the existence of Windows Installer. It lets you create a proprietary software package called a snAppShot package or AOT package/AXT package. AOT stands for Application Object Template and AXT stands for Application Object Text Template. Both packages contain the same information. However, an AOT package is an uneditable binary format, while an AXT package is an editable text-based format.

For information about using snAppShot, see [Chapter 47, “Reference: ZENworks SnAppShot,” on page 465](#).

29.2 Preparing the Software Package

- 1 To create or customize a Windows Installer package, see [Chapter 46, “Reference: AdminStudio ZENworks Edition,”](#) on page 463.

or

To create a ZENworks snAppShot package, see [Chapter 47, “Reference: ZENworks SnAppShot,”](#) on page 465.

- 2 Make sure the NetWare, Linux, or Windows server where you save the Windows Installer package or the ZENworks snAppShot package is available to Application Launcher.

For more information about what is required for Application Launcher to access a network resource, see [Chapter 23, “Novell Application Launcher: Managing Authentication and File System Access,”](#) on page 283.

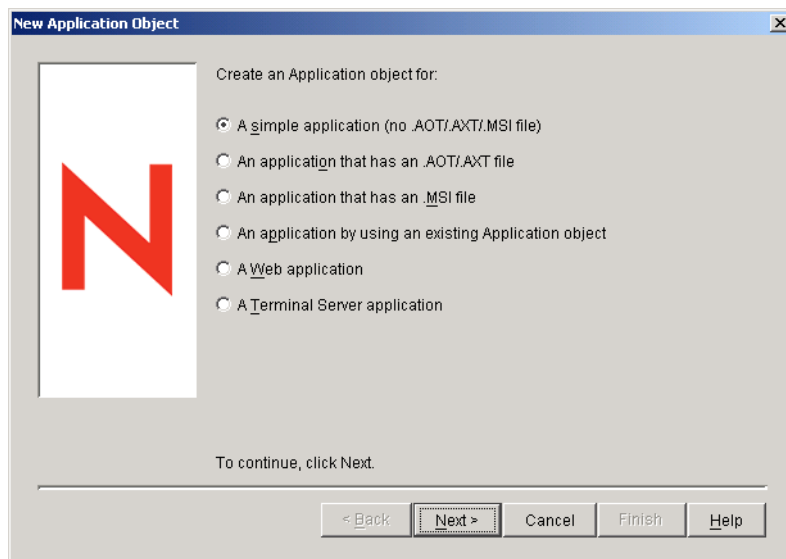
29.3 Configuring the Application in eDirectory

After you have prepared the application for distribution (see [Section 29.1, “Understanding Software Packages,”](#) on page 321), you are ready to create the application as an Application object in eDirectory, define its distribution rules, and associate it with users and workstations.

You can create the Application object in any container you want. Because Application Launcher accesses the object on behalf of the logged-in user or workstation, you should place it in a container whose partition (or a replica of the partition) is available to the user or workstation over a local area connection rather than a wide area connection. For more information, see [Chapter 51, “Reference: Application Object Location,”](#) on page 609.

To create the Application object in eDirectory and configure it:

- 1 In ConsoleOne®, right-click the container where you want to create the Application object, click *New*, then click *Application* to display the New Application Object dialog box.



- 2 Select from the following options to create the appropriate type of object for the application:

An application that has an .aot/.axt file: Lets you specify a .aot or .axt file you've created with snAppShot or exported from another Application object. The .aot or .axt file is used to populate the Application object's property fields. Skip to [Section 29.3.1, "Creating an Application Object from a ZENworks snAppshot File,"](#) on page 324.

An application that has a .msi file: Lets you specify a Microsoft Windows Installer (.msi) file. The .msi file is used to populate the Application object's property fields. Skip to [Section 29.3.2, "Creating the Application Object from a Windows Installer \(.MSI\) File,"](#) on page 326.

29.3.1 Creating an Application Object from a ZENworks snAppshot File

- 1 (Conditional) If the New Application Object dialog box is not open, see [Section 29.3, "Configuring the Application in eDirectory,"](#) on page 323.
- 2 In the New Application Object dialog box, select the *Application that has an .aot/.axt file* option, then click *Next*.
- 3 Specify the path to the .aot or .axt file.

or

Click the browse button to browse for and select the file.

The file should be in the network location where you saved it when creating it with snAppShot. If you browse for the file, the Open dialog box defaults to *.axt for its file type display. If you created an .aot file, you must change the file type display to *.aot or All Files in order to select the .aot file.

- 4 Click *Next*, then modify the following fields to customize the Application object.

Object name: This field defaults to the Application object name that was specified when running snAppShot. You can change the name if you want. The name must conform to the following rules:

- The name must be unique in the container.
- Special characters are allowed. However, plus (+), equals (=), and period (.) must be preceded by a backslash (\) if used.
- The following characters are valid in Application object names but are invalid when used in Windows folder and file names:

\ / : * ? " < > |

If you use these characters in the Application object name, they are replaced by an underscore (_) when displayed in locations controlled by Windows and not Novell Application Launcher™ (for example, on the Windows desktop).

- Uppercase and lowercase letters, as well as underscores and spaces, are displayed as you first entered them, but they aren't distinguished. For example, ZENworks_Desktop_Management and ZENWORKS DESKTOP MANAGEMENT are considered identical.

The Application object's name is visible in eDirectory. By default, the name is also used as the Application object's icon title when displayed by Application Launcher on a user's workstation. You can, if necessary, change the icon title after the Application object has been created (Application object > *Identification* tab > *Icon* page).

SOURCE_PATH (location of installation files (.fil)): This field defaults to the location where the application's files (.fil) files were stored when running snAppShot. You should

verify that the path is correct. If the path uses a drive mapping, you can either 1) ensure that all workstations have the same drive mapped to the source location or 2) change the drive mapping to another format such as UNC. For information about valid formats, see Filepath Syntax in [Section 23.2, “File System Access Overview,” on page 284](#).

The path you enter here is added as the SOURCE_PATH macro in the Macros list for the Application object (*Common* tab > *Macros* page) and used in any fields that require a path to the source location.

TARGET_PATH (client workstation directory path): This path specifies the workstation location where the application files should be installed. It defaults to the path defined in the .aot or .axt, which is the location where the application was installed when running snAppShot. You should verify that this is the workstation directory where you want the application installed.

The path you enter here is added as the TARGET_PATH macro in the Macros list for the Application object (*Common* tab > *Macros* page) and used in any fields that require a path to the target location.

- 5 Click *Next*, then define the rules used by Application Launcher to determine if a workstation meets the requirements for the application.

The distribution rules ensure that Application Launcher does not distribute the application to workstations that cannot support the application. For example, if the application runs on Windows 2000/XP only, you can create an operating system rule that prohibits distribution to Windows 98 workstations.

NOTE: The requirement for an operating system to be defined before an application is available has been removed.

In previous ZENworks versions, an OS platform had to be defined in the System Requirements before an application would be available for distribution and launching. This requirement has been removed.

The new behavior uses the following logic: If an application runs only on a specific operating system, define an operating system distribution rule. If an application does not require a specific operating system, there is no need to define a distribution rule. By default, applications without a defined operating system distribution rule are available on all supported platforms (Windows 98, Windows 2000, and Windows XP).

To add a distribution rule:

5a Click *Add*, then select the type of rule you want to define.

5b Fill in the information for the requirement (click *Help* for information about the requirement or refer to [“Distribution Rules Page” on page 527](#)), then click *OK* to add the requirement to the list.

If you want to create additional distribution rules for the application at a later time, you can use the Distribution Rules page on the Application object. For information, see [“Distribution Rules Page” on page 527](#).

- 6 Click *Next*, then associate the Application object with the users or workstations that you want to distribute the application to. To do so:

6a Click *Add*, then browse for and select User or Workstation objects. You can also select Group objects, Workstation Group objects, and container objects (Organizational Unit, Organization, or Country). If you select a container object, you are given the choice of associating all the container's User and/or Workstation objects with the application.

Each workstation that you want to associate with applications must first be imported into eDirectory as a Workstation object. If a workstation with which you want to associate the application has not been imported as a Workstation object, see [Part III, “Automatic Workstation Import and Removal,” on page 117](#).

Associating an Application object with a Group, Workstation Group, or other container object is the preferred method of associating the Application object in eDirectory. Associating the application to a large number of User or Workstation objects (for example, more than 250) might cause increased server utilization.

IMPORTANT: Do not associate the Application object with Alias objects. Alias objects are not supported.

- 6b** After you add the user or workstation to the list, select the appropriate check boxes for the user or workstation to set the characteristics (*Force run*, *App Launcher*, *Start menu*, *Desktop*, *System tray*, *Quick launch*, and *Force cache*) you want applied to the application. Click *Help* for a description of each of these characteristics, or refer to [“Associations Page” on page 524](#).

If you want to associate the application with additional users or workstations at a later time, you can use the Associations page on the Application object. For information, see [“Associations Page” on page 524](#).

- 7** Click *Next*, review the Application object settings, then click *Finish* to create the Application object.
- 8** Continue with [Section 28.3, “Establishing File System Access,” on page 319](#).

29.3.2 Creating the Application Object from a Windows Installer (.MSI) File

- 1** (Conditional) If the New Application Object dialog box is not open, see [Section 29.3, “Configuring the Application in eDirectory,” on page 323](#).
- 2** In the New Application Object dialog box, select the *Application that has an .msi file* option, then click *Next*.
- 3** In the *Path to .msi file* field, specify the complete path to the .msi file to use as the source file during distribution to workstation.

You can use a mapped drive or UNC path. If you use a drive mapping, you must ensure that all workstations have the same drive mapped to the source location. The path you enter here is added to the *Package source* list for the Application object (*Common* tab > *Sources*).

NOTE: After you create the Application object, you cannot change the .msi filename; however, you can change the path to the .msi file. If you change the .msi filename, the installation fails.

- 4** Click *Next*, then modify the following fields to customize the Application object.

Object name: This field defaults to the Application object name defined in the .msi file. You can change the name if you want. The name must conform to the following rules:

- The name must be unique in the container.
- Special characters are allowed. However, plus (+), equals (=), and period (.) must be preceded by a backslash (\) if used.

- The following characters are valid in Application object names but are invalid when used in Windows folder and file names:

\ / : * ? " < > |

If you use these characters in the Application object name, they are replaced by an underscore (_) when displayed in locations controlled by Windows and not Novell Application Launcher (for example, on the Windows desktop).

- Uppercase and lowercase letters, as well as underscores and spaces, are displayed as you first entered them, but they aren't distinguished. For example, ZENworks_Desktop_Management and ZENWORKS DESKTOP MANAGEMENT are considered identical.

The Application object's name is visible in eDirectory. By default, the name is also used as the Application object's icon title when displayed by Application Launcher on a user's workstation. You can, if necessary, change the icon title after the Application object has been created (Application object > *Identification* tab > *Icon* page).

Administration package path: This path specifies the location of the MSI package you want to use for administrative purposes. ConsoleOne uses the .msi file at this location to populate information in the Application object. This field is used only by ConsoleOne for reading of the .msi package. It is not used by Novell Application Launcher for distribution of the application. For distribution, Application Launcher uses the path defined in the *Path to .msi file* field located on the previous page.

The path defaults to the path defined in *Path to .msi file* field on the previous page. Change it if necessary. You can use a mapped drive or UNC path. If you use a drive mapping, you must ensure that all ConsoleOne workstations have the same drive mapped to the location. You cannot use macros in this field.

The path you enter here is added to the *Administration package path* field for the Application object (*Identification* tab > *Package Information* page).

NOTE: Do not use macros in this field or creation of the Application object will fail. After ConsoleOne has created the Application object, you can define a macro for the source location (*Common* tab > *Macros*) and use it in other Application object fields (such as the *Package source* list) if desired.

- 5 Click *Next*, then define the rules used by Application Launcher to determine if a workstation meets the requirements for the application.

The distribution rules ensure that Application Launcher does not distribute the application to workstations that cannot support the application. For example, if the application runs on Windows 2000/XP only, you can create an operating system rule that prohibits distribution to Windows 98 workstations.

To add a distribution rule:

5a Click *Add*, then select the type of rule you want to define.

5b Fill in the information for the requirement (click *Help* for information about the requirement or refer to [“Distribution Rules Page” on page 527](#)), then click *OK* to add the requirement to the list.

If you want to create additional distribution rules for the application at a later time, you can use the Distribution Rules page on the Application object. For information, see [“Distribution Rules Page” on page 527](#).

- 6 Click *Next*, then associate the Application object with the users or workstations that you want to distribute the application to. To do so:

6a Click *Add*, then browse for and select User or Workstation objects.

Each workstation that you want to associate with applications must first be imported into eDirectory as a Workstation object. If a workstation with which you want to associate the application has not been imported as a Workstation object, see [Part III, “Automatic Workstation Import and Removal,” on page 117](#).

You can also select Group objects, Workstation Group objects, and container objects (Organizational Unit, Organization, or Country). If you select a container object, you are given the choice of associating all the container's User and/or Workstation objects with the application.

Associating an Application object with a Group, Workstation Group, or other container object is the preferred method of associating the Application object in eDirectory. Associating the application to a large number of User or Workstation objects (for example, more than 250) might cause increased server utilization.

IMPORTANT: Do not associate the Application object with Alias objects. Alias objects are not supported.

- 6b** After you add the user or workstation to the list, select the appropriate check boxes for the user or workstation to set the characteristics (*Force run*, *App Launcher*, *Start menu*, *Desktop*, *System tray*, *Quick launch*, and *Force cache*) you want applied to the application. Click *Help* for a description of each of these characteristics, or refer to [“Associations Page” on page 524](#).

With MSI applications, you must use the *Force cache* option if users or workstations do not have network client access to the source .msi files. The Microsoft Windows Installer requires file access that is provided by a network client but not by the ZENworks Desktop Management Agent. Consider the following examples:

- Users outside your firewall need an MSI application but have no network client access to the source .msi files on a server inside your firewall. They log in to the ZENworks Middle Tier Server and Application Launcher displays the MSI application. For successful distribution to occur, the MSI application must be marked as *Force cache* so that the source .msi files are copied to the user's cache directory (through the Middle Tier Server) and then distributed from the cache directory.
- Users inside your firewall need an MSI application. They don't have the Novell Client™ installed, so they log in to the ZENworks Middle Tier Server to authenticate to eDirectory. The users are part of an Active Directory domain, and the source .msi files are located on a Windows share that they have rights to. The distribution succeeds without force caching the application because the Microsoft network client provides file access to the source .msi files.

If you want to associate the application with additional users or workstations at a later time, you can use the Associations page on the Application object. For information, see [“Associations Page” on page 524](#).

- 7 Click *Next*, review the Application object settings, then click *Finish* to create the Application object.

If, after you create an Application object for an MSI application, you receive a new MSI package (.msi file) for the application, you must create a new Application object using the new .msi file. You cannot simply replace the old .msi file with the new one.

For example, the Desktop Management Agent is packaged as an .msi file (`zfdagent.msi`) that can be distributed through an Application object. Each time you receive a new `zfdagent.msi` file (through an upgrade or support pack), you must create a new Application object for it. This ensures that the GUID (global unique identifier) contained in the .msi file is synchronized with the one in the Application object and on the workstation, thus enabling the application to be installed and uninstalled correctly.

8 Continue with [Section 28.3, “Establishing File System Access,”](#) on page 319.

29.4 Establishing File System Access

For Application Launcher to be able to distribute or launch an application from a NetWare, Linux, or Windows server, it must have the appropriate rights to the server's file system. If you have not already established file system access for users and/or workstations you've associated the application to, see [Chapter 23, “Novell Application Launcher: Managing Authentication and File System Access,”](#) on page 283.

29.5 Establishing eDirectory Rights

By default, when a user or workstation is associated with an Application object, the User object or Workstation object is assigned trustee rights to the object. This provides Application Launcher with sufficient eDirectory rights to distribute and launch the application on the user's workstation.

However, for workstation-associated applications that are installed on Windows 98 workstations, you need to also manually assign trustee rights to any users who distribute or launch the application. Windows 98 does not differentiate between the user and workstation, so Application Launcher always uses the user's eDirectory credentials when distributing or launching workstation-associated applications on a Windows 98 workstation. If you don't assign trustee rights to the user, the distribution or launch fails.

To assign trustee rights to a user:

- 1 In ConsoleOne, right-click the Application object, then click *Properties*.
- 2 Click the *NDS Rights* tab, then click *Trustees of this object*.
- 3 Click *Add trustee*, select the user you want to add as a trustee, then click *OK* to add the user to the trustee list. Repeat this step for all users you need to add.
- 4 Click *OK* to save the changes.

29.6 What's Next

To better manage the application you've distributed, you can configure the Application object to:

- Automatically cache the application's files to the local workstation (if the distribution requires installation of the application). This enables users to install or fix problems with the application when they are disconnected from eDirectory and your network. See [“Novell Application Launcher: Managing the Cache”](#) on page 293.
- Add the Application object to a folder in the Application Window, Application Explorer window, Application Browser window, or on the Windows Start menu. See [Chapter 25, “Novell Application Launcher: Organizing Applications,”](#) on page 303.
- Ensure that all dependent applications are automatically distributed before the application. For example, if AppA has a dependency on AppB and AppC, you can ensure that AppB and AppC

are installed before AppA. See [Chapter 37, “Advanced Distribution: Configuring Application Dependencies and Chains,”](#) on page 389

- Report on the success or failure of events such as distributing, caching, and uninstalling the application on workstations. See [Chapter 44, “Reporting Application Events,”](#) on page 431.
- Track the number of licenses being used for the application. See [Chapter 45, “Metering Software Licenses,”](#) on page 459.
- Determine the schedule of when the application is available. See [“Schedule Page”](#) on page 543.
- Set up backup copies of the application's file package to enable fault tolerance. See [Section 36.1, “Setting Up Fault Tolerance,”](#) on page 377.
- Define multiple Application objects for the same application and enable load balancing. See [Section 36.2, “Setting Up Load Balancing,”](#) on page 381.
- Set up site lists to enable users who travel from site to site to install applications from the closest server. See [Section 36.3, “Setting Up Site Lists,”](#) on page 385.
- Define many additional Application object properties to control the behavior of the application. For information about all Application object properties, see [Chapter 48, “Reference: Application Object Settings,”](#) on page 471.

Distribution: Terminal Server Applications

30

Novell® ZENworks® Desktop Management lets you distribute terminal server applications to users on Windows 98 and Windows 2000/XP workstations.

Distribution of a terminal server application requires Application Launcher to display an application icon that, when launched, opens a client session to the terminal server and starts the application. An example is Novell GroupWise® or Microsoft Office running on a terminal server rather than the user's local workstation.

Complete the tasks in the following order to distribute a terminal server application:

- [Section 30.1, “Preparing a Terminal Server Application,” on page 331](#)
- [Section 30.2, “Configuring the Application in eDirectory,” on page 331](#)
- [Section 30.3, “Establishing eDirectory Rights,” on page 334](#)
- [Section 30.4, “What's Next,” on page 335](#)

For Application Launcher to successfully launch a terminal server application from a user's workstation, you need to ensure that the user's workstation is properly configured. For instructions, see [Chapter 38, “Users: Supporting Terminal Server Users,” on page 397](#).

30.1 Preparing a Terminal Server Application

A terminal server application is an application being hosted on a Microsoft Windows terminal server or a Citrix MetaFrame server. Users run the application through terminal server client sessions on their workstations.

To prepare a terminal server application for distribution to users:

- 1 Install the application on the terminal server. For information about distributing applications to terminal servers, see [“Distribution: Applications to Terminal Servers” on page 341](#).
- 2 Ensure that users have the ICA client (for Citrix MetaFrame servers) or RDP client (for Windows terminal servers) installed on their workstations. For more information, see [Section 38.1, “Installing the RDP and ICA Clients,” on page 397](#).
- 3 Ensure that users have terminal server accounts that provide the file system rights needed to run the application. If desired, you can set up one account for all users. For more information, see [Section 38.3, “Managing Terminal Server User Accounts,” on page 398](#).

30.2 Configuring the Application in eDirectory

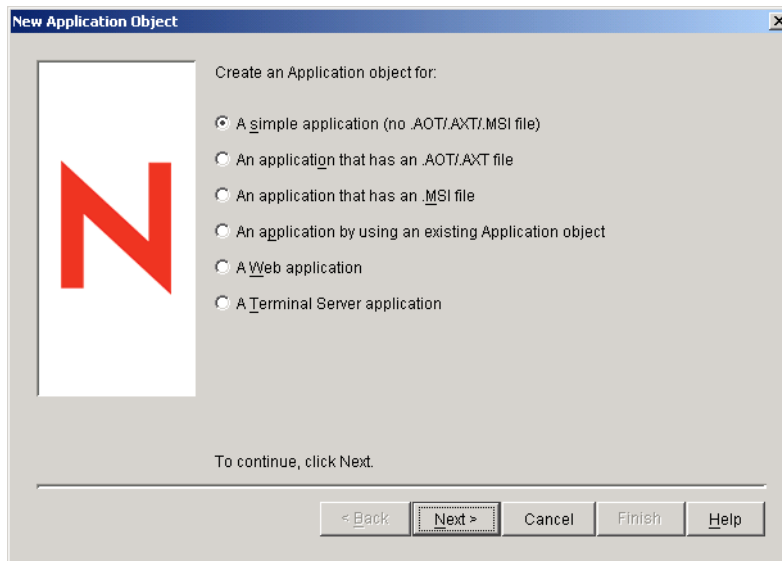
After you have prepared the application for distribution (see [Section 30.1, “Preparing a Terminal Server Application,” on page 331](#)), you are ready to create the application as an Application object in eDirectory, define its distribution rules, and associate it with users and workstations.

You can create the Application object in any container you want. Because Application Launcher accesses the object on behalf of the logged-in user or workstation, you should place it in a container

whose partition (or a replica of the partition) is available to the user or workstation over a local area connection rather than a wide area connection. For more information, see [Chapter 51, “Reference: Application Object Location,”](#) on page 609.

To create the Application object in eDirectory™ and configure it:

- 1 In ConsoleOne®, right-click the container where you want to create the Application object, click *New*, then click *Application* to display the New Application Object dialog box.



- 2 In the New Application Object dialog box, select the *Terminal server application* option, then click *Next*.
- 3 Specify a name for the Application object.

The Application object's name must conform to the following rules:

- The name must be unique in the container.
- Special characters are allowed. However, plus (+), equals (=), and period (.) must be preceded by a backslash (\) if used.
- The following characters are valid in Application object names but are invalid when used in Windows folder and file names:

\ / : * ? " < > |

If you use these characters in the Application object name, they are replaced by an underscore (_) when displayed in locations controlled by Windows and not Novell Application Launcher™ (for example, on the Windows desktop).

- Uppercase and lowercase letters, as well as underscores and spaces, are displayed as you first entered them, but they aren't distinguished. For example, ZENworks_Desktop_Management and ZENWORKS DESKTOP MANAGEMENT are considered identical.

The Application object's name is visible in eDirectory. By default, the name is also used as the Application object's icon title when displayed by Application Launcher on a user's workstation. You can, if necessary, change the icon title after the Application object has been created (Application object > *Identification* tab > *Icon* page).

- 4 Click *Next*, then fill in the following information to configure the terminal server client session in which the application runs.

ICA session: Select this option if the terminal server requires the application to run in an ICA (Independent Computing Architecture) client session. Citrix MetaFrame requires ICA client sessions. Fill in the following fields:

- **Published application name:** By default, this field is populated with the Application object name you previously entered. If the name does not match the application name exactly as it is defined in Citrix, change the name to the Citrix published application name.
- **Servers hosting this application:** Add the Citrix servers that host the application. To add a server, click the *Add* button, specify the server's IP address or hostname, then click *OK*.
The server's you define here are used only when the application is launched from Application Launcher or the NAL plug-in. The ZENworks Launch gadget uses the servers defined in its configuration settings. For information about the ZENworks Launch gadget's configuration settings, see [Chapter 26, "ZENworks Launch Gadget: Configuring Settings,"](#) on page 309.

RDP session: Select this option if the terminal server requires the application to run in an RDP (Remote Desktop Protocol) client session. Microsoft Windows Terminal Server requires RDP client sessions.

- **Terminal server address and port:** Specify the terminal server's IP address or hostname. If the terminal server is not using default port 3389, edit the *Port* field to specify the correct port number.
- **Server domain:** If the terminal server is part of a Windows NT domain or an Active Directory domain, specify the domain name. If the user's eDirectory username and password match the domain username and password, the user is not prompted to log in to the server when the RDP session is initiated.
- **Application path:** Specify the path to the application's executable file. If you are running ConsoleOne on the terminal server, you can browse for and select the file.
- **Working directory:** Specify the path to the directory you want the application to use for its working files.

- 5 Click *Next*, then define the rules used by Application Launcher to determine if a workstation meets the requirements for the application.

The distribution rules ensure that Application Launcher does not distribute the application to workstations that cannot support the application. For example, if the application runs on Windows 2000/XP only, you can create an operating system rule that prohibits distribution to Windows 98 workstations.

NOTE: The requirement for an operating system to be defined before an application is available has been removed.

In previous ZENworks versions, an OS platform had to be defined in the System Requirements before an application would be available for distribution and launching. This requirement has been removed.

The new behavior uses the following logic: If an application runs only on a specific operating system, define an operating system distribution rule. If an application does not require a specific operating system, there is no need to define a distribution rule. By default, applications without a defined operating system distribution rule are available on all supported platforms (Windows 98, Windows 2000, and Windows XP).

To add a distribution rule:

- 5a** Click *Add*, then select the type of rule you want to define.
- 5b** Fill in the information for the requirement (click *Help* for information about the requirement or refer to “[Distribution Rules Page](#)” on page 527), then click *OK* to add the requirement to the list.

If you want to create additional distribution rules for the application at a later time, you can use the Distribution Rules page on the Application object. For information, see “[Distribution Rules Page](#)” on page 527.
- 6** Click *Next*, then associate the Application object with the users or workstations that you want to distribute the application to. To do so:
 - 6a** Click *Add*, then browse for and select User or Workstation objects.

Each workstation that you want to associate with applications must first be imported into eDirectory as a Workstation object. If a workstation with which you want to associate the application has not been imported as a Workstation object, see [Part III, “Automatic Workstation Import and Removal,”](#) on page 117.

You can also select Group objects, Workstation Group objects, and container objects (Organizational Unit, Organization, or Country). If you select a container object, you are given the choice of associating all the container's User and/or Workstation objects with the application.

Associating an Application object with a Group, Workstation Group, or other container object is the preferred method of associating the Application object in eDirectory. Associating the application to a large number of User or Workstation objects (for example, more than 250) might cause increased server utilization.

IMPORTANT: Do not associate the Application object with Alias objects. Alias objects are not supported.

- 6b** After you add the user or workstation to the list, select the appropriate check boxes for the user or workstation to set the characteristics (*Force run*, *App Launcher*, *Start menu*, *Desktop*, *System tray*, *Quick launch*, and *Force cache*) you want applied to the application. Click *Help* for a description of each of these characteristics, or refer to “[Associations Page](#)” on page 524.

If you want to associate the application with additional users or workstations at a later time, you can use the Associations page on the Application object. For information, see “[Associations Page](#)” on page 524.
- 7** Click *Next*, review the Application object settings, then click *Finish* to create the Application object.

30.3 Establishing eDirectory Rights

By default, when a user or workstation is associated with an Application object, the User object or Workstation object is assigned trustee rights to the object. This provides Application Launcher with sufficient eDirectory rights to distribute and launch the application on the user's workstation.

However, for workstation-associated applications that are installed on Windows 98 workstations, you need to also manually assign trustee rights to any users who distribute or launch the application. Windows 98 does not differentiate between the user and workstation, so Application Launcher always uses the user's eDirectory credentials when distributing or launching workstation-associated

applications on a Windows 98 workstation. If you don't assign trustee rights to the user, the distribution or launch fails.

To assign trustee rights to a user:

- 1 In ConsoleOne, right-click the Application object, then click *Properties*.
- 2 Click the *NDS Rights* tab, then click *Trustees of this object*.
- 3 Click *Add trustee*, select the user you want to add as a trustee, then click *OK* to add the user to the trustee list. Repeat this step for all users you need to add.
- 4 Click *OK* to save the changes.

30.4 What's Next

To better manage the application you've distributed, you can configure the Application object to:

- Automatically cache the application's files to the local workstation (if the distribution requires installation of the application). This enables users to install or fix problems with the application when they are disconnected from eDirectory and your network. See “[Novell Application Launcher: Managing the Cache](#)” on page 293.
- Add the Application object to a folder in the Application Window, Application Explorer window, Application Browser window, or on the Windows Start menu. See [Chapter 25](#), “[Novell Application Launcher: Organizing Applications](#),” on page 303.
- Automatically distribute and run other applications on which it is dependent. See [Chapter 37](#), “[Advanced Distribution: Configuring Application Dependencies and Chains](#),” on page 389.
- Report on the success or failure of events such as distributing, caching, and uninstalling the application on workstations. See [Chapter 44](#), “[Reporting Application Events](#),” on page 431.
- Determine the schedule of when the application is available to users. See “[Schedule Page](#)” on page 543.
- Define many additional Application object properties to control the behavior of the application. For information about all Application object properties, see [Chapter 48](#), “[Reference: Application Object Settings](#),” on page 471.

Novell® ZENworks® Desktop Management lets you distribute Web applications to users on Windows 98 and Windows 2000/XP workstations.

Distribution of a Web applications requires Application Launcher to display an application icon that, when launched, opens the workstation's Web browser and displays the Web-based application (or other Web content). No files need to be copied to the workstation and no configuration settings are modified.

Complete the tasks in the following order to distribute a Web application:

1. [Section 31.1, “Preparing a Web Application,” on page 337](#)
2. [Section 31.2, “Configuring the Application in eDirectory,” on page 337](#)
3. [Section 31.3, “Establishing eDirectory Rights,” on page 340](#)
4. [Section 31.4, “What's Next,” on page 340](#)

31.1 Preparing a Web Application

A Web application is any application (or Web content) that can be launched via a URL in a Web browser. You are simply making the Web application's URL available to users through a shortcut displayed by Application Launcher. When a user selects the shortcut, Application Launcher launches the user's Web browser, which then displays the Web application.

To prepare a Web application for distribution to users:

- 1 Install the Web application to the appropriate Web servers.
- 2 If you use a security product, such as Novell iChain®, to provide secure authentication and access to your Web content, make sure you've established access for the users to whom you distribute the Web application.

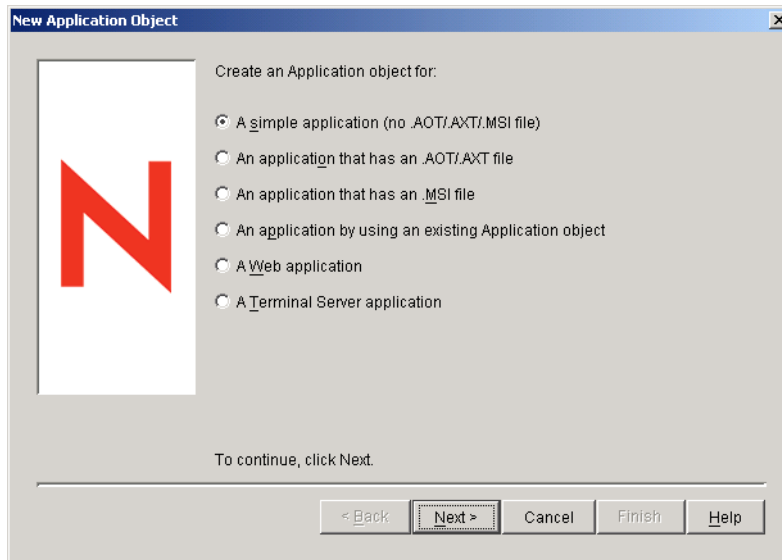
31.2 Configuring the Application in eDirectory

After you have prepared the application for distribution (see [Section 31.1, “Preparing a Web Application,” on page 337](#)), you are ready to create the application as an Application object in eDirectory, define its distribution rules, and associate it with users and workstations.

You can create the Application object in any container you want. Because Application Launcher accesses the object on behalf of the logged-in user or workstation, you should place it in a container whose partition (or a replica of the partition) is available to the user or workstation over a local area connection rather than a wide area connection. For more information, see [Chapter 51, “Reference: Application Object Location,” on page 609](#).

To create the Application object in eDirectory and configure it:

- 1 In ConsoleOne®, right-click the container where you want to create the Application object, click *New*, then click *Application* to display the New Application Object dialog box.



- 2 In the New Application Object dialog box, select the *Web application* option, then click *Next*.
- 3 Enter a name for the Application object.

The Application object's name must conform to the following rules:

- The name must be unique in the container.
- Special characters are allowed. However, plus (+), equals (=), and period (.) must be preceded by a backslash (\) if used.
- The following characters are valid in Application object names but are invalid when used in Windows folder and file names:

\ / : * ? " < > |

If you use these characters in the Application object name, they are replaced by an underscore (_) when displayed in locations controlled by Windows and not Novell Application Launcher™ (for example, on the Windows desktop).

- Uppercase and lowercase letters, as well as underscores and spaces, are displayed as you first entered them, but they aren't distinguished. For example, ZENworks_Desktop_Management and ZENWORKS DESKTOP MANAGEMENT are considered identical.

The Application object's name is visible in eDirectory™. By default, the name is also used as the Application object's icon title when displayed by Application Launcher on a user's workstation. You can, if necessary, change the icon title after the Application object has been created (Application object > *Identification* tab > *Icon* page).

- 4 Click *Next*, then enter the Web application's URL.

The URL can be to the Web application or to a Web page that provides access to the application.

- 5 Click *Next*, then define the rules used by Application Launcher to determine if a workstation meets the requirements for the application.

The distribution rules ensure that Application Launcher does not distribute the application to workstations that cannot support the application. For example, if the application runs on Windows 2000/XP only, you can create an operating system rule that prohibits distribution to Windows 98 workstations.

NOTE: The requirement for an operating system to be defined before an application is available has been removed.

In previous ZENworks versions, an OS platform had to be defined in the System Requirements before an application would be available for distribution and launching. This requirement has been removed.

The new behavior uses the following logic: If an application runs only on a specific operating system, define an operating system distribution rule. If an application does not require a specific operating system, there is no need to define a distribution rule. By default, applications without a defined operating system distribution rule are available on all supported platforms (Windows 98, Windows 2000, and Windows XP).

To add a distribution rule:

5a Click *Add*, then select the type of rule you want to define.

5b Fill in the information for the requirement (click *Help* for information about the requirement or refer to “[Distribution Rules Page](#)” on page 527), then click *OK* to add the requirement to the list.

If you want to create additional distribution rules for the application at a later time, you can use the Distribution Rules page on the Application object. For information, see “[Distribution Rules Page](#)” on page 527.

6 Click *Next*, then associate the Application object with the users or workstations that you want to distribute the application to. To do so:

6a Click *Add*, then browse for and select User or Workstation objects.

Each workstation that you want to associate with applications must first be imported into eDirectory as a Workstation object. If a workstation with which you want to associate the application has not been imported as a Workstation object, see [Part III, “Automatic Workstation Import and Removal,”](#) on page 117.

You can also select Group objects, Workstation Group objects, and container objects (Organizational Unit, Organization, or Country). If you select a container object, you are given the choice of associating all the container's User and/or Workstation objects with the application.

Associating an Application object with a Group, Workstation Group, or other container object is the preferred method of associating the Application object in eDirectory. Associating the application to a large number of User or Workstation objects (for example, more than 250) might cause increased server utilization.

IMPORTANT: Do not associate the Application object with Alias objects. Alias objects are not supported.

6b After you add the user or workstation to the list, select the appropriate check boxes for the user or workstation to set the characteristics (*Force run*, *App Launcher*, *Start menu*, *Desktop*, *System tray*, *Quick launch*, and *Force cache*) you want applied to the application. Click *Help* for a description of each of these characteristics, or refer to “[Associations Page](#)” on page 524.

If you want to associate the application with additional users or workstations at a later time, you can use the Associations page on the Application object. For information, see [“Associations Page” on page 524](#).

- 7 Click *Next*, review the Application object settings, then click *Finish* to create the Application object.

31.3 Establishing eDirectory Rights

By default, when a user or workstation is associated with an Application object, the User object or Workstation object is assigned trustee rights to the object. This provides Application Launcher with sufficient eDirectory rights to distribute and launch the application on the user's workstation.

However, for workstation-associated applications that are installed on Windows 98 workstations, you need to also manually assign trustee rights to any users who distribute or launch the application. Windows 98 does not differentiate between the user and workstation, so Application Launcher always uses the user's eDirectory credentials when distributing or launching workstation-associated applications on a Windows 98 workstation. If you don't assign trustee rights to the user, the distribution or launch fails.

To assign trustee rights to a user:

- 1 In ConsoleOne, right-click the Application object, then click *Properties*.
- 2 Click the *NDS Rights* tab, then click *Trustees of this object*.
- 3 Click *Add trustee*, select the user you want to add as a trustee, then click *OK* to add the user to the trustee list. Repeat this step for all users you need to add.
- 4 Click *OK* to save the changes.

31.4 What's Next

To better manage the application you've distributed, you can configure the Application object to:

- Automatically cache the application's files to the local workstation (if the distribution requires installation of the application). This enables users to install or fix problems with the application when they are disconnected from eDirectory and your network. See [Chapter 24, “Novell Application Launcher: Managing the Cache,” on page 293](#).
- Add the Application object to a folder in the Application Window, Application Explorer window, Application Browser window, or on the Windows Start menu. See [Chapter 25, “Novell Application Launcher: Organizing Applications,” on page 303](#).
- Automatically distribute and run other applications on which it is dependent. See [Chapter 37, “Advanced Distribution: Configuring Application Dependencies and Chains,” on page 389](#).
- Report on the success or failure of events such as distributing, caching, and uninstalling the application on workstations. See [Chapter 44, “Reporting Application Events,” on page 431](#).
- Determine the schedule of when the application is available to users. See [“Schedule Page” on page 543](#).
- Define many additional Application object properties to control the behavior of the application. For information about all Application object properties, see [Chapter 48, “Reference: Application Object Settings,” on page 471](#).

Distribution: Applications to Terminal Servers

32

Novell® ZENworks® Desktop Management lets you manage applications that are being hosted in a terminal server environment. This includes the ability to both distribute applications to the host terminal servers and then make the hosted applications available to users through Novell Application Launcher™.

This section provides information about how to distribute applications to your host terminal servers. For information about distributing terminal server applications to users, see [Chapter 28, “Distribution: Simple Applications,” on page 315](#) and [Chapter 29, “Distribution: Complex Applications,” on page 321](#).

Distributing applications to a terminal server is much the same as distributing applications to a user or workstation, which means you can follow the processes described in the sections referenced above. However, you should also be aware of the following:

- You can distribute simple applications, AOT/AXT applications, or MSI applications to a terminal server.
- You can use user associations or workstation associations to distribute applications.

To use user associations, you must install Application Launcher on the terminal server, create a User object in Novell eDirectory™ for the terminal server, and associate the desired applications with the terminal server's User object.

To use workstation associations, you must install Application Launcher and Workstation Manager on the terminal server, import the terminal server into eDirectory as a Workstation object, and associate the desired applications with the terminal server's Workstation object.

- For both user-associated applications and workstation-associated applications, you must be logged on at the terminal server console through a Windows administrator account to ensure successful distribution to the terminal server.
- Application Launcher does not create a NAL cache directory on the terminal server. Because there is no NAL cache directory, the following applies:
 - Distribution of MSI applications to the terminal server requires the appropriate network client (Microsoft Client or Novell Client™) to be installed on the terminal server. Distribution cannot occur through the ZENworks Middle Tier Server because there is no NAL cache to copy the MSI source package to. A possible workaround to this issue is to create a simple Application object that distributes the .msi package to the terminal server and launches the Windows Installer to install the package.
 - Force cache does not work.
 - Uninstall does not work. You must manually uninstall the application files.
- For MSI applications, to ensure that the applications are installed for multisession access, use the *change user /install* command in the pre-distribution script and the *change user /execute* command in the post-distribution script. This causes the application to be installed to the systemroot rather than an individual user's home directory.

- You can use the Terminal Server distribution rule to ensure that an application is only distributed to a terminal server. For information about the Terminal Server distribution rule, see [“Distribution Rules Page” on page 527](#)
- If you want an application to be distributed when a user launches it (rather than you installing), the user needs to have appropriate file system and registry access. To install an MSI application on the terminal server, the user must be a member of the Administrators group. Microsoft Windows Installer does not allow non-administrator users to do installations from a terminal client session.

Advanced Distribution: Creating Distribution Rules

33

Novell® ZENworks® Desktop Management lets you create rules to control distribution of an application.

Novell Application Launcher™ or the Workstation Helper applies the rules to the workstation when the application is associated to either the user or the workstation. If the workstation does not meet the distribution rules, the application is not distributed.

You can create distribution rules based on a variety of criteria, such as operating system type and version, available hard disk space, and existence of certain files. Rules can be simple or quite complex. The following sections provide information to help you create rules that best meet your distribution needs:

- [Section 33.1, “Types of Distribution Rules,” on page 343](#)
- [Section 33.2, “AND/OR Boolean Operators and Groups,” on page 344](#)
- [Section 33.3, “Distribution Rules vs. Legacy System Requirements,” on page 345](#)
- [Section 33.4, “Distribution Rules Examples,” on page 346](#)
- [Section 33.5, “Creating Distribution Rules,” on page 347](#)
- [Section 33.6, “Creating Distribution Rules by Importing Legacy System Requirements,” on page 348](#)
- [Section 33.7, “Maintaining Legacy System Requirements,” on page 352](#)

33.1 Types of Distribution Rules

You can use a variety of rules to determine whether or not an application is distributed to a workstation. These rules can be used individually or joined together to create more complex rules. Below are brief descriptions of each rule:

- **Applications:** Lets you base distribution on the presence (or absence) of a specific application. The application must have been distributed through an Application object.
- **Client:** Lets you base distribution on whether the workstation is authenticated to eDirectory through the Novell Client™ or the ZENworks Middle Tier Server.
- **Connection speed:** Lets you base distribution on the speed of the workstation's network connection.
- **Disk space:** Lets you base distribution on the amount of free disk space on the workstation.
- **Environment variables:** Lets you base distribution on the presence (or absence) of specific environment variables.
- **File date:** Lets you base distribution on the date of a specific file.
- **File existence:** Lets you base distribution on the presence (or absence) of a specific file.
- **File size:** Lets you base distribution on the size of a specific file.
- **File version:** Lets you base distribution on the version of a specific file.

- **Memory:** Lets you base distribution on the amount of memory on the workstation.
- **Operating system:** Lets you base distribution on a specific operating system.
- **Processor:** Lets you base distribution on a specific processor type.
- **Registry:** Lets you base distribution on the presence (or absence) of specific registry values.
- **Remote access:** Lets you base distribution on Application Launcher's operation mode, either remote mode or local (LAN) mode.
- **Terminal server:** Lets you base distribution on the presence (or absence) of Microsoft Terminal Services.

33.2 AND/OR Boolean Operators and Groups

You can use AND/OR Boolean operators to join individual rules or groups of rules to create more flexible distribution conditions.

AND Operator

When using the AND operator, both joined rules must be met for the distribution to occur. For example:

```
Processor type(Processor) >= Pentium III AND System memory(RAM) >= 512
```

For the application to be distributed to the workstation in the above example, both rules must evaluate to true: the workstation must be a Pentium III or better with a minimum of 512 MB RAM.

OR Operator

When using the OR operator, either of the joined rules must be met for the distribution to occur. For example:

```
Processor type(Processor) >= Pentium III OR System memory(RAM) >= 512
```

For the application to be distributed to the workstation in the above example, only one of the rules must evaluate to true: the workstation must be at least a Pentium III, or it must have a minimum of 512 MB RAM.

Groups

You can use both the AND and OR operators to join groups of rules. For example:

```
( Processor type(Processor) >= Pentium III AND System memory(RAM) >=
1024)
OR
( Processor type(Processor) >= Pentium IV AND System memory(RAM) >=
512)
```

For the application to be distributed to the workstation in the above example, only one of the groups must evaluate to true: either the workstation must be a Pentium III with 1 GB of RAM, or it must be a Pentium 4 with 512 MB of RAM.

Nested Groups

You can nest groups two levels deep. In the following example, Group3 and Group4 are nested within Group2:

```
Group1  
OR  
(Group2 AND (Group3 OR Group4))
```

33.3 Distribution Rules vs. Legacy System Requirements

Prior to ZENworks 6.5, distribution rules were known as system requirements and did not include the ability to use both AND/OR Boolean operators and to create groupings of rules. Because of the new operators and groupings, Application Launcher versions prior to ZENworks 6.5 cannot understand distribution rules.

To ensure that pre-ZENworks 6.5 versions of Application Launcher can continue to work in a ZENworks 7 environment, the pre-ZENworks 6.5 system requirements are preserved as legacy system requirements. Therefore, in a mixed-version environment, you need to decide how you want to use distribution rules and legacy system requirements together. You have the following options:

- **Define distribution rules only:** The ZENworks 6.5 (or later) version of Application Launcher can read the distribution rules. Pre-ZENworks 6.5 versions cannot read the distribution rules and therefore are unable to distribute the application.
- **Define distribution rules and legacy system requirements:** ZENworks 6.5 (or later) versions use the distribution rules and pre-ZENworks 6.5 versions use the legacy system requirements. This method enables you to maintain the legacy system requirements for pre-ZENworks 6.5 Application Launcher while using the grouping, operator logic, and new rules available beginning with ZENworks 6.5. If you use this method, you can define the legacy system requirements first and then use them to populate the distribution rules. After populating the distribution rules, you can modify them to meet your needs.
- **Define legacy system requirements only:** Both ZENworks 6.5 (or later) and pre-ZENworks 6.5 versions use the legacy system requirements. This solution reduces administrative maintenance of distribution rules and system requirements, but excludes you from using the new grouping, operators, and rules. Be aware that if you define any distribution rules, ZENworks 6.5 (or later) versions of Application Launcher use the distribution rules, not the legacy system requirements. The ZENworks 7 Application Launcher checks first for the existence of distribution rules; only if no distribution rules exist does it then check for legacy system requirements.

If you have Windows NT 4 workstations in your environment that you are continuing to manage through the use of the ZENworks for Desktops 4.0.1 version of Novell Application Launcher, you need to retain your legacy system requirements. For information about Windows NT 4 support in ZENworks 7, see “[Interoperability with Windows NT 4 Workstations](#)” in “[Interoperability with ZENworks for Desktops 4.x](#)” in “[Interoperability](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

33.4 Distribution Rules Examples

You can use AND and OR Boolean operators when defining the rules that control the distribution of an application. You can also use groups of rules to further control the distribution. Examples of using AND/OR Boolean operators and groups are provided below.

33.4.1 Simple Rule Using an OR Operator

You want to require a workstation to have either a Pentium III processor (or better) or the Windows 2000 operating system. To do so, use the following rule:

```
Processor type(Processor) >= Pentium III OR OS version(Windows NT/  
2000/XP) >= 5.00.2195
```

To create this rule:

- 1 On the Distribution Rules page, click the *Add* button, then select *Processor*.
- 2 In the Processor Rule dialog box, select *Greater than or equal to (>=)*, select *Pentium III*, then click *OK* to add the rule to the *Add rules to control availability of this application* list.
- 3 On the Distribution Rules page, click the *Add* button, then select *Operating system*.
- 4 In the Operating System Rule dialog box, select *Windows NT/2000/XP*, select *Greater than or equal to (>=)*, enter *5.00.2195*, then click *OK* to add the rule to the *Add rules to control availability of this application* list.

The rule is added to the list with an AND operator.

- 5 In the list, change the AND operator, located in front of the OS Version rule, to an OR operator.

33.4.2 Simple Group

You want to require a workstation to have either a Pentium III processor (or better) or the Windows 2000 operating system with at least 512 MB of memory. To do so, use the following rule:

```
Processor type(Processor) >= Pentium III OR (OS version(Windows NT/  
2000/XP) >= 5.00.2195 AND System memory(RAM) >= 512)
```

To create this rule:

- 1 On the Distribution Rules page, click the *Add* button, then select *Processor*.
- 2 In the Processor Rule dialog box, select *Greater than or equal to (>=)*, select *Pentium III*, then click *OK* to add the rule to the *Add rules to control availability of this application* list.
- 3 On the Distribution Rules page, click the *Add* button, then select *New group* to add a new group to the *Add rules to control availability of this application* list.

The new group is labeled Group 1, unless you've previously added groups to the list. In addition, it is assigned the AND operator by default.

- 4 Locate Group 1 in the list and change the AND operator to an OR operator.
- 5 Next to Group 1 in the list, click the *Add to Group* button, then select *Operating System*.
- 6 In the Operating System Rule dialog box, select *Windows NT/2000/XP*, select *Greater than or equal to (>=)*, enter *5.00.2195*, then click *OK* to add the rule under Group 1 in the list.
- 7 Next to Group 1 in the list, click the *Add to Group* button, then select *Memory*.

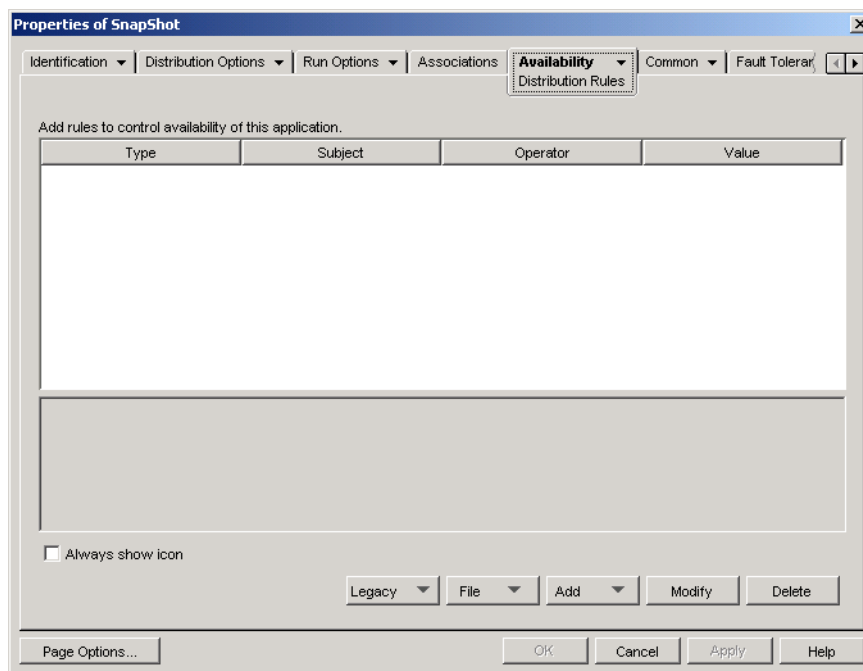
- 8 In the Memory Rule dialog box, select *greater than or equal to* (\geq), enter 512, then click *OK* to add the rule under Group 1 in the list.

33.5 Creating Distribution Rules

The following steps explain how to create distribution rules that do not have existing legacy system requirements (see [Section 33.3, “Distribution Rules vs. Legacy System Requirements,”](#) on [page 345](#)). If the application has legacy system requirements, you can import them to form the basis of the distribution rules. For instructions, see [Section 33.6, “Creating Distribution Rules by Importing Legacy System Requirements,”](#) on [page 348](#).

- 1 In ConsoleOne®, right-click the Application object for which you want to create distribution rules, then click *Properties* to display the Application object's property pages.
- 2 Click the *Availability* tab > *Distribution Rules* to display the Distribution Rules page.

If there are legacy system requirements and no distribution rules for the Application object, you are prompted to import the legacy system requirements into the distribution rules. If you want to use the legacy system requirements as the basis for your distribution rules, click *Yes*. Otherwise, click *No*. If you change your mind later, you can use the Import Legacy Settings option on the Distribution Rules page to import the requirements.



- 3 Use the *Add* button to add rules and new groups:
 - **To add a rule:** Click *Add*, then select the rule to display a dialog box you can use to define the rule. For a brief description of the rules, see [Section 33.1, “Types of Distribution Rules,”](#) on [page 343](#). For more detailed information about a rule, click the *Help* button in the rule's dialog box or see [“Distribution Rules Page”](#) on [page 527](#).
 - **To add a group:** Click *Add*, then select *New group*.
 - **To add a rule to a group:** Locate the group in the list, click *Add to group*, then select the rule.

- **To add a group to a group:** Locate the group in the list, click *Add to group*, then select *New group*.

For examples of how to use AND/OR operators and groups, see [Section 33.2, “AND/OR Boolean Operators and Groups,” on page 344](#) and [Section 33.4, “Distribution Rules Examples,” on page 346](#).

- 4 (Conditional) If you want Application Launcher to display the application's icon even if the workstation does not satisfy the distribution rules, select the *Always show icon* option.
If you select this option and one or more rules is not met, the icon is displayed in a disabled state. Users can right-click the disabled icon, select *Details*, then select *Requirements* to view a list of all of the distribution requirements that were defined for the application.
- 5 When finished, click *OK* to save your changes.

33.6 Creating Distribution Rules by Importing Legacy System Requirements

You can import an application's legacy system requirements to form the basis of its distribution rules.

If an application has legacy system requirements and no distribution rules, you are prompted to import the legacy system requirements into the distribution rules when you open the Distribution Rules page on the Application object.

If an application has distribution rules already defined, you are not prompted to import the legacy system requirements when you open the Distribution Rule page on the Application object. You can, however, use the Import Legacy Settings option on the Distribution Rules page to import the requirements.

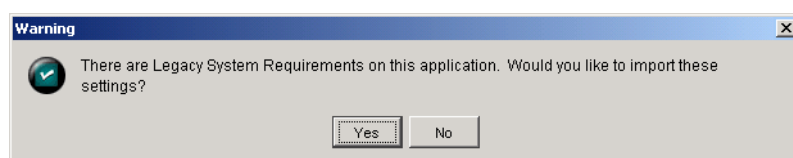
The following sections provide instructions for handling both scenarios:

- [Section 33.6.1, “Importing the Requirements When Opening the Distribution Rules Page,” on page 348](#)
- [Section 33.6.2, “Importing the Requirements After Opening the Distribution Rules Page,” on page 350](#)

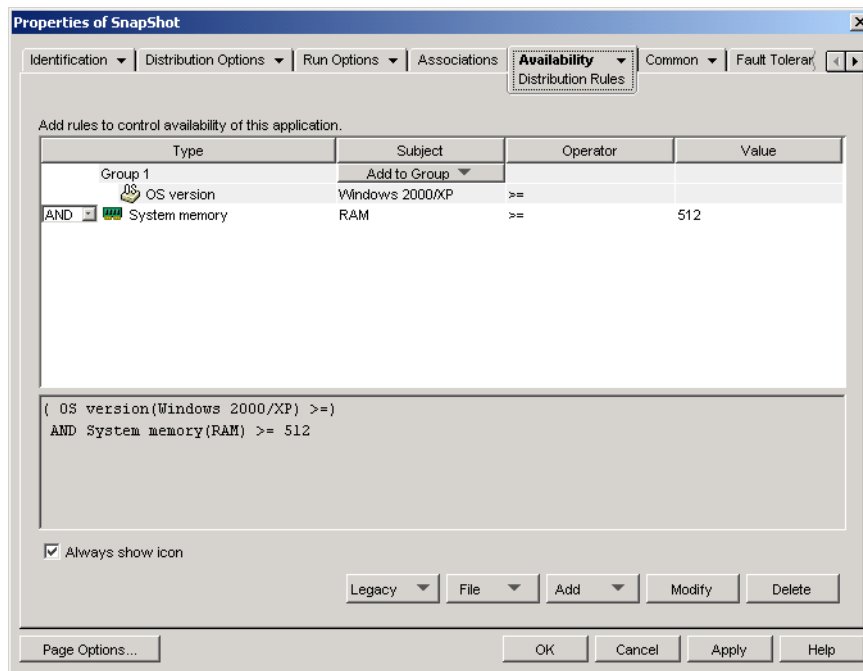
33.6.1 Importing the Requirements When Opening the Distribution Rules Page

- 1 In ConsoleOne, right-click the Application object for which you want to create distribution rules by importing legacy system requirements, then click *Properties* to display the Application object's property pages.
- 2 Click the *Availability* tab > *Distribution Rules* to display the Distribution Rules page.

If there are legacy system requirements and no distribution rules for the Application object, you are prompted to import the legacy system requirements into the distribution rules.



3 Click *Yes* to import the requirements.



4 Modify the distribution rules as desired:

- **To add a rule:** Click *Add*, then select the rule to display a dialog box you can use to define the rule. For a brief description of the rules, see [Section 33.1, “Types of Distribution Rules,” on page 343](#). For more detailed information about a rule, click the *Help* button in the rule's dialog box or see [“Distribution Rules Page” on page 527](#).
- **To add a group:** Click *Add*, then select *New group*.
- **To add a rule to a group:** Locate the group in the list, click *Add to group*, then select the rule.
- **To add a group to a group:** Locate the group in the list, click *Add to group*, then select *New group*.

For examples of how to use AND/OR operators and groups, see [Section 33.2, “AND/OR Boolean Operators and Groups,” on page 344](#) and [Section 33.4, “Distribution Rules Examples,” on page 346](#).

5 If you don't want Application Launcher to display the application's icon on workstations that don't satisfy the distribution rules, deselect the *Always show icon* option.

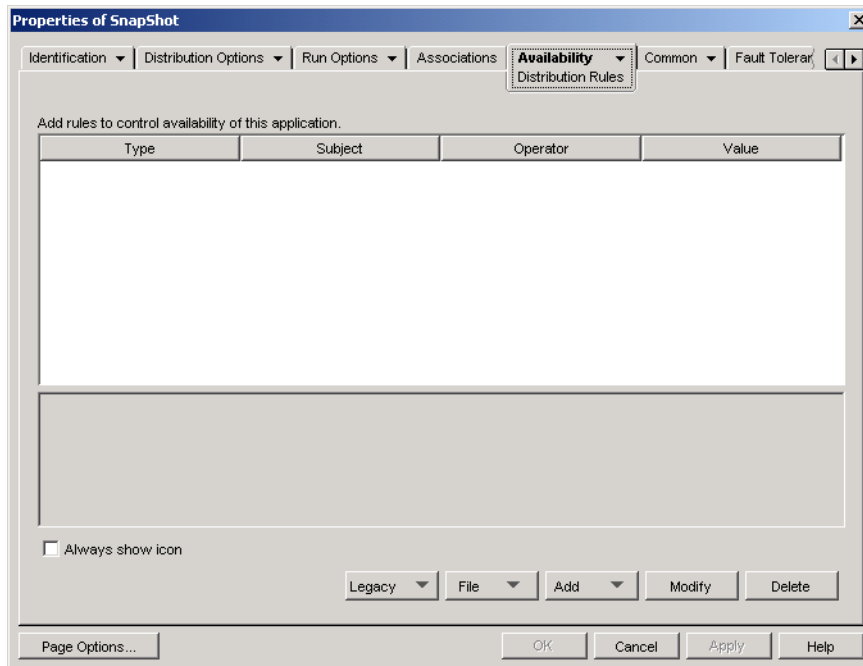
When you imported the legacy system requirements ([Step 3](#)), the *Always show icon* option was automatically turned on, even if it was previously turned off for all legacy system requirements. You might need to deselect the option to maintain the previously-configured behavior.

If you select this option and one or more rules is not met, the icon is displayed in a disabled state. Users can right-click the disabled icon, select *Details*, then select *Requirements* to view a list of all of the distribution requirements that were defined for the application.

6 When finished, click *OK* to save your changes.

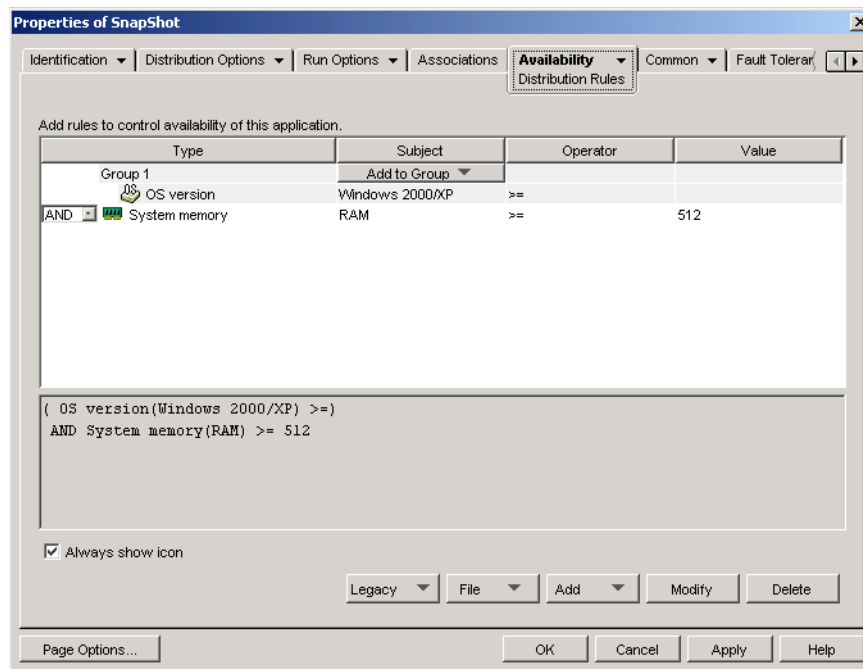
33.6.2 Importing the Requirements After Opening the Distribution Rules Page

- 1 In ConsoleOne, right-click the Application object for which you want to create distribution rules by importing legacy system requirements, then click *Properties* to display the Application object's property pages.
- 2 Click the *Availability* tab > *Distribution Rules* to display the Distribution Rules page.



- 3 Click the *Legacy* button, then click *Import legacy settings*.

If you have already defined distribution rules, you are prompted that they will be overwritten by the legacy system rules. Otherwise, the system requirements are imported without further prompting.



4 Modify the new distribution rules as desired:

- **To add a rule:** Click *Add*, then select the rule to display a dialog box you can use to define the rule. For a brief description of the rules, see [Section 33.1, “Types of Distribution Rules,” on page 343](#). For more detailed information about a rule, click the *Help* button in the rule's dialog box or see [“Distribution Rules Page” on page 527](#).
- **To add a group:** Click *Add*, then select *New group*.
- **To add a rule to a group:** Locate the group in the list, click *Add to group*, then select the rule.
- **To add a group to a group:** Locate the group in the list, click *Add to group*, then select *New group*.

For examples of how to use AND/OR operators and groups, see [Section 33.2, “AND/OR Boolean Operators and Groups,” on page 344](#) and [Section 33.4, “Distribution Rules Examples,” on page 346](#).

5 If you don't want Application Launcher to display the application's icon on workstations that don't satisfy the distribution rules, deselect the *Always show icon* option.

When you imported the legacy system requirements ([Step 3](#)), the *Always show icon* option was automatically turned on, even if it was previously turned off for all legacy system requirements. You might need to deselect the option to maintain the previously-configured behavior.

If you select this option and one or more rules is not met, the icon is displayed in a disabled state. Users can right-click the disabled icon, select *Details*, then select *Requirements* to view a list of all of the distribution requirements that were defined for the application.

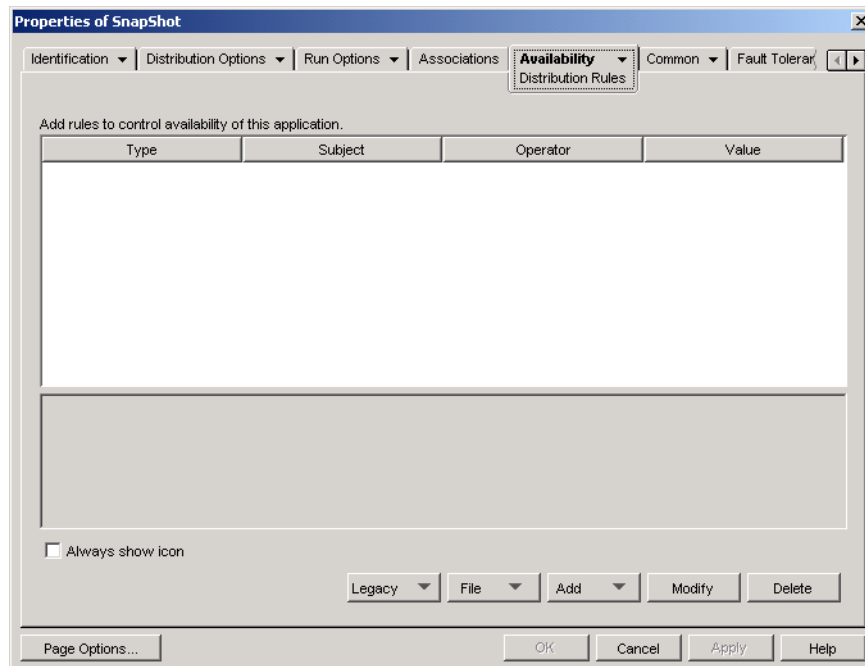
6 When finished, click *OK* to save your changes.

33.7 Maintaining Legacy System Requirements

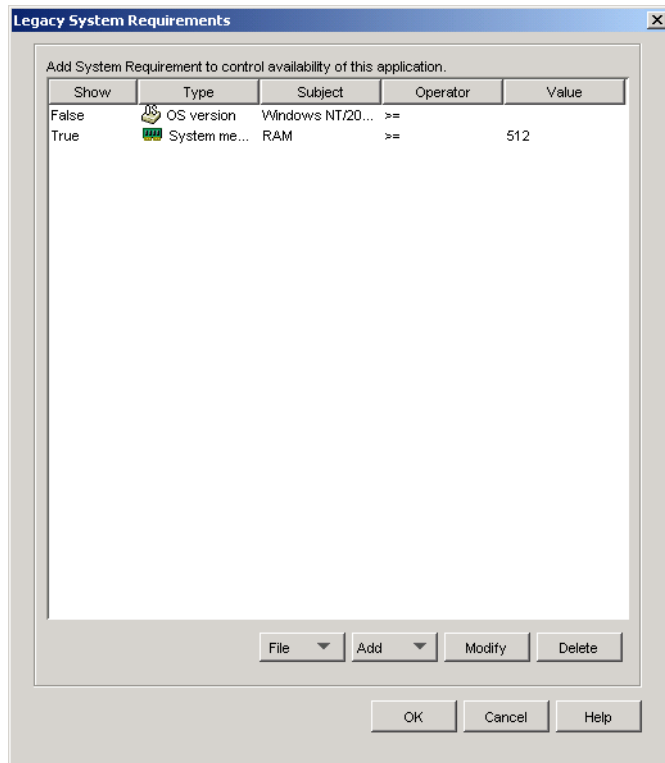
If your environment includes pre-ZENworks 7 versions of Application Launcher, you need to continue to maintain your applications' legacy system requirements in order to support the pre-7 Application Launcher versions. Application Launcher versions prior to ZENworks 7 do not support distribution rules.

To add, remove, or modify an application's legacy system requirements:

- 1 In ConsoleOne, right-click the Application object whose legacy system requirements you to add, remove, or modify, then click *Properties* to display the Application object's property pages.
- 2 Click the *Availability* tab > *Distribution Rules* to display the Distribution Rules page.



- 3 Click the *Legacy* button, then click *Edit legacy settings* to display the Legacy System Requirements dialog box.



- 4 Modify the system requirements as desired:

- **To add a requirement:** Click *Add*, then select the requirement to display a dialog box you can use to define the requirement. For information about the requirement, click the *Help* button in the requirement's dialog box.
- **To remove a requirement:** Select the requirement in the list, then click *Delete*.
- **To modify a requirement:** Select the requirement in the list, then click *Modify*. For information about the requirement, click the *Help* button in the requirement's dialog box.

- 5 When finished, click *OK* to save your changes.

Advanced Distribution: Transferring Applications Using BITS

34

This functionality is available beginning with Support Pack 1 of Novell® ZENworks® 7. The Support Pack 1 Desktop Management Agent must be installed on each workstation that will use the Microsoft® Background Intelligent Transfer Service (BITS) to transfer applications to the workstation. Versions of the Desktop Management Agent prior to Support Pack 1 do not support BITS.

Novell Application Launcher™ can use BITS to transfer applications to a workstation. Unlike Application Launcher which competes with other applications for available network bandwidth, BITS uses idle network bandwidth to transfer files, increasing or decreasing the rate at which files are transferred based on the amount of idle network bandwidth available. For example, if a network application begins to consume more bandwidth, BITS decreases its transfer rate.

The following sections provide background information and setup instructions for using BITS. You should complete the sections in the order listed.

1. [Section 34.1, “Understanding How Application Launcher Uses BITS,” on page 355](#)
2. [Section 34.2, “Setting Up Workstations,” on page 357](#)
3. [Section 34.3, “Enabling Application Launcher to Use BITS,” on page 358](#)
4. [Section 34.4, “Configuring an Application to be Transferred by BITS,” on page 360](#)
5. [Section 34.5, “Changing the Default Settings for a BITS Job,” on page 361](#)
6. [Section 34.6, “Changing the BITS Maximum Network Bandwidth Setting,” on page 362](#)

34.1 Understanding How Application Launcher Uses BITS

The following sections provide information to help you understand the interaction between Application Launcher and BITS:

- [Section 34.1.1, “Application Launcher and BITS Process,” on page 356](#)
- [Section 34.1.2, “Application Launcher Transfer vs. BITS Transfer,” on page 356](#)
- [Section 34.1.3, “BITS Job Settings,” on page 356](#)
- [Section 34.1.4, “BITS Maximum Bandwidth Setting,” on page 357](#)
- [Section 34.1.5, “Scalability,” on page 357](#)

For additional information about general BITS concepts and functionality, see [Background Intelligent Transfer Service \(http://msdn.microsoft.com/library/default.asp?url=/library/en-us/bits/bits/bits_start_page.asp\)](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/bits/bits/bits_start_page.asp) in the MSDN Library.

34.1.1 Application Launcher and BITS Process

For Application Launcher to use BITS to transfer an application, Application Launcher must be enabled to use BITS as explained in [Section 34.3, “Enabling Application Launcher to Use BITS,” on page 358](#), and the application must be configured properly as explained in [Section 34.4, “Configuring an Application to be Transferred by BITS,” on page 360](#).

After Application Launcher has been BITS enabled and an application configured for BITS, Application Launcher creates a BITS job that contains the application content (files, Application Object settings, etc.) and job settings (Minimum Retry Delay, No Progress Timeout, and Priority) and then queues the job for BITS. BITS transfers the application content to a temporary directory on the local drive (%systemroot%\temp\%jobid%, where %systemroot% is the Windows system directory and %jobid% is the ID of the BITS job). As soon as BITS completes the transfer, Application Launcher copies the application content to the NAL cache and then distributes the application when it is installed or launched.

For specific information about how BITS processes jobs, see [Life Cycle of a BITS Job \(http://msdn.microsoft.com/library/en-us/bits/bits/life_cycle_of_a_bits_job.asp\)](http://msdn.microsoft.com/library/en-us/bits/bits/life_cycle_of_a_bits_job.asp).

34.1.2 Application Launcher Transfer vs. BITS Transfer

Any of the following circumstances will cause Application Launcher to transfer the application itself rather than use BITS:

- The workstation does not have BITS v2.0 installed.
- BITS encounters a fatal error during transfer of the application content.
- BITS encounters a transient error during transfer of the application content and cannot make any progress in the allotted time (**No Progress Timeout** setting).
- The user launches the application before BITS has completed the transfer. This is the default Application Launcher behavior. However, you can configure Application Launcher to not resume control of the transfer, in which case the user cannot launch the application until BITS finishes the transfer. Or, you can have Application Launcher prompt the user as to whether or not to interrupt the BITS transfer and have Application Launcher immediately download the application. See [“Enabling Application Launcher to Use BITS” on page 358](#).

34.1.3 BITS Job Settings

When Application Launcher creates a job and passes it to BITS, it not only passes the application content (files, Application Object settings, etc.) but also passes three configuration settings:

- **Minimum Retry Delay:** If BITS encounters an error during transfer of the application, BITS classifies it as a fatal error or a transient error. BITS cannot recover from fatal errors; fatal errors require administrator intervention to resolve the problem. BITS can possibly recover from transient errors. This setting lets you specify the minimum amount of time you want BITS to wait after a transient error occurs before trying to transfer the application again. The default is 600 seconds (10 minutes).
- **No Progress Timeout:** This setting lets you specify how many days you want BITS to continue to attempt to transfer the application after a transient error has occurred if no progress is made. For example, the default setting (14 days) causes BITS to continue to attempt the transfer for 14 days after the error. If any transfer progress is made during the 14 days, the

counter is reset. If BITS times out because no progress is being made, control of the transfer is returned to Application Launcher, which then transfers the application itself.

- **Priority:** This setting lets you assign a priority level to the BITS transfer. You can choose from one foreground priority and three background priorities (high, normal, low). Foreground is the highest priority, followed by the three background priorities. The default is Background Normal.

These settings are configurable for each application (Application object > Distribution Options tab > BITS Settings page). You can use the default settings, or you can change the settings based upon application or user needs. These settings are explained in more detail in [Section 34.5, “Changing the Default Settings for a BITS Job,” on page 361](#).

34.1.4 BITS Maximum Bandwidth Setting

Windows XP includes a Group Policy setting for the maximum amount of the workstation’s idle network bandwidth that BITS uses. By default, this setting is not configured, which enables BITS to use all of the workstation’s available idle bandwidth.

If you have BITS running on a large number of workstations, this might impact your network. To reduce this impact, during periods of high utilization you can limit the amount of bandwidth available to BITS. Instructions for using ZENworks to manage the BITS maximum bandwidth setting through the use of a Windows Group Policy are provided in [Section 34.6, “Changing the BITS Maximum Network Bandwidth Setting,” on page 362](#)

IMPORTANT: Windows 2000 does not include a Group Policy setting for BITS maximum bandwidth.

34.1.5 Scalability

If you plan to deliver a large number of applications at one time or deliver applications with a large number of files, you should first review the [BITS scalability guidelines \(http://msdn.microsoft.com/library/en-us/bits/bits/best_practices_when_using_bits.asp\)](http://msdn.microsoft.com/library/en-us/bits/bits/best_practices_when_using_bits.asp) provided by Microsoft.

34.2 Setting Up Workstations

- 1 Make sure the Support Pack 1 Desktop Management Agent is installed on any workstations where you want to use BITS.

The Support Pack 1 Desktop Management Agent must be installed on each workstation that will use BITS to transfer applications to the workstation. Versions of the Desktop Management Agent prior to Support Pack 1 do not support BITS. If necessary, see “[Installing and Configuring the Desktop Management Agent](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide* for instructions about installing the Support Pack 1 Desktop Management Agent.

- 2 Install BITS v2.0 (minimum requirement) on any workstations where you want to use BITS.

BITS v2.0 is already included in Microsoft Windows XP SP2. You do not need to install it on Windows XP workstation with SP2 or newer installed.

For workstations with Windows XP, Windows XP SP1, or Windows 2000, you can download BITS v2.0 from [Microsoft Support \(http://support.microsoft.com/default.aspx?kbid=842773\)](http://support.microsoft.com/default.aspx?kbid=842773).

- 3 Make sure BITS is running on the workstations.

BITS is a Windows Service. You can verify that it is running by viewing Services under the Administrative Tools in the Windows Control Panel.

- 4 Make sure that BITS has the required network file system rights to access the application files it will transfer.

BITS requires the same access as Application Launcher to transfer files from a network server. If Application Launcher can transfer files, BITS will be able to. For more information about the required file system access, see [Chapter 23, “Novell Application Launcher: Managing Authentication and File System Access,”](#) on page 283.

- 5 Continue with the next section, [Enabling Application Launcher to Use BITS](#).

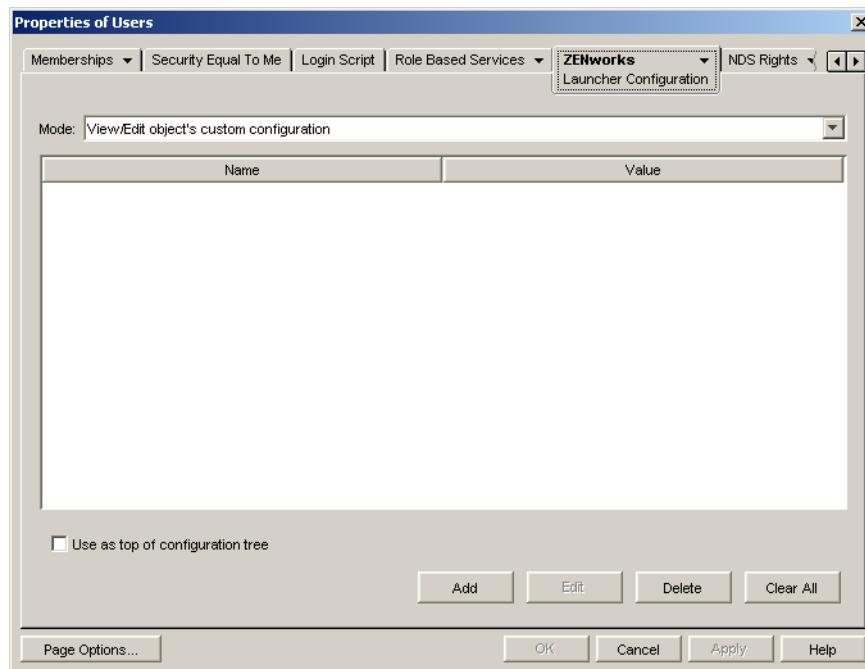
34.3 Enabling Application Launcher to Use BITS

By default, Application Launcher is not configured to use BITS. You must modify the Application Launcher configuration settings in ConsoleOne to enable BITS.

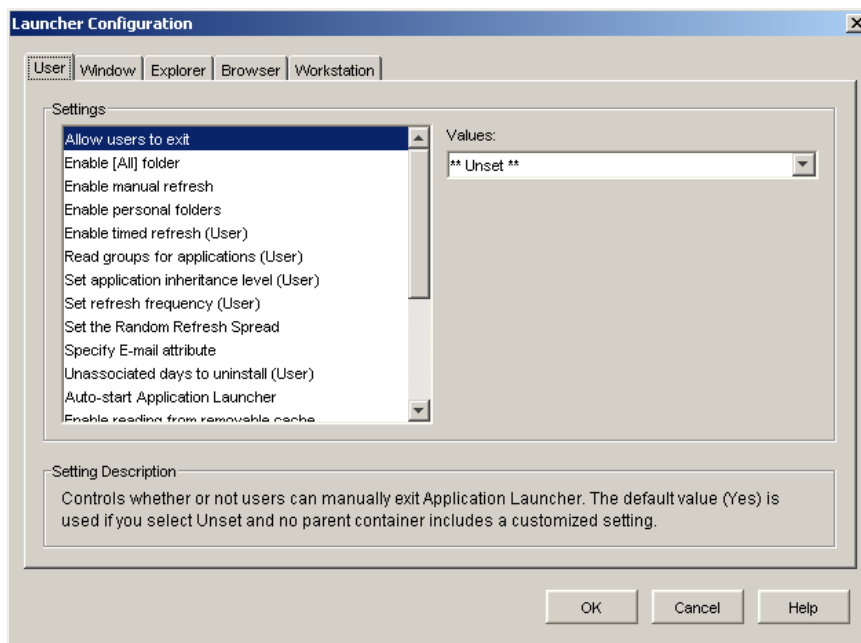
As with all Application Launcher configuration settings, you can modify the BITS settings for a User object, Workstation object, or container (Organization Unit, Organization, Group, etc.) object. For example, if you want to enable BITS for a specific user, you can modify the configuration settings for that User object only. However, if you want to enable BITS for all users in a specific container, you can modify the configuration settings for that container object, in which case all users in the container inherit the container setting.

To enable Application Launcher:

- 1 In ConsoleOne®, right-click the User, Workstation, or container object where you want to enable BITS, then click *Properties*.
- 2 Click the *ZENworks* tab > Launcher Configuration to display the Launcher Configuration page.



- 3 Click Add to display the Launcher Configuration dialog box.



Depending on the type of object you're configuring, the User tab or Workstation tab might not be available. The User tab is not displayed on Workstation or Workstation Group objects, and the Workstation tab is not displayed on User or User Group objects.

- 4 (Conditional) If you are configuring Application Launcher for a user, user group, or a container with users, open the User tab and configure the following two settings:

Enable BITS: Set this option to Yes to enabled Application Launcher to use BITS to transfer user-associated applications.

Allow User to Override BITS Transfer: Because BITS uses idle network bandwidth to transfer applications, an application might not be available when a user attempts to launch it. Specify the action you want to occur in this case:

- Yes (default): Causes Application Launcher to cancel the BITS job and immediately transfer the application itself. Rather than starting the transfer over, Application Launcher resumes transfer of the application where BITS left off.
- No: Causes BITS to maintain control of the transfer; the user is unable to launch the application until the transfer is complete.
- Prompt: Prompts the user as to whether or not to interrupt the BITS transfer and have Application Launcher immediately download the application.

- 5 (Conditional) If you are configuring Application Launcher for a workstation, workstation group, or a container with workstations, open the Workstation tab and configure the following setting:

Enable BITS (Workstation): Set this option to Yes to enabled Application Launcher to use BITS to transfer workstation-associated applications.

- 6 Click OK to save your changes, then click OK to close the object's properties pages.

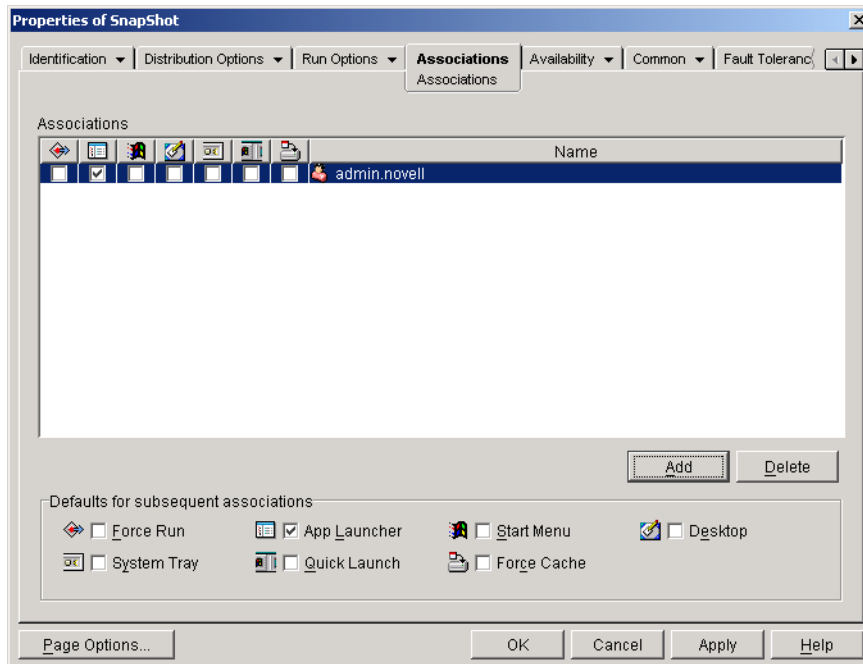
- 7 Continue with the next section, **Configuring an Application to be Transferred by BITS**.

34.4 Configuring an Application to be Transferred by BITS


Application Launcher uses BITS to transfer an application to a user or workstation only if that user's or workstation's association with the application is marked Force Cache. Otherwise, Application Launcher transfers the application.

To mark an application association as Force Cache:

- 1 In ConsoleOne, right-click the Application object for which you want to configure BITS support, then click *Properties* to display the Application object's property pages.
- 2 Click the *Associations* tab to display the Associations page



- 3 For each association (user or workstation) for which you want to use BITS to transfer the application content, select the association's Force Cache box.

For example, in the above screen shot, if you want to use BITS to transfer the application to the admin.novell user's workstation, you must select the Force Cache  box.

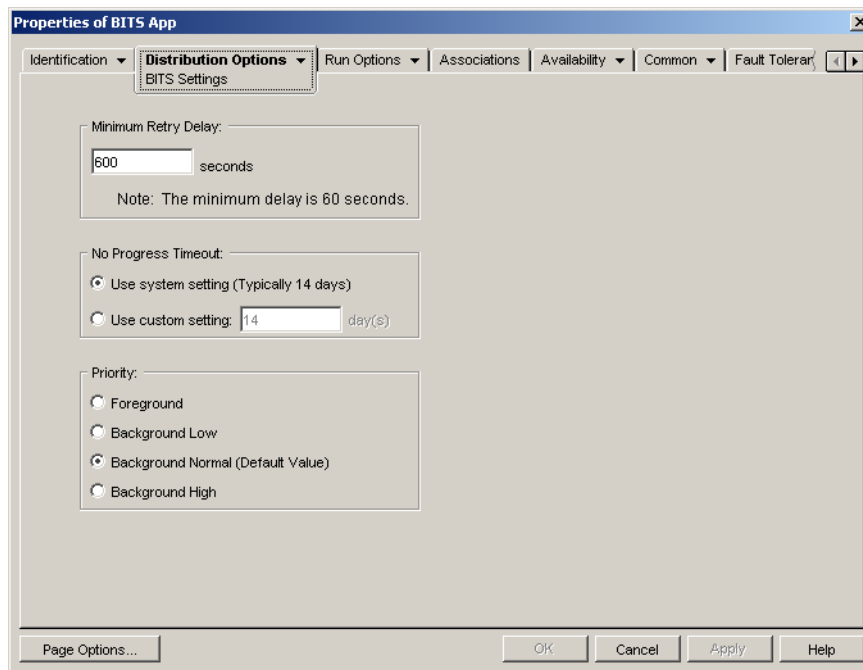
Application Launcher uses BITS only for associations that are marked Force Cache. Application Launcher transfers the application for any associations that are not marked Force Cache.

- 4 If you want to change the settings (Minimum Retry Delay, No Progress Timeout, and Priority) that Application Launcher uses when creating the application's BITS job, skip to the next section, [Changing the Default Settings for a BITS Job](#). Otherwise, click OK to save your changes and close the Application object's property pages.

34.5 Changing the Default Settings for a BITS Job

When using BITS to transfer an application, Application Launcher creates a BITS job that contains the application content (files, Application Object settings, etc.) and job settings (Minimum Retry Delay, No Progress Timeout, and Priority) and then queues the job for BITS. If necessary, you can change the job settings for an application.

- 1 In ConsoleOne, right-click the Application object for which you want to modify the BITS job settings, then click *Properties* to display the Application object's property pages.
- 2 Click the *Distribution Options* tab > *BITS Settings* to display the BITS Settings page.



- 3 Configure the following options as desired:

Minimum Retry Delay: If BITS encounters an error during transfer of the application, BITS classifies it as a fatal error or a transient error. BITS cannot recover from fatal errors; fatal errors require administrator intervention to resolve the problem. BITS can possibly recover from transient errors.

Use this option to specify the minimum amount of time you want BITS to wait after a transient error occurs before trying to transfer the application again. The default is 600 seconds, or 10 minutes. The minimum is 60 seconds. The maximum setting is 2,147,483,647 seconds.

No Progress Timeout: Use this option to specify how many days you want BITS to continue to attempt to transfer the application after a transient error has occurred if no progress is made. For example, a setting of 14 days causes BITS to continue to attempt the transfer for 14 days after the error. If any transfer progress is made during the 14 days, the counter is reset.

- *Use System Setting (Typically 14 Days):* Select this option to use the Windows system setting. The Windows system setting comes from either 1) the BITS default setting, which is 14 days, or 2) the Timeout (Days) for Inactive Jobs setting in the Windows Group Policy, which is not set by default. If you select this option, the BITS default setting (14

days) is used unless the Windows Group Policy setting has been assigned a value. You can use the Windows Group Policy Editor (gpedit.msc) to view and change the Windows Group Policy setting.

- *Use Custom Setting:* Select this option to manually enter a timeout period.
 - The minimum setting is 0 days. Enter 0 only if you do not want BITS to attempt to transfer the application again after it encounters a transient error; in this case, BITS immediately returns control of the transfer to Application Launcher.
 - The maximum setting is 24,855 days. However, BITS compares this number to the number in the Timeout (Days) for Inactive Jobs setting in the Windows Group Policy. If the Timeout (Days) for Inactive Jobs setting is less than this number, BITS uses the policy setting. For example, if you enter 45 days for this setting, but the policy is set to 30 days, BITS uses 30 days. If the Timeout (Days) for Inactive Jobs setting is undefined (the default state), the policy setting defaults to 90 days. In this case, for example, if you enter 91 days in this setting, BITS uses the policy setting (90 days).

If BITS times out because no progress is being made, control of the transfer is returned to Application Launcher, which then transfers the application itself.

Priority: Use this option to specify the priority assigned to the BITS transfer. You can choose from one foreground priority and three background priorities (high, normal, low).

The foreground priority causes BITS to transfer the application in the foreground. Foreground transfers are the highest priority. Foreground transfers compete for network bandwidth with other applications, which can impede the user's network experience. Unless the timing of the transfer is critical or the user is actively waiting, you should use a background priority.

For the three background priorities, the priority level determines when the transfer is processed relative to other transfers in the queue. Higher priority transfers preempt lower priority transfers. Transfers with the same priority level share transfer time, which prevents a large transfer from blocking the transfer queue. Lower priority transfers do not receive transfer time until all higher priority transfers are completed or in an error state.

All foreground jobs run concurrently with one background job. If there are multiple background jobs with the same priority level (high, for example), BITS splits the background transfer time among the jobs.

- 4 When finished, click OK to save your changes.

34.6 Changing the BITS Maximum Network Bandwidth Setting

Windows XP includes a Group Policy setting for the maximum amount of the workstation's idle network bandwidth that BITS uses. By default, this setting is not configured, which enables BITS to use all of the workstation's available idle bandwidth.

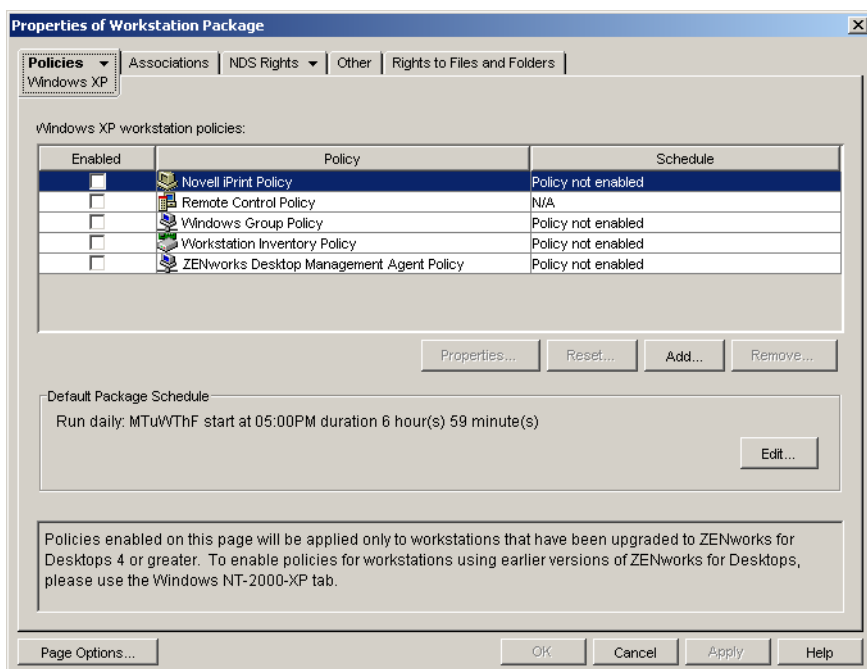
IMPORTANT: The BITS maximum network bandwidth setting is available as a Group Policy on Windows XP only. Windows 2000 does not include a Group Policy setting for BITS maximum bandwidth.

If you have BITS running on a large number of workstations, this might impact your network. To reduce this impact, during periods of high utilization you can limit the amount of bandwidth available to BITS.

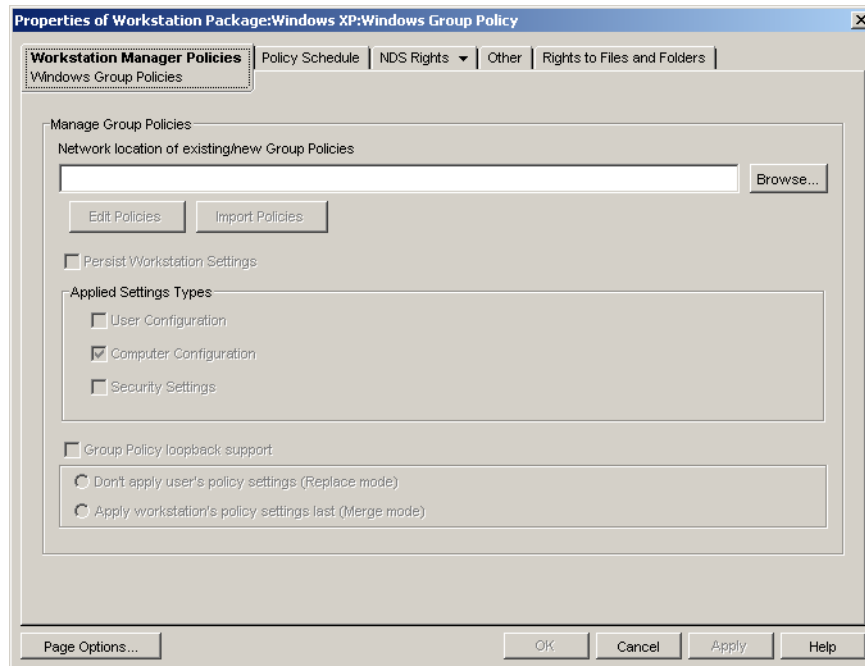
The following steps provide instructions for using a Windows Group Policy to configure the BITS maximum bandwidth setting. The instructions assume that you are familiar with how to use ZENworks policies. If you need additional instructions, see [Chapter 15, “Setting Up User and Workstation Package Policies,”](#) on page 169.

- 1 In ConsoleOne on a Windows XP workstation, right-click the *Workstation Package*, click *Properties*, click the *Policies* tab > *Windows XP*.

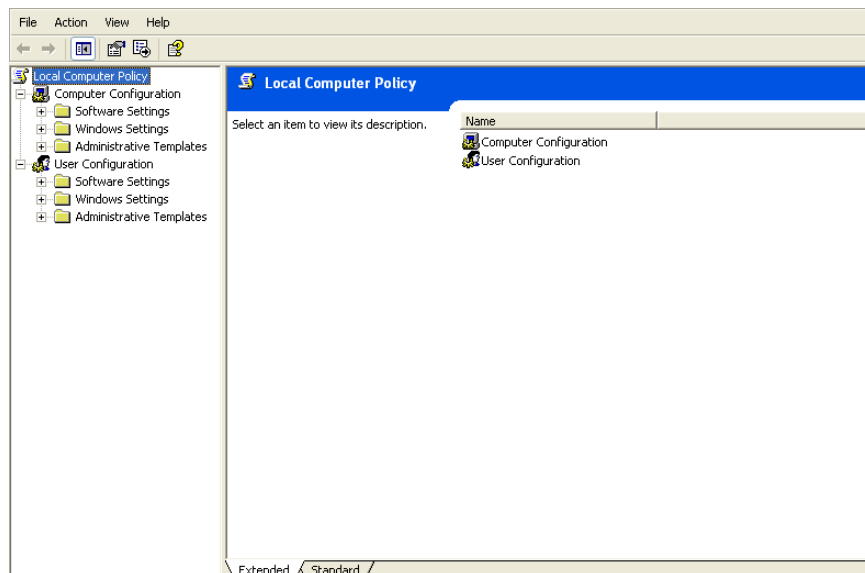
If you do not have a Workstation Package already created, see [Chapter 11, “Creating Policy Packages,”](#) on page 143



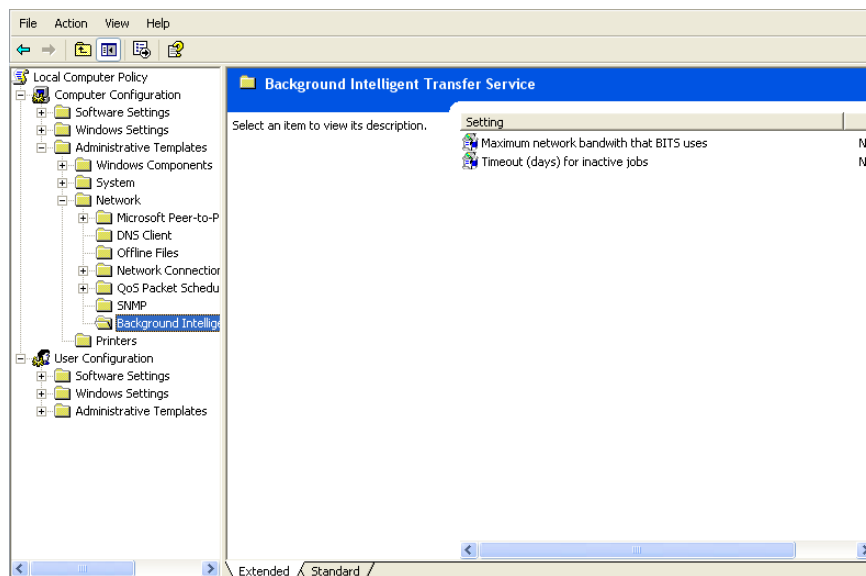
- 2 Enable the *Windows Group Policy*, then click *Properties* to display the Windows Group Policy page.



- 3 Enter a location where you want the new Group Policy file created, or select an existing Group Policy file.
- 4 Click *Edit Policies* to launch the Windows Group Policy Editor.



- 5 Expand the console tree to display the BITS setting (Local Computer Policy > Computer Configuration > Administrative Templates > Network > Background Intelligent Transfer Service).



- 6 Double-click the *Maximum network bandwidth that BITS uses* setting, then configure the settings as desired. Refer to the Help for details about the setting.
Notice that you can also configure the *Timeout (days) for inactive jobs* setting. This setting corresponds to the *No Progress Timeout* setting (configured on the Application object's *BITS Settings* page). It is used if you select the *Use System Setting* option for the *No Progress Timeout* setting (see [Section 34.5, "Changing the Default Settings for a BITS Job,"](#) on [page 361](#)).
- 7 When finished, save your changes and exit the Group Policy Editor.
- 8 Make any additional changes, schedule the policy, and make associations as necessary. For information, see [Chapter 15, "Setting Up User and Workstation Package Policies,"](#) on [page 169](#).

Advanced Distribution: Pre-Installing Applications

35

Novell® ZENworks™ Desktop Management lets you distribute portions of an application to a workstation before the user launches the application the first time. Because you can schedule the distribution, you can perform an off-line, or lights-out, distribution of the application and save the user some of the wait typically associated with a distribution. For example, you could pre-install the application after work hours so the application is ready to use the next day.

With a pre-install, all workstation-related distribution processes (file copying, modifying text files, .ini files, and workstation registry settings) are performed prior to launching of the application. When the user launches the application, the user-specific distribution processes (modifying user registry keys and so forth) are completed.

The following sections provide information for pre-installing applications:

- [Section 35.1, “User-Associated Applications vs. Workstation-Associated Applications,” on page 367](#)
- [Section 35.2, “Pre-Installing an Application Immediately,” on page 367](#)
- [Section 35.3, “Scheduling an Application Pre-Install,” on page 370](#)

35.1 User-Associated Applications vs. Workstation-Associated Applications

You can pre-install an application that is associated with either users or workstations:

- For user-associated applications, the user must be logged in and Application Launcher must be running. Application Launcher uses the logged-in user's credentials (authentication and file system access) to distribute the application.
- For workstation-associated applications, the workstation must be running but Application Launcher does not need to be running.

If the application is a non-MSI application (for example, an AOT application), NAL Workstation Helper uses the workstation's credentials to distribute the application.

If the application is an MSI application, NAL Workstation Helper uses the logged-in user's credentials. If you want it to use the workstation's credentials rather than require a user to be logged in (for example, to perform a lights-out distribution of the MSI application), you must enable the *Distribute in workstation security space if workstation associated* option (*Distribution Options* tab > *Options* page).

35.2 Pre-Installing an Application Immediately

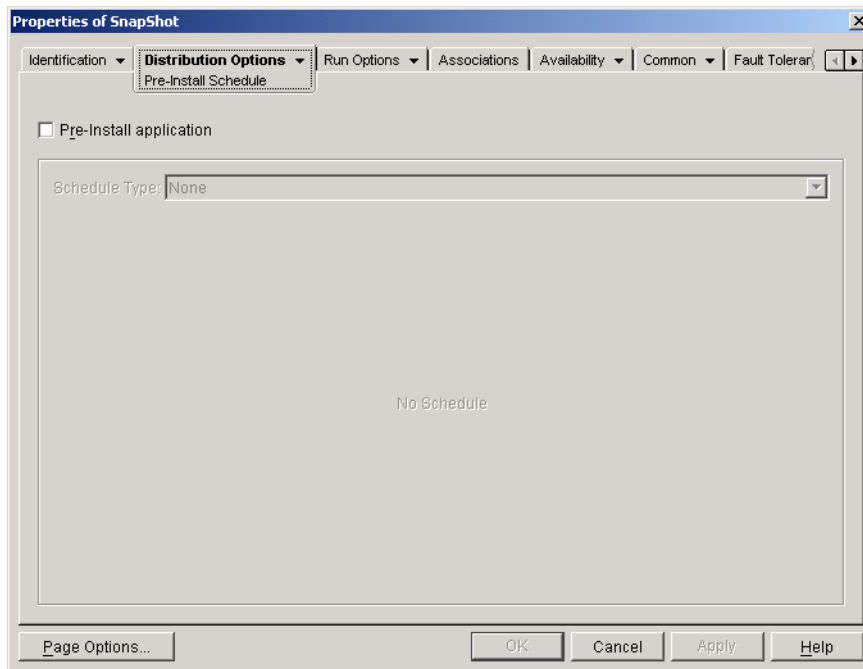
Rather than schedule a pre-install, you can have the pre-install occur as soon as possible.

For users and workstations that are already associated with the application but have not installed it yet, the pre-install occurs the next time Application Launcher refreshes (user-associated application) or NAL Workstation Helper refreshes (workstation-associated application).

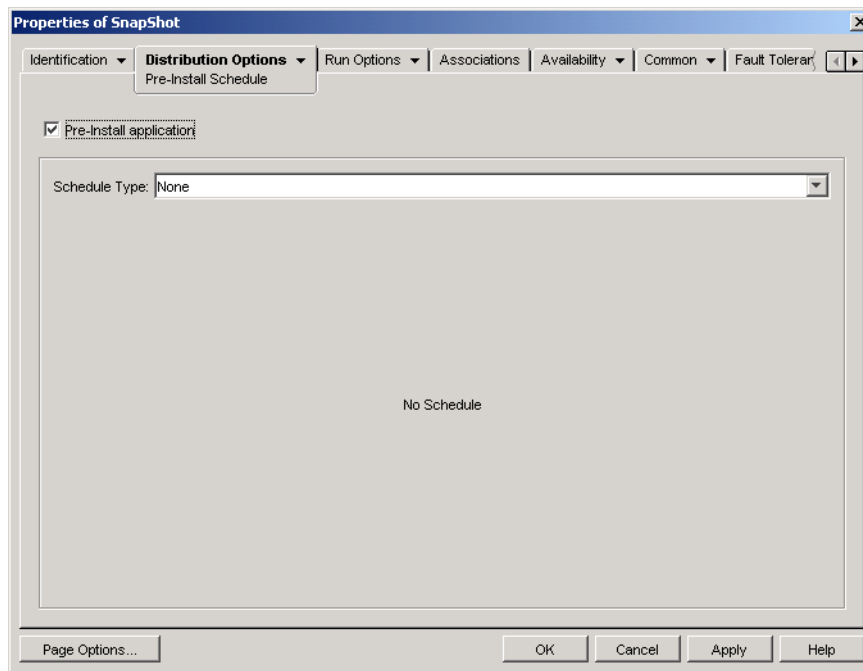
For users and workstations that you associate with the application after enabling pre-install, the pre-install occurs as soon as the association takes place and Application Launcher starts or refreshes (user-associated application) or NAL Workstation Helper starts or refreshes (workstation-associated application).

To enable an application to be pre-installed as soon as possible:

- 1 In ConsoleOne™, right-click the Application object that you want to pre-install, then click *Properties* to display the Application object's property pages.
- 2 Click the *Distribution Options* tab > *Pre-Install Schedule* to display the Pre-Install Schedule page.



- 3 Select the *Pre-install application* check box to enable the option.



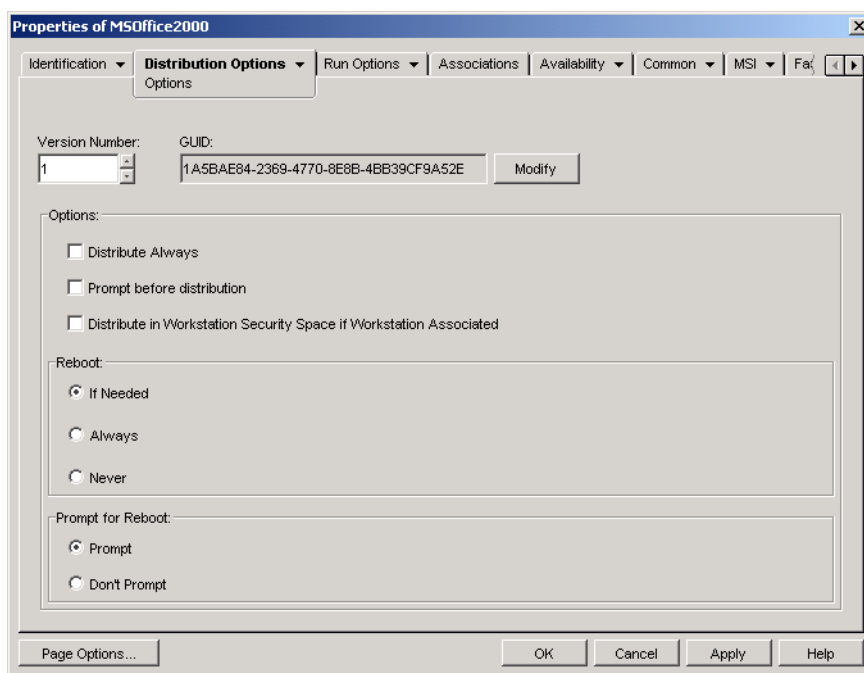
- 4 Leave the *Schedule type* set to *None*.
- 5 (Conditional) If you are pre-installing a workstation-associated MSI application and you want to use the workstation's credentials used rather than the logged-in users, you must enable the *Distribute in workstation security space if workstation associated* option.

By default, workstation-associated MSI applications are distributed in the user security space, meaning that Application Launcher uses the user's credentials and file system access. If you want to perform a lights-out distribution without requiring the user to remain logged in at the workstation, you can have Application Launcher turn over distribution to the NAL Workstation Helper, which runs in the system space and uses the workstation's credentials.

Not all MSI applications can be installed using the workstation's credentials. Some MSI applications have dependencies on a logged-in user (for example, to read and write to the HKCU hive in the Windows registry). In this situation, you must deselect this option in order to have the distribution occur in the user security space and not the workstation security space.

To use enable pre-install using the workstation's credentials:

5a Click the *Distribution Options* tab > *Options* to display the Distribution Options page.



5b Select the *Distribute in workstation security space if workstation associated* check box to enable the option.

It is important to remember that NAL Workstation Helper uses the workstation's credentials, not the user's credentials, to distribute the application. This means that you must assign the workstation the appropriate file system rights to access the network location where the source .msi files reside.

5c (Conditional) If an application requires a reboot during installation, you must select *Reboot if needed* or *Reboot always* in the Reboot group box and *Don't prompt in the prompt* for Reboot group box.

6 When finished, click *OK* to save your changes.

35.3 Scheduling an Application Pre-Install

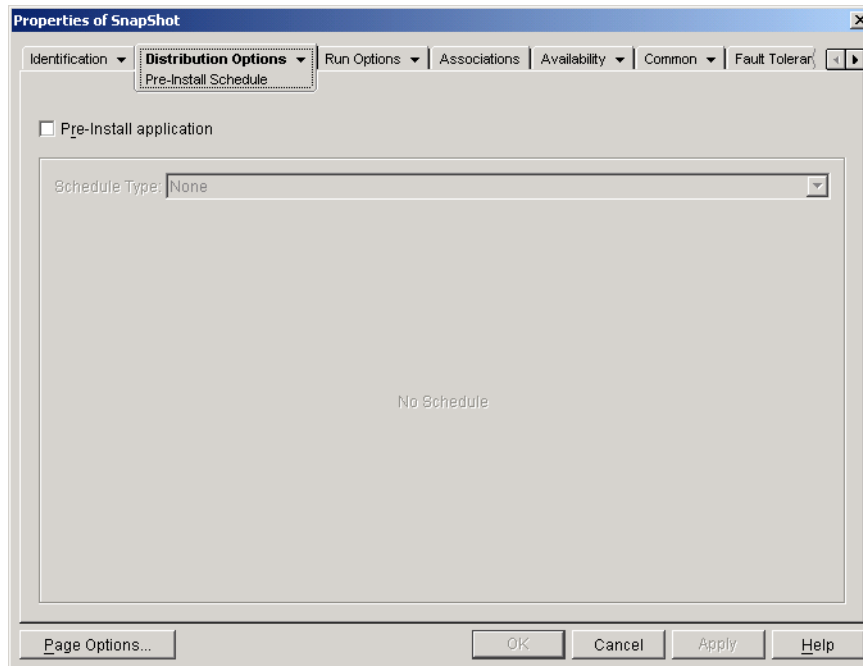
Scheduling a pre-install enables you to perform an off-line, or lights-out, distribution of the application and save the user some of the wait typically associated with a distribution. For example, you could pre-install an application after work hours so the application is ready to use the next day.

For user-associated applications to be pre-installed at the schedule time, Application Launcher must be running on the user's workstation

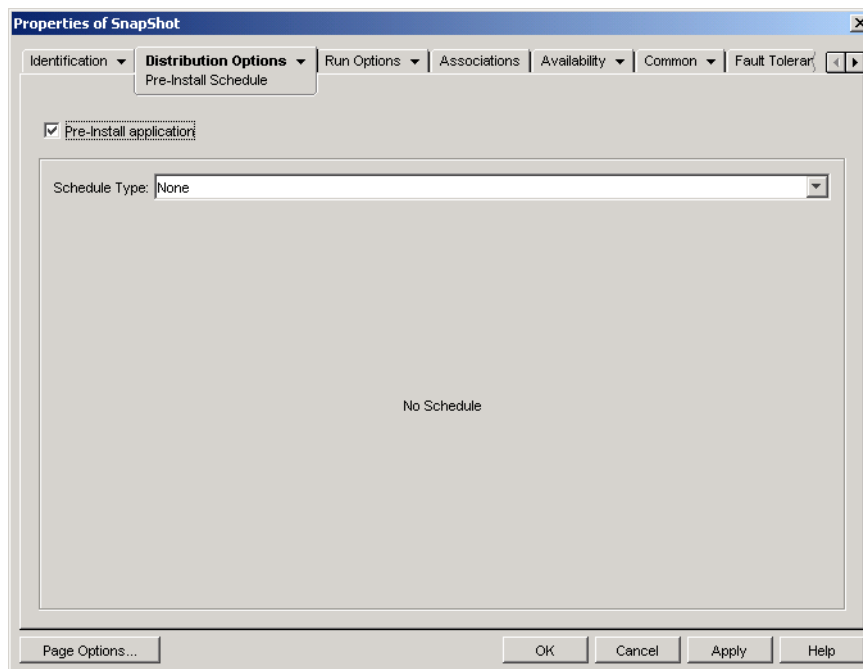
For workstation-associated applications to be pre-installed at the scheduled time, Application Launcher does not need to be running. Pre-install tasks are handled by the NAL Workstation Helper, running under the Workstation Manager.

1 In ConsoleOne, right-click the Application object that you want to pre-install, then click *Properties* to display the Application object's property pages.

- 2 Click the *Distribution Options* tab > *Pre-Install Schedule* to display the Pre-Install Schedule page.



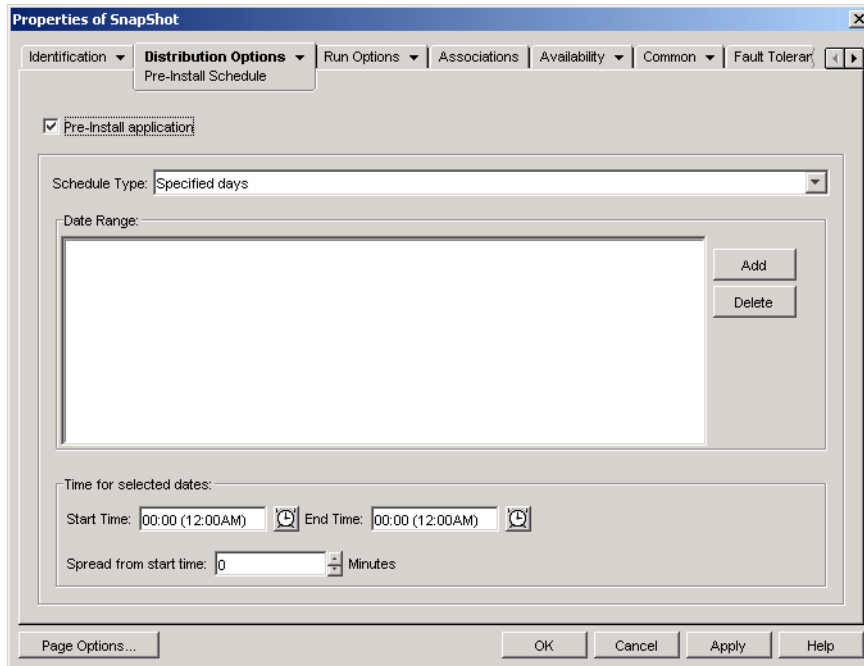
- 3 Select the *Pre-install application* check box to enable the option.



There are two schedule types for you to choose from: *Specified days* and *Range of days*.

- **Specified days:** Use this schedule type to designate specific days and times when the application can be pre-installed. You can specify up to 350 different days and times.

- **Range of days:** Use this schedule type to designate a range of days each week that the application can be pre-installed.
- 4 (Conditional) To use the specified days schedule, complete [Step 4a](#) through [Step 4c](#). Otherwise, to use the range of days schedule, skip to [Step 5](#).
- 4a In the *Schedule type* list, select *Specified days* to display the Specified Days options.



4b Fill in the following fields:

- **Date range:** The Date Range list displays all dates when the application can be pre-installed. To add a date, click Add, select the date you want, then click OK to display it in the list.
- **Time for selected dates:** Select the availability start time and end time. The times apply to all dates in the *Date range* list.

NOTE: The time increments in 5 minute intervals, with the earliest available start time being 00:00 (12:00 a.m.) and the latest end time being 23:55 (11:55 p.m.). This means there is always a 5-minute time period from 11:55 p.m. to 12:00 midnight when the application is unavailable. If you want the application to be available the entire day, you need to use the *Range of days* schedule type. For more information, see [Step 5b on page 374](#).

- **Spread from start time (in minutes):** The *Spread from start time* option spreads out user access times over the number of minutes specified so the application doesn't become available to all users at the same time. If you anticipate all users launching the application as soon as it becomes available and the application is being distributed or run from the network, you can use this option to avoid possible network overload.

For example, if you have a moderate number of users to whom the application is to be distributed (say about 100), you might specify a one-hour (60 minute) block of time (starting at the scheduled start time) to randomly distribute the application: thus

all users will gain access to the application some time during the first sixty minutes after the scheduled start time.

If you want to substantially ease the load on your servers caused by the application distribution, or if you have bandwidth concerns, you might want to make the application distribute randomly throughout the time of availability. To spread out access times across the entire time (*Specified days* and *Time for selected dates*) that the application is available, use the total availability time specified for that application in terms of minutes. This will require that you make the maximum time available for each day you specify. For example, if an application is configured for a typical business day in the United States (9 hours per day: 8:00 a.m. to 5:00 p.m.), you calculate the total time of availability for that application like this:

Number of specified hours x 60 minutes per hour = Total availability time per day

Using this equation, the example above would be calculated like this:

9 x 60 (minutes per hour) = 540 minutes of availability per day

In this example, when you enter 540 minutes in the *Spread from start time* field, the application is distributed randomly for the entire 540 minutes that you have made it available on that scheduled day. Note that this might not be suitable for applications that must be distributed in a timely fashion, such as anti-virus updates. Note also that this is an example only: you can schedule the distribution for any specified amount of time for any day of the week.

Remember that the *Time for selected dates* setting makes the last five minutes of a day unscheduleable, so you need to consider these five minutes if the application schedule ends at 11:55 p.m. for that day.

4c Continue with **Step 6**.

5 (Conditional) To use the *Range of days* schedule, complete **Step 5a** through **Step 5c**. Otherwise, to use the *Specified days* schedule, return to **Step 4**.

5a In the *Schedule type* list, select *Range of days* to display the *Range of days* options.

Properties of SnapShot

Identification | **Distribution Options** | Run Options | Associations | Availability | Common | Fault Tolerant

Pre-Install Schedule

☒ Pre-Install application

Schedule Type: Range of days

Date Range

Start Date: 5/21/04 End Date: 5/21/04

Select the day(s) the schedule will activate:

Sun Mon Tue Wed Thu Fri Sat

Time for selected range

Start Time: 00:00 (12:00AM) End Time: 00:00 (12:00AM)

Spread from start time (in Minutes): 0

☐ Use this schedule in GMT for all clients

Page Options... OK Cancel Apply Help

5b Fill in the following fields:

- **Date range:** To define the range of days, select a start date and an end date, then select the days (Sunday through Saturday) within the established date range. By default, all days are selected; a day is selected when the button appears to be pressed in.
- **Time for selected range:** Select the availability start time and end time. This option works differently depending on whether the date range includes one day, multiple days, or all seven days. If the date range includes one to six days (but not all seven days), the application is available between the start and end times on those days. For example, if you make the application available on Monday between 8:00 and 5:00, it is available during those hours. However, if the date range includes all seven days, the times are ignored and the application is available every day, 24 hours a day.
- **Spread from start time (in minutes):** The *Spread from start time* option spreads out user access times over the number of minutes specified so the application doesn't become available to all users at the same time. If you anticipate all users launching the application as soon as it becomes available and the application is being distributed or run from the network, you can use this option to avoid possible network overload.

For example, if you have a moderate number of users to whom the application is to be distributed (say about 100), you might specify a one-hour (60 minute) block of time (starting at the scheduled start time) to randomly distribute the application: thus all users will gain access to the application some time during the first sixty minutes after the scheduled start time.

If you want to ease the load of the application distribution on your servers or if you have bandwidth concerns, you might want to make the application distribute randomly throughout the time of availability. To spread out access times across the entire time (*Date range* and *Time for selected dates*) that the application is available, use the total availability time specified for that application in terms of minutes. For example, if a workstation-associated application is configured for an entire 24-hour, three-shift day, you can calculate the total time of availability for that application like this:

Number of days in date range x *Time of availability per day* = Total availability time

Using this equation, and making sure to convert hours to minutes, the example above would be calculated like this:

7 (days) x 24 (hours) = 168 hours of availability

168 x 60 (minutes per hour) = 10,080 minutes of availability

When you enter 10800 minutes in the *Spread from start time* field, the application is distributed randomly for the entire 10800 minutes that you have made it available. Note that this is not suitable for applications that must be distributed in a timely fashion, such as anti-virus updates.

- **Use this schedule in GMT for all clients:** The schedule is based on the workstation's time zone. If your network spans different time zones and you schedule an application to run at 1:00 p.m., it runs at 1:00 p.m. in each time zone. You can select this option to have workstations run applications at the same time regardless of their time zones (for example, 1:00 p.m. Rome time and 4:00 a.m. Los Angeles time).

5c Continue with **Step 6**.

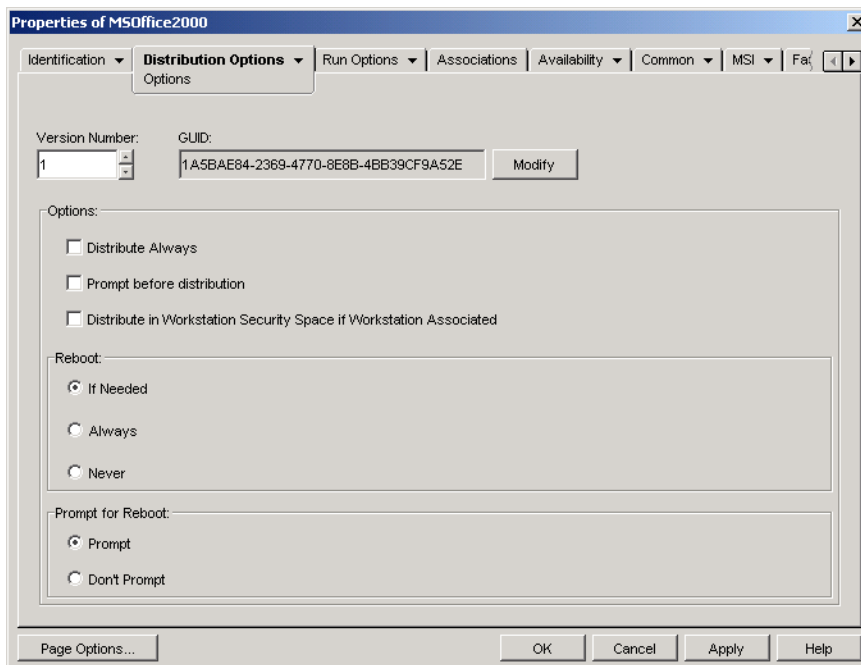
- 6** (Conditional) If you are pre-installing a workstation-associated MSI application and you want to use the workstation's credentials used rather than the logged-in users, you must enable the *Distribute in workstation security space if workstation associated* option.

By default, workstation-associated MSI applications are distributed in the user security space, meaning that Application Launcher uses the user's credentials and file system access. If you want to perform a lights-out distribution without requiring the user to remain logged in at the workstation, you can have Application Launcher turn over distribution to the NAL Workstation Helper, which runs in the system space and uses the workstation's credentials.

Not all MSI applications can be installed using the workstation's credentials. Some MSI applications have dependencies on a logged-in user (for example, to read and write to the HKCU hive in the Windows registry). In this situation, you must deselect this option in order to have the distribution occur in the user security space and not the workstation security space.

To enable pre-install using the workstation's credentials:

- 6a** Click the *Distribution Options* tab > *Options* to display the Options page.



- 6b** Select the *Distribute in workstation security space if workstation associated* check box to enable the option.

It is important to remember that NAL Workstation Helper uses the workstation's credentials, not the user's credentials, to distribute the application. This means that you must assign the workstation the appropriate file system rights to access the network location where the source .msi files reside.

If an application requires a reboot during installation, you must select *Reboot if needed* or *Reboot always* in the *Reboot* group box and *Don't Prompt* in the *Prompt for reboot* group box.

- 7** Click *OK* to save your changes.

Advanced Distribution: Configuring Fault Tolerance, Load Balancing, and Site Lists

36

Novell® ZENworks® Desktop Management provides a variety of methods to help you ensure that critical applications are always available for distribution to users. These methods are discussed in the following sections:

- [Section 36.1, “Setting Up Fault Tolerance,” on page 377](#)
- [Section 36.2, “Setting Up Load Balancing,” on page 381](#)
- [Section 36.3, “Setting Up Site Lists,” on page 385](#)

36.1 Setting Up Fault Tolerance

Network problems can make installation packages unavailable. To ensure that an application can be distributed even when its installation package is unavailable, you can establish backup installation packages. How you do so depends on the type of application, as explained in the following sections:

- [Section 36.1.1, “Setting Up Fault Tolerance for MSI Applications,” on page 377](#)
- [Section 36.1.2, “Setting Up Fault Tolerance for Simple or AOT/AXT Applications,” on page 378](#)

ZENworks Desktop Management does not provide fault tolerance for Web applications or terminal server applications.

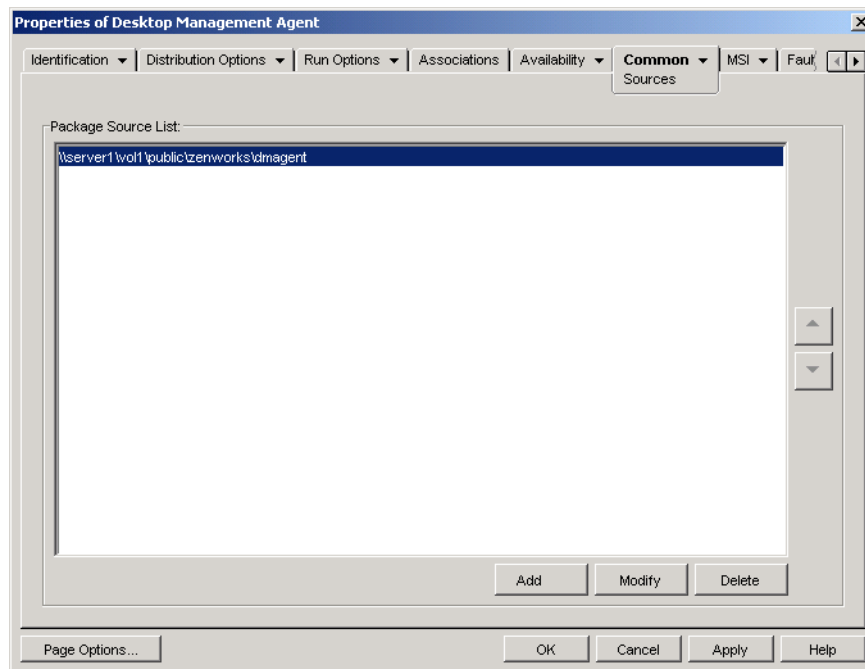
36.1.1 Setting Up Fault Tolerance for MSI Applications

You establish fault tolerance, or source resiliency, for an MSI application by having multiple installation packages available at different server locations. During distribution, if the first source fails, Application Launcher attempts to distribute from an alternate source.

To set up fault tolerance for an MSI application:

- 1 Create the additional MSI installation packages in the server locations you want.
- 2 In ConsoleOne®, right-click the MSI Application object for which you want to establish fault tolerance, then click *Properties* to display the Application object's property pages.

- 3 Click the *Common* tab > *Sources* to display the Sources page.



By default, the Sources page displays the source location that was specified when the MSI Application object was created.

- 4 Click *Add*, specify the source path for an MSI installation package, then click *OK* to add the additional source to the list.
- 5 Repeat **Step 4** until you've added all available sources.
- 6 Use the arrow buttons to list the sources in the order you want them used.
The first source listed is used first, the second is used next, and so forth until either the distribution is successful or all sources have been used.
- 7 Click *OK* to save your changes.

36.1.2 Setting Up Fault Tolerance for Simple or AOT/AXT Applications

You establish fault tolerance for a simple application or an AOT/AXT application by having multiple installation packages at different source locations. During distribution, if the application's first source fails, Application Launcher attempts to distribute from an alternate source.

When setting up fault tolerance for an application, you can link directly to additional installation packages or you can link to additional Application objects that have been created using the installation packages. For example, you want to set up fault tolerance for App1, whose installation package is located at \\server1\vol1\public\zenworks\app1. You create three additional source locations:

```
\\server2\vol1\public\zenworks\app1  
\\server3\vol1\public\zenworks\app1  
\\server4\vol1\public\zenworks\app1
```

You can define each of the additional installation packages as sources for App1, or you can create three new Application objects using each of the installation packages and then have App1 link to the three new Application objects.

Defining each of the additional installation packages as sources for App1 has the advantage of requiring configuration of only one Application object. Regardless of which installation package is used, the App1 object's distribution settings are applied.

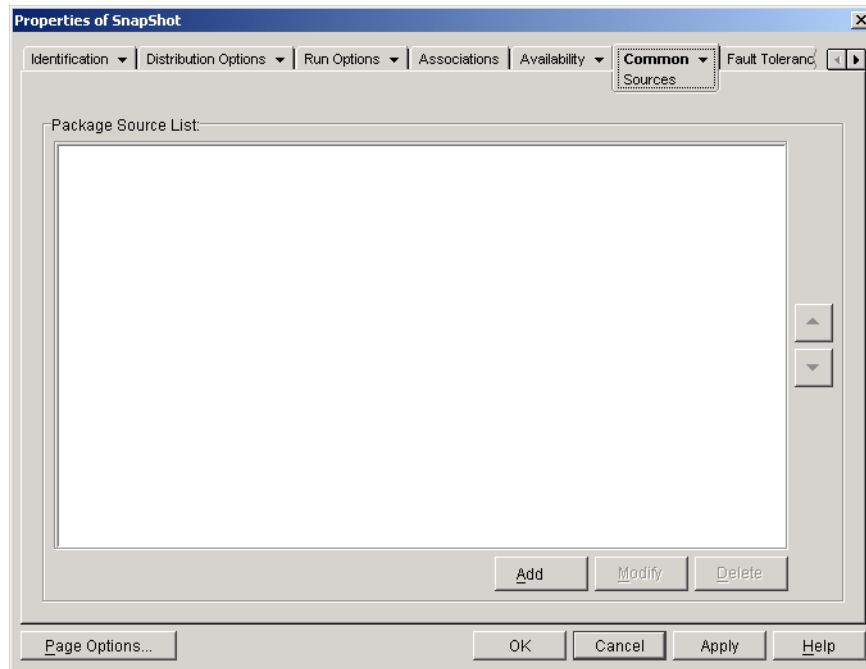
Defining additional Application objects using the installation packages enables you to have different Application object configuration settings for each installation package. If you choose to use additional Application objects rather than additional sources, please be aware of the following limitations:

- Only one-level-deep fault tolerance is supported. If Application Launcher fails over to a backup Application object and the backup Application object fails, the distribution fails even if fault tolerance has been enabled for the backup Application object.
- *Remote mode* and *Force cache* distributions do not support fault tolerance through Application objects. Both of these distributions require Application Launcher to copy installation package files to the workstation cache and then install from the cache, which requires the use of additional sources rather than additional Application objects.

To set up fault tolerance for a simple application or an AOT/AXT application:

- 1** Copy the additional installation packages to the server locations you want.
- 2** (Conditional) If you plan to create Application objects for each of the additional installation packages so that you can link to the Application objects, create the Application objects. If necessary, refer to [Section 28.2, “Configuring the Application in eDirectory,” on page 316](#).
- 3** In ConsoleOne, right-click the Application object for which you want to establish fault tolerance, then click *Properties* to display the Application object's property pages.
- 4** (Conditional) If you are using installation packages only (no Application objects for them), define the installation packages as additional sources for the application. To do so:

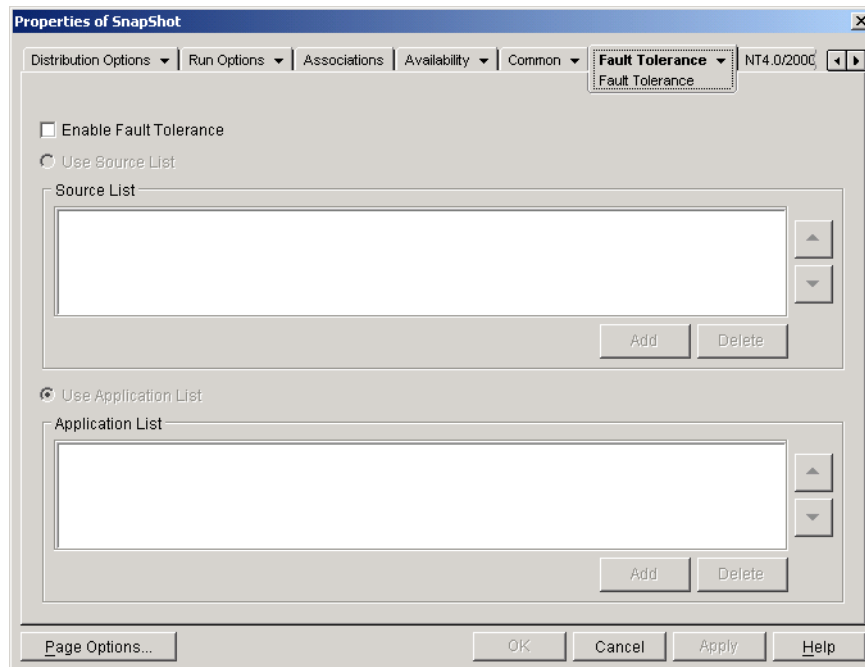
4a Click the *Common* tab > *Sources* to display the Sources page.



4b Click *Add*, specify the source path for an installation package, then click *OK* to add the additional source to the list.

4c Repeat **Step 4b** until you've added all available sources.

5 Click the *Fault Tolerance* tab > *Fault Tolerance* to display the Fault Tolerance page.



6 Fill in the following fields:

Enable fault tolerance: Select this option to enable fault tolerance. The other fault tolerance options are available only if this option is enabled.

Use source list: Select this option to have Application Launcher use a list of sources as the backup. You must have already created at least one installation package source (see [Step 4](#)).

To add a source to the Source List, click *Add*, browse to and select the source, then click *OK*.

To remove a source, select the source from the Source List, then click *Delete*.

If distribution of the application fails, Application Launcher tries the alternate sources in the order they are listed, from top to bottom. To change the order of the sources, select a source from the Source List, then click the up-arrow to move the source up in the list or click the down-arrow to move it down in the list.

Use application list: Select this option to have Application Launcher use Application objects as the backup installation packages. You must have already created additional Application objects for the application, with the installation package being stored on a different server or volume than this application (see [Step 2](#)).

To add an Application object to the Application List, click *Add*, browse to and select the Application object, then click *OK*.

To remove an Application object from the list, select the Application object, then click *Delete*.

If distribution of the application fails, Application Launcher tries the Application objects in the order they are listed, from top to bottom. To change the order of the list, select an Application object from the Application List, then click the up-arrow to move the Application object up in the list or click the down-arrow to move it down in the list.

7 Click *OK* to save your changes.

36.2 Setting Up Load Balancing

Distributing an application to many users at the same time can cause delays with the distribution. To reduce the possibility of delays, you can spread the workload across multiple servers by establishing additional installation packages on each of those servers. How you set up load balancing depends on whether the application is an MSI application or a simple/AOT/AXT application, as explained in the following sections:

- [Section 36.2.1, “Setting Up Load Balancing for MSI Applications,” on page 381](#)
- [Section 36.2.2, “Setting Up Load Balancing for Simple or AOT/AXT Applications,” on page 383](#)

ZENworks Desktop Management does not provide load balancing for Web applications or terminal server applications.

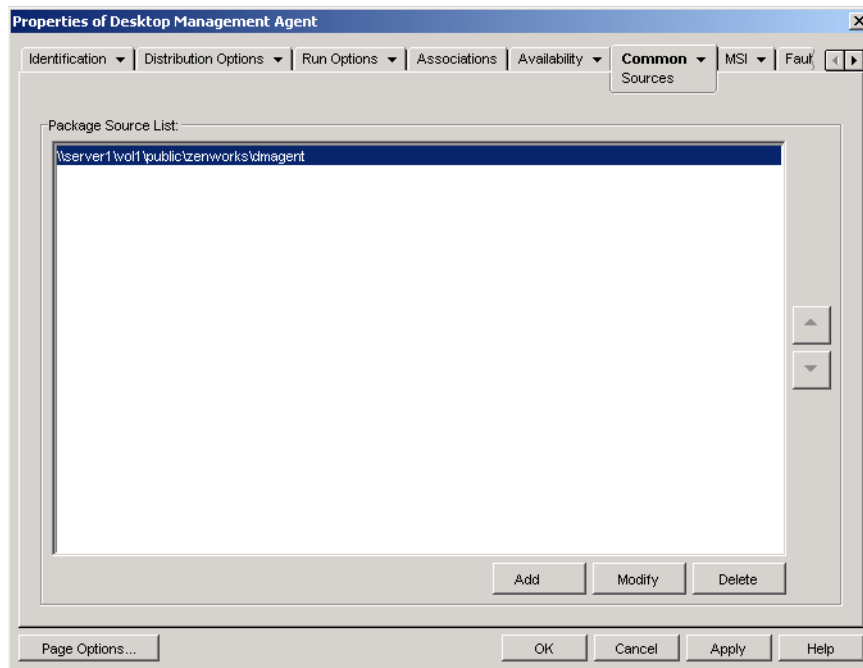
36.2.1 Setting Up Load Balancing for MSI Applications

You establish load balancing for an MSI application by having multiple installation packages available at different server locations. During distribution, if the first source is busy, Application Launcher attempts to distribute from an alternate source.

To set up load balancing for an MSI application:

- 1 Create the additional MSI installation packages in the server locations you want.

- 2 In ConsoleOne, right-click the MSI Application object for which you want to establish load balancing, then click *Properties* to display the Application object's property pages.
- 3 Click the *Common* tab > *Sources* to display the Sources page.



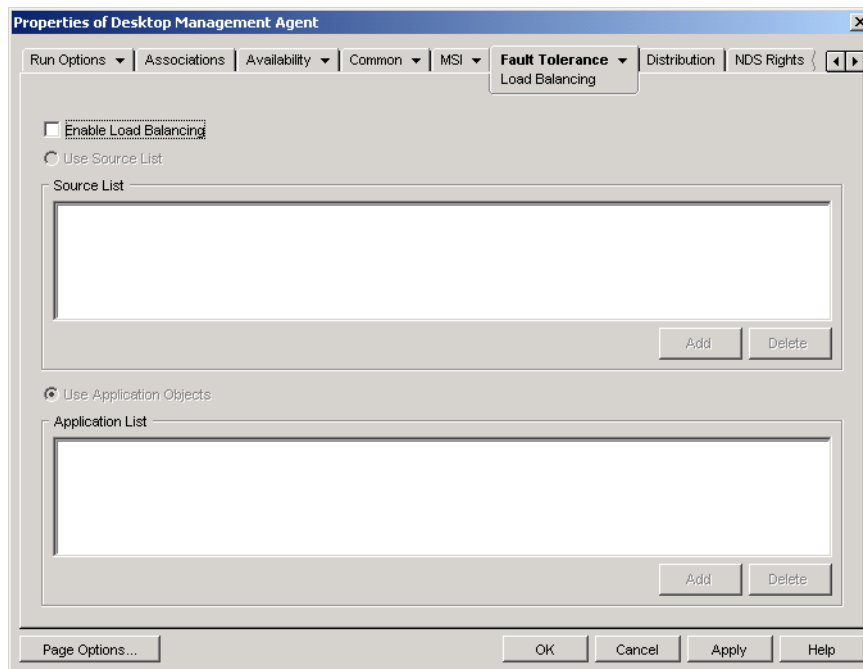
By default, the Sources page displays the source location that was specified when the MSI Application object was created.

- 4 Click *Add*, specify the source path for an MSI installation package, then click *OK* to add the additional source to the list.
- 5 Repeat **Step 4** until you've added all available sources.

For load balancing, the order in which the sources are listed does not matter. Application Launcher randomly selects the source location.

If you are also using this list for fault tolerance, the list determines the order in which sources are used. For more information, see [Section 36.1.1, “Setting Up Fault Tolerance for MSI Applications,”](#) on page 377.

6 Click the *Fault Tolerance* tab > *Load Balancing* to display the Load Balancing page.



7 Select the *Enable load balancing* check box to turn on the option.

8 Click *OK* to save your changes.

36.2.2 Setting Up Load Balancing for Simple or AOT/AXT Applications

You establish load balancing for a simple application or an AOT/AXT application by having multiple installation packages at different source locations. During distribution, if the application's first source is busy, Application Launcher attempts to distribute from an alternate source.

When setting up load balancing for an application, you can link directly to additional installation packages or you can link to additional Application objects that have been created using the installation packages. For example, you want to set up load balancing for App1, whose installation package is located at `\\server1\vol1\public\zenworks\app1`. You create three additional source locations:

```
\\server2\vol1\public\zenworks\app1
\\server3\vol1\public\zenworks\app1
\\server4\vol1\public\zenworks\app1
```

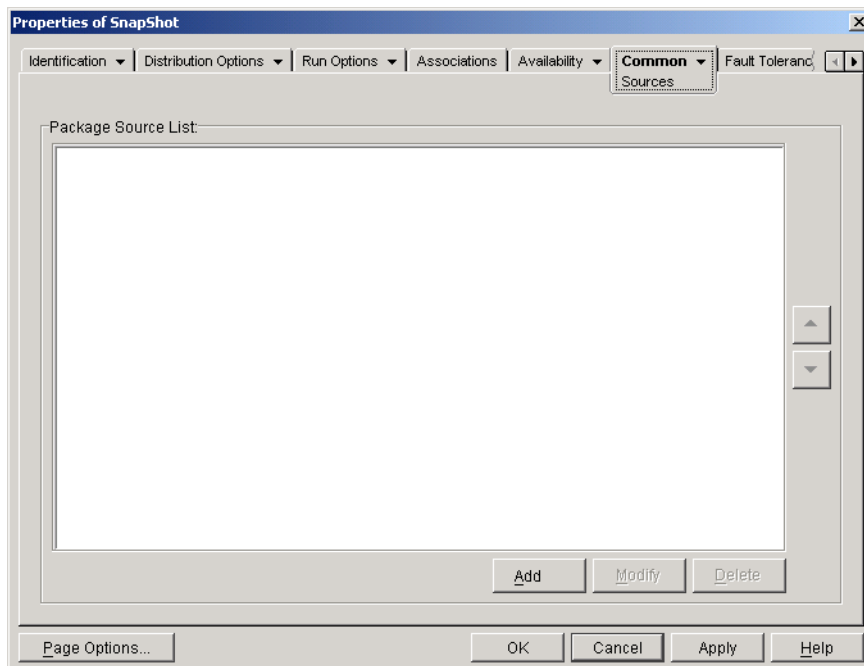
You can define each of the additional installation packages as sources for App1, or you can create three new Application objects using each of the installation packages and then have App1 link to the three new Application objects.

Defining each of the additional installation packages as sources for App1 has the advantage of requiring configuration of only one Application object. Regardless of which installation package is used, the App1 object's distribution settings are applied.

Defining additional Application objects using the installation packages enables you to have different Application object configuration settings for each installation package.

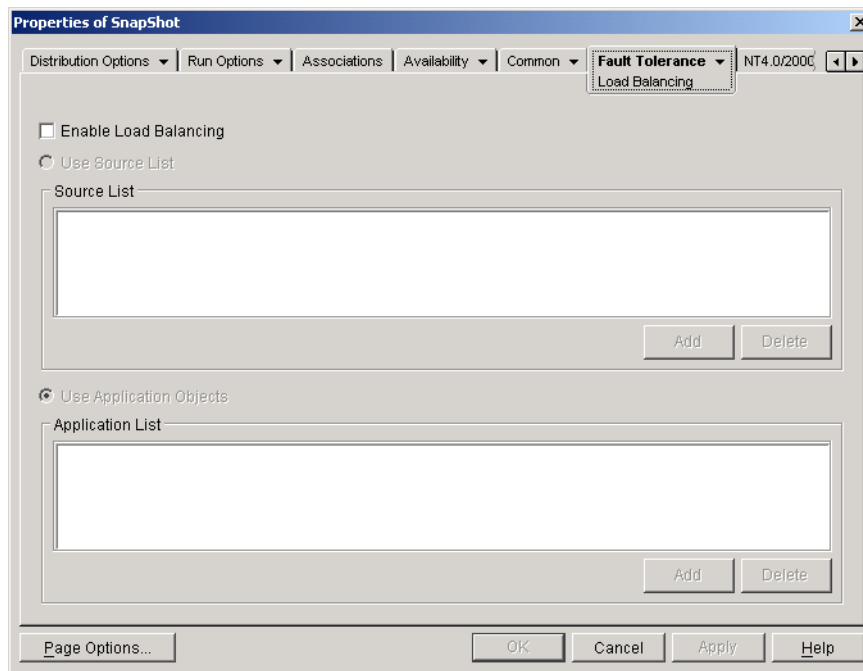
To set up load balancing for a simple application or an AOT/AXT application:

- 1** Copy the additional installation packages to the server locations you want.
- 2** (Conditional) If you plan to create Application objects for each of the additional installation packages so that you can link to the Application objects, create the Application objects. If necessary, refer to [Section 28.2, “Configuring the Application in eDirectory,” on page 316](#).
- 3** In ConsoleOne, right-click the Application object for which you want to establish load balancing, then click *Properties* to display the Application object's property pages.
- 4** (Conditional) If you are using installation packages only (no Application objects for them), define the installation packages as additional sources for the application. To do so:
 - 4a** Click the *Common* tab > *Sources* to display the Sources page.



- 4b** Click *Add*, specify the source path for an installation package, then click *OK* to add the additional source to the list.
- 4c** Repeat [Step 4b](#) until you've added all available sources.

5 Click the *Fault Tolerance* tab > *Load Balancing* to display the Load Balancing page.



6 Fill in the following fields:

Enable load balancing: Select this option to enable load balancing. The other load balancing options are available only if this option is enabled.

Use source list: Select this option to have Application Launcher use a list of sources for load balancing. You must have already created at least one installation package source (see [Step 4](#)). To add a source to the Source List, click *Add*, browse to and select the source, then click *OK*.

To remove a source, select the source from the Source List, click *Delete*.

Use application list: Select this option to have Application Launcher use Application objects for load balancing. You must have already created additional Application objects for the application, with the installation package being stored on a different server or volume than this application (see [Step 2](#)).

To add an Application object to the Application List, click *Add*, browse to and select the Application object, then click *OK*.

To remove an Application object from the list, select the Application object, then click *Delete*.

7 Click *OK* to save your changes.

36.3 Setting Up Site Lists

Site lists let you link an application at one site (Site1) to an application at another site (Site2). By linking applications whose source installation packages are located on servers at different sites, you can distribute the application from the server that is closest to the user.

For example, you have two different sites, Site1 and Site2. Employees at both sites use the same spreadsheet program. Site1 has an Application object (App1) that distributes the spreadsheet program from a Site1 server, and Site2 has its own Application object (App2) to distribute the program from a Site2 server. If you link App1 to App2, any Site1 employee who travels to Site2 and

launches App1 has App2 installed from the Site2 server. Likewise, any Site2 employee who travels to Site1 and launches App2 has App1 installed from the Site1 server.

The site list is a distribution mechanism that applies only to undistributed, non-cached applications. If an application is already distributed or cached on a user's workstation, that application is used regardless of the site list.

Novell Client vs. ZENworks Middle Tier Server

When a user logs in to Novell eDirectory™ through the ZENworks Middle Tier Server rather than the Novell Client™, site lists work slightly differently. Rather than the Novell Client being used to determine the user's location, the Middle Tier Server determines the location. This means that the application closest to the Middle Tier Server is used, which is not necessarily the application closest to the user. In the above example, the Site1 user would continue to have applications distributed from the Site1 server rather than from a Site2 server.

How to Build a Site List

You can link to only one other Application object. However, when you do so, the first Application object is automatically linked to any other Application objects that the second Application object is linked to. For example, you have three identical Application objects (App1, App2, and App3) at three different sites. You link App1 to App2, which creates the following site lists for each of the Application objects:

App1 List	App2 List	App3 List
App2	App1	(none)

Because you can link an Application object to only one other Application object, you now need to link App3 to either App1 or App2. Doing so creates the following site list for each of the Application objects:

App1 List	App2 List	App3 List
App2	App1	App1
App3	App3	App2

Synchronizing Application Object GUIDs

Each Application object has a global unique identifier, referred to as a GUID. When the application is distributed to a workstation, its GUID is added to the Windows registry. This is how Application Launcher knows that the application has been distributed to the workstation.

When using site lists, you need to make sure that all Application objects that belong to the same site list have the same GUID. Otherwise, Application Launcher cannot correctly distribute and uninstall the application. For example:

- Site1 and Site2 have the same application at each site, named App1 and App2. The two applications are part of the same site list, but App1 has GUID 1234 and App2 has GUID 5678. A Site1 user is associated to App1, but has not installed the application. The Site1 user travels to Site2 and attempts to install App1. Because App2 is the closest application, it is installed and GUID 5678 is added to the workstation's registry. The user returns to Site1 and launches App1.

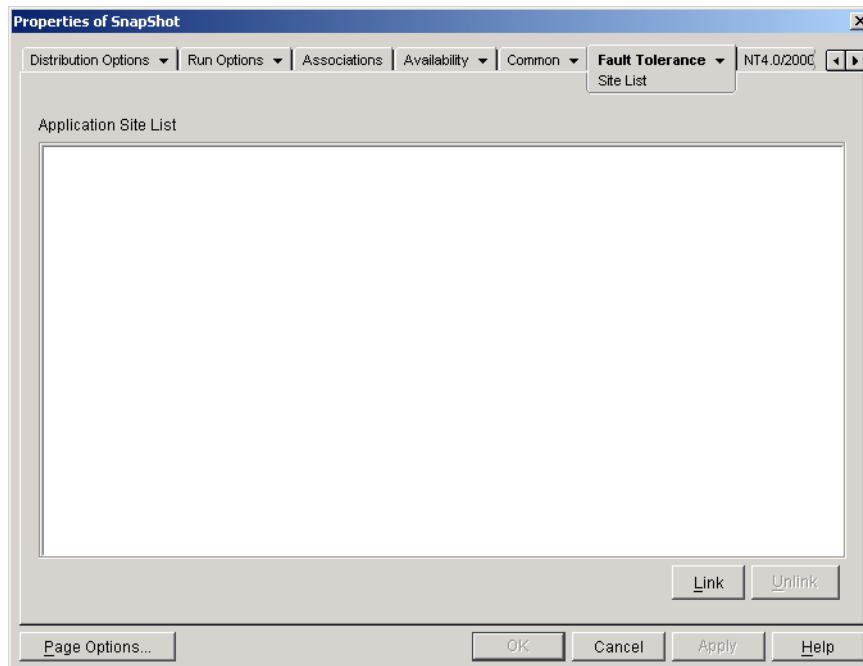
App1's GUID (1234) is not in the registry because App2's GUID is. Therefore, Application Launcher distributes App1 to the workstation even though it is identical to App2.

- The same situation occurs as listed above. However, this time the user tries to uninstall App1 after returning to Site1. Because App1's GUID is not in the registry, Application Launcher cannot uninstall the application.
- Site 1 and Site 2 have the same application chains. You must synchronize the GUIDs of each application in the chain at Site 1 with the GUIDs of each matching application at Site 2. For more information about chained applications, see [Section 37.2, “Application Chains,” on page 390](#).

The issues described above can be resolved by both applications in the site list having the same GUID. For information about synchronizing GUIDs, see [Section 50.4, “Manage Distribution GUIDs,” on page 602](#).

Establishing a Site List for an Application

- 1 In ConsoleOne, make sure that all applications to be included in the site list have the same GUID. For information about synchronizing GUIDs, see [Section 50.4, “Manage Distribution GUIDs,” on page 602](#).
- 2 Right-click the Application object for which you want to establish a site list, then click *Properties* to display the Application object's property pages.
- 3 Click the *Fault Tolerance* tab > *Site List* to display the Site List page.



- 4 Click *Link*, browse for and select the Application object you want to link to, then click *OK* to add it to the Application Site List.
If the Application object you added is also linked to other Application objects, those Application objects are also added to the list
- 5 Repeat the previous step to link to additional Application objects.

6 Click *OK* when you are finished.

Integration with ZENworks Server Management

You can use ZENworks Server Management to distribute an application's source files to other servers and to replicate its Application object to other locations within your eDirectory tree. As part of this distribution process, you can have the site lists automatically generated. For more information, see “**Desktop Application Distribution**” in “**Policy and Distribution Services**” in the *Novell ZENworks 7 Server Management Administration Guide*.

Advanced Distribution: Configuring Application Dependencies and Chains

37

If you have an application that depends on other applications (or files), you can ensure that the other applications are available by adding them as dependencies.

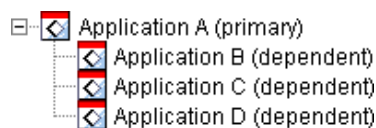
The following sections provide information and instructions to help you successfully create and manage dependencies:

- [Section 37.1, “Primary Applications vs. Dependent Applications,” on page 389](#)
- [Section 37.2, “Application Chains,” on page 390](#)
- [Section 37.3, “What Happens During the Distribution, Launch, and Uninstall of an Application That Has Dependencies,” on page 391](#)
- [Section 37.4, “Adding an Application Dependency,” on page 392](#)
- [Section 37.5, “Removing an Application Dependency,” on page 393](#)
- [Section 37.6, “Deleting an Application That Has Dependencies,” on page 394](#)
- [Section 37.7, “Creating an Application Chain,” on page 394](#)
- [Section 37.8, “Viewing an Application Chain,” on page 395](#)

37.1 Primary Applications vs. Dependent Applications

When working with application dependencies, the primary application is the application for which you are establishing dependencies. The applications that are defined as dependencies are called the dependent applications. The following illustration shows this relationship.

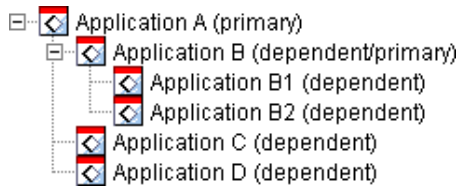
Figure 37-1 Application A as the Primary Application with Applications B, C, and D as Dependent Applications.



A primary application can have one dependent application or, as shown in the above example, it can have multiple dependent applications.

In addition, an application can be both a primary application and a dependent application, as shown in the following illustration.

Figure 37-2 *Application A as the Primary Application with Applications B, B1, B2, C, and D as Dependent Applications.*

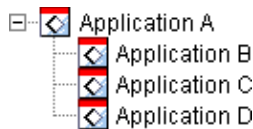


In the above example, Application B is one of Application A's dependent applications. At the same time, Application B has dependencies on two applications, Application B1 and Application B2.

37.2 Application Chains

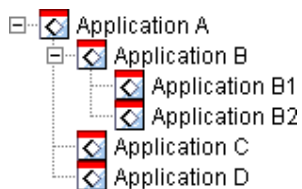
An application chain is two or more applications linked together by dependencies. In its simplest form, an application chain consists of two levels, as shown in the following illustration.

Figure 37-3 *A Two-Level Application Chain*



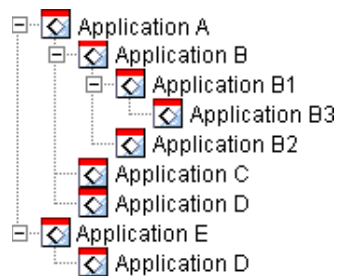
However, when application dependencies are nested, an application chain can grow to include many levels. In the following example, Application A has a dependency on Application B. Application B, in turn, has dependencies on Application B1 and Application B2. As a result, all three applications (B, B1, B2), in addition to applications C and D, must be present in order for Application A to run.

Figure 37-4 *A Three-Level Application Chain*



In some cases, an application might belong to more than one application chain, as in the following example where Application D is a dependent application for both Application A and Application E.

Figure 37-5 *An Application that Belongs to Two Different Application Chains*



37.3 What Happens During the Distribution, Launch, and Uninstall of an Application That Has Dependencies

When setting up application dependencies, you should be aware of the following:

- **Distribution:** When a user launches an application, if its dependent applications have not already been distributed to the user's workstation, Novell Application Launcher™ distributes them. Application Launcher distributes a dependent application only one time, unless the dependent application's version is updated (Application object > *Distribution Options* tab > *Options* page) or the distribution is unsuccessful. If Application Launcher is unable to distribute a dependent application (for example, the user's workstation does not meet the dependent application's system requirements), the primary application is not launched.
- **Distribution through removable media:** If you distribute an application through removable media such as a CD (see [“Distributing Applications Via Removable Media” on page 411](#)) or through an image add-on (see [“Imaging Page” on page 559](#)), its dependent applications must be included on the removable media or as another image add-on. Otherwise, the distribution of the primary application fails.
- **Distribution to disconnected workstations:** For workstations running in disconnected mode, the applications must be force cached to the workstation before it becomes disconnected (or they must be distributed through removable media). If changes are made to dependent applications after the applications have been cached to workstations, the version number of the primary application must be updated in order to force a re-cache of the applications.
- **Launch:** Each time an application is launched, Application Launcher performs any launch operations defined for its dependent applications. For example, if a dependent application has pre-launch and post-launch scripts (Application object > *Run Options* tab > *Launch Scripts* page), Application Launcher runs the pre-launch script, starts the dependent application (based on the executable file or application file listed in the Path to File field on the dependent application's Application page), and then runs the post-launch script.
If a dependent application, such as a setup program, should be run only one time, you should configure the dependent application to run once (Application object > *Run Options* tab > *Application* page).
- **Uninstall:** If you uninstall an application (Application object > *Common* tab > *Uninstall* page or Application object > *Associations* tab > *Associations* page), its dependent applications are uninstalled only if they are not used by another application.

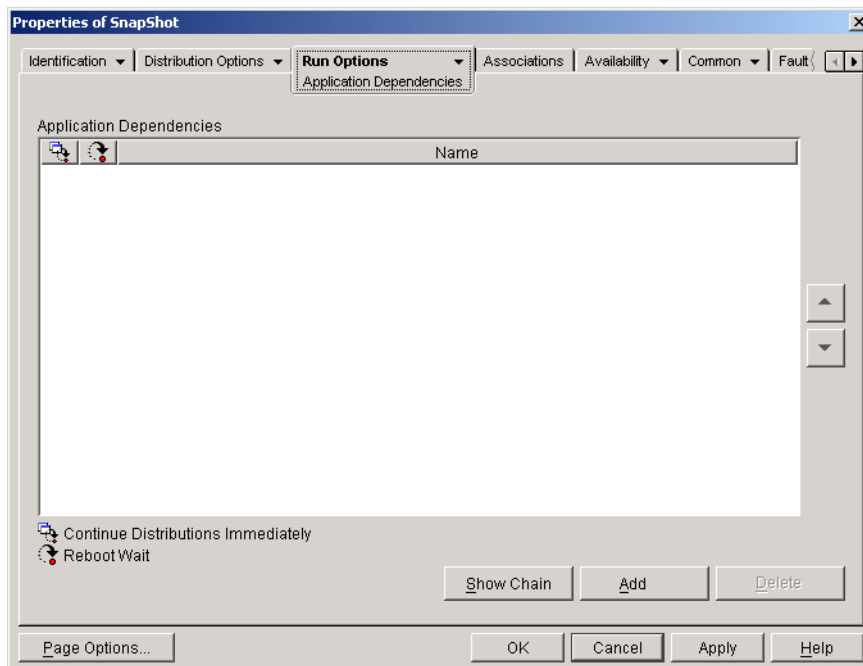
37.4 Adding an Application Dependency

Before adding a dependency to an application, consider the following:

- The dependent application must already exist as an Application object. If it does not, see [Section 28.2, “Configuring the Application in eDirectory,” on page 316](#).
- By default, each user who is associated with the primary application is added as a trustee of the dependent application. This provides the user with the eDirectory™ rights required to the dependent application. You should not associate users directly with the dependent application (dependent Application object > *Associations* tab) unless you want the dependent application to be displayed by Application Launcher.

To add a dependency to an application:

- 1 In ConsoleOne®, right-click the Application object, then click *Properties* to display the Application object's property page.
- 2 Click the *Run Options* tab > *Application Dependencies* to display the Application Dependencies page.



- 3 Add the dependent applications to the list. To do so:
 - 3a Click *Add*, browse for and select the Application object, then click *OK*.
 - 3b If necessary, modify the following distribution attributes for the dependent application:

Continue distributions immediately: By default, Application Launcher waits until it distributes and executes the application before continuing with the action. Select this option if you want Application Launcher to continue with the next action regardless of whether or not the current application's distribution and execution is complete.

For example, if Regedit has a dependency on Notepad, the default action is for Application Launcher to distribute Notepad (if necessary), launch Notepad, and wait for the user to exit Notepad before it launches Regedit. The *Continue distributions*

immediately option, however, would cause Application Launcher to distribute and launch Notepad and then, if the distribution and launch of Notepad was successful, continue immediately with Regedit. In other words, it does not wait for execution of the application to be completed.

Reboot wait: If distribution of the application requires the workstation to be rebooted, select this option to postpone the reboot until 1) Application Launcher distributes another application in the list that requires a reboot (and doesn't have this option selected) or 2) Application Launcher completes distribution of all applications in the list. This option also applies when uninstalling the application.

3c Repeat **Step 3a** and **Step 3b** to add another application.

- 4** Arrange the dependent applications in the order in which you want them distributed and launched.

The order in which the dependent applications are listed is the order in which Application Launcher distributes and launches them, going from top to bottom. However, if an application has dependencies, the dependent applications must be distributed and launched before the primary application can be distributed and launched. You can use the up and down arrows to change the order.

- 5** Click *OK* to save your changes.

37.5 Removing an Application Dependency

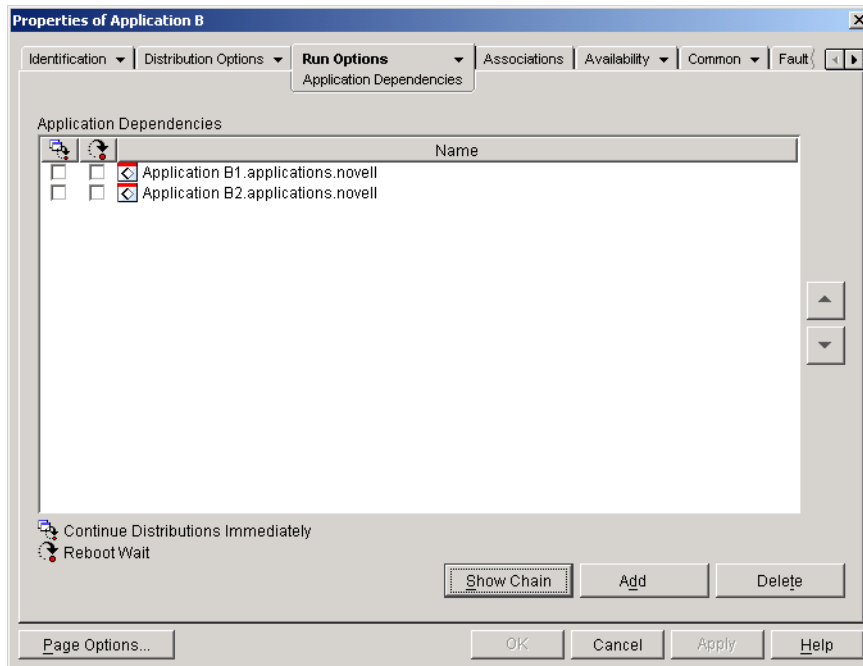
If an application no longer has a dependency on another application, you can remove the dependency. Before doing so, you should be aware of the following:

- Removing the application dependency does not cause the dependent application's files to be uninstalled from the workstation (if the initial distribution included installing of the files). If you want the dependent application uninstalled from the workstation, you must uninstall the primary application, remove the dependency, then redistribute the primary application.
- The user must restart or refresh Application Launcher before the change is recognized. Until the restart or refresh occurs, the application dependency remains.

To remove an application dependency:

- 1** In ConsoleOne, right-click the Application object, then click *Properties* to display the Application object's property page.

- 2 Click the *Run Options* tab > *Application Dependencies* to display the Application Dependencies page.



- 3 In the Application Dependencies list, select the dependent application you want to remove, then click *Delete*.

37.6 Deleting an Application That Has Dependencies

Before you delete the Application object for an application that has dependencies, you should remove the dependencies. Doing so ensures the proper removal of user rights from the dependent applications' objects.

For example, if Application A has two dependent applications, Application B and Application C, users associated with Application A are automatically assigned trustee rights to the Application B object and Application C object. These rights are removed only if you delete Application B and Application C from Application A's dependency list before deleting Application A's object.

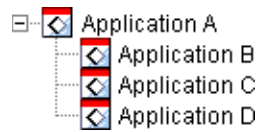
If you unknowingly delete an application before you remove its dependencies, you can manually remove users' trustee rights from the dependent application (ConsoleOne > dependent Application object > *NDS Rights* tab > *Trustees of This Object* page).

37.7 Creating an Application Chain

Application chains that consist of only two levels, as shown in the following illustration, are created by simply adding the dependent applications (B, C, and D) to the dependencies list for the primary

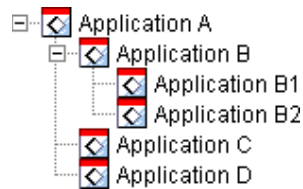
application (A). For instructions, see [Section 37.4, “Adding an Application Dependency,” on page 392](#).

Figure 37-6 *A Two-Level Application Chain*



Application chains that consist of more than two levels, as shown in the following illustration, require you to configure dependencies at each level.

Figure 37-7 *A Three-Level Application Chain*



For example, to create the application chain shown in the above illustration, you would do the following:

- 1 In the Application object for Application B, add Application B1 and B2 as dependent applications.
- 2 In the Application object for Application A, add Application B, Application C, and Application D as dependent applications.

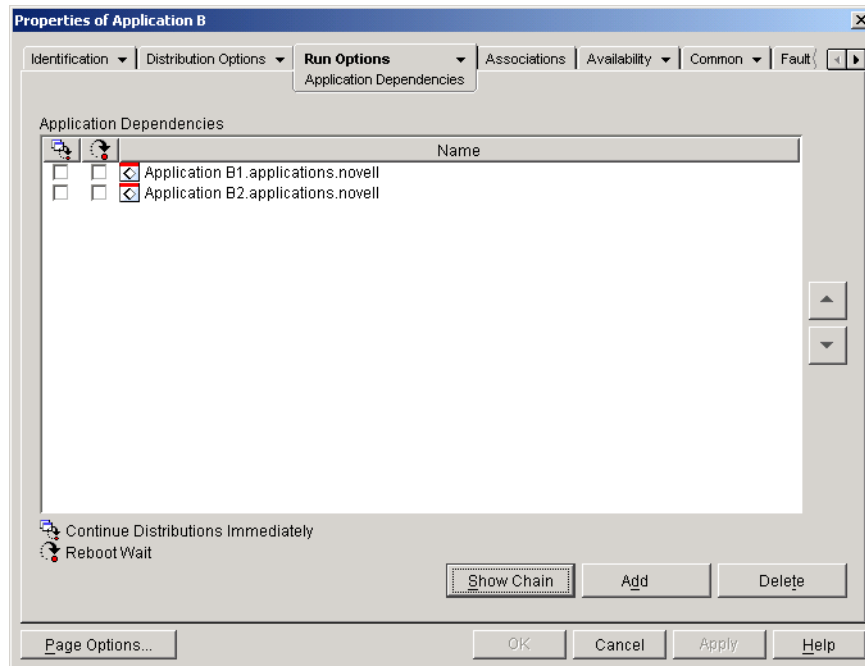
For information about adding applications as dependent applications, see [Section 37.4, “Adding an Application Dependency,” on page 392](#).

37.8 Viewing an Application Chain

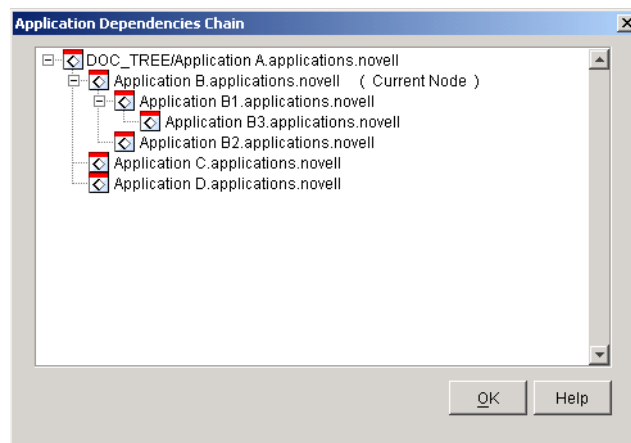
You can view the chains in which the application is a member (either as the primary application or as a dependent application).

- 1 In ConsoleOne, right-click the Application object, then click *Properties* to display the Application object's property page.

- 2 Click the *Run Options* tab > *Application Dependencies* to display the Application Dependencies page.



- 3 Click *Show chain* to display the Application Dependencies Chain dialog box.



In the above example, Application B (the current application, or current node) is a dependent application for Application A. In addition, it has two dependent applications, Application B1 and Application B2.

- 4 When you are finished viewing the chain, click *OK*.

Users: Supporting Terminal Server Users

38

Novell® ZENworks® Desktop Management provides significant flexibility in the way that you can configure application distributions to terminal server users. The following sections provide information to help you establish your distribution method:

- Section 38.1, “Installing the RDP and ICA Clients,” on page 397
- Section 38.2, “Determining Where Novell Application Launcher Runs,” on page 397
- Section 38.3, “Managing Terminal Server User Accounts,” on page 398
- Section 38.4, “Determining the Best Type of Application Objects and File Packages to Use When Distributing an Application,” on page 399
- Section 38.5, “Ensuring Terminal Server Access Through a Firewall,” on page 400

38.1 Installing the RDP and ICA Clients

In order for Application Launcher to launch terminal server applications, users must have the appropriate RDP (Remote Desktop Protocol) client or ICA (Independent Computing Architecture) client installed on their workstations. Novell Application Launcher™ calls either the RDP client or ICA client based on the protocol defined in the terminal server's Application object. The RDP or ICA client then establishes the client session to the terminal server and launches the application.

You can use either the full RDP and ICA clients or the Web clients.

- If you plan to use the full clients, refer to your Citrix and Microsoft Terminal Services documentation for installation information.
- If you plan to use the Web clients, you can download them from the Citrix and Microsoft Web sites:

Citrix ICA `wficac.cab`: (<http://www.citrix.com>)

NOTE: Select the Minimal Web Client 7.00 option.

Microsoft RDP `msrdp.cab`: (<http://www.microsoft.com/windowsxp/pro/downloads/rdwebconn.asp>)

NOTE: Download the `tswebsetup.exe` file and extract the `msrdp.cab` file from it.

38.2 Determining Where Novell Application Launcher Runs

In a terminal server environment, you can run Application Launcher on each user's workstation or you can run it on each terminal server. If necessary, you can have some users run it on their workstations and other users run it on the terminal server.

Application Launcher on User Workstations

If Application Launcher is installed on the workstation, the user starts Application Launcher from the workstation just as he or she would in a non-terminal server environment.

The user must be able to authenticate to Novell eDirectory™ (unless he or she is running in disconnected mode), which means that the workstation must have the Novell Client™ installed or you must have a ZENworks Middle Tier Server installed.

Application Launcher displays the available terminal server applications the same way it does the available non-terminal server applications. However, when the user starts a terminal server application, Application Launcher opens a client session which in turn launches the application in the session. When the user exits the application, Application Launcher closes the client session.

Application Launcher on Terminal Servers

If Application Launcher is installed on the terminal server, the user opens a client session and then starts Application Launcher in the client session.

The user must be able to authenticate to eDirectory through the client session, which means that the workstation must have the Novell Client installed or you must have a ZENworks Middle Tier Server installed.

You need to be aware that Application Launcher does not create a NAL cache directory on the terminal server. This means that Application Launcher cannot run in disconnected mode, cannot uninstall applications it installed to the terminal server, and cannot use the random refresh startup feature. For more information about the NAL cache and the functionality it enables, see [Chapter 24, “Novell Application Launcher: Managing the Cache,”](#) on page 293.

NOTE: After installing Windows 2000 Service Pack 4 (SP4), some programs might not work correctly. For example, the Novell Application Launcher window might fail to display on a Windows 2000 terminal server. To fix this problem, see [TID 10085889 \(http://support.novell.com/cgi-bin/search/searchtid.cgi?/10085889.htm\)](http://support.novell.com/cgi-bin/search/searchtid.cgi?/10085889.htm).

38.3 Managing Terminal Server User Accounts

To run an application from a terminal server, users must have a terminal server user account (either a local user account or a domain user account) and an eDirectory user account. The terminal server user account must provide sufficient file system access to run the applications being hosted on the terminal server. Typically, this requires the user to be a member of the Terminal Server User, Power User, or User group.

In addition, if users are running Application Launcher from the terminal server, the terminal server user account must provide file system access to the Application Launcher files (by default, installed in the `c:\program files\novell\zenworks` directory)

Multiple Users With the Same Terminal Server User Account

Application Launcher supports multiple users logging in to a terminal server through the same user account. However, if users log in through the same terminal server user account at the same time, you should be aware of the following issues:

- All users must also be logged in to eDirectory through the same eDirectory user account. Otherwise, Application Launcher only displays the applications and uses the configuration settings for the last user who starts or refreshes Application Launcher.
- All users need to be running Application Launcher. If one or more users is not, the application icons (distributed by Application Launcher) disappear from the desktop and Quick Launch bar of all users. The icons remain in the Application Launcher windows and the System tray. A workaround is to configure each Application object so that Application Launcher only displays the application icons in the Start menu, System Tray, and Application Launcher windows.
- Set the *Enable automatic icon cleanup* option to *No* (ConsoleOne > User object > ZENworks tab > *Launcher Configuration* page > *Add* button > *User* tab). This restricts Application Launcher from removing application icons when a user exits Application Launcher. For additional information, see [Section 21.3, “Configuring User Settings,” on page 258](#).

38.4 Determining the Best Type of Application Objects and File Packages to Use When Distributing an Application

The type of Application object and file package you create for distributing a terminal server application depends on several factors. The following list describes each type of Application object and package you can use and when you would want to use them:

- **Terminal server application:** You should use a terminal server Application object when the application is installed on the terminal server and Application Launcher is installed on users' workstations, not on the terminal server. When a user starts Application Launcher on his or her workstation and double-clicks a terminal server Application object, Application Launcher calls the RDP or ICA client on the workstation, which then opens a client session with the terminal server and launches the application in the session.

Do not use a terminal server Application object when users are running Application Launcher inside a client session. This is not supported, even if the application is hosted on a different terminal server than the one running Application Launcher. If you do so, the user receives the following error: “Unable to get attributes for Application object...”. The alternatives are to 1) configure the application as a simple Application object or 2) run Application Launcher on the user workstation, rather than the terminal server, and configure the application as a terminal server Application object.

For instructions about creating a terminal server Application object, see [Section 28.2, “Configuring the Application in eDirectory,” on page 316](#).

- **Simple application:** You should use a simple Application object when the application is already installed on the terminal server and Application Launcher is running on the terminal server (in other words, the user opens a client session to the terminal server and then runs Application Launcher in the client session). The simple Application object just points to the application executable file on the terminal server.

You could also use a simple Application object to have Application Launcher install an application to the terminal server when the user launches it. This should only be done with applications that require minimal files to be copied or configuration settings to be changed. Otherwise, an AOT/AXT Application object or an MSI Application object should be used.

For instructions about creating a simple Application object, see [Section 28.2, “Configuring the Application in eDirectory,” on page 316](#).

- **.AOT/AXT application:** You should use an AOT/AXT Application object when the user is running Application Launcher from the terminal server, you want the application distributed to the terminal server when the user launches it, and the application is too complex to be distributed as a simple Application object.

The user must have sufficient file system and registry rights to copy files and registry settings to the locations defined in the Application object. If multiple users install the application, only user-specific files and registry settings are distributed after the first distribution.

For instructions about creating an AOT/AXT Application object and file package, see [Section 28.2, “Configuring the Application in eDirectory,” on page 316](#).

- **.MSI application:** You should use an MSI Application object when the user is running Application Launcher from the terminal server, the application is a Microsoft Windows Installer (MSI) application, and you want it distributed to the terminal server when the user launches it.

The user must be a member of the Administrator group. Microsoft Windows Installer does not allow non-administrator users to do installations through a terminal server client session.

For instructions about creating an MSI Application object and file package, see [Section 28.2, “Configuring the Application in eDirectory,” on page 316](#).

38.5 Ensuring Terminal Server Access Through a Firewall

To ensure that users can access terminal servers through a firewall, you need to open the following firewall ports for sending and receiving TCP/IP packets:

- **3389:** The RDP client and Windows Terminal Services send and receive packets via this port. This is the standard RDP port. If you’ve used a non-standard RDP port, open that port.
- **1494 (in only):** The ICA client sends packets to Citrix MetaFrame servers through this port. This is the standard ICA port. If you’ve used a non-standard ICA port, open that port. For more information about Citrix firewall requirements, see the Citrix documentation.
- **1023 and above (out only):** Citrix MetaFrame servers send packets to ICA clients through these ports. For more information about Citrix firewall requirements, see the Citrix documentation.

Users: Supporting Disconnected Users

39

Novell® Application Launcher™ enables users to distribute, launch, verify, and uninstall applications while disconnected from Novell eDirectory™. This enables users to run the same applications when connected to or disconnected from eDirectory.

The following sections provide information and instructions to help you understand the Application Launcher disconnected mode and to support disconnected users:

- [Section 39.1, “Disconnected Mode Overview,” on page 401](#)
- [Section 39.2, “Configuring Applications as Disconnectable,” on page 403](#)
- [Section 39.3, “Configuring Application Launcher to Start Automatically,” on page 404](#)
- [Section 39.4, “Distributing Applications to Disconnected Workstations,” on page 404](#)

39.1 Disconnected Mode Overview

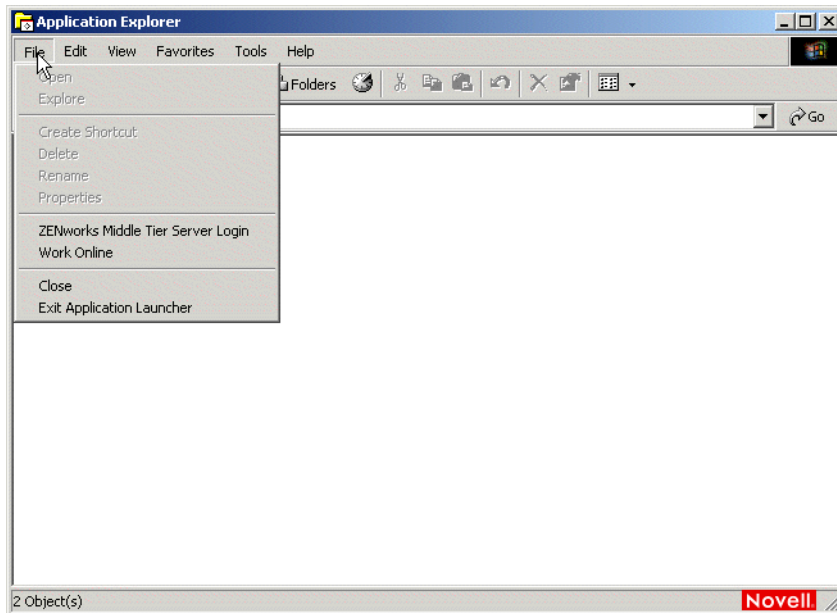
Application Launcher runs in disconnected mode when neither the user nor the workstation is authenticated to eDirectory. User authentication occurs whenever the user logs into eDirectory through the Novell Client™ or the ZENworks® Middle Tier Server. Workstation authentication occurs only if 1) the workstation has been imported as a Workstation eDirectory object and 2) Workstation Manager is installed and can perform the authentication.

Disconnected Mode Indicators

There are several ways you can tell when Application Launcher is running in disconnected mode:

- **File menu:** The File menu in the Application Window, Application Explorer window, and Application Browser window includes a *Work offline/work online* option. When Application Launcher is in disconnected mode, *Work online* is displayed.

Figure 39-1 Application Explorer Window Showing the Work Online Option Available on the File Menu



- **Application Explorer:** The Application Explorer desktop icon changes. The icon on the left below indicates connected mode. The icon on the right indicates disconnected mode.



In addition, the Application Explorer system tray icon changes. The icon on the left below indicates connected mode. The icon on the right indicates disconnected mode.



The NAL Cache

In disconnected mode, Application Launcher reads application information from the NAL cache on the workstation's local drive. Any applications that have been distributed or cached to the workstation continue to be displayed on the workstation. The NAL cache is a critical component of disconnected mode. If you have not already done so, you should review the information in [Chapter 24, “Novell Application Launcher: Managing the Cache,”](#) on page 293.

Work Offline

Application Launcher includes a Work Offline option that lets users force Application Launcher into disconnected mode while remaining authenticated to eDirectory. Work Offline causes Application Launcher to start reading the workstation's NAL cache directory for application information rather than eDirectory. The corresponding Work Online option enables users to switch back to connected mode.

Disconnected Applications

When you create an Application object, the application is automatically configured as being disconnectable. After a disconnectable application is distributed or force cached to a workstation,

Application Launcher continues to display the Application object icon even after the user has disconnected from eDirectory. When the user double-clicks the Application object icon, Application Launcher launches the application.

If an application is not marked disconnectable, Application Launcher does not display the Application object icon when the user disconnects from eDirectory.

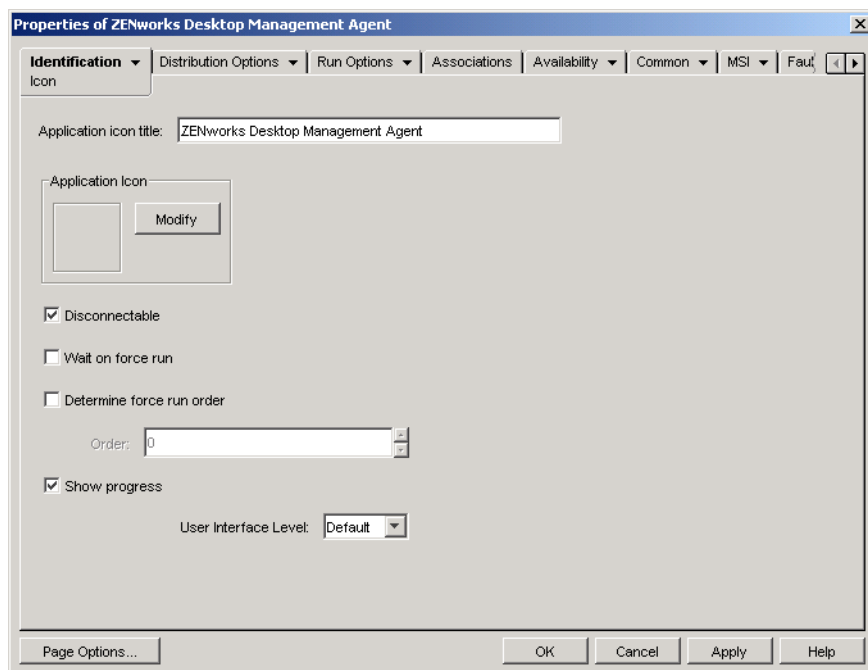
Only applications that can run on a disconnected workstation should be configured as disconnectable. Applications that rely on network resources should not be configured as disconnectable if the network resources is not available. This includes:

- Applications that access a network database
- Client/server applications
- Applications that depend on network drive mappings or print captures
- Applications that use eDirectory macros (other than %CN%) in any of the Application object property fields
- Applications that require a persistent connection to the network

39.2 Configuring Applications as Disconnectable

By default, when you create an Application object the application is marked as being disconnectable. To verify this setting or mark the application as not being disconnectable:

- 1 In ConsoleOne®, right-click the Application object, then click *Properties* to display the Icon page.



- 2 Select the *Disconnectable* option to make the application disconnectable.
- or

Deselect the option to make the application not disconnectable.

3 Click *OK* to save the changes.

39.3 Configuring Application Launcher to Start Automatically

To ensure that Application Launcher starts automatically when a user is in disconnected mode, you can add Application Launcher to the Windows Startup folder during installation of the ZENworks Desktop Management Agent. For details, see “[Installing and Configuring the Desktop Management Agent](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

39.4 Distributing Applications to Disconnected Workstations

As long as a disconnected workstation has Application Launcher installed and running, you can distribute applications to the workstation through the use of removable media such as a CD, Jaz disk, or Zip disk. The removable media functions as a second workstation cache, containing the Application object settings and application source files required to install and run the application.

For example, you have a mobile user who seldom connects to the network but needs an application that you've distributed to other users. You burn a CD with the application and send it to the user. The user inserts the CD into his or her workstation's drive, Application Launcher reads the CD and displays the Application object's icon in the places you've configured (Application Launcher window, Start menu, desktop, and so forth). The user then launches the application, which is distributed to the workstation according to the Application object's configuration.

For information about how to create removable media containing applications, see [Section 50.6](#), “[Create Virtual CD](#),” on page 604.

Novell® ZENworks® Desktop Management includes several features to support users who connect to Novell eDirectory™ through a remote (slow) connection. The following sections provide information and instructions to help you use these features:

- [Section 40.1, “Configuring How Application Launcher Detects a Remote Connection,” on page 405](#)
- [Section 40.2, “Disabling Applications,” on page 407](#)
- [Section 40.3, “Establishing Alternate Applications,” on page 408](#)
- [Section 40.4, “Distributing Applications,” on page 410](#)

40.1 Configuring How Application Launcher Detects a Remote Connection

When Application Launcher starts, it determines whether it is running in local (fast connection) mode or remote (slow connection) mode. If Application Launcher detects an active dial-up connection, it starts in remote mode. In the case where an active dial-up connection is not detected, Application Launcher can use several different methods to determine whether it is running in local or remote mode. You determine which method Application Launcher uses by configuring the Application Launcher settings in ConsoleOne®.

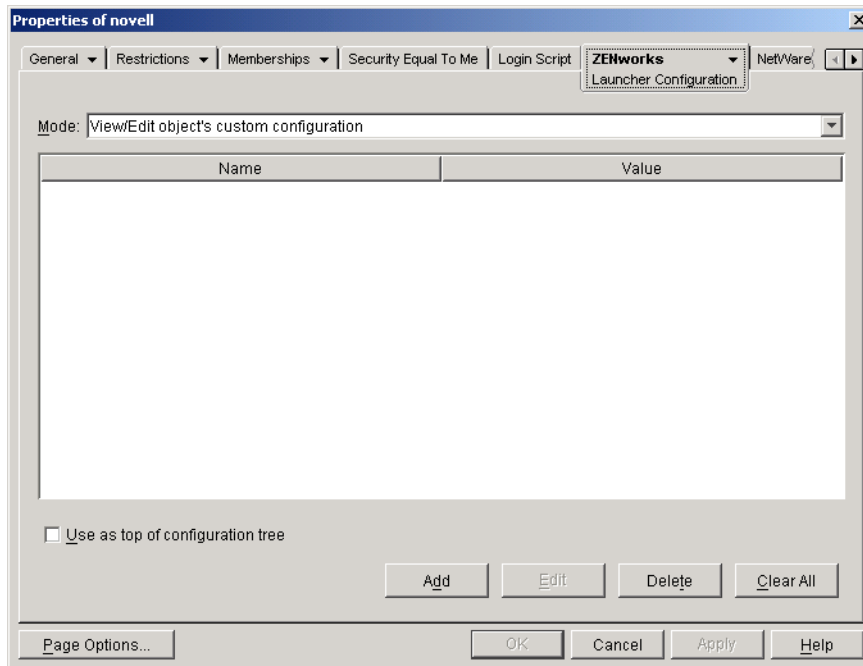
- 1 In ConsoleOne, select a container object if you want to configure the Application Launcher settings for all users in the container.

or

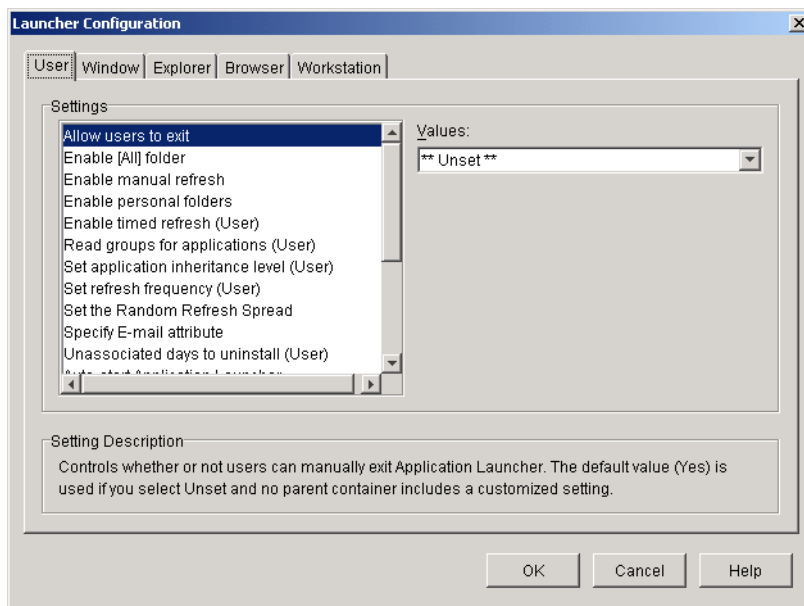
Select a User object if you want to configure an individual user's setting.

- 2 Right-click the object, then click *Properties* to display the object's property pages.

- 3 Click the *ZENworks* tab, then click *Launcher Configuration* to display the Launcher Configuration page.



- 4 Click *Add* to display the Launcher Configuration Settings page.



- 5 In the *Settings* list on the *Users* tab, select the *Configure remote access detection method* option.
- 6 In the *Values* field, select one of the following settings:
 - User will always be local:** Application Launcher functions as if the user is local.
 - User will always be remote:** Application Launcher functions as if the user is remote.

Prompt: Application Launcher prompts the user to select local or remote.

Auto-detect using max interface speed: Application Launcher detects the maximum speed of the network interface card and determines from that speed whether or not the user is local or remote. If you select this option, you must establish the connection speed (threshold) that determines local or remote status.

Detect using network ID: Application Launcher uses the workstation's network ID (also known as the network address) to establish whether or not the user is local or remote.

If you select this option, you must specify the network ID used to establish whether the user is local or remote. To determine the network ID, take the bit-wise logical AND comparison of the 32-bit IP address and 32-bit subnet mask, then convert the resulting 32-bit network ID to dotted decimal notation. In an AND comparison, the result of the two bits being compared is True (1) only when both bits are 1; otherwise, the result is False (0). For example:

10000001 00111000 10111101 00101001	(129.56.189.41 IP address)
-------------------------------------	----------------------------

11111111 11111111 11110000 00000000	(255.255.240.0 subnet mask)
-------------------------------------	-----------------------------

10000001 00111000 10110000 00000000	(129.56.176.0 network ID)
-------------------------------------	---------------------------

If you want workstations whose network IDs match the specified network ID to be considered local, select Network ID Is Equal to This Network ID.

If you want workstations whose network IDs do not match the specified network ID to be considered local, select Network ID Is Not Equal to This Network ID.

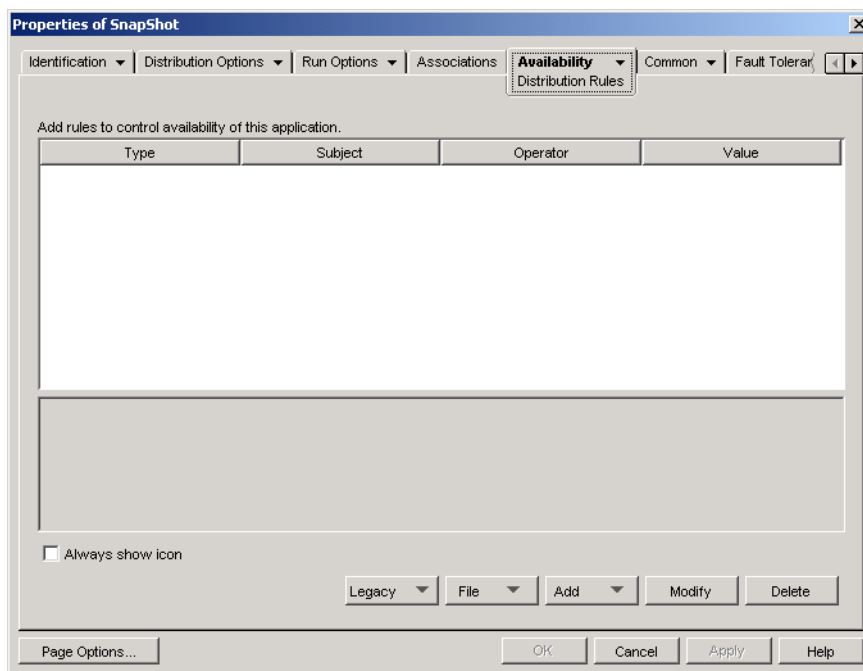
- 7 Click *OK* to save your changes.

40.2 Disabling Applications

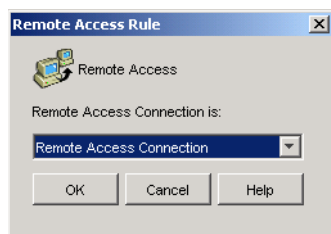
By default, Application Launcher displays an application icon regardless of whether it is running in local or remote mode. If you don't want Application Launcher to display an application in remote mode, you can use the Application object's distribution rules to disable the application.

- 1 In ConsoleOne, right-click the Application object, then click *Properties* to display the Application object's property pages.

- 2 Click the *Availability* tab > *Distribution Rules* to display the Distribution Rules page.



- 3 Click *Add* > *Remote Access* to display the Remote Access Requirements dialog box.



- 4 Select the *Remote access connection* option if you want the application icon enabled only when Application Launcher is in remote mode.

or

Select the *LAN connection* option if you want the application icon enabled only when Application Launcher is in local (LAN) mode.

- 5 Click *OK* to add the rule to the list of distribution rules.
- 6 Click *OK* to save your changes and close the Application object's property pages.

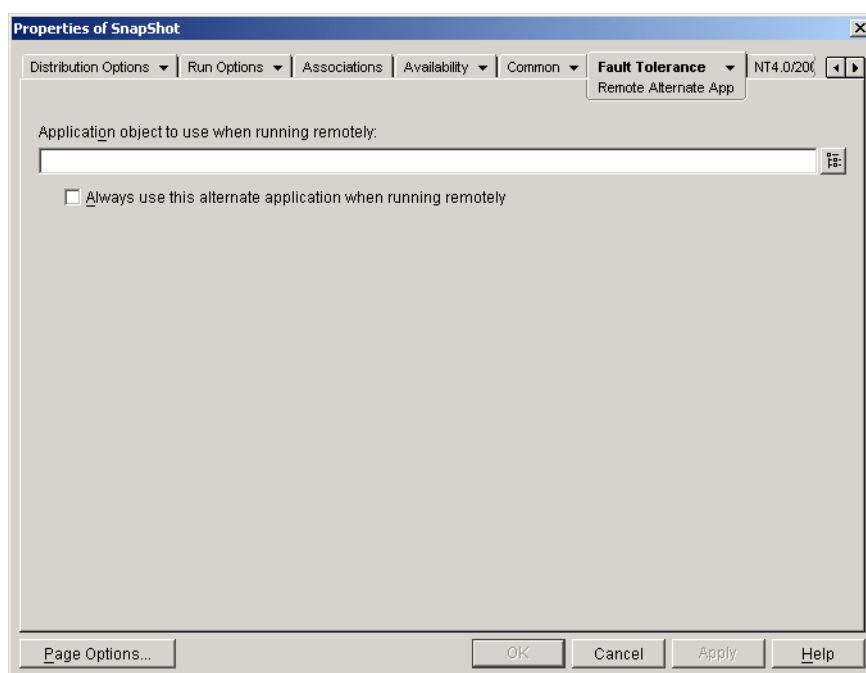
40.3 Establishing Alternate Applications

In some cases, rather than disabling an application altogether (see the previous section, [Disabling Applications](#)), you might want one instance of an application run when users are in local mode and a different instance run when they are in remote mode. To accomplish this, you can configure a “local mode” application to point to an alternate “remote mode” application. When a user launches the “local mode” application while in remote mode, Application Launcher launches the alternate “remote mode” application instead. Generally, this alternate application should be a terminal server application or Web application that is designed for use over slower remote connections.

For example, when a user is accessing an application while in local mode, you might want the application run from a network server installation. However, when the user is accessing the application while in remote mode, you might want it run from a terminal server. You would accomplish this by creating two Application objects, one for the network application and one for the terminal server application, and designating the terminal server application as the remote alternate application for the network server application.

To establish a remote alternate application for an application:

- 1 Make sure the remote alternate application is configured as an Application object in eDirectory.
- 2 In ConsoleOne, right-click the Application object for which you want to establish the remote alternate application, then click *Properties* to display the Application object's property pages.
- 3 Click the *Fault Tolerance* tab > *Remote Alternate App* to display the Remote Alternate App page.



- 4 Fill in the following fields:

Application object to use when running remotely: Select the Application object for the alternate application. Generally, this alternate application should be a terminal server application or Web application that is designed for use over slower remote connections.

Always use this alternate application when running remotely: By default, Application Launcher does not use the alternate application if the original application is installed on the user's workstation; instead, it uses the locally installed application. However, if the application requires access to a database or some other network resource that is only available if the alternate application is used, select this option to force Application Launcher to use the alternate application rather than the locally installed application.

- 5 Click *OK* to save your changes.

40.4 Distributing Applications

When a remote user attempts to run an application for the first time, Application Launcher distributes the application to the user over the slow connection. If this requires many files to be copied to the workstation, this distribution process could take a while.

To speed up the distribution process, you can cache the application to the user's workstation while he or she is still local or distribute the application to the user via removable media such as a CD, Jaz disk, or Zip disk. To let the user control the remote distribution process, you can enable checkpoint restart for the download files. The following sections provide instructions:

- [Section 40.4.1, “Adding Applications to the Cache,” on page 410](#)
- [Section 40.4.2, “Distributing Applications Via Removable Media,” on page 411](#)
- [Section 40.4.3, “Enabling Checkpoint Restart for File Downloads,” on page 411](#)

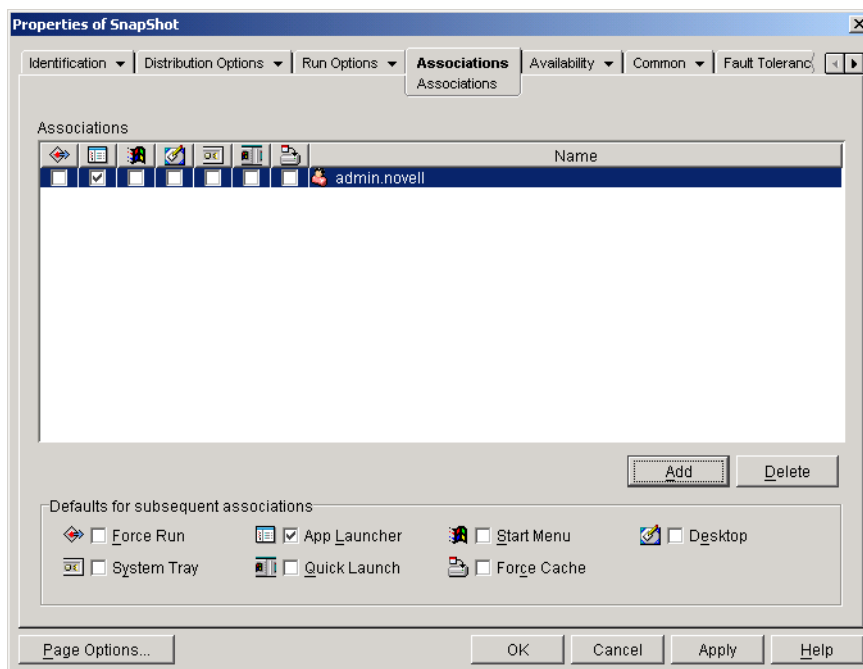
40.4.1 Adding Applications to the Cache

You can enable a user to install or verify an application from the local NAL cache rather than across a slow connection. To do so, you must copy the application's source files to the workstation's local NAL cache directory while the user is still connected via a local (LAN) connection.

For information about the NAL cache, see [Chapter 24, “Novell Application Launcher: Managing the Cache,” on page 293](#).

To cache an application:

- 1 In ConsoleOne, right-click the Application object, then click *Properties*.
- 2 Click the *Associations* tab to display the Associations page.



- 3 In the Associations list, select the *Force cache* box for the user whose workstation you want to cache the application to.

NOTE: In order to cache an application, it must be marked as *Disconnectable*. If the application is not marked as *Disconnectable*, the *Force cache* option is not available. For instructions, see [Section 39.2, “Configuring Applications as Disconnectable,” on page 403](#).

If you select the *Distribute always* option and a remote connection is detected, ZENworks behaves as if the *Force cache* and *Check point restart* options are enabled (even if you did not enable these options when you configured the Application object).

- 4 Click *OK* to save the changes.

The application is cached to the user's local drive the next time Application Launcher restarts or refreshes.

40.4.2 Distributing Applications Via Removable Media

As long as a workstation has Application Launcher installed and running, you can distribute applications to the workstation through the use of removable media such as a CD, Jaz disk, or Zip disk. The removable media function as a second workstation cache, containing the Application object settings and application source files required to install and run the application.

For example, you have a mobile user who seldom connects to the network but needs an application that you've distributed to other users. You burn a CD with the application and then send it to the user. The user inserts the CD into his or her workstation's drive, and Application Launcher reads the CD and displays the Application object's icon in the places you've configured (Application Launcher window, Start menu, desktop, and so forth). The user then launches the application, which is distributed to the workstation according to the Application object's configuration.

For information about how to create removable media containing applications, see [Section 50.6, “Create Virtual CD,” on page 604](#).

40.4.3 Enabling Checkpoint Restart for File Downloads

When a remote user attempts to run an application for the first time, Application Launcher distributes the application to the user over the slow connection (if the application is not cached to the user's local drive). If this requires many files to be copied to the workstation, this download process could take a while.

To allow a user to interrupt an application's download process and then resume it at a later time, picking up at the point the download left off, Application Launcher supports checkpoint restart. By default, this feature is enabled. If checkpoint restart is not enabled, Application Launcher starts over on the download process rather than resuming where it left off.

NOTE: If you select the *Distribute always* option and a remote connection is detected, ZENworks behaves as if the *Force cache* and *Check point restart* options are enabled (even if you did not enable these options when you configured the Application object).

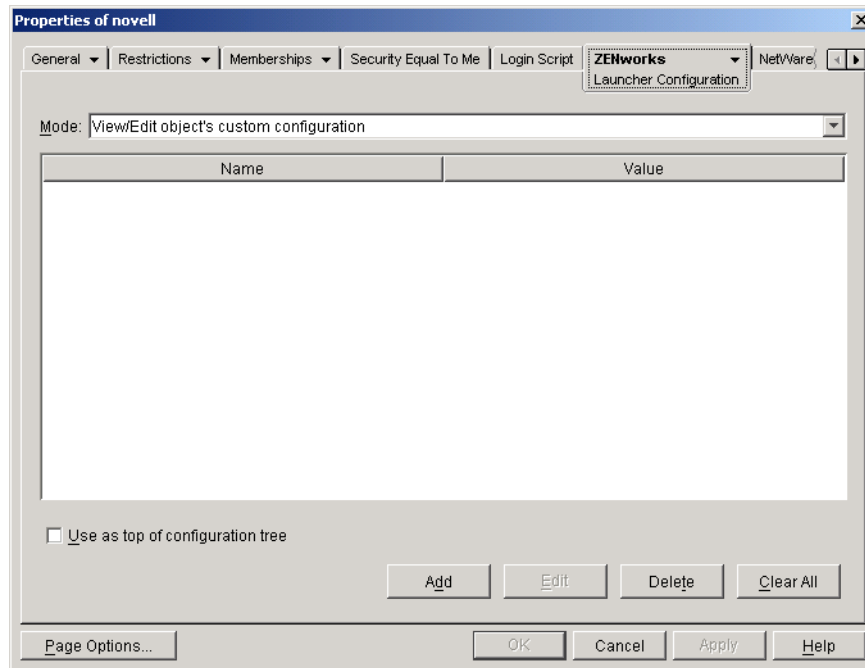
To verify that checkpoint restart is enabled, or to disable it:

- 1 In ConsoleOne, select a container object if you want to configure the checkpoint restart setting for all users in the container.

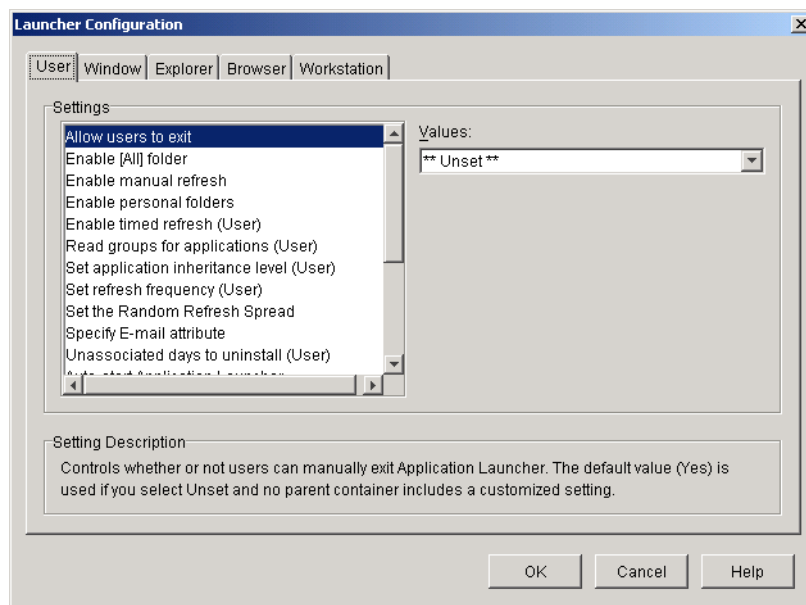
or

Select a User object if you want to configure an individual user's checkpoint restart setting.

- 2 Right-click the object, then click *Properties* to display the object's property pages.
- 3 Click the *ZENworks* tab > *Launcher Configuration* to display the Launcher Configuration page.



- 4 Click *Add* to display the Launcher Configuration Settings page.



- 5 In the *Settings* list on the *Users* tab, select the *Enable the checkpoint restart postpone button* option.

- 6** In the *Values* field, select *Yes* to enable it, *No* to disable it, or *Unset* to inherit the setting from the current object's parent container.
- 7** Click *OK* to save your changes.

Controlling Rogue Processes

41

You can configure Novell® Application Launcher™ to manage rogue processes. Rogue processes are processes that are not started by either Application Launcher or the LocalSystem user.

The following sections provide information to help you understand and implement rogue process management:

- [Section 41.1, “What Rogue Process Management Does,” on page 415](#)
- [Section 41.2, “How Rogue Process Management Works,” on page 415](#)
- [Section 41.3, “Setting Up Rogue Process Management,” on page 416](#)

41.1 What Rogue Process Management Does

To help you manage rogue processes, Application Launcher can do the following:

- Track and log the use of rogue processes.
- Ignore all rogue processes (allow them to run).
- Terminate all rogue processes.
- Apply an exceptions list. If rogue processes are being ignored, the processes included in the exceptions list are terminated. If rogue processes are being terminated, the processes in the exceptions list are ignored.

For example, if you only want to track rogue processes, you can configure Application Launcher to log rogue process information to a text file on a network server but still allow the processes to run. If, however, you want to shut down the use of rogue processes, you can configure Application Launcher to log the process information and also terminate the processes.

When you enable rogue process management, depending on the configuration setting you use, Application Launcher either ignores all rogue processes or terminates all rogue processes. However, if you want Application Launcher to either ignore or terminate all but a few rogue processes, you can create an exceptions list.

For example, if you want to allow all rogue processes except for the standard Windows games (Solitaire, Minesweep, Freecell, and Pinball), you could configure Application Launcher to ignore all rogue processes and create an exceptions list that includes the four Windows games. Application Launcher would then allow all rogue processes except the four games.

To ensure that user can't bypass the exceptions list by renaming the games' executable files, Application Launcher checks the launched processes' current executable name and the original filename (an internal filename) against the exceptions list.

41.2 How Rogue Process Management Works

The Windows operating system tracks all processes that are currently running. You can see this list by viewing the Processes tab in the Windows Task Manager (right-click the taskbar, then click *Task Manager > Processes*).

Each process has both a process identifier (PID) and a parent process identifier (parent PID). The parent PID identifies the process that launched it. Application Launcher uses a Windows API to retrieve the process list, including the PIDs and parent PIDs, every three seconds. Using the parent PIDs, Application Launcher knows whether or not the process is a rogue process. If the parent PID is not Application Launcher's PID, or if the process is not running as the LocalSystem user, then it is a rogue process.

After Application Launcher identifies the rogue processes, it performs the appropriate management actions, either ignoring or terminating the processes, taking into account any processes identified in the exceptions list. If logging is enabled, it also writes the rogue process information to the log file.

41.3 Setting Up Rogue Process Management

Rogue process management is enabled and configured through the Windows registry. The following sections explain how to manually modify the registry on Windows 98 and Windows 2000/XP workstations and how to create an Application object to distribute the registry changes through Application Launcher:

- [Section 41.3.1, “Manually Modifying the Registry,” on page 416](#)
- [Section 41.3.2, “Creating an Application Object to Distribute the Registry Modifications,” on page 418](#)

41.3.1 Manually Modifying the Registry

- 1 Use `regedit.exe` to open the Windows registry.
- 2 Locate the following key:
`HKEY_CURRENT_USER\Software\NetWare\NAL\1.0`
- 3 Add a Process Management key under the 1.0 key:
`HKEY_CURRENT_USER\Software\NetWare\NAL\1.0\Process Management`
- 4 Add a Default Action value to the Process Management key using the following information:
Value type: DWORD
Value name: Default Action
Value data: To have Application Launcher ignore all rogue processes, enter 0. To have Application Launcher terminate all rogue processes, enter 1.
- 5 Add a Report Terminated value to the Process Management key using the following information:
Value type: DWORD
Value name: Report Terminated
Value data: To disable reporting of rogue processes that Application Launcher terminates, enter 0. To enable reporting of terminated rogue processes, enter 1.
- 6 Add a Report Ignored value to the Process Management key using the following information:
Value type: DWORD
Value name: Report Ignored
Value data: To disable reporting of rogue processes that Application Launcher ignores, enter 0. To enable reporting of ignored rogue processes, enter 1.

- 7** If you enabled reporting by adding a *Report terminated* or *Report ignored* value, you need to determine where you want the reports sent. To do so:

- 7a** Add a `Reporting targets` key to the `Process management` key:

```
HKEY_CURRENT_USER\Software\NetWare\NAL\1.0\Process  
Management\Reporting Targets
```

- 7b** To configure database reporting, add a *Database* value to the `Reporting targets` key using the following information:

Value type: DWORD

Value name: Database

Value data: To disable reporting to a database, enter 0. To enable reporting to a database, enter 1. When this option is enabled, Application Launcher writes to the database determined by the Service Location Policy package associated with the user. For more information, see [“Enabling the ZENworks Database Policy” on page 435](#).

For information about queries you can use to generate reports from the database, see [Section 44.6, “Generating Reports from a Database,” on page 451](#).

- 7c** To configure SNMP reporting, add an *SNMP* value to the `Reporting targets` key using the following information:

Value type: DWORD

Value name: SNMP

Value data: To disable SNMP reporting, enter 0. To enable SNMP reporting, enter 1. When this option is enabled, Application Launcher sends to the SNMP trap targets determined by the Service Location Policy package associated with the user. For more information, see [“Enabling the SNMP Trap Targets Policy” on page 438](#).

- 7d** To configure XML reporting, add an *XML* value to the `Reporting Targets` key using the following information:

Value type: DWORD

Value name: XML

Value data: To disable XML reporting, enter 0. To enable XML reporting, enter 1. When this option is enabled, Application Launcher sends to the XML targets determined by the Service Location Policy package associated with the user. For more information, see [“Enabling the SNMP Trap Targets Policy” on page 438](#).

If the XML reports are being processed into a database, see [Section 44.6, “Generating Reports from a Database,” on page 451](#) for information about queries you can use to generate reports from the database.

- 7e** To configure log file reporting, add a *File* value to the `Reporting targets` key using the following information:

Value type: String

Value name: File

Value data: Specify the full path and filename to be used for the log file. This can be a mapped drive or a UNC path to a local or network drive. For example, `\\server1\vol1\process\rogue.txt`. If you do not enter a value, log file reporting is disabled.

For information about understanding the information written to the log file, see [Section 44.7, “Understanding Log File Reports,” on page 454](#).

- 8 If you want to use an exceptions list, create an `Exception list` key under the `Process management` key:

```
HKEY_CURRENT_USER\Software\NetWare\NAL\1.0\Process  
Management\Exception List
```

The **Default Action** setting ([Step 4](#)) determines what happens to the processes you add to the exceptions list. If the **Default Action** is set to 0 (ignore processes), then any processes you add to the exceptions list are terminated rather than ignored. If the **Default Action** is set to 1 (terminate processes), then any processes you add to the exceptions list are ignored rather than terminated.

- 9 Add a `DWORD` value to the `Exception list` key for each process you want added to the list.

Value type: `DWORD`

Value name: Enter the process filename. You can enter either the displayed executable name or the original filename. If the process has an original filename, it is listed on the **Version** tab of the executable's **Properties** dialog box (right-click the executable file > click **Properties** > click **Version**). Do not enter a path for the file, only the filename.

Value data: Do not enter anything in this field.

- 10 Save the registry changes.

41.3.2 Creating an Application Object to Distribute the Registry Modifications

- 1 In ConsoleOne®, create a simple Application object (see [Chapter 28, “Distribution: Simple Applications,”](#) on page 315 if necessary), using the following information:

Object name: Specify a unique name for the eDirectory object (for example, *Rogue Process Management*).

Path to file: Do not specify anything in this field.

Distribution rules: If you want to enforce specific rules before the registry changes are distributed to a workstation, define the rules. You can also do this at a later time.

Associations: Select the users or workstations you want the changes distributed to. You can also do this at a later time.

- 2 After you've created the Application object, right-click the object, then click *Properties* to display the object's property pages.
- 3 Click *Distribution Options*, then click *Registry* to display the Registry page.
- 4 Create the following registry key:

```
HKEY_CURRENT_USER\Software\NetWare\NAL\1.0\Process Management
```

To create the key:

- 4a Select the `HKEY_CURRENT_USER` key, click *Add*, then click *Key* to add a new entry key called *New Key*.
 - 4b Rename the key to *Software*.
 - 4c Repeat the process described in [Step 4a](#) and [Step 4b](#) to create the complete key structure.
- 5 Add a **Default Action** value to the `Process Management` key. To do so:

- 5a Select the `Process Management` key, click *Add*, click *DWORD* to display the Edit DWORD Value dialog box, then fill in the fields as follows:

Value name: Default Action

Value data: To have Application Launcher ignore all rogue processes, enter 0. To have Application Launcher terminate all rogue processes, enter 1.
- 5b Click *OK* to add the *Default Action* value to the `Process management` key.
- 6 Add a *Report Terminated* value to the `Process management` key. To do so:
 - 6a Select the `Process management` key, click *Add*, click *DWORD* to display the Edit DWORD Value dialog box, then fill in the fields as follows:

Value name: Report Terminated

Value data: To disable reporting of rogue processes that Application Launcher terminates, enter 0. To enable reporting of terminated rogue processes, enter 1.
 - 6b Click *OK* to add the Report Terminated value to the `Process management` key.
- 7 Add a *Report ignored* value to the `Process management` key. To do so:
 - 7a Select the `Process management` key, click *Add*, click *DWORD* to display the Edit DWORD Value dialog box, then fill in the fields as follows:

Value name: Report Ignored

Value data: To disable reporting of rogue processes that Application Launcher ignores, enter 0. To enable reporting of ignored rogue processes, enter 1.
 - 7b Click *OK* to add the *Report ignored* value to the `Process management` key.
- 8 If you enabled reporting by adding a *Report terminated* or *Report ignored* value, you need to determine where you want the reports sent. To do so:
 - 8a Add a `Reporting targets` key to the `Process management` key:


```
HKEY_CURRENT_USER\Software\NetWare\NAL\1.0\Process Management\Reporting Targets
```
 - 8b To configure database reporting, add a *Database* value to the `Reporting targets` key using the following information:

Value type: DWORD

Value name: Database

Value data: To disable reporting to a database, enter 0. To enable reporting to a database, enter 1. When this option is enabled, Application Launcher writes to the database determined by the Service Location Policy package associated with the user. For more information, see [“Enabling the ZENworks Database Policy” on page 435](#).

For information about queries you can use to generate reports from the database, see [Section 44.6, “Generating Reports from a Database,” on page 451](#).
 - 8c To configure SNMP reporting, add an *SNMP* value to the `Reporting targets` key using the following information:

Value type: DWORD

Value name: SNMP

Value data: To disable SNMP reporting, enter 0. To enable SNMP reporting, enter 1. When this option is enabled, Application Launcher sends to the SNMP trap targets determined by the Service Location Policy package associated with the user. For more information, see [“Enabling the SNMP Trap Targets Policy” on page 438](#).

- 8d** To configure XML reporting, add an *XML* value to the *Reporting targets* key using the following information:

Value type: DWORD

Value name: XML

Value data: To disable XML reporting, enter 0. To enable XML reporting, enter 1. When this option is enabled, Application Launcher sends to the XML targets determined by the Service Location Policy package associated with the user. For more information, see [“Enabling the SNMP Trap Targets Policy” on page 438](#).

If the XML reports are being processed into a database, see [Section 44.6, “Generating Reports from a Database,” on page 451](#) for information about queries you can use to generate reports from the database.

- 8e** To configure log file reporting, add a *File* value to the *Reporting targets* key using the following information:

Value type: String

Value name: File

Value data: Specify the full path and filename to be used for the log file. This can be a mapped drive or a UNC path to a local or network drive. For example, `\\server1\vol1\process\rogue.txt`. If you do not enter a value, log file reporting is disabled.

For information about understanding the information written to the log file, see [Section 44.7, “Understanding Log File Reports,” on page 454](#).

- 9** If you want to use an exceptions list, create an *Exception list* key under the *Process management* key:

```
HKEY_CURRENT_USER\Software\NetWare\NAL\1.0\Process  
Management\Exception List
```

The Default Action setting ([Step 4](#)) determines what happens to the processes you add to the exceptions list. If the Default Action is set to 0 (ignore processes), then any processes you add to the exceptions list are terminated rather than ignored. If the Default Action is set to 1 (terminate processes), then any processes you add to the exceptions list are ignored rather than terminated.

- 10** Add a string value to the *Exception list* key for each process you want added to the list. To do so:

- 10a** Select the *Exception list* key, click *Add..*, click *DWORD* to display the Edit DWORD Value dialog box, then fill in the fields as follows:

Value name: Enter the process filename. You can enter either the displayed executable name or the original filename. If the process has an original filename, it is listed on the Version tab of the executable's Properties dialog box (right-click the executable file, click Properties, then click Version). Do not enter a path for the file, only the filename.

Value data: Do not enter anything in this field.

- 10b** Click *OK* to add the value to the *Exception list* key.

- 11** Click the *Associations* tab to display the Associations page.

- 12** Add the users and workstation you want to distribute the changes to. To make sure the changes are made without requiring any user intervention, enable the *Force run* option on each association.

13 Click *OK* to save the changes to the Application object.

The registry modifications are distributed to associated users the next time Application Launcher refreshes and to associated workstations the next time Application Launcher Workstation Helper refreshes.

Novell® ZENworks® Desktop Management includes the ability to verify and, if necessary, repair applications distributed through Novell Application Launcher™. By default, if Application Launcher is unable to launch an application, it prompts the user to verify the application.

The following sections provide information to help you understand how automatic application verification, sometimes referred to as application self-healing, works and how users can use Application Launcher to manually verify applications:

- [Section 42.1, “How Application Launcher Detects Broken Applications,” on page 423](#)
- [Section 42.2, “How Application Files are Verified,” on page 423](#)
- [Section 42.3, “Why Automatic Verification Can Fail,” on page 423](#)
- [Section 42.4, “Using Application Launcher to Verify an Application,” on page 424](#)

42.1 How Application Launcher Detects Broken Applications

Application Launcher detects a broken application at launch time. If the application file it calls can't launch (in other words, the CreateProcess call Application Launcher makes returns a FALSE), Application Launcher assumes the application is broken and needs to be verified. When this occurs, Application Launcher prompts the user that a problem exists and lets the user choose whether or not to verify the application.

42.2 How Application Files are Verified

If an application launch is not successful and the prompted user chooses to verify the application, Application Launcher redistributes all of the application's files to the workstation. How this is done depends on whether Application Launcher is running in connected or disconnected mode:

- In connected mode, the application files are redistributed from the network.
- In disconnected mode, the application files are redistributed from the local NAL cache directory (typically, `c:\nalcache`), provided the application files have been cached to the directory. If they have not been cached, the application cannot be verified until Application Launcher is in connected mode.

42.3 Why Automatic Verification Can Fail

Occasionally, Application Launcher cannot automatically repair a broken application, even when it has access to the application's installation files (from the network in connected mode or from the NAL cache in disconnected mode). This is because of the method Application Launcher uses to detect broken applications.

When Application Launcher successfully launches the file (in other words, the CreateProcess call it makes returns a true), it assumes a successful launch. In some cases, however, the file that Application Launcher calls doesn't actually start the application but in turn calls another file to start

the application. If that file is broken, missing, or cannot launch, the application launch fails without Application Launcher prompting the user to verify the application. For example:

- If you delete WinZip's `wz32.dll` and then launch `winzip32.exe`, Application Launcher successfully calls `winzip32.exe`, so it assumes a successful launch. However, when `winzip32.exe` calls `wz32.dll`, the launch fails because `wz32.dll` does not exist. Because Application Launcher only automatically prompts users to verify applications that it cannot launch, and it successfully launched `winzip32.exe`, the application is not automatically repaired.
- You delete `consoleone.exe` and then try to launch the application. Because Application Launcher calls Java, which in turn starts ConsoleOne®, the launch fails. However, Application Launcher does not automatically verify ConsoleOne because it successfully launched Java.

In these cases, Application Launcher displays the following message:

```
Error message: Application Launcher Status - Could not launch
Application_Object_Name (id=xxx) The filename, directory name, or
volume label syntax is incorrect.
```

Although Application Launcher cannot automatically prompt users to verify applications that fit this scenario, user's can manually initiate the verification on their own. For information about how to do this, see the next section, [Using Application Launcher to Verify an Application](#).

42.4 Using Application Launcher to Verify an Application

Users can use Application Launcher's Verify option to initiate the repair of a broken application. To do so, the user must:

- 1 Right-click the application icon.
- 2 Click *Verify*.

Uninstalling Applications

43

Applications distributed through Novell® ZENworks® Desktop Management can be uninstalled. You can choose whether or not to uninstall all files, shortcuts, INI entries, and registry entries that were installed or modified with the application.

Each user's workstation contains a local NAL cache directory that contains information about applications installed on the workstation. When you uninstall an application, this cache is used to ensure that the appropriate files and settings are removed from the workstation. If the application's source files have been copied to the workstation's local cache, the source files are also removed. For more information about the local cache, see [Chapter 24, “Novell Application Launcher: Managing the Cache,”](#) on page 293.

By default, the ability to uninstall an application is disabled. You must first enable an application to be uninstalled. After that, you can uninstall an application by disassociating it from users or workstations, you can configure it to be uninstalled after a certain period of inactivity, or users can uninstall it through Novell Application Launcher™ (provided you've enabled this functionality). See the following sections for information:

- [Section 43.1, “Enabling an Application to be Uninstalled,”](#) on page 425
- [Section 43.2, “Uninstalling Applications by Disassociating Users or Workstations,”](#) on page 427
- [Section 43.3, “Uninstalling Unused Applications,”](#) on page 428
- [Section 43.4, “Using Application Launcher to Uninstall an Application,”](#) on page 429
- [Section 43.5, “Uninstalling Applications from Terminal Servers,”](#) on page 430

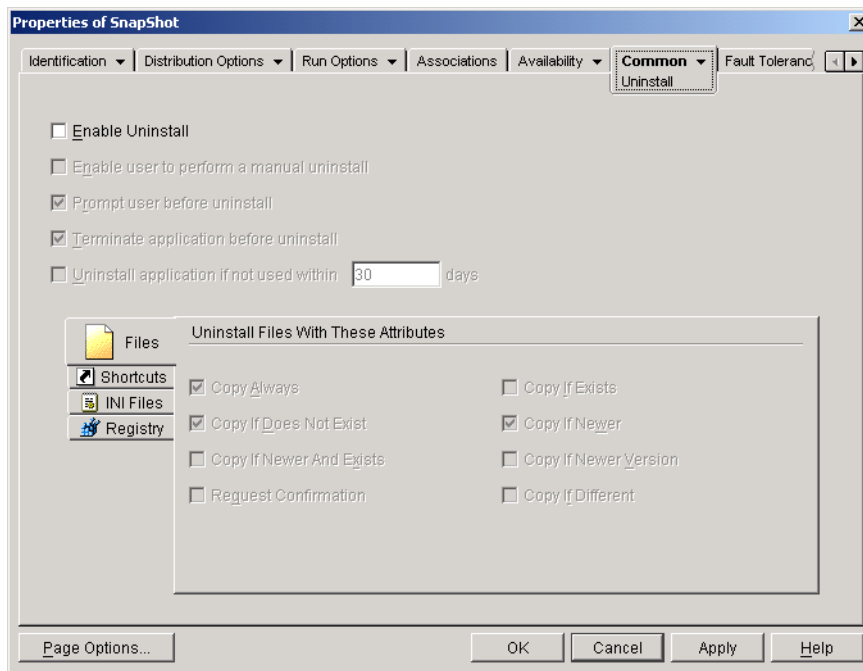
43.1 Enabling an Application to be Uninstalled

Uninstalling an application requires careful configuration of the Application object to ensure that no critical files are accidentally removed from the workstation. For this reason, the ability to uninstall an application is disabled by default.

To enable an application to be uninstalled:

- 1 In ConsoleOne®, right-click the Application object, then click *Properties*.

- 2 Click the *Common* tab > *Uninstall* to display the Uninstall page.



- 3 Click the *Enable uninstall* box to turn on the option.
- 4 If you want users to be able to uninstall the application themselves, click *Enable user to perform a manual uninstall* to turn on the option.

For information about how users can uninstall the application, see [Section 43.4, “Using Application Launcher to Uninstall an Application,”](#) on page 429.

- 5 Set the other Uninstall options as appropriate:

Prompt user before uninstall: Select this option to prompt users before removing the application from their workstations. If users answer *No* to the prompt, the application is not removed.

Prompt user before reboot: In some cases, uninstalling an application might require restarting the workstation. Select this option to prompt users before restarting the workstation. If users answer *No* to the prompt, the uninstallation is not completed until the next time they manually restart.

Terminate application before uninstall: Select this option to ensure that Application Launcher terminates the application (if the application is running) before it begins uninstalling the application files.

Uninstall application if not used within xx days: Select this option to automatically remove the application if the user has not run it within the specified number of days (the default is 30). For more information, see [Section 43.3, “Uninstalling Unused Applications,”](#) on page 428.

- 6 Select the attributes you want used when determining whether or not to uninstall files, shortcuts, INI settings, and registry settings.

Files: Click *Files*, then select the attributes you want to use to determine whether or not an application file is removed. The attributes correspond to the attributes listed on the Application Files page (*Distribution Options* tab). The default selections (*Copy always*, *Copy if does not*

exist, Copy if newer) ensure that a file is removed only if it was installed when the application was installed and not at an earlier time by another application that might still need the file.

Shortcuts: Click *Shortcuts*, then select the attributes you want to use to determine whether or not the application's shortcuts are removed. The attributes correspond to the attributes listed on the Shortcuts/Icons page (Distribution Options tab).

INI files: Click *INI files*, then select the attributes you want to use to determine whether or not an INI setting is removed. The attributes correspond to the attributes listed on the INI Settings page (Distribution Options tab). The default selections (*Create always, Create if exists, Create or Add to existing section*) ensure that a setting is removed only if it was created when the application was installed and not at an earlier time by another application that might still need the setting.

Registry: Click *Registry*, then select the attributes you want to use to determine whether or not a registry setting is removed. The attributes correspond to the attributes listed on the Registry Settings page (Distribution Options tab). The default selections (*Create always, Create if exists*) ensure that a setting is removed only if it was created when the application was installed and not at an earlier time by another application that might still need the setting.

The *Uninstall keys/values from these registry hives* option allows you to select two specific registry hives, `HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER`, to include or exclude when removing the registry settings that were added by Application Launcher during distribution of the application to the workstation. The default settings cause Application Launcher to remove settings from the `HKEY_CURRENT_USER` hive but not from the `HKEY_LOCAL_MACHINE` hive.

The purpose of this option is to help you ensure that no Windows system settings are removed during the uninstall. This is particularly important if you used snAppShot™ to capture the application's installation. When snAppShot captures an application's installation, it includes all settings that are changed during the installation. If the application's installation program causes the workstation to reboot during the installation process, these changes can include not only settings that apply to the application but also settings that apply to the Windows system. Removing Windows system settings might cause the workstation to encounter problems when starting up. It is strongly recommended that you remove these settings only if you are positive that they will not affect the workstation's ability to function properly.

If you want to use this option, you should examine the registry settings that will be removed from the `HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER` hives and delete any settings that apply to anything other than the application. The registry settings are displayed on the Registry Settings page (Distribution Options tab).

7 Click *OK* to save the changes.

43.2 Uninstalling Applications by Disassociating Users or Workstations

By default, when you disassociate an application from a user or workstation, Application Launcher no longer displays the Application object, but the application's files, shortcuts, INI settings, and registry settings are not removed from the workstation.

To configure an application to be uninstalled when it is disassociated from a user or workstation:

- 1** Enable the application to be uninstalled. To do so:
 - 1a** In ConsoleOne, right-click the Application object, then click *Properties*.

- 1b** Click the *Common* tab > *Uninstall* to display the Uninstall page.
- 1c** Select the *Enable uninstall* option to turn it on.
- 1d** Configure any other uninstall settings as desired. See [Section 43.1, “Enabling an Application to be Uninstalled,” on page 425](#) or refer to the Help on the Uninstall page.
- 1e** Click *OK* to save your changes.
- 2** Configure Application Launcher to uninstall the application rather than leave it. To do so:

You must configure Application Launcher for each user or workstation from which you want uninstallation to occur upon disassociation. You can do this through User, Workstation, Group, Workstation Group, or container objects.

 - 2a** Right-click a User, Workstation, Group, Workstation Group, or container object, then click *Properties*.
 - 2b** Click the *ZENworks* tab > *Launcher Configuration* to display the Launcher Configuration page.
 - 2c** Click the *Add* button to display the Launcher Configuration dialog box.
 - 2d** Select the *User* tab, then the *Unassociated days to uninstall* setting.
 - 2e** In the *Values* field, select *Custom*, then specify the number of days after disassociation that you want applications uninstalled.

Specify 0 if you want uninstallation to occur immediately upon Application Launcher refresh or restart.
 - 2f** Repeat [Step 2d](#) and [Step 2e](#) to configure uninstallation of workstation-associated applications, using the Workstation tab rather than the User tab.
 - 2g** Click *OK*, then click *OK* again to save your changes.

The next time you disassociate a user or workstation (for which you've configured Application Launcher) from the application, the application is uninstalled from the workstation.

43.3 Uninstalling Unused Applications

Users might install some applications, run them a few times, and then not use them again for a long period of time. These applications can unnecessarily take up valuable workstation disk space.

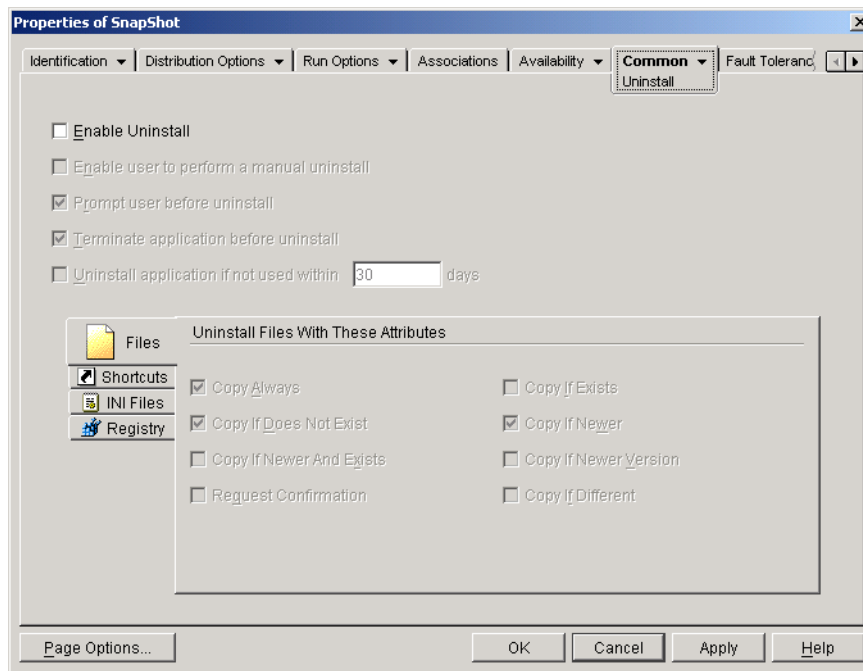
To free up disk space, you can have Application Launcher uninstall an application that has not been run for a period of time. The default time period is 30 days, but you can change the setting to meet your needs. For example, you might want one application removed after 15 days of inactivity, but you might not want to remove another application until it has not been run for 90 days.

After an unused application is uninstalled, Application Launcher continues to display the Application object icon on the workstation unless the user or workstation is disassociated from the Application object. If the user double-clicks the icon, the application is installed again.

To configure an unused application to be removed after a period of time:

- 1** In ConsoleOne, right-click the Application object, then click *Properties*.

- 2 Click the *Common* tab > *Uninstall* to display the Uninstall page.



- 3 If the *Enable uninstall* option is not turned on, select the check box to turn it on.
- 4 Click *Uninstall application if not used within xx days* to turn on the option, then select the number of days you want.
- 5 If you have not selected the attributes you want to use to determine whether or not the application's files, shortcuts, INI settings, and registry settings are removed, do so now. For information about each option, see [Section 43.1, “Enabling an Application to be Uninstalled,” on page 425](#) or refer to the Uninstall page's Help.
- 6 Click *OK* to save the changes.

43.4 Using Application Launcher to Uninstall an Application

By default, users are not allowed to uninstall distributed applications. However, if you've enabled users to uninstall applications (see [Section 43.1, “Enabling an Application to be Uninstalled,” on page 425](#)), they can do so through Application Launcher.

- 1 On the user's workstation, right-click the Application object, then click *Uninstall*.

When Application Launcher uninstalls an application, it removes all application files and settings from the workstation. However, if the Application object is still associated with the user, the Application object's icon remains on the workstation. This enables the user to reinstall the application at a later time.

43.5 Uninstalling Applications from Terminal Servers

When Application Launcher distributes an application to a workstation, it creates a NAL cache directory (typically, `c:\nalcache`) on the workstation. The NAL cache directory contains the information required to successfully uninstall the application.

However, when Application Launcher distributes an application to a terminal server, it does not create a NAL cache directory, which means that it does not have the information to uninstall the application from the terminal server. Therefore, you cannot use Application Launcher to uninstall an application that it has installed to a terminal server. If you no longer want the application on the terminal server, you must manually uninstall it.

Novell® Application Launcher™ can report on the success or failure of the following application events: launching, distributing, filtering, uninstalling, caching, and terminating.

Application Launcher can write events to the Sybase ODBC-compatible database or to a text log file, send them as SNMP traps to a management console, or send them as XML data to a Web URL for processing. Because event reporting is established on a per-application basis, you can use one reporting method for one application and a different reporting method for another. Or, you can use all four methods for the same application.

The following sections provide information about setting up each type of event reporting and configuring Application objects to use one or more reporting methods:

- [Section 44.1, “Setting Up Database Reporting,” on page 431](#)
- [Section 44.2, “Setting Up SNMP Trap Reporting,” on page 438](#)
- [Section 44.3, “Setting Up Log File Reporting,” on page 441](#)
- [Section 44.4, “Setting Up XML Reporting,” on page 442](#)
- [Section 44.5, “Configuring Applications to Use Reporting,” on page 448](#)
- [Section 44.6, “Generating Reports from a Database,” on page 451](#)
- [Section 44.7, “Understanding Log File Reports,” on page 454](#)
- [Section 44.8, “Enabling Windows Installer Verbose Logging,” on page 457](#)

NOTE: The reporting described in these sections applies only to applications launched by Application Launcher (in other words, applications that have Application objects). Application Launcher can also report on applications that it does not launch. These applications are referred to as rogue processes. For more information about setting up reporting for rogue processes, see [Chapter 41, “Controlling Rogue Processes,” on page 415](#).

For MSI applications, you can also turn on verbose logging so that the Windows Installer outputs information to a log file on the user's workstation. The following section provides information:

[Section 44.8, “Enabling Windows Installer Verbose Logging,” on page 457](#)

44.1 Setting Up Database Reporting

To set up reporting to the Sybase ODBC-compatible database, you need to complete the following tasks:

- [Section 44.1.1, “Installing the Sybase Database,” on page 432](#)
- [Section 44.1.2, “Installing ODBC Drivers to Workstations,” on page 432](#)
- [Section 44.1.3, “Creating a ZENworks Database Object,” on page 432](#)
- [Section 44.1.4, “Configuring the Database's ODBC Information,” on page 434](#)
- [Section 44.1.5, “Granting ODBC Property Rights to Users,” on page 435](#)
- [Section 44.1.6, “Enabling the ZENworks Database Policy,” on page 435](#)

- [Section 44.1.7, “Configuring Application Objects to Use Database Reporting,” on page 438](#)

44.1.1 Installing the Sybase Database

The Sybase database included on the *Novell ZENworks 7 Desktop Management* CD is the only supported database for direct ODBC reporting in ZENworks Application Management. For information about installing the Sybase database, see [“Installing the ZENworks Desktop Management Server”](#) in the *Novell ZENworks 7 Desktop Management Installation Guide*.

Sybase is also used for the Workstation Inventory database. If you plan to use a database for Application Management reports and you also plan to use Workstation Inventory, you can use the same database installation for both purposes. Each component creates its own database file. Application Management creates a `nal.db` database file and Workstation Inventory creates a `mgmt.db` database file.

Because the main requirement for Application Management reporting is that the database be at the same site as the users, you should follow the instructions provided for Workstation Inventory to deploy your databases, and then choose one or more databases to use for Application Management reporting. For information about database deployment for Workstation Inventory, see [Chapter 73, “Setting Up Workstation Inventory,” on page 887](#).

44.1.2 Installing ODBC Drivers to Workstations

Application Launcher uses an ODBC driver to write application event information to the database. You need to ensure that the correct ODBC driver for the Sybase database is installed on each workstation for which you want to record event information.

The correct ODBC driver for the Sybase database (`dbodbc7.dll`) is installed by default. However, on Windows 98, you might need to install two additional DLLs (`odbc32.dll` and `odbcint.dll`) that are not installed during a Windows minimal installation. Download the files from Microsoft's Web site or another file download site. To install these files, copy to the Windows System directory (for example, `c:\windows\system`). You can also use an Application object to distribute them to the appropriate workstation. You do not need to do this on Windows 2000/XP. The files are already present.

44.1.3 Creating a ZENworks Database Object

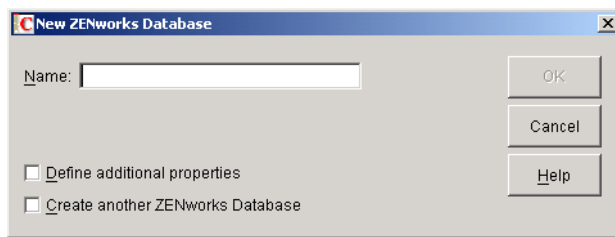
If you are using the Sybase database that comes with ZENworks® and have already installed it, the installation program creates a Database object (Desktop Management Database_*servername*) in eDirectory. You can skip to the next section, [“Configuring the Database's ODBC Information” on page 434](#).

If you are using another database, you must create a ZENworks Database object in eDirectory to represent the database.

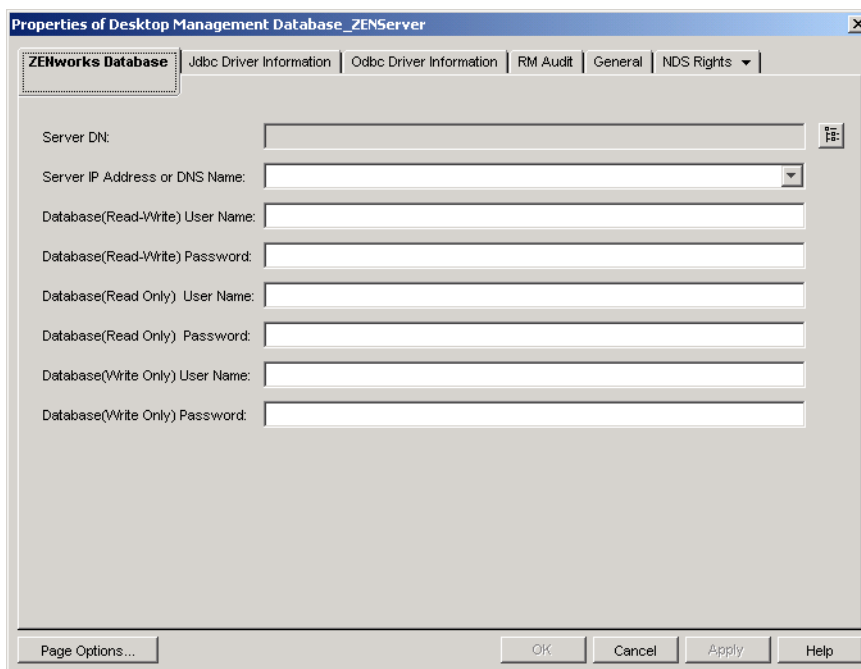
To create a ZENworks Database object:

- 1 In ConsoleOne®, right-click the container where you want to create the object, click *New*, then click *Object* to display the New Object dialog box.

- 2 Select *ZENworks database*, then click *OK* to display the New ZENworks Database dialog box.

A dialog box titled "New ZENworks Database" with a close button (X) in the top right corner. It contains a "Name:" label followed by a text input field. Below the input field are three buttons: "OK", "Cancel", and "Help". At the bottom left, there are two checkboxes: "Define additional properties" and "Create another ZENworks Database".

- 3 In the Name box, type a name for the database, such as Desktop Management Database_ZENServer.
- 4 Select the *Define additional properties* check box, then click *OK* to display the ZENworks Database property page.

A dialog box titled "Properties of Desktop Management Database_ZENServer" with a close button (X) in the top right corner. It has a tabbed interface with tabs: "ZENworks Database", "Jdbc Driver Information", "Odbc Driver Information", "RM Audit", "General", and "NDS Rights". The "ZENworks Database" tab is selected. It contains several input fields: "Server DN:" with a browse button, "Server IP Address or DNS Name:" with a dropdown arrow, "Database(Read-Write) User Name:", "Database(Read-Write) Password:", "Database(Read Only) User Name:", "Database(Read Only) Password:", "Database(Write Only) User Name:", and "Database(Write Only) Password:". At the bottom left is a "Page Options..." button, and at the bottom right are "OK", "Cancel", "Apply", and "Help" buttons.

- 5 In the *Server DN* field, browse for and select the Server object for the server where the database is physically installed and running.
- 6 Fill in the name and password fields for the Read-write, Read only, and Write only users:

Database (read-write) user name: Specify a username to provide both read and write access to the database. If you are using a Sybase database created by the Desktop Management Server installation program, the user name is MW_DBA.

Database (read-write) password: Specify a password for the Read-Write user. If you are using a Sybase database created by the Desktop Management Server installation program, the password is novell.

Database (read only) user name: Specify a username to provide only read access to the database. If you are using a Sybase database created by the Desktop Management Server installation program, the user name is MW_READER.

Database (read only) password: Specify a password for the Read Only user. If you are using a Sybase database created by the Desktop Management Server installation program, the password is novell.

Database (write only) user name: Specify a username to provide only write access to the database. If you are using a Sybase database created by the Desktop Management Server installation program, the user name is MW_UPDATER.

Database (write only) password: Specify a password for the Write Only user. If you are using a Sybase database created by the Desktop Management Server installation program, the password is novell.

- 7 Click *OK* to save the information.

44.1.4 Configuring the Database's ODBC Information

Application Launcher uses an ODBC driver to write event information to the database. You need to configure the database object with the ODBC driver information that Application Launcher needs.

To provide the ODBC information:

- 1 Right-click the database object, then click *Properties*.
- 2 Click the *ODBC Driver Information* tab.

The screenshot shows a Windows-style dialog box titled "Properties of ZfDAppManReports". It has several tabs: "ZENworks Database", "Jdbc Driver Information", "Odbc Driver Information" (which is selected and highlighted), "RM Audit", "General", "NDS Rights", and "Other...". Below the tabs, there are three text input fields: "Driver File Name:", "Data Source Name:", and "Connection Parameters:". At the bottom of the dialog, there are four buttons: "Page Options...", "OK", "Cancel", and "Apply".

- 3 Fill in the following fields:

Driver file name: Specify the name of the workstation ODBC driver file that Application Launcher will use to access the database. For Sybase, you can leave the field empty, in which case Application Launcher automatically detects the installed driver.

Data source name: Enter NAL Reporting.

Connection parameters: Specify the appropriate commands to connect to the database. For Sybase, these commands are:

```
CommLinks=TCPIP{Host=IPAddress:2638};AutoStop=Yes;Integrated=No;DB
N=NAL;ENG=IPAddress
```

where *IPAddress* is the actual IP address of the server where the database resides.

- 4 Click *OK* to save the ODBC driver information.

44.1.5 Granting ODBC Property Rights to Users

You need to grant users Read and Compare rights to the ODBC properties you defined for the database object in the previous section. This allows Application Launcher to retrieve the ODBC information it needs to access the database.

To grant rights:

- 1 Right-click the ZENworks Database object, then click *Trustees of this object*.
- 2 Click *Add trustee*.
- 3 Select *[PUBLIC]*, then click *OK* to add *[PUBLIC]* to the list of trustees.

Adding *[PUBLIC]* as a trustee gives every user Read and Compare rights to all of the database object's properties, including the various user names and passwords that can be used to access the database. To avoid this, you need to limit the *[PUBLIC]* access to the three ODBC properties.

- 4 In the Property list, select *[All Attribute Rights]*, then click *Delete property* to remove it from the list.
- 5 Click *Add property* to display the Add Property dialog box, select *zendbODBCConnectionParameters*, then click *OK* to add it to the Property list.

The default rights, Read and Compare, are sufficient. You do not need to change these rights.

- 6 Repeat **Step 5** to add the following properties (keep the default rights: Read and Compare):

```
zendbODBCDataSourceName
zendbODBCDriverFileName
Host Server
Network Address
zendbUser
zendbPassword
```

- 7 Click *OK*, then click *OK* again to save the changes.

44.1.6 Enabling the ZENworks Database Policy

Before Application Launcher can use the database, you need to:

- In ConsoleOne, activate a Database policy in a Service Location Package. The Database policy simply points to the location of the ZENworks database you are using. A Service Location Package can have only one Database policy, and each Database policy can point to only one database. If you haven't created a Service Location Package, or if your current packages' Database policies are being used for other databases, you need to create a new Service Location Package. Instructions are provided in the steps below.

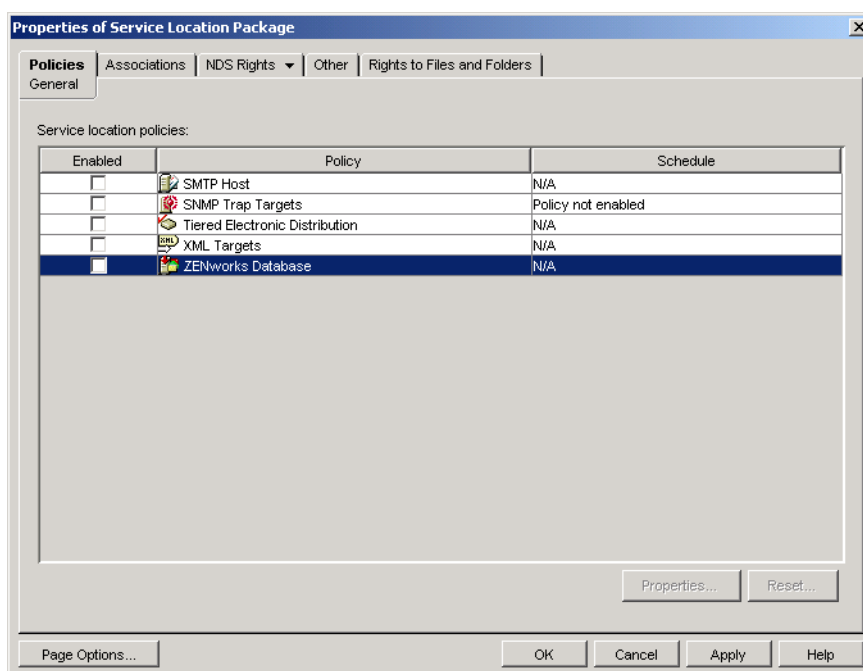
- Associate the Service Location Package with the containers where the users or workstations reside whose reports you want sent to the database. This association is how Application Launcher knows which database to use when reporting events for a user or workstation.

To activate a ZENworks Database policy and associate containers with it:

- 1 In ConsoleOne[®], right-click the Service Location Package you want to use, then click *Properties*.

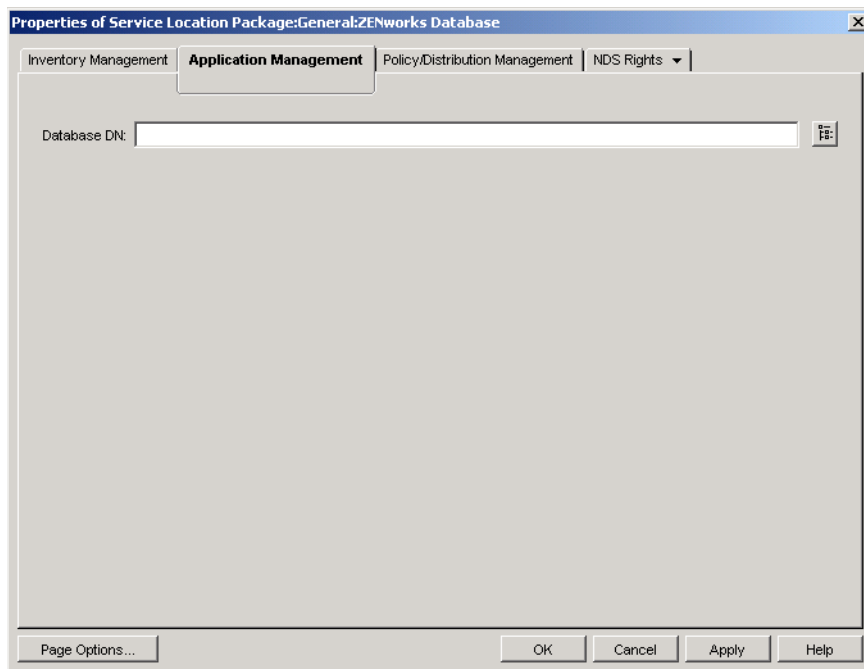
or

If you do not have a Service Location Package, right-click the container where you want to create one, click *New*, then click *Policy Package*. Follow the instructions provided in the Policy Package Wizard to create a Service Location Package.

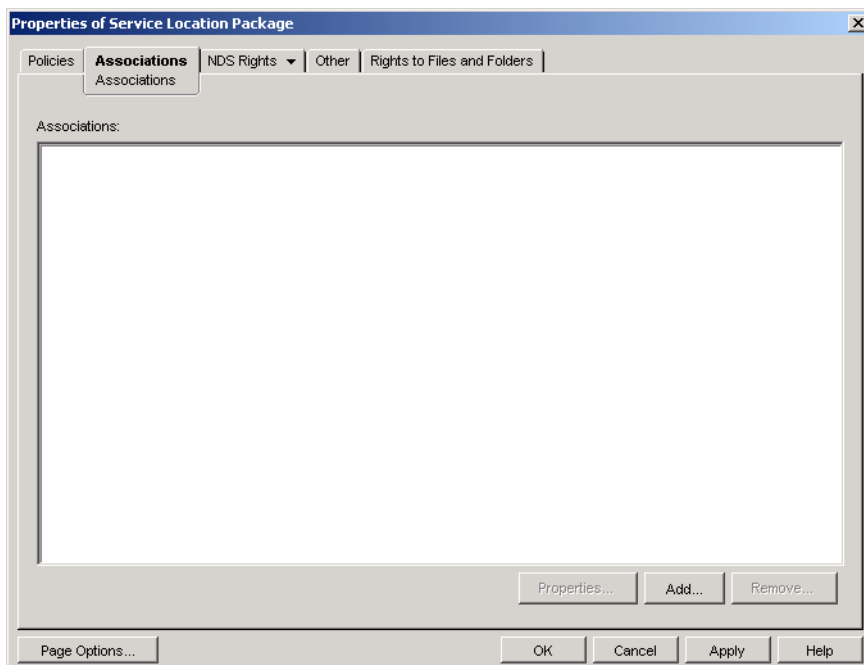


- 2 On the General page, select the check box in the *Enabled* column to enable the ZENworks Database Policy.

- 3 Select the *ZENworks Database Policy* in the list, click *Properties* to display the ZENworks Database properties page, then click the *Application Management* tab to display the Application Management page.



- 4 In the *Database DN* field, browse for and select the database object you want to use for application event reporting. This should be the same object you configured in [“Configuring the Database's ODBC Information”](#) on page 434.
- 5 Click *OK* to return to the General page.
- 6 Click *Associations* to display the Associations page.



You use this page to associate the Service Location Package with the containers where the users or workstations reside whose reports you want sent to the database. If a parent container includes several containers where User and Workstation objects reside, you can select the parent container rather than each individual container.

- 7 Click *Add*, browse for and select the container you want to add, then click *OK* to add it to the list.
- 8 Repeat **Step 7** to add additional containers.
- 9 When you've finished adding containers, click *OK* to save the information.

44.1.7 Configuring Application Objects to Use Database Reporting

After you've set up the database you will use for reporting, you can start configuring the Application objects for which you want events reported. Because event reporting is configured on a per-application basis, you can choose which applications you want to collect event reports for and which ones you don't.

For detailed instructions about configuring an application to use database reporting, SNMP trap reporting, or log file reporting, see [Section 44.5, “Configuring Applications to Use Reporting,” on page 448](#).

44.2 Setting Up SNMP Trap Reporting

If you have a management console to collect SNMP traps, you can have Application Launcher send SNMP traps to the management console. ZENworks Server Management includes a management console you can use to collect SNMP traps. For information, see “[Management and Monitoring Services](#)” in the *Novell ZENworks 7 Server Management Administration Guide*.

To set up SNMP trap reporting, you need to complete the following tasks:

- [Section 44.2.1, “Enabling Firewall Access,” on page 438](#)
- [Section 44.2.2, “Enabling the SNMP Trap Targets Policy,” on page 438](#)
- [Section 44.2.3, “Configuring Application Objects to Use SNMP Trap Reporting,” on page 441](#)

44.2.1 Enabling Firewall Access

For SNMP traps to be sent from workstations to your management console, you need to ensure that there are no firewalls between the workstations and the management console that filter UDP or TCP on port 161. This includes both personal firewalls on the user workstations and network firewalls.

44.2.2 Enabling the SNMP Trap Targets Policy

Before Application Management can use SNMP traps for event reporting, you need to:

- In ConsoleOne, activate an SNMP Trap Targets policy in a Service Location Package. The SNMP Trap Targets policy simply points to the IP address (or addresses) of the management console that displays the traps. A Service Location Package can have only one SNMP Trap Targets policy. If you haven't created a Service Location Package, or if your current packages'

SNMP Trap Targets policies are being used for other databases, you need to create a new Service Location Package. Instructions are provided in the steps below.

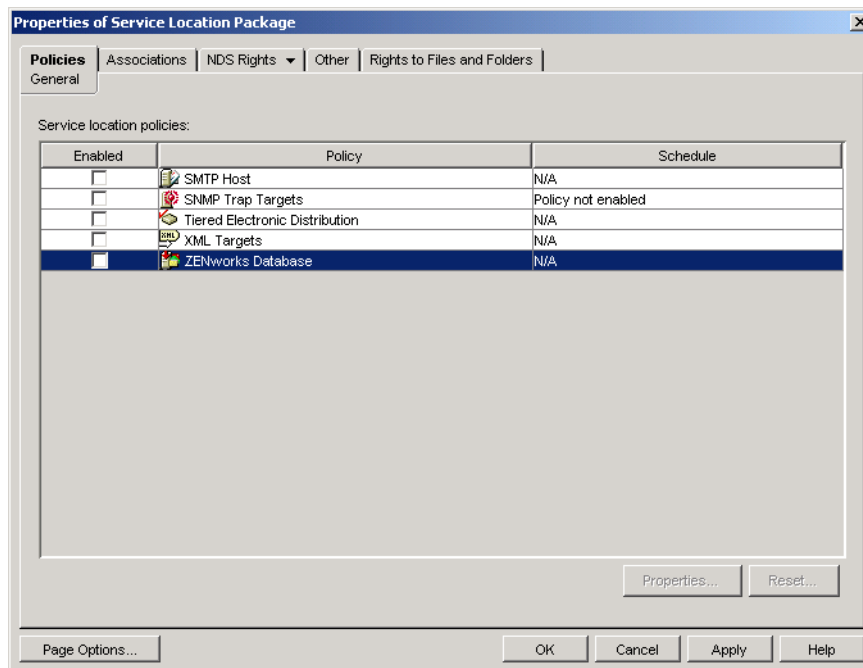
- Associate the Service Location Package with the containers where the users or workstations reside that you want the SNMP Trap Targets policy applied to. This association is how Application Launcher knows which SNMP trap target to use when reporting events for the users or workstations.

To activate an SNMP Trap Targets policy and associate it with containers:

- 1 In ConsoleOne, right-click the Service Location Package you want to use, then click *Properties*.

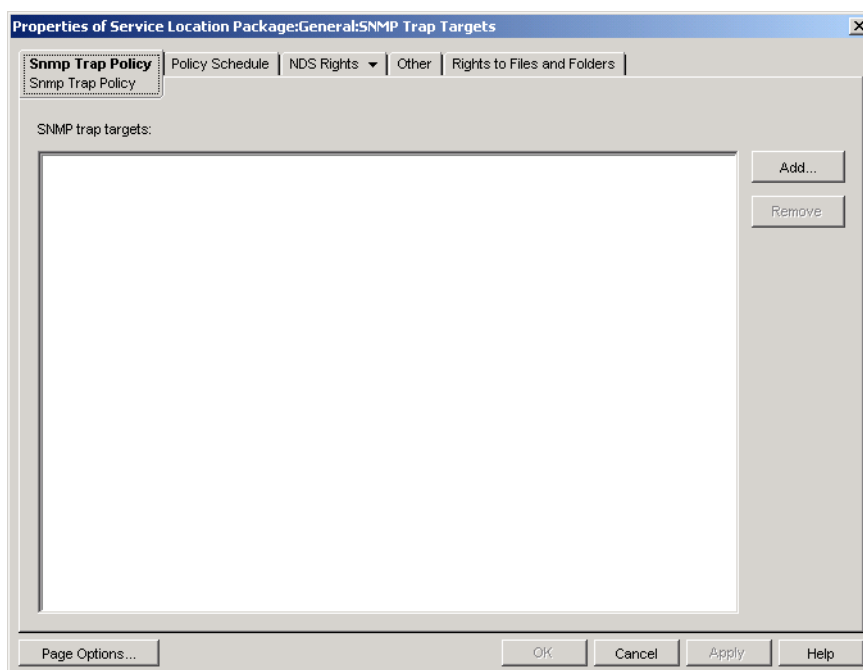
or

If you do not have a Service Location Package, right-click the container where you want to create one, click *New*, then click *Policy package*. Follow the instructions provided in the Policy Package Wizard to create a Service Location Package.

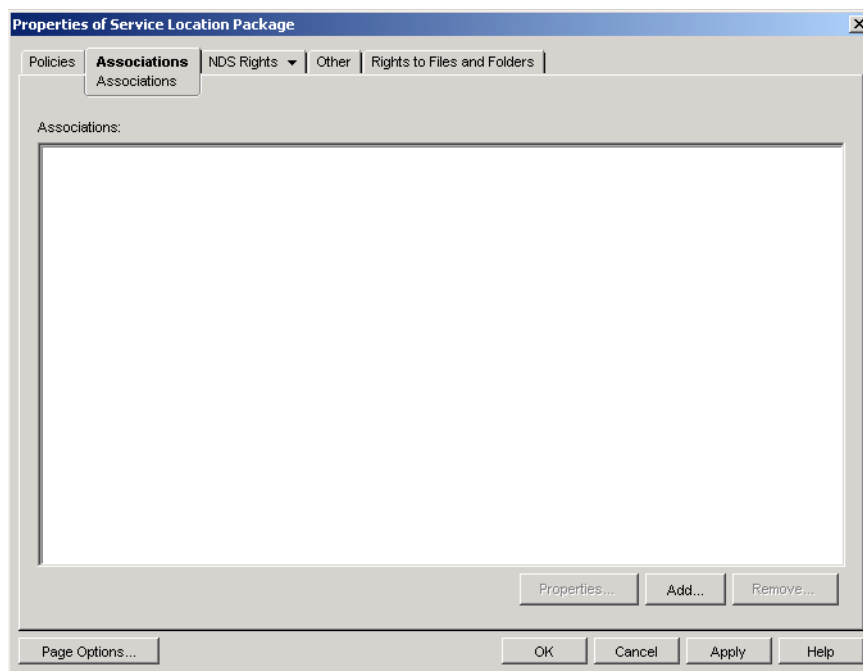


- 2 On the General page, select the box in the *Enabled* column to enable the SNMP Trap Targets Policy.

- 3 Select the policy in the list, then click *Properties* to display the SNMP Trap Targets list.



- 4 Click *Add* to display the SNMP Target dialog box, specify the IP address of the workstation or server where the management console is running, then click *OK* to add the IP address to the list.
- 5 Repeat **Step 4** to add additional targets.
- 6 When you've finished adding targets, click *OK* to return to the General page.
- 7 Click *Associations* to display the Associations page.



You use this page to associate the Service Location Package with the containers where the users or workstations reside that you want the SNMP Trap Targets policy applied to. If a parent container includes several containers where User and Workstation objects reside, you can select the parent container rather than each individual container.

- 8 Click *Add*, browse for and select the container you want to add, then click *OK* to add it to the list.
- 9 Repeat **Step 8** to add additional containers.
- 10 When you've finished adding containers, click *OK* to save the information.

When ZENworks Workstation Manager enforces the SNMP Trap Targets policy on a user's workstation, it adds the SNMP trap targets as values on the following registry key:

```
HKCU\Software\NetWare\NAL\1.0\Reporting\tree_name\TrapTargets\User
```

If events are not being sent to the SNMP management console, you should verify that the trap targets have been added to the registry.

44.2.3 Configuring Application Objects to Use SNMP Trap Reporting

After you've enabled the SNMP Trap Targets policy and have your management console running, you can start configuring Application objects to use SNMP trap reporting. Because event reporting is configured on a per-application basis, you can choose which applications you want to collect event reports for and which ones you don't.

For detailed instructions about configuring an application to use SNMP trap reporting, database reporting, or log file reporting, see [Section 44.5, "Configuring Applications to Use Reporting," on page 448](#).

44.3 Setting Up Log File Reporting

You can have Application Launcher record events to a log file. This can be an individual log file located on the user's workstation or a common log file on a network server. When using a common log file, users must be given Read and Write rights to the log file, but Application Launcher automatically authenticates them to the log file location.

To set up log file reporting, you need to complete the following tasks:

- [Section 44.3.1, "Setting Up a Common Log File Location," on page 441](#)
- [Section 44.3.2, "Configuring Application Objects to Use Log File Reporting," on page 442](#)

44.3.1 Setting Up a Common Log File Location

With log file reporting, you have two options. You can have Application Launcher log events for each individual user to a file on the user's local drive, or you can have Application Launcher log events for all users to a file in a common network location.

If you want Application Launcher to log events to a file in a common network location, you need to establish the network directory and provide users with Read and Write rights to files in the directory.

Because log file names are established on a per-application basis, you can have individual log files for each application (by specifying a different log file name for each Application object) or one log file for all applications (by specifying the same log file name for all Application objects). You cannot have log files on a per-user basis, unless you have Application Launcher save the files to the users' local drives.

44.3.2 Configuring Application Objects to Use Log File Reporting

After you've set up a common log file location (if you plan to use a common log file), you can start configuring Application objects to use log file reporting. Because event reporting is configured on a per-application basis, you can choose which applications you want to collect event reports for and which ones you don't.

For detailed instructions about configuring an application to use log file reporting, database reporting, or SNMP trap reporting, see [Section 44.5, “Configuring Applications to Use Reporting,” on page 448](#).

44.4 Setting Up XML Reporting

Application Launcher can use the HTTP or HTTPS protocol to send event information as XML data to the Desktop Management Application Reporting servlet (`zfdamrServlet`). The servlet processes the messages and adds them to a database compliant with JDBC, such as the Sybase database included with ZENworks.

To set up XML reporting, you need to complete the following tasks:

- [Section 44.4.1, “Meeting the Reporting Servlet Requirements,” on page 442](#)
- [Section 44.4.2, “Installing the Reporting Servlet on Linux,” on page 443](#)
- [Section 44.4.3, “Installing the Reporting Servlet on NetWare and Windows,” on page 443](#)
- [Section 44.4.4, “Configuring the Reporting Servlet to be Used with an Apache Web Server,” on page 444](#)
- [Section 44.4.5, “Configuring the Reporting Servlet to Write to the Database,” on page 444](#)
- [Section 44.4.6, “Enabling the XML Targets Policy,” on page 445](#)
- [Section 44.4.7, “Configuring Application Objects to Use XML Reporting,” on page 448](#)

44.4.1 Meeting the Reporting Servlet Requirements

The Reporting servlet requires one of the following server environments. The version numbers listed are minimum requirements.

Table 44-1 *Reporting Servlet Requirements*

Server	Java Servlet Engine	JVM
NetWare® 6.5 (Support Pack 1 or later)	Tomcat 4.1x	Novell JVM* for NetWare 1.4.2
NetWare 6 (Support Pack 2 or later) ¹	Tomcat 3.3a	Novell JVM for NetWare 1.3.1

Server	Java Servlet Engine	JVM
Windows Server 2003 (with latest service pack)	Tomcat 3.3a	Sun JDK* 1.3.1_01
Windows 2000 (with latest service pack)	Tomcat 3.3a	Sun JDK 1.3.1_01
SUSE Linux Enterprise Server (SLES) 9 SP1	Tomcat 4.1x	JVM 1.4.2 ²
Novell Open Enterprise Server (Linux) 1.0	Tomcat 4.1x	JVM 1.4.2 ³

¹ Support Pack 2 or later is required. Without Support Pack 2 or later, the Reporting servlet causes server utilization to jump to 100% and remain there.

² The JVM is installed on the SLES 9 SP1 server by the ZENworks 7 Middle Tier Server installation program. If you want to use a SLES 9 SP1 server other than the Middle Tier Server, you will need to install the correct Tomcat and JVM versions manually.

³ The JVM ships with and is installed by the Novell Open Enterprise Server installation program.

For information about installing Tomcat on NetWare 6.5, see the [NetWare 6.5 documentation \(http://www.novell.com/documentation/nw65/index.html\)](http://www.novell.com/documentation/nw65/index.html).

For information about installing Tomcat on NetWare 6, see the [NetWare 6 documentation \(http://www.novell.com/documentation/lg/nw6p\)](http://www.novell.com/documentation/lg/nw6p).

For information about installing Tomcat on Windows 2000, see the [Apache Tomcat Web site \(http://jakarta.apache.org/tomcat\)](http://jakarta.apache.org/tomcat).

OES Linux ship with Tomcat installed.

44.4.2 Installing the Reporting Servlet on Linux

- 1 Make sure the server environment where you are installing the Reporting servlet meets the software requirements listed in the previous section, [Meeting the Reporting Servlet Requirements](#).
- 2 Copy the `zfdamrServlet.war` file from the Desktop Management server's `/opt/novell/zenworks/zdm/winutils/nalreporting` directory to `/var/opt/novell/tomcat4/webapps`.
- 3 Restart Tomcat to expand the `zfdamrServlet.war` file. To restart Tomcat on Linux, enter `/usr/share/tomcat/bin/startup.sh` at the command line.
or
If you don't want to restart Tomcat, use the tools provided with Tomcat to expand the file.

44.4.3 Installing the Reporting Servlet on NetWare and Windows

- 1 Make sure the server environment where you are installing the Reporting servlet meets the software requirements listed in the previous section, [Meeting the Reporting Servlet Requirements](#).
- 2 Copy the `zfdamrServlet.war` file from the Desktop Management server's `sys:\public\reporting\canned\nal` reports directory to `sys:\tomcat\4\webapps`.

- 3 Restart Tomcat to expand the `zfdamrServlet.war` file.

or

If you don't want to restart Tomcat, use the tools provided with Tomcat to expand the file.

44.4.4 Configuring the Reporting Servlet to be Used with an Apache Web Server

This section applies only if you are using an Apache Web server.

- 1 Open the `sys:/apache2/conf/httpd.conf` file.
- 2 Add the following line to the bottom of the file:

```
Include sys:/public/Reporting/canned/Nal Reports/  
zfdamrServlet.conf
```
- 3 Save the `httpd.conf` file.
- 4 Restart the Apache Web server.

44.4.5 Configuring the Reporting Servlet to Write to the Database

Before completing the steps in this section, you need to ensure that the database to which the Reporting servlet will write is set up and configured properly.

The Reporting servlet needs to know information about the database to which it will write the reporting events. To provide this information:

- 1 Open the `web.xml` file. The file is located in the Tomcat `webapps\zfdamrservlet\web-inf` directory
- 2 If you are using a Sybase database, locate the `dbip` parameter, then change the parameter value to the IP address of the database server. The IP address is the only parameter you need to modify for a Sybase database.

or

If you are using a database other than Sybase, modify the parameters, described below, as required by your database. If you are using a Microsoft SQL database, follow the directions in [TID 10094306 \(http://support.novell.com/cgi-bin/search/searchtid.cgi?/10094306.htm\)](http://support.novell.com/cgi-bin/search/searchtid.cgi?/10094306.htm).

dbuser: Specify a user name that has Write access to the database. Read access is not required. The preconfigured user name (MW_DBA) is the default Read-Write user name for a Sybase database created by the Desktop Management Server installation program. If you are using a ZENworks Sybase database and have not changed the default Read-Write username, you do not need to modify this parameter.

dbpasswd: Specify the password for the user name specified in the `dbuser` parameter. The preconfigured password (novell) is the default Read-Write user's password for a Sybase database created by the Desktop Management Server installation program. If you are using a ZENworks Sybase database and have not changed the default Read-Write user's password, you do not need to modify this parameter.

dbip: Specify the IP address of the server running the database.

dbport: Specify the port where the database is listening. The preconfigured port (2638) is the default NetWare server port for a Sybase database created by the Desktop Management Server installation program. If you are using a ZENworks Sybase database installed on NetWare and have not changed the default port, you do not need to modify this parameter.

dbprotocol: Specify the protocol to use when accessing the database. For Sybase, this is jdbc: (the preconfigured value).

dbsubprotocol: Specify the subprotocol to use when accessing the database. For Sybase, this is sybase: (the preconfigured value).

dbsubname: Specify the subname to use when accessing the database. For Sybase, this is Tds: (the preconfigured value).

dbdriver: Specify the full class of the driver to use when accessing the database. The driver must support the protocol listed in the dbprotocol parameter. For Sybase, this is `com.sybase.jdbc2.jdbc.SybDriver` (the preconfigured value).

3 Save the file.

4 Restart Tomcat.

44.4.6 Enabling the XML Targets Policy

Before Application Launcher can report application events through XML, you need to:

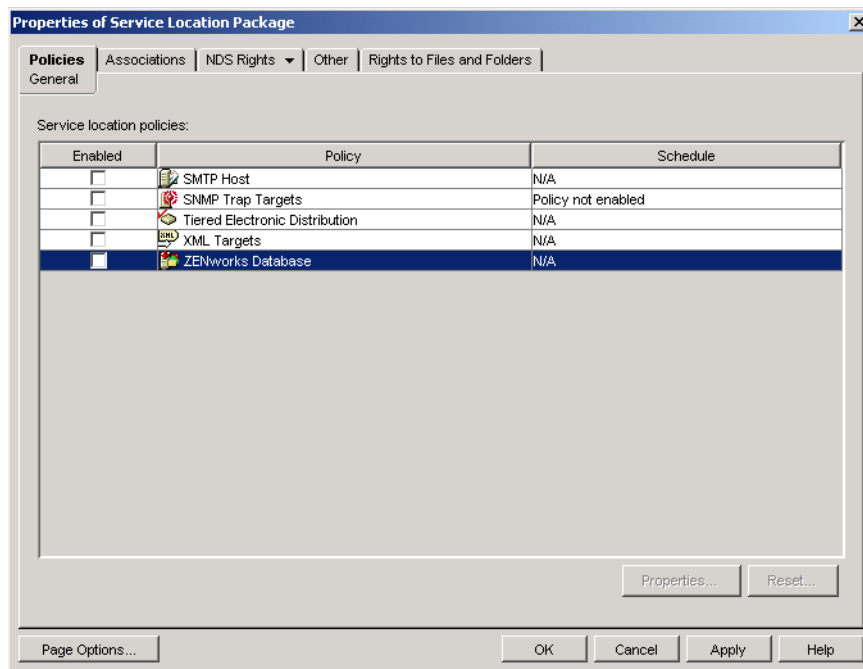
- In ConsoleOne, activate an XML Targets policy in a Service Location Package. The XML Targets policy identifies the Web locations (URLs) where you want the XML data sent. If you are using the Application Management Reporting servlet, this is the URL of that servlet. A Service Location Package can have only one XML Targets policy. If you haven't created a Service Location Package, or if your current packages' XML Targets policies are being used to specify other locations, you need to create a new Service Location Package. Instructions are provided in the steps below.
- Associate the Service Location Package with the containers where the users or workstations reside whose reports you want sent to the Web URL.

To activate an XML Targets policy and associate containers with it:

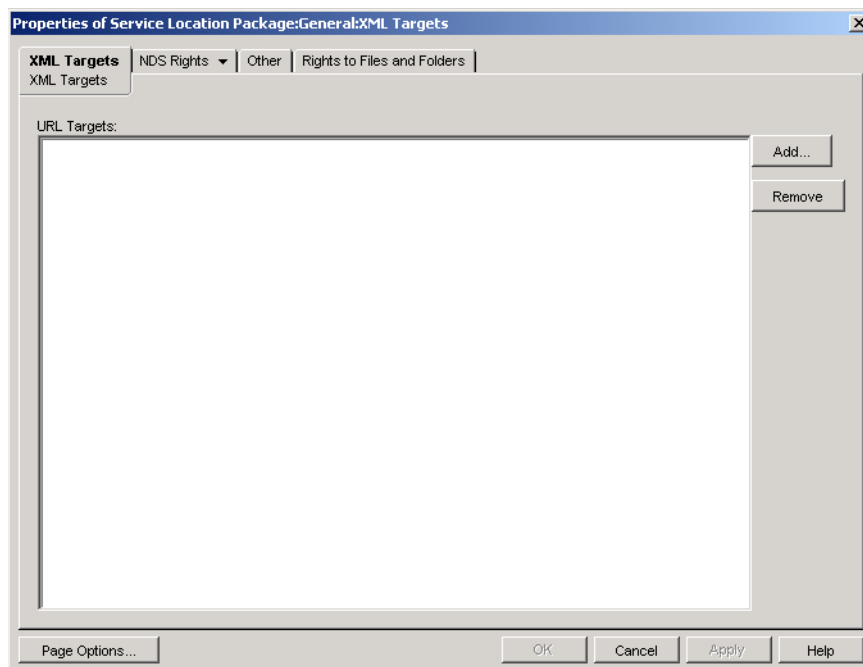
1 In ConsoleOne, right-click the Service Location Package you want to use, then click *Properties*.

or

If you do not have a Service Location Package, right-click the container where you want to create one, click *New*, then click *Policy package*. Follow the instructions provided in the Policy Package Wizard to create a Service Location Package.



- 2 On the General page, select the box in the *Enabled* column to enable the XML Targets policy.
- 3 Select the *XML Targets* policy in the list, then click *Properties* to display the XML Targets properties page.



- 4 Click *Add* to display the XML URL dialog box, enter the URL where you want the XML data sent, then click *OK* to add the URL to the list.

The URL needs to include the port number, which by default is port 8080 on Windows or on NetWare, and 8180 on OES Linux and SLES. This port is the default Tomcat port in these environments, and is necessary for the Service Location Policy for XML reporting to find the `zfdamrServlet` running on Tomcat.

The URL for the Reporting servlet on Windows or NetWare would be:

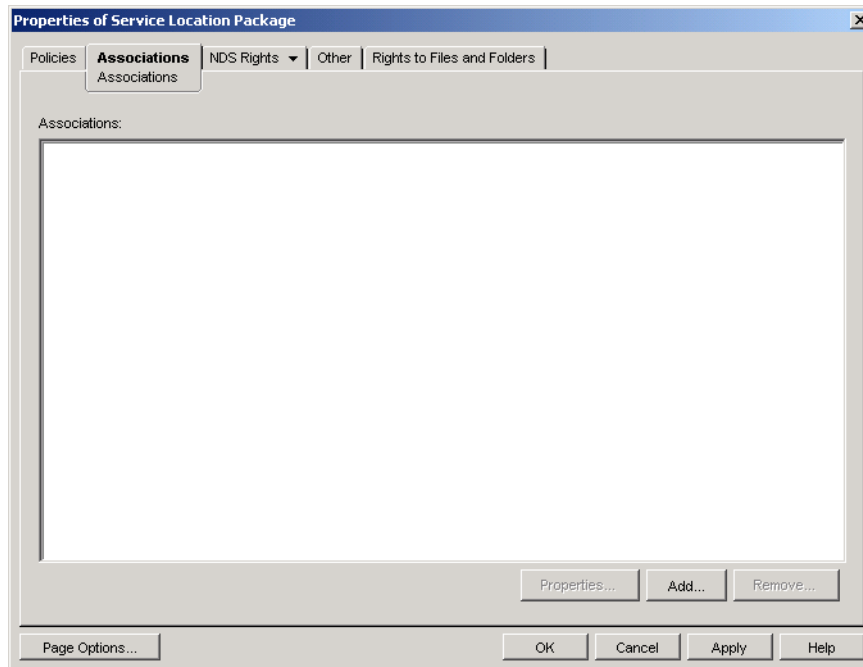
`http://ip_address:8080/zfdamrServlet/run`

and the URL for the Reporting servlet on Linux (OES Linux or SLES) would be:

`http://ip_address:8180/zfdamrServlet/run`

where *ip_address* is the IP address or DNS host name of the server where the Reporting servlet is running.

- 5 Repeat **Step 4** to add additional URLs.
- 6 When you are finished adding URLs, click *OK* to return to the General page.
- 7 Click *Associations* to display the Associations page.



You use this page to associate the Service Location Package with the containers where the users or workstations reside whose XML reports you want sent to the Web URL. If a parent container includes several containers where User and Workstation objects reside, you can select the parent container rather than each individual container.

- 8 Click *Add*, browse for and select the container you want to add, then click *OK* to add it to the list.
- 9 Repeat **Step 8** to add additional containers.
- 10 When you've finished adding containers, click *OK* to save the information.

44.4.7 Configuring Application Objects to Use XML Reporting

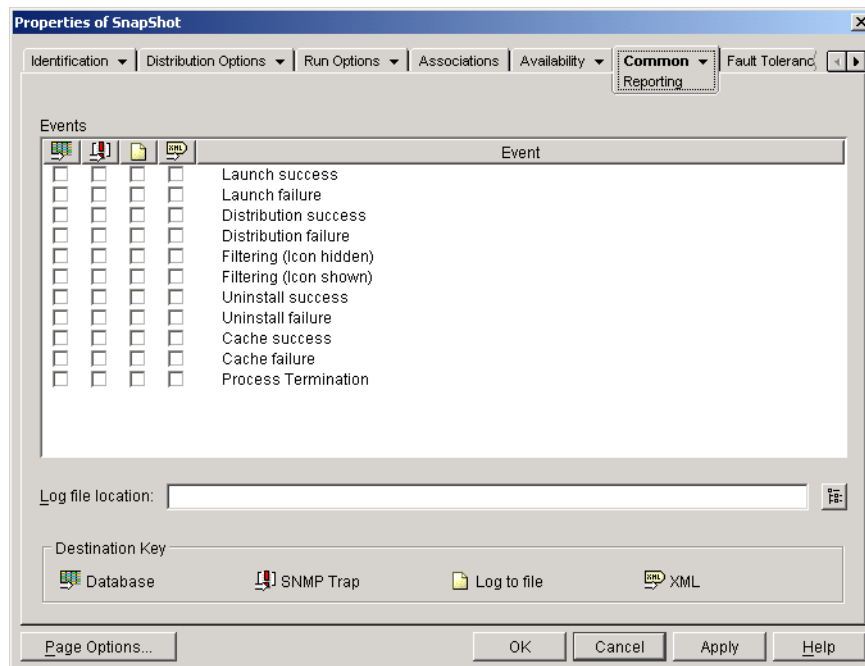
After you've enabled the XML Targets policy, you can start configuring Application objects to use XML reporting. Because event reporting is configured on a per-application basis, you can choose which applications you want to collect event reports for and which ones you don't.

For detailed instructions about configuring an application to use XML reporting, see [Section 44.5](#), “Configuring Applications to Use Reporting,” on page 448.

44.5 Configuring Applications to Use Reporting

Application Launcher must know which method of reporting (database, SNMP trap, or log file) to use for an application and which events to report for the application. You provide this information through the Application object's Reporting page (Common tab).

- 1 In ConsoleOne, right-click the Application object for which you want to configure reporting, then click *Properties*.
- 2 Click the *Common* tab > *Reporting* to display the Reporting page.







- 3 Fill in the following fields:

Events: Select the events (launch, distribution, filtering, uninstall, cache, and process termination) that you want reported and the destination (database, SNMP trap, log file, or XML) where you want the events sent. If necessary, you can send events to multiple destinations (for example, both a database and a log file). Events and destinations are described in the following tables:

Event	Description
Launch Success	Occurs when a user double-clicks the Application object and Application Launcher successfully starts the application.

Event	Description
Launch Failure	Occurs when a user double-clicks the Application object and Application Launcher cannot start the application.
Distribution Success	Occurs when Application Launcher successfully modifies the workstation to support the application. Modifications include installation of files, changing of settings (registry, INI, etc.), creation of shortcuts, and so forth.
Distribution Failure	Occurs when Application Launcher cannot modify the workstation to support the application. Modifications include installation of files, changing of settings (registry, INI, etc.), creation of shortcuts, and so forth.
Uninstall Success	Occurs when Application Launcher successfully uninstalls the application from the workstation.
Uninstall Failure	Occurs when Application Launcher cannot uninstall the application from the workstation.
Cache Success	Occurs when Application Launcher successfully caches the application to the workstation.
Cache Failure	Occurs when Application Launcher cannot cache the application to the workstation.
Filter (Icon Hidden)	Occurs when Application Launcher cannot display an Application object on a workstation because the workstation does not meet one or more of the Application object's distribution rules (Application object > <i>Availability</i> tab > <i>Distribution Rules</i> page) and the <i>Always show icon</i> option (on the <i>Distribution Rules</i> page) is turned off. The Application object's icon is hidden, or not shown, on the workstation.
Filter (Icon Shown)	Occurs when Application Launcher can only display a disabled (dimmed) Application object on a workstation. This occurs because the workstation does not meet one or more of the distribution rules (Application object > <i>Availability</i> tab > <i>Distribution Rules</i> page) and the <i>Always show icon</i> option (on the <i>Distribution Rules</i> page) is turned on. Users can right-click the disabled icon and click <i>Details</i> to see what system requirements are not being met.
Process Termination	Occurs when a user or Application Launcher terminates the application.

Destination	Description
 Database	<p>Application Launcher can write events to any ODBC-compliant database (for example, the Sybase database included with ZENworks). To use a database, you must also:</p> <ul style="list-style-type: none"> • Create a ZENworks Database object to use for application event reporting. • If necessary, create a Service Location Package. Associate the Service Location Package with the containers where the users or workstations reside whose reports you want sent to the database. • Enable the ZENworks Database policy in the Service Location Package. • Associate the ZENworks Database policy with the ZENworks Database object. • Make sure users have the appropriate ODBC database driver installed and configured. • After you've set up database reporting, you can use one of the predefined reports to see information about specific application events. To access the reports, right-click the ZENworks Database object you created for application event reporting > click <i>Reporting</i>.
 SNMP Traps	<p>Application Launcher can send SNMP traps to any SNMP management console. To use SNMP traps, you must also enable an SNMP Trap Target policy in a Service Location Package. It might be necessary to first create the Service Location Package.</p> <ul style="list-style-type: none"> • Associate the Service Location Package with the containers where the users or workstations reside that you want the SNMP Trap Target policy applied to. • Add the SNMP Trap Targets (IP addresses) for the locations you want the traps sent. • Have a management console that displays the SNMP traps.
 Text Log File	<p>Application Launcher can write events to a text log file. You use the Log File Location field (described below) to specify the location of the log file.</p>
 XML	<p>Application Launcher can send events, as XML data, to a URL using the standard HTTP or HTTPS protocol. XML reporting is the recommended method if you want Application Launcher to report events for users located outside of your firewall.</p> <p>To use XML, you must also:</p> <ul style="list-style-type: none"> • Enable an XML URL policy in a Service Location Package. It might be necessary to first create the Service Location Package. • Associate the Service Location Package with the containers where the users or workstations reside whose reports you want sent as XML data. • Make sure you've set up the XML processing mechanism and data storage mechanism. For example, if you are using the Application Management Reporting servlet and the Sybase database, make sure that each one is set up and configured properly.

Log file location: If you selected a log file as the destination for any of the event reports, enter (or browse to and select) the location and name for the log file. You can specify a local drive or

a network drive. If you enter a location that does not exist, Application Launcher creates it. Do not use extended characters in the path; extended characters are not supported.

If you want Application Launcher to log events to a file in a common network location, you need to establish the network directory and provide users with Read and Write rights to files in the directory. Because log file names are established on a per-application basis, you can have individual log files for each application (by specifying a different log file name for each Application object) or one log file for all applications (by specifying the same log file name for all Application objects).

IMPORTANT: You should only use log file reporting if users have a network client, such as the Novell Client™ or Microsoft Client for Networks, that enables writing to a NetWare, Linux, or Windows server, or if you specify a local drive as the log file location.

- 4 Click *OK* to save the changes.

44.6 Generating Reports from a Database

You can use the predefined reports included with ZENworks Database Management to view information about the application events recorded by Application Launcher, or you can use your own database tools to create your own custom reports. The following sections provide information:

- [Section 44.6.1, “Predefined Reports,” on page 451](#)
- [Section 44.6.2, “Custom Reports,” on page 451](#)
- [Section 44.6.3, “Database Tables and Fields,” on page 452](#)

44.6.1 Predefined Reports

ZENworks Desktop Management includes predefined reports for successful application events and failed application events.

To generate a predefined report:

- 1 Right-click the Desktop Management Database object, then click *Reporting*.
- 2 In the *Available reports* list, expand the *ZENworks Application Launcher* category, then select the report you want.
- 3 Click *Run selected report*.

44.6.2 Custom Reports

Using your database tools of choice, you can create custom database reports to search for information not included in the predefined reports, or to generate different report formats. The following samples are SQL queries you can use to generate reports from your database tools if you are using the Sybase database included with ZENworks. Refer to [“Database Tables and Fields” on page 452](#) for additional information.

All Fields for an Event

The following queries return all information fields for a successful, failed, or rogue process management event stored in the database. Events are sorted by the order in which they were entered into the database.

```
SELECT * FROM T_SUCCESS
SELECT * FROM T_FAILURE
SELECT * FROM T_INFO
```

All Fields for an Event, Sorted on a Specific Field

To sort the list on a specific field, add ORDER BY *field_name*, as in the following examples:

```
SELECT * FROM T_SUCCESS ORDER BY zenWSTDN
SELECT * FROM T_FAILURE ORDER BY zenAppTDN
SELECT * FROM T_INFO ORDER BY zenUserTDN
```

The valid field names are listed in the table in [“Database Tables and Fields” on page 452](#)

All Fields for Specific Event Types

To include only a specific event type (launch, distribute, etc.) for an event (success, failure, etc.), add WHERE zenEventType=*event_type*, as in the following examples:

```
SELECT * FROM T_SUCCESS WHERE zenEventType="Launch Success"
SELECT * FROM T_FAILURE WHERE zenEventType="Launch Failure"
SELECT * FROM T_INFO WHERE zenEventType="Process Terminated"
```

The valid event types are listed in the table in [“Database Tables and Fields” on page 452](#)

Specific Fields for an Event

To include only specific fields, replace the * with a comma-delimited field list, as in the following example:

```
SELECT zenEventType, zenDateTime, zenUserTDN, zenAppTDN FROM T_SUCCESS
WHERE zenEventType="Cache Success" ORDER BY zenUserTDN
```

44.6.3 Database Tables and Fields

The database includes the following three tables:

- **T_Success:** Stores information about successful events.
- **T_Failure:** Stores information about failed events.
- **T_Info:** Stores information about rogue process management events. For information about rogue process management, see [Chapter 41, “Controlling Rogue Processes,” on page 415](#).

Each database table contains as many as 17 information fields. The following table lists the fields and the database tables that include the fields. The data type for all fields is varchar(256).

Table 44-2 Database Tables and Fields

Field	Tables	Description
zenEventType	T_Success T_Failure T_Info	<p>The event that occurred.</p> <ul style="list-style-type: none"> Successful event types (T_Success) are: <ul style="list-style-type: none"> Launch Success Distribute Success Uninstall Success Cache Success Process Terminated Failed event types (T_Failure) are: <ul style="list-style-type: none"> Launch Failed Distribute Failed Uninstall Failed Cache Failed Filter Hide Filter Show Rogue process management event types (T_Info) are: <ul style="list-style-type: none"> Process Terminated Process Ignored
zenDateTime	T_Success T_Failure T_Info	The date and time the event occurred.
zenUserTDN	T_Success T_Failure T_Info	The distinguished name and tree of the user for which the event occurred.
zenWSTDN	T_Success T_Failure T_Info	The distinguished name and tree of the workstation on which the event occurred. If the workstation has not been imported into eDirectory as a Workstation object, the field contains WORKSTATION NOT REGISTERED.
zenWSAddr	T_Success T_Failure T_Info	The IPX™ or IP address of the workstation on which the event occurred.
zenAppTDN	T_Success T_Failure T_Info	<p>The distinguished name and tree of the Application object for which the event occurred.</p> <p>Because rogue processes do not have an Application object, this field is always “ZEN Process Management” in the T_Info table.</p>
zenAppGUID	T_Success T_Failure T_Info	<p>The global unique identifier assigned to the Application object. The GUID is located on the Application object's Options page (Distribution Options tab).</p> <p>Because rogue processes do not have an Application object, this field is always empty in the T_Info table.</p>

Field	Tables	Description
zenAppVer	T_Success T_Failure T_Info	<p>The version number assigned to the Application object. Possible numbers range from 0 to 65535. The version number is located on the Application object's Options page (Distribution Options tab).</p> <p>Because rogue processes do not have an Application object, this field is always empty in the T_Info table.</p>
zenMajor	T_Success T_Failure T_Info	<p>For successful events (T_Success table), this field is always 0.</p> <p>For failed events (T_Failure table), this field lists the error code generated by Application Launcher.</p> <p>For rogue process events (T_Info table), this field is left blank.</p>
zenMinor	T_Success T_Failure T_Info	<p>For successful events (T_Success table), this field is always 0.</p> <p>For failed events (T_Failure table), this field lists additional error code information.</p> <p>For rogue process events (T_Info table), this field is left blank.</p>
zenEventString1	T_Failure T_Info	<p>For failed events (T_Failure table), this field might list additional information describing the reason for the failure.</p> <p>For rogue process events (T_Info table), this field lists the executable path for the rogue process.</p>
zenEventString2	T_Failure T_Info	<p>For failed events (T_Failure table), this field might list additional information describing the reason for the failure.</p> <p>For rogue process events (T_Info table), this field lists the original filename of the process.</p>
zenEventString3	T_Failure T_Info	<p>For failed events (T_Failure table), this field might list additional information describing the reason for the failure.</p> <p>For rogue process events (T_Info table), this field contains the process ID (PID).</p>
zenEventString4	T_Failure T_Info	<p>For failed events (T_Failure table), this field might list additional information describing the reason for the failure.</p> <p>For rogue process events (T_Info table), this field contains the parent process ID (parent PID).</p>
zenEventString5	T_Failure T_Info	<p>For failed events (T_Failure table), this field might list additional information describing the reason for the failure.</p> <p>For rogue process events, this field contains the event action, either "process ignored" or "process terminated successfully."</p>
zenAppFlags	T_Success T_Failure T_Info	<p>For successful events (T_Success table) and failed events (T_Failure table), this field lists the Application object bitmask.</p> <p>For rogue process events (T_Info table), this field is always 0.</p>

44.7 Understanding Log File Reports

The following is a log file entry for a single event. Each field in the entry is described below.

```
"Launch Failure","11","7/25/2002 9:27:52 AM",
"JSMITH.NOVELL.NOVELL_TREE",".WORKSTATION NOT
REGISTERED","137.65.45.25","NOTEPAD.APPS.NOVELL.NOVELL_TREE","3054A94E
-BBFF-4851-9D8E-58973623B728","2","Could not launch
NOTEPAD.APPS.NOVELL.NOVELL_TREE (using c:\winnt\notepa) (id=123)","The
filename, directory name, or volume label syntax is
incorrect.","c:\winnt\notepa","","","","","524288"
```

Table 44-3 Log File Fields and Descriptions

Field	Example	Description
Event Type	Launch Failure	<p>The event that occurred and whether it was successful or failed. Possible event types are:</p> <p>Launch Success Launch Failure Distribution Success Distribution Failure Filter Show Filter Hide Uninstall Success Uninstall Failure Cache Success Cache Failure Application Termination Process Ignored Process Terminated</p>
Event Type Code	11	<p>The code associated with the event. Possible codes are:</p> <p>10 - Launch Success 11 - Launch Failure 20 - Distribution Success 21 - Distribution Failure 30 - Filter Hide 40 - Filter Show 50 - Uninstall Success 51 - Uninstall Failure 60 - Cache Success 61 - Cache Failure 70 - Application Termination 80 - Process Ignored 81 - Process Terminated</p>
Date and Time	7/25/2002 9:27:52 AM	<p>The date (7/25/2002) and time (9:27:52 AM) the event occurred.</p>
User Distinguished Name and Tree	JSMITH.NOVELL.NOVELL_TREE	<p>The distinguished name and tree of the user for which the event occurred.</p>
Workstation Distinguished Name and Tree	.WORKSTATION NOT REGISTERED	<p>The distinguished name and tree of the workstation on which the event occurred. If the workstation has not been imported into eDirectory as a Workstation object, the field contains WORKSTATION NOT REGISTERED.</p>

Field	Example	Description
Workstation Address	137.65.45.25	The IPX or IP address of the workstation on which the event occurred.
Application Distinguished Name and Tree	NOTEPAD.APPS.NOVELL.NOVELL_TREE	The distinguished name and tree of the Application object for which the event occurred. For rogue processes, this field contains ZEN Process Management.
Application GUID	3054A94E-BBFF-4851-9D8E-58973623B728	The global unique identifier assigned to the Application object. The GUID is located on the Application object's Options page (Distribution Options tab). For rogue processes, this field is left blank.
Application Version Number	2	The version number assigned to the Application object. Possible numbers range from 0 to 65535. The version number is located on the Application object's Options page (Distribution Options tab). For rogue processes, this field is left blank.
Error Code Major	Could not launch NOTEPAD.APPS.NOVELL.NOVELL_TREE (using c:\winnt\notepa) (id=123)	For failed events, the error code generated by Application Launcher. For successful events, this field is always 0. For rogue processes, this field is left blank.
Error Code Minor	The filename, directory name, or volume label syntax is incorrect.	Additional error code information. For successful events, this field is always 0. For rogue processes, this field is left blank.
Event String 1	c:\winnt\notepa	Optional event information. For rogue processes, this field contains the process executable path.
Event String 2	no example	Optional event information. For rogue processes, this field contains the Original Filename of the process.
Event String 3	no example	Optional event information. For rogue processes, this field contains the process ID (PID).
Event String 4	no example	Optional event information. For rogue processes, this field contains the parent process ID (parent PID).
Event String 5	no example	Optional event information. For rogue processes, this field contains the event action, either "process ignored" or "process terminated successfully."

Field	Example	Description
Application Flag	524288	Application object bitmask. For rogue processes, this field is always 0.

44.8 Enabling Windows Installer Verbose Logging

When you distribute an application based on an MSI package rather than an AOT/AXT package, Application Launcher launches the Microsoft Windows Installer so that it can install the application according to the information and files in the MSI package. By default, the Windows Installer creates an `msixxxxx.log` file that includes basic information and messages.

If you need to troubleshoot problems with the installation, you can set up verbose logging for the Windows Installer. The Windows Installer creates a log file, `zappmsi.log`, in the user's temporary directory on the workstation. Enabling verbose logging will slow down installation of MSI applications, so you should do it only as a troubleshooting procedure.

To enable verbose logging on a workstation:

- 1 Modify the Windows registry to add the following key:

```
HKEY_LOCAL_MACHINE\Software\NetWare\NAL\1.0\Debug
```

- 2 Under the Debug key, add a *DWORD* value. Set the value name to *MSI* and the value data to *1*.
- 3 Save the registry.
- 4 Restart the workstation.

You need to modify the registry of each workstation where you want to enable verbose logging. We recommend that you create an Application object whose only function is to modify the registry.

For information about Windows Installer error messages included in the `msixxxxx.log` file or the `zappmsi.log` file, see the [Windows Installer Error Messages document \(http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/erro_89f7.asp\)](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/erro_89f7.asp) at the Microsoft Developer Network (MSDN) site.

For information about Windows Installer error codes returned through Application Launcher, see the [Error Codes document \(http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/code_13ub.asp\)](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/code_13ub.asp) at the Microsoft Developer Network site.

Novell® ZENworks® Desktop Management integrates with Novell Licensing Services to enable you to track an application's usage and comply with the application's license agreement.

Novell Licensing Services is a component of Novell NetWare® 6.x and Novell Open Enterprise Server (OES). To use Licensing Services with ZENworks, you must have a ZENworks Server installed on a NetWare 6.x server or an OES NetWare server. Novell Licensing Services also requires the Novell Client. You can download the latest client from the [Novell Product Downloads site \(http://download.novell.com/index.jsp\)](http://download.novell.com/index.jsp).

When a user launches an application that has been configured as part of Novell Licensing Services, Novell Application Launcher™ checks to make sure that a license is available before running the application.

License metering applies only to simple applications, AOT/AXT applications, and MSI applications. Licensing metering is not available for terminal server applications or Web applications.

To set up software metering, complete the tasks in the following sections:

- [Section 45.1, “Installing Novell Licensing Services,” on page 459](#)
- [Section 45.2, “Creating Metered Certificates,” on page 459](#)
- [Section 45.3, “Installing the Novell Client and Licensing Files to Workstations,” on page 461](#)
- [Section 45.4, “Configuring Applications to Use License Metering,” on page 461](#)

45.1 Installing Novell Licensing Services

Novell Licensing Services must be installed before you can use Application Launcher to meter software licenses. It is installed by default on NetWare 6.x and OES servers. For information about ensuring that Licensing Services is installed and configured correctly, see the documentation for the appropriate NetWare version:

- [NetWare 6 \(http://www.novell.com/documentation/nw6p/nls502enu/data/htoz9uzc.html\)](http://www.novell.com/documentation/nw6p/nls502enu/data/htoz9uzc.html)
- [NetWare 6.5 \(http://www.novell.com/documentation/nw65/nlsadmin/data/htoz9uzc.html\)](http://www.novell.com/documentation/nw65/nlsadmin/data/htoz9uzc.html)
- [OES NetWare \(http://www.novell.com/documentation/oes/nlsadmin/data/htoz9uzc.html\)](http://www.novell.com/documentation/oes/nlsadmin/data/htoz9uzc.html)

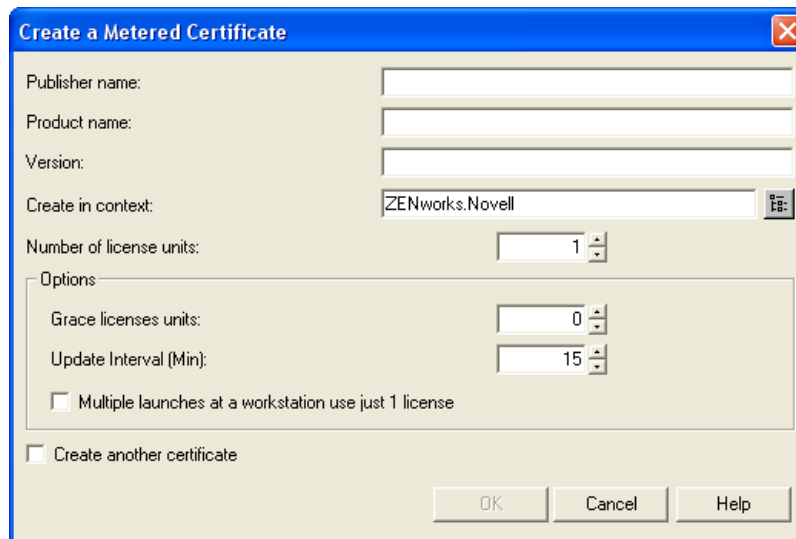
45.2 Creating Metered Certificates

You must create a metered certificate for each application whose usage you want to track. The metered certificate defines the number of licenses you have available for the application.

If necessary, you can have more than one metered certificate for an application. For example, if you initially have 200 licenses for the application, you can create a metered certificate of 200 licenses. Later, if you purchase 100 additional licenses, you can create a second metered certificate of 100 licenses.

You must use NetWare Administrator (NWAdmin), not ConsoleOne or iManager, to create metered certificates. To do so:

- 1 Launch NetWare Administrator from the NetWare 6.x or OES NetWare server (`sys:\public\win32\nwadmin32.exe`).
- 2 Select the container where you want to create the metered certificate, then click the *Tools* menu > *Novell Licensing Services* > *Add Licenses* to display the *Add a License Certificate* dialog box.
- 3 Select the *License Metering* option, then click *OK* to display the *Create a Metered Certificate* dialog box.



- 4 Fill in the following fields:

Publisher Name: Enter the name of the product vendor.

Product Name: Enter the name of the product (for example, Microsoft Office).

Version: Enter the product version.

Create in Context: Verify that this field displays the container where you want the metered certificate created. If not, click the browse button to find and select the correct container.

Grace License Units: Enter the number of units beyond the licensed units that you want to make available for use. This allows additional users to install and run the application while you purchase additional licenses. You can comply with your software license agreement without interrupting users' work flow or productivity.

Update Interval: Enter how often, in minutes, you want Licensing Services to poll the metered certificate to see how many licenses are still available.

Multiple Launches at a Workstation Use Just 1 License: Select this option if only one license should be used even if the application is installed or launched multiple times on the workstation.

- 5 Click *OK* to create the metered license.

NetWare Administrator creates a license container and adds the metered license to the container. The license container is named *publisher+product+version* (for example, Microsoft+Office+2003). You can double-click the license container to view the metered certificate, which is named with the date and time that it was created. You can double-click the metered license to see information such as how many units are in use.

- 6 If you need to add licenses for the product, follow the steps above making sure you do the following:
- Start by selecting the same container where the product's license container resides.
 - When you open the *Create a Metered Certificate* dialog box, use the same publisher name, product name, and version that you used for the first metered certificate. This causes the new metered certificate to be created in the same license container as the first certificate.

45.3 Installing the Novell Client and Licensing Files to Workstations

- 1 Make sure that the Novell Client™ is installed on users' workstations.

Novell Licensing Services requires the Novell Client. You can download the latest client from the [Novell Product Downloads site \(http://download.novell.com/index.jsp\)](http://download.novell.com/index.jsp).

- 2 Copy the `nls32.dll` and `nlsapi32.dll` to users' workstations.

- On Windows 98, copy the files to `c:\windows\system`.
- On Windows 2000/XP, copy the files to `c:\winnt\system32`.

The Novell Client requires `nls32.dll` for license metering. The `nls32.dll` file is included in the `\license` directory on the *Novell ZENworks 7 Companion 1 CD*.

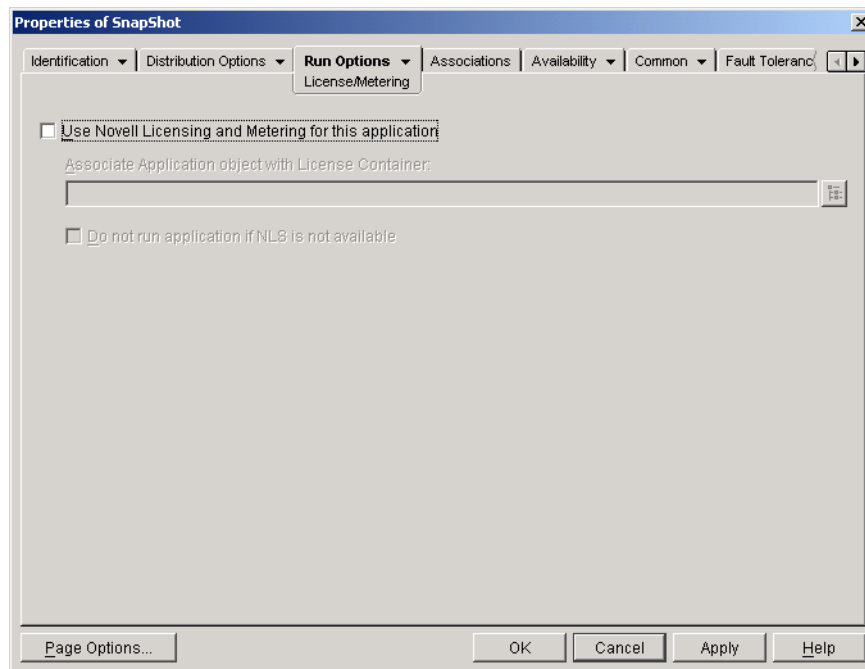
45.4 Configuring Applications to Use License Metering

After you have installed Novell Licensing Services, the Novell Client and its required `nls32.dll`, and have a license container and metered certificate created for an application, you need to configure the Application object to use Novell Licensing Services. This enables Application Launcher to enforce the licensing you've established for the application.

To enable Application Launcher to enforce an application's licensing:

- 1 In ConsoleOne®, right-click the Application object, then click *Properties*.

- 2 Click the *Run Options* tab > *License/Metering* to display the License/Metering page.



- 3 Select the *Use novell licensing and metering for this application* check box to turn on the option.
- 4 In the *Associate application object with License container* field, click the *Browse* button and select the application's license container.
- 5 If you don't want Application Launcher to run the application when Novell Licensing Services is not available, select the *Do not run if NLS is not available* check box. Otherwise, Application Launcher runs the application.
- 6 Click *OK*.

Reference: AdminStudio ZENworks Edition

46

Novell® ZENworks® 7 includes FLEXnet AdminStudio 7.5 ZENworks Edition to help you create and manage Windows Installer (MSI) software packages. AdminStudio ZENworks Edition includes the following tools:

- **Repackager:** Lets you repackage and convert Novell ZENworks projects (.axt/.aot) and other legacy setups into Windows Installer packages (.msi).
- **Tuner:** Lets you customize MSI packages. For example, you can create custom transforms that limit the features installed, add custom files to the installation, and set property values. You can also make multiple customizations from the same base setup.
- **Distribution Wizard:** Lets you deploy your MSI package to the source locations from which users can install the MSI application. It also lets you create an Application object for the MSI application in Novell eDirectory™.
- [Section 46.1, “Installing AdminStudio ZENworks Edition,” on page 463](#)
- [Section 46.2, “Using AdminStudio ZENworks Edition,” on page 464](#)

46.1 Installing AdminStudio ZENworks Edition

AdminStudio ZENworks Edition is included on the *Novell ZENworks 7 Software Packaging CD*.

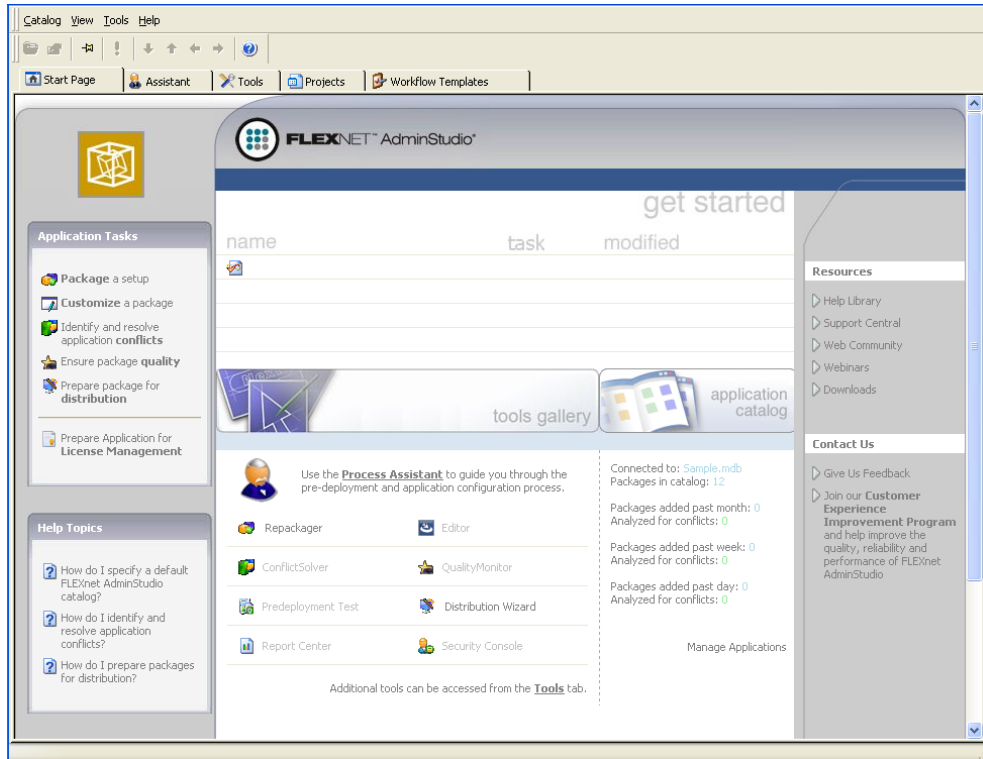
To install AdminStudio ZENworks Edition:

- 1 Make sure the Windows workstation where you want to install AdminStudio ZENworks Edition meets the system requirements. See the [AdminStudio ZENworks Edition Installation Guide](http://www.novell.com/documentation/beta/zenworks7/pdfdoc/spinstall/AS6ZENWorksInstallGuide.pdf) (<http://www.novell.com/documentation/beta/zenworks7/pdfdoc/spinstall/AS6ZENWorksInstallGuide.pdf>) for details.
- 2 At the Windows workstation, insert the *Novell ZENworks 7 Software Packaging CD* to display the ZENworks 7 installation program.

The `winsetup.exe` program automatically runs. If it does not run, launch the program from the root of the CD.
- 3 On the installation program’s main page, click *Software Packaging* to display the Software Packaging page.
- 4 Click *AdminStudio ZENworks Edition* to launch the AdminStudio installation program.
- 5 Follow the prompts to complete the installation, making sure you complete the registration process so that you receive your software key.

46.2 Using AdminStudio ZENworks Edition

- 1 On the Windows workstation where you installed AdminStudio ZENworks Edition, click the *Start* menu > *Programs* > *Macrovision* > *FLEXnet AdminStudio 7.5* to display the following screen.



The Tools Gallery displays the various tools provided by AdminStudio. The Repackager, Tuner, and Distribution Wizard are available in the ZENworks Edition. Only the Repackager and Distribution Wizard are displayed in the Tools Gallery; the Tuner is available on the Tools tab.

The tools that are dimmed are available in the professional or enterprise edition of AdminStudio. For a comparison of editions and information about purchasing the professional or enterprise edition, see the [FLEXnet AdminStudio ZENworks Edition site \(http://www.macrovision.com/products/flexnet_adminstudio/adminstudio/editions/zenworks.shtml\)](http://www.macrovision.com/products/flexnet_adminstudio/adminstudio/editions/zenworks.shtml).

- 2 For instructions about how to use AdminStudio, click the *Help* menu, then click *Contents* to display the Help system.

When distributing applications to Windows 98 or Windows 2000/XP workstations, Novell® ZENworks® Desktop Management supports two types of software packages: Microsoft Windows Installer (MSI) packages and ZENworks snAppShot™ (AOT/AXT) packages.

Based on the benefits of using the native Windows Installer, Novell recommends using Windows Installer packages rather than snAppShot packages. For more details regarding this recommendation, see [Novell snAppShot versus FLEXnet AdminStudio's Repackager \(http://www.macrovision.com/company/news/newsletter/tips/novell_vs_adminstudio.shtml\)](http://www.macrovision.com/company/news/newsletter/tips/novell_vs_adminstudio.shtml).

If you decide to use ZENworks snAppShot, the following sections provide information about snAppShot and instructions for using the utility.

- [Section 47.1, “Understanding SnAppShot,” on page 465](#)
- [Section 47.2, “Preparing a SnAppShot Workstation,” on page 467](#)
- [Section 47.3, “Creating an Installation Package,” on page 467](#)
- [Section 47.4, “Command Line Switches,” on page 468](#)

47.1 Understanding SnAppShot

SnAppshot records the changes that occur on a workstation as an application is installed. As the installation proceeds, snAppShot captures the differences between the workstation's pre-installation configuration state and the workstation's post-installation state, compares the two pictures, and creates an application installation package that consists of two Application object template (.aot or .axt) files, one or more application source (.fil) files, and one file definition (filedef.txt) file.

47.1.1 Application Object Templates

You use the Application object template file to create the Application object in Novell eDirectory™. Both Application object template (.aot and .axt) files contain the same information, which is used to populate the Application object property fields during creation of the object:

- The eDirectory name and workstation shortcut name to be given the Application object.
- The modifications that need to be made to the workstation's configuration settings (registry settings, INI settings, text file modifications, and so forth) during installation of the application.
- The macro definitions to use during installation.
- The list of application files to copy to the workstation during installation, including the source location to copy the files from and the target location to copy the files to.

The .aot file is a binary file that cannot be edited; the .axt file is a text file that can be modified with a text editor. If you need to modify the Application object template after snAppShot has created it, you should modify the .axt file and use it to create the Application object. Otherwise, you should use the .aot file because data from the .aot file is imported more quickly.

47.1.2 Application Source Files

SnAppShot also tracks all of the application files that are copied to the workstation. These files, which become the application source files, are copied to a network source location, renamed numerically starting with 1, and given a `.fil` file extension (for example, `1.fil`). Novell Application Launcher™ uses these source files when installing the application to the workstation.

47.1.3 Application File Definition File

To map the `.fil` files to their original files, snAppShot creates a file definition (`filedef.txt`) file. This text file not only maps the `.fil` files to the original files, but also specifies the target location and name to be used when installing the files to the workstation. For example:

```
1.fil=c:\dmi\win32\_deisl1.isu
2.fil=c:\dmi\win32\bin\wdmiutil.dll
```

47.1.4 SnAppShot Limitations

Please be aware of the following before using snAppShot:

- SnAppShot does not work with MSI applications installed by Microsoft Windows Installer. This includes applications such as Microsoft Office 2000 and Microsoft Office XP.

MSI applications often install portions of the application “on-demand,” which means that a snapshot of an MSI application's installation could possibly not include all features and functionality available in the application. For this reason, MSI applications must be distributed as MSI applications rather than as AOT/AXT (snAppShot) applications. For more information, see [Chapter 29, “Distribution: Complex Applications,” on page 321](#).

- SnAppShot does not support some of the new Windows XP registry types, such as `hex(800000007)`. Care should be taken when using snAppShot on Windows XP to ensure that the generated `.axt/.aot` file (or Registry page in the resulting Application object) does not include changes that could adversely affect the operation of Windows XP workstations to which the application is distributed.
- SnAppShot fails when the Windows registry is larger than 30 MB. The following message displays:

```
A critical 'out of memory' error has occurred. snAppShot must
close.
```

The recommended solution is to use AdminStudio ZENworks Edition instead. For information, see the [AdminStudio ZENworks Edition Installation Guide \(http://www.novell.com/documentation/zenworks65/pdfdoc/spinstall/AS_ZENworksInstallGuide.pdf\)](http://www.novell.com/documentation/zenworks65/pdfdoc/spinstall/AS_ZENworksInstallGuide.pdf).

- SnAppShot does not support Windows terminal servers. Do not use snAppShot on a terminal server to create an AOT/AXT application you want to deliver to other terminal servers.
- The Application object template changed from version 4.0.1 to 6.5 to accommodate several functionality changes, including the change from system requirements to distribution rules. If you have a pre-ZENworks 6.5 environment, you must select the Create Pre 6.5 Application Object Template File option while creating the `.aot` file in order to use the file in your environment. If you use the default option, Create 6.5 Application Object Template File, the resulting `.aot` file is not usable in a pre-ZENworks 6.5 environment.

47.2 Preparing a SnAppShot Workstation

Before running snAppShot on a workstation to create an installation package for an application, you should:

- Make sure the workstation is clean. A clean workstation has only the operating system and Microsoft Client.
- Make sure the workstation is representative of the type of workstation to which the application will be distributed. For example, if you are distributing the application to Windows 2000 users on a Dell* OptiPlex* GX110, run snAppShot on a Dell OptiPlex GX110 running Windows 2000. Depending on the application and what occurs during an install, it might be necessary to create different Application objects to be used for different types of workstations.

47.3 Creating an Installation Package

To create an installation package, snAppShot uses the following process:

- Takes an image of the workstation before the application is installed. You determine which drives are scanned and which configuration settings (registry settings, INI settings, and so forth) are recorded.
- Has you install the application.
- Takes another image of the workstation, records the differences between the two images, and creates the installation package (.aot and .axt files, .fil files, and filedef.txt file) in the network location you've specified.

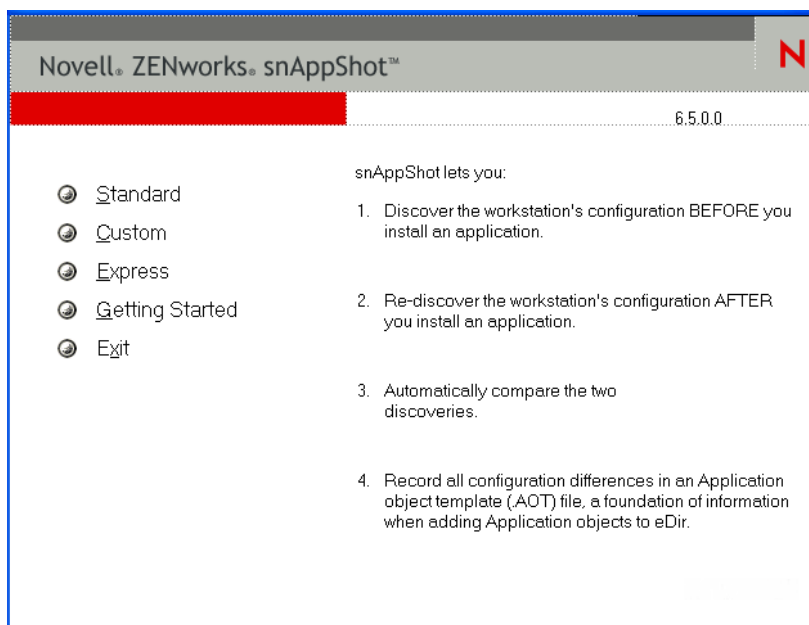
To run snAppShot and create an installation package:

- 1 On the clean and representative workstation (see [Section 47.2, “Preparing a SnAppShot Workstation,” on page 467](#)), start snAppShot (snapshot.exe) from the ZENworks Desktop Management Server.

The location of snapshot.exe depends on the server operating system:

- NetWare: sys:\public\snapshot
- Windows: c:\novell\public\snapshot
- Linux: /opt/novell/zenworks/zdm/winutils/snapshot

For information about switches you can use when starting snAppShot, see [Section 47.4, “Command Line Switches,”](#) on page 468.



2 Select the mode you want to use:

Standard: Uses the snAppShot default preference file during the discovery process. In most cases, these preferences should be sufficient.

Custom: Allows you to choose a previously created preference file to apply to the discovery process or to use the snAppShot default preference file. Unlike the Standard mode, Custom mode lets you make changes to specific preferences to discover drives, files, folders, registry settings, and shortcuts.

Express: Lets you choose a previously created preference file. No modifications can be made to the preferences.

3 Follow the on-screen prompts to create the installation package. If you need more information than is provided on the screen, click the *Help* button.

47.4 Command Line Switches

SnAppShot includes two switches that you can use on the command line. The syntax is:

```
snapshot switch
```

/u:filename.ini

This switch enables you specify the file from which snAppShot retrieves preference settings. You must have already created the preferences file during a previous snAppShot session. Using this switch is similar to running snAppShot, selecting the Express option, and then selecting the preferences file.

If the file is not in the same directory as snAppShot, specify the full path to the file.

/slow

By default, the snAppShot discovery process is optimized for a single-byte operating system. If you are running snAppShot on a double-byte operating system, you should use the */slow* switch. This causes snAppShot to use a string comparison routine optimized for double-byte characters. As a result, SnAppShot runs slower.

Reference: Application Object Settings

48

An Application object includes many settings (properties) you can modify to manage the application. The following sections correspond to each tab on the Application object property page.

- [Section 48.1, “Identification Tab,” on page 471](#)
- [Section 48.2, “Distribution Options Tab,” on page 479](#)
- [Section 48.3, “Run Options Tab,” on page 509](#)
- [Section 48.4, “Associations Tab,” on page 524](#)
- [Section 48.5, “Availability Tab,” on page 527](#)
- [Section 48.6, “Common Tab,” on page 548](#)
- [Section 48.7, “MSI Tab,” on page 568](#)
- [Section 48.8, “Terminal Server Client Tab,” on page 574](#)
- [Section 48.9, “Fault Tolerance Tab,” on page 576](#)

48.1 Identification Tab

The Identification tab includes the following pages to help you configure how the Application object is displayed to users:

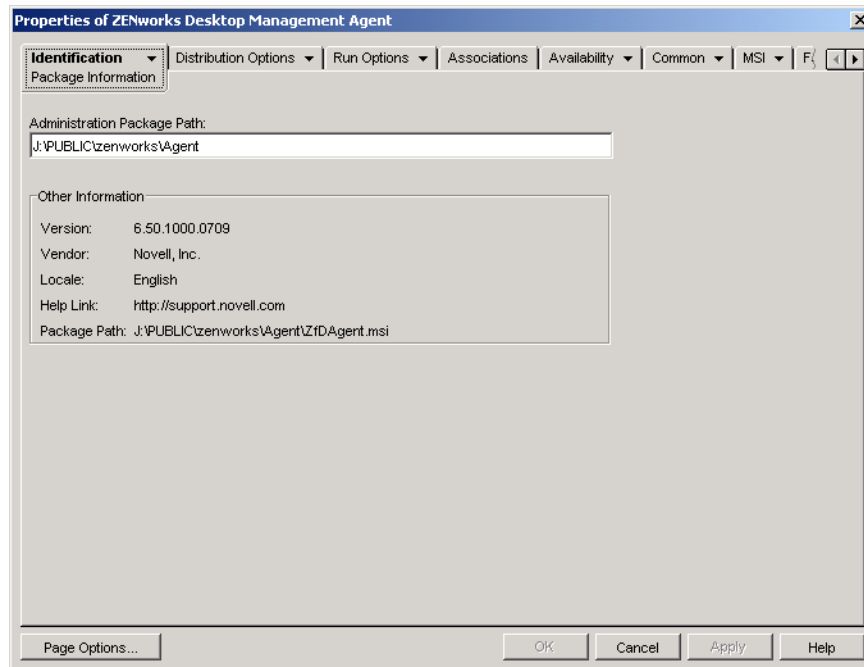
- [Section 48.1.1, “Package Information Page,” on page 471](#)
- [Section 48.1.2, “Icon Page,” on page 472](#)
- [Section 48.1.3, “Description Page,” on page 475](#)
- [Section 48.1.4, “Folders Page,” on page 475](#)
- [Section 48.1.5, “Contacts Page,” on page 477](#)
- [Section 48.1.6, “Administrator Notes Page,” on page 478](#)

48.1.1 Package Information Page

The Package Information property page is available on Application objects created for MSI applications only. It is not available on Application objects created for simple applications, AOT/AXT applications, Web applications, and terminal server applications.

The Package Information property page, shown below, displays information about the Microsoft Windows Installer package file (.msi file) associated with the application. This page is for informational purposes only; you cannot use this page to modify the package's information.

Figure 48-1 *ApplicationN Object > Identification Tab > Package Information Page*



Package path

Displays the location of the .msi file being used by the Application object.

Version

Displays the version of the .msi file.

Vendor

Displays the creator of the .msi file.

Locale

Displays the locale defined in the .msi file.

Help Link

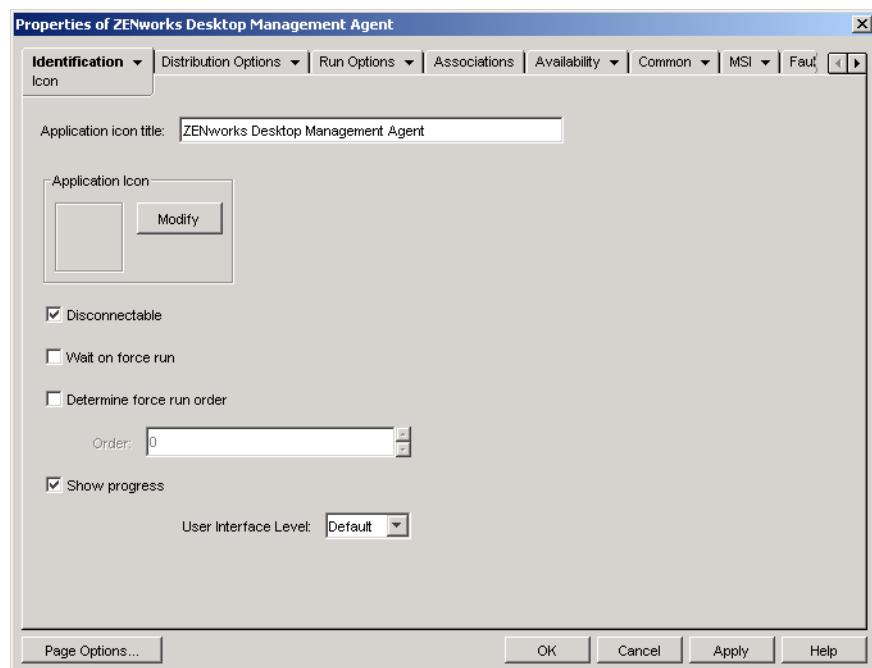
Displays the Web location to visit for information and help about the application.

48.1.2 Icon Page

The Icon property page is available on Application objects created for all application types (simple, AOT/AXT, MSI, Web, and terminal server).

The Icon property page, shown below, determines the Application object's icon that Novell® Application Launcher™ displays on a workstation. You can give the application icon a title, select the graphic to use for the icon, and give the icon a display order and force run priority. You can determine whether or not Application Launcher should continue to display the Application object on the workstation when the user has disconnected from Novell eDirectory™.

Figure 48-2 *ApplicaTion Object > Identification Tab > Icon Page*



Application Icon Title

Specify the text you want to use as the icon title for the Application object. The icon title must conform to standard Windows folder and filename conventions. If you use the following invalid Windows folder and filename characters, they are replaced on the user's desktop with an underscore (_):

\ / : * ? " < > |

Application Icon

Select the icon you want to appear wherever the Application object's icon is displayed. If you do not specify an icon, a default Application object icon is used.

Disconnectable

Select this option to mark the application as being able to be run on a workstation that is disconnected from eDirectory.

The application must be installed or cached to the workstation before the user can run it in disconnected mode. You can force the application to be installed on the workstation by selecting the *Force run* characteristic (*Associations* page). You can force the application to be cached to the workstation by selecting the *Force cache* characteristic (*Associations* page).

Wait on Force Run

This option applies only if the application and at least one other application are using the *Force run* option (*Associations* page).

Select this option to force the application to wait until the application that started before it terminates. The application order is defined in the *Determine force run order* field. Reboots are queued until the final application has terminated.

Determine Force Run Order

This option dictates the order in which applications set as *Force run* are started. Select this option to enable it, and then use the Order list to select the application's position in the *Force run* order.

You control the order in which the application is started by entering a numeric value in the *Order* box. A value of zero gives the application the highest priority. The maximum value is 9999999. For example, if you want this application to start after two other applications that have been given the order of 0 and 1, you would enter 2 in the *Order* box.

Application Launcher runs the application without waiting for the previously started application to terminate, unless the *Wait on force run* option is enabled.

Show Progress

This option displays a progress bar to users when an application is distributed to or removed from their workstations. Turn off this option if you are distributing only a small change, such as a registry modification. Turn on this option if you are distributing or removing a large application and want to give the user an idea of how long the process takes.

With this option turned off, if the workstation must be rebooted to complete the installation process and the Prompt for Reboot setting is enabled (*Distribution Options* tab > *Options* page), the user is not prompted and the workstation automatically reboots. The same is true if the workstation must be rebooted to complete the uninstall process and the Prompt User Before Uninstall setting is enabled (*Common* tab > *Uninstall* page).

User Interface Level

This option appears only if the Application object uses a Microsoft Windows Installer (MSI) package. During distribution of an MSI Application object, Application Launcher launches Windows Installer to install the application. As a result, rather than showing the standard Application Launcher installation progress bar, Windows Installer uses the installation user interface established for the MSI package. You can use the following settings to determine the amount of user interface the Windows Installer displays during installation.

- Default: Displays an appropriate user interface level (as chosen by Windows Installer).
- Silent: Displays no user interface.
- Progress: Displays simple progress information and error messages/prompts.
- Reduced: Displays a full user interface with Wizard dialog boxes suppressed.
- Full: Displays a full user interface (Wizard dialog boxes, progress information, error messages and prompts, and so forth).

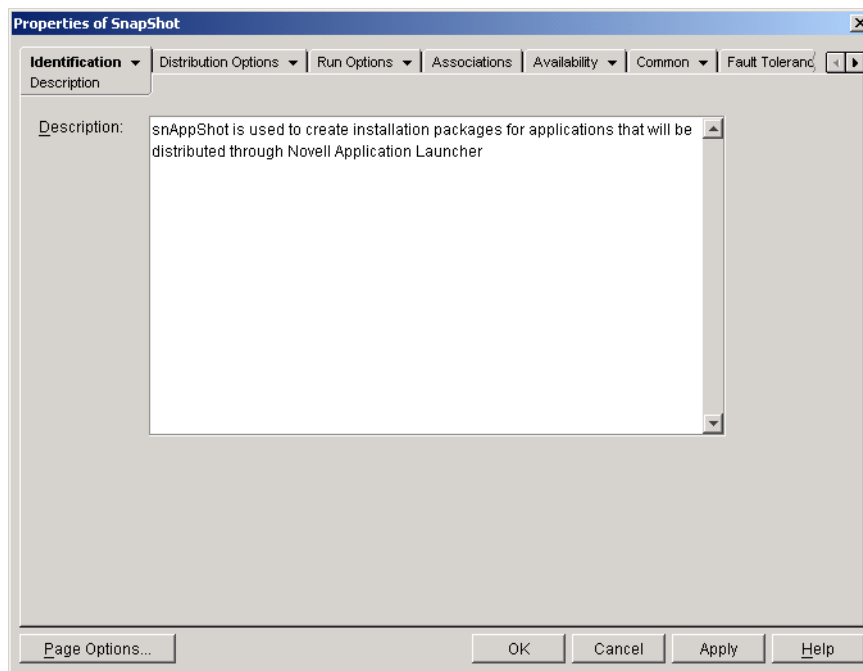
Application Launcher passes the selected setting to Windows Installer as a startup parameter. For more information about these settings, see the Microsoft Windows Installer documentation.

48.1.3 Description Page

The Description property page is available on Application objects created for all application types (simple, AOT/AXT, MSI, Web, and terminal server).

The Description property page, shown below, provides users more complete information about the Application object than the application icon title allows.

Figure 48-3 *Application Object > Identification Tab > Description Page*



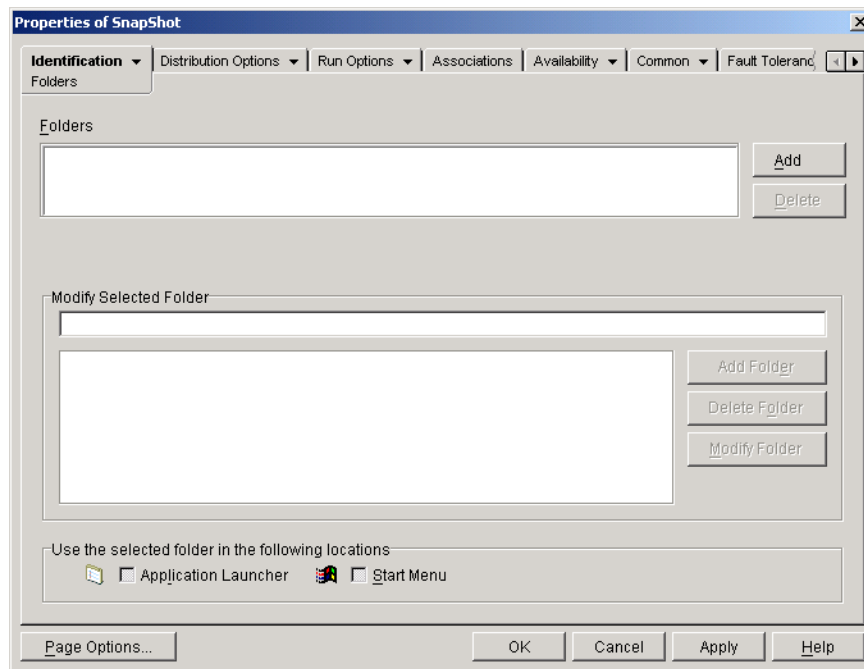
If you have enabled the Prompt User Before Distribution option (*Distribution Options > Options* page), users see this description when Application Launcher first distributes the application to them. They can also view an Application object's properties to see the description. To display the properties, right-click the Application object (on the workstation), then click *Properties*.

48.1.4 Folders Page

The Folders property page is available on Application objects created for all application types (simple, AOT/AXT, MSI, Web, and terminal server).

The Folders property page, shown below, lets you specify the folders where you want Application Launcher to place the application when distributing it to a workstation.

Figure 48-4 *Application Object > Identification Tab > Folders Page*



You can add the application to two different types of folders: a custom folder and a linked folder.

A custom folder is a folder created specifically for the Application object. No other Application objects can be included in the folder. Custom folders support folders within folders, which means that you can create a custom folder structure. For example, although you could not have Calculator and Notepad in the same custom folder, you could create two subfolders within the same custom folder and place the two programs in the two subfolders (in other words, `winapps\calculator\calc.exe` and `winapps\notepad\notepad.exe`).

A linked folder is simply an association to an existing Application Folder object. The Application Folder object must already exist in eDirectory. If the Application Folder object includes multiple folders (a folder structure) you can add the application to any folder in the structure.

If you plan to create a complex folder structure for the applications you distribute, we recommend that you use an Application Folder object and then link Application objects to the Application Folder object. An Application Folder object requires you to define the folder structure one time only, whereas custom folders must be defined for each Application object. If you choose to use custom folders for your folder structure, make sure you use the same folder names when defining the custom folder structure for each Application object. Any variation causes Application Launcher to create different custom folder structures.

Folders

The Folders list displays the custom folders and linked folders (Application Folder objects) that the application has been added to. Application Launcher creates (if necessary) the listed folders when distributing the application to the workstation.

Add

Click *Add* to add a custom folder or a linked folder to the Folders list. If you want the application to appear in multiple folders, add each folder to the list.

When you add a custom folder, it appears in the list with New Folder as its title. You can select the folder in the list and use the *Modify selected folder* box to change the folder's name or to add subfolders to it (see [Modify Selected Folder](#) below).

Delete

Select a folder in the folder list, then click *Delete* to remove the folder from the list. The change is applied the next time Application Launcher restarts.

Modify Selected Folder

The Modify Selected Folder box lets you modify name and structure information for the folder that is selected in the Folders list. You can modify information for custom folders and linked folders. However, after you modify a linked folder's information, it is converted to a custom folder.

Add Folder

Select the folder in the folder tree, then click *Add Folder* to add a subfolder to the folder. After you add a subfolder and Application Launcher refreshes, users see the application in the subfolder rather than in the folder.

Delete Folder

Select the folder in the folder tree, then click *Delete Folder* to delete the folder. The change is applied the next time Application Launcher restarts.

Modify Folder

Select the folder in the folder tree, then click *Modify Folder* to change the name of the folder.

If you want to add the application to a new subfolder of an existing folder, enter `existing_folder_name\new_subfolder_name`.

Use the Selected Folder in the Following Locations

Application Launcher can display folders on the Windows Start menu and in the Application Launcher windows (Application Window and Application Explorer window), if these locations are enabled on the Application object's Associations page. Select a folder in the Folders list, then select the check boxes for the locations where you want to use the folder.

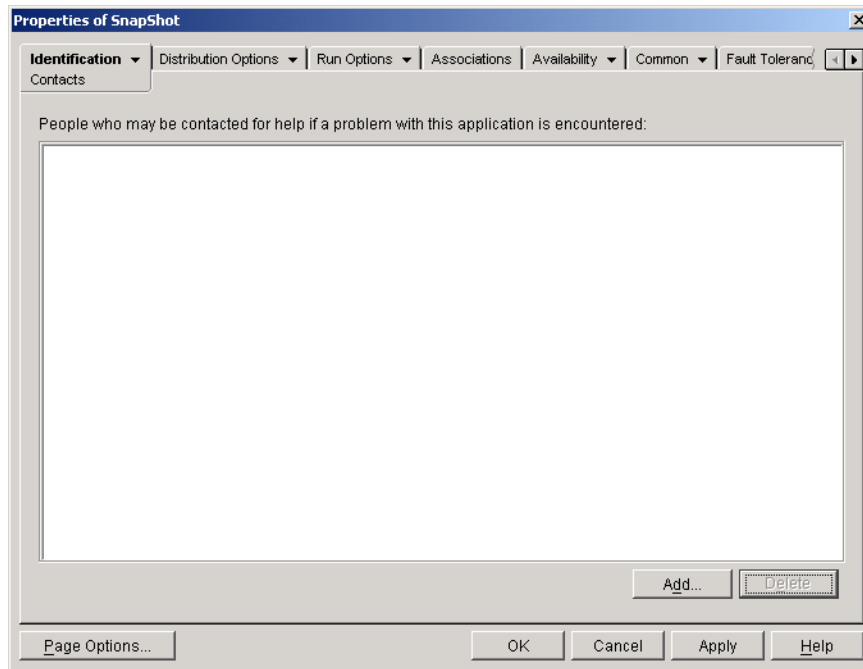
If you don't select either location, Application Launcher still displays the Application object on the Start menu and in the Application Launcher windows, but the object does not appear in the folders you've defined.

48.1.5 Contacts Page

The Contacts property page is available on Application objects created for all application types (simple, AOT/AXT, MSI, Web, and terminal server).

The Contacts property page, shown below, lists the names, e-mail addresses, and phone numbers of the application's support staff. Users can access this information through the Application object's properties. To display the properties, right-click the Application object (on the workstation), click *Properties*, then click *Help contacts*.

Figure 48-5 *Application Object > Identification Tab > Contacts Page*



You can tailor the information to direct users to the support staff at their locations. If you enter the support contact's e-mail address, users can send an e-mail message directly from the *Help Contacts* page of the Properties dialog box.

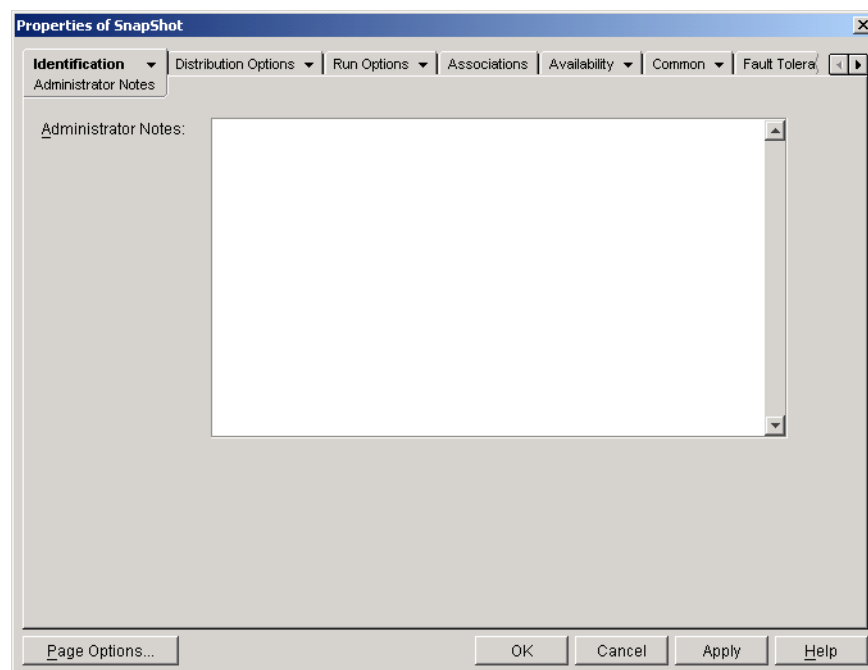
NOTE: Users must have the eDirectory rights required to read the *E-mail address* field (*Internet email address* attribute) and *Telephone* field (*Telephone number* attribute) of the users defined as contacts.

48.1.6 Administrator Notes Page

The Administrator Notes property page is available on Application objects created for all application types (simple, AOT/AXT, MSI, Web, and terminal server).

The Administrator Notes property page, shown below, lets you record notes for yourself or other administrators. For example, you could remind yourself about special settings for an application. Or, if you have several administrators, you could write a history of upgrades and file changes.

Figure 48-6 *Application Object > Identification Tab > Administrator Notes Page*



48.2 Distribution Options Tab

The Distribution Options tab includes the following pages to help you configure how the Application object is distributed to users:

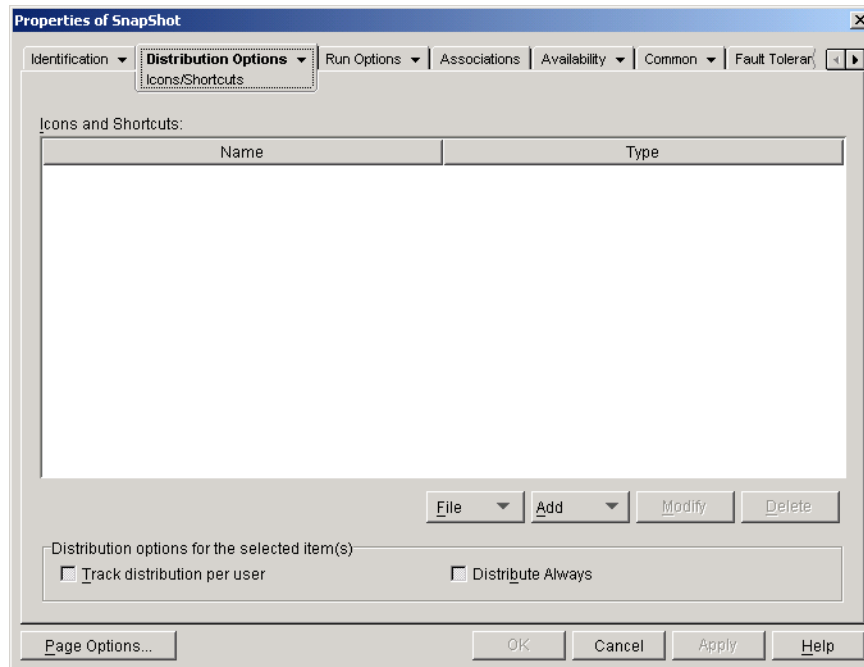
- [Section 48.2.1, "Icons/Shortcuts Page," on page 479](#)
- [Section 48.2.2, "Registry Page," on page 482](#)
- [Section 48.2.3, "Application Files Page," on page 485](#)
- [Section 48.2.4, "INI Settings Page," on page 489](#)
- [Section 48.2.5, "Text Files Page," on page 493](#)
- [Section 48.2.6, "Distribution Scripts Page," on page 496](#)
- [Section 48.2.7, "Pre-Install Schedule Page," on page 499](#)
- [Section 48.2.8, "Pre-Distribution Process Termination Page," on page 503](#)
- [Section 48.2.9, "Options Page," on page 504](#)
- [Section 48.2.10, "BITS Settings Page," on page 507](#)

48.2.1 Icons/Shortcuts Page

The Icons/Shortcuts property page is available only on Application objects created for simple applications and AOT/AXT applications. It is not available on Application objects created for MSI applications, Web applications, and terminal server applications.

The Icons/Shortcuts property page, shown below, determines the icons and shortcuts that Application Launcher creates when distributing the application to the workstation. You can add the application's icon as an item in a program group or as a shortcut on the workstation's desktop or in a folder. You can also delete existing icons, shortcuts, and program groups.

Figure 48-7 *Application Object > Distribution Options Tab > Icons/shortcuts Page*



The icons and shortcuts you add with this page are in addition to the Application object's icon. Although the Application object's icon might cause various actions to occur, including installing the application or running it, the icons and shortcuts defined on this page link directly to the application's executable file and simply launch the application.

You can use icons and shortcuts in combination with other options to create the user environment you want. For example, you could define the icons and shortcuts you want to be created and configure the Application object to run one time (*Run Options > Applications*). When a user selects the Application object, Application Launcher runs the application one time, creates the icons and shortcuts, performs any other tasks specified by the Application object's properties, and then removes the Application object's icon from the workstation. Thereafter, the user needs to select the icon or shortcut to launch the application.

IMPORTANT: If Application Launcher cannot create a shortcut, the application is not distributed. In this case, all application files and settings are removed. However, if other shortcuts were created before the shortcut that failed, those shortcuts are not removed.

Icons and Shortcuts

This list displays the icons and shortcuts that are created when the application is distributed to a workstation.

Files

Click *File > Find* to search for icon and shortcut definitions that include certain information.

Click *File > Import* to import icons and shortcuts from another Application object. The Open dialog box defaults to *.axt for its file type display. If you are importing from an .aot file, you must change the file type display to *.aot or *All files* in order to select the .aot file.

Add

Click *Add* to add a new program group, program group item, or shortcut. Program groups and program group items are supported on Windows 98 workstations but not on Windows 2000/XP workstations. Shortcuts are supported on all Windows versions.

IMPORTANT: When defining the target path for a shortcut, if the application will be distributed to a Windows 2000/XP workstation you must use a UNC path rather than a mapped drive path. Long mapped drive paths are truncated on Windows 2000/XP, resulting in an invalid shortcut that does not work.

Modify

Select an icon or shortcut from the Icons and Shortcuts list, then click *Modify* to change the information associated with it.

Delete

Select an icon or shortcut from the Icons and Shortcuts list, then click *Delete* to delete it from the list.

Track Distribution Per User

If you have implemented roaming user profiles, use this option to ensure that particular icons and shortcuts are distributed to each workstation a user logs in to.

In the Icons and Shortcuts list, select the desired icon or shortcut, then select *Track distribution per user*.

Distribute Always

By default, Application Launcher creates the icons and shortcuts defined in the Icons and Shortcuts list only at the following times:

- The first time the application is launched on a workstation.
- The first time the application is launched after the application's version number (*Distribution Options* tab > *Options* page) has been changed.

To force Application Launcher to create an icon or shortcut each time the application is launched, select the icon or shortcut in the Icons and Shortcuts list, then select *Distribute always*.

If the user has a NAL cache directory on his or her local machine, Application Launcher uses the information stored in the NAL cache directory to create the icon or shortcut. If the user does not have a NAL cache directory (for example, the user is running Application Launcher through a terminal server client session) or if writing to the cache has been disabled for the user (User object >

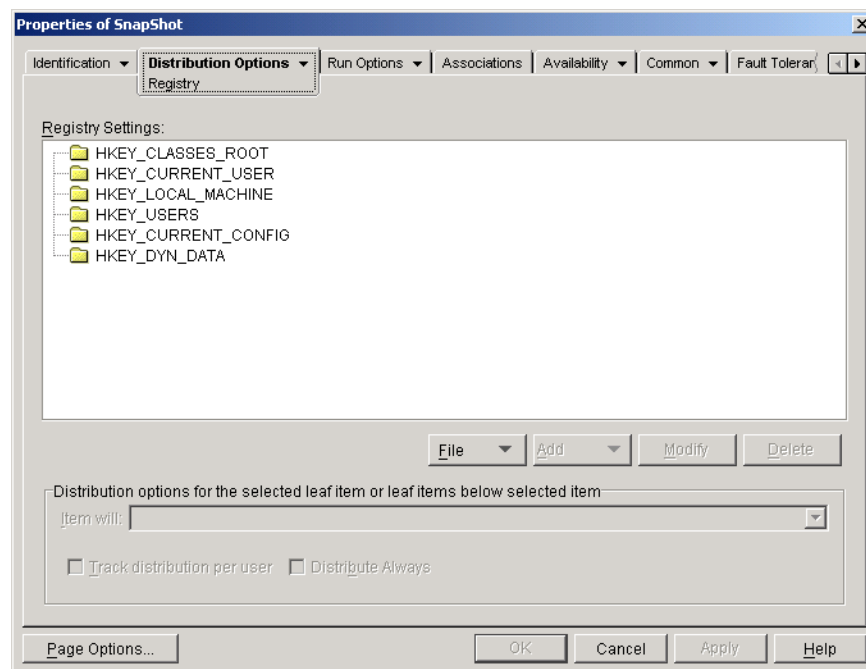
ZENworks tab > *Launcher Configuration* page > *Enable writing to cache* option), Application Launcher uses the information stored in eDirectory.

48.2.2 Registry Page

The Registry property page is available only on Application objects created for simple applications, AOT/AXT applications, and MSI applications. It is not available on Application objects created for Web applications and terminal server applications.

The Registry property page, shown below, determines the registry modifications that Application Launcher makes when distributing the application to a workstation.

Figure 48-8 *Application Object > Distribution Options Tab > Registry Page*



Registry Settings

The Registry Settings tree displays all settings that are modified when the application is distributed to a workstation. If you used an .aot, .axt, or .msi file when creating the Application object, the tree automatically includes all registry settings that are defined in those templates.

If there are additional registry settings you want created or deleted during distribution, you need to add the settings to the *Registry settings* tree and then specify the appropriate action (create or delete) in the *Item will* field.

NOTE: For Application objects created for AOT/AXT applications, the Novell Application Launcher (NAL) handles the distribution of the registry settings and the distribution of the application. If you modify registry settings for an AOT/AXT application and the registry settings fail to distribute, the application itself fails and NAL rolls back the application's installation.

For Application objects created for MSI applications, NAL handles the distribution of registry settings and the Microsoft Windows Installer (MSI) handles distribution of the application. If you modify the Application object's registry settings for a MSI application and the registry settings fail

to distribute, the application is installed by Windows Installer, but the registry settings do not roll back. As a result, the application might not function properly, depending on how the registry settings affect the application.

File

This option lets you search for keys or values in the *Registry settings* tree, import settings into the tree, and export settings from the tree.

Click *File*, then choose one of the following options:

- **Find:** Searches for specific keys, value names, or value data in the registry.
- **Find next:** Finds the next occurrence of the key, value name, or value data previously searched for.
- **Import:** Imports registry settings from another Application object's .aot or .axt file, or from a registry file (.reg). The Open dialog box defaults to *.axt for its file type display. If you are importing from an .aot file or .reg file, you must change the file type display to *.aot, *.reg, or *All files* in order to select the appropriate file.
- **Export:** Exports the registry settings to a registry file (.reg). To export the settings to an .aot or .axt file format, you must export the entire Application object using the Export Application Object option located on the *Tools > ZENworks Utilities > Application Launcher Tools* menu.

Add

This option lets you add registry settings to the *Registry settings* tree. Only settings displayed in the Registry Settings tree are created or deleted when the application is distributed.

To add a registry key or value, select the registry folder where you want to add the key, or select the key where you want to add a value, click the Add button, then choose one of the following options:

- **Key:** Adds a key to the selected registry folder.
- **Binary:** Adds a binary value to the selected key.
- **Expand string:** Adds an expand string value to the selected key. The expand string setting does not exist in the Windows 98 registry; if you use this setting, it is changed to a string setting during distribution to Windows 98 workstations.
- **Default:** Adds a default string value to the selected key.
- **DWORD:** Adds a DWORD value to the selected key.
- **Multi-string value:** Adds a multi-value string to the selected key. The multi-value string setting does not exist in the Windows 98 registry; if you use this setting, it is changed to a binary setting during distribution to Windows 98 workstations.
- **String:** Adds a string value to the selected key.

After the key or value is added to the Registry Settings tree, you can use the Distribution Options list to determine whether or not the key or value is created in the workstation's registry or deleted from the registry.

You can use a macro for a key name, value name, or value data. For information about macros, see [Chapter 49, "Reference: Macros," on page 585](#).

Modify

Select the key or value you want to modify, then click *Modify*.

Delete

Select the key or value you want to delete, then click *Delete*. When you delete a key, everything subordinate to the key is also deleted.

Distribution Options

The distribution options let you determine how individual registry settings (included in the Registry Settings tree) are handled during distribution of the application.

Item Will

In the Registry Settings tree, select the setting, then select the action that you want to occur for the setting when the application is distributed:

- **Create always:** The setting is always created in the registry, even if it already exists. If it exists, the setting's current values are overwritten. For example, if `PATH=C:\` already exists, `PATH=C:\TEMP` replaces it.
- **Create if does not exist:** The setting is created only if it does not already exist.
- **Create if exists:** The setting is created only if it already exists. The setting's current values are overwritten. For example, if `PATH=C:\` already exists, `PATH=C:\TEMP` replaces it.
- **Delete:** The setting is deleted. If the registry setting has subordinate settings, Application Launcher deletes the subordinate settings also.
- **Append if exists otherwise create:** This option applies only to string values (*String*, *Default string*, *Expanded string*, and *Multi-value string*). The string value's data is added to the existing string as the last entry. If the string value (or its key) does not exist, it is created.

When specifying the string value, you must include a semicolon (;) delimiter before the value if the string has existing values. For example, assume that the registry already includes a `string1=value1` setting. You want to append a second value (`value2`). When specifying the string value, you must specify `;value2` so that the resulting string is `string1=value1;value2`.

- **Prepend if exists otherwise create:** This option applies only to string values (*String*, *Default string*, *Expanded string*, and *Multi-value string*). The string value's data is added to the existing string as the first entry. If the string value (or its key) does not exist, it is created.

When specifying the string value, you must include a semicolon (;) delimiter after the value if the string has existing values. For example, assume that the registry already includes a `string1=value1` setting. You want to prepend a second value (`value2`). When specifying the string value, you must specify `value2;` so that the resulting string is `string1=value2;value1`.

Track Distribution Per User

If you have implemented roaming user profiles, use this option to ensure that particular registry settings are distributed to each workstation a user logs in to. You should enable this option for all registry settings that are not saved as part of roaming user profiles.

In the Registry Settings list, select the desired registry modification, then select the Track Distribution Per User check box.

Distribute Always

By default, Application Launcher distributes the registry modifications defined in the Registry Settings list only at the following times:

- The first time the application is launched on a workstation.
- The first time the application is launched after the application's version number (*Distribution Options* tab > *Options* page) has been changed.

To force Application Launcher to distribute a registry modification each time the application is launched, select the registry setting in the *Registry settings* list, then select the *Distribute always* check box.

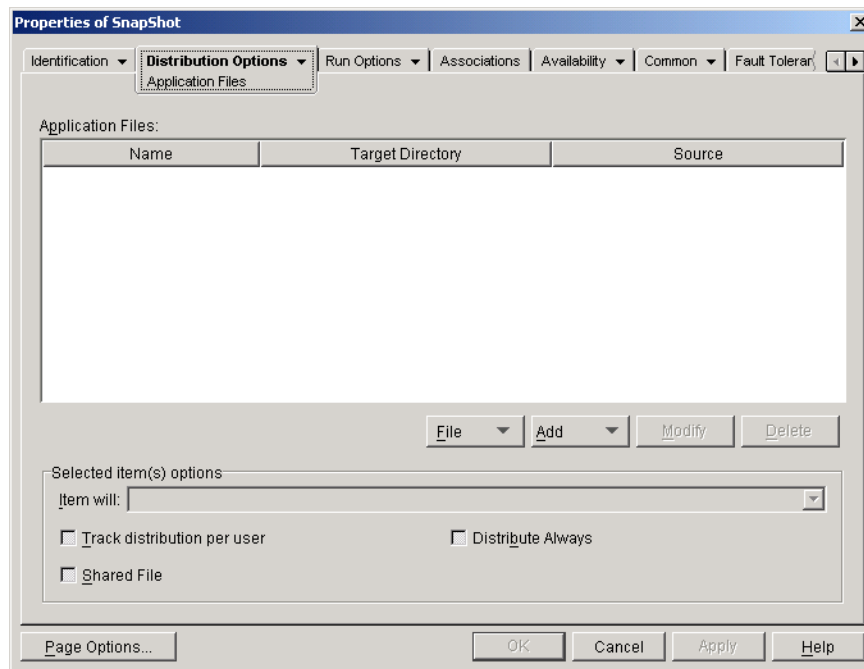
If the user has a NAL cache directory on his or her local machine, Application Launcher uses the setting information stored in the NAL cache directory to modify the registry. If the user does not have a NAL cache directory (for example, the user is running Application Launcher through a terminal server client session) or if writing to the cache has been disabled for the user (User object > *ZENworks* tab > *Launcher Configuration* page > *Enable writing to cache* option), Application Launcher uses the setting information stored in eDirectory.

48.2.3 Application Files Page

The Application Files property page is available only on Application objects created for simple applications and AOT/AXT applications. It is not available on Application objects created for MSI applications, Web applications, and terminal server applications.

The Application Files property page, shown below, specifies the application files that Application Launcher installs or removes when distributing the application to a workstation.

Figure 48-9 *Application Object > Distribution Options Tab > Application Files Page*



Application Files

The Application Files list displays all files and directories that are installed, removed or copied during distribution. The name, target directory (the location on the workstation where the file is installed), and source (the file or directory that is being used to install the file) are listed for each application file or directory.

If you used an .aot or .axt file when creating the Application object, the list automatically includes all files and directories that are defined in those templates.

File

This option lets you search for items in the Application Files list and import files and directories into the list.

Click *File* > choose one of the following options:

- **Find:** Searches for specific items in the list. You can search for text in the *Name*, *Target Directory*, or *Source* fields. For example, you could search for all files and directories that are being installed under the *Program Files* directory.
- **Find next:** Finds the next occurrence of the item specified by the initial search.
- **Import:** Imports application files and directories from another Application object's .aot or .axt file. The Open dialog box defaults to *.axt for its file type display. If you are importing from an .aot file, you must change the file type display to *.aot or *All files* in order to select the .aot file.

Add

This option lets you add files or directories to the *Application files* list. Only files and directories displayed in the *Application files* list are installed to, removed from, or copied to the workstation during distribution.

- **File:** To add a file to the list, click *Add*, then click *File* to display the Edit Files dialog box.

In the *Source file* field, specify the file to be used as the source of the installation. You can use a mapped drive, UNC path, or macro, or you can browse and select the file (for example, \\server1\vol1\bookmarks\bookmark.htm or %SOURCE_PATH%\bookmark.htm). The source file can be a single file that is copied, multiple files (for example, %SOURCE_PATH%*.*), or a snAppShot™ application source (.fil) file.

If you are deleting a file from the workstation, leave this field blank.

In the *Target file* field, specify the file on the workstation where the source file is to be copied (for example, c:\program files\novell\browser\bookmark.htm). You can also substitute a macro for the target path (for example, %TARGET_PATH%\bookmark.htm). If you are copying multiple files using a wildcard (*.*), specify the destination directory only (for example, c:\program files\novell\browser\).

If you are deleting the file from a workstation, enter the full path for the file from the perspective of the workstation, then select the *Target file to be deleted* check box.

- **Directory:** To add a directory to the list, click *Add*, then click *Directory* to display the Edit Directory dialog box.

In the *Source directory* field, specify the directory to be used as the source, if you are copying the directory. You can use a mapped drive, UNC path, or macro, or you can browse and select the directory (for example, c:\program files\novell). You can also substitute a macro for the directory path (for example, %DIRECTORY_TARGET_PATH%\novell).

If you are creating or deleting a directory, the *Source directory* field is disabled.

In the *Target directory* field, specify the directory to create or delete, or you can specify the directory on the workstation where the source directory is to be copied (for example, c:\program files\novell). You can also substitute a macro for the directory path (for example, %DIRECTORY_TARGET_PATH%\novell).

Select *Create directory* to create the directory on the workstation.

Select *Delete directory* to delete the directory from the workstation.

Select *Copy directory* to copy the directory to the workstation. When you select *Copy directory*, the *Include subdirectories* option becomes available. Click the *Include subdirectories* check box if you want to copy the subdirectories of the directory listed in the *Source directory* field.

Modify

Select the file or folder you want to modify, then click *Modify*.

Delete

Select the file or folder you want to delete, then click *Delete* to remove it from the *Application files* list.

Selected Item(s) Options

Use these options to set individual distribution options for files and directories included in the *Application files* list.

Item Will

Select a file in the *Application files* list > select one of the following options from the *Item will* list:

- **Copy always:** Copies the file regardless of whether the file currently exists on the workstation.
- **Copy if exists:** Copies the file only if the file currently exists on the workstation.
- **Copy if does not exist:** Copies the file only if the file does not currently exist on the workstation.
- **Copy if newer:** Copies the file only if its date and time are newer than the existing file's date and time, or if the file does not currently exist on the workstation.
- **Copy if newer and exists:** Copies the file only if it already exists on the workstation and has an older date or time.
- **Copy if newer version:** Copies the file only if its internal version is newer than the existing file's version (if version information is present). This is useful if you want to update the version of an .exe or .dll file based on the compiled version information.
- **Request confirmation:** Prompts the user to verify that the file should be copied.
- **Copy if different:** Copies the file if its date, time, or size is different than the existing file's date, time, or size.
- **Delete:** Deletes the file from the workstation.

Select a folder in the *Application files* list, then select one of the following options from the *Item will* list:

- **Create:** Creates the directory on the workstation.
- **Delete:** Deletes the directory from the workstation.

Track Distribution Per User

If you have implemented roaming user profiles, use this option to ensure that application files are distributed to each workstation a user logs in to. You should enable this option for all application files that are not saved as part of roaming user profiles.

In the *Application files* list, select the desired application files, then select *Track distribution per user*.

Distribute Always

By default, Application Launcher distributes the file and folder modifications defined in the *Application files* list only at the following times:

- The first time the application is launched on a workstation.
- The first time the application is launched after the application's version number (*Distribution Options* tab > *Options* page) has been changed.

To force Application Launcher to distribute a file or folder modification each time the application is launched, select the file or folder in the *Application files* list, then select *Distribute always*.

If the user has a NAL cache directory on his or her local machine, Application Launcher uses the information stored in the NAL cache directory to install or remove the file or folder. If the user does not have a NAL cache directory (for example, the user is running Application Launcher through a terminal server client session) or if writing to the cache has been disabled for the user (User object > *ZENworks* tab > *Launcher Configuration* page > *Enable writing to cache* option), Application Launcher uses the information stored in eDirectory.

Shared File

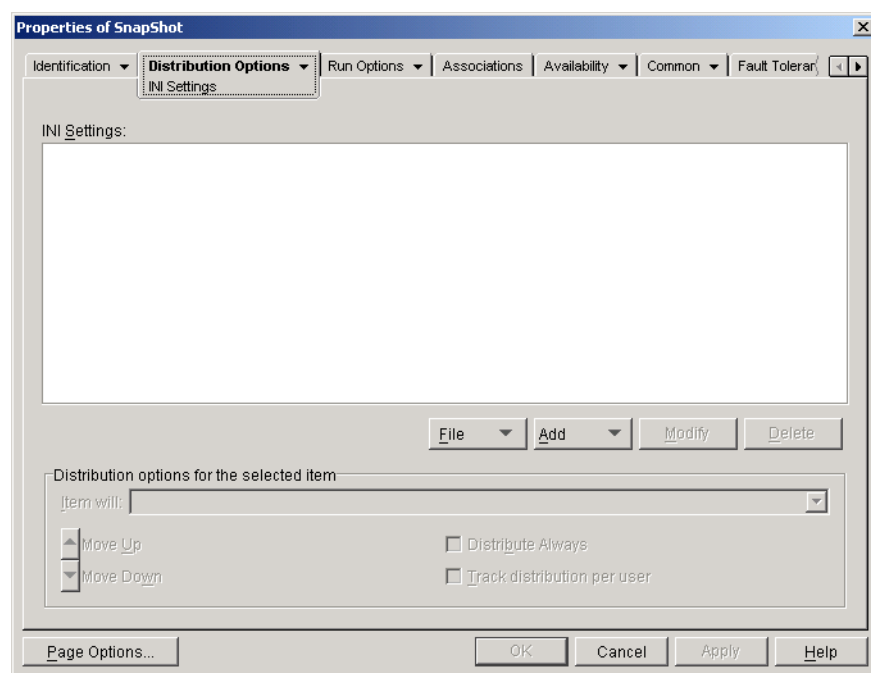
Use this option to mark a file as a shared file (that is, one that is used by more than one application). Shared files are usually Windows DLL files. SnapShot detects shared files when it discovers application installation changes on a workstation.

48.2.4 INI Settings Page

The INI Settings property page is available only on Application objects created for simple applications, AOT/AXT applications, and MSI applications. It is not available on Application objects created for Web applications and terminal server applications.

The INI Settings property page, shown below, determines the INI settings that Application Launcher creates or deletes when distributing the application to a workstation.

Figure 48-10 *INI Settings Page*



INI Settings

The INI Settings tree displays the INI settings that are modified when the application is distributed to the workstation. If you used an .aot, .axt, or .msi file when creating the Application object, the tree automatically includes all INI settings defined in those templates.

If there are additional INI settings you want created or deleted during distribution, you need to add the settings to the *INI settings* tree and then specify the appropriate action (create or delete) in the *Item will* field.

The INI Settings tree can include multiple INI files and each file can include multiple sections. When you add a setting to the INI Settings tree, you must add it to a file and section. This means that you might need to add new files and new sections to the tree before you can add new settings.

For example, assume that you want to add a `CLASSPATH=` setting to the `ENVIRONMENT` section of the `sample.ini` file. You would 1) add a file entry to the *INI settings* tree for the `sample.ini` file, 2) add an `ENVIRONMENT` section under the `sample.ini` file, 3) add the `CLASSPATH=` setting under the `ENVIRONMENT` section, and 4) select the `CLASSPATH=` setting and choose the appropriate *Create* action in the *Item will* field.

If, instead of adding the `CLASSPATH=` setting, you wanted to delete it, you would follow the same process but then choose the appropriate *Delete* action in the *Item will* field.

NOTE: For Application objects created for AOT/AXT applications, the Novell Application Launcher (NAL) handles the distribution of the INI settings and the distribution of the application. If you modify INI settings for an AOT/AXT application and the INI settings fail to distribute, the application itself fails and NAL rolls back the application's installation.

For Application objects created for MSI applications, NAL handles the distribution of INI settings and the Microsoft Windows Installer (MSI) handles distribution of the application. If you modify the Application object's INI settings for a MSI application and the INI settings fail to distribute, the application is installed by Windows Installer, but the INI settings do not roll back. As a result, the application might not function properly, depending on how the INI settings affect the application.

File

This option lets you search for files, sections, or values in the INI Settings tree, import settings into the tree, export settings from the tree, or view a file's INI settings.

Click *File* > choose one of the following options:

- **Find:** Searches for specific files, sections, or values.
- **Find next:** Finds the next occurrence of the item specified by the initial search.
- **Import:** Imports INI settings from another Application object's `.aot` or `.axt` file, or from a `.ini` file. The Open dialog box defaults to `*.axt` for its file type display. If you are importing from an `.aot` file or `.ini` file, you must change the file type display to `*.aot`, `*.ini`, or *All files* in order to select the appropriate file.
- **Export:** Exports the settings to an `.ini` file. To export the settings to an `.aot` or `.axt` file, you must export the entire Application object using the *Export application object* option located on the *Tools > ZENworks Utilities > Application Launcher Tools* menu.
- **View file:** Displays the INI settings for a specific file that are modified when the application is distributed. You must select the file from the INI Settings tree before you click *File > View File*.

Add

This option lets you add INI settings to the INI Settings tree. Only settings displayed in the INI Settings tree are created or deleted when the application is distributed. You can add a file to the tree, a section to a file, or a value to a section.

To do so, select the appropriate item in the tree, click the *Add* button, then choose one of the following options:

- **File:** Adds a file to the INI Settings tree. In addition to providing a file name, you can specify the target location for the file. By default, the `%*WINDIR%` macro is used, which represents the workstation's Windows directory (typically `c:\windows` or `c:\winnt`). After you name the file, you can begin adding sections to it.
- **Section:** Adds a section to the selected file. After you name the section, you can begin adding values to it.
- **Value:** Adds a value to the selected section. You must specify the value name and value data.

After you've added a value to the INI Settings tree, you can use the *Distribution options* list to determine whether or not it is created or deleted from the workstation. If the value needs to be created but the file or section does not exist, Application Launcher creates the file or section before adding the value.

You can use a macro for a section name, value name, or value data. For more information about macros, see [Chapter 49, "Reference: Macros," on page 585](#).

Modify

You can modify a file's name, a section's name, or a value's name and data. Select the file, section, or value you want to modify, then click *Modify*.

Delete

Select the file, section, or value you want to delete from the *INI settings* tree, then click *Delete*. When deleting a file or section, everything subordinate to it is also deleted.

Distribution Options for the Selected Item

The distribution options let you determine how individual INI settings (included in the INI Settings tree) are handled during distribution of the application.

Item Will

Use this option to determine whether a setting is created or deleted when the application is distributed. Select a value in the *INI settings* tree, then select one of the following options from the *Item will* list:

- **Create always (default):** Creates the value regardless of whether the value currently exists in the section.
- **Create if does not exist:** Creates the value only if the value does not currently exist in the section.
- **Create if exists:** Creates the value only if the value currently exists in the section.
- **Create or add to existing section:** Creates the value if the value does not currently exist in the section. If the value exists, it adds this value to the section in addition to the one that already

exists. This is useful, for example, if you need multiple values of the same type, such as two "DEVICE=" values.

- **Create or append to existing value:** Creates the value if the value does not currently exist in the section. If the value exists, it appends the data for the new value to the existing value. The first character in the value data needs to be the separator character, such as a space.
- **Delete:** Deletes the value from the section.
- **Delete or remove from existing value:** Deletes the value from the section, or, if the value has multiple data entries, removes this value's data entry from the value. For example, suppose the following setting is in the `win.ini` file: `Run = sol.exe calc.exe`. Using this option, you can remove just `calc.exe`, leaving the following: `Run = sol.exe`. The first character in the value data needs to be a separator character, such as a space.

Move Up / Move Down

Use these options to position sections and values in the order in which you want them to be created, modified, or deleted.

In the *INI settings* tree, select the section or value to move, then click *Move Up* or *Move Down*.

Distribute Always

By default, Application Launcher distributes the modifications defined in the INI Settings list only at the following times:

- The first time the application is launched on a workstation.
- The first time the application is launched after the application's version number (*Distribution Options* tab > *Options* page) has been changed.

If the user has a NAL cache directory on his or her local machine, Application Launcher uses the information stored in the NAL cache directory to make the INI modification. If the user does not have a NAL cache directory (for example, the user is running Application Launcher through a terminal server client session) or if writing to the cache has been disabled for the user (User object > *ZENworks* tab > *Launcher Configuration* page > *Enable writing to cache* option), Application Launcher uses the information stored in eDirectory.

To force Application Launcher to distribute an INI modification each time the application is launched, select the INI setting in the *INI settings* list, then select *Distribute always*.

NOTE: After you save the Application object and open it again, settings that you mark as *Distribute always* are grouped after settings that are not marked *Distribute always*, regardless of their creation order or their forced order (by using the *Move Up* and *Move Down* arrows).

For example, if you have a section with two *Distribute always* values (DAValue1 and DAValue2) and two non-Distribute Always value (Value3 and Value 4), the values are listed in the following order: Value3, Value4, DAValue1, DAValue2.

You can use the *Move Up* and *Move Down* arrows to change the order within the two groupings, but the *Distribute always* group is always listed second. For example, using the previous ordering (Value3, Value4, DAValue1, DAValue 2), you could change the order of the first two values and the order of the second two values to get the following order: Value4, Value3, DAValue2, DAValue1. However, if you change the order to list the Distribute Always values first (DAValue2, DAValue1,

Value4, Value3), when you save the Application object the order reverts to Value4, Value3, DAValue2, DAValue1.

Track Distribution Per User

If you have implemented roaming user profiles, use this option to ensure that particular `.ini` file settings are distributed to each workstation a user logs in to. You should enable this option for all `.ini` file settings that are not saved as part of roaming user profiles.

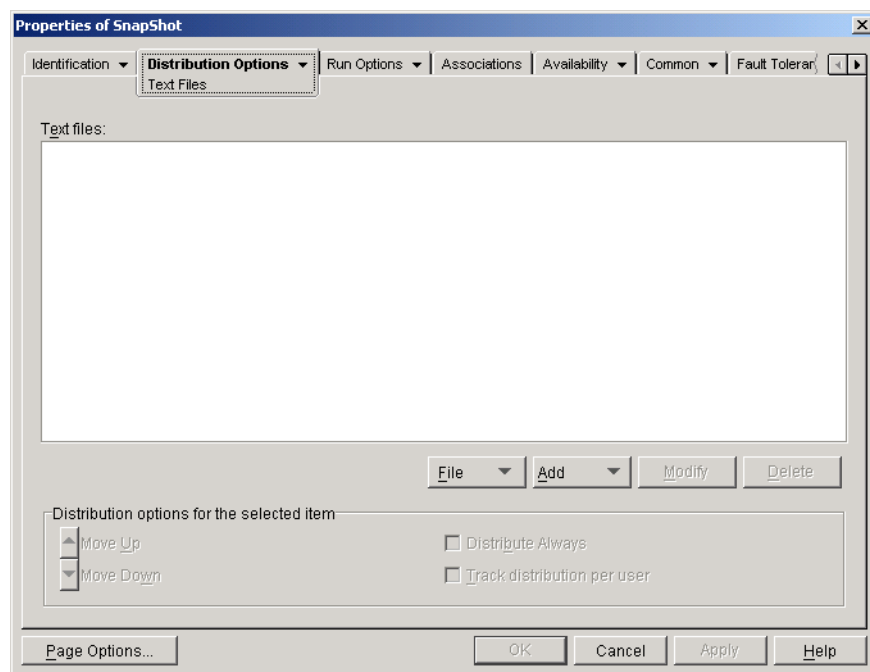
In the *INI settings* tree, select the setting you want to track, then select *Track distribution per user*.

48.2.5 Text Files Page

The Text Files property page is available only on Application objects created for simple applications and AOT/AXT applications. It is not available on Application objects created for MSI applications, Web applications, and terminal server applications.

The Text Files property page, shown below, determines the modifications that Application Launcher makes to text files (such as `config.sys` and `autoexec.bat`) when distributing the application to a workstation.

Figure 48-11 Application Object > Distribution Options Tab > Text Files Page



Text Files

The Text Files tree shows the text files that Application Launcher modifies. Each modification to a file is displayed subordinate to the file.

File

This option lets you search for files or text in the *Text files* tree and import files into the tree.

Click *File*, then choose one of the following options:

- **Find:** Searches for specific files or information in the *Text files* tree.
- **Find next:** Finds the next occurrence of the item specified by the initial search.
- **Import:** Imports text files from another Application object's .aot or .axt file. The Open dialog box defaults to *.axt for its file type display. If you are importing from an .aot file, you must change the file type display to *.aot or *All files* in order to select the .aot file.

Add

This option lets you add text file modifications to the *Text files* tree. Only the modifications displayed in the *Text files* tree are made when the application is distributed.

- **File:** To add a text file to the tree, click *Add > File* to create the file entry. You can type the filename or the path and filename (for example, autoexec.bat or c:\autoexec.bat). Only local workstation drives, UNC server paths, and macros are valid.

You should specify a path if possible. If you enter only the filename, Application Launcher searches all directories specified in the workstation's PATH environment variable. If it does not find a matching filename, it assumes the file doesn't exist and creates it in the first directory specified in the PATH variable.

- **Change:** To add a change to a file that is in the Text Files list, select the file, click *Add > Change* to display the Edit Text File dialog box. Make the desired changes. Click *Help* in the Edit Text File dialog box for information about each of the dialog box fields.

You can add multiple modifications to a text file. For example, you might want to make one modification that replaces text in the file and another modification that adds text to the end of the file. Each modification you add is displayed beneath the text file in the *Text files* list.

IMPORTANT: If you make changes to a text file (adding text, for example), you can add only one line at a time. If you press Enter to create a line break, your change saves.

Modify

To change the name of a text file, select the file in the *Text files* tree, click *Modify*, then specify the new name.

To edit one of the text file's modifications, select the modification in the *Text files* tree, click *Modify* to display the Edit Text File dialog box, then make the desired changes. Click *Help* in the Edit Text File dialog box for information about each of the dialog box fields.

Delete

In the *Text file* tree, select the text file or text file modification you want to delete > click *Delete*.

Distribution Options for the Selected Item

Use these options to set individual distribution options for text files and text file modifications. The options change depending on whether you have selected a text file or a text file modification in the Text Files tree.

No Reboot Needed If Modified

This option appears only when you have selected a text file. Select this option if you don't want users to reboot after you make changes to the selected text file. The *Reboot* and *Prompt reboot* options on the *Distribution Options > Options* page override this setting.

Move Up / Move Down

These options appear only when you have selected a text file modification. Click *Move Up* or *Move Down* to position the modification according to the order in which you want it applied.

Distribute Always

By default, Application Launcher distributes the text file modifications defined in the *Text files* list only at the following times:

- The first time the application is launched on a workstation.
- The first time the application is launched after the application's version number (*Distribution Options* tab > *Options* page) has been changed.

If the user has a NAL cache directory on his or her local machine, Application Launcher uses the information stored in the NAL cache directory to make the modification. If the user does not have a NAL cache directory (for example, the user is running Application Launcher through a terminal server client session) or if writing to the cache has been disabled for the user (User object > *ZENworks* tab > *Launcher Configuration* page > *Enable writing to cache* option), Application Launcher uses the information stored in eDirectory.

To force Application Launcher to distribute a text file modification each time the application is launched, select the modification in the *Text files* list, then select *Distribute always*.

NOTE: After you save the Application object and open it again, modifications that you mark as *Distribute always* are grouped after modifications that are not marked *Distribute always*, regardless of their creation order or their forced order (by using the *Move Up* and *Move Down* arrows).

For example, if you have a file with two *Distribute always* modifications (DAMod1 and DAMod2) and two non-Distribute Always modifications (Mod3 and Mod4), the modifications are listed in the following order: Mod3, Mod4, DAMod1, DAMod2.

You can use the *Move Up* and *Move Down* arrows to change the order within the two groupings, but the *Distribute always* group is always listed second. For example, using the previous ordering (Mod3, Mod4, DAMod1, DAMod2), you could change the order of the first two modifications and the order of the second two modifications to get the following order: Mod4, Mod3, DAMod2, DAMod1. However, if you change the order to list the *Distribute always* modifications first (DAMod2, DAMod1, Mod4, Mod3), when you save the Application object the order reverts to Mod4, Mod3, DAMod2, DAMod1.

Track Distribution Per User

If you have implemented roaming user profiles, use this option to ensure that particular text file modifications are distributed to each workstation a user logs in to. You should enable this option for all modifications that are not saved as part of roaming user profiles.

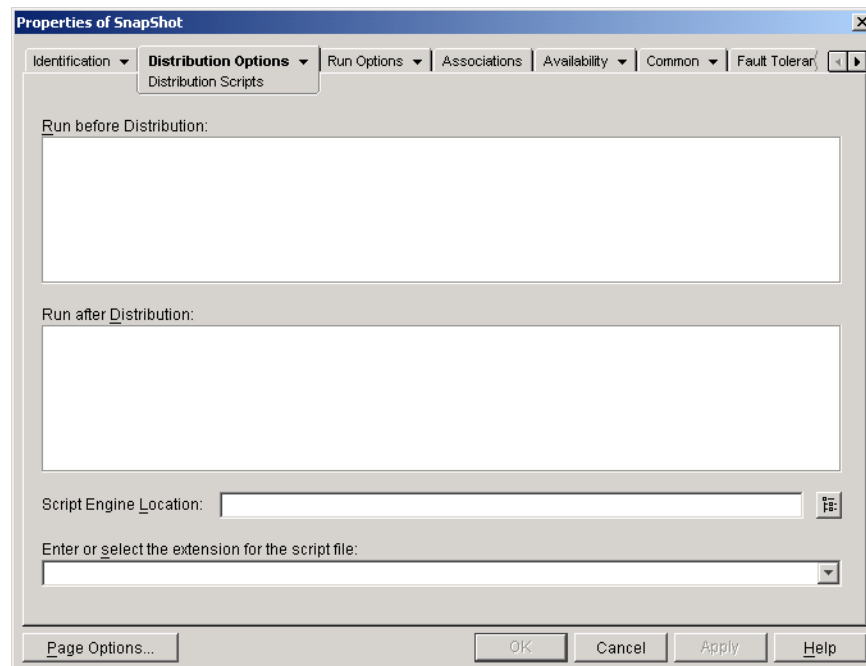
In the *Text files* list, select the desired modification, then select *Track distribution per user*.

48.2.6 Distribution Scripts Page

The Distribution Scripts property page is available on Application objects created for simple applications, AOT/AXT applications, and MSI applications only. It is not available on Application objects created for Web applications and terminal server applications.

As part of the process of distributing an application, Application Launcher can launch a script engine to execute a “before distribution” script and an “after distribution” script (for details about the order of script execution, see [“Script Execution Order” on page 498](#)). The Distribution Scripts property page, shown below, defines the script engine that you want Application Launcher to use and the scripts you want executed.

Figure 48-12 Application Object > Distribution Options Tab > Distribution Scripts Page



On Windows 2000/XP, distribution scripts are run in the secure system space, which means that users do not see any of the script commands or command results. Therefore, you should not include any commands that require or initiate user interaction. If you do so, the script halts at that point. For example, you would not want to include a command to run a program that requires user interaction because the program, which runs in secure system space, is never displayed to the user. On Windows 98, distribution scripts are run in the user space (because there is no system space).

Run Before Distribution

Use this text window to enter any script commands you want executed before the application is distributed. Do not use extended characters in the script; extended characters are not supported. For script example, see [“Script Example” on page 497](#).

Run After Distribution

Use this text window to enter any script commands you want executed after the application is distributed. Do not use extended characters in the script; extended characters are not supported. For script example, see [“Script Example” on page 497](#).

Script Engine Location

The script engine determines the script commands and scripting language you need to use. If you do not define a script engine in the *Script engine location* field, Application Launcher uses the Novell Client™ as the script engine (if the workstation has the Novell Client installed), which means that you can use most Novell Client login script commands (see [“Supported Novell Client Login Script Commands” on page 498](#)).

If you want to use a script engine other than the Novell Client, specify the alternate script engine. The script engine must reside in a location that is always available to users, such as their local drives. The script engine can reside on a network server only if users can map a drive to the server (for example, through the Novell Client or the Client for Microsoft Networks). If Application Launcher cannot find the script engine, it displays an error to the user and fails to distribute the application.

If you use the Windows command interpreter as the script engine, you must include the /C switch, as shown in the following examples:

- Windows 2000/XP: `%*winsysdir%\cmd.exe /c`
- Windows 98: `%*windir%\command.com /c`

The `%*winsysdir%` and `%*windir%` variables specify the Windows system directory (for example, `c:\winnt\system32`), and the `/c` switch instructs the command interpreter to execute the script and then stop. If the `/c` switch is not used, the script does not complete.

For a script example, see [“Script Example” on page 497](#).

Script File Extension

This applies only if you specified a script engine in the Script Engine Location field.

When the application is distributed, Application Launcher creates temporary script files for the *Run before distribution* scripts and *Run after distribution* scripts. These files are passed to the script engine, which then executes the script. You need to specify the file extension that the script engine requires for its script files.

For a script example, see [“Script Example” on page 497](#).

Script Example

The following script uses the Windows 2000/XP command interpreter as the script engine. Before the distribution occurs, a listing of the `c:\` directory is saved to a text file and the `autoexec.bat` file is backed up.

Run Before Distribution Field

```
dir c:\ >c:\1.txt
copy autoexec.bat autoexec.bak /y
```

Script Engine Location Field

cmd.exe /c

Enter or Select the Extension of the Script File Field

.bat

Script Execution Order

Application Launcher can execute up to four different scripts when distributing and launching an application:

- **Distribution scripts:** Run Before Distribution and Run After Distribution (*Distribution Options* tab > *Distribution Scripts* page)
- **Launch scripts:** *Run before launching* and *Run after termination* (*Run Options* tab > *Launch Scripts* page)

Application Launcher executes the scripts in the following order:

1. Run Before Launching script executed
2. Run Before Distribution script executed
3. Application distributed (files copied, settings modified, etc.)
4. Run After Distribution script executed
5. Application launched
6. Application closed (by user)
7. Run After Termination script executed

Supported Novell Client Login Script Commands

When using the Novell Client as the script engine, you can use all but the following script commands:

Table 48-1 Supported Novell Client Login Script Commands

CLS	INCLUDE	PCOMPATIBLE
DISPLAY	LASTLOGINTIME	SCRIPT_SERVER
EXIT	NO_DEFAULT	SET_TIME
FDISPLAY	NOSWAP	SWAP
IF MEMBER OF	PAUSE	WRITE

Application Launcher does not output anything to the screen or display script errors.

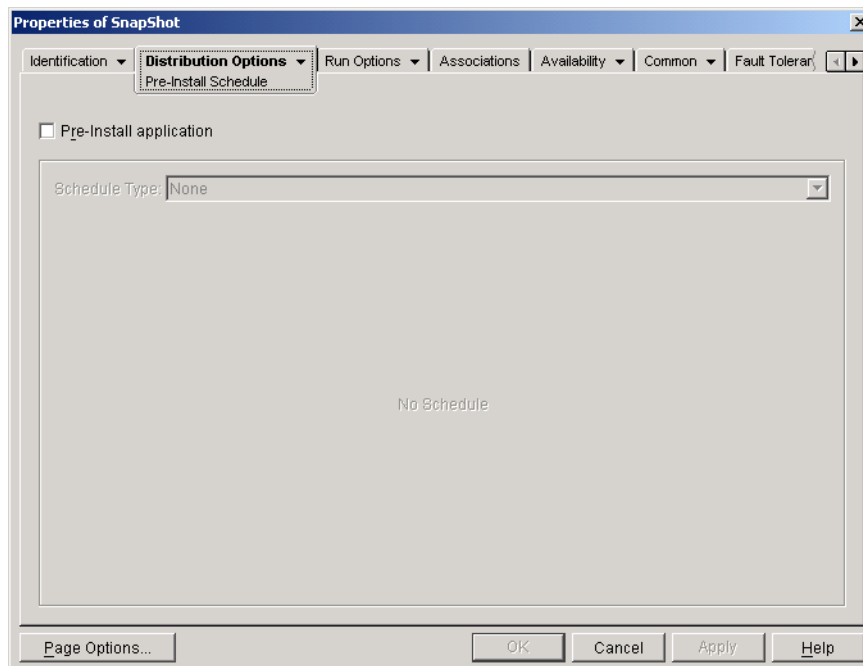
For script commands, syntax, and examples, see the [Novell Client documentation \(http://www.novell.com/documentation/lg/noclienu/docui/index.html\)](http://www.novell.com/documentation/lg/noclienu/docui/index.html) on the [Novell Documentation Web site \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

48.2.7 Pre-Install Schedule Page

The Pre-Install Schedule property page is available only on Application objects created for simple applications, AOT/AXT applications, and MSI applications. It is not available on Application objects created for Web applications and terminal server applications.

The Pre-Install Schedule property page, shown below, enables you to distribute portions of the application to a workstation before the user launches the application the first time. Because you can schedule the distribution, you can perform an off-line, or lights-out, distribution of the application and save the user some of the wait typically associated with a distribution. For example, you could pre-install the application after work hours so the application is ready to use the next day.

Figure 48-13 Application Object > Distribution Options Tab > Pre-install Schedule Page



With a pre-install, all workstation-related distribution processes (file copying, modifying text files, .ini files, and workstation registry settings) are performed prior to launching of the application. When the user launches the application, the user-specific distribution processes (modifying user registry keys and so forth) are completed.

You can pre-install an application that is associated with either workstations or users:

- For user-associated applications, the user must be logged in and Application Launcher must be running. Application Launcher uses the logged-in user's credentials (authentication and file system access) to distribute the application.
- For workstation-associated applications, the workstation must be running but Application Launcher does not need to be running. If the application is a non-MSI application (for example, an AOT application), NAL Workstation Helper uses the workstation's credentials to distribute the application. If the application is an MSI application, NAL Workstation Helper uses the logged-in user's credentials. If you want it to use the workstation's credentials rather than require a user to be logged in (for example, to perform a lights-out distribution of the MSI

application), you must enable the *Distribute in workstation security space if workstation associated* option (*Distribution Options* tab > *Options* page).

When pre-installing a workstation-associated application, you should also be aware of the following:

- Any shortcuts, registry settings, application files, INI settings, and text file modifications that are marked as *Track distribution per user* must also be marked as *Distribute always*. Otherwise, they are not distributed. To do so, use the *Track distribution per user* and *Distribute always* options on the **Icons/Shortcuts** page, **Registry** page, **Application Files** page, **INI Settings** page, and **Text Files** page.
- On Windows 2000/XP workstations, if a user is not logged in, any user-specific macros (*Common > Macros* page) point to the default user directories. This scenario affects the ability to place folders and icons on the Start menu. There are two ways to solve this issue: 1) Mark the macro entries in the Application object as *Track distribution per user* or 2) change the user-specific macro to an All Users macro (such as %*PROGRAMS% to %*COMMONPROGRAMS%).
- If an application requires a reboot during installation, you must select *Reboot if needed* or *Reboot always* in the Reboot group box and *Don't prompt* in the *Prompt for reboot* group box.

Pre-Install Application

Select this option to enable the application to be pre-installed. If you don't select this option, the application is not pre-installed, even if you establish a schedule.

Schedule Type

Select the type of schedule you want to use. You can choose *None*, *Specified days*, or *Range of days*.

None

Use this option to indicate no schedule. The application is pre-installed as soon as the application is associated with a user or workstation (*Associations* page).

Specified Days

Use this option to select specific dates when you want to pre-install the application. You cannot select more than 350 specific dates.

- **Date range:** The Date Range list displays all dates when the application can be pre-installed. To add a date, click *Add*, select the date you want, then click *OK* to display it in the list.
- **Time for selected dates:** Select the availability start time and end time. The times apply to all dates in the *Date range* list.

NOTE: The time increments in 5 minute intervals, with the earliest available start time being 00:00 (12:00 a.m.) and the latest end time being 23:55 (11:55 p.m.). This means there is always a 5-minute time period from 11:55 p.m. to 12:00 midnight when the application is unavailable. If you want the application to be available the entire day, you need to use the *Range of days* schedule type. For more information, see **“Range of Days” on page 545**.

- **Spread from start time (in minutes):** The *Spread from start time* option spreads out user access times over the number of minutes specified so the application doesn't become available to all users at the same time. If you anticipate all users launching the application as soon as it

becomes available and the application is being distributed or run from the network, you can use this option to avoid possible network overload.

For example, if you have a moderate number of users to whom the application is to be distributed (say about 100), you might specify a one-hour (60 minute) block of time (starting at the scheduled start time) to randomly distribute the application: thus all users will gain access to the application some time during the first sixty minutes after the scheduled start time.

If you want to substantially ease the load on your servers caused by the application distribution, or if you have bandwidth concerns, you might want to make the application distribute randomly throughout the time of availability. To spread out access times across the entire time (*Specified days* and *Time for selected dates*) that the application is available, use the total availability time specified for that application in terms of minutes. This will require that you make the maximum time available for each day you specify. For example, if an application is configured for a typical business day in the United States (9 hours per day: 8:00 a.m. to 5:00 p.m.), you calculate the total time of availability for that application like this:

Number of specified hours x 60 minutes per hour = Total availability time per day

Using this equation, the example above would be calculated like this:

9 x 60 (minutes per hour) = 540 minutes of availability

In this example, when you enter 540 minutes in the *Spread from start time* field, the application is distributed randomly for the entire 540 minutes that you have made it available on that scheduled day. Note that this might not be suitable for applications that must be distributed in a timely fashion, such as anti-virus updates. Note also that this is an example only: you can schedule the distribution for any specified amount of time for any day of the week.

Remember that the *Time for selected dates* setting makes the last five minutes of a day unscheduleable, so you need to consider these five minutes if the application schedule ends at 11:55 p.m. for that day.

Range of Days

Use this option to select a range of days to pre-install the application. You can also use this option to pre-install the application only on certain days of the week within a given range of dates.

- **Date range:** To define the range of days, select a start date and an end date > select the days (Sunday through Saturday) within the established date range. By default, all days are selected; a day is selected when the button appears to be pressed in.
- **Time for selected range:** Select the availability start time and end time. This option works differently depending on whether the date range includes one day, multiple days, or all seven days. If the date range includes one to six days (but not all seven days), the application is available between the start and end times on those days. For example, if you make the application available on Monday between 8:00 and 5:00, it is available during those hours. However, if the date range includes all seven days, the times are ignored and the application is available every day, 24 hours a day.
- **Spread from start time (in minutes):** The *Spread from start time* option spreads out user access times over the number of minutes specified so the application doesn't become available to all users at the same time. If you anticipate all users launching the application as soon as it becomes available and the application is being distributed or run from the network, you can use this option to avoid possible network overload.

For example, if you have a moderate number of users to whom the application is to be distributed (say about 100), you might specify a one-hour (60 minute) block of time (starting at

the scheduled start time) to randomly distribute the application: thus all users will gain access to the application some time during the first sixty minutes after the scheduled start time.

If you want to ease the load of the application distribution on your servers or if you have bandwidth concerns, you might want to make the application distribute randomly throughout the time of availability. To spread out access times across the entire time (*Date range* and *Time for selected dates*) that the application is available, use the total availability time specified for that application in terms of minutes. For example, if a workstation-associated application is configured for an entire 24-hour, three-shift day, you can calculate the total time of availability for that application like this:

Number of days in date range x *Time of availability per day* = Total availability time

Using this equation, and making sure to convert hours to minutes, the example above would be calculated like this:

7 (days) x 24 (hours) = 168 hours of availability

168 x 60 (minutes per hour) = 10,080 minutes of availability

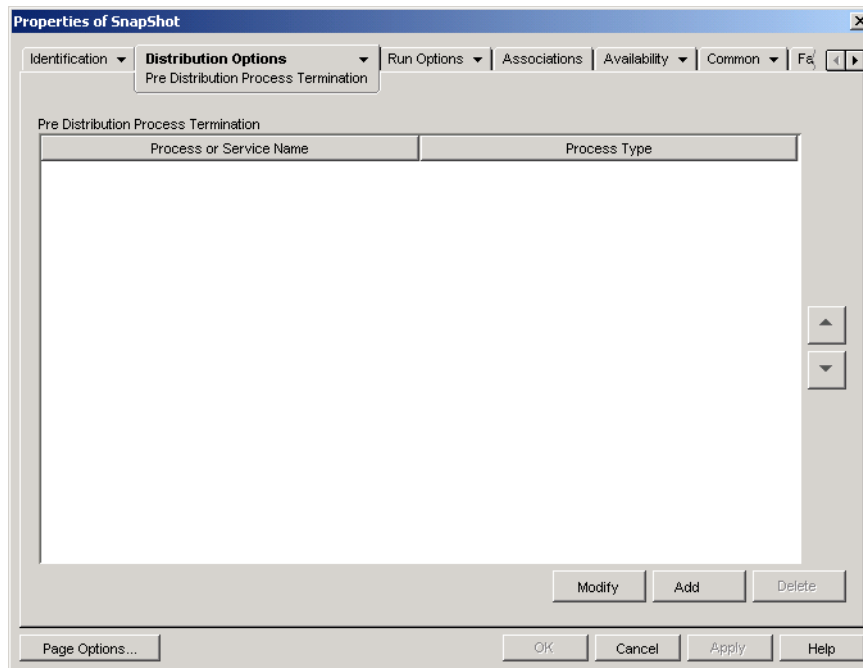
When you enter 10800 minutes in the *Spread from start time* field, the application is distributed randomly for the entire 10800 minutes that you have made it available. Note that this is not suitable for applications that must be distributed in a timely fashion, such as anti-virus updates.

- **Use this schedule in GMT for all clients:** The schedule is based on the workstation's time zone. If your network spans different time zones and you schedule an application to run at 1:00 p.m., it runs at 1:00 p.m. in each time zone. You can select this option to have workstations run applications at the same time regardless of their time zones (for example, 1:00 p.m. Rome time and 4:00 a.m. Los Angeles time).

48.2.8 Pre-Distribution Process Termination Page

The Pre-Distribution Process Termination property page, shown below, determines the executables and services that Application Launcher terminates before distributing the application to a workstation.

Figure 48-14 *Application Object > Distribution Options > Pre-distribution Process Termination Page*



Application Launcher can terminate any process running in the user space. In addition, it can terminate any service running in the system space (provided the service is displayed in the Microsoft Management Console's Services list and you use that service name). Application Launcher cannot terminate executables running in the system space.

When terminating a process, Application Launcher terminates all processes that match the specified filename. For example, if you specify `notepad.exe` as the process executable to terminate, all instances of `notepad.exe` terminate. In other words, if both `c:\notepad.exe` and `c:\winnt\notepad.exe` are running, both terminate. You cannot target specific instances of a process (for example, only `c:\notepad.exe` or `c:\winnt\notepad.exe`).

Add

This option lets you add processes to the list. Only processes displayed in the list are terminated before the application is distributed.

Click *Add* to display the Edit Processes dialog box. In the *Process* or *Service name* box, enter the executable (`.exe`) filename or enter the service name (as defined in the Services list in the Microsoft Management Console). Do not include the full file paths; if you do so, the termination fails.

Click *Service* if the process is a Windows service, then click *OK* to add the process to the *Pre-distribution process termination* list.

Modify

You can modify a process name and type. Select the process in the list, then click *Modify*.

Delete

Select the process you want to delete from the list, then click *Delete*.

Up-Arrow and Down-Arrow

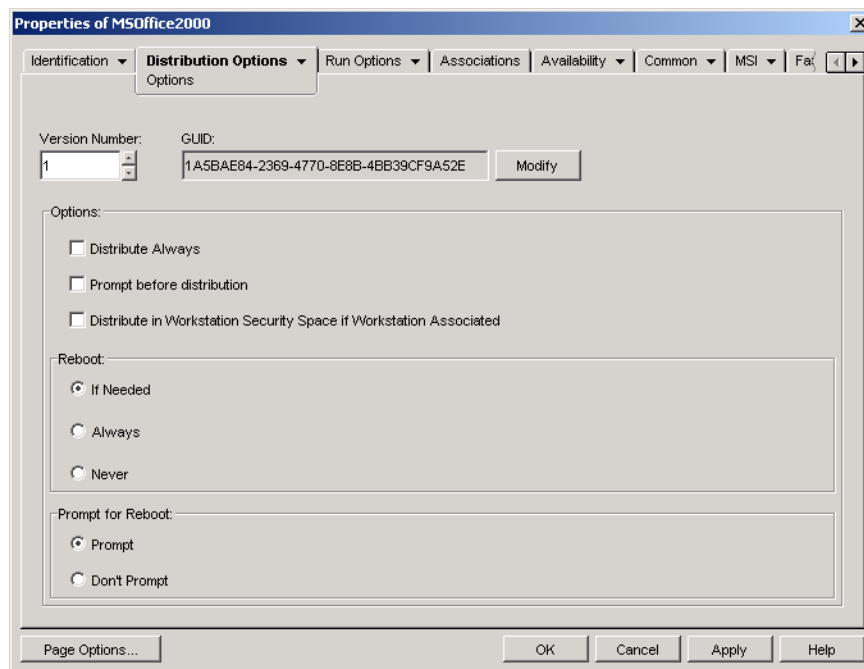
Select a process from the list, then click the up-arrow to move the process up in the list or click the down-arrow to move it down in the list. Application Launcher terminates the processes in the order they are listed, from top to bottom.

48.2.9 Options Page

The Options property page is available on Application objects created for all application types (simple, AOT/AXT, MSI, Web, and terminal server).

The Options property page, shown below, determines general options to be used by Application Launcher when distributing the application to a workstation.

Figure 48-15 *Application Object > Distribution Options Tab > Options Page*



GUID and Version Number

Application Launcher uses the application's GUID (global unique identifier) and version number to manage the distribution of the application. When Application Launcher distributes an application to a workstation, it adds the GUID and the version number to the workstation's Windows registry. If either the GUID or version number changes, Application Launcher redistributes the application.

The GUID is randomly generated when the Application object is created. In general, you should not need to change the GUID. There are, however, situations such as the following that might necessitate changing an application's GUID:

- The Application object is accidentally deleted from eDirectory. You re-create the Application object, but when you do so it is given a new, unique GUID. Because the new GUID causes the application to be redistributed to all users and workstations associated with the application, you use the GUID Manager (available by clicking the *Modify* button) to change the new GUID to the old GUID.
- You have multiple Application objects for the same application (to enable fault tolerance, load balancing, site lists, and so forth). You want to make sure that all Application objects have the same GUID so that the application is distributed one time only regardless of the Application object that is used. You use the GUID Manager to synchronize the GUIDs.
- Site 1 and Site 2 have the same applications chains. You must synchronize the GUIDs of each application in the chain at Site 1 with the GUIDs of each matching application at Site 2. Use the GUID Manager to synchronize the GUIDs.

The version number is a unique number between 0 and 65535 (0 is assigned when the Application object is first created) that you can increment as you make revisions to the Application object. If you make a change to the Application object's information, you should increment the version number so that Application Launcher redistributes the application. Application Launcher redistributes the application only if the new version number is larger than the current version number in the workstation's Windows registry.

Options

These options let you determine if Application Launcher should redistribute the application each time the application is run and if Application Launcher should prompt the user to accept or reject the distribution. The Options fields are not displayed on Application objects created for Web applications and Terminal Server applications because they do not apply

Distribute Always

By default, Application Launcher makes the distribution changes associated with the Application object at the following times:

- The first time the application is launched on a workstation.
- The first time the application is launched after the application's version number has been changed.

To force Application Launcher to redistribute the application each time it is launched, select *Distribute always*.

This option is useful to ensure that all application settings and files are updated every time the application runs. If the user has a NAL cache directory on his or her local machine, the files and settings are distributed from the NAL cache directory. If the user does not have a NAL cache directory (for example, the user is running Application Launcher through a terminal server client session) or if writing to the cache has been disabled for the user (User object > *ZENworks* tab > *Launcher Configuration* page > *Enable writing to cache* option), the application files and settings are updated from eDirectory. To force a distribution from eDirectory even if the user has a NAL cache directory on his or her local machine, you need to change the application's version number or have individual users right-click the Application object and click *Verify*.

If you need only specific files or settings to be distributed each time, you can update these on a case-by-case basis. For example, if you want to always distribute a particular registry key and value, you can set the *Distribute always* option on the Registry Settings page (*Distribution Options* tab) for that particular key and value.

Because this setting causes all application files and settings to be distributed each time, it overrides the *Distribute always* option on the Registry, INI Settings, Application Files, Icons/Shortcuts, and Text Files pages (**Distribution Options** tab).

Prompt Before Distribution

Select this option to prompt users to accept the distribution. Users are prompted the first time they click the application icon; all subsequent times they are not prompted. To better help users make a decision about installing the application, the prompt includes the text you've entered in the Description page (*Identification* tab).

Distribute in Workstation Security Space if Workstation Associated

The function of this option is conditional, based on whether you are configuring an MSI application or an AOT/Simple application.

If the application is an MSI: This check box is *not* selected by default. Workstation-associated MSI applications are normally distributed in the user security space, meaning that Application Launcher uses the user's credentials and file system access.

Select this option to instruct Application Launcher to distribute the application *in the workstation security space*. Application Launcher turns over distribution to the NAL Workstation Helper, which runs in the system space and uses the workstation's credentials. Using this option enables you to 1) do a lights-out distribution of the application and 2) better secure the application's source .msi files by giving the workstation, not the user, access to the source .msi files. Consider the following examples:

- You want to associate the application with a workstation and have it distributed before the user launches it. This is referred to as a lights-out distribution. To do so, you associate the application with the workstation on the Associations page (*Associations* tab), set the distribution schedule on the *Pre-Install Schedule* page (*Distribution Options* tab), and then enable this option. As long as the workstation is running at the scheduled distribution time, the NAL Workstation Helper distributes the application using the workstation security space rather than the user space normally used for installation of MSI applications.
- You want to distribute the application to a workstation but you don't want to give the user rights to the application's source files on the network. To do so, you associate the application with the workstation on the *Associations* page (*Associations* tab) and then select this option. When the user launches the application, Application Launcher calls NAL Workstation Helper. Workstation Helper distributes the application using the workstation security space.

It is important to remember that Application Launcher uses the workstation's credentials, not the user's credentials, to distribute the application. This means that you must assign the workstation the appropriate file system rights to access the network location where the source .msi files reside.

Not all MSI applications can be installed using this option. Some MSI applications have dependencies on a logged-in user (for example, to read and write to the HKCU hive in the Windows registry). In this situation, you must deselect this option in order to have the distribution occur in the user security space and not the workstation security space.

NOTE: If an application requires a reboot during installation, you must select *Reboot if needed* or *Reboot always* in the *Reboot* group box and *Don't prompt* in the *Prompt for reboot* group box.

If the application is an AOT or a simple application: This check box is selected by default. Workstation-associated AOT or simple applications are normally distributed in the workstation security space, meaning that Application Launcher uses the workstation's credentials and file system access.

Deselect this option to instruct Application Launcher to distribute the application *in the user security space*. Application Launcher then runs in the user space and uses the user credentials to distribute the files, even if the application is associated to the workstation.

Reboot

Select how a workstation reboot should occur. The available options are:

- **If needed:** Application Launcher reboots the workstation if changes need to be made that cannot occur while Windows is running (such as replacing open DLLs).
- **Always:** Application Launcher always reboots the workstation after distributing the application.
- **Never:** Application Launcher does not reboot the workstation. The changes take effect the next time the workstation reboots.

The NAL Service, which runs in the “system” space rather than the “user” space, distributes workstation-associated applications on Windows 2000/XP workstations. If you select the *Always* option, the NAL Service automatically reboots the workstation, even if you've set the *Prompt reboot* option to *Prompt* (see below); in other words, the NAL Service ignores the *Prompt reboot* setting. The same is true if you select the *If needed* option and a reboot is needed.

Prompt Reboot

Select whether or not the user is prompted to reboot the workstation. If you select *Prompt*, but deselect the *Show progress* option (*Identification* tab > *Icon* page), the user is not prompted (in other words, disabling the *Show progress* option overrides enabling the *Prompt reboot* option).

48.2.10 BITS Settings Page

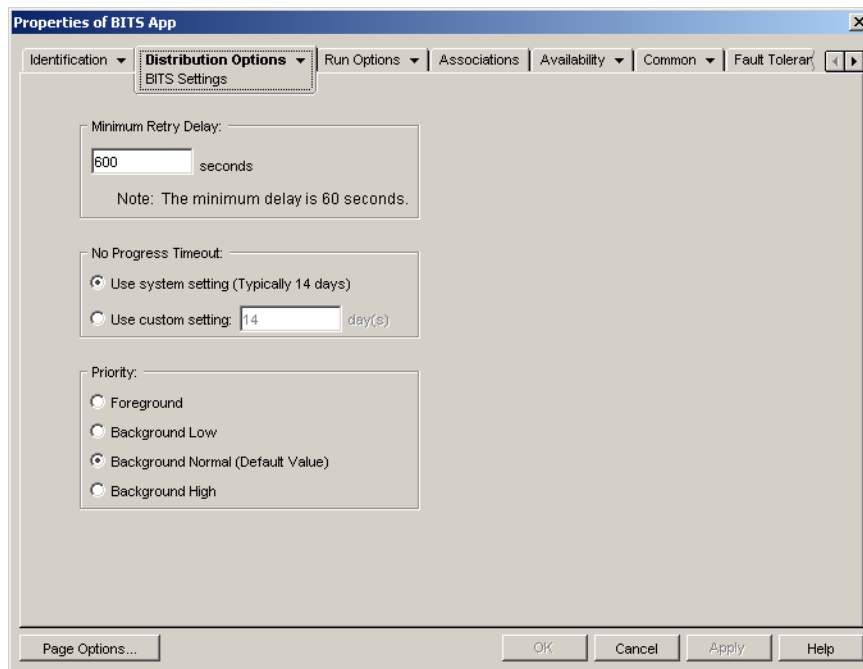
This functionality is available beginning with Support Pack 1 of Novell ZENworks 7.

The BITS Settings property page is available only on Application objects created for simple applications, AOT/AXT applications, and MSI applications. It is not available on Application objects created for Web applications and terminal server applications.

The BITS Settings page lets you configure the settings used by the Microsoft Background Intelligent Transfer Service (BITS) when transferring the application to a workstation. BITS is used only if

Novell Application Launcher and the application are configured to use BITS (see [Chapter 34, “Advanced Distribution: Transferring Applications Using BITS,”](#) on page 355).

Figure 48-16 *Application Object > Distribution Options Tab > BITS Setting Page*



Minimum Retry Delay

If BITS encounters an error during transfer of the application, BITS classifies it as a fatal error or a transient error. BITS cannot recover from fatal errors; fatal errors require administrator intervention to fix the problem. BITS can possibly recover from transient errors.

Use this option to specify the minimum amount of time you want BITS to wait after a transient error occurs before trying to transfer the application again. The default is 600 seconds, or 10 minutes. The minimum setting is 60 seconds. The maximum setting is 2,147,483,647 seconds.

No Progress Timeout

Use this option to specify how many days you want BITS to continue to attempt to transfer the application after a transient error has occurred if no progress is being made.

- **Use System Setting (Typically 14 Days):** Select this option to use the Windows system setting. The Windows system setting comes from either 1) the BITS default setting, which is 14 days, or 2) the Timeout (Days) for Inactive Jobs setting in the Windows Group Policy, which is undefined by default. If you select this option, the BITS default setting (14 days) is used unless the Windows Group Policy setting has been assigned a value. You can use the Windows Group Policy Editor (gpedit.msc) to view and change the Windows Group Policy setting.
- **Use Custom Setting:** Select this option to manually enter a timeout period.
 - The minimum setting is 0 days. Enter 0 only if you do not want BITS to attempt to transfer the application again after it encounters a transient error; in this case, BITS immediately returns control of the transfer to Application Launcher.

- The maximum setting is 24,855 days. However, BITS compares this number to the number in the Timeout (Days) for Inactive Jobs setting in the Windows Group Policy. If the Timeout (Days) for Inactive Jobs setting is less than this number, BITS uses the policy setting. For example, if you enter 45 days for this setting, but the policy is set to 30 days, BITS uses 30 days. If the Timeout (Days) for Inactive Jobs setting is undefined (the default state), the policy setting defaults to 90 days. In this case, for example, if you enter 91 days in this setting, BITS uses the policy setting (90 days).

If any transfer progress is made during the timeout period, the counter is reset. If BITS times out because no progress is being made, control of the transfer is returned to Application Launcher, which then transfers the application using its standard distribution process.

Priority

Use this option to assign a transfer priority level to the application. You can choose from one foreground priority and three background priorities (low, normal, high).

The foreground priority causes BITS to transfer the application in the foreground. Foreground transfers are the highest priority and are processed before any background transfers. Foreground transfers compete for network bandwidth with other applications, which can impede the user's network experience. Unless the timing of the transfer is critical or the user is actively waiting, you should use a background priority. In addition, BITS only supports foreground priority for files less than 2 GB.

For the three background priorities, the priority level determines when the transfer is processed relative to other transfers in the queue. Higher priority transfers preempt lower priority transfers. Transfers with the same priority level share transfer time, which prevents a large transfer from blocking the transfer queue. Lower priority transfers do not receive transfer time until all higher priority transfers are completed or are in an error state.

48.3 Run Options Tab

The Run Options tab includes the following pages to help you configure how the application runs on the workstation:

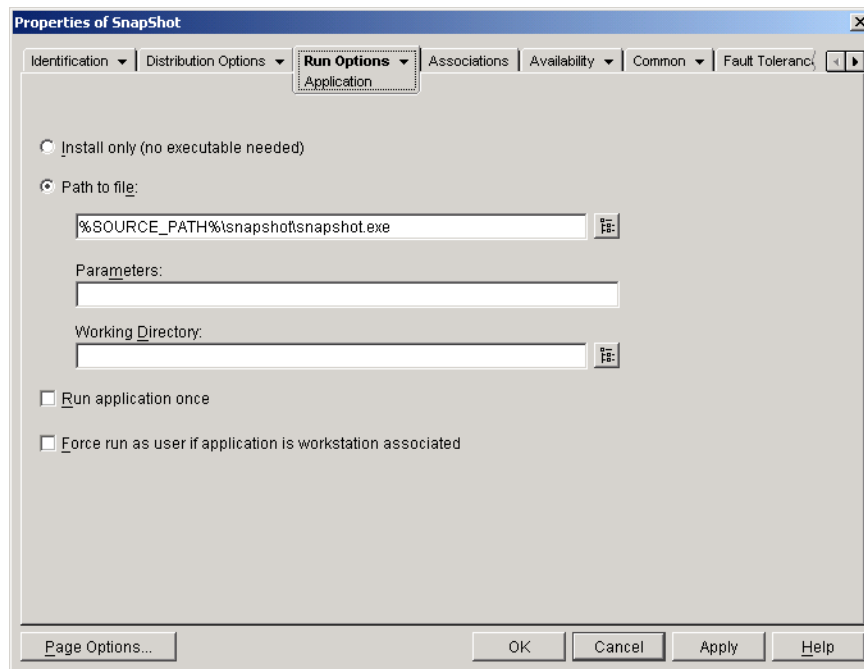
- [Section 48.3.1, "Application Page," on page 509](#)
- [Section 48.3.2, "Environment Page," on page 512](#)
- [Section 48.3.3, "Launch Scripts Page," on page 515](#)
- [Section 48.3.4, "Environment Variables Page," on page 518](#)
- [Section 48.3.5, "Web URL," on page 519](#)
- [Section 48.3.6, "License/Metering Page," on page 520](#)
- [Section 48.3.7, "Application Dependencies Page," on page 521](#)

48.3.1 Application Page

The Application property page is available only on Application objects created for simple applications, AOT/AXT applications, and MSI applications. It is not available on Application objects created for Web applications and terminal server applications.

The Application property page, shown below, determines general options to be used by Application Launcher when running the application on a workstation.

Figure 48-17 *Application Object > Run Options Tab > Application Page*



Install Only (No Executable Needed)

Select this option if the distribution does not include an executable file for Application Launcher to launch after the distribution. For example, you would want to use this option if the Application object's only purpose is to update some files on the workstation, such as a driver or font, or to make modifications to some workstation settings, such as the registry settings.

Path to File

Enter, or browse for, the path to the executable that Application Launcher runs after the application is distributed. Typically, this path is defined when you create the Application object and should already contain the path to where the executable is located on the network or where it is located on the user's workstation after distribution. If you enter the path, make sure to include the `.exe` extension on the application executable filename (for example, enter `notepad.exe`, not `notepad`).

IMPORTANT: The ZENworks Desktop Management Agent and Middle Tier Server do not support launching of applications from a network location. If the executable is located on the network, you should only use this option if users have a network client (Novell Client or Microsoft Client for Networks) installed that enables launching from a NetWare[®], Linux, or Windows server.

You can also enter the path for a file type other than `.exe`. If you do so, when the user double-clicks the Application object, Application Launcher passes the file to the Windows system, which can then use the application associated with that file type to open the file. For example, if you entered a `.txt` file, the application associated with `.txt` files would be used to open the file.

You can use a mapped drive or a UNC path. The following path syntaxes are valid:

```
server\volume:path  
\\server_name\volume\path  
\\IP_address\volume\path  
volume_object_name:path  
directory_map_object_name:path  
driveletter:\path
```

If you use a UNC path, applications running on Windows 2000 servers might launch slowly because of the way Windows resolves UNC paths. For more information, see [Microsoft Knowledge Base Article Q150807](http://support.microsoft.com/support/kb/articles/Q150/8/07.asp) (<http://support.microsoft.com/support/kb/articles/Q150/8/07.asp>).

You can also use macros in this field. For information about macros, see [Chapter 49, “Reference: Macros,” on page 585](#).

Parameters

Specify any command line parameters that need to be passed to the executable specified in the *Path to file* field. The field limit is 250 characters.

Application Launcher simply passes the parameters exactly as they are entered. Therefore, the parameter syntax you use must exactly match the syntax the executable requires. For example, if `word.exe` has a `/f=filepath` parameter that requires paths with spaces to be enclosed in quotation marks, you would enter the following:

```
/f="c:\my docs\sample.doc"
```

Working Directory

Specify the working directory of the executable you specified in the *Path to file* field. Typically, this is the directory in which the executable file is located. However, if another directory contains additional files required by the application to run, specify that directory. See your Windows documentation for more information.

The following path syntaxes are valid:

```
server\volume:path  
\\server\volume\path  
volume_object_name:path  
directory_map_object_name:path  
driveletter:\path
```

You can also use macros in this field. For information about macros, see [Chapter 49, “Reference: Macros,” on page 585](#).

Run Application Once

Select this option to have Application Launcher run the application one time only and then remove the Application object’s icon from the workstation. If the Application object’s version number (*Distribution Options > Options* page) changes, the Application object icon appears again so that the new version can be distributed.

This option can be useful when an Application object’s only purpose is to install software to a workstation. Having the Application object’s icon remain after the application has been installed can

be confusing to users, especially if you have an application shortcut or program group icon created during the distribution (see the *Distribution Options > Icons/Shortcuts* page).

This option can also be used in combination with other Application object settings. For example, if the application is specified as *Force run* on the Associations page (meaning that without any user involvement, the application runs when it becomes available to Application Launcher), the application is forced to run only one time.

Force Run As User If Application Is Workstation Associated

With workstation-associated applications that are marked as *Force run* (*Associations* tab > *Associations* page), the Workstation Helper launches the application as soon as the workstation is started, typically before the user has logged in to Windows. This means that the only workstation-associated applications you would want to force run would be applications that don't require user interaction.

Select this option if you want to delay the force running of a workstation-associated application until Application Launcher starts. In this case, Application Launcher, not Workstation Helper, distributes and launches the application. Application Launcher uses the workstation's file system rights to distribute the application and the user's file system rights to launch it.

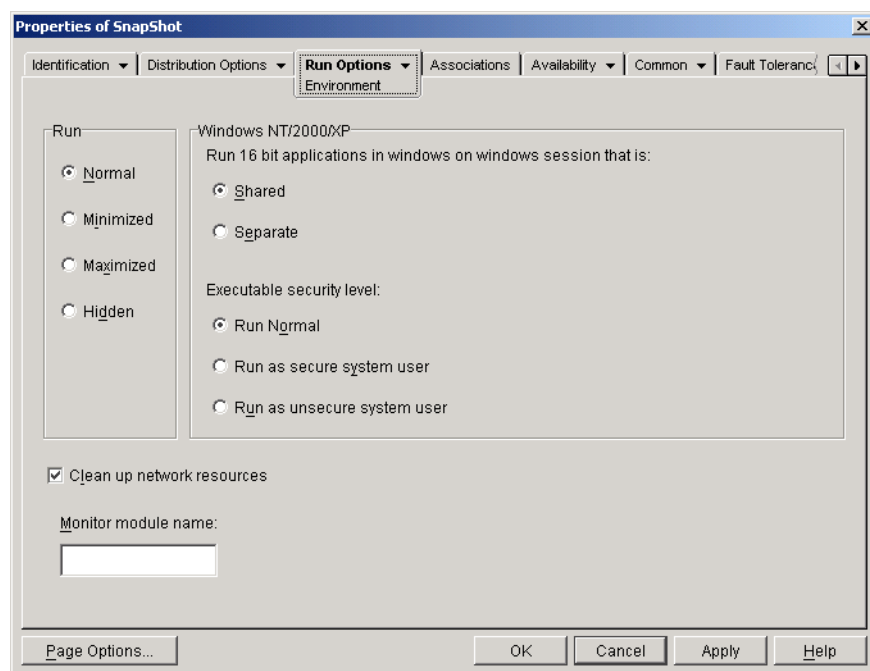
Basically, this option enables workstation-associated applications that you are force running to function the same as user-associated applications that you force run.

48.3.2 Environment Page

The Environment property page is available only on Application objects created for simple applications, AOT/AXT applications, and MSI applications. It is not available on Application objects created for Web applications and terminal server applications.

The Environment property page, shown below, defines the environment in which Application Launcher runs the application.

Figure 48-18 *Application Object > Run Options Tab > Environment Page*



Run

Select the application's initial window size: Normal, Minimized, Maximized, or Hidden. In Hidden mode, the application runs normally without a user interface available. This is useful if you want the application to process something then go away without user intervention. For example, you could use it for the Remote Control agent if you don't want it to appear in the taskbar.

NOTE: Some applications cannot be run in Minimized, Maximized, or Hidden mode. Depending on the application, the initial window size setting might be ignored. For example, `calc.exe` cannot be run in Hidden mode.

Windows NT/2000/XP

Use these options to specify how the application runs on Windows 2000/XP workstations.

Run 16-Bit Applications in Windows on Windows Session That Is

If you are setting up a 16-bit application to run on Windows 2000/XP, specify either a shared or separate Windows on Windows (WOW) session. To run on Windows 2000/XP, 16-bit applications must run in a Virtual DOS Machine (VDM) that emulates Windows 3.1 functionality. 16-bit Windows applications can run in their own separate WOW sessions or they can share a WOW session with other 16-bit applications. Sharing a WOW session saves memory and allows applications to use DDE or OLE to communicate with other applications in the same WOW session. Running an application in its own separate WOW session allows for more robust operation because the application is isolated from other 16-bit applications. Because some applications do not run

properly in a separate WOW session, the default option is to run the 16-bit Windows application in a shared WOW session.

Executable Security Level

On Windows 2000/XP, the application executable (as defined in the *Path to file* field on the **Application Page**) can run in either the “user” space or the “system” space. By default, the *Run normal* option is selected, which causes the application to run in the “user” space and inherit the same workstation security level as the logged-in user.

If the logged-in user's security level does not provide sufficient rights and file access to run the application, you can configure the application to run in the “system” space. The two “system” space options, as well as the *Run normal* (“user” space) option are described below:

- **Run normal:** The application inherits the logged-in user's credentials. For example, the application has the same rights to the registry and the file system as the logged-in user.
- **Run as secure system user:** The application is run under the Local System user and inherits Administrator-level credentials. For example, the application has full rights to the registry and the file system. Because the security level is set to *Secure*, the application's interface is not displayed to the user and the application is only visible in the Task Manager. This option is useful when running applications that require full access to the workstation but require no user intervention, such as a service pack or update.
- **Run as unsecure system user:** This option is the same as *Run as secure system user*, with the exception that the application's interface is displayed to the user. This means that the application can display dialog boxes and prompt the user for information if necessary. In return, the user has the ability to do whatever that application offers on the workstation. For example, if you run REGEDIT as an unsecure system user, the workstation's user is able to edit any registry values.

In a terminal server environment, you should not use the *Run as secure system user* and *Run as unsecure system user* options if users are running Application Launcher in a terminal server client session. Doing so causes the NAL Service (running on the terminal server) to launch the application. Because the NAL Service runs as a System user, the launched application displays only in the terminal server's Task Manager (for *Run as secure system user*) or on the terminal server's desktop (*Run as unsecure system user*). It does not display in the users' terminal server client sessions.

Clean Up Network Resources

Select this option to remove network connections, drive mappings, and port captures that were established for running the application. If this option is not selected, the network resources remain in effect. If the resource is already in use when Application Launcher starts the application, it is not cleaned up until all other distributed applications are finished using it. If distributed applications are still running when Application Launcher is terminated, the allocated resources remain intact.

Monitor Module Name

When an application is launched, Application Launcher monitors the executable of the application. When the executable terminates, the process of cleaning up network resources begins. However, it's possible that the executable filename is actually a “wrapper” that sets up environments, runs other executables, and then terminates. If Application Launcher monitors the wrapper executable, it might prematurely start cleaning up network resources before the application has terminated. Consult your application documentation about whether the application uses a wrapper executable. If it does, find

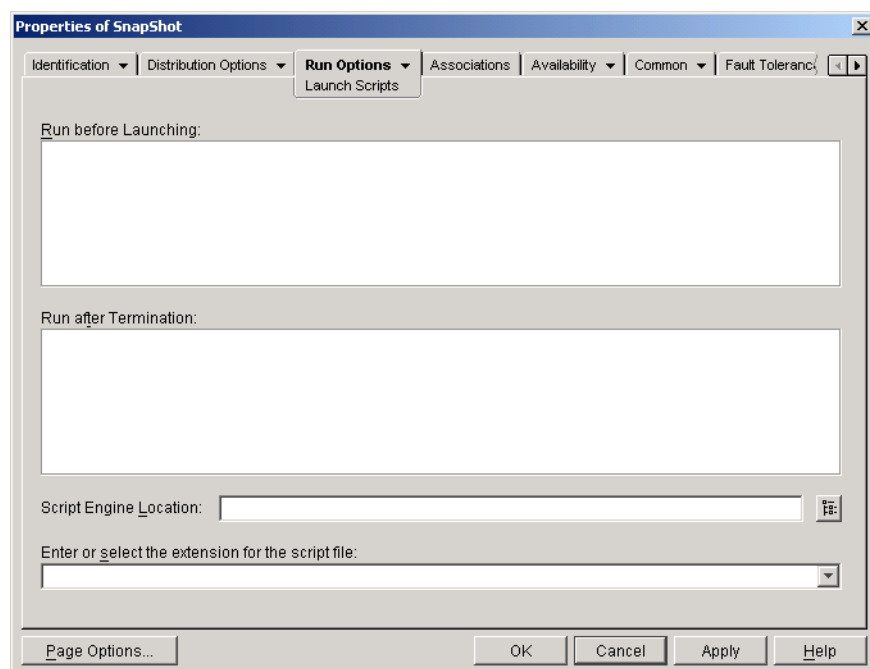
out the name of the module that remains running. Type this name (without the extension) in the text box provided.

48.3.3 Launch Scripts Page

The Launch Scripts property page is available on Application objects created for simple applications, AOT/AXT applications, and MSI applications only. It is not available on Application objects created for Web applications and terminal server applications.

As part of the process of launching the application, Application Launcher can launch a script engine to execute a “before launch” script and an “after termination” script (for details about the order of script execution, see [“Script Execution Order” on page 517](#)). The Launch Scripts property page, shown below, defines the script engine that you want Application Launcher to use and the scripts you want executed.

Figure 48-19 *Application Object > Run Options Tab > Launch Scripts Page*



On Windows 2000/XP, launch scripts always run in the user space, meaning that they inherit the file system rights assigned to the logged-in user. This is true even if the application's executable is configured to run in the system space (*Run Options* tab > *Environment* page > *Executable security level* option). This behavior is different than the behavior for distribution scripts (*Distribution Options* tab > *Distribution Scripts* page), which run in the secure system space.

Run Before Launching

Use this text window to enter any script commands you want executed before launching the application. Do not use extended characters in the script; extended characters are not supported.

For a script example, see [“Script Example” on page 516](#).

Run After Termination

Use this text window to enter any script commands you want executed after the user closes the application. Do not use extended characters in the script; extended characters are not supported.

For a script example, see [“Script Example” on page 516](#).

The *Run after termination* script is executed before the network resources are cleaned up (*Run Options > Environment* page). However, the *Clean up network resources* option does not clean up drive mappings or port captures created by the *Run before launching* script. To clean up these resources, enter the appropriate commands in the *Run after termination* script.

Script Engine Location

The script engine determines the script commands and scripting language you need to use. If you do not define a script engine in the *Script engine location* field, Application Launcher uses the Novell Client as the script engine (if the workstation has the Novell Client installed), which means that you can use most Novell Client login script commands (see [“Supported Novell Client Login Script Commands” on page 498](#)).

If you want to use a script engine other than the Novell Client, specify the script engine. The script engine must reside in a location that is always available to users, such as their local drives. The script engine can reside on a network server only if users can map a drive to the server (for example, through the Novell Client or the Client for Microsoft Networks). If Application Launcher cannot find the script engine, it displays an error to the user and fails to launch the application.

If you use the Windows command interpreter as the script engine, you must include the `/c` switch, as shown in the following examples:

- Windows 2000/XP: `%*winsysdir%\cmd.exe /c`
- Windows 98: `%*windir%\command.com /c`

The `%*winsysdir%` and `%*windir%` variables specify the Windows system directory (for example, `c:\winnt\system32`), and the `/c` switch instructs the command interpreter to execute the script and then stop. If the `/c` switch is not used, the script does not complete.

For a script example, see [“Script Example” on page 516](#).

Script File Extension

This applies only if you specified a script engine in the *Script engine location* field.

When the application is launched, Application Launcher creates temporary script files for the *Run before distribution* scripts and *Run after distribution* scripts. These files are passed to the script engine, which then executes the script. You need to specify the file extension that the script engine requires for its script files.

For a script example, see [“Script Example” on page 516](#).

Script Example

The following script uses the Windows 2000/XP command interpreter as the script engine. Before the launch occurs, a listing of the `c:\` directory is saved to a text file and the `autoexec.bat` file is backed up.

Run Before Distribution Field

```
dir c:\ >c:\1.txt  
copy autoexec.bat autoexec.bak /y
```

Script Engine Location Field

```
cmd.exe /c
```

Enter or Select the Extension of the Script File Field

```
.bat
```

Script Execution Order

Application Launcher can execute up to four different scripts when distributing and launching an application:

- **Distribution scripts:** *Run before distribution* and *Run after distribution* (*Distribution Options* tab > *Distribution Scripts* page)
- **Launch scripts:** *Run before launching* and *Run after termination* (*Run Options* tab > *Launch Scripts* page)

Application Launcher executes the scripts in the following order:

1. Run Before Launching script executed
2. Run Before Distribution script executed
3. Application distributed (files copied, settings modified, etc.)
4. Run After Distribution script executed
5. Application launched
6. Application closed (by user)
7. Run After Termination script executed

Supported Novell Client Login Script Commands

When using the Novell Client as the script engine, you can use all but the following script commands:

Table 48-2 *Supported Novell Client Login Script Commands*

CLS	INCLUDE	PCOMPATIBLE
DISPLAY	LASTLOGINTIME	SCRIPT_SERVER
EXIT	NO_DEFAULT	SET_TIME
FDISPLAY	NOSWAP	SWAP
IF MEMBER OF	PAUSE	WRITE

Application Launcher does not output anything to the screen or display script errors.

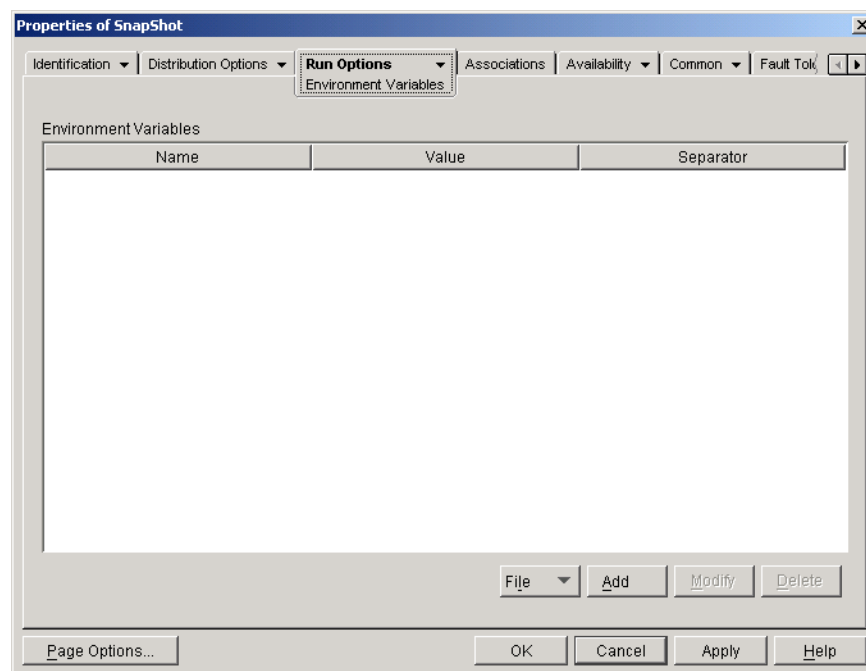
For script commands, syntax, and examples, see the [Novell Client documentation \(http://www.novell.com/documentation/lg/noclienu/docui/index.html\)](http://www.novell.com/documentation/lg/noclienu/docui/index.html) on the Novell Documentation Web site (<http://www.novell.com/documentation>).

48.3.4 Environment Variables Page

The Environment Variables property page is available only on Application objects created for simple applications, AOT/AXT applications, and MSI applications. It is not available on Application objects created for Web applications and terminal server applications.

The Environment Variables property page, shown below, specifies the environment variables that Application Launcher sets before running the application. For example, you can specify the application's working directory in the PATH environment variable.

Figure 48-20 *Application Object > Run Options Tab > Environment Variables Page*



IMPORTANT: On Windows 98 workstations, Application Launcher cannot set environment variables if the Novell Client is not installed. This is not an issue on Windows 2000/XP workstations.

Environment Variables

The Environment Variables list displays all variables that are modified before the application is run. Application Launcher modifies only the variables in this list.

File

This option lets you search for variables or variable data in the *Environment variables* list and import variables from another Application object into the tree.

Click *File*, then choose one of the following options:

- **Find:** Searches for variables or variable data in the *Environment variables* list.
- **Find next:** Finds the next occurrence of the item specified by the initial search.
- **Import:** Imports variables from another Application object's .aot or .axt file. The Open dialog box defaults to *.axt for its file type display. If you are importing from an .aot file, you must change the file type display to *.aot or *All files* in order to select the .aot file.

Add

To add a variable to the *Environment variables* list, click *Add* to display the Edit Environment Variables dialog box, specify the variable name and data, select *Append to existing data using separator character* (only if you want to append the data to the workstation's existing variable) and enter a separator character, then click *OK*.

Modify

In the Environment Variables list, select the variable you want to modify, then click *Modify*.

Delete

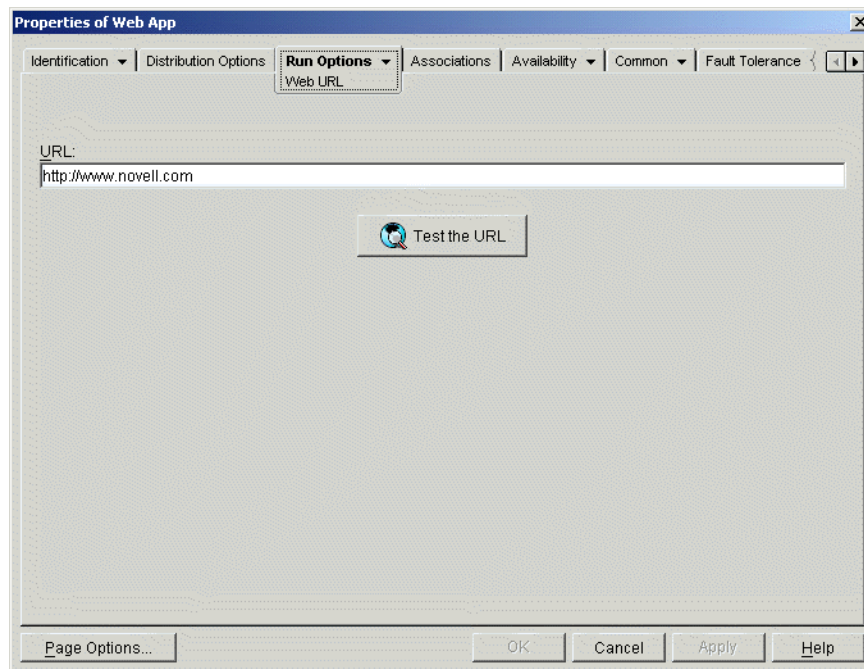
In the Environment Variables list, select the variable you want to delete, then click *Delete* to remove it from the list.

48.3.5 Web URL

The Web URL property page is available on Application objects created for Web applications only. It is not available on Application objects created for simple, AOT/AXT, MSI, and terminal server applications.

The Web URL property page, shown below, specifies the location (URL) of the Web application.

Figure 48-21 Application Object > Run Options Tab > Web URL Page



URL

This field defaults to the URL you entered when creating the Application object. The URL should point to the primary file for the Web application or to a Web page that allows access to the Web application. If necessary, you can modify the URL.

Test the URL

Click this button to launch the Web application. The current workstation must have a Web browser installed for this functionality to work.

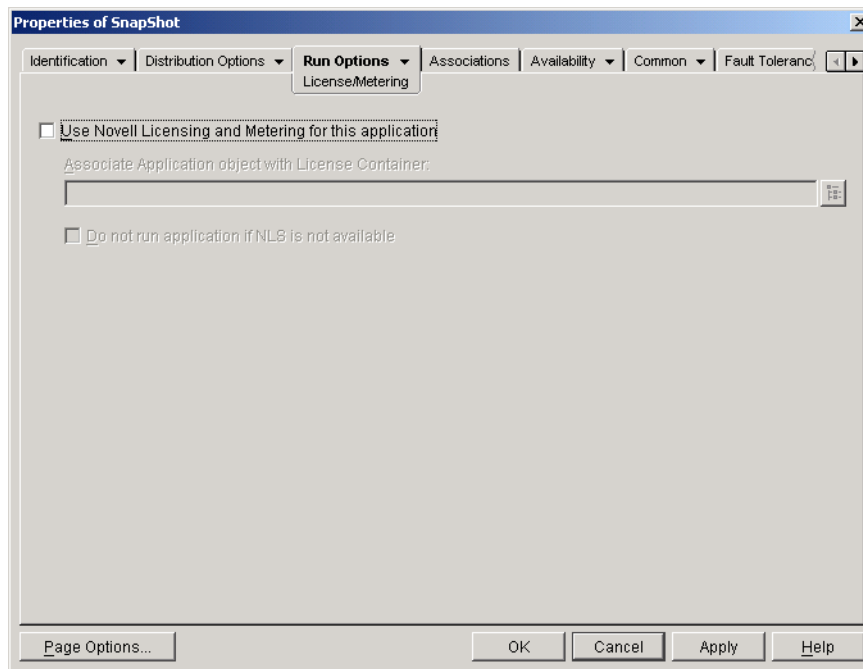
48.3.6 License/Metering Page

The License/Metering property page is available on Application objects created for all application types (simple, AOT/AXT, MSI, Web, and terminal server).

The License/Metering property page, shown below, configures Application Launcher to use Novell Licensing Services to track application usage and comply with the application's licensing agreement. Novell Licensing Services must already be installed, you must have created a License Container and a Metered Certificate for the application, and users' workstations must be running the

Novell Client. For detailed information about setting up license metering, see [Chapter 45, “Metering Software Licenses,”](#) on page 459.

Figure 48-22 *Application Object > Run Options Tab > License/metering Page*



Use Novell Licensing and Metering for this Application

Select this option to enable metering of the application.

Associate Application Object with License Container

After metering is enabled, select the License Container in which you’ve created the application’s Metered Certificate.

Do Not Run Application if NLS Is Not Available

Select this option to prevent users from running the application if Novell Licensing Services is not running.

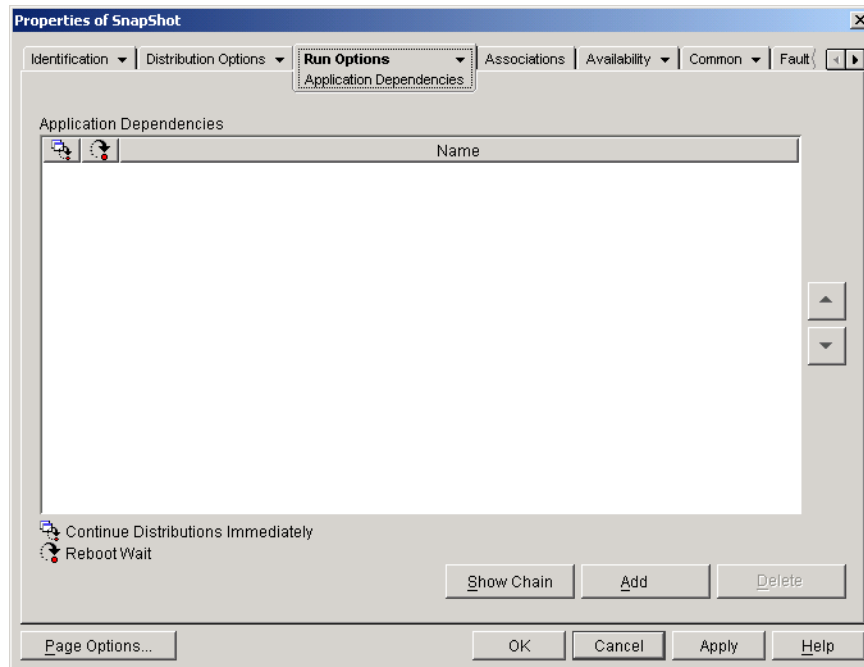
48.3.7 Application Dependencies Page

The Application Dependencies property page is available on Application objects created for all application types (simple, AOT/AXT, MSI, Web, and terminal server).

This section provides information about the fields located on the Application Dependencies property page. For complete instructions on setting up application dependencies, see [“Advanced Distribution: Configuring Application Dependencies and Chains”](#) on page 389.

The Application Dependencies property page, shown below, lets you create a list of applications (referred to as dependent applications) that must be distributed and launched before this application (referred to as the primary application) is distributed and launched.

Figure 48-23 *Application Object > Run Options Tab > Application Dependencies Page*



You can specify one or more dependent applications. For example, assume that the primary application (Application A) is dependent on three other applications (Application B, Application C, and Application D). By adding all three applications to the Application Dependencies list on this page, Application Launcher ensures that all three dependent applications are distributed and launched before running Application A.

A dependent application can be a single application or it can be an application chain. An application chain exists when a dependent application is dependent on additional applications. Continuing the above example, if Application C is dependent on Application C1 and Application C2, then Application B, C, C1, C2, and D must all be distributed and launched before Application A is distributed and launched.

When setting up application dependencies, you should be aware of the following:

- **Distribution:** Novell Application Launcher only distributes a dependent application the first time the user launches the primary application, unless the dependent application's version is updated (Application object > *Distribution Options* tab > *Options* page) or the distribution is unsuccessful. If Application Launcher is unable to distribute a dependent application (for example, the user's workstation does not meet the dependent application's system requirements), the primary application is not distributed or launched.
- **Distribution through removable media:** If you distribute the primary application through removable media such as a CD (see [“Distributing Applications Via Removable Media” on page 411](#)) or through an image add-on (see [“Imaging Page” on page 559](#)), its dependent applications must be included on the removable media or as another image add-on.

- **Distribution to disconnected workstations:** For workstations running in disconnected mode, the applications must be force cached to the workstation before it becomes disconnected (or they must be distributed through removable media). If changes are made to dependent applications after the applications have been cached to workstations, the version number of the primary application must be updated in order to force a re-cache of the applications.
- **Launch:** Application Launcher launches a dependent application each time the primary application is launched. During launching, Application Launcher executes the dependent application's pre-launch and post-launch scripts, and then launches the dependent application. If a dependent application, such as a setup program, should be run only one time, you should configure the dependent application to run once (Application object > *Run Options* tab > *Application* page).
- **Uninstall:** If you uninstall the primary application (*Common* tab > *Uninstall* page or *Associations* tab > *Associations* page), all dependent applications that are not used by another application are also uninstalled.

Application Dependencies List

The Application Dependencies list displays the applications that the primary application has a dependency on. The order in which the dependent applications are listed, going from bottom to top, is the order in which they are distributed and launched on the user's workstation when the primary application is launched.

Add

To add an application to the list, click *Add*, browse for and select the Application object, then click *OK*. After the application is added to the list, you can modify the following two attributes:

- **Continue distributions immediately:** Select this option if you want Application Launcher to distribute and run the application but not wait for the application to finish running before continuing with the next application distribution.

If this option is not selected (the default), Application Launcher waits until it has distributed and run the application before continuing with the distribution of the next application in the list. Application Launcher only continues after all files, registry settings, and so forth have been distributed and the application (or file) listed in the *Path to file* field (*Run* tab > *Application* page) has been run and completed.

- **Reboot wait:** If distribution of the application requires the workstation to be rebooted, select this option to have Application Launcher postpone the reboot until 1) it distributes another application in the list that requires a reboot (and doesn't have this option selected) or 2) it has distributed all applications in the list. This option also applies when uninstalling the application.

Delete

To remove a dependent application from the list, select the application in the list, then click *Delete*.

Show Chain

To see whether or not a dependent application consists of an application chain, select the dependent application in the list, then click *Show chain*.

Up-Arrow and Down-Arrow

The order in which the dependent application are listed is the order in which they are distributed and launched, going from bottom to top. You can use the up and down arrows to change the order.

48.4 Associations Tab

The Associations tab includes only one page. This page lets you associate the Application object with users and workstations.

- [Section 48.4.1, “Associations Page,” on page 524](#)

48.4.1 Associations Page

The Associations property page is available on Application objects created for all application types (simple, AOT/AXT, MSI, Web, and terminal server).

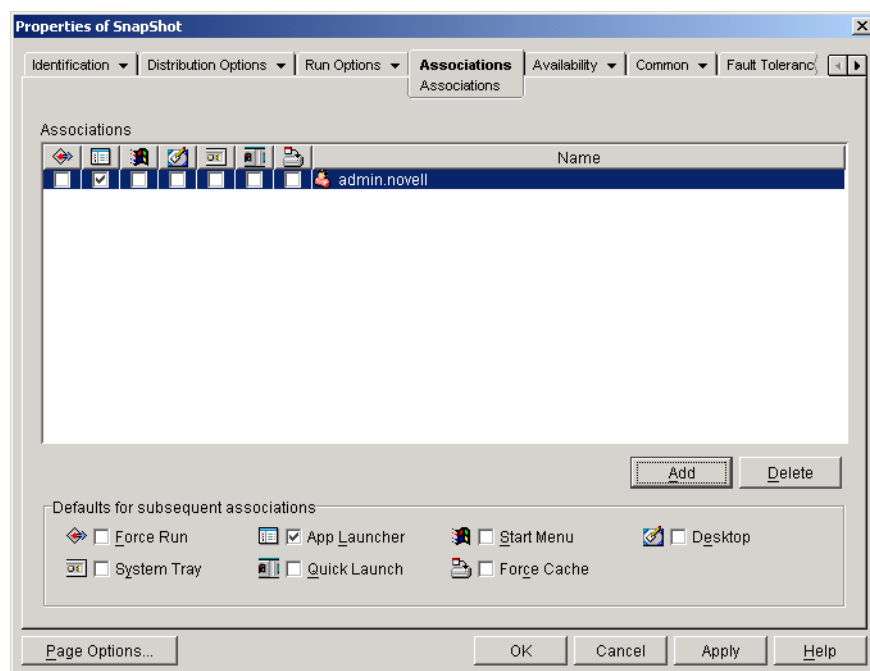
The Associations property page, shown below, lets you associate the Application object with the users and workstations to which you want the application distributed.

You can associate the Application object with individual users or workstations by selecting the appropriate User or Workstation objects. You can also associate it with groups of users or workstations by selecting Group, Workstation Group, Organizational Unit, Organization, and Country objects.

NOTE: Associating an Application object with a Group, Workstation Group, or other container object is the preferred method of associating the Application object in eDirectory. Associating the application to a large number of User or Workstation objects (for example, more than 250) might cause increased server utilization.

Although you are not restricted from associating Application objects with Alias objects, do not do so; Alias objects are not a supported object for associations.

Figure 48-24 *Application Object > Associations Tab > Associations Page*



Associations

The *Associations* list displays the objects associated with the Application object and lets you add or delete objects.

Add

To associate an object with the Application object, click *Add*, browse and select the object, then click *OK*. All objects receive the default characteristics (*Force run*, *App Launcher*, *Start menu*, *Desktop*, *System tray*, *Quick launch*, *Force cache*) selected in the *Defaults for subsequent associations* list. After you add an object to the *Associations* list, you can modify its characteristics by selecting or deselecting the appropriate check boxes.

Delete

To disassociate an object from the Application object, select the object in the *Associations* list, then click *Delete*.

Defaults for Subsequent Associations

When you add an object to the Associations list, the object receives the default characteristics selected in this box. The characteristics determine the locations (*App Launcher*, *Start Menu*, *Desktop*, *System Tray*, and *Quick Launch*) where the Application object's icon are displayed and the actions (*Force run* and *Force cache*) that are performed on the application. If you change the characteristics that are selected, any objects you add after that receive the new characteristics.

Force Run

Automatically runs the application. With a user-associated application, the application is run immediately after Application Launcher starts. With a workstation-associated application, the application is run immediately after the workstation starts up (initial startup or reboot).

You can use the *Force run* option in conjunction with several other settings to achieve unique behaviors. For example, if you use the *Force run* option with the *Run application once* option (*Run Options* tab > *Applications* page), as soon as the Application object is distributed it is run one time and then removed from the workstation. Or, suppose that you want to run the Application object immediately one time at a pre-determined time. If so, select *Force run*, select the *Run application once* option on the *Application* page (*Run Options* tab), and define a schedule using the *Schedule* page (*Availability* tab).

If you want to force run several applications in a specific order, mark each of them as *Force run*. Then give each Application object a numeric order by using the *Order icon display* option on the *Icon* page (*Identification* tab).

IMPORTANT: When using the *Force run* option for an MSI application associated with a workstation, you must also turn on the *Distribute in workstation security space if workstation associated* option (*Distribution Options* tab > *Options* page) and assign the workstation the appropriate file system rights to access the network location where the source .msi files reside. Otherwise, the distribution and subsequent forced running of the application fails.

If an application requires a reboot during installation, you must select *Reboot if needed* or *Reboot always* in the *Reboot* group box and *Don't prompt* in the *Prompt for reboot* group box.

App Launcher

Adds the Application object's icon to the Application Window, the Application Explorer window, and the Application Browser window.

Start Menu

If the workstation is running Application Explorer, this option adds the Application object to the Windows Start menu. The Application object is added to the top of the Start menu, unless you assign the Application object to a folder and use the folder structure on the Start menu. See the Application object's Folders page (*Identification* tab).

Desktop

If the workstation is running Application Explorer, this option displays the Application object's icon on the Windows desktop.

System Tray

If the workstation is running Application Explorer, this option displays the Application object's icon in the Windows system tray.

Quick Launch

If the workstation is running Application Explorer, this option displays the Application object's icon on the Windows Quick Launch bar.

Force Cache

This option applies only if the Application object is marked as disconnectable (*Identification* tab > *Icon* page).

Without *Force cache* enabled, users can launch the application while in disconnected mode as long as the application has already been distributed (installed) to the workstation. With *Force cache* enabled, Application Launcher automatically copies the application source files and other files required for distribution to the workstations cache directory. The user can then install or repair the application while disconnected from Novell eDirectory. The files are compressed to save space on the workstation's local drive. For more information about caching applications, see [Chapter 39, “Users: Supporting Disconnected Users,” on page 401](#).

When distributing an MSI application, you must use the *Force cache* option if users or workstations do not have network client access to the source .msi files. The Microsoft Windows Installer requires file access that is provided by a network client but not by the ZENworks Desktop Management Agent. Consider the following examples:

- Users outside your firewall need an MSI application but have no network client access to the source .msi files on a server inside your firewall. They log in to the ZENworks Middle Tier Server and Application Launcher displays the MSI application. For successful distribution to occur, the MSI application must be marked as *Force cache* so that the source .msi files are copied to the user's cache directory (through the Middle Tier Server) and then distributed from the cache directory.
- Users inside your firewall need an MSI application. They don't have the Novell Client installed, so they log in to the ZENworks Middle Tier Server to authenticate to eDirectory. The users are part of an Active Directory domain, and the source .msi files are located on a Windows share that they have rights to. The distribution succeeds without force caching the application because the Microsoft network client provides file access to the source .msi files.

48.5 Availability Tab

The Availability tab includes the following pages to help you define the rules for distributing the application to workstations, the days and times the application is available to users, and the messages and warnings Application Launcher displays to users when terminating an application that has become unavailable:

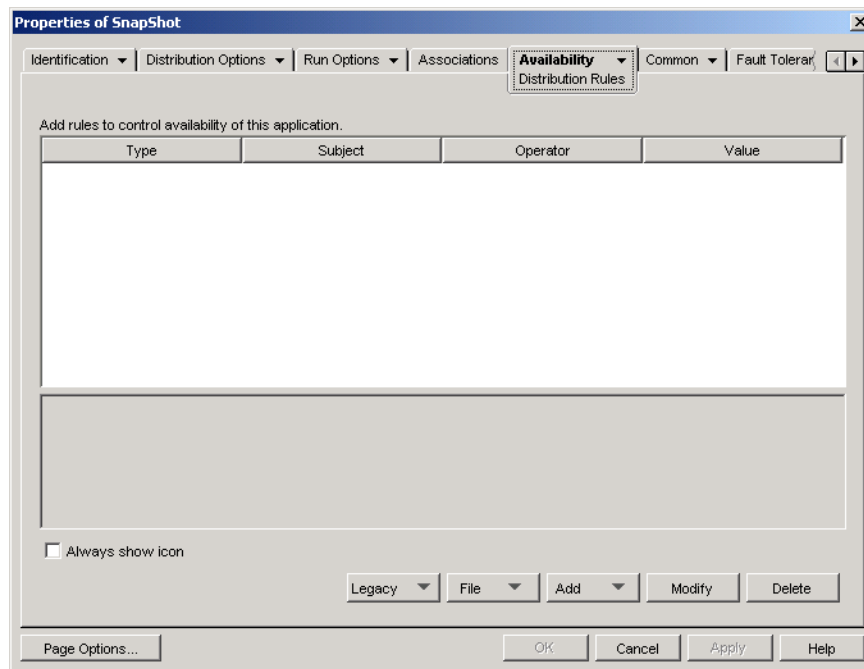
- [Section 48.5.1, “Distribution Rules Page,” on page 527](#)
- [Section 48.5.2, “Schedule Page,” on page 543](#)
- [Section 48.5.3, “Termination Page,” on page 546](#)

48.5.1 Distribution Rules Page

The Distribution property page is available on Application objects created for all application types (simple, AOT/AXT, MSI, Web, and terminal server).

The Distribution Rules property page, shown below, lets you define the rules applied to a workstation to determine whether or not Application Launcher distributes the application to it.

Figure 48-25 *Application Object > Availability Tab > Distribution Rules Page*



For example, you can define a disk space rule that instructs Application Launcher to only distribute the application on a workstation if the available disk space is greater than 2 GB. Or, you can define a rule that requires at least a Pentium III processor.

When creating rules, you can use AND/OR Boolean logic. For example, you can define a rule that instructs Application Launcher to only distribute the application if the available disk space is greater than 2 GB AND the processor is at least a Pentium III. You can also create groups of rules. For examples of distribution rules that use Boolean logic and groups, see [“Distribution Rules Examples” on page 531](#).

The distribution rules are used only by the ZENworks 7 (or later) versions of Application Launcher. Pre-ZENworks 7 versions of Application Launcher do not use distribution rules and require the use of legacy system requirements. If you have pre-ZENworks 7 versions of Application Launcher in your environment, see [Legacy](#) below for information about using legacy system requirements.

Add Rules to Control Availability of This Application

This list displays all the rules associated with the distribution of the application. For each rule, the following information is displayed:

- **Type:** You can define different types of rules, such as operating system rules, memory rules, and disk space rules. This column shows the rule’s type. The types are explained under [Add](#) below.
- **Subject:** This column shows the subject of the rule. For example, if the type is OS Version, the subject could be Windows 98 or Windows NT/2000/XP.

- **Operator:** This column shows if a condition (greater than, less than, equal to, etc.) must be met for the assigned value.
- **Value:** This column shows if a value is associated with the subject. For example, if Windows NT/2000/XP is the subject, the rule might require that the version be greater than or equal to 4.00.950 in order for the application to be distributed.

Always Show Icon

Select this option if you want Application Launcher to always display the Application object's icon regardless of whether or not the workstation meets the requirements defined by the distribution rules.

If you select this option and one or more rules is not met, the icon is displayed in a disabled state. Users can right-click the disabled icon, select *Details*, then select *Requirements* to view a list of all of the distribution requirements that were defined for the application.

Legacy

The Legacy options let you manage system requirements in a mixed environment consisting of ZENworks 7 (or later) versions of Application Launcher and pre-ZENworks 7 Application Launcher versions.

- **Edit legacy settings:** Only ZENworks 7 (or later) versions of Application Launcher have the ability to process the new grouping and operator (AND/OR) logic used with the distribution rules on this page. To maintain backward compatibility with the pre-ZENworks 7 versions, you must define legacy system requirements.

Click *Legacy > Edit Legacy Settings* to display the Legacy System Requirements dialog box. If you created the Application object in a pre-ZENworks 7 version, the dialog box displays any previously-defined system requirements. If you created the Application object in ZENworks 7, the dialog box is empty. You can add, modify, or remove requirements using the options in the dialog box.

- **Import legacy settings:** This option copies the legacy system requirements into the *Add rules to control availability of this application* list. If you've already added rules to the list, the legacy settings replace any rules you've added. To import legacy system requirements, click *Legacy > Import Legacy Settings*.

In a mixed-version environment, you need to decide how you want to use the new distribution rules and legacy system requirements together. In general, you have the following options:

- Define distribution rules only. The ZENworks 7 (or later) version of Application Launcher can read the distribution rules. Pre-ZENworks 7 versions cannot read the distribution rules and therefore are unable to distribute the application.
- Define distribution rules and legacy system requirements. ZENworks 7 (or later) versions use the distribution rules and pre-ZENworks 7 versions use the legacy system requirements. This method enables you to maintain the legacy system requirements for pre-ZENworks 7 Application Launcher while using the grouping, operator logic, and new rules available beginning with ZENworks 7. If you use this method, you can define the legacy system requirements first and then use the Import Legacy Settings option to populate the distribution rules. After populating the distribution rules, you can modify them to meet your needs.
- Define legacy system requirements only. Both ZENworks 7 (or later) and pre-ZENworks 7 versions use the legacy system requirements. This solution reduces administrative

maintenance of distribution rules and system requirements, but excludes you from using the new grouping, operators, and rules. Be aware that if you define any distribution rules, ZENworks 7 (or later) versions of Application Launcher use the distribution rules, not the legacy system requirements. The ZENworks 7 Application Launcher checks first for the existence of distribution rules; only if no distribution rules exist does it then check for legacy system requirements.

File

This option lets you search for requirements in the list and import requirements into the `.aot` or `.axt` file.

Click *File* > choose one of the following options:

- **Find:** Searches for requirements that include certain information. For example, you could search for requirements that include “Windows,” “>=,” or “system memory.”
- **Find next:** Finds the next occurrence of the requirement.
- **Import:** Imports requirements from another Application object’s `.aot` or `.axt` file. The Open dialog box defaults to `*.axt` for its file type display. If you are importing from a `.aot` file, you must change the file type display to `*.aot` or *All files* in order to select the `.aot` file.

Add

Click *Add*, then select one of the following distribution rules:

- **Applications:** Lets you require a specific application to be present or not be present on the workstation. The application must have been distributed through an Application object. For more information, see [“Applications” on page 532](#).
- **Client:** Lets you require the workstation to be running (or not running) the Novell Client. For more information, see [“Client” on page 533](#).
- **Connection speed:** Lets you require a specific network connection speed. For more information, see [“Connection Speed” on page 533](#).
- **Disk space:** Lets you require a specific amount of free disk space on the workstation. For more information, see [“Disk Space” on page 534](#).
- **Environment variables:** Lets you require specific environment variables to be present or not present. For more information, see [“Environment Variables” on page 535](#).
- **File date:** Lets you require a file to be a specific date. For more information, see [“File Date” on page 536](#).
- **File existence:** Lets you require a file to be present or not present. For more information, see [“File Existence” on page 536](#).
- **File size:** Lets you require a file to be a specific size. For more information, see [“File Size” on page 537](#).
- **File version:** Lets you require a file to be a specific version. For more information, see [“File Version” on page 538](#).
- **New group:** Lets you add a new rules group. For examples of how to use groups, see [“Distribution Rules Examples” on page 531](#).
- **Memory:** Lets you require a specific amount of memory on the workstation. For more information, see [“Memory” on page 539](#).

- **Operating system:** Lets you require a specific operating system. For more information, see [“Operating System” on page 539](#).
- **Processor:** Lets you require a specific processor type. For more information, see [“Processor” on page 540](#).
- **Registry:** Lets you require specific registry values to be present or not present. For more information, see [“Registry” on page 541](#).
- **Remote access:** Lets you require that Application Launcher be running in a specific mode, either remote mode or local (LAN) mode. For more information, see [“Remote Access” on page 542](#).
- **Terminal server:** Lets you require the workstation to be (or not be) a terminal server. For more information, see [“Terminal Server” on page 542](#).

Modify

Select a rule in the list, then click *Modify* to edit the information.

Delete

Select a rule in the list, then click *Delete* to remove the requirement.

Distribution Rules Examples

You can use AND and OR Boolean operators when defining the rules that control the distribution of an application. You can also use groups of rules to further control the distribution. Examples of using AND/OR Boolean operators and groups are provided below.

Simple Rule Using an OR Operator

You want to require a workstation to have either a Pentium III processor (or better) or the Windows 2000 operating system. To do so, use the following rule:

```
Processor type(Processor) >= Pentium III OR OS version(Windows NT/2000/XP) >= 5.00.2195
```

To create this rule:

- 1 On the Distribution Rules page, click the *Add* button, then select *Processor*.
- 2 In the Processor Rule dialog box, select *Greater than or equal to (>=)*, select *Pentium III*, then click *OK* to add the rule to the *Add rules to control availability of this application* list.
- 3 On the Distribution Rules page, click the *Add* button, then select *Operating system*.
- 4 In the Operating System Rule dialog box, select *Windows NT/2000/XP*, select *Greater than or equal to (>=)*, enter *5.00.2195*, then click *OK* to add the rule to the *Add rules to control availability of this application* list.
The rule is added to the list with an AND operator.
- 5 In the list, change the AND operator, located in front of the OS Version rule, to an OR operator.

Simple Group

You want to require a workstation to have either a Pentium III processor (or better) or the Windows 2000 operating system with at least 512 MB of memory. To do so, use the following rule:

```
Processor type(Processor) >= Pentium III OR (OS version(Windows NT/2000/XP) >= 5.00.2195 AND System memory(RAM) >= 512)
```

To create this rule:

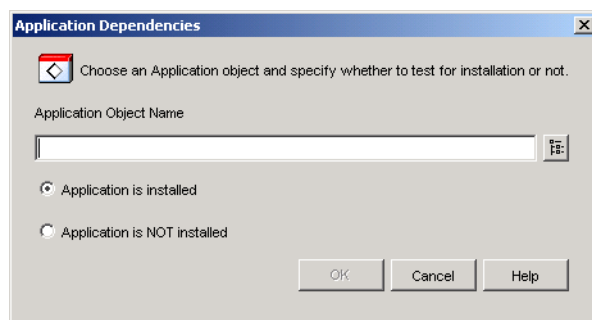
- 1 On the Distribution Rules page, click the *Add* button, then select *Processor*.
- 2 In the Processor Rule dialog box, select *Greater than or equal to (>=)*, select *Pentium III*, then click *OK* to add the rule to the *Add rules to control availability of this application* list.
- 3 On the Distribution Rules page, click the *Add* button, then select *New group* to add a new group to the *Add rules to control availability of this application* list.
The new group is labeled Group 1, unless you've previously added groups to the list. In addition, it is assigned the AND operator by default.
- 4 Locate Group 1 in the list and change the AND operator to an OR operator.
- 5 Next to Group 1 in the list, click the *Add to Group* button, then select *Operating System*.
- 6 In the Operating System Rule dialog box, select *Windows NT/2000/XP*, select *Greater than or equal to (>=)*, enter 5.00.2195, then click *OK* to add the rule under Group 1 in the list.
- 7 Next to Group 1 in the list, click the *Add to Group* button, then select *Memory*.
- 8 In the Memory Rule dialog box, select *Greater than or equal to (>=)*, enter 512, then click *OK* to add the rule under Group 1 in the list.

Applications

The Application Dependencies dialog box (*Distributions* page > *Add* > *Applications*), shown below, bases distribution on whether or not another application is installed on the workstation. The other application must be one that is represented in eDirectory as an Application object.

If you require an application that is not present, the distribution fails. To ensure that the distribution occurs, you can have Application Launcher install the dependent application. For information, see [“Application Dependencies Page” on page 521](#).

Figure 48-26 Application Dependencies Dialog Box



Application Object Name

Browse to and select the application whose existence on the workstation Application Launcher will check for.

Application Is Installed

Select this option to indicate that the selected application must already be installed on the workstation.

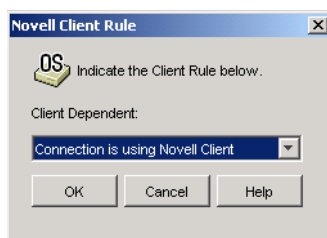
Application Is Not Installed

Select this option to indicate that the selected application must not be installed on the workstation.

Client

The Novell Client Rule dialog box (*Distribution Rules* page > *Add* > *Client*), shown below, lets you base distribution on whether or not the Novell Client is installed on the workstation.

Figure 48-27 Novell Client Rule Dialog Box



Client Dependent

Select *Connection is using Novell Client* if you want the application to be available only on workstations that are running the Novell Client.

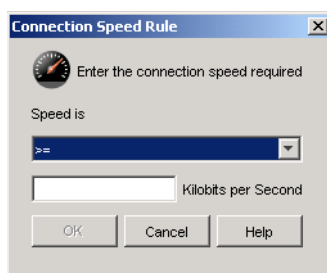
Select *Connection is not using Novell Client* if you want the application to be available only on workstations that are not running the Novell Client.

Connection Speed

The Connection Speed Rule dialog box (*Distribution Rules* page > *Add* > *Connection speed*) lets you base distribution on the speed of the workstation's network connection.

For example, if you don't want the application to be available on remote workstations whose connection speed is less than 56 Kbps, you could require a connection speed of 56 Kbps or greater.

Figure 48-28 Connection Speed Rule Dialog Box



Speed Is (Conditional Statement)

Select whether the connection speed must be less than (<), less than or equal to (<=), greater than (>), or greater than or equal to (>=) the speed entered in the Kilobits per Second field.

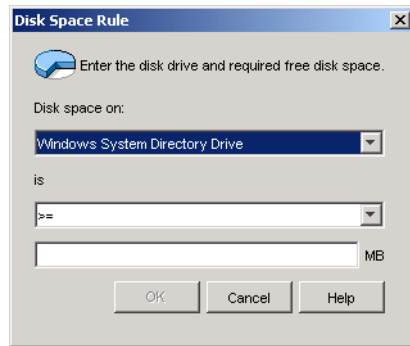
Kilobits per Second (Condition)

Specify the connection speed in kilobits per second.

Disk Space

The Disk Space Rule dialog box (*Distribution Rules* page > *Add* > *Disk space*), shown below, lets you base distribution on the workstation's free disk space. This ensures that Application Launcher does not attempt to distribute an application to a workstation that does not have sufficient free disk space.

Figure 48-29 Disk Space Rule Dialog Box



Disk Space On

Select the disk where you are requiring free space. The list includes the following options:

- **A through Z:** Allows you to select the disk that is mapped to drive A, B, C, and so on.
- **Windows system directory drive:** Allows you to select the disk where the Windows system directory (for example, `winnt\system32`) resides.
- **Windows directory drive:** Allows you to select the disk where the Windows directory (for example, `winnt`) resides.
- **Temp directory drive:** Allows you to select the disk where the Windows temporary directory (for example, `winnt\temp`) resides.

If you create multiple disk space requirements for the application, Application Launcher adds the requirements together to determine the total disk space requirement. For example, if you specify 20 MB free on the Windows directory drive (which happens to be the C: drive), 10 MB free on the temp directory drive (which is also the C: drive), and 50 MB free on the D: drive, Application Launcher distributes the Application object only if there is 30 MB available on the C: drive and 50 MB free on the D: drive.

Is (Conditional Statement)

Select whether the available disk space must be less than, less than or equal to, equal to, greater than, greater than or equal to the amount listed in the MB field. The corresponding operators are as follows:

Less than: <

Less than or equal to: <=

Equal to: =

Greater than or equal to: >=

Greater than: >

For example, if you want to require at least 50 MB of free disk space, select >= (greater than or equal to) and then enter 50 in the MB field.

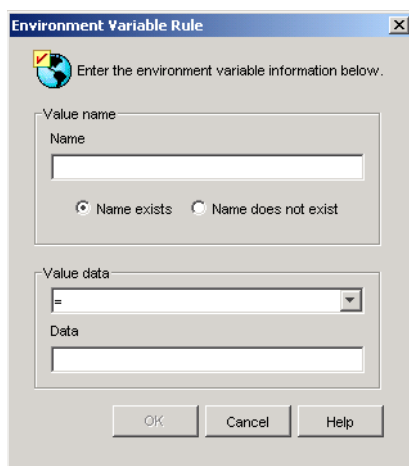
MB (Condition)

Specify the disk space requirement.

Environment Variables

The Environment Variable Rule dialog box (*Distribution Rules* page > *Add* > *Environment variables*), shown below, lets you base distribution on whether or not an environment variable containing specific data exists.

Figure 48-30 *Environment Variable Rule Dialog Box*



Value Name

Specify the name of the environment variable. Select the *Name exists* option to require the variable to already exist on the workstation, or select the *Name does not exist* option to require the variable to not exist on the workstation.

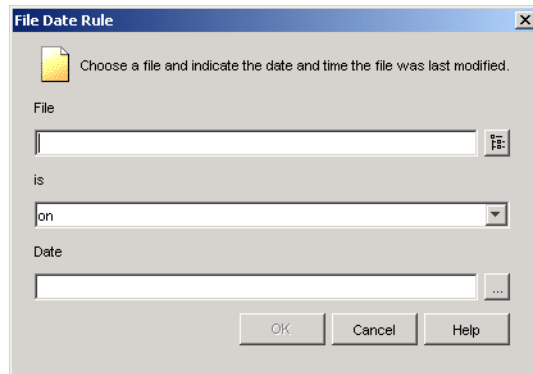
Value Data

Specify whether the variable data must be equal to, not equal to, contain, or not contain the data you enter in the Data field.

File Date

The File Date Rule dialog box (*Distribution Rules* page > *Add* > *File date*), shown below, lets you base distribution on the date of a specific file located on the workstation.

Figure 48-31 File Date Rule Dialog Box



File

Browse to select the file whose date Application Launcher will check.

Is (Conditional Statement)

Select whether the file date must be before, on or before, on, on or after, or after the date entered in the *Date* field. For example, if you want to make sure the application is distributed only if the file is dated 15 January 2000 or older, you would select *On or before* and then select the date.

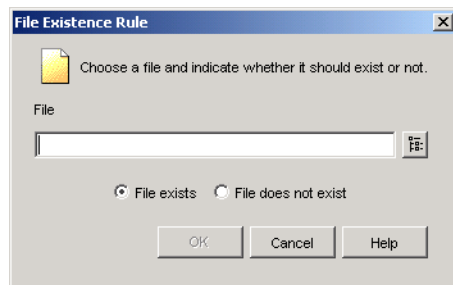
Date (Condition)

Use the Calendar to select the appropriate date.

File Existence

The File Existence Rule dialog box (*Distribution Rules* page > *Add* > *File existence*), shown below, lets you base distribution on whether or not a specific file exists on the workstation.

Figure 48-32 File Existence Rule Dialog Box



File

Browse and select the file that Application Launcher will check for.

File Exists

Select this option to require the file to exist on the workstation.

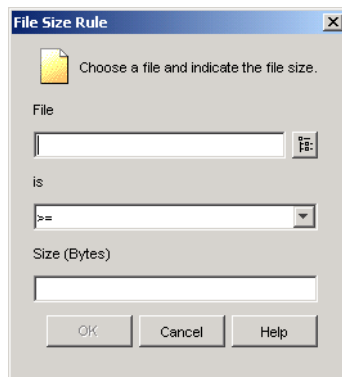
File Does Not Exist

Select this option to require the file to not exist on the workstation.

File Size

The File Size Rule dialog box (*Distribution Rules* page > *Add* > *File size*), shown below, lets you base distribution on the size of a specific file located on the workstation.

Figure 48-33 File Size Rule Dialog Box



File

Browse to select the file whose size Application Launcher will check.

Is (Conditional Statement)

Select whether the size must be less than, less than or equal to, equal to, greater than, or greater than or equal to the size entered in the Size field. The corresponding operators are as follows:

Less than: <

Less than or equal to: <=

Equal to: =

Greater than or equal to: >=

Greater than: >

For example, if you want to require the file to be at least 200 KB, select >= (greater than or equal to) and then enter 200000 in the Size field.

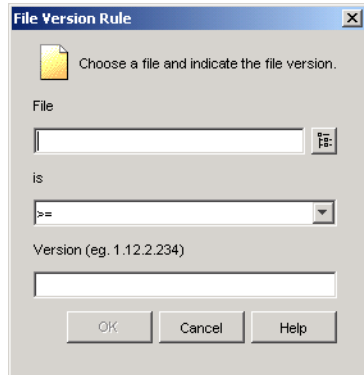
Size

Specify the file size in kilobytes.

File Version

The File Version Rule dialog box (*Distribution Rules* page > *Add* > *File version*), shown below, lets you base distribution on the version of a specific file located on the workstation.

Figure 48-34 File Version Rule Dialog Box



File

Browse to select the file whose version you want Application Launcher to check.

Is (Conditional Statement)

Select whether the version must be less than, less than or equal to, equal to, greater than, greater than or equal to the version entered in the Version field. The corresponding operators are as follows:

Less than: <

Less than or equal to: <=

Equal to: =

Greater than or equal to: >=

Greater than: >

For example, if you want to require at least version 1.12.2.234, select >= (greater than or equal to) and then enter 1.12.2.234 in the Version field.

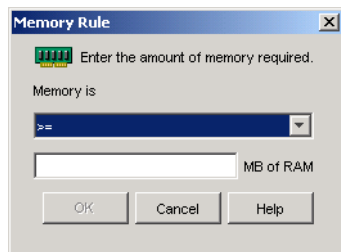
Version (Condition)

Specify the file version.

Memory

The Memory Rule dialog box (*Distribution Rules* page > *Add* > *Memory*), shown below, lets you base distribution on the amount of memory (RAM) required on the workstation.

Figure 48-35 Memory Rule Dialog Box



Memory Is (Conditional Statement)

Select whether the total memory must be less than, less than or equal to, equal to, greater than, greater than or equal to the memory entered in the MB of RAM field. The corresponding operators are as follows:

Less than: <

Less than or equal to: <=

Equal to: =

Greater than or equal to: >=

Greater than: >

For example, if you want to require at least 32 MB of free RAM, select >= (greater than or equal to) and then enter 32 in the MB of RAM field.

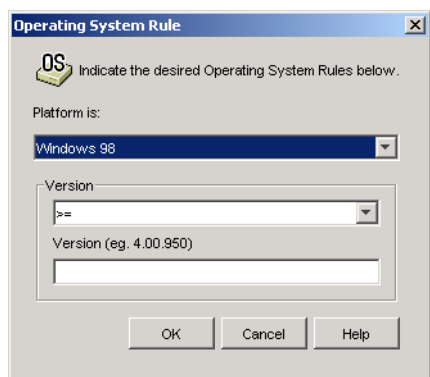
MB of RAM (Condition)

Specify the required memory amount.

Operating System

The Operating System Rule dialog box (*Distribution Rules* page > *Add* > *Operating system*), shown below, lets you base distribution on the workstation's operating system and version.

Figure 48-36 Operating System Rule Dialog Box



Platform Is

Select the operating system (Windows 98 or Windows NT/2000/XP) the workstation must be running.

NOTE: The requirement for an operating system to be defined before an application is available has been removed.

In previous ZENworks versions, an OS platform had to be defined in the System Requirements before an application was available for distribution and launching. This requirement has been removed.

The new behavior uses the following logic: If an application runs only on a specific operating system, define an operating system distribution rule. If an application does not require a specific operating system, there is no need to define a distribution rule. By default, applications without a defined operating system distribution rule are available on all supported platforms (Windows 98, Windows 2000, and Windows XP).

Version

Select whether the version number must be less than, less than or equal to, equal to, greater than, greater than or equal to the number entered in the Version field.

Less than: <

Less than or equal to: <=

Equal to: =

Greater than or equal to: >=

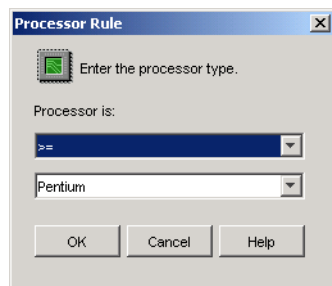
Greater than: >

For example, if you want to require at least version 4.00.950, select >= (greater than or equal to) and then enter 4.00.950 in the Version field.

Processor

The Processor Rule dialog box (*Distribution Rules* page > *Add* > *Processor*), shown below, lets you base distribution on the workstation's processor.

Figure 48-37 Processor Rule Dialog Box



Processor Is

Select whether the processor must be less than, less than or equal to, equal to, greater than, or greater than or equal to the processor type (386, 486, Pentium, Pentium Pro, Pentium II, Pentium III) selected in the processor list.

Less than: <

Less than or equal to: <=

Equal to: =

Greater than or equal to: >=

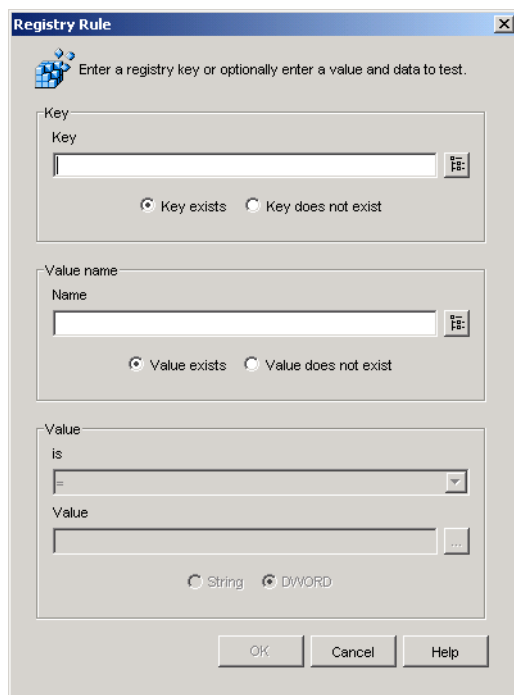
Greater than: >

For example, if you want to require at least a Pentium II processor, select >= (greater than or equal to) and then select Pentium II.

Registry

The Registry Rule dialog box (*Distribution Rules* page > *Add* > *Registry*), shown below, lets you base distribution on whether or not a specific registry key or value exists.

Figure 48-38 Registry Rule Dialog Box

The image shows the 'Registry Rule' dialog box. It has a title bar with 'Registry Rule' and a close button. Below the title bar is a message: 'Enter a registry key or optionally enter a value and data to test.' The dialog is divided into three main sections. The first section is labeled 'Key' and contains a text box for the key name, a browse button (folder icon), and two radio buttons: 'Key exists' (selected) and 'Key does not exist'. The second section is labeled 'Value name' and contains a text box for the value name, a browse button, and two radio buttons: 'Value exists' (selected) and 'Value does not exist'. The third section is labeled 'Value' and contains a dropdown menu for the comparison operator (currently showing '=') and a text box for the value. Below these are two radio buttons: 'String' and 'DWORD' (selected). At the bottom are three buttons: 'OK', 'Cancel', and 'Help'.

Key

Browse and select the registry key you want to check before distribution. Select *Key exists* if the key must exist for the distribution to take place, or select *Key does not exist* if the key cannot exist for the distribution to take place.

Name

If the key has a specific value you want to check for, browse and select the value. Select *Value exists* if the value must exist for the distribution to take place, or select *Value does not exist* if the value cannot exist for the distribution to take place.

Value

If you specified a value in the *Name* field, select an operator (<, <=, =, !=, >=, >) for the value's data, enter the data in the *Value* field, then select whether the value data is a String or DWORD type.

The operator definitions are as follows:

Less than: <

Less than or equal to: <=

Equal to: =

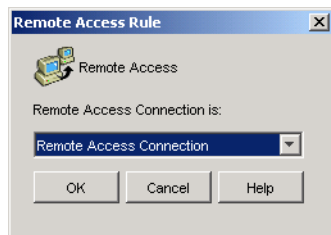
Greater than or equal to: >=

Greater than: >

Remote Access

The Remote Access Rule dialog box (*Distribution Rules* page > *Add* > *Remote access*), shown below, lets you base distribution on whether Application Launcher is in remote mode or local (LAN) mode. The method Application Launcher uses to detect which mode it is in is determined by the Remote Access Detection setting (User/Workstation/container object > *ZENworks* tab > *Launcher Configuration* page > *Add* button > *User* tab).

Figure 48-39 Remote Access Rule Dialog Box



Remote Access Connection Is

Select whether the connection must be a remote access connection or a LAN connection. For example, if you select *Remote access connection*, the application is distributed to a user only if Application Launcher is running in remote mode.

Terminal Server

The Terminal Server Rule dialog box (*Distribution Rules* page > *Add* > *Terminal server*), shown below, lets you base distribution on whether or not the machine is a terminal server (in other words, Windows Terminal Services is active on the machine).

Figure 48-40 Terminal Server Rule Dialog Box



Select *Terminal server required* if you want the application to be distributed only to terminal servers. Select *Terminal server not required* if you want the application to be distributed only to non-terminal servers.

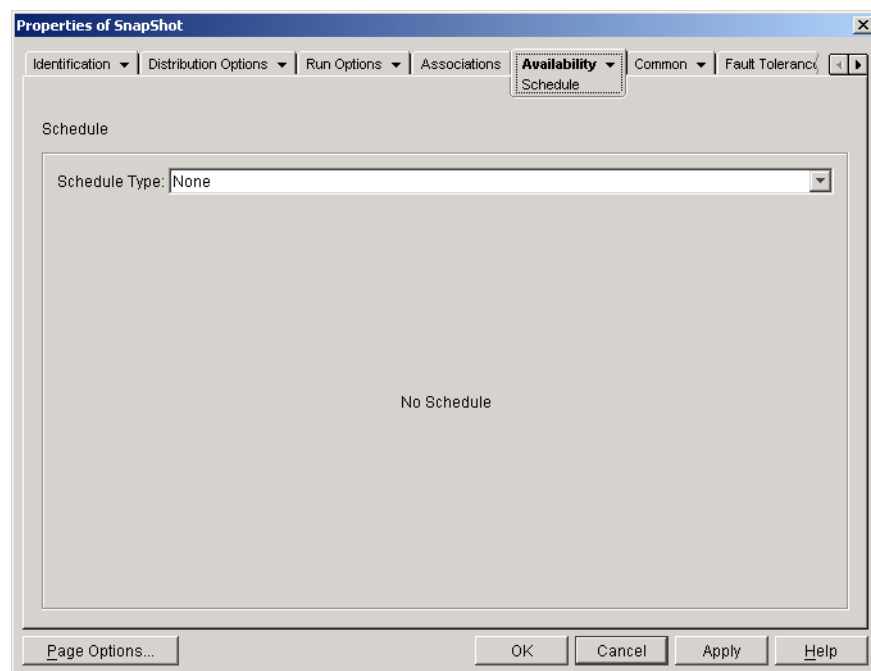
48.5.2 Schedule Page

The Schedule property page is available on Application objects created for all application types (simple, AOT/AXT, MSI, Web, and terminal server).

The Schedule property page, shown below, defines the dates and times when the application is available to users. Application Launcher displays the application icon only during the times defined by the schedule.

The schedule applies regardless of whether or not the application is installed. For example, if a user has not yet installed the application, it is only available for installation at the times specified by the schedule. Likewise, if a user has already installed the application, it is only available for running during the scheduled times.

Figure 48-41 *Application Object > Availability Tab > Schedule Page*



Schedule Type

Select the type of schedule you want to use. You can choose *None*, *Specified days*, or *Range of days*.

None

Use this option to indicate no schedule. The Application object becomes available to an object as soon as the application's system requirements have been established (*Availability > System Requirements* page) and the application has been associated with the object (*Associations* page).

Specified Days

Use this option to select specific dates when you want the Application object to be available. After selecting this option, fill in the following fields:

- **Date range:** The Date Range list displays all dates when the Application object is available. To add a date, click *Add* > select the date you want > click *OK* to display it in the list. You cannot select more than 350 specific dates.
- **Time for selected dates:** Select the availability start time and end time. The times apply to all dates in the Date Range list.

NOTE: The time increments in 5 minute intervals, with the earliest available start time being 00:00 (12:00 a.m.) and the latest end time being 23:55 (11:55 p.m.). This means there is always a 5-minute time period from 11:55 p.m. to 12:00 midnight when the application is unavailable. If you want the application to be available the entire day, you need to use the *Range of days* schedule type. For more information, see [“Range of Days” on page 545](#).

- **Spread from start time (in minutes):** The *Spread from start time* option spreads out user access times over the number of minutes specified so the application doesn't become available to all users at the same time. If you anticipate all users launching the application as soon as it becomes available and the application is being distributed or run from the network, you can use this option to avoid possible network overload.

For example, if you have a moderate number of users to whom the application is to be distributed (say about 100), you might specify a one-hour (60 minute) block of time (starting at the scheduled start time) to randomly distribute the application: thus all users will gain access to the application some time during the first sixty minutes after the scheduled start time.

If you want to substantially ease the load on your servers caused by the application distribution, or if you have bandwidth concerns, you might want to make the application distribute randomly throughout the time of availability. To spread out access times across the entire time (*Specified days* and *Time for selected dates*) that the application is available, use the total availability time specified for that application in terms of minutes. This will require that you make the maximum time available for each day you specify. For example, if an application is configured for a typical business day in the United States (9 hours per day: 8:00 a.m. to 5:00 p.m.), you calculate the total time of availability for that application like this:

Number of specified hours x 60 minutes per hour = Total availability time per day

Using this equation, the example above would be calculated like this:

9 x 60 (minutes per hour) = 540 minutes of availability

In this example, when you enter 540 minutes in the *Spread from start time* field, the application is distributed randomly for the entire 540 minutes that you have made it available on that scheduled day. Note that this might not be suitable for applications that must be distributed in a timely fashion, such as anti-virus updates. Note also that this is an example only: you can schedule the distribution for any specified amount of time for any day of the week.

Remember that the *Time for selected dates* setting makes the last five minutes of a day unscheduleable, so you need to consider these five minutes if the application schedule ends at 11:55 p.m. for that day.

Range of Days

Use this option to select a range of dates to make the application available. You can also use this option to make applications available only on certain days of the week within a given range of dates. After selecting this option, fill in the following fields:

- **Date range:** To define the range of days, select a start date and an end date, then select the days (Sunday through Saturday) within the established date range that the application is available. By default, all days are selected; a day is selected when the button appears to be pressed in.
- **Time for selected range:** Select the availability start time and end time. This option works differently depending on whether the date range includes one day, multiple days, or all seven days. If the date range includes one to six days (but not all seven days), the application is available between the start and end times on those days. For example, if you make the application available on Monday between 8:00 and 5:00, it is available during those hours. However, if the date range includes all seven days, the times are ignored and the application is available every day, 24 hours a day.
- **Spread from start time (in minutes):** The *Spread from start time* option spreads out user access times over the number of minutes specified so the application doesn't become available to all users at the same time. If you anticipate all users launching the application as soon as it becomes available and the application is being distributed or run from the network, you can use this option to avoid possible network overload.

For example, if you have a moderate number of users to whom the application is to be distributed (say about 100), you might specify a one-hour (60 minute) block of time (starting at the scheduled start time) to randomly distribute the application: thus all users will gain access to the application some time during the first sixty minutes after the scheduled start time.

If you want to ease the load of the application distribution on your servers or if you have bandwidth concerns, you might want to make the application distribute randomly throughout the time of availability. To spread out access times across the entire time (*Date range* and *Time for selected dates*) that the application is available, use the total availability time specified for that application in terms of minutes. For example, if a workstation-associated application is configured for an entire 24-hour, three-shift day, you can calculate the total time of availability for that application like this:

Number of days in date range x *Time of availability per day* = Total availability time

Using this equation, and making sure to convert hours to minutes, the example above would be calculated like this:

7 (days) x 24 (hours) = 168 hours of availability

168 x 60 (minutes per hour) = 10,080 minutes of availability

When you enter 10800 minutes in the *Spread from start time* field, the application is distributed randomly for the entire 10800 minutes that you have made it available. Note that this is not suitable for applications that must be distributed in a timely fashion, such as anti-virus updates.

- **Use this schedule in GMT for all clients:** The schedule is based on the workstation's time zone. If your network spans different time zones and you schedule an application to run at 1:00 p.m., it runs at 1:00 p.m. in each time zone. You can select this option to have workstations run applications at the same time regardless of their time zones (for example, 1:00 p.m. Rome time and 4:00 a.m. Los Angeles time).

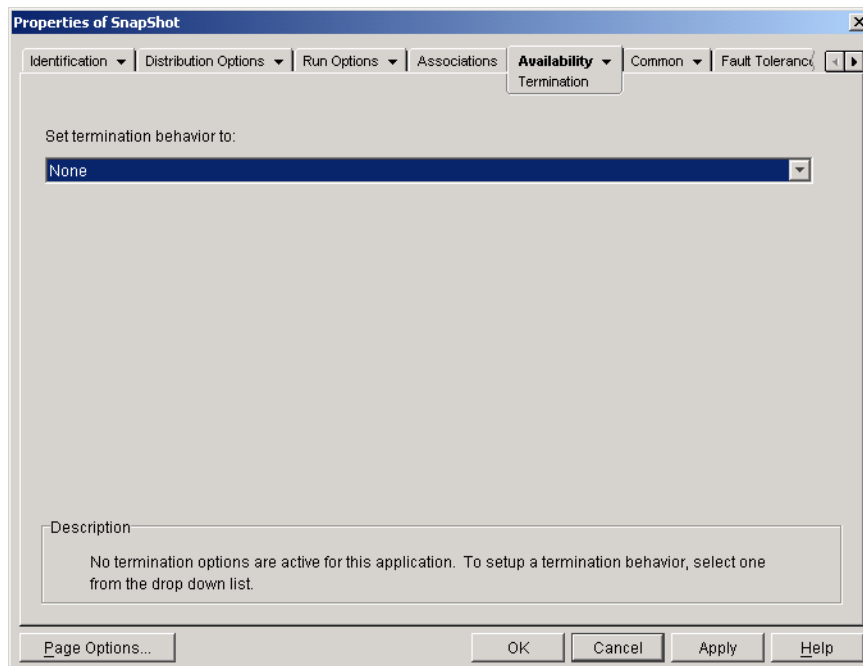
48.5.3 Termination Page

The Termination property page is available on Application objects created for all application types (simple, AOT/AXT, MSI, Web, and terminal server).

The Termination property page, shown below, determines how Application Launcher terminates the application if it becomes unavailable to a user while the user is running the application. An application becomes unavailable to a user when:

- You disassociate it from the user.
- The availability schedule expires.
- The application's distribution rules change and the user's workstation no longer complies with the requirements.

Figure 48-42 *Application Object > Availability Tab > Termination Page*



Set Termination Behavior To

Select the behavior you want used when the application terminates.

None

Select this option to disable any termination behaviors.

Send Message to Close Application

This option causes Application Launcher to display a message instructing the user to close the application. The message appears periodically until the user closes the application.

In the Basic Closing Message box, select how often you want Application Launcher to display the message. The following default message is used unless you click the Message button and define a custom message:

WARNING! Your access to this application has expired. Please close the application to avoid losing your work.

Send Message to Close Then Prompt to Save Data

This option causes Application Launcher to first display a message instructing the user to close the application. If the user does not close the application, Application Launcher sends a call to the application instructing it to close. If the user has no unsaved data, the application closes immediately. If the user has unsaved data, the application displays a Save dialog box to allow the user to save the data. After the application closes, users cannot launch it again.

IMPORTANT: Some applications display a Save dialog box that includes a *Cancel* button in addition to *Yes* and *No* buttons. The *Cancel* button aborts the close operation and the application remains open. If the application's Save dialog box includes a *Cancel* button and you want to ensure that the application is closed, you must use the *Send message to close, Prompt to save, Then Force to close* option.

After selecting this option, fill in the following fields:

- **Warning message (optional):** Select the *Send warning* option if you want to warn the user to close the application, then specify the number of times to display the warning message and the interval between messages. The following default message is used unless you click the *Message* button and define a custom message:

WARNING! Your access to this application has expired. Please close the application to avoid losing your work.

- **Prompt closing message:** This message is displayed if the user does not close the application after receiving the warning message the specified number of times, or if the warning message option is not enabled.

In the Prompt Closing Message box, specify how often you want to prompt the user to close the application. If, after receiving the prompt, the user does not close the application, Application Launcher attempts to close the application. The following default message is used unless you click the *Message* button and define a custom message:

WARNING! Your access to this application has expired and the application will close shortly. Please save your work and exit the application.

Send Message to Close, Prompt to Save, Then Force Close

This option causes Application Launcher to first display a message instructing the user to close the application. If the user does not close the application, Application Launcher sends a call to the application instructing it to close. If the user has no unsaved data, the application closes immediately. If the user has unsaved data, the application displays a Save dialog box to allow the user to save the data. Regardless of the option (*Yes*, *No*, *Cancel*) the user selects, the application is closed.

After selecting this option, fill in the following fields:

- **Warning message (optional):** Select the *Send warning* option if you want to warn the user to close the application, then specify the number of times to display the warning and the interval between warnings. The following default message is used unless you click the *Message* button and define a custom message:

WARNING! Your access to this application has expired. Please close the application to avoid losing your work.

- **Prompt closing message:** This message is displayed if the user does not close the application after receiving the warning message the specified number of times, or if the warning message option is not enabled.

In the Prompt Closing Message box, specify how often you want to prompt the user to close the application. If, after receiving the prompt, the user does not close the application, Application Launcher attempts to close the application. The following default message is used unless you click the *Message* button and define a custom message:

WARNING! Your access to this application has expired and the application will close shortly. Please save your work and exit the application.

- **Application termination:** This message is displayed after Application Launcher closes the application. If you don't want to use the default termination message, click the *Message* button and define a custom message. The default message is:

The application you were running has expired. For additional usage, please contact your system administrator.

Send Message to Close Then Force Close with Explanation

This option prompts the user to close the application. If the user does not, Application Launcher closes the application automatically and displays a termination message.

After selecting this option, fill in the following fields:

- **Warning message (optional):** Select the *Send warning* option if you want to warn the user to close the application, then specify the number of times to display the warning and the interval between warnings. If the user does not close the application, Application Launcher closes the application automatically after the last warning message. The following default message is used unless you click the *Message* button and define a custom message:

WARNING! Your access to this application has expired. Please close the application to avoid losing your work.

- **Application termination:** This message is displayed after Application Launcher closes the application. If you don't want to use the default termination message, click the *Message* button and define a custom message. The default message is:

The application you were running has expired. For additional usage, please contact your system administrator.

48.6 Common Tab

The Common tab includes the following pages:

- [Section 48.6.1, "Macros Page," on page 549](#)
- [Section 48.6.2, "Drives/Ports Page," on page 551](#)
- [Section 48.6.3, "File Rights Page," on page 554](#)
- [Section 48.6.4, "Reporting Page," on page 556](#)
- [Section 48.6.5, "Imaging Page," on page 559](#)
- [Section 48.6.6, "Sources Page," on page 562](#)

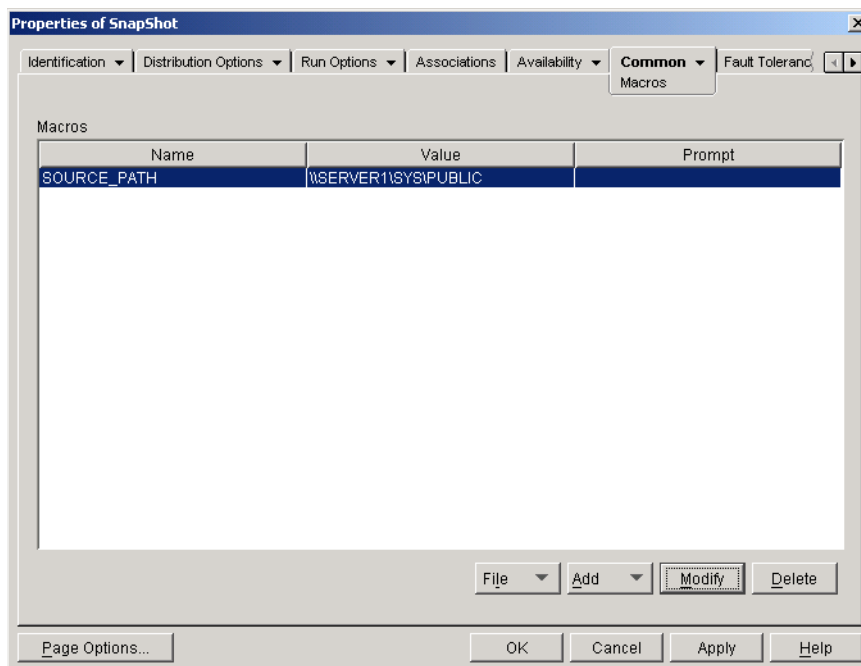
- [Section 48.6.7, “Uninstall Page,” on page 563](#)
- [Section 48.6.8, “Uninstall Scripts Page,” on page 566](#)

48.6.1 Macros Page

The Macros property page is available on Application objects created for all application types (simple, AOT/AXT, MSI, Web, and terminal server).

The Macros property page, shown below, displays the macros that have been defined for use with the Application object. For information about the Application object fields that support macros, see [Section 49.8, “Application Object Properties Where Macros Can Be Used,” on page 597](#)

Figure 48-43 *Application Object > Common Tab > Macros Page*



These macros, referred to as Application object macros, are simply variable names that are associated with values, typically string values.

For example, when you create an Application object using an .aot or .axt file, a SOURCE_PATH macro is automatically added to the list. This macro defines the location of the source files from which the application is installed. Many times, you must enter the source path when defining other properties for the Application object. By creating a SOURCE_PATH macro, you only need to enter %SOURCE_PATH% rather than the actual source path.

IMPORTANT: When using a macro for any of these properties, you must enclose the macro name in % characters (for example, %SOURCE_PATH%).

Macros

The Macros list displays all macros that have been defined for use with the Application object.

File

This option lets you search for specific macro information and import macros from other Application objects.

Click *File*, then choose one of the following options:

- **Find:** Searches for specific information in the *Name*, *Value*, and *Prompt* fields.
- **Find next:** Finds the next occurrence of the information.
- **Import:** Imports macros from another Application object's .aot or .axt file. The Open dialog box defaults to *.axt for its file type display. If you are importing from an .aot file, you must change the file type display to *.aot or All files in order to select the .aot file.

Add

Use the Add button to define an Application object macro and add it to the Macros list. You can add either a String Value macro or a Prompted macro.

String Value

A String Value macro is used to create a variable that has a string value associated with it. This lets you use the variable in multiple locations while defining the value in one location.

To create a String Value macro, click *Add > String value* to display the Edit String Value dialog box. In the Value Name box, type a name for the variable, then type the value for the variable in the Value Data box. Click *OK* to add the macro to the Macros list.

You can place macros within macros. In the following example, a special Windows macro, *WINDISK, is used when defining the TARGET_PATH macro:

```
Value Name: TARGET_PATH
Value Data: %*WINDISK%\Program Files
```

When embedding another macro in the string, you must enclose the macro in % characters, as shown in the above example. You can embed special Windows macros, eDirectory attribute macros, environment variable macros, login script macros, language variable macros, and other Application object macros. For information about these types of macros, see [Chapter 49, "Reference: Macros," on page 585](#).

Prompted

A Prompted macro is used to create a macro that prompts the user to accept a default value (either a drive or string) or enter a new value. There are two types of Prompted macros: *Prompted drive* macros and *Prompted string* macros. Because Windows Installer, and not Application Launcher, controls the installation of MSI applications, *Prompted* macros do not work with MSI applications.

To create a *Prompted drive* macro, click *Add > Prompted > Drive* to display the Prompted Drive Macros dialog box. Fill in the fields as described below:

- **Macro name:** Give the macro any name you want. Do not use spaces.
- **Prompt text:** Specify the text you want presented to users. For example, "This application will be installed to your C: drive. Enter a different drive letter if desired:"
- **Default value:** Select the drive that is used if the user does not enter another drive letter.

- **Minimum disk space in MB:** Specify the minimum amount of free disk space required to install the application.

To create a *Prompted string* macro, click *Add > Prompted > String* to display the Prompted String Macros dialog box. Fill in the fields as described below:

- **Macro name:** Give the macro any name you want. Do not use spaces.
- **Prompt text:** Specify the text you want presented to users.
- **Default value:** Select the value that is used if the user does not enter another value in response to the prompt text.
- **Minimum disk space in MB:** Specify the minimum amount of free disk space required to install the application.
- **Maximum string length in chars:** Specify the maximum number of characters the user can enter as a response to the prompt.

Modify

Select the macro whose information you want to modify, then click *Modify*.

Delete

Select the macro you want to delete, then click *Delete*.

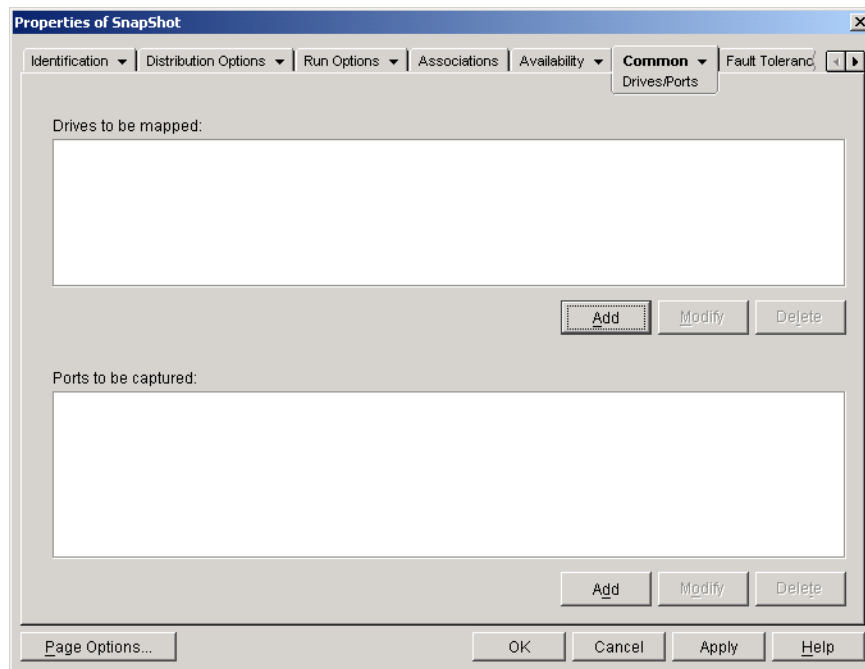
48.6.2 Drives/Ports Page

The Drives/Ports property page is available only on Application objects created for simple applications, AOT/AXT applications, and MSI applications. It is not available on Application objects created for Web applications and terminal server applications.

The Drives/Ports property page, shown below, determines the drive mappings and port captures for the application. Drive mappings and port captures are performed by the workstation's network

clients, not by Application Launcher. This requires that the workstation have the network clients (for example, the Novell Client and the Microsoft Client) needed to perform the mappings and captures.

Figure 48-44 *Application Object > Common Tab > Drives/ports Page*



For example, suppose you've set up a database application to run from drive W:. To ensure that W is mapped to the location of the application, you could map drive W: to the server, volume, and directory where the application exists. When Application Launcher runs the application, it establishes the drive mapping according to the conditions defined when setting up the drive mapping.

Or, maybe users need access to a network location to store files created with a word processor. If you map a drive, the drive mapping becomes active as soon as the application runs.

By default, drive mappings and port captures are released when the user closes the application. If several launched applications use the same drive mappings or port captures, the drive mappings and port captures aren't released until the last application terminates. If you don't want drive mappings and port captures released, you must deselect the *Clean up network resources* option (*Run Options > Environment* page).

Drives to Be Mapped

The *Drives to be mapped* list displays all drives that are mapped before the application is launched.

Add

Click *Add* to display the Drive to Be Mapped dialog box. Fill in the following fields:

- **Root:** Select this option to treat the path as the root of the drive.
- **Option:** Select the type of drive to map. The available types are:
 - **DRIVE:** Select this option to map to a drive letter (A through Z).

- **S1:** Select this option to assign the drive to the first available search drive.
- **S16:** Select this option to assign the drive to the last search drive.

NOTE: Starting with ZENworks for Desktops 4.x, selecting the S1 or S16 option does not affect the system's global path. Only applications started by this NAL process uses this search path; applications external to the NAL process cannot use this search path.

- **Drive:** Assign a drive letter. The options are drives A through Z, or the next available drive.
- **Path:** Enter, or browse and select, the path you want mapped to the selected drive. If you enter the path, use the following syntax:

```
server\volume:path
\\server\volume\path
volume_object_name:path
directory_map_object_name:path
driveletter:\path
```

You can also use a macro in this field. For information about macros, see [Chapter 49](#), “Reference: Macros,” on page 585.

- **Map if drive mapping doesn't exist or same as existing:** Select this option if you want Application Launcher to map the drive if 1) it doesn't exist already or 2) it is the same as an existing drive mapping.
- **Overwrite any existing drive mapping:** Select this option if you want Application Launcher to replace any mapping that uses the requested drive letter. For example, if S: is mapped to \\server1\sys\public and you've specified the new S: drive mapping as \\server1\apps\timecard, the end result is that drive S: is mapped to \\server1\apps\timecard.

To identify this option in the *Drives to be mapped* list, the word **FORCE** is added to the mapping information.

- **Use the existing drive mapping if already mapped:** Select this option to use the existing drive mapping even if it is not the same as the path requested. For example, if S: is mapped to \\server1\sys\public and you've specified the new S: drive mapping as \\server1\apps\timecard, the end result is that drive S: is still mapped to \\server1\sys\public.

To identify this option in the *Drives to be mapped* list, the word **REUSE** is added to the mapping information.

Modify

Select a drive mapping in the *Drives to be mapped* list, then click *Modify* to display the Drive to be Mapped dialog box. Change the drive mapping information as needed. See the field descriptions above or click the *Help* button in the dialog box.

Delete

Select a drive mapping in the *Drives to be mapped* list, then click *Delete* to remove the mapped drive.

Ports to Be Captured

The *Ports to be captured* list displays all ports that are captured before the application is launched.

Add

Click *Add* to display the Ports to Be Captured dialog box. Fill in the following fields:

- **Port:** Select an LPT port to assign to the printer or queue.
- **Printer or queue:** Browse to select a printer or queue.

You can also use a macro in this field. For information about macros, see [Chapter 49, “Reference: Macros,”](#) on page 585.

- **Capture flags:** You can use this option to override notification, banner, and form feed settings defined on the user’s workstation. Whenever a user prints from the application, the settings you defined are used.

In the *Capture flags* box, select the *Override workstation setting* box for the corresponding *Capture* setting you want to override. After you do this, the corresponding *Capture* setting becomes active. Select the setting to turn it on. Leave the setting deselected to turn it off.

For example, if you select the *Override workstation setting* box for *Notify* and also select the *Capture setting* box for *Notify*, when the user prints a document, the Novell Client displays a Notify alert panel to indicate the completion of the print job, no matter which Capture settings are on the user’s workstation. However, if you select the *Override workstation setting* box for *Notify* but do not select the *Capture setting* box for *Notify*, when the user prints a document, the Novell Client does not display a Notify alert panel to indicate the completion of the print job, no matter which Capture settings are used on the user’s workstation.

Modify

Select a port capture in the *Ports to be captured* list, then click *Modify* to display the Ports to be Captured dialog box. Change the capture information as needed. See the field descriptions above or click the *Help* button in the dialog box.

Delete

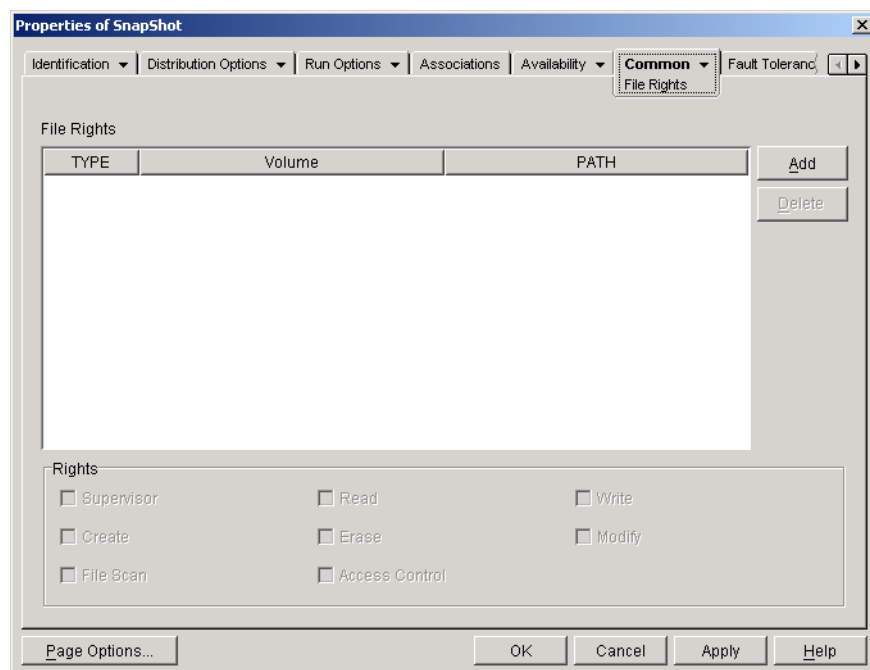
Select a port capture in the *Ports to be captured* list, then click *Delete* to remove the captured port.

48.6.3 File Rights Page

The File Rights property page is available on Application objects created for simple applications, AOT/AXT applications, and MSI applications only. It is not available on Application objects created for Web applications and terminal server applications.

The File Rights property page, shown below, specifies the file, directory, and volume rights a user must have to run the application. This page applies only to NetWare file system rights. Microsoft Windows file system rights cannot be assigned through eDirectory.

Figure 48-45 *Application Object > Common Tab > File Rights Page*



A user receives these NetWare rights when his or her User object is associated with the Application object, or when a Group, Organizational Unit, Organization, or Country object of which the user is a member is associated with the Application object. The rights are removed from the user when the object is no longer associated with the Application object.

The file rights you set up are not dependent on whether the user is actually using the application. The user has continual file rights from the time the Application object is associated with the user until the time the association is removed.

If two separate Application objects give file rights to the same file, directory, or volume and the user is unassociated with only one of them, then the user loses all rights even though the user might still be associated with the other Application object.

File Rights

The *File rights* list displays all files, directories, and volumes to which rights are given. When you select a file, directory, or volume, the rights that have been granted are displayed in the Rights box. You can grant or remove rights by selecting or deselecting the appropriate check boxes.

Add

Click *Add*, browse for and select the file, directory, or volume you want to add, then click *OK* to display it in the list.

Delete

Select the file, directory, or volume you want to delete from the list, then click *Delete*. Any users associated with the Application object lose rights to the file, directory, or volume.

Rights

Select the file, directory, or volume (in the *File rights* list) for which you are establishing users' rights, then select the appropriate check boxes.

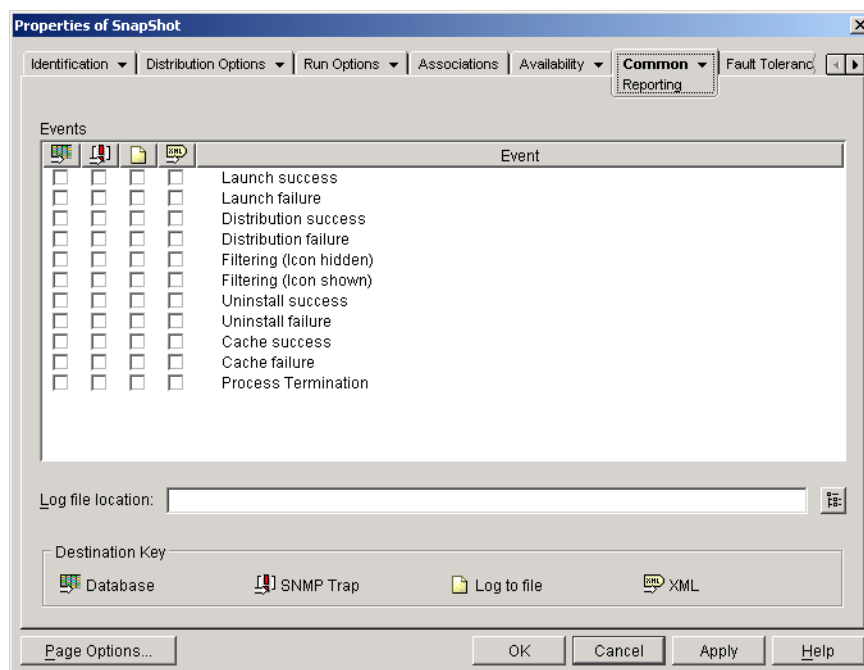
48.6.4 Reporting Page

The Reporting property page is available on Application objects created for all application types (simple, AOT/AXT, MSI, Web, and terminal server).

This section provides information about the fields located on the Reporting property page. For complete instructions on setting up reporting, see [“Reporting Application Events” on page 431](#).

Use the Reporting property page, shown below, to enable Application Launcher to report event information for the application. You can define the events you want Application Launcher to report and also define the destination where you want to send the event reports.

Figure 48-46 Application Object > Common Tab > Reporting Page



Reports contain the following information: event type, date and time, user distinguished name, workstation distinguished name, workstation address, application distinguished name, application global unique identifier (GUID), application version string, and event strings.

Events





Select the events you want reported and the destinations where you want them reported. If necessary, you can send an event report to multiple destinations. All events are described in the following table:

Table 48-3 *Reporting Events*

Event	Description
Launch Success	Occurs when a user double-clicks the Application object and Application Launcher successfully starts the application.
Launch Failure	Occurs when a user double-clicks the Application object and Application Launcher cannot start the application.
Distribution Success	Occurs when Application Launcher successfully modifies the workstation to support the application. Modifications include installation of files, changing of settings (registry, INI, etc.), creation of shortcuts, and so forth.
Distribution Failure	Occurs when Application Launcher cannot modify the workstation to support the application. Modifications include installation of files, changing of settings (registry, INI, etc.), creation of shortcuts, and so forth.
Uninstall Success	Occurs when Application Launcher successfully uninstalls the application from the workstation.
Uninstall Failure	Occurs when Application Launcher cannot uninstall the application from the workstation.
Cache Success	Occurs when Application Launcher successfully caches the application to the workstation.
Cache Failure	Occurs when Application Launcher cannot cache the application to the workstation.
Filter (Icon Hidden)	Occurs when Application Launcher cannot display an Application object on a workstation because the workstation does not meet one or more of the Application object's system requirements (Application object > Availability tab > System Requirements page) and the system requirement's Show Application Icon Even If Criteria Are Not Met option is set to False. The Application object's icon is hidden, or not shown, on the workstation.
Filter (Icon Shown)	Occurs when Application Launcher can only display a disabled (dimmed) Application object on a workstation. This occurs because the workstation does not meet one or more of the system requirements (Application object > Availability tab > System Requirements page) and the system requirement's Show Application Icon Even If Criteria Are Not Met option is set to True. Users can right-click the disabled icon and click Details to see what system requirements are not being met.
Process Termination	Occurs when a user or Application Launcher terminates the application.

All destinations are described in the following table:

Table 48-4 *Reporting Destinations*

Destination	Description
 Database	<p>Application Launcher can write events to any ODBC-compliant database (for example, the Sybase database included with ZENworks). To use a database, you must also create a ZENworks Database object to use for Application Management reporting. This cannot be the same database object used for Inventory reporting.</p> <ul style="list-style-type: none"> • If necessary, create a Service Location Package. Associate the Service Location Package with the containers where the users or workstations reside whose reports you want sent to the database. • Enable the ZENworks Database policy in the Service Location Package. • Associate the ZENworks Database policy with the ZENworks Database object. • Make sure users have the appropriate ODBC database driver installed and configured. • After you've set up database reporting, you can use one of the predefined reports to see information about specific application events. To access the reports, right-click the ZENworks Database object you created for Application Management reporting > click <i>Reporting</i>.
 SNMP Traps	<p>Application Launcher can send SNMP traps to any SNMP management console. To use SNMP traps, you must also enable an SNMP Trap Target Policy in a Service Location Package. It might be necessary to first create the Service Location Package.</p> <ul style="list-style-type: none"> • Associate the Service Location Package with the containers where the users or workstations reside that you want the SNMP Trap Target Policy applied to. • Add the SNMP Trap Targets (IP addresses) for the locations you want the traps sent. • Have a management console that displays the SNMP traps.
 Text Log File	<p>Application Launcher can write events to a text log file. You use the Log File Location field to specify the location of the log file.</p>
 XML	<p>Application Launcher can send events, as XML data, to a URL using the standard HTTP or HTTPS protocol. XML reporting is the recommended method if you want Application Launcher to report events for users located outside of your firewall.</p> <p>To use XML, you must also:</p> <ul style="list-style-type: none"> • Enable an XML URL policy in a Service Location Package. It might be necessary to first create the Service Location Package. • Associate the Service Location Package with the containers where the users or workstations reside whose reports you want sent as XML data. • Make sure you've set up the XML processing mechanism and data storage mechanism. For example, if you are using the Application Management Reporting servlet and the Sybase database, make sure that each are set up and configured properly.

Log File Location

If you selected a log file as the destination for any of the event reports, enter (or browse to and select) the location and name for the log file. You can specify a local drive or a network drive. If you

enter a location that does not exist, Application Launcher creates it. Do not use extended characters in the path; extended characters are not supported.

If you want Application Launcher to log events to a file in a common network location, you need to establish the network directory and provide users with Read and Write rights to files in the directory. Because log file names are established on a per-application basis, you can have individual log files for each application (by specifying a different log file name for each Application object) or one log file for all applications (by specifying the same log file name for all Application objects).

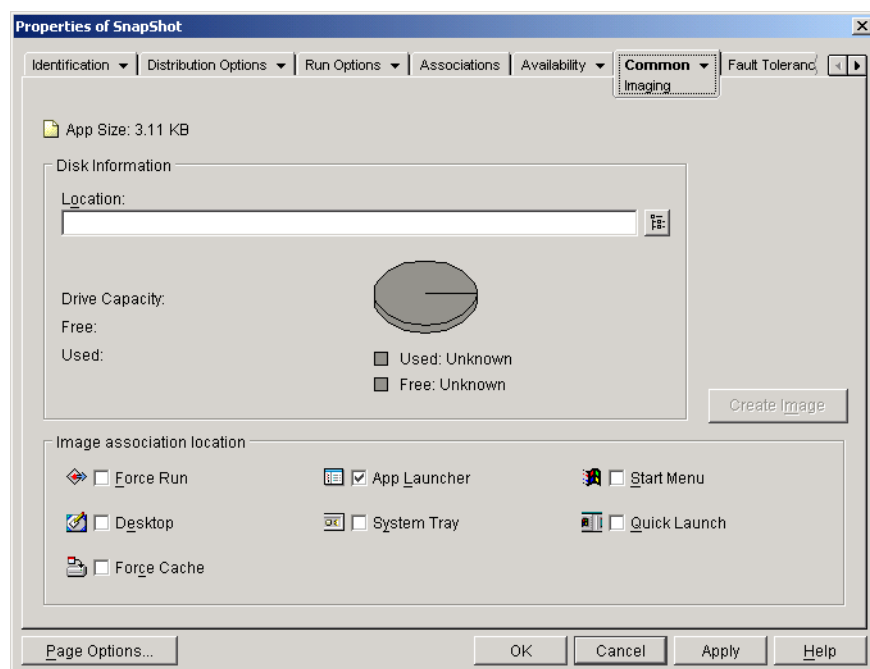
IMPORTANT: You should use log file reporting only if users have a network client such as the Novell Client or Microsoft Client that enables writing to a NetWare, Linux, or Windows server, or if you specify a local drive as the log file location.

48.6.5 Imaging Page

The Imaging property page is available only on Application objects created for simple applications, AOT/AXT applications, and MSI applications. It is not available on Application objects created for Web applications and terminal server applications.

The Imaging property page, shown below, lets you create an image file for the Application object. You can use the image file as an add-on image to a base image file.

Figure 48-47 *Application Object > Common Tab > Imaging Page*



If the application includes any dependent applications (*Application object > Run Options tab > Application Dependencies page*), the dependent applications must also be included as add-on images if they have not already been distributed to the user's workstation.

App Size

This field displays the size of the of the Application object. This includes all Application object information and application source files (as listed on the Application Files page). This is the size of the image file if you do not use a compression option.

When you image an MSI Application object, ConsoleOne is unaware of the files referenced or included in the `.msi` file. Therefore, it includes the `.msi` file and all files and folders at the same level or below. This ensures that all related files are included with the `.msi` file, but might also result in non-related files being included. To avoid this situation, make sure the folder where the `.msi` file is located contains only the `.msi` file and its related files and folders.

Disk Information

These fields let you specify a location and filename for the image and ensure that the disk to which you are saving the image has sufficient free space.

Location

Specify the location and filename for the image. You might want to save it in the same location as the base image file. The filename must have a `.zmg` file extension.

Drive Capacity, Free, and Used

After you've entered a location for the file, these fields display the amount of space on the disk, the amount of available free disk space, and the amount of used disk space. Verify that the Application object fits in the amount of free disk space.

In addition to the image location, the NAL cache directory located on the workstation's Windows drive (typically `c:\nalcache`) is used temporarily to store the application's source files (`.fil` files) and the Application object's settings (`.aot/.axt` file). The size of the source files varies; the size of the settings file is typically less than 200 KB. Make sure that the workstation's Windows drive has sufficient disk space for these files.

Image Association Location

Specify the association characteristics for the Application object. These are enforced when the image is applied to the workstation.

Force Run

Automatically runs the application. With a user-associated application, the application is run immediately after Application Launcher starts. With a workstation-associated application, the application is run immediately after the workstation starts up (initial startup or reboot).

You can use the *Force run* option in conjunction with several other settings to achieve unique behaviors. For example, if you use the *Force run* option with the *Run application once* option (*Run Options* tab > *Applications* page), as soon as the Application object is distributed it runs one time and is removed from the workstation. Or, suppose that you want to run the Application object immediately one time at a predetermined time. If so, select *Force run*, select the *Run application once* option on the Application page (Run Options tab), and define a schedule using the Schedule page (Availability tab).

If you want to force run several applications in a specific order, mark each of them as *Force run*. Then give each Application object a numeric order by using the *Determine force run order* option on the Icon page (Identification tab).

App Launcher

Adds the Application object's icon to the Application Window, the Application Explorer window, and the Application Browser window.

Start Menu

If the workstation is running Application Explorer, this option adds the Application object to the Windows Start menu. The Application object is added to the top of the Start menu, unless you assign the Application object to a folder and use the folder structure on the Start menu. See the Application object's Folders page (Identification tab).

Desktop

If the workstation is running Application Explorer, this option displays the Application object's icon on the Windows desktop.

System Tray

If the workstation is running Application Explorer, this option displays the Application object's icon in the Windows system tray.

Quick Launch

Displays the Application object's icon on the Windows Quick Launch bar.

Force Cache

Forces the application source files and other files required for installation to be copied to the workstation's cache directory. The user can then install or repair the application while disconnected from eDirectory. The files are compressed to save space on the workstation's local drive.

Create Image

After you've defined the image location and selected the image associations, click the *Create Image* button to create the image. A dialog box appears that lets you select from the following compression options:

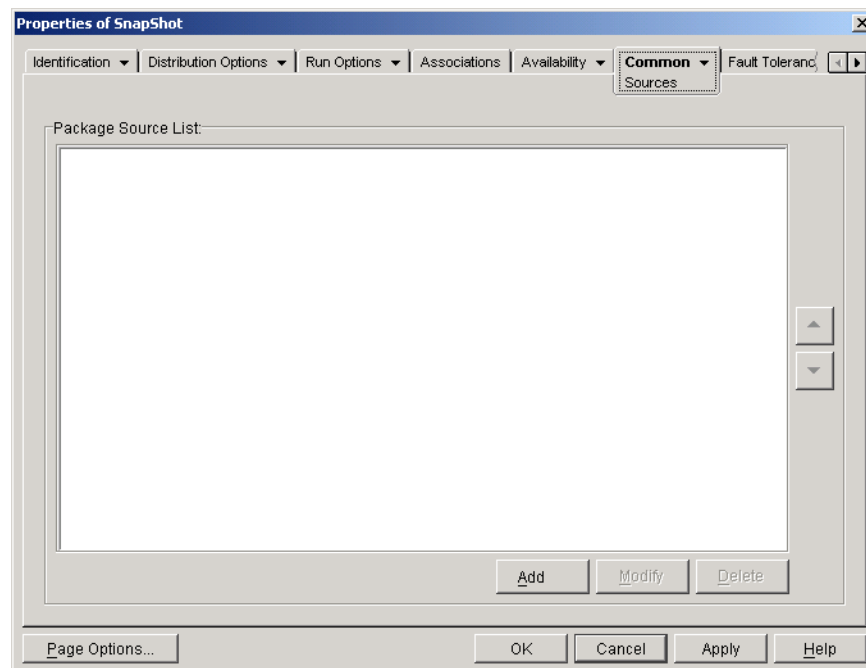
- **None:** Creates the image file but does not compress it. This results in the largest image size produced by any of the compression options.
- **Optimize compression time:** Applies the lowest level of compression. This minimizes the time required to compress the image file, but results in a larger file size than could be achieved by using the *Balance compression time and image size* option or *Optimize image size* option.
- **Balance compression time and image size:** Applies a medium level of compression in order to balance the amount of time required to compress the file against the size of the image file.
- **Optimize image size:** Applies the highest level of compression. This decreases the image file size but increases the time required to compress the image file as compared to the *Optimize compression time* option and *Balance compression time and image size* option.

48.6.6 Sources Page

The Sources property page is available on Application objects created for simple applications, AOT/AXT applications, and MSI applications only. It is not available on Application objects created for Web applications and terminal server applications.

The Sources property page, shown below, specifies additional network locations that contain installation packages from which Application Launcher can distribute the application. If the Application object was created from an .aot or .axt file, the installation packages must be snAppShot packages (.aot, .axt, and .fil files). If the Application object was created from an .msi file, the installation packages must be Microsoft Windows Installer packages (.msi files). The source list is used only if the original source location is unavailable, in which case Application Launcher begins with the first location in the list and continues down the list until an accessible package is found.

Figure 48-48 *Application Object > Common Tab > Sources Page*



Before you can define additional source locations, you need to make sure to copy the original package to the new source locations. For snAppShot packages, copy the .aot, .axt, .fil, and .txt files. For Windows Installer packages, copy the administrative installation folder and all subfolders.

With Application objects that use an .msi file rather than an .aot or .axt file, this source list can be extremely important. Because Windows Installer supports on-demand installations (installation of files as the user requests certain features or components), the source list can provide source resiliency for installations that occur after the initial installation. If the original installation source is no longer available and no source list has been established, the on-demand installation fails. However, if you create additional source locations and define them in the source list, the on-demand installation has a better chance of succeeding.

IMPORTANT: If you have used the SOURCE_PATH macro (Common > Macros page) in any of the Application object's property fields, you should verify that you used all uppercase letters and no lowercase letters. If the original source location is referenced through the SOURCE_PATH macro and Application Launcher cannot access the location, it uses the package sources in this list only if the SOURCE_PATH macro is all uppercase.

Package Source List

The *Package source* list displays the additional package source locations that have been defined for the application. When the application is distributed to a workstation, Application Launcher uses these locations, in the order listed, if the original source location is unavailable.

When distributing applications that use the Windows Installer, Application Launcher passes the source list to the Windows Installer, which then uses the list for the locations from which to install the application files.

Add

To add a source location to the list, click *Add*, browse to and select the directory that contains the installation package, then click *OK*.

Delete

To remove a source location from the list, select the location > click *Delete*.

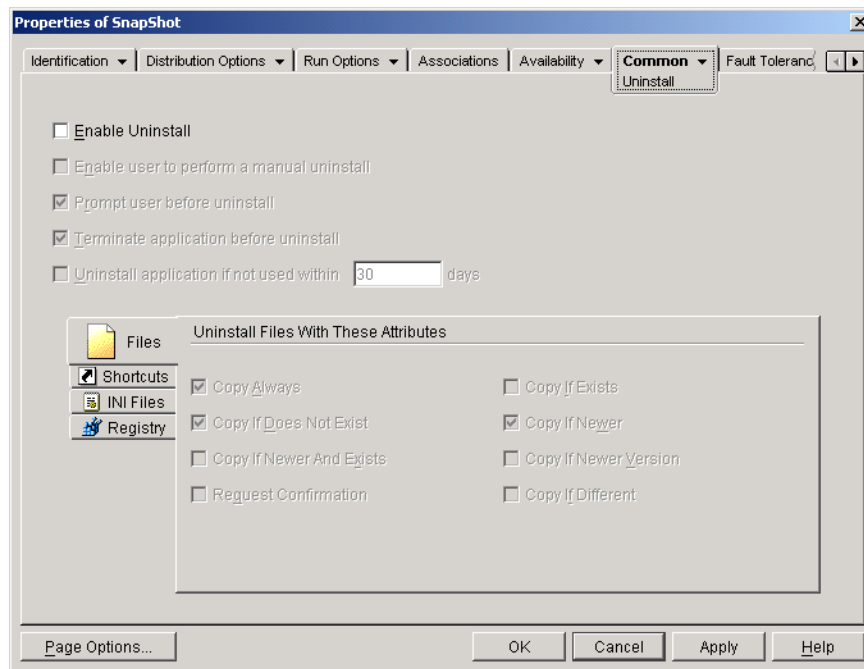
48.6.7 Uninstall Page

The Uninstall property page is available on Application objects created for all application types (simple, AOT/AXT, MSI, Web, and terminal server).

This section provides information about the fields located on the Uninstall property page. For complete instructions on uninstalling applications, see [“Uninstalling Applications” on page 425](#).

The Uninstall property page, shown below, enables the application to be uninstalled and determines the behaviors associated with uninstalling the application.

Figure 48-49 Application Object > Common Tab > Uninstall Page



When Application Launcher distributes an application to a workstation, it creates a cache directory on the workstation that contains the information required to successfully uninstall the application. However, when Application Launcher distributes an application to a terminal server, it does not create a cache directory, which means that it does not have the information to uninstall the application from the terminal server. Therefore, the *Uninstall* options on this page do not apply when the application is installed on a terminal server. If you no longer want the application on the terminal server, you must manually uninstall it.

Enable Uninstall

Select this option to enable the application to be removed from the workstation. The other uninstall options are available only if this option is enabled.

Enable User to Perform a Manual Uninstall

Select this option to enable users to remove the application from their workstations. If this option is not enabled, only you or other administrators can remove applications.

Prompt User Before Uninstall

Select this option to prompt users before removing the application from their workstations. If users answer “No” to the prompt, the application is not removed.

Terminate Application Before Uninstall

Select this option to ensure that Application Launcher terminates the application (if the application is running) before it begins uninstalling the application files.

Uninstall Applications If Not Used Within XX Days

Select this option to automatically remove the application if the user has not run it within the specified number of days (the default is 30).

Files

Click *Files*, then select the attributes you want to use to determine whether or not a file is removed. The attributes correspond to the attributes listed on the Application Files page (Distribution Options tab). The default selections (*Copy always*, *Copy if does not exist*, *Copy if newer*) ensure that a file is removed only if it was installed when the application was installed and not at an earlier time by another application that also needs the file.

Application Launcher does not uninstall files that are copied to the workstation using wildcards. For example, assume you copy `\\server\vol\public\zenworks\sysapps*. *` to `c:\winnt\system32`. When you uninstall the application, its files are not removed from `c:\winnt\system32`. To perform an uninstall, Application Launcher simply reverses the install process, which means that if it uninstalled the files in the previous example, it would do so by doing a wildcard delete (delete `c:\winnt\system32*. *`). Because this could have undesirable results, Application Launcher has been designed to not uninstall files that are copied using wildcards.

Shortcuts

Click *Shortcuts*, then select the attributes you want to use to determine whether or not the application's shortcuts are removed. The attributes correspond to the attributes listed on the Shortcuts/Icons page (Distribution Options tab).

INI Files

Click *INI Files*, then select the attributes you want to use to determine whether or not an INI setting is removed. The attributes correspond to the attributes listed on the INI Settings page (Distribution Options tab). The default selections (*Create always*, *Create if exists*, *Create or add to existing section*) ensure that a setting is removed only if it was created when the application was installed and not at an earlier time by another application that also needs the setting.

Registry

Click *Registry*, then select the attributes you want to use to determine whether or not a registry setting is removed. The attributes correspond to the attributes listed on the Registry Settings page (Distribution Options tab). The default selections (*Create always*, *Create if exists*) ensure that a setting is removed only if it was created when the application was installed and not at an earlier time by another application that still needs the setting.

Uninstall Keys/Values From These Registry Hives

This option allows you to select two specific registry hives, `HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER`, to include or exclude when removing the registry settings that were added

by Application Launcher during distribution of the application to the workstation. The default settings cause Application Launcher to remove settings from the HKEY_CURRENT_USER hive but not from the HKEY_LOCAL_MACHINE hive.

The purpose of this option is to help you ensure that no Windows system settings are removed during the uninstall. This is particularly important if you used snAppShot to capture the application's installation. When snAppShot captures an application's installation, it includes all settings that are changed during the installation. If the application's installation program causes the workstation to reboot during the installation process, these changes can include not only settings that apply to the application but also settings that apply to the Windows system. Removing Windows system settings might cause the workstation to encounter problems when starting up. We strongly recommended that you remove these settings only if you are positive that they do not affect the workstation's ability to function properly.

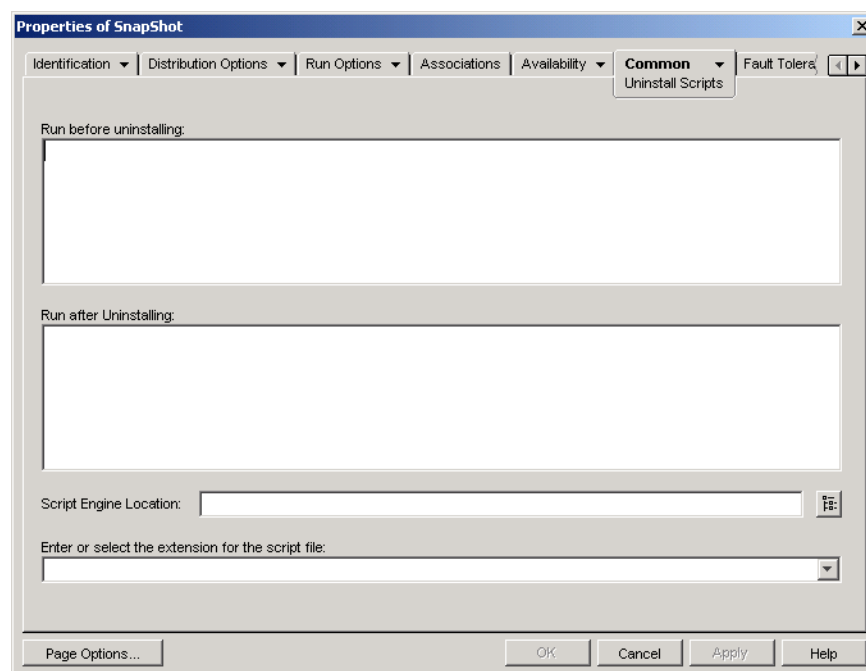
If you want to use this option, you should examine the registry settings that will be removed from the HKEY_LOCAL_MACHINE and HKEY_CURRENT_USER hives and delete any settings that apply to anything other than the application. The registry settings are displayed on the Registry Settings page (Distribution Options tab).

48.6.8 Uninstall Scripts Page

The Uninstall Scripts property page is available only on Application objects created for simple applications, AOT/AXT applications, and MSI applications. It is not available on Application objects created for Web applications and terminal server applications.

As part of the process of uninstalling the application, Application Launcher can launch a script engine to execute a “before uninstall” script and an “after uninstall” script. The Uninstall Scripts page, shown below, defines the script engine that you want Application Launcher to use and the scripts you want executed.

Figure 48-50 Application Object > Common Tab > Uninstall Scripts



On Windows 2000/XP, uninstall scripts always run in the user space for both user-associated applications and workstation-associated applications. This is the same behavior as launch scripts (*Run Options* tab > *Launch Scripts*) but different than the behavior for distribution scripts (*Distribution Options* tab > *Distribution Scripts*), which run in the secure system space.

Run Before Uninstalling

Use this text box to specify any script commands you want executed before the application is uninstalled. Do not use extended characters in the script; extended characters are not supported. For script example, see “[Script Example](#)” on page 568.

Run After Uninstalling

Use this text box to specify any script commands you want executed after the application is uninstalled. Do not use extended characters in the script; extended characters are not supported. For script example, see “[Script Example](#)” on page 568.

Script Engine Location

The script engine determines the script commands and scripting language you need to use. If you do not define a script engine in the *Script engine location* field, Application Launcher uses the Novell Client as the script engine (if the workstation has the Novell Client installed), which means that you can use most Novell Client login script commands (see “[Supported Novell Client Login Script Commands](#)” on page 568).

If you want to use a script engine other than the Novell Client, specify the alternate script engine. The script engine must reside in a location that is always available to users, such as their local drives. The script engine can reside on a network server only if users can map a drive to the server (for example, through the Novell Client or the Client for Microsoft Networks). If Application Launcher cannot find the script engine, it displays an error to the user and fails to uninstall the application.

If you use the Windows command interpreter as the script engine, you must include the `/c` switch, as shown in the following examples:

- Windows 2000/XP: `%*winsysdir%\cmd.exe /c`
- Windows 98: `%*windir%\command.com /c`

The `%*winsysdir%` and `%*windir%` variables specify the Windows system directory (for example, `c:\winnt\system32`), and the `/c` switch instructs the command interpreter to execute the script and then stop. If the `/c` switch is not used, the script does not complete.

For a script example, see “[Script Example](#)” on page 568.

Script File Extension

This applies only if you specified a script engine in the *Script engine location* field.

When the application is uninstalled, Application Launcher creates temporary script files for the *Run before uninstall* scripts and *Run after uninstall* scripts. These files are passed to the script engine, which then executes the script. You need to specify the file extension that the script engine requires for its script files.

For a script example, see “[Script Example](#)” on page 568.

Script Example

The following script uses the Windows 2000/XP command interpreter as the script engine. Before the distribution occurs, a listing of the `c:\` directory is saved to a text file and the `autoexec.bat` file is backed up.

Run Before Uninstalling Field

```
dir c:\ >c:\1.txt  
copy autoexec.bat autoexec.bak /y
```

Script Engine Location Field

```
cmd.exe /c
```

Enter or Select the Extension of the Script File Field

```
.bat
```

Supported Novell Client Login Script Commands

When using the Novell Client as the script engine, you can use all but the following script commands:

Table 48-5 *Supported Novell Client Login Script Commands*

CLS	INCLUDE	PCOMPATIBLE
DISPLAY	LASTLOGINTIME	SCRIPT_SERVER
EXIT	NO_DEFAULT	SET_TIME
FDISPLAY	NOSWAP	SWAP
IF MEMBER OF	PAUSE	WRITE

Application Launcher does not output anything to the screen or display script errors.

For script commands, syntax, and examples, see the [Novell Client documentation \(http://www.novell.com/documentation/lg/noclienu/docui/index.html\)](http://www.novell.com/documentation/lg/noclienu/docui/index.html) on the [Novell Documentation Web site \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

48.7 MSI Tab

The MSI tab is available only on Application objects created for MSI applications.

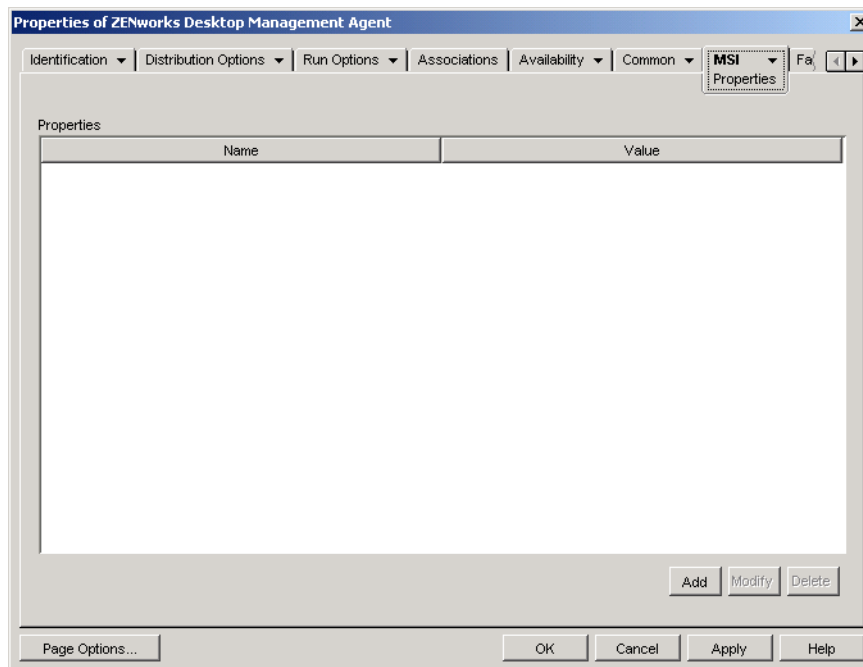
The MSI tab includes the following pages to help you configure and manage the distribution of MSI applications installed through the Microsoft Windows Installer:

- [Section 48.7.1, “Properties Page,” on page 569](#)
- [Section 48.7.2, “Transforms Page,” on page 570](#)
- [Section 48.7.3, “Verify Page,” on page 571](#)
- [Section 48.7.4, “Patches Page,” on page 573](#)

48.7.1 Properties Page

The Properties property page, shown below, lets you override the public property values contained in the MSI package and add new public properties.

Figure 48-51 *Application Object > MSI Tab > Properties Page*



The MSI package contains the property values that were defined during the administrative installation of the application. These property values determine the way the Microsoft Windows Installer installs the application to the user's workstation. In some cases, you might want to change one or more of the property values. For example, a property value might define the default location for a user's work files. By adding the property to the Properties list and changing the property's value, you can override the default location defined in the MSI package.

If necessary, you can add public properties that were not included in the MSI package. When doing so, you should be careful to add only those properties that are valid for the package.

Add

To override a property value, you change the property value and add the property to the *Properties* list so that Application Launcher knows to use that property value rather than the one defined in the MSI package. To do so, click *Add* to display the Select Property to Add dialog box. In the *Value name* field, select the property whose value you want to override, specify the new value in the *Value data* field, then click *OK* to add the property to the *Properties* list.

To define a new property that is not already included in the MSI package, click *Add* to display the Select Property to Add dialog box. In the *Value name* field, specify the new property's name, enter the property's value in the *Value data* field, then click *OK* to add the property to the *Properties* list.

For a list of properties and descriptions, see the [Microsoft Developer Network \(MSDN\)](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/property_reference.asp) (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/property_reference.asp).

Although you can add and define new properties, the *SOURCELIST* property is reserved for Application Launcher use.

NOTE: When Application Management distributes and installs an MSI application, it uses the AlwaysInstallElevated policy, which installs the MSI application using elevated (system) privileges. Because of this, in order to set the *ALLUSERS* property value to null so that the application is installed on a per-user basis, you need to leave the *Value data* field empty. Using double quotation marks (“”) causes the distribution to fail.

Modify

To modify a property that is in the *Properties* list, select the property, click *Modify* to display the Edit String Value dialog box, modify the value data, then click *OK*.

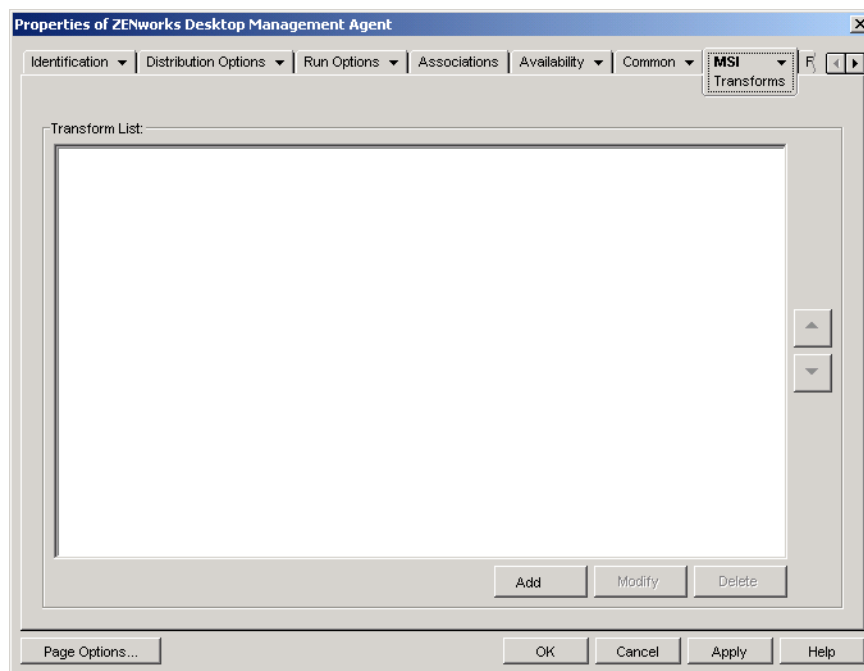
Delete

To delete a property from the Properties list, select the property, then click *Delete*. Deleting the property causes future installations of the application to use the property value defined in the MSI package.

48.7.2 Transforms Page

The Transforms property page, shown below, lists the transforms that Microsoft Windows Installer applies to the MSI package during distribution. A transform adds, deletes, or changes properties in the MSI package to enable customizing of the installation for different groups of users.

Figure 48-52 *Application Object > MSI Tab > Transforms Page*



Transforms are applied in the order they appear in the *Transform* List. If two transforms modify the same package property, the property retains the value applied by the last transform.

For information about creating transforms for your MSI package, see the documentation you received with the software application.

Add

Click *Add*, browse to and select the transform file (.mst file) you want added to the *Transform* list, then click *OK* to add it to the list. If the transform file is in the same directory as the .msi file, you can simply enter the filename in the *Transform path* field rather than browsing to and selecting it. If you select the file, make sure that the resulting path is either a UNC path or mapped path common to all users.

Delete

Select a transform from the *Transforms list*, then click *Delete* to remove it from the list.

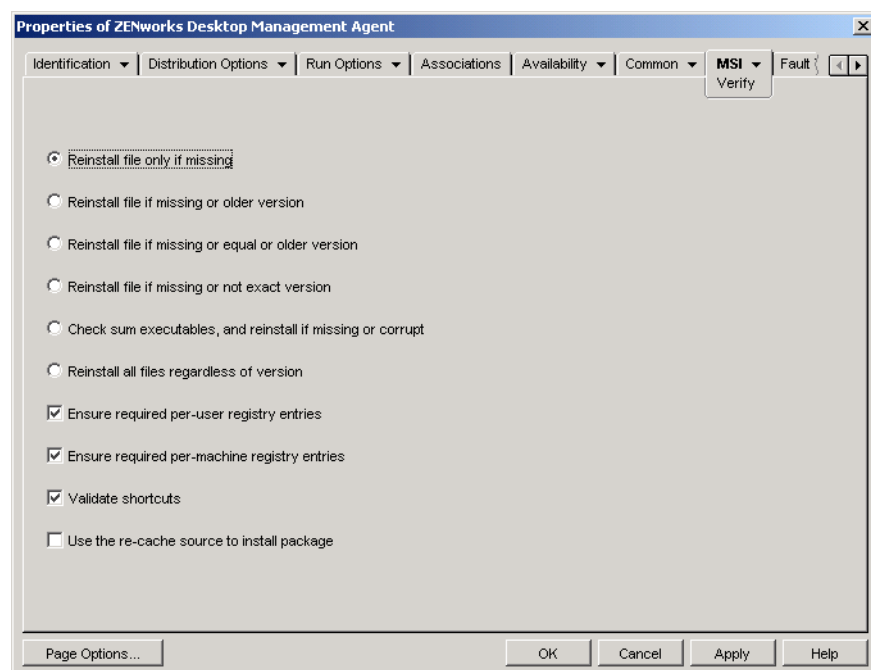
Up-Arrow and Down-Arrow

Select a transform from the *Transform list*, then click the up-arrow to move the transform up in the list or click the down-arrow to move it down in the list. Microsoft Windows Installer applies the transforms in the order they are listed, from top to bottom.

48.7.3 Verify Page

The Verify property page, shown below, determines the actions that Microsoft Windows Installer takes when instructed to verify the application.

Figure 48-53 *Application Object > MSI Tab > Verify Page*



When a user verifies the MSI application, Application Launcher launches Windows Installer. If no options are selected, Windows Installer performs a full verification, which results in all files,

settings, and so forth being reinstalled. If one or more options are selected, Windows Installer only performs the actions specified by the selected options.

The reinstall options are mutually exclusive, meaning that you can only select one of the options. The remaining four options are independent of one another: some, all, or none can be selected.

Reinstall File Only if Missing

Instructs Windows Installer to reinstall a file only if it is missing.

Reinstall File if Missing or Older Version

Instructs Windows Installer to reinstall a file if it is missing or if the installed file's version is older than the file in the MSI package.

Reinstall File if Missing or Equal or Older Version

Instructs Windows Installer to reinstall a file if it is missing or if the installed file's version is the same as or older than the file in the MSI package.

Reinstall File if Missing or Not Exact Version

Instructs Windows Installer to reinstall a file if it is missing or if the installed file's version is not exactly the same as the file in the MSI package.

Check Sum Executables, and Reinstall if Missing or Corrupt

Instructs Windows Installer to perform a checksum on all executable files and to reinstall a file if it is missing or if the checksum verifies that the file is corrupt. Only files that have `msidbFileAttributesChecksum` in the *Attributes* column of the MSI package's File Table are repaired.

Reinstall All Files Regardless of Version

Instructs Windows Installer to reinstall all files.

Ensure Required Per-User Registry Entries

Instructs Windows Installer to rewrite all per-user entries from the MSI package to the Windows system registry. Per-user entries are those entries contained in the `HKEY_CURRENT_USER` and `HKEY_USERS` registry hives.

Ensure Required Per-Machine Registry Entries

Instructs Windows Installer to rewrite all per-machine entries from the MSI package to the Windows system registry. Per-machine entries are those entries contained in the `HKEY_LOCAL_MACHINE` and `HKEY_CLASSES_ROOT` registry hives.

Validate Shortcuts

Instructs Windows Installer to reinstall the MSI application's shortcuts, overwriting any existing shortcuts and icons.

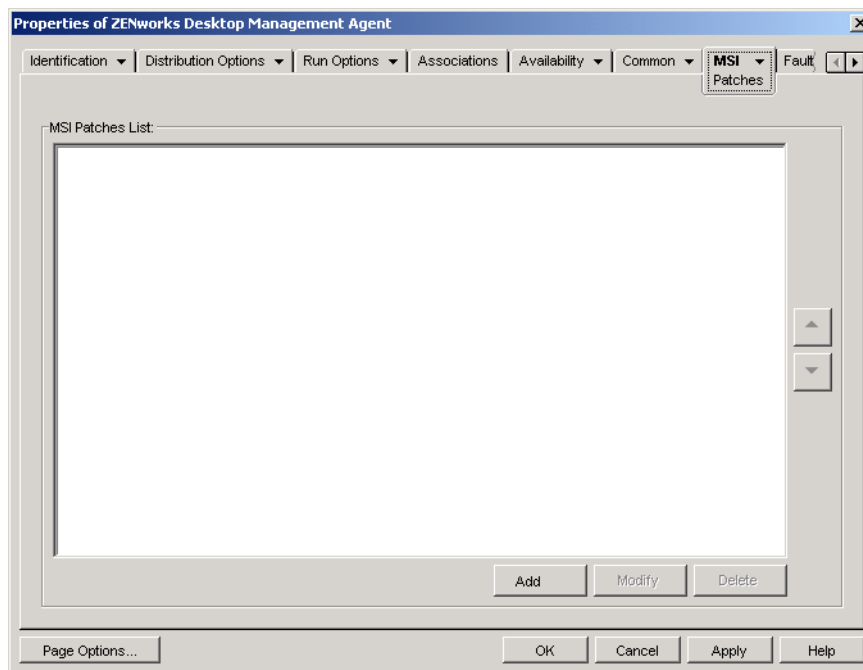
Use the Re-Cache Source to Install Package

Instructs Windows Installer to install files from the re-cache (local) source rather than the source package.

48.7.4 Patches Page

The Patches property page, shown below, lists the patch files that Microsoft Windows Installer applies to the MSI package during distribution. Each patch is applied in the order listed in the MSI Patches List.

Figure 48-54 *Application Object > MSI Tab > Patches Page*



Add

Click *Add*, browse to and select the patch file (.msp file or other MSI-based patch file) you want added to the MSI Patches List, then click *OK* to add it to the list. If the patch file is in the same directory as the .msi file, you can simply enter the filename in the MSI Patch File field rather than browsing to and selecting it. If you select the file, make sure that the resulting path is either a UNC path or mapped path that is common to all users.

Modify

Select a patch from the *MSI patches* list, then click *Modify* to edit the location of the patch.

Delete

Select a patch from the *MSI patches* list, then click *Delete* to remove it from the list.

Up-Arrow and Down-Arrow

Select a patch from the MSI Patches List, then click the up-arrow to move the patch up in the list or click the down-arrow to move it down in the list. Microsoft Windows Installer applies the patches in the order they are listed, from top to bottom.

48.8 Terminal Server Client Tab

The Terminal Server Client tab is available only on Application objects created for terminal server applications.

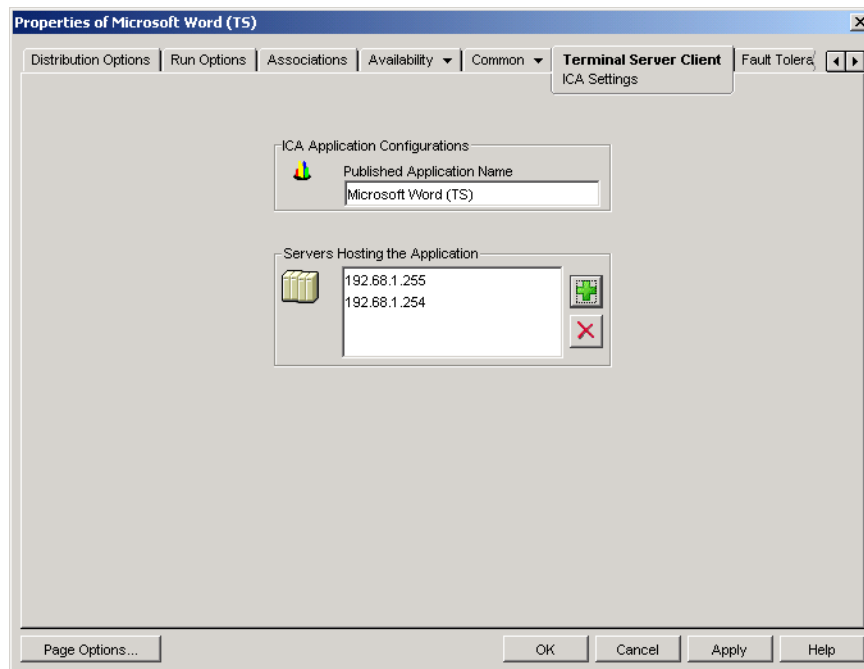
The Terminal Server Client tab includes one of the following pages, depending on whether the Application object's defined client protocol is ICA or RDP:

- “ICA Settings Page” on page 574
- “RDP Settings Page” on page 575

48.8.1 ICA Settings Page

The ICA Settings property page, shown below, lets configure the settings used by the Citrix ICA client when launching the application from a Citrix MetaFrame Server.

Figure 48-55 Application Object > Terminal Server Client Tab > ICA Settings Page



Published Application Name

Specify the application name exactly as it is defined in Citrix.

Servers Hosting This Application

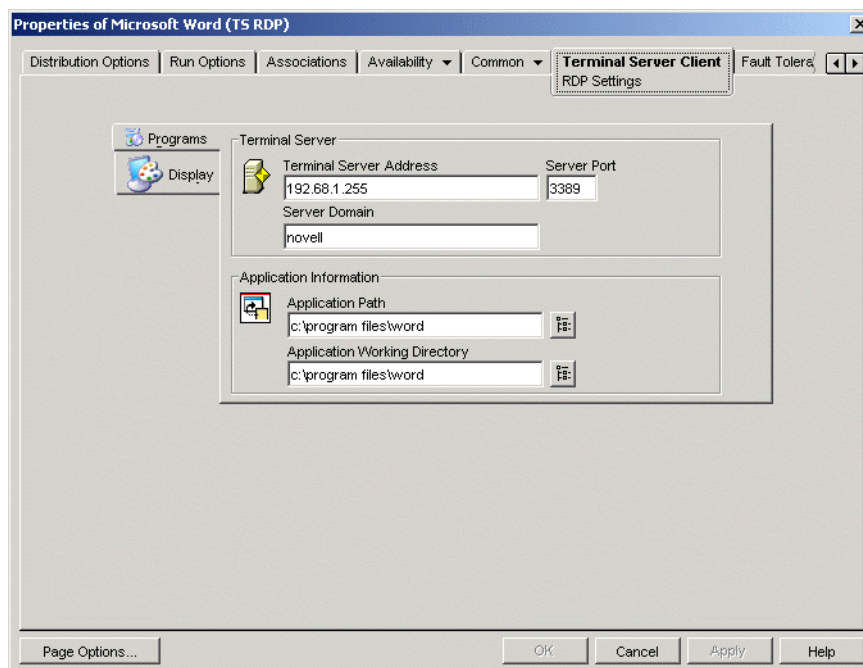
Add the Citrix servers that host the application. To add a server, click the *Add* button, specify the server's IP address or hostname, then click *OK*.

The server's you define here are used only when the application is launched from Application Launcher or the NAL plug-in. The ZENworks Launch gadget uses the servers defined in its configuration settings. For information about the ZENworks Launch gadget's configuration settings, see [Chapter 26, “ZENworks Launch Gadget: Configuring Settings,” on page 309](#).

48.8.2 RDP Settings Page

The RDP Settings property page lets you configure the settings used by the RDP client when launching the application from a Windows Terminal Server.

Figure 48-56 *Application Object > Terminal Server Client Tab > Window Page*



Programs

The Program settings define the location from which the application runs. Click the *Programs* tab to show the following settings.

- **Terminal server address and server port:** Specify the terminal server's IP address or hostname. If the terminal server is not using default port 3389, edit the Server Port field to specify the correct port number.
- **Server domain:** If the terminal server is part of a Windows NT domain or an Active Directory domain, specify the domain name. If a user's name and password in the domain matches the user name and password in eDirectory, the user is not prompted to log in to the terminal server when launching the application.

- **Application path:** Specify the path to the application's executable file from the perspective of the terminal server. If you are running ConsoleOne on the terminal server, you can browse for and select the file.
- **Working directory:** Specify the path to the directory you want the application to use for its working files.

Display

The Display settings determine the window size and number of colors used for the RDP client session. Click the Display tab to show the following settings.

- **Remote desktop size:** Select the window size for the RDP client session. The window size determines the resolution at which information is displayed and the amount of screen area used for the window. The higher the resolution, the smaller the window size and information display.
- By default, the user's RDP client setting is used. You can change the size to full screen or another standard screen resolution.
- **Colors:** Select the number of colors for the RDP client session. You can select 256 colors, high color (15 bits), high color (16 bits), or true color (32 bits). The default is 256 colors.

48.9 Fault Tolerance Tab

The Fault Tolerance tab includes the following pages to help you balance the workload required to host an application between multiple servers and provide access to backup applications in case of server failure:

- [Section 48.9.1, “Fault Tolerance Page,” on page 576](#)
- [Section 48.9.2, “Load Balancing Page,” on page 578](#)
- [Section 48.9.3, “Site List Page,” on page 580](#)
- [Section 48.9.4, “Remote Alternate App Page,” on page 582](#)

48.9.1 Fault Tolerance Page

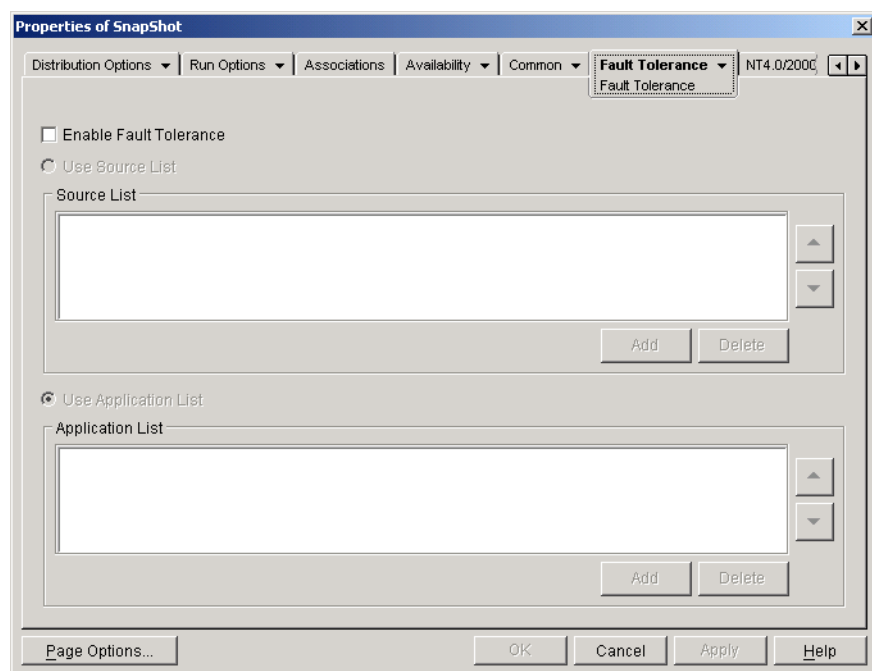
The Fault Tolerance property page is available only on Application objects created for simple applications and AOT/AXT applications. It is not available on Application objects created for MSI applications, terminal server applications, and Web applications.

This section provides information about the fields located on the Fault Tolerance property page. For complete instructions on setting up fault tolerance, see [Section 36.1, “Setting Up Fault Tolerance,” on page 377](#).

The Fault Tolerance property page, shown below, specifies the installation package sources or Application objects that Application Launcher uses as backups if this Application object becomes

unavailable. Application Launcher tries the package sources or Application objects in the order shown in the *Source List* or *Application List*, from top to bottom.

Figure 48-57 *Application Object > Fault Tolerance Tab > Fault Tolerance Page*



The Fault Tolerance page varies according to the type of application. For simple/AOT/AXT applications, the page looks like the one shown above. For Web applications, the page includes only the Application List because the Source List functionality is not supported.

Enable Fault Tolerance

Select this option to enable fault tolerance. The other fault tolerance options are available only if this option is enabled.

Use Source List

Select this option to have Application Launcher use a list of installation package sources as the backup. You must have already created at least one package source (*Common > Sources* page).

Add

Click *Add*, browse to and select a package source, then click *OK* to add it to the Source List.

Delete

Select a package source from the Source List, then click *Delete* to remove it from the Source List.

Up-Arrow and Down-Arrow

Select a package source from the *Source* list, then click the up-arrow to move the source up in the list or click the down-arrow to move it down in the list. Application Launcher tries the sources in the order they are listed, from top to bottom.

Use Application List

Select this option to have Application Launcher use a list of Application objects as the backup. You must have already created additional Application objects for the application, with the application files being stored on a different server or volume than this application. If the application is not available, then Application Launcher tries each Application object in the specified order.

Only one-level-deep fault tolerance is supported. If Application Launcher fails over to one of the backup Application objects in the list and the backup Application object fails, the distribution fails even if fault tolerance is enabled for the backup Application object.

NOTE: If Application Launcher has detected a remote connection and is running in remote mode, it does not use the Application List for fault tolerance. Application Launcher uses only the Source List.

Add

Click *Add*, browse to and select an Application object, then click *OK* to add it to the Application List.

Delete

Select an Application object from the *Application* list, then click *Delete* to remove it from the Application List.

Up-Arrow and Down-Arrow

Select an Application object from the *Source* list, then click the up-arrow to move the Application object up in the list or click the down-arrow to move it down in the list. Application Launcher tries the Application objects in the order they are listed, from top to bottom.

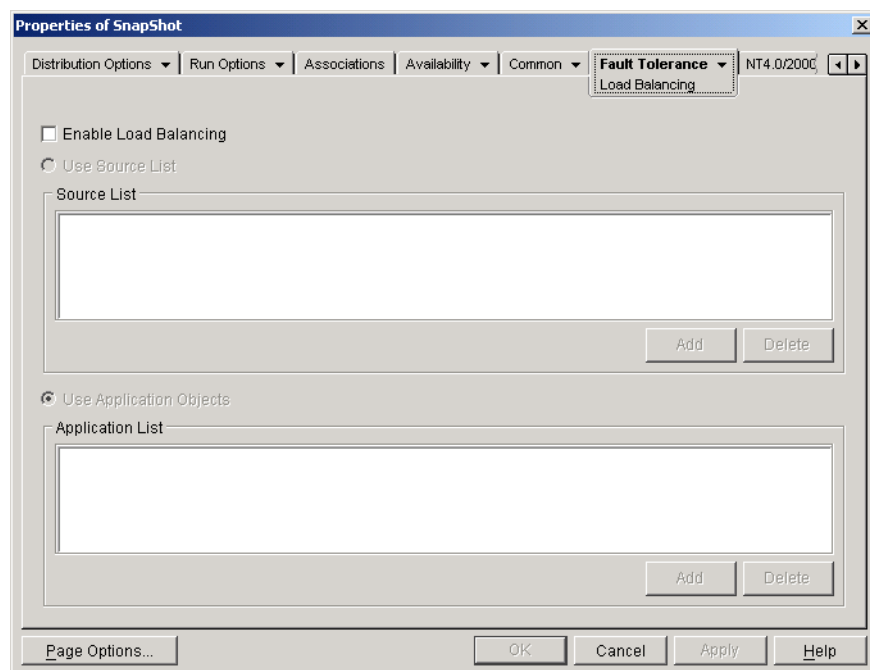
48.9.2 Load Balancing Page

The Load Balancing property page is available only on Application objects created for simple applications, AOT/AXT applications, and MSI applications. It is not available on Application objects created for terminal server applications and Web applications.

This section provides information about the fields located on the Load Balancing property page. For complete instructions on setting up load balancing, see [Section 36.2, “Setting Up Load Balancing,” on page 381](#).

The Load Balancing property page, shown below, lets you balance the work of distributing the application. With load balancing enabled, Application Launcher distributes the application from all servers offering the application, ensuring a more balanced workload across servers.

Figure 48-58 *Application Object > Fault Tolerance Tab > Load Balancing Page*



The Load Balancing page varies according to the type of application. For simple/AOT/AXT applications, the page looks like the one shown above. For MSI applications, it looks like the one above, but Enable Load Balancing is the only available option. For Web applications, the page includes only the Application List because the Source List functionality is not supported.

To use load balancing, you must first have multiple installation package sources or Application objects defined for the application, with the application source files located on different servers. When a user launches the application, Application Launcher selects one of the package sources or Application objects to use. If the package source or Application object is unavailable, Application Launcher selects another one.

Enable Load Balancing

Select this option to enable load balancing. The other load balancing options are available only if this option is enabled.

For Application objects that use Microsoft Windows Installer (MSI) packages, the *Enable load balancing* option is the only option that is enabled on this page; the *Use source list* and *Use application list* options are disabled. To enable load balancing for an MSI Application object, select this option and then use the Application object's Sources page (Common tab) to define the list of source locations where you've created additional installation packages for the application. Application Launcher randomly selects source locations from the list to balance the workload.

Use Source List

Select this option to have Application Launcher use a list of package sources for load balancing. You must have already created at least one package source (*Common > Sources* page).

Add

Click *Add*, browse to and select a package source, then click *OK* to add it to the Source List.

Delete

Select a package source from the Source List, then click *Delete* to remove it from the Source List.

Use Application List

Select this option to have Application Launcher use a list of Application objects for load balancing. You must have already created additional Application objects for the application, with the application files being stored on a different server or volume than this application.

Add

Click *Add*, browse to and select an Application object, then click *OK* to add it to the Application List.

Delete

Select an Application object from the *Application* list, then click *Delete* to remove it from the Application List.

48.9.3 Site List Page

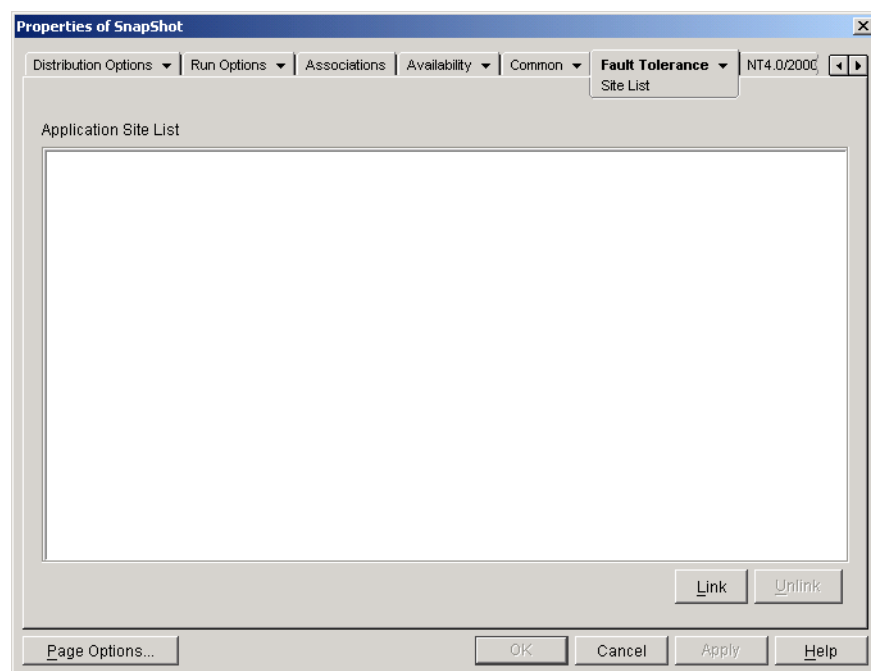
The Site List property page is available only on Application objects created for simple applications, AOT/AXT applications, MSI applications, and terminal server applications. It is not available on Application objects created for Web applications.

This section provides information about the fields located on the Site List property page. For complete instructions on setting up site lists, see [Section 36.3, “Setting Up Site Lists,” on page 385](#).

The Site List property page, shown below, lets you link an application at one site (Site1) to an application at another site (Site2). By linking applications whose source installation packages are

located on servers at different sites, you can distribute the application from the server that is closest to the user.

Figure 48-59 *Application Object > Fault Tolerance Tab > Site List Page*



For example, you have two different sites, Site1 and Site2. Employees at both sites use the same spreadsheet program. Site1 has an Application object (App1) that distributes the spreadsheet program from a Site1 server, and Site2 has its own Application object (App2) to distribute the program from a Site2 server. If you link App1 to App2, any Site1 employee who travels to Site2 and launches App1 has App2 installed from the Site2 server. Likewise, any Site2 employee who travels to Site1 and launches App2 has App1 installed from the Site1 server.

The site list is a distribution mechanism that applies only to undistributed, non-cached applications. If an application is already distributed or cached on a user's workstation, that application is used regardless of the site list.

Novell Client vs. ZENworks Middle Tier Server

When a user logs in to Novell eDirectory through the ZENworks Middle Tier Server rather than the Novell Client, site lists work slightly differently. Rather than the Novell Client being used to determine the user's location, the Middle Tier Server determines the location. This means that the application closest to the Middle Tier Server is used, which is not necessarily the application closest to the user. In the above example, the Site1 user would continue to have applications distributed from the Site1 server rather than from a Site2 server.

How to Build a Site List

You can link to only one other Application object. However, when you do so, the first Application object is automatically linked to any other Application objects that the second Application object is linked to. For example, you have three identical Application objects (App1, App2, and App3) at

three different sites. You link App1 to App2, which creates the following site lists for each of the Application objects:

App1 List	App2 List	App3 List
App2	App1	(none)

Because you can link an Application object to only one other Application object, you now need to link App3 to either App1 or App2. Doing so creates the following site list for each of the Application objects:

App1 List	App2 List	App3 List
App2	App1	App1
App3	App3	App2

Link

Click *Link*, browse for and select the Application object you want to link to, then click *OK* to add it to the *Application Site* list. Any other Application objects that the selected Application object is linked to are also added to the list.

Unlink

Click *Unlink* to remove the Application object's link to the Application objects displayed in the *Application Site* list.

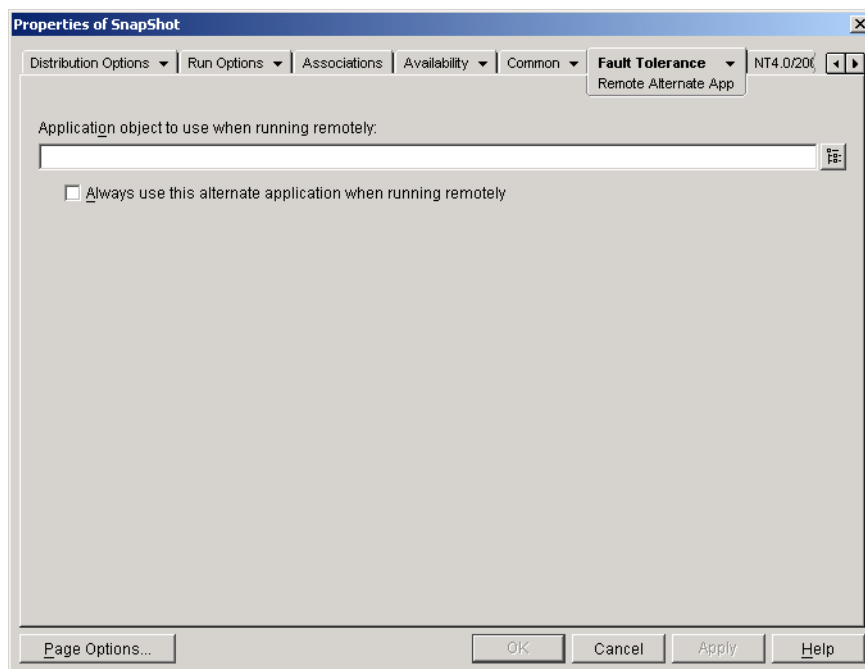
48.9.4 Remote Alternate App Page

The Remote Alternate App property page is available on Application objects created for all application types (simple, AOT/AXT, MSI, Web, and terminal server).

The Remote Alternate App property page, shown below, lets you specify an alternate application that Application Launcher launches if the user's workstation is running in remote mode rather than

local mode. Generally, this alternate application should be a terminal server application or Web application that is designed for use over slower remote connections.

Figure 48-60 *Application Object > Fault Tolerance Tab > Remote Alternate App Page*



Application Object to Use When Running Remotely

Select the Application object for the alternate application.

Always Use this Alternate Application When Running Remotely

By default, Application Launcher does not use the alternate application if the original application is installed on the user's workstation; instead, it uses the locally installed application. However, if the application requires access to a database or some other network resource that is only available if the alternate application is used, select this option to force Application Launcher to use the alternate application rather than the locally installed application.

Novell® Application Launcher™ supports the use of macros, or variables, with many of the properties available on the Application object pages in ConsoleOne®. You can use any of the six types of macros listed below.

- Application object macros
- Special Windows macros
- Login script macros
- Novell® eDirectory™ attribute macros
- Environment variable macros
- Language variable macros

Each macro type gives you various abilities. For example, Application object macros are basically variables to which you can assign values. By using an Application object macro, you have the flexibility to change the macro's value in one location and have it automatically changed anywhere you have used the macro. Special Windows macros, on the other hand, let you specify Windows locations, such as the Windows temporary directory, by specifying a variable name (for example, %*WINTEMP%) that exists on the workstation and defines the location on that workstation. This enables you to specify locations that might vary from workstation to workstation.

NOTE: Be aware that using macros causes increased network traffic because the ZENworks® macro lookup checks with eDirectory on the network before it checks the local environment.

The following sections provide information about the five types of macros supported by Application objects, the precedence order, and the Application object properties where macros can be used.

- [Section 49.1, “Application Object Macros,” on page 585](#)
- [Section 49.2, “Special Windows Macros,” on page 587](#)
- [Section 49.3, “Login Script Macros,” on page 590](#)
- [Section 49.4, “eDirectory Attribute Macros,” on page 592](#)
- [Section 49.5, “Environment Variable Macros,” on page 594](#)
- [Section 49.6, “Language Variable Macros,” on page 594](#)
- [Section 49.7, “Macro Precedence,” on page 597](#)
- [Section 49.8, “Application Object Properties Where Macros Can Be Used,” on page 597](#)
- [Section 49.9, “Refreshing Macro Information,” on page 599](#)

49.1 Application Object Macros

An Application object macro is defined on the Application object's Macros page and can only be used with that Application object. The macro is simply a variable that has a value associated with it, as shown in the following two examples:

Variable	Value
SOURCE_PATH	\\server1\sys\public\zen\word
TARGET_PATH	c:\program files\word

In the examples, SOURCE_PATH defines the network location from which Novell Application Launcher™ distributes the application to the user's workstation, and TARGET_PATH defines the workstation location to which Application Launcher copies the files.

You can also create a macro that prompts the user to accept a default value you've assigned or to enter a different value. For example, you could use a macro that prompts the user with a default installation drive (such as c:) but lets the user change it to another drive (such as d:).

The following sections provide information about nesting other macros in Application object macros and instructions to help you define Application object macros:

- [Section 49.1.1, “Nesting Macros,” on page 586](#)
- [Section 49.1.2, “Defining an Application Object Macro,” on page 586](#)

49.1.1 Nesting Macros

When defining an Application object macro, you can embed other macros in the definition. In the following example, a special Windows macro, *WINDISK, is used when defining the TARGET_PATH macro:

```
%*WINDISK%\Program Files
```

Any time you use the TARGET_PATH macro in an Application object property field, Application Launcher substitutes the current workstation's Windows drive letter for %*WINDISK% (for example, c:\temp).

When embedding another macro in the string, you must enclose the macro in % characters, as shown in the above example. You can embed special Windows macros, eDirectory attribute macros, environment variable macros, login script macros, and other Application object macros.

49.1.2 Defining an Application Object Macro

- 1 In ConsoleOne, right-click the Application object for which you want to define the macro, then click *Properties*.
- 2 Click the *Common* tab > *Macros* to display the Macros page.
- 3 To define a macro consisting of a variable name and a value (a String Value macro), continue with [“Defining a String Value \(Non-Prompted\) Macro” on page 586](#).
or
To define a macro that prompts the user to accept a default value or enter a different value, skip to [“Defining a Prompted Macro” on page 587](#).

Defining a String Value (Non-Prompted) Macro

- 1 On the Macros page, click *Add* > *String value* to display the Edit String Value dialog box.

- 2 In the Value Name box, type a name for the macro variable (for example, TARGET_PATH). Do not use spaces in the name.
- 3 In the Value Data box, type the value for the macro variable (for example, c:\program files\word).
- 4 Click *OK* to add the macro to the Macros list.

For information about using the macro in a valid Application object property, see [Section 49.8, “Application Object Properties Where Macros Can Be Used,” on page 597](#).

Defining a Prompted Macro

Prompted macros do not apply to MSI applications. With all applications other than MSI applications, Application Launcher controls the installation process and can therefore supply the prompt. With MSI applications, Windows Installer, not Application Launcher, installs the applications; Application Launcher has no opportunity to supply the prompt.

- 1 On the Macros page, click *Add > Prompted > Drive* to create a macro that prompts the user for a drive or click *Add > Prompted > String* to create a macro that prompts the user for text input.
- 2 Fill in the following fields:

Macro name Specify any name that describes the macro. Do not use spaces in the name.

Prompt text: Specify the text you want presented to the user. For example, if you are prompting for an installation drive you could enter the following: “This application will be installed to your C: drive. Enter a different drive letter if desired.”

Default value: For a prompted drive macro, select the drive to display as the default drive. For a prompted string macro, specify the text to display as the default text.

Minimum disk space in MB: Specify the minimum amount of free disk space required. The user cannot install to any drive that does not meet the minimum disk space requirement.

Maximum string length in chars (prompted string macro only): Specify the maximum number of characters the user can enter as a response to a prompted string macro.

- 3 Click *OK* to add the macro to the Macros list.

For information about using the macro in a valid Application object property, see [Section 49.8, “Application Object Properties Where Macros Can Be Used,” on page 597](#).

49.2 Special Windows Macros

A special Windows macro is one that defines Windows 98 and Windows 2000/XP directories. The typical paths listed below are based on default installations and might or might not match your specific setup. On Windows 98 workstations, macros behave differently if User Profiles are enabled.

Suppose that you have installed Windows to drive d: (for example, d:\winnt). However, an application installation expects Windows to be on drive c: (for example, c:\winnt). Using the *WinDisk macro, you can substitute drive d: with the macro for the files that require it.

The following two sections describe the special Windows macros you can use.

- [Section 49.2.1, “Windows 98 and Windows 2000/XP Macros,” on page 588](#)
- [Section 49.2.2, “Windows 2000/XP Macros,” on page 589](#)

For information about using the macros in a valid Application object property, see [Section 49.8, “Application Object Properties Where Macros Can Be Used,”](#) on page 597.

49.2.1 Windows 98 and Windows 2000/XP Macros

The following macros apply to Windows 98 and Windows 2000/XP unless otherwise noted.

IMPORTANT: The asterisk character (*) is a required syntax for these macros. Don’t confuse these asterisk characters with the Novell trademark asterisk. In addition, when using the macro in one of the Application object’s property fields, you must enclose it in % characters (for example, %*WinDisk%).

Table 49-1 Windows 98 and Windows 2000/XP Macros

Macro	Description
%*AppData%	File system directory that serves as a common repository for application specific data. Typically c:\winnt\profiles\user name\application data. Used only by Windows NT version 4.
%*CommonDesktop%	File system directory that contains files and folders that appear on the desktop for all users. Typically c:\winnt\profiles\all users\desktop. If not available, the *DESKTOP value is used.
%*CommonPrograms%	File system directory that contains the directories for the common program groups that appear on the Start menu for all users. Typically c:\winnt\profiles\all users\start menu\programs. If not available, the *PROGRAMS value is used.
%*CommonStartMenu%	File system directory that contains the programs and folders that appear on the Start menu for all users. Typically c:\winnt\profiles\all users\start menu. If not available, the *STARTMENU value is used.
%*CommonStartup%	File system directory that contains the programs that appear in the Startup folder for all users. The system starts these programs whenever any user logs on to Windows NT 4 or starts Windows 98. Typically this directory is c:\winnt\profiles\all users\start menu\programs\startup. If not available, the *STARTUP value is used.
%*CommonWinDesktop%	Windows NT 4 common desktop directory (c:\winnt\profiles\all users\desktop). This is an Application Launcher 2.0 macro that is allowed for backward compatibility.
%*Cookies%	Files system directory that contains the user’s cookies. Typically c:\windows\cookies or c:\winnt\profiles\username\cookies.
%*Desktop%	File system directory used to physically store file objects on the desktop (not to be confused with the desktop folder itself). Typically this directory is c:\windows\desktop or c:\winnt\profiles\username\desktop.
%*Favorites%	File system directory that serves as a common repository for the user’s favorite items. Typically this directory is c:\windows\favorites or c:\winnt\profiles\username\favorites.
%*Fonts%	Virtual folder containing fonts. Typically c:\windows\fonts or c:\winnt\fonts.

Macro	Description
%*History%	File system directory that contains the user's history of visited Internet addresses. Typically <code>c:\windows\history</code> or <code>c:\winnt\profiles\username\history</code> .
%*NetHood%	File system directory containing objects that appear in the network neighborhood. Typically <code>c:\windows\nethood</code> or <code>c:\winnt\profiles\username\nethood</code> .
%*Personal%	File system directory that serves as a common repository for documents. Typically <code>c:\myfiles</code> or <code>c:\winnt\profiles\username\personal</code> .
%*PrintHood%	File system directory that serves as a common repository for printer links. Typically <code>c:\winnt\profiles\username\printhood</code> . Only used by Windows NT 4.
%*Programs%	File system directory that contains the user's program groups (which are also file system directories). Typically <code>c:\windows\start menu\programs</code> or <code>c:\winnt\profiles\username\start menu\programs</code> .
%*Recent%	File system directory that contains the user's most recently used documents. Typically <code>c:\windows\recent</code> or <code>c:\winnt\profiles\username\recent</code> .
%*SendTo%	File system directory that contains Send To menu items. Typically <code>c:\windows\sendto</code> or <code>c:\winnt\profiles\username\sendto</code> .
%*StartMenu%	File system directory containing Start menu items. Typically <code>c:\windows\start menu</code> or <code>c:\winnt\profiles\username\start menu</code> .
%*Startup%	File system directory that corresponds to the user's Startup program group. Typically <code>c:\windows\start menu\programs\startup</code> or <code>c:\winnt\profiles\username\start menu\programs\startup</code> .
%*TempDir%	Windows temporary directory (<code>c:\windows\temp</code>).
%*Templates%	File system directory that serves as a common repository for document templates. Typically <code>c:\windows\shellnew</code> or <code>c:\winnt\shellnew</code> .
%*WinDesktop%	Windows desktop directory (<code>c:\windows\desktop</code> or <code>c:\winnt\profiles\username\desktop</code> for Windows NT 4). This is an Application Launcher 2.0 macro that is allowed for backward compatibility.
%*WinDir%	Windows directory. Typically <code>c:\windows</code> or <code>c:\winnt</code> .
%*WinDisk%	Drive letter (plus colon) for the Windows directory. Typically <code>c:.</code>
%*WinSysDir%	Windows system directory. Typically <code>c:\windows\system</code> or <code>c:\winnt\system32</code> .
%*WinSysDisk%	Drive letter (plus colon) for the Windows system directory. Typically <code>c:.</code>

49.2.2 Windows 2000/XP Macros

The following macros apply to Windows 2000/XP only.

IMPORTANT: The asterisk character (*) is a required syntax for these macros. Don't confuse these asterisk characters with the Novell trademark asterisk. In addition, when using the macro in

one of the Application object's property fields, you must enclose it in % characters (for example, %*WinDisk%).

Table 49-2 *Windows 2000/XP Macros*

Macro	Description
%*AdminTools%	File system directory that contains the administrative tools that appear in the Control Panel when a specific user logs in to Windows 2000/XP. Typically c:\documents and settings\username\start menu\programs\administrative tools.
%*CommonAdminTools%	File system directory that contains the administrative tools that appear in the Control Panel for all users who log in to Windows 2000/XP. Typically c:\documents and settings\all users\start menu\programs\administrative tools.
%*CommonAppData%	File system directory that contains the application-specific data for all users who log in to Windows 2000/XP. Typically c:\documents and settings\all users\application data.
%*CommonDocuments%	File system directory that contains the documents shared by all users who log in to Windows 2000/XP. Typically c:\documents and settings\all users\documents.
%*CommonTemplates%	File system directory that contains the document templates shared by all users who log in to Windows 2000/XP. Typically c:\documents and settings\all users\templates.
%*MyPictures%	File system directory that contains a specific user's graphics files. Typically c:\documents and settings\username\my documents\my pictures.
%*ProgramFiles%	File system directory that contains the program files. Typically c:\program files.
%*ProgramFilesCommon%	File system directory that contains the program files shared by multiple applications. Typically c:\program files\common.
%*UserProfile%	File system directory that contains the logged-in user's profile. Typically c:\documents and settings\username.

49.3 Login Script Macros

Novell Client login script commands allow you to use identifier variables to make login scripts more efficient and flexible. Application Launcher supports many, but not all, login script identifier variables for use in Application object macros.

- [Section 49.3.1, “Supported Login Script Identifier Variables,” on page 591](#)
- [Section 49.3.2, “Unsupported Login Script Identifier Variables,” on page 592](#)

For information about using the macros in a valid Application object property, see [Section 49.8, “Application Object Properties Where Macros Can Be Used,” on page 597](#).

49.3.1 Supported Login Script Identifier Variables

The following is a list of supported login script identifier variables and what they mean. Alternate variable names are shown in parentheses.

Table 49-3 *Supported Login Script Identifier Variables*

Macro	Description
%COMPUTER_NAME%	The name of the computer. For example: work_pc.
%DAY%	Numeric day of the month. For example: 01, 10, 15.
%FILESERVER% (%FILE_SERVER%)	Name of the NetWare file server or eDirectory monitored connection. For example: APPS_PROD.
%FULL_NAME%	Full name attribute of the User object. This is supported by virtue of Application Launcher's support for eDirectory attributes from the User object.
%HOUR24% (%24HOUR%)	Time of the day according to a 24-hour clock. For example: 02, 05, 14, 22.
%HOUR% (%HOURS%)	Hour of the day. For example: 0 = 12, 13 = 1.
%LAST_NAME%	Last name of the current user (also known as the user's eDirectory Surname attribute). For example: Jones.
%LOGIN_NAME%	First eight bytes of the user's eDirectory object name. For example: jsmith.
%MINUTE% (%MINUTES%)	Current minute. For example: 02, 59.
%MONTH%	Current month number. For example: 01 for January.
%NDAY_OF_WEEK%	Numeric day of the week. For example: 1 for Sunday, 2 for Monday.
%NETWORK% (%NETWORK_ADDRESS%)	Workstation network address. For example: 01010120.
%OS_VERSION%	Version of the OS. For example: v5.00 (Win3x shows the DOS version, Win 98 and Win 2000/XP shows the Windows version).
%OS	OS type. For example: MSDOS, WIN98, WINNT, WIN2000, WINXP. (Win3 shows MSDOS.)
%PLATFORM%	Platform running. For example: WIN, W98, WNT, W2000, WXP.
%PHYSICAL_STATION% (%P_STATION%)	MAC address. For example: 0000C04FD92ECA.
%REQUESTER_CONTEXT%	Context of the requester for the selected tree.
%SECOND% (%SECONDS%)	Number of seconds. For example: 03, 54.
%SHORT_YEAR%	Short year number. For example: 97, 00.
%WINVER%	Windows version. For example: v3.11, v4.00.
%WORKSTATION_ID%	The name of the workstation object.
%WORKSTATION_TREE%	The name of the tree in which the workstation is located.

Macro	Description
%WORKSTATION_DN%	The distinguished name and context of the workstation object.
%YEAR%	Full year number. For example: 2000, 2001.

49.3.2 Unsupported Login Script Identifier Variables

The following is a list of login script macros that Application Launcher does not support:

ACCESS_SERVER
 AM_PM
 DAY_OF_WEEK
 DIALUP
 ERROR_LEVEL
 GREETING_TIME
 LOGIN_ALIAS_CONTEXT
 LOGIN_CONTEXT
 MACHINE
 MEMBER OF
 NOT MEMBER OF
 MONTH_NAME
 NETWARE_REQUESTER
 OFFLINE
 PASSWORD_EXPIRES
 REQUESTER_VERSION
 SHELL_TYPE
 SHELL_VERSION
 SMACHINE
 STATION
 USER_ID

49.4 eDirectory Attribute Macros

Application Launcher supports macros that pull information from the attributes of the currently logged-in user, the current Application object, or from the attributes of other eDirectory objects.

The following sections explain the macro syntax and provide examples:

- [Section 49.4.1, “Syntax,” on page 592](#)
- [Section 49.4.2, “Examples,” on page 593](#)

For information about using the macros in a valid Application object property, see [Section 49.8, “Application Object Properties Where Macros Can Be Used,” on page 597](#).

49.4.1 Syntax

eDirectory attribute macros use the following syntax:

`%object_name.container;eDirectory_attribute%`

Table 49-4 Macro Syntax

Element	Description
<code>%</code>	Flags the text as a macro. The entire macro must be enclosed in% characters.
<code>.object_name.container;</code>	Indicates the eDirectory object from which to read the attribute. To use an attribute from the currently logged in user, leave this element out. For example, %CN% would return the common name of the currently logged in user. To use an attribute from the Application object, replace <i>.object_name.container</i> with an asterisk (*). For example, %*;DN% would return the distinguished name of the Application object.
<code>eDirectory_attribute</code>	Defines the attribute to be read. You can use the ConsoleOne Schema Manager (available from the Tools menu) to view an eDirectory object's available attributes.

49.4.2 Examples

The following table provides examples of eDirectory attribute macros.

Table 49-5 Macro Examples

Macro	Description
<code>%CN%</code>	Returns the common name of the currently logged-in user.
<code>%DN%</code>	Returns the distinguished name of the currently logged-in user.
<code>%Full Name%</code>	Returns the full name of the currently logged-in user. This is the name defined in User object > General tab > Identification page > Full Name field.
<code>%Given Name%</code>	Returns the first name of the currently logged-in user. This is the name defined in User object > General tab > Identification page > Given Name field.
<code>%Surname%</code>	Returns the last name of the currently logged-in user. This is the name defined in the User object > General tab > Identification page > Last Name field.
<code>%*;DN%</code>	Returns the distinguished name of the Application object (the one in which the macro is being used).
<code>%*;App:Caption%</code>	Returns the application icon title given the Application object. This is the title defined in the Application object > Identification tab > Icon page > Application Icon Title field.

Macro	Description
*;App:Path%	Returns the path to the application's executable as defined for the Application object. This is the path defined in the Application object > Run Options tab > Application page > Path to File field.
%*;App:GUID%	Returns the Application object's global unique identifier (GUID). This is the GUID defined in the Application object > Distribution Options tab > Options page > GUID field.
%.JSmith.Novell;Description%	Returns the description for the JSmith User object located in the Novell container. This is the description defined in the User object > General tab > Identification page > Description field.

49.5 Environment Variable Macros

Application Launcher supports all valid Windows 98 and Windows 2000/XP environment variables. The value of the variable must not exceed the length of the Application object name; otherwise, the variable fails.

Here are a few examples:

- NWLANGUAGE
- TEMP
- PATH

When using an environment variable, you must enclose it in % characters (%PATH%).

For information about using the macros in a valid Application object property, see [Section 49.8, “Application Object Properties Where Macros Can Be Used,” on page 597](#).

49.6 Language Variable Macros

To minimize the number of Application objects required to distribute the same application in different languages, you can use language variables to represent language-related information in MSI Application objects. Language variables are not supported for simple, AOT/AXT, terminal server, or Web applications.

For example, assume you want to distribute language-appropriate versions of the ZENworks Desktop Management Agent, which has a separate .msi file for each language. By default, the Desktop Management Agent's .msi files are installed to the Desktop Management server's `sys:\public\zenworks\zfdagent\language` directory, where *language* represents the various supported languages. In the Desktop Management Agent's Application object, you could include a language variable in the source path for the *language* directory. For example:

```
\\server\sys\public\zenworks\zfdagent\%LOCALE_SYS_NATIVE_LANG%\zfdagent.msi
```

During distribution, Application Launcher retrieves the requested language information from the workstation's system and substitutes it for the language variable.

As another example, assume you have an .msi file such as `app1.msi`. When installing a specific language, you must apply a language-specific transform (.mst) file. To accommodate this need,

you could create language directories for each of the .mst files and then use a variable for the language directory when specifying the transform path.

```
\\server\sys\public\zenworks\appl\%LOCALE_SYS_NATIVE_LANG%\appl.mst
```

Language variables can be used in the same MSI Application object properties that other macro variables (special Windows macros, environment variables, and so forth) can be used. For a list of these locations, see [Section 49.8, “Application Object Properties Where Macros Can Be Used,” on page 597](#)

The following table describes the available language variables.

Table 49-6 *Language Variable Macros*

Language Variable	Description
%LOCALE_SYS_DEFAULT_ANSI_CP%	Retrieves the American National Standards Institute (ANSI) code page associated with the system locale. If the locale does not use an ANSI code page, the value is 0. Example: 1252
%LOCALE_SYS_DEFAULT_OEM_CP%	Retrieves the original equipment manufacturer (OEM) code page associated with the system locale. If the locale does not use an OEM code page, the value is 1. Example: 437
%LOCALE_SYS_LANGID%	Retrieves the language identifier for the system locale. The language identifier is a standard international numeric abbreviation for the language in a country or geographical region. Example: 0409
%LOCALE_SYS_ABBR_LANG%	Specifies the abbreviated name of the system language. In most cases, it is created by taking the two-letter language abbreviation from the International Organization for Standardization (ISO) Standard 639 and adding a third letter, as appropriate, to indicate the sublanguage. Example: ENU
%LOCALE_SYS_ENG_LANG%	Specifies the full English name of the system language from ISO Standard 639. This is always restricted to characters that can be mapped into the ASCII 127-character subset. Example: English
%LOCALE_SYS_LANG%	Specifies the full localized name of the system language. This name is based on the localization of the product and might vary for each localized version. Example: English (United States)

Language Variable	Description
%LOCALE_SYS_ISO639_LANG%	<p>Specifies the abbreviated name of the system language based only on ISO Standard 639.</p> <p>Example: en</p>
%LOCALE_SYS_NATIVE_LANG%	<p>Specifies the native name of the system language.</p> <p>Example: English</p>
%LOCALE_USER_DEFAULT_ANSI_CP%	<p>Retrieves the American National Standards Institute (ANSI) code page associated with the user locale. If the locale does not use an ANSI code page, the value is 0.</p> <p>Example: 1252</p>
%LOCALE_USER_DEFAULT_OEM_CP%	<p>Retrieves the original equipment manufacturer (OEM) code page associated with the user locale. If the locale does not use an OEM code page, the value is 1.</p> <p>Example: 850</p>
%LOCALE_USER_LANGID%	<p>Retrieves the language identifier for the user locale. The language identifier is a standard international numeric abbreviation for the language in a country or geographical region.</p> <p>Example: 0c09</p>
%LOCALE_USER_ABBR_LANG%	<p>Specifies the abbreviated name of the user language. In most cases, it is created by taking the two-letter language abbreviation from the International Organization for Standardization (ISO) Standard 639 and adding a third letter, as appropriate, to indicate the sublanguage.</p> <p>Example: ENA</p>
%LOCALE_USER_ENG_LANG%	<p>Specifies the full English name of the user language from ISO Standard 639. This is always restricted to characters that can be mapped into the ASCII 127-character subset.</p> <p>Example: English</p>
%LOCALE_USER_LANG%	<p>Specifies the full localized name of the user language. This name is based on the localization of the product and might vary for each localized version.</p> <p>Example: English (Australia)</p>
%LOCALE_USER_ISO639_LANG%	<p>Specifies the abbreviated name of the user language based only on ISO Standard 639.</p> <p>Example: en</p>
%LOCALE_USER_NATIVE_LANG%	<p>Specifies the native name of the user language.</p> <p>Example: English</p>

49.7 Macro Precedence

To resolve conflicts with macro names, Application Launcher uses the following order of precedence:

- Application object macros
- Special Windows macros
- Login script macros
- eDirectory attribute macros
- Environment variable macros

The macro types are listed in order of precedence. For example, Application object macros take precedence over special Windows macros, special Windows macros take precedence over login script macros, and so forth.

49.8 Application Object Properties Where Macros Can Be Used

You can use macros when defining the Application object properties.

When entering a macro in a property field, you must enclose the macros in % characters (for example, %TARGET_PATH% or %*WINDISK%). This enables Application Launcher to recognize and treat the macro as a macro.

The following sections describe the fields on each page on which you can use macros:

- [Section 49.8.1, “Common Tab,” on page 597](#)
- [Section 49.8.2, “Distribution Options Tab,” on page 598](#)
- [Section 49.8.3, “MSI Tab,” on page 598](#)
- [Section 49.8.4, “Run Options Tab,” on page 599](#)

49.8.1 Common Tab

You can use macros in the following fields on the Common tab:

Table 49-7 *Using Macros on the Common Tab*

Field Name	Access to Field
<i>Drive to be mapped/path</i>	<i>Common tab > Drives/Ports page > Add</i>
<i>Port to be captured/printer or queue</i>	
<i>Run before uninstalling</i>	<i>Common tab > Uninstall Scripts page</i>
<i>Run after uninstalling</i>	
NOTE: To use macros in these two fields, you must be using a script engine rather than the Novell Client, as specified in the Script Engine Location field.	

Field Name	Access to Field
<i>Package source path</i>	<i>Common tab > Sources > Add</i>

49.8.2 Distribution Options Tab

You can use macros in the following fields on the Distribution Options tab:

Table 49-8 *Using Macros on the Distribution Options Tab*

Field Name	Access to Field
Key, Value name, and Value data stings	Distribution Options tab > Registry page
Section, Value name, and Value data strings	Distribution Options tab > INI Settings page
Source file	Distribution Options tab > Application Files page > Add > File or Directory
Target file	
Target directory	
Add text to the file	Distribution Options tab > Text Files page > Add > Change
Delete text from the file	
Find file and replace text in the file	
All Icon/Shortcut properties	Distribution Options tab > Icons/Shortcuts page
	NOTE: the Icons/Shortcuts page is not available for MSI applications.
Run before distribution	Distribution Options tab > Distribution Scripts page
Run after distribution	
NOTE: To use macros in these two fields, you must be using a script engine rather than the Novell Client, as specified in the Script Engine Location field.	

49.8.3 MSI Tab

You can use macros in the following fields on the MSI tab:

Table 49-9 *Using Macros on the MSI Tab*

Field Name	Access to Field
<i>Transform path</i>	<i>MSI tab > Transforms > Add</i>
<i>MSI Patch file</i>	<i>MSI tab > Patches > Add</i>

49.8.4 Run Options Tab

You can use macros in the following fields on the Run Options tab:

Table 49-10 *Using Macros on the Run Options Tab*

Field Name	Access to Field
<i>Path to file</i>	<i>Run Options tab > Application page</i>
<i>Parameter</i>	
<i>Working directory</i>	
<i>Run before launching</i>	<i>Run Options tab > Launch Scripts page</i>
<i>Run after termination</i>	

NOTE: To use macros in these two fields, you must be using a script engine rather than the Novell Client, as specified in the Script Engine Location field.

49.9 Refreshing Macro Information

When Application Launcher starts, it caches the macro information defined for each Application object associated with the logged in user or workstation. To refresh macro information, the user must restart Application Launcher.

The Novell Client also caches the macro information. If users are authenticated through the Novell Client, they must not only restart Application Launcher but must also log out of eDirectory and log in again.

For example, if you are using the %DN% (distinguished name) eDirectory attribute macro in a folder name and you move a User object from one eDirectory container to another, the change is not be reflected on the user's workstation until he or she restarts Application Launcher and, if authenticated through the Novell Client, uses the Novell Client to log out and log in again.

Reference: Novell Application Launcher Tools

50

Novell® ZENworks® Desktop Management provides several tools that can be helpful as you manage applications for your users. These tools, located on the Tools > ZENworks Utilities > Application Launcher Tools menu in ConsoleOne®, are explained in the following sections:

- [Section 50.1, “Export Application Object,” on page 601](#)
- [Section 50.2, “Show Inherited Applications,” on page 601](#)
- [Section 50.3, “Search and Replace,” on page 601](#)
- [Section 50.4, “Manage Distribution GUIDs,” on page 602](#)
- [Section 50.5, “AOT/AXT File Tools,” on page 603](#)
- [Section 50.6, “Create Virtual CD,” on page 604](#)

50.1 Export Application Object

This tool enables you to export an Application object's properties to a new .aot or .axt file. You can perform a default export, which exports all general properties, INI settings, registry settings, text file changes, shortcuts, environment variables, and application files, or you can perform a custom export, which enables you to choose which settings you want exported.

- 1 In ConsoleOne, select the Application object.
- 2 Click the *Tools* menu > *ZENworks Utilities* > *Application Launcher Tools* > *Export Application Object*.
- 3 Select the export option you want, click *Next*, then follow the prompts to complete the export.

50.2 Show Inherited Applications

This tool enables you to see the applications that have been associated with a user or workstation, including applications associated with groups or containers that the user or workstation belong to. The applications are listed by mode of delivery, such as *Force run*, *App Launcher*, *Desktop*, *Start menu*, and *System tray*.

- 1 In ConsoleOne, select a User object or Workstation object.
- 2 Click the *Tools* menu > *ZENworks Utilities* > *Application Launcher Tools* > *Show Inherited Applications*.

50.3 Search and Replace

This tool lets you search and replace text strings in an Application object's general settings, registry settings, INI settings, copy files settings, icon settings, and text file settings. As settings are found that match your search criteria, you are given the choice of whether or not to replace the text string.

- 1 In ConsoleOne, select the Application object.

- 2 Click the *Tools* menu > *ZENworks Utilities* > *Application Launcher Tools* > *Search and Replace*.
- 3 In the *Search for* box, type the text string you are searching for.
- 4 In the *Replace with* box, type the text string you want to use in place of the text string you are searching for.
- 5 Select the *Match case* box to require the search results to match the case (uppercase and lowercase) of the text string you entered in the *Search For* box.
- 6 If you want to limit the Application object settings that are searched, click *Options*, deselect any settings you don't want searched, then click *OK* to return to the *Search and Replace* dialog box.
- 7 To start the search, click *Find Next*.

The dialog box expands to display the search results. If a setting is found that matches the search criteria, the setting's text is displayed in the *Text found* box.
- 8 To replace the setting's text with the text listed in the *Replace with* box, click *Replace*.

or

To replace the text for all settings that match the criteria, click *Replace All*.

or

To skip replacing the setting's text, click *Find Next*.
- 9 Repeat **Step 8** until all settings have been searched.

50.4 Manage Distribution GUIDs

The GUID Manager lets you change an application's GUID (global unique identifier). You can randomly generate a new GUID, manually specify a new GUID, or change the GUID to match another application's GUID. You might want to change an application's GUID for the following reasons:

- The Application object is accidentally deleted from Novell eDirectory™. When you re-create the Application object, it is randomly assigned a new, unique GUID. Because the new GUID causes the application to be redistributed to all users and workstations associated with the application, you use the GUID Manager to change the new GUID to the old GUID.
- You have multiple Application objects for the same application to enable fault tolerance, site lists, and so forth. You want to make sure that all Application objects have the same GUID so that the application is distributed only one time regardless of the Application object that is used. You use the GUID Manager to synchronize the GUIDs.

Changing the GUID of an undistributed application has no redistribution consequences. However, before you change the GUID of a distributed application, be aware that doing so might result in Application Launcher redistributing the application. In particular, redistribution occurs in the following situations:

- You give the application a new, unique GUID (one that is different from all other applications' GUIDs). A new, unique GUID always results in redistribution.
- You give the application the same GUID as another application that is not distributed on the workstation. For example, App1 has GUID 1234 and App2 has GUID 5678. You synchronize

App1 with App2 so that both applications now have 5678 as their GUIDs. Any workstations that had App1 but not App2 now has App1 redistributed to it.

To use the GUID Manager:

- 1 In ConsoleOne, select the Application object whose GUID you want to modify.
- 2 Click the *Tools* menu > *ZENworks Utilities* > *Application Launcher Tools* > *Manage Distribution GUIDs*.

Alternately, you can access the GUID Manager by opening the Application object, clicking *Distribution Options* > *Options* to display the Options page and then clicking the *Modify* button next to the *GUID* field.
- 3 In the *Applications to receive new GUID* list, add the applications that will be assigned the new GUID.

The list already contains the application you selected before opening the GUID Manager.
- 4 In the *GUID source* box, select the method you want to use to assign the new GUID:

Randomly generate new GUID: Use this option to have the GUID Manager randomly generate a new GUID. If you've added multiple applications to the Applications to Receive New GUID list, choose from the following two options:
 - **All selected apps share same GUID:** Assigns the same randomly-generated GUID to all of the applications.
 - **All selected apps get new GUID:** Assigns different randomly-generated GUIDs to each application.
Select GUID from existing application: Use this option to synchronize the GUIDs of all listed applications with an existing application. Click the *Browse* button to browse for and select the Application object whose GUID you want to share. The source application's GUID (the one you select using this option) does not change. Only the GUIDs for the applications displayed in the Application to *Receive new GUID* list change.

Manually specify new GUID: Use this option to define a specific GUID for all listed applications. Click *Modify* to display the Edit GUID dialog box used to define the GUID.
- 5 After you've defined the target applications and the GUID source, click *Change GUIDs*.

50.5 AOT/AXT File Tools

This tool converts an .aot file to an .axt file or an .axt file to an .aot file.

- 1 In ConsoleOne, click the *Tools* menu > *ZENworks Utilities* > *Application Launcher Tools* > *AOT/AXT File Tools*.
- 2 To convert an .aot file to an .axt file, click *AOT -> AXT*.

or

To convert an .axt file to an .aot file, click *AXT -> AOT*.
- 3 In the Open dialog box, browse for and select the file you want to convert, then click *Open*.
- 4 In the Save As dialog box, type a name for the new file, then click *Save As*. The correct extension (.aot or .axt) is added automatically.

50.6 Create Virtual CD

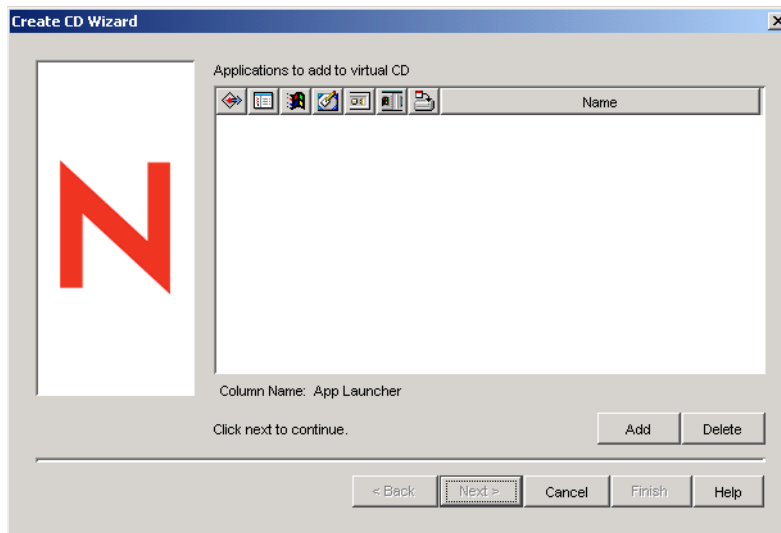
This tool lets you create a cache of applications that can be added to removable media (CD, Jaz drive, Zip drive, and so forth). The removable media functions as a second workstation cache, containing the Application object settings and application source files required to install and run the application. Any user whose workstation has Application Launcher installed can use the media to install and run the applications.

For example, you have a mobile user who seldom connects to the network but needs an application that you've distributed to other users. You burn a CD with the application and send it to the user. The user inserts the CD into his or her workstation's drive, Application Launcher reads the CD and displays the Application object's icon in the places you've configured (Application Launcher window, Start menu, desktop, and so forth). The user then launches the application, which is distributed to the workstation according to the Application object's configuration.

If the application includes any dependent applications (see [Chapter 37, “Advanced Distribution: Configuring Application Dependencies and Chains,”](#) on page 389), the dependent applications must be included on the removable media unless they have already been distributed to the user's workstation.

To create a cache on removable media:


- 1 In ConsoleOne, click the *Tools* menu > *ZENworks Utilities* > *Application Launcher Tools* > *Create Virtual CD* to start the Create CD Wizard and display the following page.




- 2 Click *Add*, then browse for and select the Application object for the application you want to distribute. Repeat this step to add additional applications.


If you add an MSI application, make sure the MSI source directory includes only MSI package files and subdirectories. The Create CD Wizard includes all files and subdirectories located in the source directory, causing Application Launcher to install all of the files and subdirectories regardless of whether or not they are part of the MSI package. The source directory is specified by the `SOURCE_PATH` variable on the Application object's Macros page (Common tab).


- 3 For each application you added to the list, select the locations where you want the Application object's icon to appear and select whether or not you want to force run and force cache the application. These settings are described below:


Force run:  Automatically runs the application. With a user-associated application, the application is run immediately after Novell Application Launcher™ starts or refreshes. With a workstation-associated application, the application is run immediately after the workstation starts up (initial startup or reboot) or after NAL Workstation Helper refreshes.


You can use the *Force run* option in conjunction with several other settings to achieve unique behaviors. For example, if you use the *Force run* option with the *Run application once* option (*Application* object > *Run Options* tab > *Applications* page), as soon as the Application object is distributed it runs one time and then is removed from the workstation. Or, suppose that you want to run the Application object immediately one time at a predetermined time. If so, select *Force run*, select the *Run application once* option on the Application page (*Application* object > *Run Options* tab), and define a schedule using the Schedule page (*Application* object > *Availability* tab).


App Launcher:  Adds the Application object's icon to the Application Window, the Application Explorer window, and the Application Browser window.

Start menu:  Causes Application Explorer, if running, to add the Application object to the Windows Start menu.

Desktop:  Causes Application Explorer, if running, to display the Application object's icon on the Windows desktop.

System Tray:  Causes Application Explorer, if running, to display the Application object's icon in the Windows system tray.

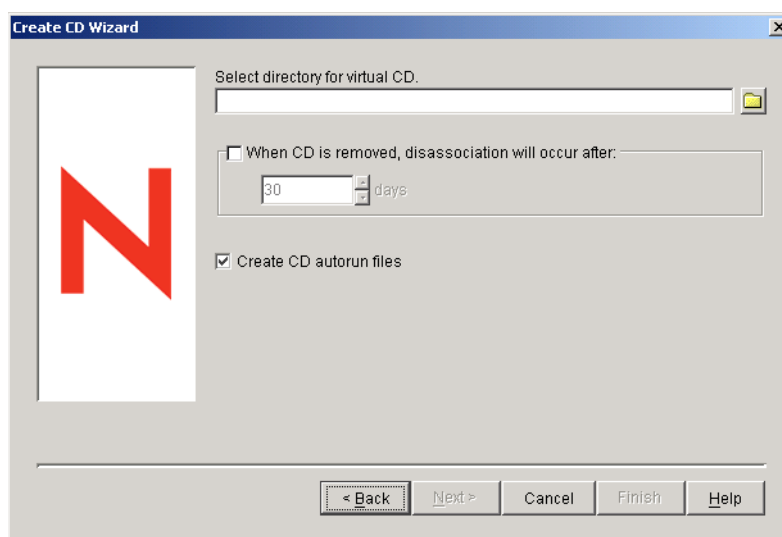
Quick Launch:  Causes Application Explorer, if running, to display the Application object's icon on the Windows Quick Launch bar.

Force cache:  Applies only if the Application object is marked as disconnectable (*Application* object > *Identification* tab > *Icon* page). With *Force cache* enabled, the first time the application is launched, Application Launcher copies the application source files and other files required for installation to the workstation's cache directory. The user can then install or verify the application while disconnected from eDirectory. The files are compressed to save space on the workstation's local drive.

The *Force cache* behavior for a removable media application (described in the previous paragraph) is different than the behavior for a network (eDirectory) application. With a network application, Application Launcher caches the application as soon as it becomes aware of the application, even if the application has not been launched yet. With a removable media application, Application Launcher does not cache the application until the application is launched the first time. This ensures that the user is not required to wait through the caching of multiple applications when Application Launcher initially reads the removable media.

NOTE: Do not use an asterisk character (*) in the name of the container that contains applications to be distributed using a virtual CD. Because Windows does not support the asterisk character in filenames, Windows changes the asterisk to an underscore character (_) and the force cache returns an error (D018).

- 4 After you've finished adding applications, click *Next* to display the following page.



- 5 Fill in the following fields:

Select directory for virtual CD: Select the location where you want to create the cache for the applications. Make sure the location you select has sufficient disk space for the cache. If enough disk space does not exist, you'll receive a message stating that an error has occurred.

You can also specify the path to the directory. If you specify a path to a network directory, you must use a mapped drive and not a UNC path. UNC paths are not supported.

When CD is removed disassociation will occur after: If you want to restrict the amount of time the user can continue to use an application after the CD or other media have been removed from the workstation, select this option, then select the number of days after which the disassociation occurs.

The time is measured from when the CD (or removable media) is removed from the user's workstation. The default time is 30 days. The valid range is 0 to 65535 days. Entering 0 instructs Application Launcher to disassociate the application the first time an Application Launcher refresh occurs after the CD (or removable media) is removed.

When the disassociation occurs, Application Launcher removes the application icon and the application files from the workstation.

Create CD autorun files: Select this option to create an `autorun.inf` file. The `autorun.inf` file initiates an Application Launcher refresh so that the Application objects included on the virtual CD are immediately displayed. If the user's workstation is not configured to autorun CDs, or you use another media type, the user must manually refresh Application Launcher. This is done by right-clicking the Application Launcher icon and clicking *Refresh*.

In ZENworks 7, the method that the `autorun.exe` file uses to trigger an Application Launcher refresh changed from previous ZENworks versions. As a result, ZENworks 7 Application Launcher does not automatically refresh for virtual CDs created with previous ZENworks versions. Likewise, pre-ZENworks 7 versions of Application Launcher do not automatically refresh for ZENworks 7 virtual CDs. Although automatic refresh does not work, users can insert the CD and then manually refresh Application Launcher to have it read the CD.

- 6 Click *Next*, review the settings, then click *Finish* to create the cache.

7 If necessary, copy the cache to the removable media (for example, burn the CD).

NOTE: Some CD-burning software does not allow for leading periods in filenames. When you create a virtual CD, ZENworks creates the virtual CD using a leading period in the application directory file pathname. If your CD-burning software does not allow for leading periods in filenames, and converts the period to another character such as an underscore, the virtual CD is not usable.

Currently, ZENworks does not support virtual CDs that are burned using the K3B CD-burning software.

Reference: Application Object Location

51

Each application you distribute is represented by an Application object that you create in Novell® eDirectory™. The Application object lets you configure distribution settings as well as other settings that determine how Novell Application Launcher™ manages the application.

Before you create an Application object, you need to decide where to locate the object in the eDirectory tree. The primary principle to follow is that an Application object should be placed in a container at the same site as the application's users. The following two sections provide examples:

- [Section 51.1, “Single Site,” on page 609](#)
- [Section 51.2, “Multiple Sites,” on page 610](#)

51.1 Single Site

If your eDirectory tree encompasses only one site, you can place Application objects in any container. For example, if you have a small site consisting of one or two organizations, you might want to create a common APPS container.

Figure 51-1 Common APPS Container Under an Organizational Unit



If your site is divided into many organizations, you might want to create a general APPS container for your corporate-wide Application objects and then create APPS containers within each organization container for the organization-specific applications.

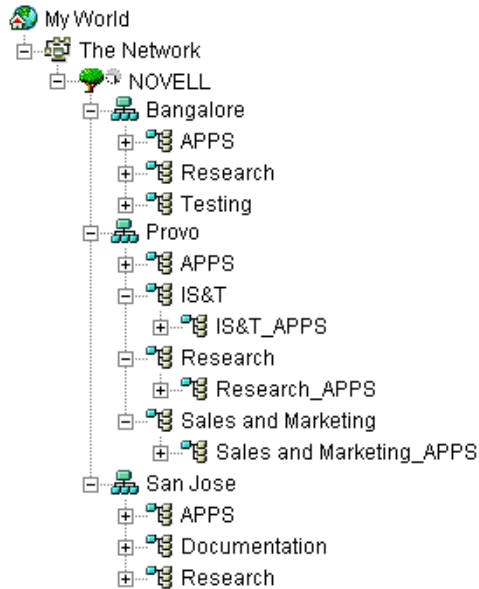
Figure 51-2 Common APPS Container and Organization-Specific APPS Containers



51.2 Multiple Sites

If your eDirectory tree encompasses several sites, we recommend that you place your Application objects in the tree at the same site as the users who access them, and ensure that the eDirectory partition for that site is replicated to one or more servers at that site. Typically, this means that you have APPS containers at multiple sites, as shown below.

Figure 51-3 APPS Containers at Three Different Sites



In the above example, the eDirectory tree has been established geographically, with each Organization container comprising a different site. Ideally, this is the most efficient way to organize your tree. If you have not organized your tree by geographical location, you can still place Application objects in the same location as the users who access them, but you need to discover these locations.

Undoubtedly, you have an application that you need to distribute to users at all your sites. In this case, you should create multiple Application objects (at least one at each site) for the application.

When giving users access to the application, you would associate the users with the Application object located at their site. Ensuring that users are accessing applications at their own site speeds user access to the applications and reduces cross-site network traffic.

If you have users who travel from site to site, you can set up site lists for any applications you want them to have access to at all sites. An application site list ensures that the user is accessing the application from the site where he or she is located, regardless of which Application object the user has been associated with. For more information about site lists, see [Chapter 48, “Reference: Application Object Settings,”](#) on page 471.

Reference: Novell Application Launcher Authentication Hook

52

Novell® Application Launcher™ includes an authentication developer hook. You can write your own dynamic link library (DLL) that takes advantage of the Novell Application Launcher hook. In order to implement a Novell Application Launcher authentication hook, you should understand ZENworks® Desktop Management, Novell Application Launcher, and DLL development.

The DLL (typically created in C) must contain the function **NWAPPAAuthenticateExtern**. The DLL enables you to hook into the `zenlite.dll` library to authenticate application launches based on the criteria you choose. Novell Licensing Services, ZENworks OnDemand Services™, and other applications use this service to prompt user's input before launching an application.

As a practical example, once authenticated to a network, a user can retain a persistent connection, yet the DLL can be configured to prompt for any specified method (for example, a fingerprint scanner or other biometric device) to quickly reauthenticate if the user temporarily steps away from the workstation. Other examples of how the application hook can be used include the following:

- **Licensing:** You can regulate the number of users of an application. The authentication hook can track the application users in a database or text file and prevent the application from launching when the number of users reaches a predefined limit.
- **Specialized credentials:** You can prompt certain users who access an application for special credentials, such as biometric information.
- **Application grouping:** You can group applications, for example, that require purchase or billing information.

Refer to the following sections for development and implementation guidelines:

- **Section 52.1, “Creating an Authentication Hook,” on page 611**
- **Section 52.2, “Registering an Authentication Hook,” on page 612**
- **Section 52.3, “Authentication Function (NWAPPAAuthenticateExtern),” on page 612**

52.1 Creating an Authentication Hook

Write a standard DLL that exports a function called **NWAPPAAuthenticateExtern**.

The implementation is left up to you. If the function returns `FALSE`, the application does not launch (distribute or run), and the `NWAPPAAuthenticateExtern` function must display the reason to the user.

None of the DLL parameters passed in should be larger than 512 bytes (as designated by `MAX_DN_BYTES`).

For sample code and a compellable Microsoft Developer Studio Project file you can use to help create the DLL, download [nalauthhook.zip](http://www.novell.com/documentation/lg/zdpr/zdpradmn/data/nalauthhook.zip) (<http://www.novell.com/documentation/lg/zdpr/zdpradmn/data/nalauthhook.zip>).

52.2 Registering an Authentication Hook

- 1 Create a string value called Authentication DLL in the *HKCU\Software\NetWare\NAL\1.0* key of the Windows registry.
- 2 Enter the full path to the authentication hook DLL as the value of the Authentication DLL entry created in Step 1.

If the DLL library cannot be found, you receive the following error message:

```
Could not locate Third Party Authentication DLL\n%s
```

If the DLL is found inside the library but the NWAPPAuthenticateExtern function cannot be found (such as when the function is not exported), you receive the message:

```
Could not locate Entry Point in Third Party Authentication DLL\n%s
```

NOTE: %s refers to a variable that is passed in by the user and prints out on the screen.

52.3 Authentication Function (NWAPPAuthenticateExtern)

The NWAPPAuthenticateExtern function provides an external authentication hook into the `zenlite.dll` library.

52.3.1 Syntax

```
#include <afxwin.h>

bool __stdcall NWAPPAuthenticateExtern
{
    char          *szTreeName,
    char          *DSName,
    char          szWho
}
```

52.3.2 Parameters

szTreeName

(IN) Points to the name of the directory tree where the DLL is located on the client.

DSName

(IN) Points to the name of the application object provided to the user. For example, this application can request name and/or password or some other authentication method like a thumbprint for a biometric scanner.

szWho

(IN) Specifies the fully qualified user name.

52.3.3 Return Values

TRUE	Launch the application.
FALSE	Do not launch the application.

52.3.4 Remarks

The implementation of this function is left up to you. Values passed to NWAPPAuthenticateExtern that exceed MAX_DN_BYTES bytes (MAX_DN_BYTES = 512) overflow the buffer and return an access violation.

IMPORTANT: Make certain you export the function.

Documentation Updates

J

This section contains information on documentation content changes that have been made in the *Administration* guide since the initial release of Novell® ZENworks® 7 Desktop Management (August 26, 2005). The information will help you to keep current on updates to the documentation.

All changes that are noted in this section were also made in the documentation. The documentation is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the documentation changes listed in this section.

The documentation update information is grouped according to the date the changes were published. Within a dated section, the changes are alphabetically listed by the names of the main table of contents sections for ZENworks 7 Desktop Management.

If you need to know whether a copy of the PDF documentation you are using is the most recent, the PDF document contains the date it was published on the front title page.

The documentation was updated on the following dates:

- [Section J.1, “July 14, 2006 \(Support Pack 1\),” on page 615](#)
- [Section J.2, “February 28, 2006,” on page 618](#)
- [Section J.3, “January 31, 2006,” on page 619](#)
- [Section J.4, “December 9, 2005,” on page 621](#)
- [Section J.5, “October 24, 2005,” on page 621](#)
- [Section J.6, “September 30, 2005,” on page 621](#)

J.1 July 14, 2006 (Support Pack 1)

Updates were made to the following sections. The changes are explained below.

- [Section J.1.1, “Advanced Distribution: Transferring Applications Using BITS,” on page 615](#)
- [Section J.1.2, “Metering Software Licenses,” on page 616](#)
- [Section J.1.3, “Novell Application Launcher: Configuring Settings,” on page 616](#)
- [Section J.1.4, “Novell Application Launcher: Customizing Views,” on page 616](#)
- [Section J.1.5, “Novell Application Launcher: Installing and Starting,” on page 616](#)
- [Section J.1.6, “Novell Application Launcher: Managing the Cache,” on page 617](#)
- [Section J.1.7, “Reference: AdminStudio ZENworks Edition,” on page 617](#)
- [Section J.1.8, “Reference: Application Object Settings,” on page 617](#)
- [Section J.1.9, “Reference: ZENworks sNappShot,” on page 617](#)
- [Section J.1.10, “Reporting Application Events,” on page 618](#)

J.1.1 Advanced Distribution: Transferring Applications Using BITS

The following section was added to cover new functionality:

Location	Change
Chapter 34, "Advanced Distribution: Transferring Applications Using BITS," on page 355	New section added.

J.1.2 Metering Software Licenses

The following updates were made in this section:

Location	Change
Section 45.1, "Installing Novell Licensing Services," on page 459	Updated the links to information about installing Novell Licensing Services on NetWare 6.x servers and OES NetWare servers.
Section 45.2, "Creating Metered Certificates," on page 459	Added information about how to create the metered certificates required for software license metering.

J.1.3 Novell Application Launcher: Configuring Settings

The following updates were made in this section:

Location	Change
Section 21.3, "Configuring User Settings," on page 258	Provided best practice information for using the Unassociated Days to Uninstall Application Launcher configuration setting.
Section 21.7, "Configuring Workstation Settings," on page 267	Provided best practice information for using the Unassociated Days to Uninstall Application Launcher configuration setting.

J.1.4 Novell Application Launcher: Customizing Views

The following updates were made in this section:

Location	Change
Section 22.2, "Customizing the Application Browser View," on page 272	Added information about a new configuration file, axnalview.js, that you must modify in addition to the myapps.html file in order to customize the Application Browser view. Information was added specifically to Section 22.2.1, "File Location," on page 273 and Section 22.2.2, "Modifying the Myapps.html and Axnalview.js Files," on page 274 .

J.1.5 Novell Application Launcher: Installing and Starting

The following updates were made in this section:

Location	Change
Section 20.5, "Application Window Command Line Switches," on page 244	Added the /restrictonline=3 option and updated the descriptions to reflect the modified functionality.
Section 20.6, "Application Explorer Command Line Switches," on page 251	Added the /restrictonline=3 option and updated the descriptions to reflect the modified functionality.

J.1.6 Novell Application Launcher: Managing the Cache

The following updates were made in this section:

Location	Change
Section 24.1.2, "Install Cache," on page 296	Added information about how Application Launcher, when running in remote mode, creates an application's install cache on the local workstation prior to launching the application.

J.1.7 Reference: AdminStudio ZENworks Edition

The following updates were made in this section:

Location	Change
Chapter 46, "Reference: AdminStudio ZENworks Edition," on page 463	Updated version information to AdminStudio 7.5 ZENworks Edition.
Section 46.2, "Using AdminStudio ZENworks Edition," on page 464	Updated the AdminStudio screenshot to reflect the new version. Also revised information about where to get AdminStudio help.

J.1.8 Reference: Application Object Settings

The following section was added to cover new functionality:

Location	Change
Section 48.2.10, "BITS Settings Page," on page 507	New section added.

J.1.9 Reference: ZENworks sNappShot

The following updates were made in this section:

Location	Change
Chapter 47, "Reference: ZENworks SnAppShot," on page 465	Added recommendation to use Windows Installer packages rather than snAppShot packages whenever possible. Included a link to an article explaining the reason for this recommendation.
Section 47.3, "Creating an Installation Package," on page 467	Under Step 1 on page 467 , added information about the location of <code>snapshot.exe</code> on Windows and Linux servers. Also updated the snAppShot screenshot.

J.1.10 Reporting Application Events

The following section was added to cover new functionality:

Location	Change
Section 44.2, "Setting Up SNMP Trap Reporting," on page 438	Added Section 44.2.1, "Enabling Firewall Access," on page 438 to provide information about how to ensure communication between user workstations and the management console when using SNMP traps as the reporting method.
Section 44.4.6, "Enabling the XML Targets Policy," on page 445	Under Step 4 on page 447 , corrected the Reporting Servlet's port number in the URL for a Linux server (OES Linux and SLES). The correct port number (8180) is now listed.

J.2 February 28, 2006

Updates were made to the following section. The changes are explained below.

- **Section J.2.1, "Advanced Distribution: Pre-Installing Applications," on page 618**
- **Section J.2.2, "Reference: Application Object Settings," on page 618**
- **Section J.2.3, "Reporting Application Events," on page 619**
- **Section J.2.4, "Setting Up Database Reporting," on page 619**

J.2.1 Advanced Distribution: Pre-Installing Applications

The following updates were made in this section:

Location	Change
Section 35.3, "Scheduling an Application Pre-Install," on page 370	Modified Step 4b on page 372 by adding additional, clarifying information about the <i>Time for selected dates</i> and the <i>Spread from start time</i> fields. Modified Step 5b on page 374 by adding additional, clarifying information about the <i>Spread from start time</i> field.

J.2.2 Reference: Application Object Settings

The following updates were made in this section:

Location	Change
Section 48.5, "Availability Tab," on page 527	Modified the <i>Time for selected dates</i> and the <i>Spread from start time</i> fields in "Specified Days" on page 544 to further clarify their function. Modified the <i>Spread from start time</i> field in "Range of Days" on page 545 to further clarify its function.
Section 48.2, "Distribution Options Tab," on page 479	Modified the <i>Time for selected dates</i> and the <i>Spread from start time</i> fields in "Specified Days" on page 500 to further clarify their function. Modified the <i>Spread from start time</i> field in "Range of Days" on page 501 to further clarify its function.

J.2.3 Reporting Application Events

The following updates were made in this section:

Location	Change
Chapter 44, "Reporting Application Events," on page 431	Revised the first sentence in the second paragraph to read: "Application Launcher can write events to the Sybase ODBC-compatible database...." Testing has shown that only Sybase is fully supported for ZENworks Application Management ODBC reporting.

J.2.4 Setting Up Database Reporting

The following updates were made in this section:

Location	Change
Section 44.1.1, "Installing the Sybase Database," on page 432	Deleted a section entitled "Using an ODBC-Compliant Database" because it implied that ODBC databases other than Sybase are supported in ZENworks Application Management. Testing has shown that only Sybase is fully supported for ZENworks Application Management ODBC reporting.
Section 44.1.1, "Installing the Sybase Database," on page 432	Modified the first sentence in the section to read: "The Sybase database included on the Novell ZENworks 7 Desktop Management CD is the only supported database for direct ODBC reporting in ZENworks Application Management." Testing has shown that only Sybase is fully supported for ZENworks Application Management ODBC reporting.

J.3 January 31, 2006

Updates were made to the following section. The changes are explained below.

- Section J.3.1, "Configuring Applications to Use Reporting," on page 620
- Section J.3.2, "Establishing File System Access," on page 620
- Section J.3.3, "INI Settings," on page 620
- Section J.3.4, "Installing Novell Licensing Services," on page 620

- [Section J.3.5, “Reference: Macros,” on page 620](#)
- [Section J.3.6, “Registry Settings,” on page 621](#)

J.3.1 Configuring Applications to Use Reporting

The following updates were made in this section:

Change	Location
Section 44.5, “Configuring Applications to Use Reporting,” on page 448.	Added reference to Linux servers in the note at the end of Step 3 .

J.3.2 Establishing File System Access

The following updates were made in this section:

Change	Location
Section 28.3, “Establishing File System Access,” on page 319.	Added reference to Linux servers, where file system rights also need to be assigned.

J.3.3 INI Settings

The following updates were made in this section:

Change	Location
Section 48.2.4, “INI Settings Page,” on page 489.	Added information in the note to clarify that INI values will not roll back in the case of a failure during installation.

J.3.4 Installing Novell Licensing Services

The following updates were made in this section:

Change	Location
Section 45.1, “Installing Novell Licensing Services,” on page 459.	Clarified text to indicate that license metering cannot be used either in an all-Windows or in an all-Linux environment.

J.3.5 Reference: Macros

The following updates were made in this section:

Change	Location
Chapter 49, “Reference: Macros,” on page 585.	Added a note in the chapter introduction to indicate that using macros causes increased network traffic because the ZENworks macro lookup checks with eDirectory on the network before it checks the local environment.

J.3.6 Registry Settings

The following updates were made in this section:

Change	Location
Section 48.2.2, "Registry Page," on page 482.	Added information in the note to clarify that registry values will not roll back in the case of a failure during installation.

J.4 December 9, 2005

Page design was reformatted to comply with revised Novell documentation standards.

J.5 October 24, 2005

Updates were made to the following section. The changes are explained below.

- Section J.5.1, "Reporting Application Events," on page 621

J.5.1 Reporting Application Events

The following updates were made in this section:

Location	Change
"Enabling the XML Targets Policy" on page 445.	Revised Step 4 to show the correct Reporting servlet URLs for Windows/NetWare and Linux.

J.6 September 30, 2005

Updates were made to the following section. The changes are explained below.

- Section J.6.1, "Novell Application Launcher: Installing and Starting," on page 621

J.6.1 Novell Application Launcher: Installing and Starting

The following updates were made in this section:

Change	Location
Section 20.5, "Application Window Command Line Switches," on page 244.	Deleted the /restrictonline=3 switch. This has been disabled in the code due to modified product functionality.
Section 20.6, "Application Explorer Command Line Switches," on page 251.	Deleted the /restrictonline=3 switch. This has been disabled in the code due to modified product functionality.

Workstation and Server Imaging

VI

Novell® ZENworks® 7 Desktop Management supports imaging Windows workstations using a Linux, NetWare®, or Windows imaging server. The addition of a Linux imaging server is new in ZENworks 7.

Beginning with ZENworks 7 Desktop Management, imaging support is also provided on a limited basis for the following:

- **Linux and Windows servers:** Imaging Linux and Windows servers is possible with the following exceptions:
 - Software RAID configurations are not supported, but hardware RAID is supported.
 - Volume managers, such as LVM and EVMS, are not supported.
 - A Windows server image intended for deployment to multiple servers must be prepared using the Microsoft sysprep tool so that Windows can properly manage SIDs.However, an image of a Windows server that is intended as disaster recovery for a specific server does not require sysprep.

When imaging servers, you must image them manually one at a time.

- **Linux workstations:** Novell eDirectory™ objects are not created for Linux workstations in Desktop Management. Therefore, you can only manage and image Linux workstations in ConsoleOne® as unimported objects. For workstation object-based automatic imaging of Linux workstations, use **ZENworks Linux Management**.

Imaging of NetWare servers is not supported. Although you can make and deploy NetWare server images using Desktop Management in certain simple server configurations, Novell does not support these practices. For more information, see TID 10092081 in the [Novell Support Knowledgebase](http://support.novell.com/search/kb_index.jsp) (http://support.novell.com/search/kb_index.jsp).

The following sections provide information on the Desktop Management Imaging procedures and features:

- Chapter 53, “Common Imaging Deployment Strategies,” on page 625
- Chapter 54, “Preparing a ZENworks Imaging Server,” on page 629
- Chapter 55, “Preparing an Imaging Boot Method,” on page 631
- Chapter 56, “Using ZENworks Desktop Management Preboot Services,” on page 637
- Chapter 57, “Setting Up Workstations for Imaging,” on page 693
- Chapter 58, “Setting Up Imaging Policies,” on page 697
- Chapter 59, “Creating and Restoring Images,” on page 703
- Chapter 60, “Performing Manual Imaging Operations,” on page 711
- Chapter 61, “Setting Up Disconnected Imaging Operations,” on page 719
- Chapter 62, “Multicasting Images,” on page 725
- Chapter 63, “Imaging Utilities and Components,” on page 737
- Chapter 64, “ZENworks Imaging Engine Commands,” on page 773
- Chapter 65, “Updating ZENworks Imaging Resource Files,” on page 789

- [Chapter 66, “Supported Ethernet Cards,” on page 803](#)
- [Chapter 67, “Accessing IP Addresses for Devices Running Dual NICs,” on page 805](#)
- [Appendix K, “Documentation Updates,” on page 807](#)

Common Imaging Deployment Strategies

53

The following overview sections present possible approaches to deploying the Imaging component of Novell® ZENworks® 7 Desktop Management for some common enterprise scenarios. Use the following sections to determine which procedures to perform and in what order:

- [Section 53.1, “Installing a Standard Image Before Deploying New Workstations,” on page 625](#)
- [Section 53.2, “Enabling Existing Workstations for Future Reimaging,” on page 626](#)
- [Section 53.3, “Reimaging Corrupted Workstations,” on page 627](#)
- [Section 53.4, “Restoring Lab or Classroom Workstations to a Clean State,” on page 627](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

53.1 Installing a Standard Image Before Deploying New Workstations

As new workstations are purchased and before deploying them, you can install a standard software platform and enable the workstation for future unattended reimaging.

1. Create a model workstation of each type that you’ll deploy.
2. Create an image of each model workstation on a ZENworks Imaging server. For more information, see [Section 60.1, “Manually Taking an Image of a Workstation,” on page 711](#).

These images should include the Desktop Management Agent, which includes the ZENworks Imaging Windows Agent. ZENworks Desktop Management lets ZENworks work with or without an installation of the Novell Client™ on the workstation. For more information, see [“Installing and Configuring the Desktop Management Agent” in the *Novell ZENworks 7 Desktop Management Installation Guide*](#).

3. If you are using Preboot Services, install Desktop Management Preboot Services (PXE Support) on your ZENworks Imaging server. For more information, see [Section 55.1, “Using Preboot Services \(PXE\),” on page 631](#).

or

If you are using a bootable CD or DVD, or a hard-disk partition, create a boot CD or DVD that points to the ZENworks Imaging server where the model images are stored. For more information, see [“Preparing an Imaging Boot Method” on page 631](#).

4. Create a policy for unregistered workstations that specifies which image to put on a new machine, depending on its hardware. For more information, see [Section 58.1, “Defining an Imaging Policy for Unregistered Workstations \(Server Policy\),” on page 697](#).

As each new workstation comes in, do the following:

1. If you are using Preboot Services, check to see if the workstation is PXE capable. Enable PXE if it isn't enabled by default. For more information, see [Section 55.1, "Using Preboot Services \(PXE\)," on page 631](#).
2. Physically connect the workstation to the network.
3. If you are using Preboot Services, boot the workstation from the ZENworks Imaging server.
or
If you are not using Preboot Services, boot the workstation with the imaging boot CDs or DVDs and consider installing the ZENworks partition to enable auto-imaging without needing to supply the CD or DVD. For more information, see [Step 5 on page 696 of Section 57.2, "Enabling a Windows Workstation for Auto-Imaging Operations," on page 694](#). After you have installed the partition, reboot the workstation from the ZENworks partition.
4. Let the workstation be auto-imaged by the policy.
5. After deploying the machine, register it as a Workstation object in Novell eDirectory™. For more information, see [Part III, "Automatic Workstation Import and Removal," on page 117](#).

53.2 Enabling Existing Workstations for Future Reimaging

With minimal disruption to users, you can enable existing workstations for possible future reimaging.

This process might need to be phased in by local administrators. Each administrator could do the following:

1. Install the ZENworks Imaging Windows Agent on each workstation by distributing an Application object. For more information, see [Step 3 on page 695 of Section 57.2, "Enabling a Windows Workstation for Auto-Imaging Operations," on page 694](#).
2. Register each workstation as a Workstation object in eDirectory. For more information, see [Part III, "Automatic Workstation Import and Removal," on page 117](#).
3. If the workstations are PXE capable, make sure PXE is enabled (see [Section 55.1, "Using Preboot Services \(PXE\)," on page 631](#)) and make sure that Desktop Management Preboot Services (PXE Support) is installed on your ZENworks Imaging server (see [Chapter 56, "Using ZENworks Desktop Management Preboot Services," on page 637](#)).
or
Prepare imaging CDs or DVDs that users can use when they run into trouble (see ["Preparing an Imaging Boot Method" on page 631](#)). These devices could point to a ZENworks Imaging server that contains the same clean images used for new workstations.
4. If a user runs into trouble, use the strategy for reimaging corrupted workstations. For more information, see [Section 53.3, "Reimaging Corrupted Workstations," on page 627](#).

53.3 Reimaging Corrupted Workstations

Without data loss or undue disruption to users, you can fix workstations that have become misconfigured or corrupted.

1. Create a policy for registered workstations. Use the same image-selection logic as the policy for new (unregistered) workstations. For more information, see [Section 58.2, “Defining an Imaging Policy for Registered Workstations \(Workstation Policy\),”](#) on page 699.
2. When a workstation needs to be fixed, have the user back up any files to the network that he or she wants to keep.
3. Flag the Workstation object in eDirectory using Novell ConsoleOne® to receive an image the next time it boots. For more information, see [Section 59.5, “Performing an Automatic Imaging Creation or Restoration,”](#) on page 709.
4. If it’s a newer workstation (with a ZENworks partition or PXE-enabled), the user should boot the workstation from the ZENworks partition or ZENworks Imaging server. If you are using Preboot Services, make sure that Desktop Management Preboot Services (PXE Support) is installed on your ZENworks Imaging server. For more information, see [Chapter 56, “Using ZENworks Desktop Management Preboot Services,”](#) on page 637.

or

If it’s an older workstation (without a ZENworks partition), the user should boot the workstation with the imaging boot CD or DVD.

5. After the image is laid down, restore any user files that are backed up to the network.

53.4 Restoring Lab or Classroom Workstations to a Clean State

After each lab session, you can restore every workstation to a clean state, removing any changes or additions made during the session. The following steps assume that the workstations are unregistered (not imported into eDirectory).

1. Create an image of a clean model workstation and store it on a ZENworks Imaging server. For more information, see [Section 60.1, “Manually Taking an Image of a Workstation,”](#) on page 711.

These images should include the Desktop Management Agent, which includes the ZENworks Imaging Windows Agent. ZENworks Desktop Management lets ZENworks work with or without an installation of the Novell Client™ on the workstation. For more information, see [“Installing and Configuring the Desktop Management Agent”](#) in the *Novell ZENworks 7 Desktop Management Installation Guide*.

2. If you are using Preboot Services, make sure that Desktop Management Preboot Services (PXE Support) is installed on your ZENworks Imaging server. For more information, see [Chapter 56, “Using ZENworks Desktop Management Preboot Services,”](#) on page 637.
3. If you are using Preboot Services and the workstations are PXE capable, make sure that PXE is enabled. For more information, see [Section 55.1, “Using Preboot Services \(PXE\),”](#) on page 631.

or

If you are not using Preboot Services or the ZENworks partition, create an imaging boot CD or DVD that points to the ZENworks Imaging server where the clean image is stored. For more information, see [“Preparing an Imaging Boot Method” on page 631](#).

4. Create a policy for unregistered workstations that specifies the clean image to restore. Choose the option to always force down the same base image. For more information, see [Section 58.1, “Defining an Imaging Policy for Unregistered Workstations \(Server Policy\),” on page 697](#).

Deploy each lab workstation as follows:

1. Physically connect the workstation to the lab network.
2. If you are using Preboot Services, boot the workstation from the ZENworks Imaging server.

or

If you are not using Preboot Services, boot the workstation with the imaging boot CD or DVD and install the ZENworks partition. For more information, see [Step 5 on page 696 of Section 57.2, “Enabling a Windows Workstation for Auto-Imaging Operations,” on page 694](#). After you have installed the partition, reboot the workstation from the ZENworks partition.

3. At the end of each lab session, reboot each workstation and let it be auto-imaged by the policy.

Preparing a ZENworks Imaging Server

54

Before you can use Novell® ZENworks® Desktop Management imaging services, you must install the Imaging components. If you have already done a typical Desktop Management installation on the server, the server is ready to act as an imaging server.

For further preparation instructions:

- [Section 54.1, “Imaging Server Prerequisites,” on page 629](#)
- [Section 54.2, “Preparing an Imaging Server Where Automatic Workstation Import Is Not Installed,” on page 630](#)

54.1 Imaging Server Prerequisites

Make sure your server meets the requirements specified in “[Preparation](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

In addition to the specific hardware requirements for the server, the ZENworks Imaging server must meet the following requirements:

- **A fixed IP address:** When you connect to the ZENworks Imaging server during a workstation imaging operation, you must do so using the fixed IP address or DNS name of the ZENworks Imaging server.
- **Enough space to store workstation images:** Unless you use compression (which is enabled by default) for your workstation images, they are nearly the same size as the data on the workstation hard disk, which could be hundreds of megabytes to several gigabytes.

Although the System Account should already have Full Control rights to the directory where you store image files, you should make sure that this is the case if you are running the Imaging component on a Microsoft server.

If you want to store an image locally (on a CD, DVD, hard disk, or Jaz drive) rather than on an ZENworks Imaging server, see [Section 61.1, “Using a CD or DVD for Disconnected Imaging Operations,” on page 719](#) and [Section 61.2, “Using a Hard Disk or Jaz Drive for Disconnected Imaging Operations,” on page 721](#).

- **Proxy DHCP server (Linux imaging servers only):** To avoid confusion, the Proxy DHCP daemon (novell-proxydhcp) is installed, but not enabled. For PXE devices to be able to communicate with Preboot Services, this daemon must be started manually on at least one server on each network segment.

Exactly how many servers and which specific servers should run this daemon is dictated by your network topology. As a rule of thumb, for every DHCP server deployed in your network, you should have a corresponding Proxy DHCP server.

- **Automatic Workstation Import (NetWare and Windows imaging servers only):** If you want to deploy images based on specific workstations, you should also install the Automatic Workstation Import component for ease in managing these deployments.

If you do not install Automatic Workstation Import, see [Section 54.2, “Preparing an Imaging Server Where Automatic Workstation Import Is Not Installed,”](#) on page 630 for further instructions.

54.2 Preparing an Imaging Server Where Automatic Workstation Import Is Not Installed

If you did not install the Automatic Workstation Import and Imaging components during installation of Desktop Management, use the following steps to install the necessary components:

- 1 Run the Desktop Management installation program (`winsetup.exe`) either on your server (Windows 2000/2003) or from a Windows workstation with a drive mapped to your server (NetWare®).
- 2 When prompted for the Novell eDirectory™ tree to install to, choose the tree that your server is in.
- 3 When prompted for the components to install, click *Automatic Workstation Import and Imaging*.
- 4 When prompted for the import/removal role, click *Import*.
- 5 If you are installing Preboot Services (PXE), select it when prompted.
- 6 When the installation is done, restart your server.

Preparing an Imaging Boot Method

55

The Novell® ZENworks® Desktop Management ZENworks Imaging Engine that performs the actual imaging of a workstation is a Linux application. Therefore, the workstation must be temporarily booted to Linux while the imaging is performed.

Unless you use Preboot Services, you need to prepare a boot device that has the Linux kernel, Desktop Management Workstation ZENworks Imaging Engine, and network drivers installed.

The following sections contain additional information:

- [Section 55.1, “Using Preboot Services \(PXE\),” on page 631](#)
- [Section 55.2, “Preparing Imaging Boot CDs or DVDs,” on page 632](#)
- [Section 55.3, “Using the ZENworks Imaging Floppy Boot Disk Creator,” on page 633](#)
- [Section 55.4, “Creating an Imaging Hard-Disk Partition,” on page 635](#)

55.1 Using Preboot Services (PXE)

Preboot Execution Environment (PXE) is an industry-standard protocol that allows a workstation to boot up and execute a program from the network before the workstation operating system starts. PXE uses DHCP (Dynamic Host Configuration Protocol) and TFTP (Trivial File Transfer Protocol). The PXE environment is loaded from either the NIC in flash memory or read-only memory, or in the same memory as the system BIOS.

Desktop Management Preboot Services uses PXE to find out if there is imaging work specified for a workstation and to provide the workstation with the files necessary to boot to the Desktop Management imaging environment.

Before you can use Preboot Services, you need to do the following:

- Install the Desktop Management Imaging and Preboot Services (PXE Support) components on your ZENworks Imaging server.
- Enable PXE on the workstation.
- Have a standard DHCP server, either on your ZENworks Imaging server or on another network server.

For information about the requirements and installation of Preboot Services, see the *Novell ZENworks 7 Desktop Management Installation Guide*. For information about deployment and administration of Preboot Services, see [Chapter 56, “Using ZENworks Desktop Management Preboot Services,” on page 637](#).

55.1.1 If You Have Previously Installed a ZENworks partition

An existing partition is not updated when a ZENworks support pack is applied.

If you decide to use Preboot Services but have previously installed a ZENworks partition on the workstation, you can disable or delete the partition.

You can disable (and enable) the ZENworks partition when you boot to Linux using any imaging boot device or method.

You can delete the ZENworks partition only when you boot the workstation from an imaging boot method other than the ZENworks partition.

For more information on disabling or deleting a partition, see [Step 9](#) in “[Creating a Workstation Image Object](#)” on [page 706](#).

IMPORTANT: After you have deleted the ZENworks partition, you need to make sure that the image you put on the workstation was made on a workstation without a ZENworks partition. Otherwise, the wrong MBR (Master Boot Record) is restored, and the workstation fails to boot. In addition, if you remove the ZENworks partition from a Windows NT, Windows 2000, or Windows XP machine, Windows is not able to boot. You should only remove the ZENworks partition if you are going to restore an image to the workstation.

55.2 Preparing Imaging Boot CDs or DVDs

If you have CD- or DVD-burning software and hardware, you can create an imaging boot CD or DVD for performing imaging operations. If you have WinIso, a third-party CD image file utility, you can use it to insert the `settings.txt` and other needed files directly into the imaging boot CD rather than following the instructions in this section.

NOTE: Desktop Management Imaging does not currently support booting from a SCSI CD-ROM device.

You can use the `bootcd.iso` image available on the ZENworks Imaging server to create an imaging boot CD or DVD.

To create an imaging boot CD or DVD:

- 1 In a temporary working area, copy the `settings.txt` file containing the settings you want for the imaging boot process.

This file is located in the `\public\zenworks\imaging` directory in your Desktop Management installation (on the ZENworks Imaging server). For more information, see [Section 63.5, “Imaging Configuration Parameters \(Settings.txt\),” on page 758](#).

- 2 In the temporary working area, add any image files you want to store on the CD or DVD.
- 3 Use your CD- or DVD-burning software to create a CD or DVD from the `bootcd.iso` image.

The `bootcd.iso` file is located in the `\public\zenworks\imaging` directory in your Desktop Management installation (on the ZENworks Imaging server).

- 4 Use your CD- or DVD-burning software to add the contents of your temporary working area to the root of the CD or DVD, including the `settings.txt` file, any Linux network drivers, and any Desktop Management image files.

IMPORTANT: Adding these files makes the CD or DVD a multisession CD or DVD. To boot a workstation from such a CD or DVD, the CD or DVD drive must support multisession CDs or DVDs.

If you can't create a multisession CD or DVD, or you are using a drive that does not support multisession CDs or DVDs and you don't need to store the image on the CD or DVD, you can still create an imaging boot CD or DVD. Create the CD or DVD from the `bootcd.iso` file as in [Step 3 on page 632](#). Boot the workstation using the CD or DVD. When you are prompted for `settings.txt`, insert the diskette containing this file in the diskette drive.

- 5 Use your CD- or DVD-burning software to finalize the CD or DVD.

For information on how to use the CD or DVD to perform disconnected imaging operations, see [“Setting Up Disconnected Imaging Operations” on page 719](#).

55.3 Using the ZENworks Imaging Floppy Boot Disk Creator

The ZENworks Imaging Floppy Boot Disk Creator allows you to do the following:

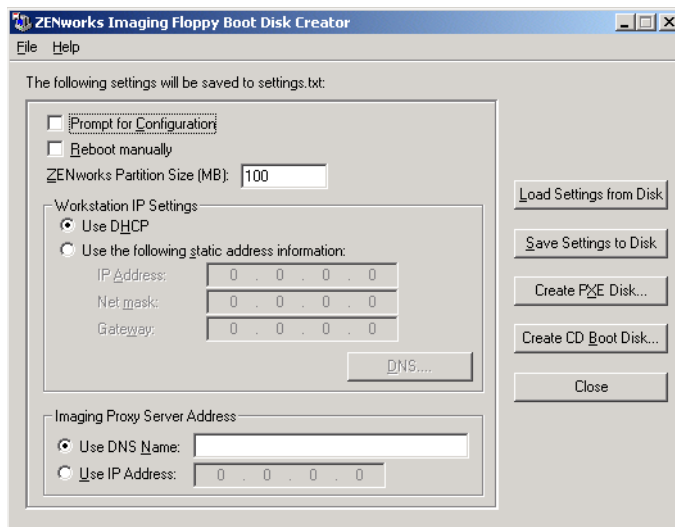
- [Section 55.3.1, “Starting the ZENworks Imaging Boot Disk Creator,” on page 633](#)
- [Section 55.3.2, “Preparing a CD Boot Diskette,” on page 634](#)
- [Section 55.3.3, “Configuring the Settings.txt File,” on page 634](#)
- [Section 55.3.4, “Creating a PXE Disk,” on page 635](#)

55.3.1 Starting the ZENworks Imaging Boot Disk Creator

- 1 To start the boot disk creator as a standalone Windows utility, double-click the `zimboot.exe` file (`sys:public\zenworks\imaging\zimboot.exe` on the ZENworks Imaging server). There are no command line parameters.

or

To start the utility from ConsoleOne from the server, click *Tools > ZENworks Utilities > Imaging > Create or Modify Boot Diskette*.



- 2 Continue with the appropriate section:
 - “Preparing a CD Boot Diskette” on page 634
 - “Configuring the Settings.txt File” on page 634
 - “Creating a PXE Disk” on page 635

TIP: If the Imaging Boot Disk Creator fills up too much of your screen, change your screen resolution to a setting greater than 800 X 600.

For details on these and other configuration options, see the context-sensitive help (click the *Help* menu or press F1) in the utility. The configuration settings you make in the utility are saved to the `settings.txt` file. You can edit this file later if needed. For details on the format of this file, see [Section 63.5, “Imaging Configuration Parameters \(Settings.txt\),” on page 758](#).

55.3.2 Preparing a CD Boot Diskette

The CD boot diskette is easy to prepare. One diskette is required. The `zimghboot.exe` utility is used to create the diskette, which is used to enable devices that cannot normally boot a CD or DVD to do so.

To create a CD boot diskette:

- 1 Format one high-density diskette, or use a preformatted blank diskette.
- 2 Start the ZENworks Imaging Boot Disk Creator (see [“Starting the ZENworks Imaging Boot Disk Creator” on page 633](#)).
- 3 Insert the formatted blank diskette, click *Create CD Boot Disk*, then click *OK*.
- 4 When you are finished using this utility, click *Close*.

Use this diskette to boot workstations that cannot be booted using a CD or DVD. The diskette boots the workstation, enabling access to the imaging CD or DVD.

55.3.3 Configuring the Settings.txt File

The `settings.txt` file is required for imaging workstations. A default copy is provided with Desktop Management, so you can create and configure a version for an imaging session.

To configure a `settings.txt` file for imaging:

- 1 Format one high-density diskette, or use a preformatted blank diskette.
- 2 Start the ZENworks Imaging Boot Disk Creator (see [“Starting the ZENworks Imaging Boot Disk Creator” on page 633](#)).
- 3 Click *Load Settings from Disk*.

This allows you to browse for the `settings.txt` file. Then it populates the fields in this dialog box from information in the `settings.txt` file. You can modify the `settings.txt` file, as instructed in subsequent steps.

- 4 Browse for the `settings.txt` file, then click *Open*.

The default copy shipped with Desktop Management is located in the `\zenworks\imaging` directory on your ZENworks Imaging server.

- 5 (Required) In the ZENworks Imaging Floppy Boot Disk Creator dialog box, go to the Imaging Proxy Server Address section, then specify either the fixed IP address or the full DNS name of your ZENworks Imaging server.
- 6 (Optional) For the other fields and options on the dialog box, keep the default settings, unless you have a specific reason to change a setting, such as to specify a particular device's IP Address in the Workstation IP Settings section.
Click *Help* for details on specific settings, or see [Section 63.5, "Imaging Configuration Parameters \(Settings.txt\)," on page 758](#).
- 7 Click *Save Settings to Disk*.
- 8 Browse for where you want to save the `settings.txt` file, then click *Save*.
The default location is `A:\`. You can save to a different location for use in burning it to an imaging CD or DVD.
- 9 When you are finished using this utility, click *Close*.

55.3.4 Creating a PXE Disk

You can use the Boot Disk Creator to create a PXE boot diskette that allows you to use PXE on a workstation that is not PXE-enabled.

- 1 Format one high-density diskette, or use a preformatted blank diskette.
- 2 Start the ZENworks Imaging Boot Disk Creator (see ["Starting the ZENworks Imaging Boot Disk Creator" on page 633](#)).
- 3 Insert the formatted blank diskette, then click *Create PXE Disk* to launch PXE-on-Disk.
For more information, see [Section 56.7, "Using the Desktop Management Preboot Services PXE-on-Disk Utility," on page 677](#).
- 4 When you are finished using this utility, click *Close*.

55.4 Creating an Imaging Hard-Disk Partition

If you want to set up a workstation for unattended imaging operations and are unable to use Preboot Services (PXE), you can create a ZENworks partition on the hard disk. If you make the partition big enough, you can even store an image of the workstation's hard disk, which can be useful if the workstation becomes misconfigured or corrupted when the network connection is lost.

WARNING: Installing the ZENworks partition destroys all data on that hard drive.

To create a ZENworks partition:

- 1 Create an imaging CD or DVD (see [Section 55.2, "Preparing Imaging Boot CDs or DVDs," on page 632](#)).
- 2 Take an image of the workstation as instructed in [Section 60.1, "Manually Taking an Image of a Workstation," on page 711](#).

IMPORTANT: Do this even if you have taken an image of the workstation previously. This ensures that the new image captures the changes you made in the preceding steps.

- 3 After the image is created, reboot the workstation with the imaging boot method, type `install` at the boot prompt, then press Enter.

This starts the process of creating the ZENworks partition in the first partition slot. It also destroys all existing partitions, even if slot 1 is empty and available. By default, the ZENworks partition size is 150 MB.

If the ZENworks partition already exists, it is upgraded, and your existing Windows partitions are left intact.

- 4 (Optional) After the ZENworks partition is created and the bash prompt is displayed, type `img dump`, then press Enter.

This displays a list of the partition slots on the workstation. Unless you are upgrading your ZENworks partition, each partition slot should be empty and none should be active. The ZENworks partition is hidden from the list, so the number of partition slots in the list should be one less than before.

or

Type `img` to display a menu, select *Dump*, then select *No Geometry*.

- 5 At the bash prompt, restore the image you took in [Step 2](#).

Use the `img restorep` command or select *Restore an Image*, then select *Proxy Image* from the menu as instructed in [Step 6](#) of [Section 60.2](#), “[Manually Putting an Image on a Workstation](#),” on page 715.

- 6 (Optional) After the image is restored and the bash prompt is displayed, use the `img dump` command to redisplay the list of the partition slots on the workstation.

or

Type `img` to display a menu, select *Dump*, then select *No Geometry*.

You should now see information about the Windows partitions that are restored and activated. There should still be one less partition slot than before because the ZENworks partition is still hidden (and will continue to be).

- 7 At the bash prompt, type `lilo.s`, then press Enter.

- 8 When the bash prompt is displayed, reboot the workstation.

The workstation should boot to Windows. If the bash prompt is displayed, enter the `lilo.s` command again and reboot a second time.

Using ZENworks Desktop Management Preboot Services

56

This section provides information about using Novell® ZENworks® Desktop Management Preboot Services on your network.

There are three methods that you can use for imaging: Preboot Services, a bootable CD or DVD, or a Linux hard-disk partition. For more information, see [“Preparing an Imaging Boot Method” on page 631](#).

Because Preboot services offers the greatest flexibility and options, we recommend using it.

- [Section 56.1, “Understanding Desktop Management Preboot Services,” on page 637](#)
- [Section 56.2, “Installing and Setting Up Desktop Management Preboot Services,” on page 649](#)
- [Section 56.3, “Checking the Preboot Services Server Setup,” on page 649](#)
- [Section 56.4, “Deploying Desktop Management Preboot Services in a Network Environment,” on page 654](#)
- [Section 56.5, “Enabling PXE on a Workstation,” on page 668](#)
- [Section 56.6, “Administering Desktop Management Preboot Services,” on page 670](#)
- [Section 56.7, “Using the Desktop Management Preboot Services PXE-on-Disk Utility,” on page 677](#)
- [Section 56.8, “Editing the Desktop Management Preboot Services Menu,” on page 681](#)

56.1 Understanding Desktop Management Preboot Services

This section contains the following information to help you to understand ZENworks Desktop Management Preboot Services:

- [Section 56.1.1, “About Desktop Management Preboot Services,” on page 637](#)
- [Section 56.1.2, “A Typical Preboot Services Operation,” on page 638](#)
- [Section 56.1.3, “Illustrating the Preboot Services Processes for Linux Imaging Servers,” on page 639](#)
- [Section 56.1.4, “Illustrating the Preboot Services Processes for NetWare and Windows Imaging Servers,” on page 646](#)

56.1.1 About Desktop Management Preboot Services

PXE (Preboot Execution Environment) is an industry-standard protocol that allows a workstation to boot up and execute a program from the network before the workstation operating system starts. PXE uses DHCP (Dynamic Host Configuration Protocol) and TFTP (Trivial File Transfer Protocol). The PXE environment is loaded from either the NIC in flash memory or read-only memory, or in the same memory as the system BIOS.

Desktop Management Preboot Services uses PXE to find out if there is imaging work specified for a workstation and to provide the workstation with the files necessary to boot to the Desktop Management imaging environment.

By using Preboot Services, you can put an image on a workstation even if the workstation's hard disk is blank. You do not need to use a ZENworks Desktop Management imaging boot CD or DVD, or a Desktop Management imaging hard-disk (Linux) partition on the workstation.

Before you can use Preboot Services, you need to do the following:

- Install the Desktop Management Imaging and Preboot Services (PXE Support) components on your ZENworks Imaging server.
- Enable PXE on the workstation.
- Have a standard DHCP server, either on your ZENworks Imaging server or on another network server.

For information about requirements, installing Desktop Management and Preboot Services on your ZENworks Imaging server, enabling PXE on a workstation, and configuring your DHCP server, see [Section 56.2, “Installing and Setting Up Desktop Management Preboot Services,” on page 649.](#)

56.1.2 A Typical Preboot Services Operation

When a PXE-enabled workstation starts to boot up, it sends a DHCP discovery request to determine the IP address of the ZENworks Imaging server. The DHCP server responds with an IP address for the client to use, and the Proxy DHCP server responds with the IP addresses of the Transaction server, TFTP, and MTFTP (Multicast TFTP) servers, as well as the filename of the Preboot Services client.

The PXE workstation then downloads the Preboot Services client (`dinic.sys`) using either TFTP or MTFTP.

After the Preboot Services client is downloaded and executed, the workstation checks the Preboot Services Transaction server to see if there is any imaging work to do. If there is imaging work to do, it downloads the Desktop Management Workstation Imaging environment (`/srv/tftp/boot/linux` and `linld.com`) from the server so that the workstation can be booted to Linux and any imaging tasks can be performed. If there are no imaging tasks to perform, these files are not downloaded and the workstation proceeds to boot to its operating system.

In addition to using PXE for automation, you can also execute Preboot work manually using one of the following:

- Preboot Services Menu (if enabled for the device)
- Preboot Services bootable CD or DVD
- ZENworks partition

For more information, see [Chapter 60, “Performing Manual Imaging Operations,” on page 711.](#)

56.1.3 Illustrating the Preboot Services Processes for Linux Imaging Servers

The following illustrations show the interaction between a Preboot Services (PXE) device and a ZENworks Imaging server, starting when the PXE device is turned on and begins to boot, and ending when imaging work begins on that device. The information assumes that the devices and imaging servers are in the same network segment.

Depending on whether novell-proxydhcp is configured on the same server as the standard DHCP server or on a different server, the imaging process begins differently. The following sections illustrate how the process begins for each configuration:

- “Phase 1a: Standard DHCP and Novell Proxy DHCP Configured on Separate Servers” on page 640
- “Phase 1b, Part A: Standard DHCP and Novell Proxy DHCP Configured on the Same Server” on page 641
- “Phase 1b, Part B: Standard DHCP and Novell Proxy DHCP Configured on the Same Server” on page 642

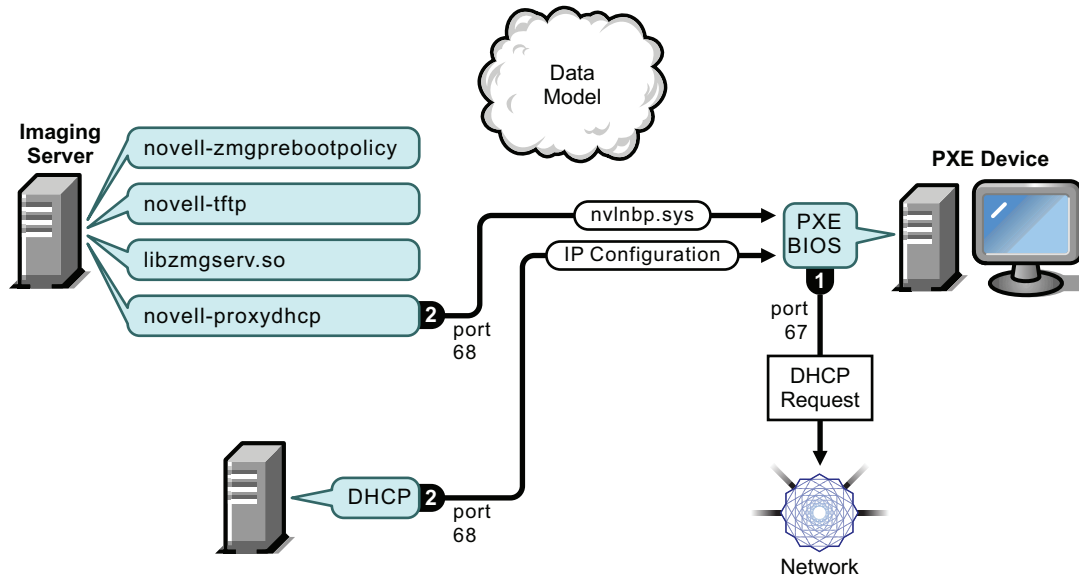
Then, the subsequent phases are the same:

- “Phase 2” on page 642
- “Phase 3” on page 643
- “Phase 4” on page 643
- “Phase 5” on page 644
- “Phase 6” on page 644
- “Phase 7” on page 645
- “Phase 8” on page 645

Phase 1a: Standard DHCP and Novell Proxy DHCP Configured on Separate Servers

For this example, the DHCP server and the ZENworks Imaging server are two separate servers on the network.

Figure 56-1 DHCP Configuration on Separate Servers



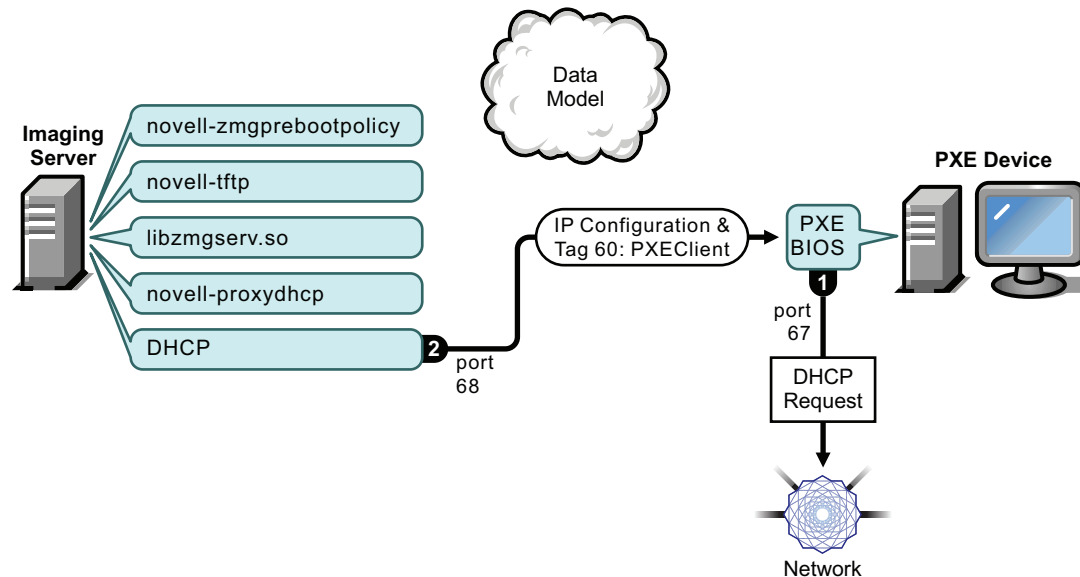
Processes:

1. When the device boots, the PXE BIOS issues a DHCP request with PXE extensions. The request is broadcast on port 67.
2. The DHCP server responds with IP configuration information on port 68, and the Proxy DHCP server responds on port 68 with the name of the bootstrap program (`nvlnbp.sys`) and the IP address of the TFTP daemon where it can be found.
3. Continue with **“Phase 2”** on page 642.

Phase 1b, Part A: Standard DHCP and Novell Proxy DHCP Configured on the Same Server

For this example, the DHCP server and the ZENworks Imaging server are configured on the same server on the network. See “[Phase 1b, Part B: Standard DHCP and Novell Proxy DHCP Configured on the Same Server](#)” on page 642 for the second part of this example.

Figure 56-2 DHCP Configuration on the Same Server, Part A

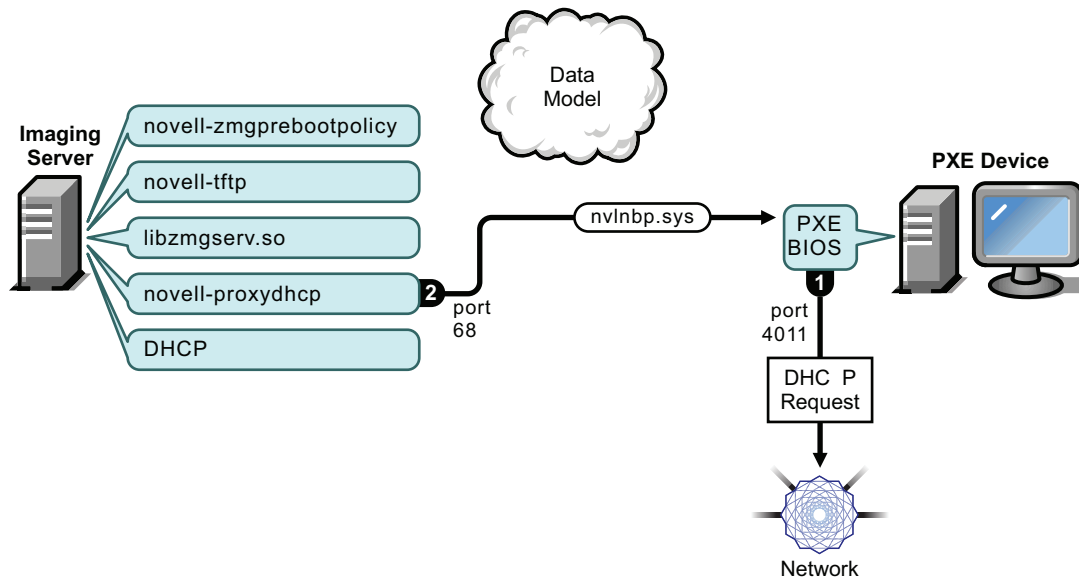


Processes:

1. When the device boots, the PXE BIOS issues a DHCP request with PXE extensions. The request is broadcast on port 67.
2. The DHCP server responds with IP configuration information on port 68, including **tag 60 for PXEClient**, which indicates that novell-proxydhcp is running on the same server.

Phase 1b, Part B: Standard DHCP and Novell Proxy DHCP Configured on the Same Server

Figure 56-3 DHCP Configuration on the Same Server, Part B

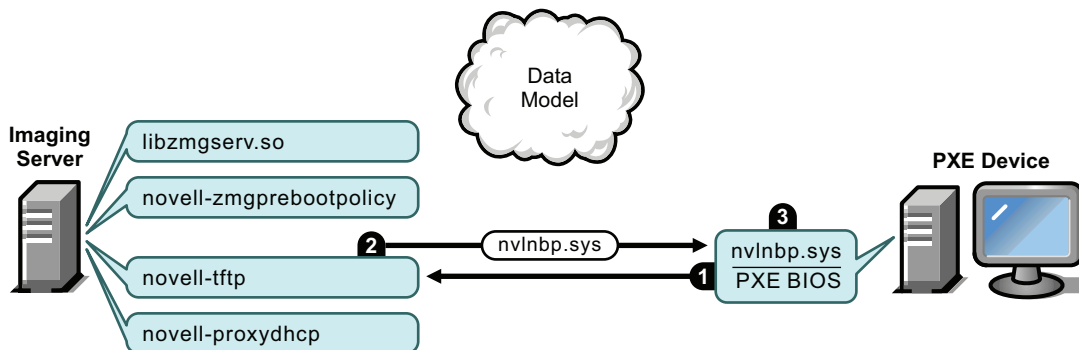


Processes:

1. When the device sees tag 60 in the DHCP response, the PXE BIOS reissues the DHCP request on port 4011.
2. The Proxy DHCP server responds on port 68 with the name of the bootstrap program (`nvlnbp.sys`) and the IP address of the TFTP daemon where it can be found.
3. Continue with **“Phase 2”** on page 642.

Phase 2

Figure 56-4 Phase 2 of the Preboot Services Process

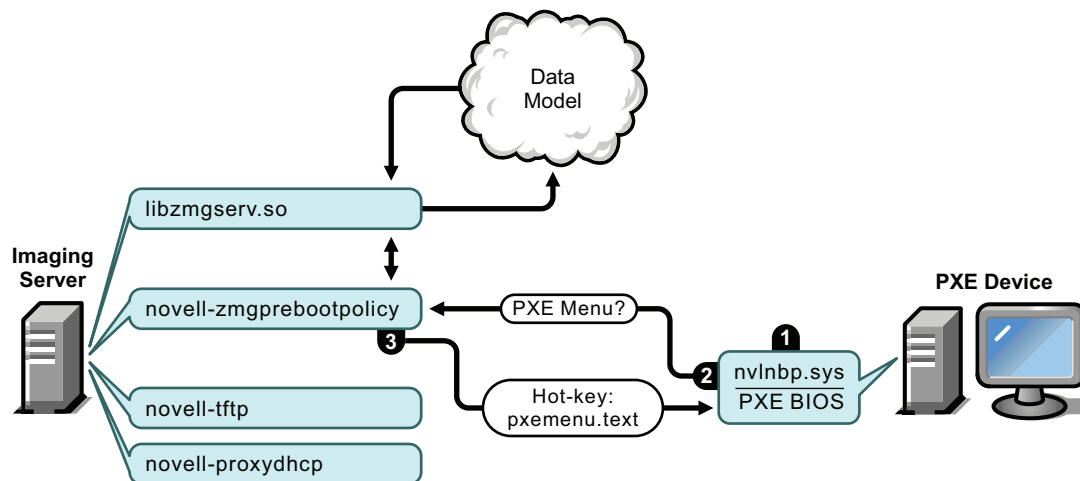


Processes:

1. The PXE BIOS requests `nvlnbp.sys` from the TFTP server.
2. The TFTP server sends `nvlnbp.sys` to the PXE device.
3. The PXE device loads `nvlnbp.sys` into memory.

Phase 3

Figure 56-5 Phase 3 of the Preboot Services Process

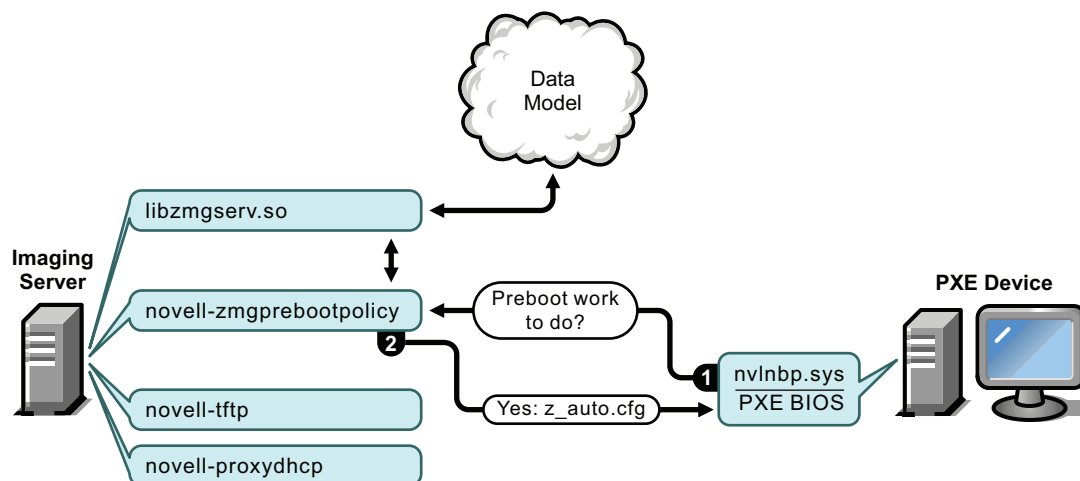


Processes:

1. Hardware detection is performed by `nvlnbp.sys` and it reads the image-safe data.
2. `Nvlnbp.sys` requests the Preboot Services Menu configuration from the Data Model via the `novell-zmgprebootpolicy` daemon.
3. The `novell-zmgprebootpolicy` daemon returns the Preboot Services Menu configuration. In this case, the menu described in `pxemenu.txt` is displayed when a user presses the hot key.

Phase 4

Figure 56-6 Phase 4 of the Preboot Services Process



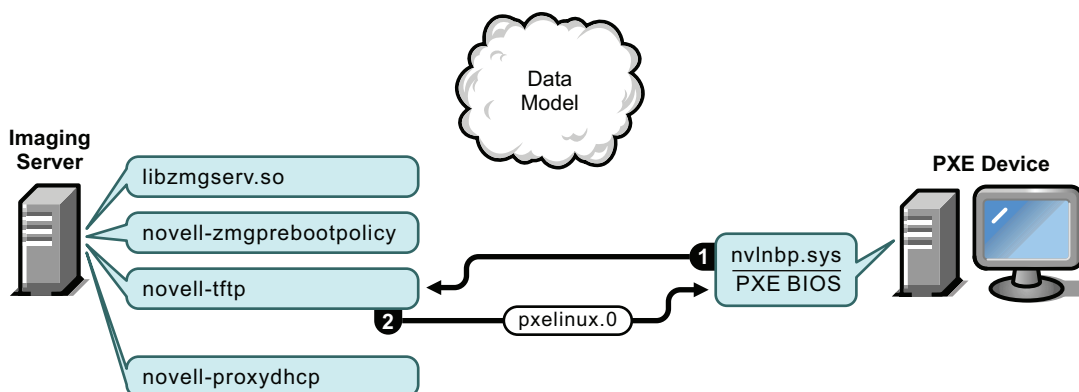
Processes:

1. Assuming no Preboot Services Menu is displayed, the device asks the Data Model (via `novell-zmgprebootpolicy`) if any work is assigned.

- Assuming work is assigned, the novell-zmgprebootpolicy daemon responds with the name of the configuration file to use in performing the preboot work (`z_auto.cfg` in this example).

Phase 5

Figure 56-7 Phase 5 of the Preboot Services Process

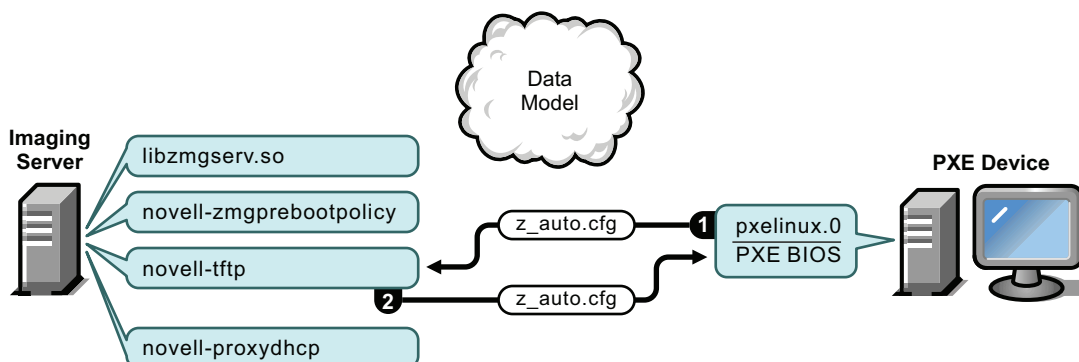


Processes:

- The PXE device requests `pxelinux.0` from the TFTP server.
- The TFTP server sends `pxelinux.0` to the device.

Phase 6

Figure 56-8 Phase 6 of the Preboot Services Process

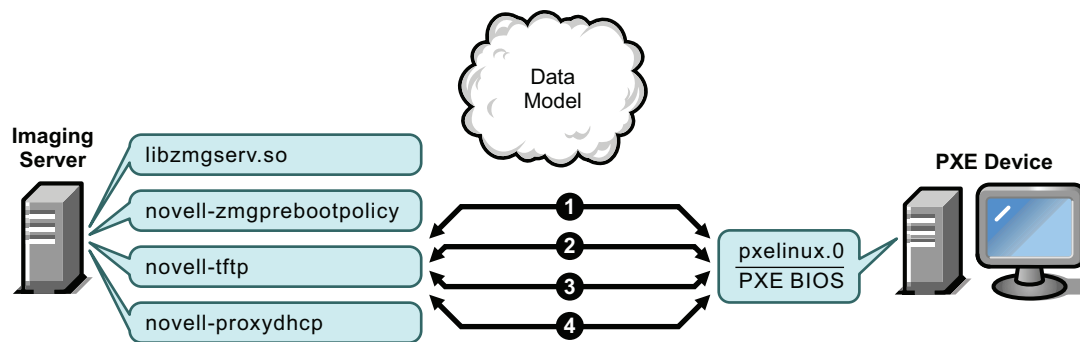


Processes:

- Pxelinux.0 replaces `nvlnbp.sys` in memory and requests `z_auto.cfg` from the TFTP server.
- The TFTP server sends the `z_auto.cfg` file to the device.

Phase 7

Figure 56-9 Phase 7 of the Preboot Services Process

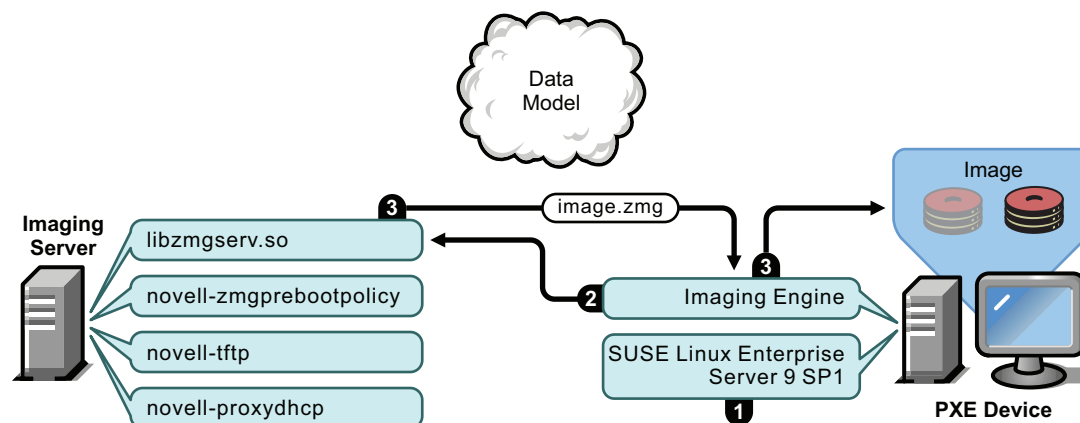


Processes:

1. `Pxelinux.0` requests and receives `/boot/kernel` from the TFTP server.
2. `Pxelinux.0` requests and receives `/boot/initid` from the TFTP server.
3. `Pxelinux.0` requests and receives `/boot/root` from the TFTP server.
4. `Pxelinux.0` requests and receives `/boot/updateDrivers.tgz` from the TFTP server, but is denied because the file does not exist (it is used to provide post-release software updates).

Phase 8

Figure 56-10 Phase 8 of the Preboot Services Process



Processes:

1. SUSE Linux Enterprise Server (SLES) 9 SP1 is loaded and run on the device.
2. The ZENworks Imaging Engine (`img`) requests the assigned Preboot Services work details, then performs the work.
3. The image is laid down on the device and it automatically reboots.

56.1.4 Illustrating the Preboot Services Processes for NetWare and Windows Imaging Servers

The following diagrams show the interaction between a Preboot Services (PXE) client workstation and a ZENworks Imaging server, starting when the PXE client workstation is turned on and begins to boot up, and ending when imaging work begins on that workstation.

Three diagrams are used to show one complete process. The first diagram shows steps 1-5, the second diagram shows steps 6-11, and the third diagram shows steps 12-19. Each number corresponds to explanatory text in a table following the diagram.

In this example, the DHCP server and the ZENworks Imaging server are two separate servers on the network, although it is possible to run both from the same server with some additional configuration. This example also assumes that the client workstation and the servers are in the same segment.

- “Diagram 1 (Steps 1-5)” on page 646
- “Diagram 2 (Steps 6-11)” on page 647
- “Diagram 3 (Steps 12-19)” on page 648

Diagram 1 (Steps 1-5)

Figure 56-11 Preboot Services Processes, Diagram 1 (Steps 1-5)

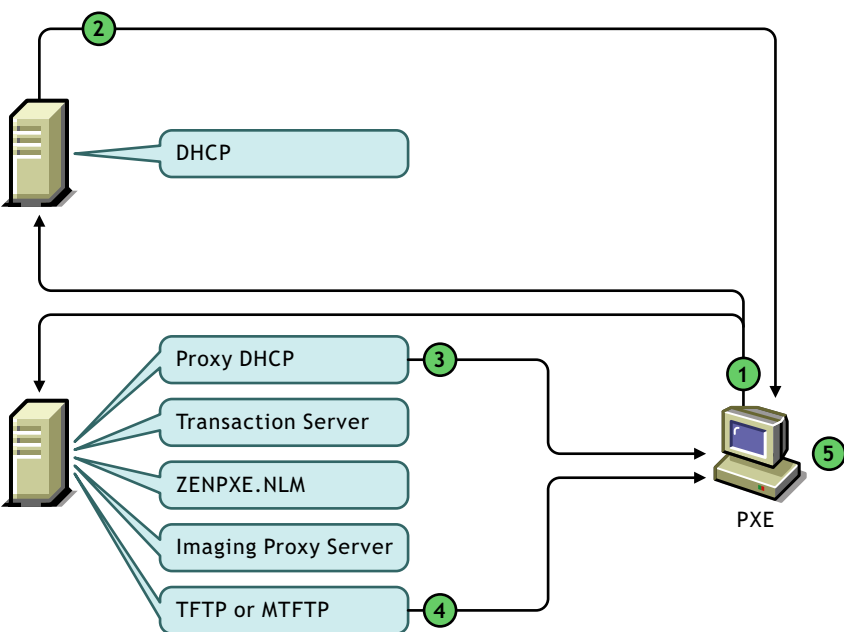


Table 56-1 Preboot Services Processes, Steps 1-5

Step	Explanation
1	The workstation is turned on and begins to boot up. PXE (triggered by the BIOS, network interface card, or PXE-on-Disk boot diskette) sends a DHCP request to the network. The DHCP request includes PXE extensions.

Step	Explanation
2	The DHCP server responds with an IP address for the workstation to use. This step might occur before or after Step 3.
3	<p>The Proxy DHCP server responds with the IP addresses of the Preboot Services Transaction server, Preboot Services TFTP and MTFTP servers, and with the name of the Preboot Services client (<code>dinic.sys</code>).</p> <p>The Preboot Services client includes a preboot component that makes the workstation available on the network before the operating system has loaded. This component ensures that the workstation can contact the Transaction server (in Step 7) even when there is no operating system installed on the workstation.</p>
4	<p>Using TFTP or MTFTP, the Preboot Services client (<code>dinic.sys</code>) is downloaded to the PXE client workstation.</p> <p>TFTP is used by default because it speeds the workstation's boot process; however, you can change the configuration to use MTFTP. For more information, see Section 56.2, "Installing and Setting Up Desktop Management Preboot Services," on page 649.</p> <p>If a PXE-on-Disk boot diskette was used in Step 1, the Preboot Services client does not need to be downloaded, and this step does not occur.</p>
5	The Preboot Services client is loaded on the PXE client workstation.

Diagram 2 (Steps 6-11)

Figure 56-12 Preboot Services Processes, Diagram 2 (Steps 6-11)

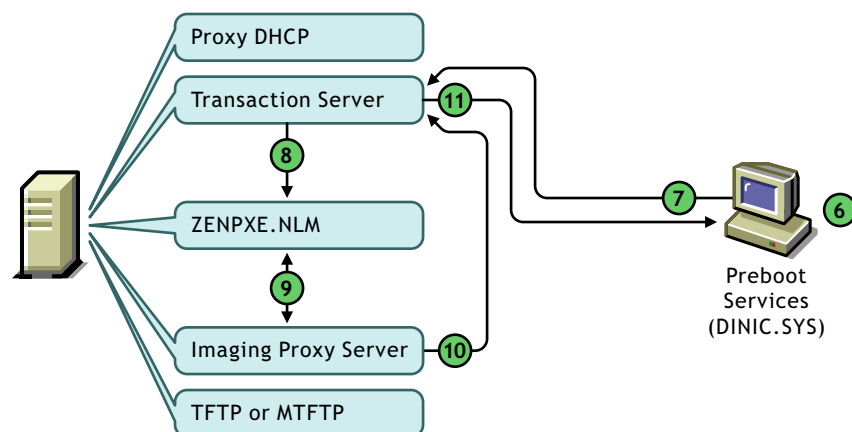


Table 56-2 Preboot Services Processes, Steps 6-11

Step	Explanation
6	The Preboot Services client reads the image-safe data and discovers the hardware on the workstation.
7	The Preboot Services client connects to the Transaction server and authenticates with the server. The Preboot Services client sends information about the workstation to the Transaction server with a request to find out if the PXE menu should be displayed on this workstation.

Step	Explanation
15	<p>zenpxe.nlm checks with the Imaging Proxy Server to see if there is any imaging work specified for this workstation.</p> <p>The Imaging Proxy Server performs a limited check of attributes, multicast sessions, and imaging rules. (A more detailed check for imaging work is performed by the ZENworks Imaging Engine after the workstation is booted to Linux.)</p>
16	The Imaging Proxy Server sends information about any imaging work specified for this workstation to the Transaction server.
17	The Transaction server sends information about any imaging work specified for this workstation to the Preboot Services client.
18	The Preboot Services client contacts the TFTP server and downloads the files necessary to boot to the Desktop Management Workstation Imaging (Linux) environment (/srv/tftp/boot/linux and linld.com).
19	The workstation boots to the Desktop Management Imaging environment and proceeds with the imaging work.

56.2 Installing and Setting Up Desktop Management Preboot Services

For information about the hardware requirements for the Preboot Services server, see “[Preboot Services Subinstallation Hardware Requirements](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

For information about the requirements for workstations using Preboot Services, see “[User Workstation Hardware Requirements](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

For information about installing and setting up Desktop Management Preboot Services, see “[Desktop Management Server Installation Procedure](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

56.3 Checking the Preboot Services Server Setup

This section provides information on how to check the configuration of Desktop Management Preboot Services after it is installed, and how to set up standard DHCP and Proxy DHCP services on the same server.

- [Section 56.3.1, “Overview of Preboot Services Components,”](#) on page 650
- [Section 56.3.2, “Checking Imaging Server Setup,”](#) on page 651
- [Section 56.3.3, “Setting up Standard DHCP and Proxy DHCP Services on the Same Server,”](#) on page 652

56.3.1 Overview of Preboot Services Components

The Preboot Services components are different for the supported imaging servers:

- “Preboot Services Components for Linux Imaging Servers” on page 650
- “Preboot Services Components for NetWare and Windows Imaging Servers” on page 650

Preboot Services Components for Linux Imaging Servers

The following components are installed as part of Preboot Services:

Table 56-4 *Preboot Service Components*

Daemon	Description
libzmgsserv.so	This library file is used by eDirectory to provide imaging services to the devices.
novell-proxydhcp	The novell-proxydhcp daemon runs alongside a standard DHCP server to inform PXE devices of the IP address of the TFTP server. The Proxy DHCP server also responds to PXE devices to indicate which bootstrap program (<code>nvlntp.sys</code>) to use.
novell-tftp	<p>The novell-tftp daemon is used by PXE devices to request files that are needed to perform imaging tasks. The TFTP server also provides a central repository for these imaging files, such as the Linux kernel, <code>initrd</code>, and <code>nvlntp.sys</code>.</p> <p>A PXE device uses this server to download the bootstrap program (<code>nvlntp.sys</code>).</p>
novell-zmgprebootpolicy	The PXE devices use the novell-zmgprebootpolicy daemon to check if there are any images associated with the device.

The novell-proxydhcp daemon must be started manually and does not need to be run on all ZENworks Imaging servers.

The other three daemons are started automatically when installing ZENworks Linux Management, or any time the server is rebooted, and must run on all ZENworks Imaging servers.

For more information on these daemons, see [Section 63.7, “Imaging Server \(Imgserv.nlm or .dll or .dlm, or Linux Daemons\),” on page 761](#).

Preboot Services Components for NetWare and Windows Imaging Servers

The following components are installed as part of Preboot Services:

- “Proxy DHCP Server” on page 651
- “TFTP/MTFTP Server” on page 651
- “Transaction Server” on page 651

Proxy DHCP Server

The Preboot Services Proxy DHCP server runs alongside a standard DHCP server to inform Preboot Services clients of the IP address of the TFTP, MTFTP, and Transaction servers. The Proxy DHCP server also responds to PXE clients to indicate which boot server (TFTP or MTFTP) to use.

TFTP/MTFTP Server

The Preboot Services TFTP/MTFTP server is used by the Preboot Services client to request files that are needed to perform imaging tasks. The TFTP server also provides a central repository for these imaging files (`/srv/tftp/boot/linux` and `linld.com`).

A PXE client uses this server to download the Preboot Services client.

TFTP is used by default because it speeds up the workstation's boot process; however, you can change the configuration to use MTFTP.

Transaction Server

The Preboot Services client connects to the Transaction server to check if there are any imaging actions that need to be performed on the workstation.

56.3.2 Checking Imaging Server Setup

The methods for checking the setup on ZENworks Imaging servers depends on the server's platform:

- [“Checking the Setup on a Linux Server” on page 651](#)
- [“Checking the Setup on a NetWare Server” on page 652](#)
- [“Checking the Setup on a Windows Server” on page 652](#)

Checking the Setup on a Linux Server

After the Desktop Management Preboot Services components are installed, the following services should be installed and running on the server:

Table 56-5 *Preboot Services Daemons*

Service	Command to Check Its Status
<code>novell-tftp</code>	<code>/etc/init.d/novell-tftp status</code>
<code>novell-zmgprebootpolicy</code>	<code>/etc/init.d/novell-zmgprebootpolicy status</code>

You should not need to change the default configuration of these daemons.

The status of the `libzmgserv.so` file cannot be checked.

If the Preboot Services components are installed to a Linux server that is also a standard DHCP server, see [“Linux DHCP Server” on page 653](#).

Checking the Setup on a NetWare Server

After the Desktop Management Preboot Services components are installed, the following services should be installed and running on the server:

- `pmap.nlm`
- `tftp.nlm`
- `pdhcp.nlm`
- `ds.nlm`

You can use the `pstart.ncf` file to start Preboot Services with a single command.

You can use the `pstop.ncf` file to stop Preboot Services with a single command.

You should not need to change the default configuration of these services unless the default multicast IP is already in use in your environment or you moved any of the PXE-installed files from their default directories.

For information about configuring these services, see [“Configuring Preboot Services Servers in NetWare” on page 671](#).

If the Preboot Services components are installed to a NetWare® 6.x server that is also a standard DHCP server, see [“NetWare 6.x DHCP Server” on page 653](#).

Checking the Setup on a Windows Server

After the Desktop Management Preboot Services components are installed, the following services should be installed and running on the server:

- Proxy DHCP Server
- MTFTP Server
- TFTP Server
- Transaction Server

You should not need to change the default configuration of these services unless the default multicast IP is already in use in your environment or you moved any of the PXE-installed files from their default directories.

For information about configuring these services, see [“Server Configurations” on page 655](#).

If the 2000/XP/2003 server where the Preboot Services components are installed is also a DHCP server, see [“Windows 2000 Advanced Server” on page 654](#).

56.3.3 Setting up Standard DHCP and Proxy DHCP Services on the Same Server

When you have standard DHCP and Proxy DHCP services on the same server, do the following according to the server’s platform:

- [“Linux DHCP Server” on page 653](#)
- [“NetWare 6.x DHCP Server” on page 653](#)
- [“Windows 2000 Advanced Server” on page 654](#)

Linux DHCP Server

For the case where you have Preboot Services and DHCP running on separate servers, no network configuration is required.

For the case where you have Preboot Services and DHCP are running on the same server, option tag 60 must be set on the DHCP server. Do the following to set up standard DHCP and Proxy DHCP on the same server:

- 1 Stop the DHCP services on the Linux imaging server.
- 2 On this server, open the `dhcp.conf` file in an editor.
- 3 Insert the following line in the file:

```
option vendor-class-identifier "PXEClient";
```
- 4 Save the file.
- 5 Restart the DHCP service.

NetWare 6.x DHCP Server

Use the following steps to set up standard DHCP and Proxy DHCP Services on the same NetWare 6.x DHCP server.

IMPORTANT: Installing and running the Proxy DHCP server on a NetWare 5.x server that is already running a standard DHCP server is not supported because the DHCP protocol on NetWare 5.1 does not deliver option 60.

If you are running a NetWare 5.1 server but have upgraded the DHCP service to NetWare 6.x, follow [Step 1 on page 653](#) through [Step 6 on page 653](#). If you are running a NetWare 6.x server, begin at [Step 7 on page 653](#).

- 1 Install the DNS-DHCP client from NetWare 6.x.
- 2 Copy `dhcprsvr.nlm`, `dnipinst.nlm`, and `nddprefs.dat` from the `sys:\system` directory on the server to a backup location.
- 3 Copy `dhcprsvr.nlm`, `dnipinst.nlm`, and `nddprefs.dat` from the `sys\system` directory on the NetWare 6.x CD to the `sys\system` directory on the server.
- 4 Using the DNS-DHCP console, export the DNS and DHCP records.
Note the Novell eDirectory™ locations of the DNS-DHCP locator and group objects and the DNS zone objects.
- 5 At the system console, enter `load DNIPINST -R` to remove DNS-DHCP and related schema extensions.
- 6 At the system console, enter `load DNIPINST` to install the updated DNS-DHCP and schema extensions.
- 7 Using the DNS-DHCP console, import the DNS and DHCP records.
- 8 Using the DNS-DHCP console, click *Global Preferences* on the toolbar, then click the *Global DHCP Options* tab.
or
Using the DNS-DHCP console, click the subnet in the left panel, then click the *Other DHCP Options* tab.

- 9 Click *Modify*.
- 10 Select *Option 60* under *Available DHCP Options*, then click *Add*.
- 11 Type `PXEClient` in the *Vendor Class Identifier* text box, then click *OK* twice.
- 12 If this server is also a DNS server, enter `load NAMED` at the system console.
- 13 At the system console, enter `load DHCP SRVR`.
- 14 Using a text editor, make the following changes to `sys\system\pdhcp.ini`:
Set `USE_DHCP_Port` to 0.
Make sure `USE_BINL_PORT` is set to 1.
- 15 Unload and reload `pdhcp.nlm`.

Windows 2000 Advanced Server

Use the following steps to set up standard DHCP and Proxy DHCP Services on the same Windows 2000 Advanced Server:

- 1 At the command prompt, enter `netsh`.
- 2 At the netsh prompt, enter `dhcp server`.
- 3 At the dhcp server prompt, enter the following:
`add optiondef 60 ClassID STRING 0 PXEClient`
- 4 Add the definition type in the DHCP setup menus.

56.4 Deploying Desktop Management Preboot Services in a Network Environment

To implement the network deployment strategies outlined in this section, you must have a solid understanding of the TCP/IP network protocol and specific knowledge of TCP/IP routing and the DHCP discovery process.

Deploying Desktop Management Preboot Services (PXE) in a single segment is a relatively simple process that only requires configuring the ZENworks Imaging server. However, Preboot Services deployment in a routed environment is far more complex and might require configuration of both the ZENworks Imaging server and the network switches and routers that lie between the server and the PXE workstations.

Configuring the routers or switches to correctly forward Preboot Services network traffic requires a solid understanding of the DHCP protocol, DHCP relay agents, and IP forwarding. The actual configuration of the switch or router needs to be carried out by a person with detailed knowledge of the hardware.

We strongly recommend that you initially set up Preboot Services in a single segment to ensure that the servers are configured correctly and are operational.

This section includes the following information:

- [Section 56.4.1, “Server Configurations,” on page 655](#)
- [Section 56.4.2, “Network Configuration,” on page 657](#)
- [Section 56.4.3, “Configuring Filters on Switches and Routers,” on page 667](#)

- [Section 56.4.4, “Spanning Tree Protocol in Switched Environments,” on page 667](#)

56.4.1 Server Configurations

Server configurations depend on the server’s platform:

- [“Linux Server Configuration” on page 655](#)
- [“NetWare or Windows Server Configuration” on page 656](#)

Linux Server Configuration

There are three important points about configuring servers for Preboot Services:

- **DHCP server:** The Preboot Services environment requires a standard DHCP server. It is up to you to install your standard DHCP server.
- **Preboot Services daemons and Library File:** The three Preboot Services daemons (`novell-tftp`, `novell-proxydhcp`, and `novell-zmgprebootpolicy`) and the `libzmgserve.so` library file are all installed on the ZENworks Imaging server when you install ZENworks Desktop Management. These daemons must run together on the same server.
- **Imaging server:** The Preboot Services daemons can be installed and run on the same or different server than DHCP.

The following sections give general information about these services:

- [“The DHCP Server” on page 655](#)
- [“The libzmgserve.so Library File” on page 655](#)
- [“The novell-proxydhcp daemon” on page 656](#)
- [“The novell-tftp daemon” on page 656](#)
- [“The novell-zmgprebootpolicy daemon” on page 656](#)

It is seldom necessary to make changes to the default configuration of these services. However, if you need more detailed configuration information, see [Section 56.6.1, “Configuring Preboot Services Servers in Linux,” on page 670](#).

The DHCP Server

The standard DHCP server must be configured with an active scope to allocate IP addresses to the PXE devices. The scope options should also specify the gateway or router that the PXE devices should use.

If Preboot Services (specifically `novell-proxydhcp`) is installed on the same server as the DHCP server, then the DHCP server must be configured with a special option tag. For more information, see [“WAN/VLAN Environment” on page 660](#).

The libzmgserve.so Library File

The `libzmgserve.so` library file is used by eDirectory to provide imaging services to the devices.

This includes sending and receiving image files, discovering assigned imaging tasks from eDirectory, acting as session master for multicast imaging, and so on.

The novell-proxydhcp daemon

The Preboot Services Proxy DHCP server runs alongside a standard DHCP server to inform PXE devices of the IP address of the TFTP server, the IP address of the server where novell-zmgprebootpolicy is running, and the name of the network bootstrap program (`nvlmbp.sys`).

The novell-tftp daemon

The Preboot Services novell-tftp daemon is used by PXE devices to request files that are needed to perform imaging tasks. The TFTP server also provides a central repository for these files.

A PXE device uses one of these servers to download the network bootstrap program (`nvlmbp.sys`).

The novell-zmgprebootpolicy daemon

PXE devices use novell-zmgprebootpolicy to check if there are any imaging actions that need to be performed on the device. It forwards requests to eDirectory (the `libzmgserver.so` library file) on behalf of PXE devices.

NetWare or Windows Server Configuration

The Preboot Services environment requires a standard DHCP server, Proxy DHCP server, TFTP or MTFTP boot server, and a Transaction server to function correctly. With the exception of the standard DHCP server, these are installed when you install Desktop Management Preboot Services.

The following sections give general information about these services:

- [“DHCP Server” on page 656](#)
- [“Proxy DHCP Server” on page 657](#)
- [“TFTP and MTFTP Servers” on page 657](#)
- [“Transaction Server” on page 657](#)

It is seldom necessary to make changes to the default configuration of these services. However, if you need more detailed configuration information, see [“Configuring Preboot Services Servers in Windows” on page 673](#) or [“Configuring Preboot Services Servers in NetWare” on page 671](#).

DHCP Server

The standard DHCP server must be configured with an active scope that allocates IP addresses to the PXE workstations. The scope options should also specify the gateway or router that the PXE workstations should use.

If Preboot Services (specifically the Proxy DHCP server) is installed on the same server as the DHCP server, then the DHCP server must be configured with a special option tag. For more information, see [“Windows 2000 Advanced Server” on page 654](#) and [“NetWare 6.x DHCP Server” on page 653](#).

IMPORTANT: Installing and running the Proxy DHCP server on a NetWare 5.x server that is already running a standard DHCP server is not supported; you can, however, upgrade the DHCP server.

Proxy DHCP Server

The Preboot Services Proxy DHCP server runs alongside a standard DHCP server to inform PXE clients of the IP address of the TFTP server, MTFTP server, and Transaction server. The Proxy DHCP server also responds to PXE clients to indicate which boot server (TFTP or MTFTP) to use.

It is seldom necessary to make any changes to the default configuration.

If you don't want to run the Proxy DHCP server on the same server as the Transaction server or TFTP server, you can change the Proxy DHCP settings to direct PXE workstations to a different server.

IMPORTANT: Installing and running the Proxy DHCP server on a NetWare 5.x server that is already running a standard DHCP server is not supported.

TFTP and MTFTP Servers

The Preboot Services TFTP and MTFTP servers are used by the Preboot Services client to request files that are needed to perform imaging tasks. The TFTP server also provides a central repository for these files.

A PXE client uses one of these servers to download the Preboot Services client.

By default, TFTP is used because it speeds the workstation's boot process; however, you can change the configuration to use MTFTP. For more information, see [“Configuring Preboot Services Servers in Windows” on page 673](#) or [“Configuring Preboot Services Servers in NetWare” on page 671](#).

Transaction Server

The Preboot Services client connects to the Transaction server to check if there are any imaging actions that need to be performed on the workstation.

It is seldom necessary to make any changes to the default configuration.

You can change the UDP port that the Transaction server uses for communicating with the Preboot Services client (by default it is UDP Port 18753). You should do this only if the Transaction server is conflicting with another service running on the server. For more information, see [Section 56.2, “Installing and Setting Up Desktop Management Preboot Services,” on page 649](#).

56.4.2 Network Configuration

The configuration required to run Preboot Services in your network depends on your network setup. You can configure Preboot Services using any of the following network setups:

- LAN environment with Preboot Services and DHCP running on separate servers
- LAN environment with Preboot Services and DHCP running on the same server
- WAN/VLAN environment with Preboot Services and DHCP running on separate servers
- WAN/VLAN environment with Preboot Services and DHCP running on the same server

This section covers the following topics:

- “General Network Design Considerations” on page 658
- “LAN Environment” on page 658
- “WAN/VLAN Environment” on page 660
- “Configuring a WAN/VLAN With Preboot Services and DHCP Running on the Same Server” on page 662
- “Configuring a WAN/VLAN With Preboot Services and DHCP Running on Separate Servers” on page 665

General Network Design Considerations

Design your network so that Preboot Services clients can effectively connect to the Transaction server as well as to the TFTP or MTFTP servers. Make sure you consider the number of Preboot Services clients to be installed on the network and the bandwidth available to service these clients. To understand how the clients and servers need to interact during the Preboot Services process, see “Illustrating the Preboot Services Processes for NetWare and Windows Imaging Servers” on page 646.

TFTP servers should be installed so that Preboot Services clients have access to a TFTP server within their LAN. The bulk of network traffic generated by Preboot Services is between the Preboot Services clients and the TFTP server. A good design ensures that a client does not need to connect to its TFTP server through a slow WAN link.

Although you can have any number of imaging servers, generally only one Proxy DHCP server should be enabled per DHCP server scope.

LAN Environment

The following sections provide information about setting up Preboot Services in a LAN environment:

- “LAN Environment With Preboot Services and DHCP Running on Separate Servers” on page 658
- “LAN Environment With Preboot Services and DHCP Running on the Same Server” on page 659
- “Configuring LAN Environments for Preboot Services” on page 659

LAN Environment With Preboot Services and DHCP Running on Separate Servers

Table 56-6 *DHCP Running on Separate Servers in LAN Environment*

Information	Details for This Setup
Scope	Only PXE workstations in the LAN connect to the Preboot Services server.
Example of Usage	A small school workstation lab that is using Imaging to prepare the workstations between classes.

Information	Details for This Setup
Advantages	<ul style="list-style-type: none"> • Easiest installation and setup. • No network configuration is required. • No DHCP server configuration is required.
Disadvantages	Limited use, because a single-LAN environment only exists in small lab-type networks.

LAN Environment With Preboot Services and DHCP Running on the Same Server

Table 56-7 *DHCP Running on the Same Server in LAN Environment*

Information	Details for This Setup
Scope	Only PXE workstations in the LAN connect to the Preboot Services server.
Example of Usage	A small school workstation lab with only one server that is using Imaging to prepare the workstations between classes.
Configuration Required	<p>Because Preboot Services and DHCP are running on the same server, option tag 60 is set on the DHCP server.</p> <p>For information on setting this tag, see “Windows 2000 Advanced Server” on page 654 and “NetWare 6.x DHCP Server” on page 653.</p>
Advantages	<ul style="list-style-type: none"> • Easy installation and setup. • No network configuration is required.
Disadvantages	<ul style="list-style-type: none"> • DHCP server configuration is required (option tag 60). • Limited use, because a single-LAN environment only exists in small lab-type networks.

Configuring LAN Environments for Preboot Services

If you have Preboot Services and DHCP running on separate servers, no network configuration is required.

If you have Preboot Services and DHCP running on the same server, option tag 60 must be set on the DHCP server. Do the following to set up standard DHCP and Proxy DHCP on the same server:

- 1 Stop the DHCP services on the Linux imaging server.
- 2 On this server, open the `dhcp.conf` file in an editor.
- 3 Insert the following line in the file:

```
option vendor-class-identifier "PXEClient";
```
- 4 Save the file.
- 5 Restart the DHCP service.

WAN/VLAN Environment

In a WAN, the PXE workstation is usually separated from the Proxy DHCP and DHCP servers by one or more routers. The PXE workstation broadcasts for DHCP information, but by default the router does not forward the broadcast to the servers, causing the Preboot Services session to fail.

In a VLAN (Virtual LAN) environment, the PXE workstation is logically separated from the Proxy DHCP server and the DHCP server by a switch. At the IP level, this configuration looks very similar to a traditional WAN (routed) environment.

In a typical VLAN environment, the network is divided into a number of subnets by configuring virtual LANs on the switch. Workstations in each virtual LAN usually obtain their IP address information from a central DHCP server. In order for this system to work, it is necessary to have Bootp or IP helpers configured on each gateway. These helpers forward DHCP requests from workstations in each subnet to the DHCP server, allowing the DHCP server to respond to workstations in that subnet.

The following sections provide information about setting up Preboot Services in a WAN/VLAN environment:

- “WAN or VLAN Environment With Preboot Services and DHCP Running on Separate Servers” on page 660
- “WAN or VLAN Environment With Preboot Services and DHCP Running on the Same Server” on page 661

WAN or VLAN Environment With Preboot Services and DHCP Running on Separate Servers

Table 56-8 *DHCP Running on Separate Servers in WAN/VLAN Environment*

Information	Details for This Setup
Scope	PXE workstations over the entire WAN/VLAN connect to the Preboot Services server.
Example of Usage	Any corporate or mid-size network that has the network divided into multiple subnets, but is running only one DHCP server.
Configuration Required	<p>A DHCP relay agent or IP helper is configured on the router or switch serving the subnet that the PXE workstation belongs to. The helper is configured to forward all DHCP broadcasts that are detected in the subnet to the DHCP and Proxy DHCP servers.</p> <p>This normally requires two helpers to be configured: the first to forward DHCP broadcasts to the DHCP server, and the second to forward the DHCP broadcasts to the Proxy DHCP server.</p>

Information	Details for This Setup
Advantages	<ul style="list-style-type: none"> • Common network setup. • Multiple Preboot Services servers can be installed so that each server provides service only for certain subnets. If multiple Preboot Services are installed, the Proxy DHCP server must be configured so it supplies the IP address of the central Transaction server. <p>With this solution, the PXE workstation receives a response from a Proxy DHCP server located on its subnet, but the workstation is redirected to a single central Transaction server to check for imaging work to do.</p> <p>For information about changing the Proxy DHCP configuration, see Section 56.2, “Installing and Setting Up Desktop Management Preboot Services,” on page 649.</p>
Disadvantages	The network equipment (routers/switches) must be configured with additional IP helpers. Some network equipment might not function properly when more than one additional IP helper is configured.
Detailed Setup Information	“Configuring a WAN/VLAN With Preboot Services and DHCP Running on Separate Servers” on page 665

IMPORTANT: For Linux imaging servers only, if the switch is acting as a firewall and limiting the type of traffic on the network, understand that the novell-tftp and novell-zmgprebootpolicy daemons are not firewall or network filter friendly. You should not attempt to run these daemons through a firewall. If users need to pass preboot work through a firewall, then all Preboot Services work needs to be on the outside and merely reference a Web service inside the firewall.

WAN or VLAN Environment With Preboot Services and DHCP Running on the Same Server

Table 56-9 DHCP Running on the Same Server in WAN/VLAN Environment

Information	Details for This Setup
Scope	PXE workstations over the entire WAN/VLAN connect to the Preboot Services server.
Example of Usage	Any corporate or mid-size network that has the network divided into multiple subnets, but is running only one DHCP server.
Configuration Required	<ul style="list-style-type: none"> • The routers or switches have been configured with IP helpers to forward network traffic to the DHCP server. • Because Preboot Services and DHCP are running on the same server, option tag 60 is set on the DHCP server. <p>For information on setting this tag, see “Windows 2000 Advanced Server” on page 654 and “NetWare 6.x DHCP Server” on page 653.</p>
Advantages	No network equipment (routers/switches) needs to be configured to forward network traffic to the Proxy DHCP server.

Information	Details for This Setup
Disadvantages	<ul style="list-style-type: none"> • DHCP server configuration required (option tag 60). • Only one Preboot Services server can be installed because it needs to run on the same server as the DHCP server (and there is usually only one DHCP server).
Detailed Setup Information	“Configuring a WAN/VLAN With Preboot Services and DHCP Running on the Same Server” on page 662

IMPORTANT: For Linux imaging servers only, if the switch is acting as a firewall and limiting the type of traffic on the network, understand that the novell-tftp and novell-zmgprebootpolicy daemons are not firewall or network filter friendly. You should not attempt to run these daemons through a firewall. If users need to pass preboot work through a firewall, then all Preboot Services work needs to be on the outside and merely reference a Web service inside the firewall.

Configuring a WAN/VLAN With Preboot Services and DHCP Running on the Same Server

If the switch is acting as a firewall and limiting the type of traffic on the network, it might be necessary to open certain UDP ports in the firewall. For a list of UDP ports used by Desktop Management Preboot Services, see [“Configuring Filters on Switches and Routers” on page 667](#).

This section includes the following topics:

- [“Implementation” on page 662](#)
- [“Installing the Proxy DHCP Server and the TFTP Server on the DHCP Server” on page 663](#)

Implementation

The Desktop Management installation provides for a complete installation of the Preboot Services and Imaging components. If you want to install all of Imaging and Preboot Services on the DHCP server, then run the standard installation on the server.

However, you might want to run the Preboot Services components (Proxy DHCP and TFTP services) on the DHCP server and the Imaging and Transaction Server components on another server.

If you want to configure the system like this, you need to do so manually by following the steps below.

- 1 Install Desktop Management Preboot Services on a server.
- 2 Test to make sure that the server is set up correctly.
 - 2a Connect the server to a LAN with a PXE workstation in the same LAN.
 - 2b Assign imaging work to the workstation through a server or workstation policy in Novell ConsoleOne®.
 - 2c Boot the workstation.
 - 2d Verify that it picks up the imaging work correctly.

3 Stop the Desktop Management Proxy DHCP service on the server.

For Windows, go to the Services panel and stop the Proxy DHCP Service. Set the service to *Disabled* so that it does not start the next time the server is started.

For NetWare, enter `unload pdhcp` at the server console to unload the Proxy DHCP service. Edit the `zfdstart.ncf` file and comment out the line that loads the Proxy DHCP service to prevent it from loading the next time the server is started.

4 If the Proxy DHCP service was running on the same server that was running DHCP, delete option tag 60 from the DHCP server that you added during the installation.

5 Install the Proxy DHCP service and TFTP service on the server that is running DHCP services.

For instructions on how to do this, see [“Installing the Proxy DHCP Server and the TFTP Server on the DHCP Server” on page 663](#).

6 Configure option tag 60 on the DHCP server and set the tag to the text string “PXEClient.”

For instructions on how to do this, see [“Windows 2000 Advanced Server” on page 654](#) and [“NetWare 6.x DHCP Server” on page 653](#).

7 Configure the Proxy DHCP service to redirect PXE workstations to the Preboot Services server that you set up in [Step 1](#).

For Windows, run the Proxy DHCP service configuration application and set the *VSP IP* to the IP address of the server that you set up in [Step 1](#).

For NetWare, open `pdhcp.ini` and change the `TRANSACTION_SERVER_IP` entry to the IP address of the server that you set up in [Step 1](#).

8 Start the Proxy DHCP service that has just been installed on the server running DHCP services.

For Windows, start the service in the Service Control Manager.

For NetWare, enter `load pdhcp` at the server console.

PXE workstations in all VLANs that are supported by the DHCP server are able to pick up work through PXE.

Installing the Proxy DHCP Server and the TFTP Server on the DHCP Server

This section includes the following topics:

- Installing and Configuring Proxy DHCP and TFTP Servers on a NetWare Server
- Installing and Configuring Proxy DHCP and TFTP Servers on a Windows Server

Installing and Configuring Proxy DHCP and TFTP Servers on a NetWare Server

1 Copy the following files to `sys:\system` on the destination server. These files can be obtained either from your working ZENworks Imaging server, or from the *ZENworks Desktop Management Program CD*.

```
pdhcp.nlm  
pdhcp.ini  
tftp.nlm  
tftp.ini
```

2 Copy all of the files from the `sys:\tftp` directory to a directory with the same name on the destination server.

- 3 Edit the `tftp.ini` file. Make sure that the `ReadPath` is the same as the path where you copied the TFTP files in [Step 2](#).
- 4 If you want the services to start automatically, edit the `autoexec.ncf` file and add the following lines:


```
Load tftp
Load pdhcp
```
- 5 Start the services on the server by entering the following lines at the server console:


```
Load tftp
Load pdhcp
```

Installing and Configuring Proxy DHCP and TFTP Servers on a Windows Server

- 1 Stop all Desktop Management Preboot Services on the server where you installed Preboot Services.

To do this, open the Service Control Manager (*Control Panel > Administrative Tools > Services*), and stop the Preboot Transaction Server, Preboot Port Mapper, Proxy DHCP Service, and Preboot TFTP/MTFTP Service.
- 2 Copy the entire subdirectory where you installed Desktop Management Preboot Services to the destination server. Typically, this subdirectory is `\program files\zen_preboot_services`.
- 3 Using the Service Control Manager, restart the services on the original server that you stopped in [Step 1](#).
- 4 On the destination server, perform the following steps. You need to be logged in to the server with administrator rights.

This example assumes you copied all of the files to `c:\program files\zen_preboot_services`.

 - 4a Click *Start > Run*.
 - 4b Type `cmd`, then press Enter to open a command console.
 - 4c Type `cd c:\program files\zen_preboot_services\pdhcp`, then press Enter.
 - 4d Type `dhcbservice -i`, then press Enter.
 - 4e Type `dhcpcfg`, then press Enter.

This starts the Proxy DHCP configuration application.
 - 4f Set the *VSP Host IP* to the IP address of the ZENworks Imaging server, click *Save All*, then click *Exit*.
 - 4g Switch back to the command console.
 - 4h Type `cd c:\program files\zen_preboot_services\tftp`, then press Enter.
 - 4i Type `tftp-service -I`, then press Enter.
 - 4j Type `tftpcfg`, then press Enter.

The TFTP configuration applet starts. Make sure the TFTP Read Path is correct, and points to a subdirectory containing the TFTP files (`dinic.sys`, `boot.dnx`, `bootzen2.bin`, `bootzen5.bin`), as well as other files.

4k Click *Exit* to close the application.

5 Open the Service Control Manager, then start the Proxy DHCP and TFTP services that are now listed there.

or

Reboot the server and the services start automatically.

Configuring a WAN/VLAN With Preboot Services and DHCP Running on Separate Servers

If the switch is acting as a firewall and limiting the type of traffic on the network, it might be necessary to open certain UDP ports in the firewall. For a list of UDP ports used by ZENworks Desktop Management Preboot Services, see [“Configuring Filters on Switches and Routers” on page 667](#).

An **example deployment** is given below of a WAN/VLAN environment with Preboot Services and DHCP running on the same server. The subsequent sections provide the specific steps required to configure network equipment so that it correctly forwards Preboot Services network traffic.

- [“Example Deployment” on page 665](#)
- [“Configuring Cisco Equipment” on page 665](#)
- [“Configuring Nortel Network Equipment” on page 666](#)
- [“Configuring Bay Network Equipment” on page 666](#)

Example Deployment

In this example, three VLANs are configured on a Bay Networks Accel 1200 switch running firmware version 2.0.1. One VLAN hosts the Proxy DHCP server, the second VLAN hosts the DHCP server, and the third VLAN hosts the PXE client. The PXE client’s DHCP broadcast is forwarded by the switch to both the Proxy DHCP server and the DHCP server. The response from both servers is then routed correctly back to the PXE client, and the PXE client starts the Preboot Services session correctly.

The three VLANs are all 24-bit networks; their subnet mask is 255.255.255.0.

The first VLAN gateway is 10.0.0.1. This VLAN hosts the PXE client that is allocated an IP in the range of 10.0.0.2 to 10.0.0.128. This VLAN is named VLAN1.

The second VLAN gateway is 10.1.1.1. This VLAN hosts the DHCP server with IP 10.1.1.2. This VLAN is named VLAN2.

The third VLAN gateway is 196.10.229.1. This VLAN hosts the server running the Proxy DHCP server and the Transaction server. The server’s IP is 196.10.229.2. This VLAN is named VLAN3.

Routing is enabled between all VLANs. Each VLAN must be in its own spanning tree group.

Configuring Cisco Equipment

- 1** Go to Global Configuration mode.
- 2** Type `ip forward-protocol udp 67`, then press Enter.
- 3** Type `ip forward-protocol udp 68`, then press Enter.
- 4** Go to the LAN interface that serves the PXE workstation.

- 5 Type `ip helper-address 10.1.1.2`, then press Enter.
- 6 Type `ip helper-address 196.10.229.2`, then press Enter.
- 7 Save the configuration.

Configuring Nortel Network Equipment

- 1 Connect to the router with Site Manager.
- 2 Make sure that IP is routable.
- 3 Enable *Bootp* on the PXE workstation subnet or VLAN.
- 4 Select the interface that the PXE workstations are connected to.
- 5 Edit the circuit.
- 6 Click *Protocols*.
- 7 Click *Add/Delete*.
- 8 Make sure that the *Bootp* check box is selected.
- 9 Click *OK*.
- 10 Click *Protocols > IP > Bootp > Relay Agent Interface Table*.
The interface where Bootp was enabled is visible in the list.
- 11 Click *Preferred Server*.
- 12 Change the *Pass Through Mode* value to *Bootp* and *DHCP*.
- 13 Set up the relay agents:
 - 13a Click *Add*.
 - 13b In the Relay Agent IP Address box, enter the local LAN IP address.
 - 13c In the Target Server IP Address box, enter the DHCP server IP address.
 - 13d Click *OK*.
 - 13e Change the *Pass Through Mode* value to *Bootp* and *DHCP*.
 - 13f Perform **Step 1 to Step 5 on page 666** again and enter the Proxy DHCP server IP address at **Step 3 on page 666**.
 - 13g Apply the configuration.

Configuring Bay Network Equipment

Perform the following steps on the switch:

- 1 Enable DHCP for the client VLAN using the following command lines:

```
# config vlan1 ip
# dhcp enable
```
- 2 Configure IP helpers to forward DHCP requests from the workstation subnet to the Proxy DHCP server, using the following command lines:

```
# config ip dhcp-relay
# create 10.0.0.1 10.1.1.2 mode dhcp state enable
# create 10.0.0.1 196.10.229.2 mode dhcp state enable
```

The create command has the form:

```
create agent server mode dhcp state enable
```

where *agent* is the IP address of the gateway that serves the PXE workstation, and *server* is the IP address of the server that the DHCP frame should be forwarded to.

- 3 Save the configuration.

56.4.3 Configuring Filters on Switches and Routers

Some network devices filter network traffic that passes through them. Preboot Services makes use of several different types of traffic, and all of these must be able to pass through the router or switch successfully for the Preboot Services session to be successful. The Preboot Services session uses the following destination ports:

Table 56-10 Ports Used by Preboot Services Components

Component	Port
DHCP and Proxy DHCP Servers	UDP Port 67, 68, and 4011
TFTP Server	UDP Port 69
RPC Port Map Server	UDP Port 111
Transaction Server	UDP Port 18753

56.4.4 Spanning Tree Protocol in Switched Environments

Spanning tree protocol (STP) is available on certain switches and is designed to detect loops in the network. When a device (typically a network hub or a workstation) is patched into a port on the switch, the switch indicates to the device that the link is active, but instead of forwarding frames from the port to the rest of the network, the switch checks each frame for loops and then drops it. The switch can remain in this listening state from 15 to 45 seconds.

The effect of this is to cause the DHCP requests issued by PXE to be dropped by the switch, causing the Preboot Services session to fail.

It is normally possible to see that the STP is in progress by looking at the link light on the switch. When the workstation is off, the link light on the switch is obviously off. When the workstation is turned on, the link light changes to amber, and after a period of time changes to a normal green indicator. As long as the link light is amber, STP is in progress.

This problem only affects PXE or Preboot Services clients that are patched directly into an Ethernet switch. To correct this problem, perform one of the following:

- Turn off STP on the switch entirely.
- Set *STP to Port Fast* for every port on the network switch where a PXE workstation is attached.

After the problem is resolved, the link light on the port should change to green almost immediately after a workstation connected to that port is turned on.

Information about STP and its influence on DHCP can be found at [Using PortFast and Other Commands to Fix End-Station Startup Connectivity Problems \(http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1923.htm#xtocid897350\)](http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1923.htm#xtocid897350).

56.5 Enabling PXE on a Workstation

To image a workstation using Preboot Services, you need to find out if the workstation is PXE capable, and then make sure that PXE is enabled.

PXE code is typically delivered with newer workstations (PC 99 compliant or later) on the NIC.

- [Section 56.5.1, “Enabling PXE on a PXE-Capable Workstation,” on page 668](#)
- [Section 56.5.2, “Verifying That PXE Is Enabled on a Workstation,” on page 669](#)
- [Section 56.5.3, “If a Workstation Is Not PXE Capable,” on page 669](#)

56.5.1 Enabling PXE on a PXE-Capable Workstation

When PXE is enabled, it can lengthen the time of the boot process slightly, so most NICs have PXE turned off by default. To enable PXE on a PXE-capable workstation:

- 1 Access the computer system BIOS and look at the *Boot Sequence* options.

The PXE activation method for a workstation varies from one manufacturer to another, but generally one of the following methods is used:

- Some BIOSs have a separate entry in the BIOS configuration to enable or disable the PXE functionality. In this case, set either the *PXE Boot* setting or the *Network Boot* setting to *Enabled*.
- Some BIOSs extend the entry that allows you to configure boot order. For example, you can specify that the system should try to boot from a diskette before trying to boot from the hard drive. In this case, set the system to try *Network Boot* before trying to boot from a diskette or from the hard disk.

- 2 If PXE is not listed in the *Boot Sequence* options and if the NIC is embedded in the motherboard, look at the Integrated Devices section of the BIOS, which might have an option to enable PXE. PXE might be called by another name, such as MBA (Managed Boot Agent) or Pre-Boot Service.

After enabling PXE in the Integrated Devices section, look at the *Boot Sequence* options and move PXE so that it is first in the Boot Sequence.

- 3 Save any changes you have made and exit the system BIOS.
- 4 Reboot the workstation.

If the workstation does not have the network adapter and PXE integrated into the motherboard, it uses the installed NIC management software to prompt you to start PXE configuration during the boot process.

For example, many network adapters that are PXE aware prompt you to press Ctrl+S during the boot process to allow you to configure the PXE functionality. Other network adapters might prompt you to press Ctrl+Alt+B or another key combination to configure PXE.

If the computer system does not have an integrated NIC, you might need to use NIC management software to configure your NIC to support PXE. Refer to your NIC documentation for support of PXE.

56.5.2 Verifying That PXE Is Enabled on a Workstation

After you have activated PXE, it becomes available in the Boot section of the BIOS. PXE is correctly enabled on a workstation when the workstation attempts to establish a PXE session during the boot process. You can see this happening when the workstation pauses during the boot process and displays the following on the screen:

```
CLIENT MAC ADDR: 00 E0 29 47 59 64
```

```
DHCP...
```

The actual message displayed varies from one manufacturer to another, but you can identify it by the obvious pause in the boot process as the workstation searches for DHCP.

56.5.3 If a Workstation Is Not PXE Capable

Some older workstations might not support PXE and require you to install PXE on them. There are several ways to do this:

- Update your NIC or NIC driver. Most network adapter manufacturers supply a PXE Boot ROM chip that you can fit into your network adapter to enable PXE on the workstation. Contact the NIC manufacturer or a supplier to see if they sell a PXE Boot ROM. It is also possible that your current NIC might need an upgraded driver to become PXE-enabled.
- Update your BIOS version. Most manufacturers that supply motherboards with the network adapter embedded in the motherboard offer a BIOS upgrade that enables PXE on the workstation. Check the manufacturer's Web site or contact a supplier to check for a BIOS upgrade.
- Use the Desktop Management Preboot Services PXE-on-Disk utility if no PXE is available for the workstation. With this utility, you can create a boot diskette that enables the workstation to participate in the PXE environment.

The PXE-on-Disk utility is installed to the ZENworks Imaging server as part of Preboot Services (PXE Support) in Desktop Management and is available from the *Create PXE Disk* button in the Imaging Boot Disk Creator (in ConsoleOne, click *Tools > ZENworks Utilities > Imaging > Create or Modify Boot Diskette*).

For more information about using PXE-on-Disk, see [Section 56.7, "Using the Desktop Management Preboot Services PXE-on-Disk Utility,"](#) on page 677.

56.6 Administering Desktop Management Preboot Services

This section includes information about administering and configuring Desktop Management Preboot Services.

It includes the following topics:

- [Section 56.6.1, “Configuring Preboot Services Servers in Linux,” on page 670](#)
- [Section 56.6.2, “Configuring Preboot Services Servers in NetWare,” on page 671](#)
- [Section 56.6.3, “Configuring Preboot Services Servers in Windows,” on page 673](#)
- [Section 56.6.4, “Configuring IP Port Usage,” on page 676](#)

56.6.1 Configuring Preboot Services Servers in Linux

In Preboot Services, the daemons do not use switches. Instead, to configure a daemon to do something that is not a default, you need to edit the configuration files.

You can edit configuration files while the daemon is running, because the files are only read when the daemon starts. Therefore, after editing the file you must restart the daemon for the changes to take effect.

For more information on the daemon configuration files, see [Section 63.7.1, “Initiating the Imaging Processes on Linux Imaging Servers,” on page 762](#).

The following sections explain how to configure the following ZENworks Imaging server components:

- [“Configuring the TFTP Server” on page 670](#)
- [“Configuring the Proxy DHCP Server” on page 671](#)
- [“Configuring Novell-zmgprebootpolicy” on page 671](#)
- [“Configuring the DHCP Server” on page 671](#)

The `libzmgserver.so` library file cannot be configured.

Configuring the TFTP Server

It is seldom necessary to change the default TFTP server configuration values. If you need to change them, use the following procedure:

- 1 Open the following file in an editor:

```
/etc/opt/novell/novell-tftp.conf
```

- 2 Edit the configuration settings per instructions within the file.
- 3 Save the changes.
- 4 In a shell console, enter the following command:

```
/etc/init.d/novell-tftp restart
```

Configuring the Proxy DHCP Server

The Proxy DHCP server provides PXE devices with the information that they require to be able to connect to the Preboot Services system.

Use the following steps to modify the settings of novell-proxydhcp:

- 1 Open the following file in an editor:

```
/etc/opt/novell/novell-proxydhcp.conf
```

- 2 Edit the configuration settings per instructions within the file.

- 3 Save the changes.

- 4 In a shell console, enter the following command:

```
/etc/init.d/novell-proxydhcp restart
```

You can set any of the IP address fields in the configuration utility to 0.0.0.0. The server replaces these entries with the IP address of the first network adapter installed in the server.

Configuring Novell-zmgprebootpolicy

The novell-zmgprebootpolicy daemon is used to check if there are any imaging actions that need to be performed on the device. It forwards requests to eDirectory (the libzmgserv.so library file) on behalf of PXE devices.

Use the following steps to modify the settings of novell-zmgprebootpolicy:

- 1 Open the following file in an editor:

```
/etc/opt/novell/zenworks/preboot/novell-zmgprebootpolicy.conf
```

- 2 Edit the configuration settings per instructions within the file.

- 3 Save the changes.

- 4 In a shell console, enter the following command:

```
/etc/init.d/novell-zmgprebootpolicy restart
```

Configuring the DHCP Server

The DHCP server needs to have option 60 (decimal) added to the DHCP tags if the Proxy DHCP and DHCP servers are running on the same physical server. This option should be a string type and must contain the letters PXEClient.

For more information, see [“Network Configuration” on page 657](#).

56.6.2 Configuring Preboot Services Servers in NetWare

After Desktop Management Preboot Services is installed, it is seldom necessary to change the default server values. If you need to change the settings, however, you can do so by editing the appropriate .ini file for the server you want to change. These .ini files can be found on the Preboot Services server in the sys:\system directory.

This section contains the following information:

- “Configuring the MTFTP/TFTP Module” on page 672
- “Configuring the Proxy DHCP Module” on page 672
- “Configuring the Transaction Server Module” on page 673
- “Configuring the DHCP Server” on page 673

Configuring the MTFTP/TFTP Module

You can set the path that the MTFTP/TFTP module uses for file access by modifying the `tftp.ini` file. The following options are available:

ReadPath: Set the path that the MTFTP/TFTP module uses for file access. The default value for this setting is `sys:\tftp\`.

WriteProtect: Set the value to 0 to cause the MTFTP/TFTP module to accept Write requests, or set the value to 1 to disallow Write requests.

NOTE: The variable names (for example, ReadPath) are case sensitive.

Configuring the Proxy DHCP Module

You can set the parameters that the Proxy DHCP module uses by modifying the `pdhcp.ini` file. The following options are available:

TRANSACTION_SERVER_IP: The Preboot client contacts the server on this IP address to check for imaging work.

TFTP_SERVER_IP: The PXE/Preboot client contacts the server on this IP address to download the Preboot client (`dnic.sys`) and the ZENworks Imaging Engine if imaging work is required.

PDHCP_Server_IP: If this address is set, the Proxy DHCP server tries to bind to this IP address on the server. The IP address set must be a valid IP address on the server.

This setting can also be used to force the Proxy DHCP server to use the virtual LAN adapter on a cluster server, rather than the physical LAN adapter of the server.

This setting can be used to force the PDHCP server to respond on only one interface on a multi-homed server.

BOOT_MENU_TIMEOUT: This setting controls how long (in seconds) the PXE boot menu is displayed while a PXE workstation boots.

USE_DHCP_PORT: Set this to 0 to bind to the BINL port (4011). This is only necessary if you are running proxy DHCP and another DHCP Server on the same machine. This setting replaces the older `USE_BINL_PORT` setting.

USE_MTFTP: Set this option to 0 to disable multicast TFTP transfers. This is the default setting.

Set this option to 1 to enable multicast TFTP transfers. In this mode, the PXE client waits to join a multicast group for the transfer of the initial `dnic.sys` file. Enabling this option adds 10 to 20 seconds to the PXE boot-up sequence, so this is not recommended.

MTFTP_IP: This value specifies the multicast IP that the server should use for MTFTP transfers.

MTFTP_SERVER_PORT: This value specifies the server port to use for MTFTP transfers.

MTFTP_CLIENT_PORT: This value specifies the client port to use for MTFTP transfers.

MTFTP_OPEN_TIMEOUT: Sets the time to wait before opening the MTFTP session.

MTFTP_REOPEN_TIMEOUT: Sets the time to wait before reopening the MTFTP session.

NOTE: The variable names (for example, MTFTP_IP) are case sensitive.

Configuring the Transaction Server Module

You can set the parameters that the Transaction server module uses by modifying the `dtls.ini` file. The following option is available:

Server UdpPort: Set this value to the UDP port number you want to use.

NOTE: This variable name is case sensitive.

Configuring the DHCP Server

For information on running the DHCP server and Proxy DHCP server on the same NetWare 6 server, see [Section , “NetWare 6.x DHCP Server,” on page 653](#).

56.6.3 Configuring Preboot Services Servers in Windows

These sections explain how to configure the following Desktop Management Preboot Services servers:

- [“Configuring the TFTP Server” on page 673](#)
- [“Configuring the MTFTP Server” on page 674](#)
- [“Configuring the Proxy DHCP Server” on page 674](#)
- [“Configuring the DHCP Server” on page 675](#)

Configuring the TFTP Server

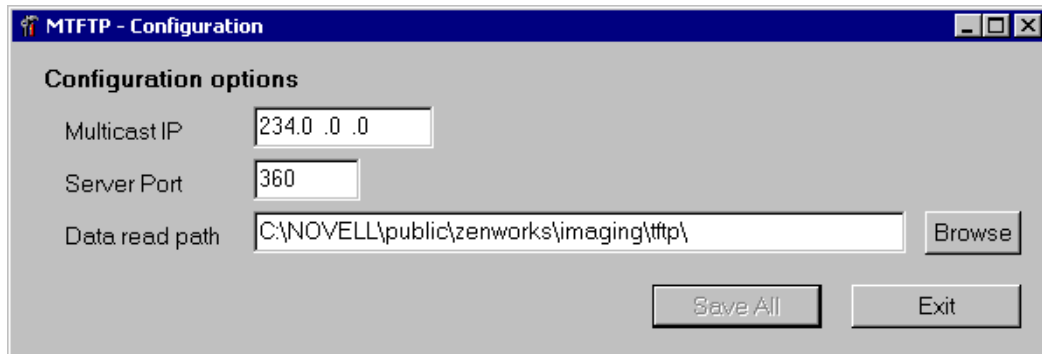
It is seldom necessary to change the default TFTP server configuration values. If you need to change them, use the following procedure:

- 1 From the Windows desktop, click *Start > Programs > ZENworks Preboot Services > ZENworks Preboot Services configuration > TFTP configuration* to display the TFTP Configuration window.
- 2 Fill in the field:
TFTP Data Path: The data path should point to a directory where the TFTP server looks for files that are requested or written to by clients.
- 3 Click *Save all* to save new settings.
or
Click *Exit* to close the configuration utility without saving changes.

Configuring the MTFTP Server

It is seldom necessary to change the default MTFTP server configuration values. If you need to change them, use the following procedure:

- 1 From the Windows desktop, click *Start > Programs > ZENworks Preboot Services > ZENworks Preboot Services configuration > MTFTP configuration* to display the MTFTP Configuration dialog box.



- 2 Fill in the fields:

Multicast IP: Specify the address to be used as a destination during multicast transfers. Make sure that the address used falls within the IP address range designated for multicast. If you change this value, be sure to update the corresponding entry in the Proxy DHCP configuration.

Server Port: Specify the port number that the server expects to receive requests on. If you change this value, be sure to update the corresponding entry in the Proxy DHCP configuration.

Data Read Path: Specify the directory where the MTFTP server reads the files that are requested by clients.

- 3 Click *Save all* to save new settings.

or

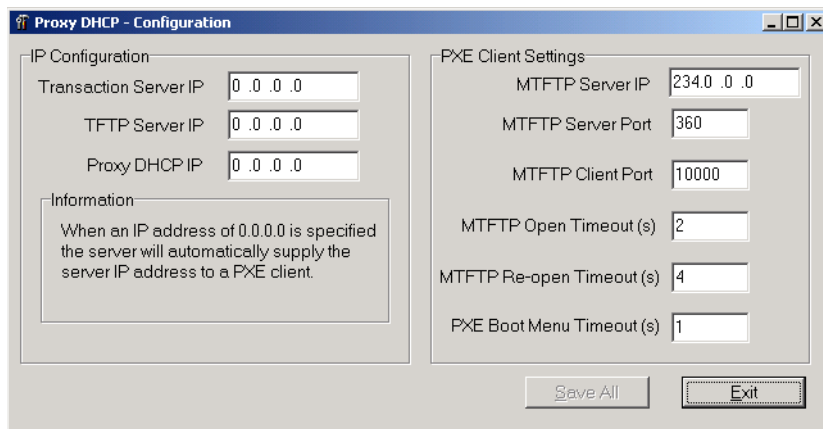
Click *Exit* to close the configuration utility without saving changes.

Configuring the Proxy DHCP Server

The Proxy DHCP server provides Preboot Services clients with the information that they require to be able to connect to the Preboot Services system.

Use the following steps to check the settings of the Proxy DHCP server:

- 1 From the Windows desktop, click *Start > Programs > ZENworks Preboot Services > ZENworks Preboot Services configuration > Proxy DHCP configuration* to display the Proxy DHCP Configuration dialog box.



The image shows the 'Proxy DHCP - Configuration' dialog box. It is divided into two main sections: 'IP Configuration' and 'PXE Client Settings'. The 'IP Configuration' section contains three text boxes for 'Transaction Server IP', 'TFTP Server IP', and 'Proxy DHCP IP', all of which are set to '0 .0 .0 .0'. Below these is an 'Information' box with text explaining that when an IP address of 0.0.0.0 is specified, the server will automatically supply the server IP address to a PXE client. The 'PXE Client Settings' section contains several text boxes: 'MTFTP Server IP' (234.0 .0 .0), 'MTFTP Server Port' (360), 'MTFTP Client Port' (10000), 'MTFTP Open Timeout (s)' (2), 'MTFTP Re-open Timeout (s)' (4), and 'PXE Boot Menu Timeout (s)' (1). At the bottom of the dialog are two buttons: 'Save All' and 'Exit'.

- 2 Check the fields:

Transaction Server IP: The Preboot client contacts the server on this IP address to check for imaging work.

TFTP Server IP: The PXE Preboot client contacts the server on this IP address to download the Preboot client (*dnic.sys*) and the ZENworks Imaging Engine if imaging work is required.

Proxy DHCP IP: If this address is set, the Proxy DHCP server tries to bind to this IP address on the server. The IP address set must be a valid IP address on the server.

This setting can be used to force the Proxy DHCP server to use the virtual LAN adapter on a cluster server, rather than the physical LAN adapter of the server.

This setting can also be used to force the PDHCP server to respond on only one interface on a multi-homed server.

All of the MTFTP settings in this dialog box should be the same as the settings that appear in the MTFTP Configuration Utility. Do not modify the MTFTP Client Port, MTFTP Open Timeout, MTFTP Reopen Timeout, and PXE Boot Menu Timeout settings from their default values.

- 3 Click *Save All* to save new settings.

or

Click *Exit* to close the configuration utility without saving changes.

You can set any of the IP address fields in the configuration utility to 0.0.0.0. The server replaces these entries with the IP address of the first network adapter installed in the server.

Configuring the DHCP Server

The DHCP server needs to have option tag 60 (decimal) added to the DHCP tags if the PDHCP and the DHCP servers are running on the same physical server. This option should be a string type and must contain the letters PXEClient.

For more information, see [“Windows 2000 Advanced Server” on page 654](#).

56.6.4 Configuring IP Port Usage

This section describes the network ports used by Desktop Management Preboot Services. Using this information in this section, you can configure routers or firewalls to correctly forward the network traffic generated by Preboot Services.

- “Available Ports” on page 676
- “Changing Port Usage in NetWare” on page 677
- “Changing Port Usage in Windows Server” on page 677

Port usage for Linux imaging servers cannot be changed. For further information about configuring routers, see [Section 56.4, “Deploying Desktop Management Preboot Services in a Network Environment,”](#) on page 654.

Available Ports

This section describes the network ports used by ZENworks Desktop Management Preboot Services. Using the information in this section, you can configure routers to correctly forward the network traffic generated by Preboot Services. For further information about configuring routers, see [Section 56.4, “Deploying Desktop Management Preboot Services in a Network Environment,”](#) on page 654.

Desktop Management Preboot Services uses both well-known and proprietary IP ports.

The well-known IP ports include:

- **67 decimal:** The Proxy DHCP server listens on this port for PXE information requests. This is the same port used by a standard DHCP server.
- **68 decimal:** The DHCP/Proxy DHCP server listens on this port for client requests.
- **69 decimal:** The TFTP server listens on this port for file requests from PXE or Preboot Services clients.
- **111 decimal:** Port mapper port. Refer to [RFC 1057 \(http://sunsite.serc.iisc.ernet.in/collection/rfc/rfc1057.html\)](http://sunsite.serc.iisc.ernet.in/collection/rfc/rfc1057.html) for a description of this server.
- **4011 decimal:** When running on the same server as the DHCP daemon, the Proxy DHCP server listens on this port for PXE information requests.

For NetWare and Windows imaging servers, the proprietary IP ports include:

- **360 decimal:** The MTFTP server listens on this port for MTFTP requests from PXE or Preboot Services clients.
- **4011 decimal:** The Proxy DHCP server uses this port to communicate with PXE clients, but only when running on the same server as the standard DHCP server.
- **18753 decimal:** Transaction server client connection port. The Transaction server receives all connection requests from the Preboot Services clients on this port.

For Linux imaging servers, the proprietary IP ports include:

- **998 decimal:** Imaging client connection port. eDirectory (`libzmgserver.so`) receives all connection requests from the Preboot Services devices on this port.
- **13331 decimal:** novell-zmgprebootpolicy client connection port. The novell-zmgprebootpolicy daemon receives all connection requests from the PXE devices on this port.

Although PXE devices make their initial requests to the `novell-tftp` and `novell-zmgprebootpolicy` daemons on the ports listed above, the remainder of the transactions can occur on any available port. For this reason, ZENworks Imaging servers cannot be separated from their clients by a firewall.

IMPORTANT: The `novell-tftp` and `novell-zmgprebootpolicy` daemons are not firewall or network filter friendly. You should not attempt to run these daemons through a firewall. If users need to pass preboot work through a firewall, then all Preboot Services work needs to be on the outside and merely reference a Web service inside the firewall.

Changing Port Usage in NetWare

- 1 Edit the `dtc.ini` file located in the same directory as the `dtc.nlm` module.
- 2 Set `ServerUdpPort` to the port number you want to use.
- 3 Stop and start `dtc.nlm` for the changes to take effect.

Changing Port Usage in Windows Server

The Transaction server and MTFTP server can be configured to use different ports if necessary. To change the port, use the following procedure:

- 1 From the Windows server desktop, click *Start > Programs > ZENworks Preboot Services > ZENworks Preboot Services configuration > preboot_service_configuration*.
- 2 Change the relevant settings in the configuration.
- 3 Stop and start the servers for the changes to take effect.

56.7 Using the Desktop Management Preboot Services PXE-on-Disk Utility

This section contains information to help you understand the ZENworks Desktop Management Preboot Services PXE-on-Disk utility, prepare a Windows workstation for it, and use it.

- [Section 56.7.1, “What Is PXE-on-Disk Setup?,” on page 677](#)
- [Section 56.7.2, “Creating a PXE-on-Disk Diskette,” on page 678](#)
- [Section 56.7.3, “Booting with a PXE-on-Disk Diskette,” on page 681](#)
- [Section 56.7.4, “If PXE-on-Disk Fails to Operate Correctly,” on page 681](#)

56.7.1 What Is PXE-on-Disk Setup?

PXE-on-Disk Setup helps you create a 1.44 MB floppy diskette that contains all of the files needed to allow a non-PXE-compatible network adapter on a Windows workstation to communicate with a Desktop Management Preboot Services server. When you boot a workstation with a PXE-on-Disk diskette in the floppy drive, it is as if that workstation had a PXE-enabled network adapter.

The PXE-on-Disk Setup program runs on the following operating systems:

- Windows 95/98/ME
- Windows 2000/XP

56.7.2 Creating a PXE-on-Disk Diskette

This section contains the following information:

- “Creating the Diskette in a Windows Server Environment” on page 678
- “Creating the Diskette in a NetWare Server Environment” on page 680

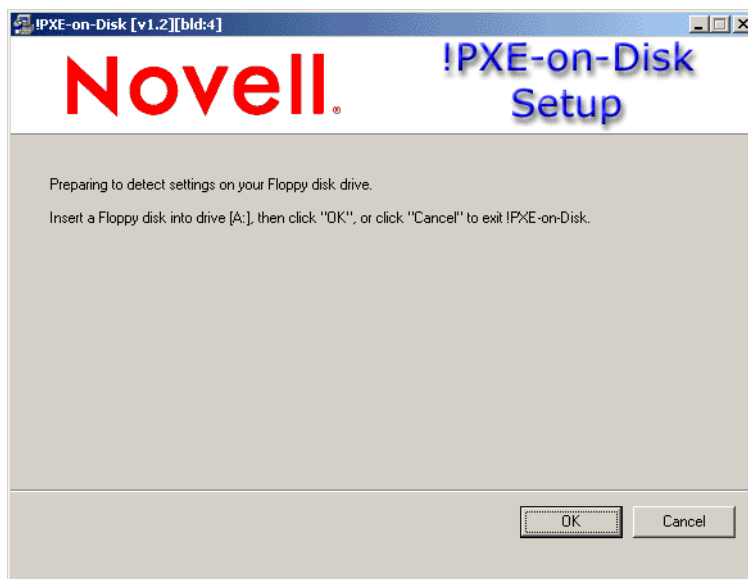
Creating the Diskette in a Windows Server Environment

When you installed the Desktop Management Preboot Services component on a Windows server, the PXE-on-Disk creation program was also installed and registered. Use the following procedure to create a PXE-on-Disk diskette from your Windows server.

- 1 From the Windows desktop, click *Start > Programs > ZENworks Preboot Services > PXE-on-Disk* to display the PXE-on-Disk Setup window.

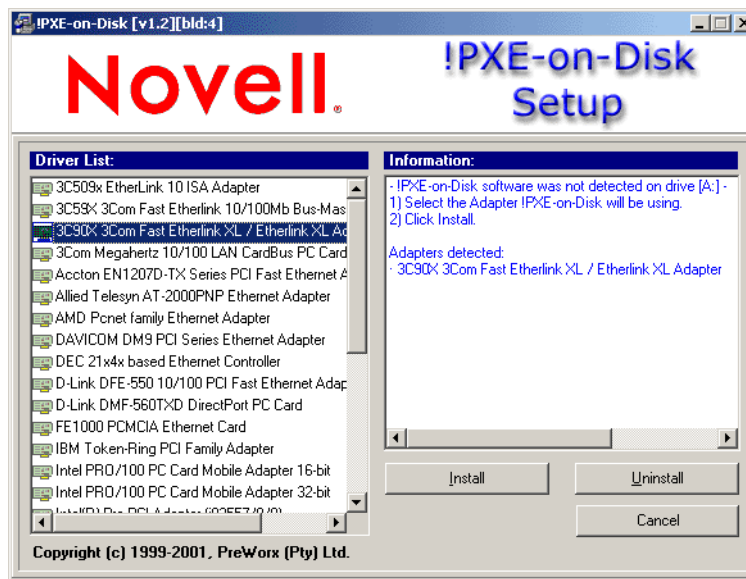
or

In ConsoleOne, click *Tools > ZENworks Utilities > Imaging > Create or modify boot diskette > Create PXE disk*.



- 2 Insert an empty, formatted, high-density diskette in the disk drive.

- 3 Click *OK* to display the *Driver and Information* lists for PXE-compatible network adapters.



Note that the network adapter (or adapters) installed on your server is detected and the specifications are listed in the *Information* list box of the Setup window. Some driver types might be duplicated. For example, Accton En1207d is the same as SMC 1211TX.

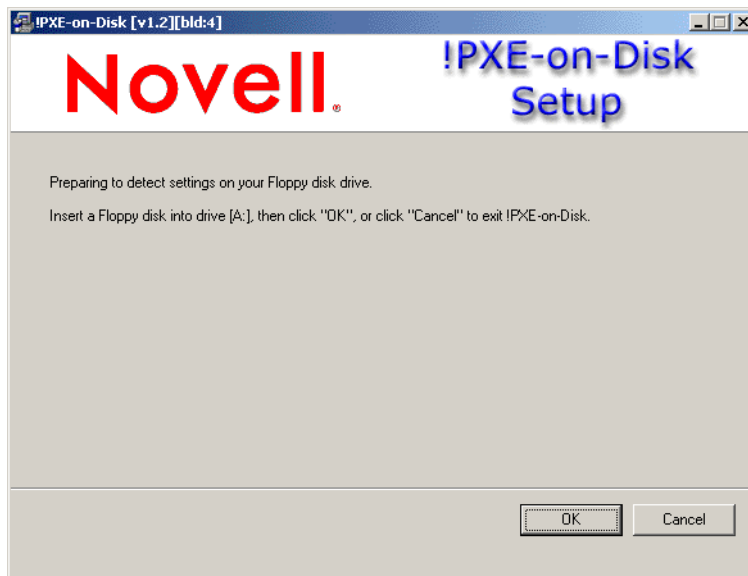
- 4 From the *Driver List*, select the name of the network adapter driver (or its nearest equivalent) that is installed on the client workstation you want to connect to the Preboot Services server.
- 5 Insert an empty, formatted, high-density diskette in the disk drive, then click *Install* to start creating a PXE-on-Disk diskette.

When the installation is complete, the diskette contains appropriate PXE-on-Disk information for the intended client workstation.

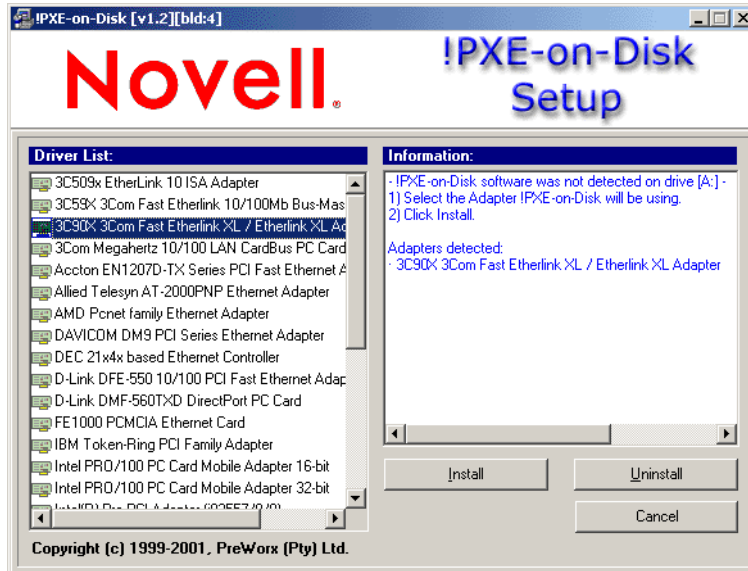
- 6 Click *Close* to complete the creation of the PXE-on-Disk diskette.

Creating the Diskette in a NetWare Server Environment

- 1 From the `sys:\public\zenworks\pxe` directory, run `psetupn.exe` to display the PXE-on-Disk Setup window.



- 2 Insert an empty, formatted, high-density diskette in the disk drive.
- 3 Click *OK* to display the *Driver and Information* lists for PXE-compatible network adapters.



The network adapter of machine you are using is detected and its specifications listed in the *Information* list box of the Setup window.

- 4 From the *Driver List*, select the name of the network adapter driver (or its nearest equivalent) that is installed on the client workstation you want to connect to the Preboot Services server.
- Some driver types might be duplicated. For example, Accton En1207d is the same as SMC 1211TX.

- 5 Click *Install* to start creating a PXE-on-Disk diskette.

When the installation is complete, the diskette contains appropriate PXE-on-Disk information for the intended client workstation.

- 6 Click *Close* to complete the creation of the PXE-on-Disk diskette.

56.7.3 Booting with a PXE-on-Disk Diskette

Before you boot a client workstation with a PXE-on-Disk diskette, you should make sure that Desktop Management Preboot Services is installed on a network server. This is the server that communicates with the client workstation and give it workstation imaging tasks to perform. For more information about installing ZENworks Desktop Management Preboot Services on a server, see Step 12 under “[Desktop Management Server Installation Procedure](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

When you know that Desktop Management Preboot Services is installed on the server, you can reboot the client workstation with a PXE-on-Disk diskette. During the reboot cycle, the client workstation does the following:

- Establishes a connection with the Desktop Management Preboot Services server.
- Executes any imaging work to be performed.
- Continues its boot cycle.

56.7.4 If PXE-on-Disk Fails to Operate Correctly

If PXE-on-Disk is not working, an incorrect network adapter is installed, or PXE-on-Disk is not installed on the diskette you are using to boot the workstation. To correct this, install a PXE-enabled network adapter or reinstall PXE files on a diskette using the PXE-on-Disk setup utility. See “[Creating a PXE-on-Disk Diskette](#)” on page 678.

56.8 Editing the Desktop Management Preboot Services Menu

When a PXE-enabled workstation is booted, it broadcasts for DHCP information and receives a response from both the DHCP and Proxy DHCP servers. The workstation then downloads the Preboot Services client and checks for imaging work with the Transaction server. If there is imaging work to do, the workstation displays a default Desktop Management Preboot Services (PXE) Menu with the following options:

- *Start ZENworks Imaging in Automatic Mode*
- *Start ZENworks Imaging in Maintenance Mode*
- *Disable the ZENworks Partition*
- *Enable the ZENworks Partition*
- *Exit*

HISTORICAL NOTE

The PXE (Preboot Execution Environment) environment provided by PreWorX is used for Windows and NetWare imaging servers. Novell's internally-developed PXE solution for Linux imaging servers in ZENworks 7 with SP1 supports the SLES-based ZENworks Imaging distribution.

The PXE process based on PreWorX files differs from Novell's solution. For example, PreWorX uses a combination of Caldera* DOS, the `linld` Linux loader program, and `.cmd` configuration files for passing parameters to the Linux kernel. Novell's PXE solution is based on the `pxelinux` boot loader and `.cfg` configuration files.

Therefore, depending on where the Preboot Services Menu file resides, there are two methods for editing the menu. One menu is provided by PreWorX for Windows for imaging servers, the other by Novell for Linux for imaging servers.

Contact [PreWorX \(http://www.preworx.com\)](http://www.preworx.com) for their toolkit if more capability is needed in editing the menu in Windows.

Review the applicable sections for instructions on editing the Preboot Services Menu:

- [Section 56.8.1, “Editing the Preboot Services Menu on Linux,” on page 682](#)
- [Section 56.8.2, “Understanding the Windows-based Preboot Services Menu Editor,” on page 684](#)
- [Section 56.8.3, “Editing the Preboot Services Menu on Windows,” on page 685](#)

56.8.1 Editing the Preboot Services Menu on Linux

There might be circumstances when you want to modify the options on the Preboot Services Menu. You can customize these options by editing a text file contained on the Linux imaging server. For example, you can:

- Add, delete, and modify menu options
- Change the color scheme
- Change the menu title and screen name

The following procedure should be done on each ZENworks Imaging server where you want to customize the menu.

To edit the Preboot Services Menu:

- 1 In a text editor, open the following file on a ZENworks Imaging server where novell-proxydhcp is running:

```
/srv/tftp/pxemenu.txt
```

IMPORTANT: If you want to save the default options for this menu, we recommend that you make a backup copy of `pxemenu.txt`, such as `pxemenu_orig.txt`.

The following is the content of the default Preboot Services Menu's pxemenu.txt file:

```
#This file describes a PXEMenu

ScreenName = Novell Preboot Services Menu
ScreenInfo = Version 1.0 August, 2005
MenuTitle = ZENworks Preboot Options

#The screen colors determine the color of the main part of the menu
screen
ScreenColor = bright_white
ScreenBackgroundColor = blue

#The info colors determine the color of the screen information at
the top
#of the menu screen
InfoColor = yellow
InfoBackgroundColor = blue

#The hint colors determine the color of the hint line at the bottom
of the screen
HintColor = lt_cyan
HintBackgroundColor = blue

#The menu colors determine the color of the menu box and menu title
MenuColor = yellow
MenuBackgroundColor = blue

#The option colors determine the color of the menu option
OptionColor = BRIGHT_WHITE
OptionBackgroundColor = BLUE

#The chosen colors determine the color of the high-lighted option
ChosenColor = BRIGHT_WHITE
ChosenBackgroundColor = RED

#Maximum of 9 menu items
MenuOptionCount = 7

option1 = Start ZENworks Imaging
option2 = Start ZENworks Imaging Maintenance
option3 = Disable ZENworks Partition
option4 = Enable ZENworks Partition
option5 = Exit

CFG1 = z_auto.cfg
CFG2 = z_maint.cfg
CFG3 = z_zpdis.cfg
CFG4 = z_zpen.cfg
CFG5 = 0

Hint1 = ZENworks Imaging in Automated Mode
Hint2 = ZENworks Imaging Linux Session in Interactive Mode
Hint3 = Disable Existing ZENworks Partition
```

Hint4 = Re-enable a Disabled ZENworks Partition
Hint5 = Boot to Local Hard Drive

- 2** To change the appearance of the menu, edit the first seven sections (title and colors).

To change colors, the mnemonics you enter must be selected from the following:

BLACK	RED	GRAY	LT_GREEN
BLUE	MAGENTA	YELLOW	LT_CYAN
GREEN	BROWN	BRIGHT_WHITE	LT_RED
CYAN	WHITE	LT_BLUE	LT_MAGENTA

- 3** To change the menu options, edit the last four sections, beginning with `MenuOptionCount`.

The menu options, their code, and their hint descriptions are correlated by the number (see “#” where used below).

MenuOptionCount: This number must match the total number of options defined in the next three sections. The limit is 9 menu options.

option#: Displayed in the menu as the option’s text.

CFG#: The configuration file that is used upon selecting the menu option.

Hint#: Displayed at the bottom of the screen to explain the selected menu option’s function. It changes as you select a menu option.

IMPORTANT: If you add or subtract a menu option, make sure that you do the same thing to each of the last three sections. The numbering should be consecutive (such as 1 through 5). Be sure to keep the corresponding items matched in each of the last three sections.

- 4** When finished, save the `pxemenu.txt` file.

56.8.2 Understanding the Windows-based Preboot Services Menu Editor

If you want to create a custom Preboot Services (PXE) menu, you can use the Desktop Management Preboot Services Menu Editor to set and run your own actions and DOS utilities on the client workstation. Novell provides this utility as a service; no custom DOS or Linux utilities have been developed by Novell.

NOTE: Contact [PreWorX \(http://www.preworx.com\)](http://www.preworx.com) for their toolkit if more capability is needed in editing the menu in Windows.

The Menu Editor is a Windows-based, option-driven utility that lets you do the following on the Preboot Services (PXE) menu:

- Add menu items or submenus to the Preboot Services (PXE) menu
- Add executable commands to be performed on the client workstation
- Delete a submenu or an action from an existing menu

The Menu Editor generates menu files and stores them on the Desktop Management Preboot Services server. These files can be selected from the Menu Editor interface and downloaded to a Preboot Services client workstation.

- “Installing the Preboot Services Menu Editor” on page 685
- “Accessing the Preboot Services Menu Editor” on page 685
- “Understanding the Preboot Services Menu Editor Interface” on page 685

Installing the Preboot Services Menu Editor

If you chose the Preboot Services component during the Desktop Management Preboot Services installation program, the Menu Editor is automatically installed on Windows servers you designate as Preboot Services servers. For more information, see “[Desktop Management Server Installation Procedure](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*. The Menu Editor is not installed to a NetWare server during the Preboot Services installation; the files must be accessed from a Windows workstation.

Accessing the Preboot Services Menu Editor

If you installed to a Windows server, you can access the Menu Editor from the Windows desktop (after the PXE-enabled Windows workstation is imaged) by clicking *Start > Programs > ZENworks Preboot Services > ZENworks Preboot Services Menu Editor*.

If you need to access the Menu Editor from a NetWare server, locate the files on the *ZENworks Desktop Management Program* CD in the `\menu editor` directory, then copy them to your NetWare server. Then, from a Windows machine, you can map a drive to the location on the server and run the Menu Editor.

Understanding the Preboot Services Menu Editor Interface

The Menu Editor interface is not available unless you are creating or editing an existing menu. Add and delete functions are available from the Options menu or from icons on the toolbar. Menu Editor functions can also be initiated with keyboard commands from a Windows workstation. For example, pressing the Insert key while in the Menu Editor adds a menu item, and pressing the Delete key deletes a menu item.

You can enter descriptive text about the menu in the *Information* field. You can also add help by entering appropriate text in the *Help* field.

56.8.3 Editing the Preboot Services Menu on Windows

Although you could use the default Preboot Services (PXE) Menu for Desktop Management Preboot Services, you might want to take advantage of the flexibility of the Preboot Services Menu Editor to create a new menu or to modify the default menu.

This section contains the following information:

- “Modifying the Default Menu” on page 686
- “Creating a New Preboot Services (PXE) Menu” on page 688
- “Creating a Submenu” on page 689
- “Creating Functions Within the Menu” on page 690

- “Saving the Menu as a .Dat File” on page 690

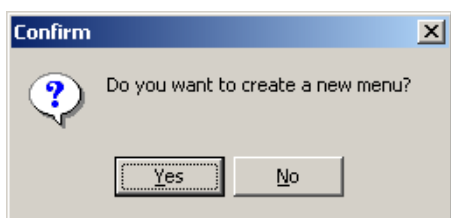
Modifying the Default Menu

There might be circumstances that require you to limit the options on the Desktop Management Preboot Services (PXE) menu. For example, you might want to restrict the user from using the Linux bash command line options. In such a case, you must create a new default menu and copy it to proper location on the Preboot Services server.

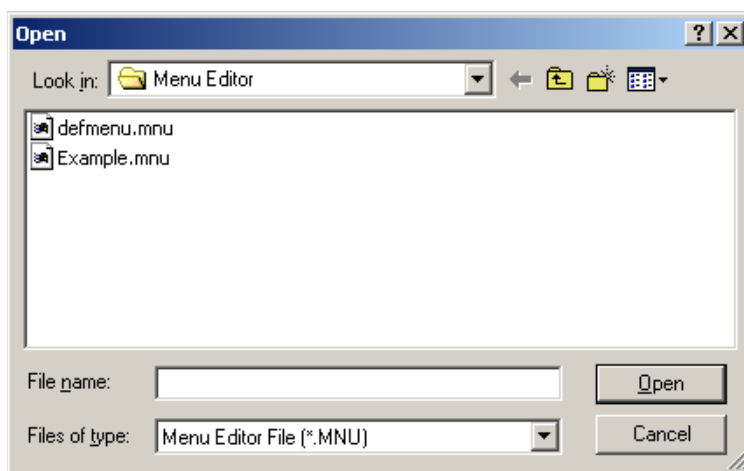
The following steps assume that you want to overwrite the existing default menu. If you want to save the options of this menu, we recommend that you rename `defmenu.mnu` (for example, `defmenu_old.mnu`), edit it with the Menu Editor to meet your needs, then save it again as `defmenu.mnu`.

To modify the default menu:

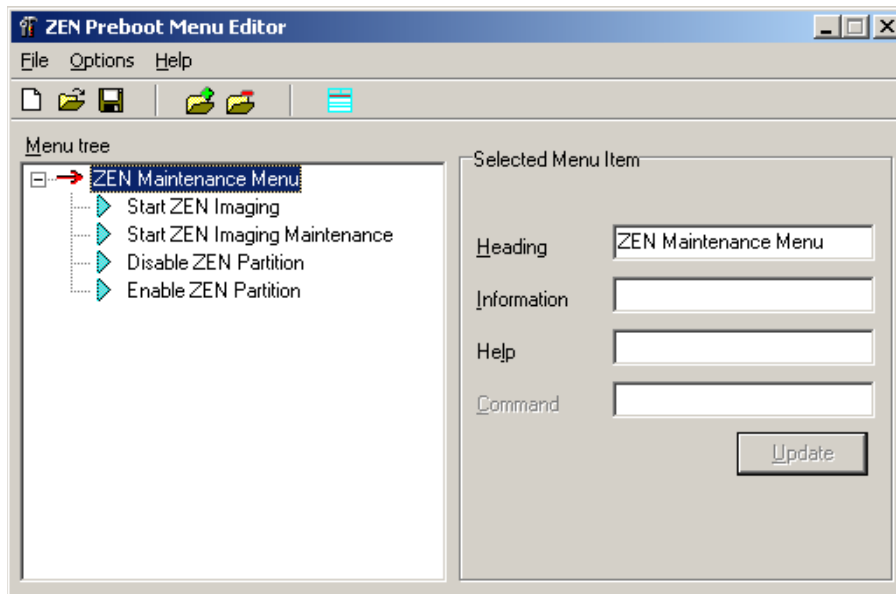
- 1 In the Windows desktop, click *Start > Programs > ZENworks Preboot Services > ZENworks Preboot Services Menu Editor* to display the following dialog box:



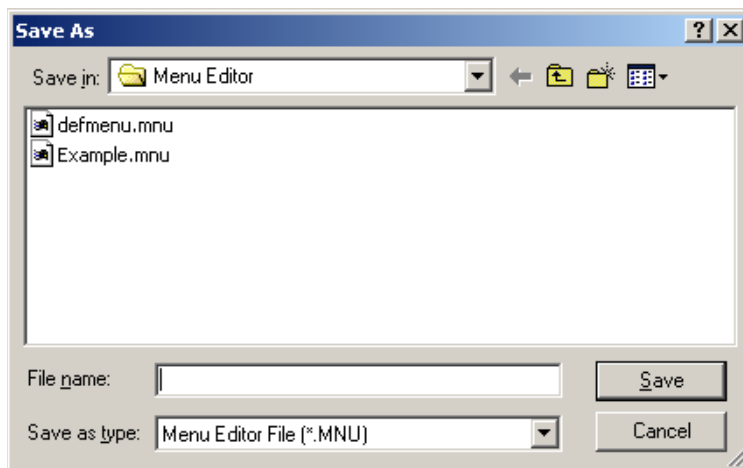
- 2 Click *No* to display the menu files that reside in the directory from which `meditor.exe` is running.



- 3 Select (or browse to) the `defmenu.mnu` file that you want to change, then click *Open*.



- 4 Select the menu item that you want to delete, click *Options*, then click *Delete* to display a message similar to the following:
Do you want to delete *Start ZENworks Imaging Maintenance* and its subitems?
- 5 Click *Yes* to return to the Menu Editor.
- 6 Click *File > Save* to open the Save As dialog box.



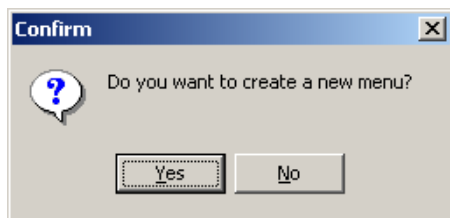
- 7 Select `defmenu.mnu` to enter this filename in the *Filename* field, then click *Save*. The following prompt is displayed:
Do you want to overwrite the old file?
- 8 Click *Yes* to overwrite the file and to return to the Menu Editor window.
You have now modified the `defmenu.mnu` menu template.
- 9 In the Menu Editor window, click *File > Save* to reopen the Save As dialog box.

- 10 In the *Save As Type* drop-down list, select *ZENworks Preboot Menu file (*.dat)*.
- 11 Select *defmenu.dat* to enter this filename in the *Filename* field, then click *Save*. The following prompt is displayed:
Do you want to overwrite the old file?
- 12 Click *Yes* to overwrite the file and to return to the Menu Editor window.
You have now modified the data file that is displayed as the menu on a PXE workstation.
- 13 Copy the new *defmenu.dat* file to the */tftp* directory on the Preboot Services server.

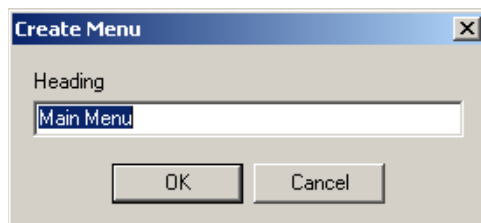
Creating a New Preboot Services (PXE) Menu

Use the following steps to create a new Preboot Services (PXE) menu using the Desktop Management Preboot Services Menu Editor:

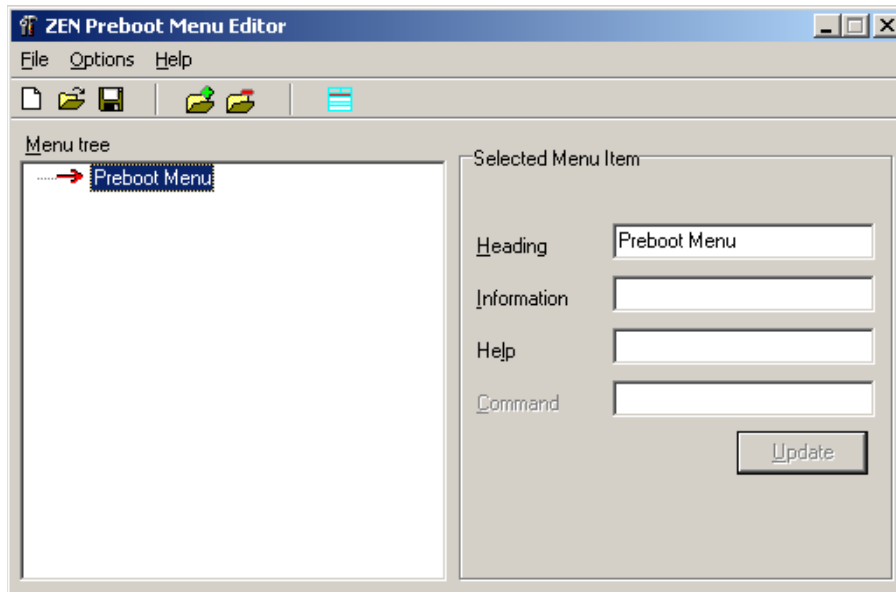
- 1 In the Windows desktop, click *Start > Programs > ZENworks Preboot Services > ZENworks Preboot Services Menu Editor* to display the following dialog box:



- 2 Click *Yes* to display the Create Menu dialog box.



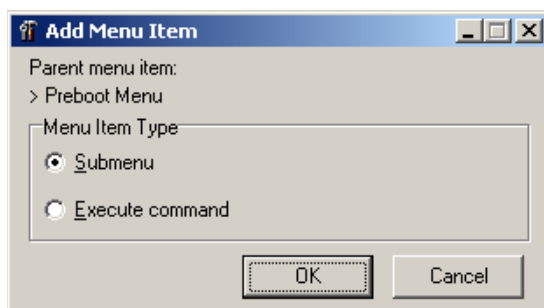
- 3 Specify the name of menu you want to create, then click *OK* to display the ZENworks Preboot Menu Editor window.



Creating a Submenu

If you want to create your own functions for the Preboot Services (PXE) menu, you need to create a submenu of these functions. Use the following steps to create a submenu.

- 1 Select *Add* from the Options menu to display the Add Menu Item window.



- 2 Select *Submenu*, then click *OK* to display the Add Menu dialog box.
- 3 In the *Heading* field of the dialog box, specify the text you want to use as the option in the submenu, then click *OK*.
The Menu Editor displays the submenu option as a subordinate item to the main menu you have already created.
- 4 Type a description and the help text in the *Information* and *Help* fields.
- 5 Click *Update* to save the text of the submenu option and any accompanying text you have created.

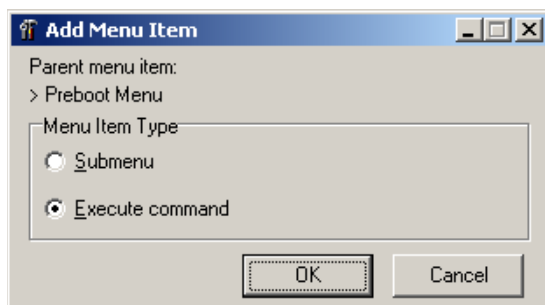
Although the submenu item is now created and appears on the Preboot Services (PXE) menu, it does not launch any utility; it is merely a text heading that serves as a navigation tool to options that actually perform functions.

Creating Functions Within the Menu

As stated earlier in this document, Desktop Management Preboot Services ships with a Preboot Services (PXE) menu that allows only limited, predesigned actions from the client workstation. Novell does not ship other DOS or Linux utilities. However, if you want to add functionality of your own, you can do so with the Preboot Services Menu Editor.

To add executable commands to the Menu Editor:

- 1 In the Preboot Services Menu Editor window, select a menu item, click *Options*, then click *Add* to display the Add Menu Item window.



- 2 Select *Execute Command*, then click *OK*.
- 3 In the Execute Command dialog box, specify the menu text that describes the functionality of your program, then click *OK*.
- 4 Specify the command parameters of the utility you want to run, then click *OK*.
- 5 Specify descriptive text about the item you have created, then click *OK*.
- 6 Specify any help text that you want to be accessible by an F1 command for this menu item, then click *OK*.
- 7 When you have finished creating the menu, click *File > Save* to save the structure.

By default, the file is saved in `.mnu` format, which is used as a template by the Preboot Services Menu Editor interface. To be used by the Preboot Services (PXE) menu, this file must be exported to a binary (`.dat`) format. For more information, see [“Saving the Menu as a .Dat File” on page 690](#).

Saving the Menu as a .Dat File

To create a `.dat` file for the Preboot Services (PXE) menu using a `.mnu` file:

- 1 Open the Preboot Services Menu Editor, then click *No* to display the existing `.mnu` files saved to your default directory (the same directory where the menu editor, `meditor.exe`, resides).
- 2 Select the `.mnu` file of the menu you want to export for later use by the Preboot Services (PXE) menu, click *File*, then click *Export*.
- 3 In the *Save As Type* drop-down list, select *ZENworks Preboot Menu file (*.dat)*.
- 4 In the *Filename* field, type `DEFMENU`, then click *Save* to return to the Menu Editor window.

You have now created a data file that can be displayed as the default menu on a PXE-enabled workstation.

- 5** Copy the `defmenu.dat` file to the `/tftp` directory on the Preboot Services Server.

The `.dat` file is saved in the local directory from which you are running the Preboot Services Menu Editor. You must copy the file to the `\tftp` directory at the Preboot Services server.

Setting Up Workstations for Imaging

57

The following sections cover procedures to prepare workstations for imaging, depending on your imaging deployment strategy. For more information, see [Chapter 53, “Common Imaging Deployment Strategies,”](#) on page 625.

If you are using Preboot Services (PXE) as your imaging method, you need to enable PXE on the workstation. For more information, see [Section 55.1, “Using Preboot Services \(PXE\),”](#) on page 631.

If you are using a ZENworks (hard-disk) partition as your imaging method, you need to create the partition on the workstation. For more information, see [Section 55.4, “Creating an Imaging Hard-Disk Partition,”](#) on page 635.

The following sections contain additional information:

- [Section 57.1, “Windows Workstation Requirements,”](#) on page 693
- [Section 57.2, “Enabling a Windows Workstation for Auto-Imaging Operations,”](#) on page 694

57.1 Windows Workstation Requirements

It is possible (but usually not as convenient) to image a workstation without connecting to the network. It is also possible to image non-Windows workstations, but such operations can’t be fully automated through Novell® eDirectory™ and the images can only be raw, bit-by-bit images of the entire hard disk, as opposed to customizable, file-by-file images of the data.

The following are the requirements for the workstation:

Table 57-1 Workstation Requirements for ZENworks Imaging

Requirement	Explanation
A supported Ethernet card	The workstation must connect with the ZENworks Imaging server to store or retrieve the images. This connection is made when the workstation is under the control of the Desktop Management Workstation ZENworks® Imaging Engine (which is a Linux application), not when the workstation is running under Windows. Therefore, make sure the workstation has a supported Ethernet card. For more information, see Chapter 66, “Supported Ethernet Cards,” on page 803.
Windows 98, 2000, or XP installed	Unattended operations based on Workstation objects are currently supported only on 32-bit Windows platforms.
50 MB free disk space	Unless you are using Preboot Services, unattended operations require a ZENworks partition to be installed on the workstation hard disk, so that the ZENworks Imaging Engine can gain control when booting. The default partition size is 150 MB, and the minimum partition size is 50 MB. This partition is not required if you are performing manual imaging operations using bootable CDs or DVDs.

Requirement	Explanation
Standard hardware architecture	NEC* PC98 architecture is not supported.
PXE enabled	If you are using Desktop Management Preboot Services, PXE must be enabled either in the BIOS or through a PXE boot disk. See Section 55.1, “Using Preboot Services (PXE),” on page 631 for more information.

NOTE: Desktop Management Imaging does not support workstations running boot managers, such as System Commander. Boot managers create their own information in the MBR and overwrite the ZENworks boot system, which prevents the workstation from communicating with the ZENworks Imaging server. If you are using boot managers in your environment, you should disable or remove them before performing imaging operations.

57.2 Enabling a Windows Workstation for Auto-Imaging Operations

The following procedure explains how to register the workstation as an object in your eDirectory tree, install a ZENworks Imaging Windows Agent on the workstation, and install a permanent ZENworks partition on the hard disk.

Complete this procedure if you are not using Preboot Services (PXE). If you have enabled PXE on the workstation and have installed Desktop Management Preboot Services on your ZENworks Imaging server, this procedure is not a prerequisite to performing unattended imaging operations. For more information, see [Section 55.1, “Using Preboot Services \(PXE\),” on page 631](#).

When you put a new base image on a Windows workstation, the workstation receives the same identification data as the workstation from which the image was taken, including such settings as the IP address and computer (NETBIOS) name. To work around this, you can install the [ZENworks Imaging Windows Agent](#) on the target workstation before reimaging it. This saves the workstation’s current identity settings to an area on the hard disk that’s safe from reimaging. When the workstation reboots after being reimaged, the agent restores the original settings.

IMPORTANT: The ZENworks Imaging Windows Agent does not save or restore any Windows 2000/XP Domain information. If you change a workstation’s domain and then restore an image, the workstation receives whatever domain is embedded in the new image.

This procedure needs to be performed only once prior to performing auto-imaging (unattended) operations. It is not a prerequisite to performing manual imaging operations.

- 1 If you haven’t already done so, register the workstation as an object in your eDirectory tree that contains the ZENworks Imaging server.

When you boot a Windows workstation from an imaging device or method and allow the boot process to proceed in auto-imaging mode, the ZENworks Imaging Engine runs on the workstation and contacts a ZENworks Imaging server. In order for the workstation to be imaged, you must first either define an eDirectory policy for the ZENworks Imaging server (for more information, see [Section 58.1, “Defining an Imaging Policy for Unregistered Workstations \(Server Policy\),” on page 697](#)), or you must register the workstation as an object and configure Imaging on the Workstation object.

For more information on registering the workstation as an object, see [Part III, “Automatic Workstation Import and Removal,” on page 117](#).

You don’t need to complete all of the tasks mentioned in the instructions. Just create a Server policy package that contains a minimal Workstation Import policy (use the defaults for naming, groups, and limits), and then associate the Server package with the container where you want the Workstation object to be created. Then, configure the workstation to communicate with the import service on the ZENworks Imaging server, and reboot the workstation. Before proceeding with the next step, check your eDirectory tree to make sure that the Workstation object was created.

- 2 Set a flag in the Workstation object that triggers the imaging operation you want.

For more information, see [Section 59.5, “Performing an Automatic Imaging Creation or Restoration,” on page 709](#).

- 3 Install the ZENworks Imaging Windows Agent on the workstation:

- 3a Browse to the `sys:\public\zenworks\imaging` directory in your ZENworks Desktop Management installation (on the ZENworks Imaging server).

- 3b Complete the steps that correspond to the type of workstation:

Workstation Type	Steps
Windows 98	<ol style="list-style-type: none">1. Copy <code>ziswin.exe</code>, <code>zislib16.dll</code>, and <code>zislib32.dll</code> to the <code>novell\zenis</code> directory.2. Run <code>ziswin.exe</code> from the <code>novell\zenis</code> directory.3. Run <code>regedit.exe</code> and browse to <code>HKEY_LOCAL_MACHINE > Software > Microsoft > Windows > CurrentVersion > RunServices</code>.4. Add the string value <code>ZENwork Imaging Service</code> and set it to the filename and path of the <code>ziswin.exe</code> file. For example, <code>c:\novell\zenis\ziswin.exe</code>5. Save the changes and close <code>regedit</code>.
Windows 2000	<ol style="list-style-type: none">1. Copy <code>ziswin.exe</code> and <code>ziswinr.dll</code> (in the <code>nls\english</code> subdirectory or the appropriate language subdirectory) to your <code>winnt\system32</code> directory.2. From a command prompt, change to your <code>winnt\system32</code> directory, type <code>ziswin -install</code>, then press Enter.
Windows XP	<ol style="list-style-type: none">1. Copy <code>ziswin.exe</code> and <code>ziswinr.dll</code> (in the <code>nls\english</code> subdirectory or the appropriate language subdirectory) to your <code>windows\system32</code> directory.2. From a command prompt, change to your <code>windows\system32</code> directory, type <code>ziswin -install</code>, then press Enter.

- 3c Reboot the workstation.

- 4 Take an image of the workstation as instructed in [Section 60.1, “Manually Taking an Image of a Workstation,” on page 711](#).

IMPORTANT: Do this even if you have taken an image of the workstation previously. This ensures that the new image captures the changes you made in the preceding steps.

- 5 After the image is created, reboot the workstation with the imaging boot method, type `install` at the boot prompt, then press Enter.

This starts the process of creating the ZENworks partition in the first partition slot. It also destroys all existing partitions, even if slot 1 is empty and available. By default, the ZENworks partition size is 150 MB.

If the ZENworks partition already exists, it is upgraded, and your existing Windows partitions are left intact.

- 6 (Optional) After the ZENworks partition is created and the bash prompt is displayed, type `img dump`, then press Enter.

This displays a list of the partition slots on the workstation. Unless you are upgrading your ZENworks partition, each partition slot should be empty and none should be active. The ZENworks partition is hidden from the list, so the number of partition slots in the list should be one less than before.

or

Type `img` to display a menu, select *Dump*, then select *No Geometry*.

- 7 At the bash prompt, restore the image you took in [Step 4](#).

Use the `img restorep` command or select *Restore an Image*, then select *Proxy Image* from the menu as instructed in [Step 6](#) of [Section 60.2](#), “[Manually Putting an Image on a Workstation](#),” on page 715.

- 8 (Optional) After the image is restored and the bash prompt is displayed, use the `img dump` command to redisplay the list of the partition slots on the workstation.

or

Type `img` to display a menu, select *Dump*, then select *No Geometry*.

You should now see information about the Windows partitions that are restored and activated. There should still be one less partition slot than before because the ZENworks partition is still hidden (and will continue to be).

- 9 At the bash prompt, type `lilo.s`, then press Enter.

- 10 When the bash prompt is displayed, reboot the workstation.

The workstation should boot to Windows. If the bash prompt is displayed, enter the `lilo.s` command again and reboot a second time.

From this point on, whenever the workstation is rebooted, the ZENworks Imaging Engine takes control and checks the ZENworks Imaging server to see if an imaging operation should be performed. If you have not configured the Workstation object in eDirectory to trigger an unattended imaging operation, the ZENworks Imaging Engine simply exits and automatically reboots the workstation to Windows.

The following sections explain how to set up policies for Novell® ZENworks® Desktop Management imaging services, and how to select general imaging server settings. The procedures that are applicable to you depend on your imaging deployment strategy. For more information, see [Chapter 53, “Common Imaging Deployment Strategies,” on page 625](#).

- [Section 58.1, “Defining an Imaging Policy for Unregistered Workstations \(Server Policy\),” on page 697](#)
- [Section 58.2, “Defining an Imaging Policy for Registered Workstations \(Workstation Policy\),” on page 699](#)
- [Section 58.3, “Allowing Overwriting Filenames and Restricting the Save Location of Image Files \(Imaging Server Settings\),” on page 701](#)

58.1 Defining an Imaging Policy for Unregistered Workstations (Server Policy)

If a Windows workstation hasn't been registered as a Workstation object in Novell eDirectory™ and you boot that workstation from an imaging method in auto-imaging mode, the ZENworks Imaging server is contacted and checks its Imaging Server policy in eDirectory to determine which image to put down on the workstation.

If the base image specified by the policy is the same as the base image currently on the workstation (as reported by the ZENworks Imaging Engine), the ZENworks Imaging server doesn't send any new images to put down on the workstation, unless the policy specifies to force down the base image again. If the policy specifies to force down the base image, or if the base image currently on the workstation is different than the base image specified by the policy, the ZENworks Imaging server sends down the new base image and any add-on images specified by the policy, and the ZENworks Imaging Engine puts these images down on the workstation.

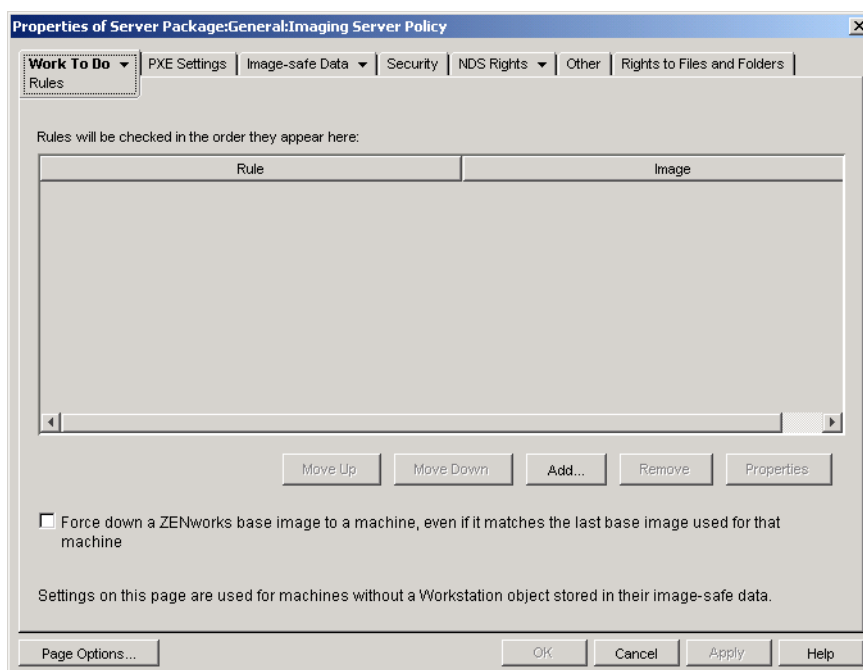
IMPORTANT: If you configure a ZENworks Imaging server policy to send an add-on image only (no base image) to a workstation, the workstation receives the add-on image, but it also reboots and brings down the image again, resulting in a reboot/imaging loop.

In addition, if the ZENworks Imaging Engine reports to the ZENworks Imaging server that data is missing from the workstation's image-safe area, the ZENworks Imaging server obtains the missing data from the Imaging Server policy and sends it to the ZENworks Imaging Engine, which then saves the data to the image-safe area.

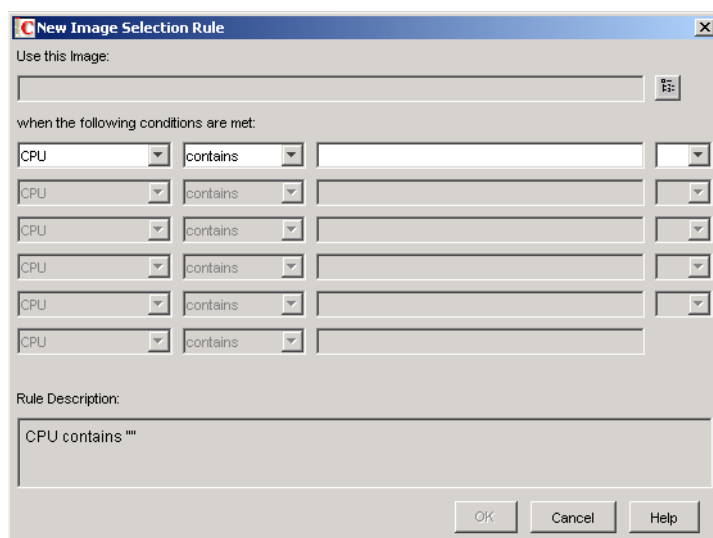
To define the Imaging Server policy for one or more ZENworks Imaging servers:

- 1 Prepare the various workstation images that the policy can prescribe. For details, see [Chapter 59, “Creating and Restoring Images,” on page 703](#).
- 2 If a Server Package hasn't already been created to hold the policies for the target ZENworks Imaging servers, create one as instructed in [Chapter 11, “Creating Policy Packages,” on page 143](#).
- 3 Right-click the Server Package, then click *Properties*.

- 4 Enable the Imaging Server policy, then click *Properties* to display the Rules page.



- 5 Click *Add* to display the New Image Selection Rule dialog box.



- 6 Click the browse button next to the *Use This Image* field to select a Workstation Image object (for more information, see [“Creating a Workstation Image Object” on page 706](#)), use the drop-down fields and operators to specify the conditions under which the selected image should be used (click *Help* for details), then click *OK*.

Repeat this step as needed to provide rules that covers all workstations serviced by the target ZENworks Imaging servers.

These rules are used by your ZENworks Imaging server to determine which image to put on workstations during unattended imaging operations. The various hardware configuration data specified in the rules is compared against the actual hardware configuration data detected by

the Workstation ZENworks Imaging Engine on the workstation. To see this data for a particular workstation, boot it with the imaging boot CD or DVD in manual mode and issue the `img info` command or enter `img`, then select *Information* from the menu.

Take care to choose rules that apply only to the unregistered workstations you want imaged. Otherwise, an image could be unintentionally pushed to another workstation.

- 7 (Optional) If you want the ZENworks Imaging server to force down the base image determined by this policy even if it is the same as the base image currently on the workstation, select the *Force Down a ZENworks Base Image to a Machine* check box on the bottom of the Rules page.

WARNING: Use this option with care, because putting down a base image destroys all data that was added to the workstation since the last base image was put down. In most scenarios, you'll want to use this option only while a specific workstation is being imaged and not generally for all workstations, unless this policy is designed for a lab environment where you want the workstations to be reimaged every time they reboot. If you select this option as a temporary measure, be sure to deselect it after the specific imaging task is done.

- 8 (Conditional) If you are using Preboot Services but previously booted workstations from a ZENworks partition, you can disable the ZENworks partition on the Imaging Partition property page (click the down-arrow next to *Work To Do*, click *Imaging Partition*, then select the *Disable the ZENworks Imaging Partition, If It Exists* check box). The partition is disabled but is not removed with this option.
- 9 (Optional) If you want to specify the availability of the PXE menu, which is displayed when you boot a PXE-enabled workstation, click the *PXE Settings* tab, then select an option. Click *Help* for details.

If you want to specify a different image when using Preboot Services, rather than the default image that is defined, specify the image file and pathname.

- 10 On the *Image-safe Data* tab, fill in the IP Configuration, Windows Networking, and DNS Settings pages.

These pages supply image-safe data values that might be missing on the workstations that are serviced by the target ZENworks Imaging servers. For details on these pages, click *Help*.

IMPORTANT: Image-safe data is not supported on Linux workstations.

- 11 Click *OK* to save the policy.
- 12 On the properties of the Server Package, click the *Associations* tab, add the containers and server objects that represent the target set of ZENworks Imaging servers, then click *OK*.

Remember that the policy won't actually be consulted by the associated ZENworks Imaging servers, unless the client requesting the imaging operation is an unregistered workstation that booted in auto-imaging mode.

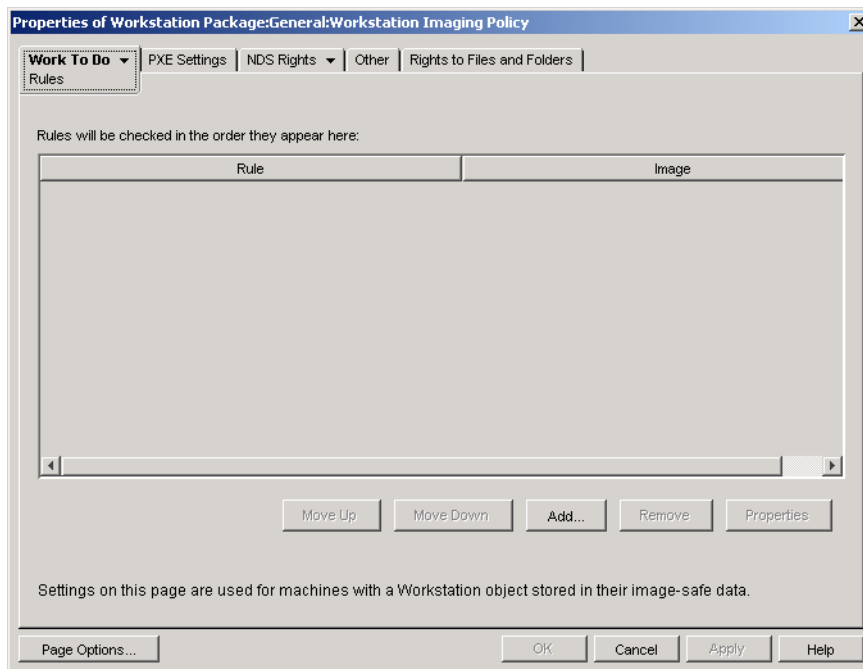
58.2 Defining an Imaging Policy for Registered Workstations (Workstation Policy)

If a Windows workstation is registered as a Workstation object in eDirectory and you boot that workstation from an imaging method in auto-imaging mode, the ZENworks Imaging server is contacted and checks the Workstation object to see if the administrator has flagged it to receive an image. If this is the case and the administrator hasn't specified which image to use, the ZENworks

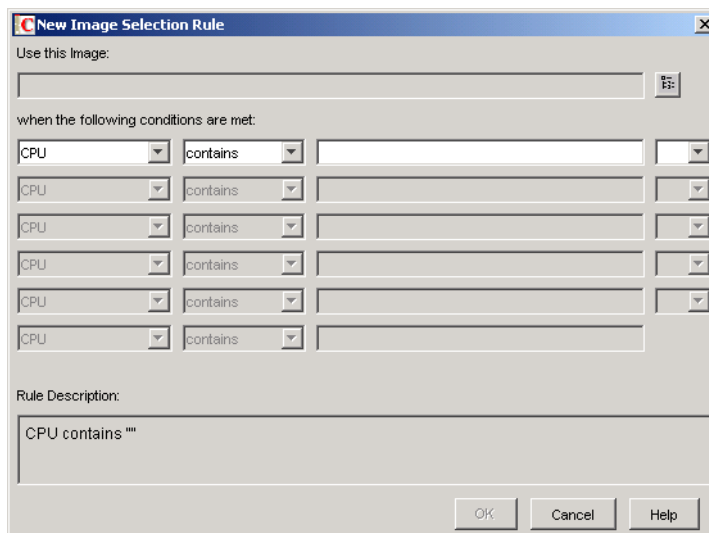
Imaging server consults the Workstation Imaging policy associated with the Workstation object to determine which image to send down.

To define the Workstation Imaging policy for one or more workstations:

- 1 Prepare the various workstation images that the policy can prescribe. For details, see [Chapter 59, “Creating and Restoring Images,” on page 703](#).
- 2 If a Workstation Package hasn’t already been created to hold the policies for the target workstations, create one as instructed in [Chapter 11, “Creating Policy Packages,” on page 143](#).
- 3 Right-click the Workstation Package, then click *Properties*.
- 4 Enable the Workstation Imaging policy, then click *Properties* to display the Rules page.



- 5 Click *Add* to display the New Image Selection Rule dialog box.



- 6 Click the browse button next to the *Use This Image* field to select a Workstation Image object (for more information, see “[Creating a Workstation Image Object](#)” on page 706), use the drop-down fields and operators to specify the conditions under which the selected image should be used (click *Help* for details), then click *OK*.

Repeat this step as many times as needed to specify the particular images that should be used under different conditions.

These rules are used by your ZENworks Imaging server to determine which image to put on workstations during unattended imaging operations. The various hardware configuration data specified in the rules is compared against the actual hardware configuration data detected by the Workstation ZENworks Imaging Engine on the workstation. To see this data for a particular workstation, boot it with the imaging boot CD or DVD in manual mode and issue the `img info` command or enter `img`, then select *Information* from the menu.

Take care to choose rules that apply only to the workstations you want imaged. Otherwise, an image could be pushed to another workstation unintentionally.

- 7 (Conditional) If you are using Preboot Services but previously booted workstations from a ZENworks partition, you can disable the ZENworks partition on the Imaging Partition property page (click the down-arrow next to *Work To Do*, click *Imaging Partition*, then select the *Disable the ZENworks Imaging Partition, If It Exists* check box). The partition is disabled but is not removed with this option.
- 8 (Optional) If you want to specify the availability of the PXE menu, which is displayed when you boot a PXE-enabled workstation, click the *PXE Settings* tab, then select an option. Click *Help* for details.

If you want to specify a different image when using Preboot Services, rather than the default image that is defined, specify the image file and pathname.
- 9 Click *OK* to save the policy.
- 10 On the properties of the Server Package, click the *Associations* tab, add the container, Workstation Group, or Workstation objects that represent the target set of workstations, then click *OK*.

Remember that the policy won't actually be consulted by the ZENworks Imaging server unless you (or another administrator) flag a Workstation object to receive an image on the next boot.

58.3 Allowing Overwriting Filenames and Restricting the Save Location of Image Files (Imaging Server Settings)

Most of the rules that comprise an Imaging Server policy apply only when the ZENworks Imaging server is servicing a request to auto-image a workstation. Such rules aren't in force when the ZENworks Imaging server is servicing a manual (command line or menu) imaging request.

However, the following two aspects of the Imaging Server policy are actually ZENworks Imaging server settings that always apply, including when the ZENworks Imaging server is servicing an automatic imaging request, when the ZENworks Imaging server is servicing a manual imaging request, when registered workstations are booting, and when unregistered workstations are booting:

- Whether to allow the creation of new image files that overwrite existing image files on the server
- Whether to restrict the creation of new image files on the server to specific areas

To define these general behaviors for one or more ZENworks Imaging servers:

- 1** If a Server Package hasn't already been created to hold the policies for the target ZENworks Imaging servers, create one as instructed in [Chapter 11, "Creating Policy Packages," on page 143](#).
- 2** Right-click the Server Package, then click *Properties*.
- 3** Enable the Imaging Server policy, then click *Properties*.
- 4** Fill in the items on the *Security* tab. Click *Help* for details.
- 5** Click *OK* to save the policy.
- 6** On the Associations page, add the containers and server objects that represent the target set of ZENworks Imaging servers.
- 7** Click *OK* to save the association.

Novell® ZENworks® Desktop Management provides tools for creating and compressing images of workstation hard disks as well as images of specific add-on applications or file sets. Desktop Management also provides tools for customizing such images and for making images available to auto-imaging operations through Novell eDirectory™.

Desktop Management Imaging supports devices that physically connect to the network and that meet the minimum requirements for workstations. For more information, see “[User Workstation Hardware Requirements](#)” in the “[Novell ZENworks 7 Desktop Management Installation Guide](#)”. Desktop Management Imaging does not support imaging operations (creating or restoring images) using wireless connectivity.

NOTE: Desktop Management Imaging does not support workstations running boot managers, such as System Commander. Boot managers create their own information in the MBR and overwrite the ZENworks boot system, which prevents the workstation from communicating with the ZENworks Imaging server. If you are using boot managers in your environment, you should disable or remove them before performing imaging operations.

The following sections explain how to perform these tasks:

- [Section 59.1, “Creating a Workstation \(Base\) Image,” on page 703](#)
- [Section 59.2, “Creating an Add-On Image,” on page 704](#)
- [Section 59.3, “Using Image Explorer to Customize an Image,” on page 704](#)
- [Section 59.4, “Making an Image Available for Automatic Imaging,” on page 706](#)
- [Section 59.5, “Performing an Automatic Imaging Creation or Restoration,” on page 709](#)

59.1 Creating a Workstation (Base) Image

A base image is an image of all partitions and data on a source workstation’s storage devices, such as hard disks. Normally, such an image is prepared with the intent to completely replace the contents of a target workstation’s storage devices.

The overall process to create a base image is:

1. Boot the source workstation from an imaging method.
2. Run the Desktop Management Workstation ZENworks Imaging Engine to take an image of the workstation.

You can do this manually or automatically. In manual mode, you interrupt the boot process and issue an imaging command at the Linux prompt. For more information, see [Section 60.1, “Manually Taking an Image of a Workstation,” on page 711](#). In automatic mode, you set a flag in the workstation’s Workstation object using Novell ConsoleOne® and then let the boot process proceed without interruption. For more information, see [Section 59.5, “Performing an Automatic Imaging Creation or Restoration,” on page 709](#).

59.2 Creating an Add-On Image

An add-on image is an archived collection of files to be applied to an existing Windows installation on a target workstation. This is sometimes referred to as an application overlay. The existing partitions and files on the target workstation are left intact, except for any files that the add-on image might update.

An add-on image typically corresponds to an application or utility, or simply to a set of data files or configuration settings. There are two ways to create an add-on image, each resulting in a different kind of add-on image:

- Produce the add-on image from an Application object

You do this in ConsoleOne by using the Imaging property page (on the *Common* tab) of the Application object. For details, click *Help* on that property page.

An add-on image created in this manner is not fully installed on the target workstation until after the workstation reboots from being imaged, the user logs in locally, and Application Launcher/Explorer starts up and force runs the new Application object. Deploying the image is essentially another way to distribute an Application object.

- Drag files into a new image archive using Image Explorer

You do this by starting Image Explorer, dragging files and folders from an existing Windows installation into the new image archive, and saving the archive to a file with a `.zmg` extension (case-sensitive). For more information, see [Section 63.1, “Image Explorer \(imgexp.exe\),” on page 737](#).

Generally, an add-on image created in this manner doesn’t require any post-processing on the target workstation. It is simply a set of files that are copied to the appropriate locations on the hard disk, much like what happens when you unzip a WinZip archive. One exception is that the add-on image can contain Windows registry (`.reg`) files that are applied to the registry automatically when the workstation reboots after being imaged, if the ZENworks Imaging Windows Agent is installed on the workstation. For more information, see [Section 59.3, “Using Image Explorer to Customize an Image,” on page 704](#).

59.3 Using Image Explorer to Customize an Image

After you have created a base or add-on image as explained in the previous sections, you can customize it using the Image Explorer utility. Specifically, you can:

- **Compress the image:** You can compress an image (including images created by previous versions of Desktop Management) by 40-60% of the original file size, if you have not done so already during the imaging process.

There are three compression options: *Optimize for Speed* takes the least amount of time but creates the largest compressed image file; *Optimize for Space* creates the smallest image file but might take a significant amount of time; and, *Balanced* is a compromise between compression time and image file size. The *Balanced* option is used by default if you compress an image when it is created.

Image Explorer provides the following compression methods:

- **Compress:** Use this option to compress an image file that you currently have open in Image Explorer. For more information, see [“Compressing an Open Image” on page 741](#).
- **QuickCompress:** Use this option to compress an image file without waiting for the file to fully load into Image Explorer. For more information, see [“Compressing Any Image without Waiting for the File to Fully Load into Image Explorer” on page 741](#).

You can also use the options on the ZENworks Imaging Configuration property page for the workstation object in ConsoleOne to specify compression options if you do not want the default setting, which is *Balanced*.

- **Split the image:** You can specify a workstation image file that you want to split into separate files so that the entire image can be spanned across several CDs or DVDs. Splitting a workstation image is helpful for putting down or restoring images in a disconnected environment. For more information, see [“Splitting an Image” on page 742](#).
- **Resize a partition in an image:** For workstation (base) images, you can edit the value in the *Original Size* text box to allow you to change how big the ZENworks Imaging Engine makes the partition when the image is restored. For more information, see [“Resizing a Partition in an Image” on page 742](#).
- **Purge deleted files:** Excluded or hidden files and folders can be completely removed from an open image. This saves space in the image if you no longer want to include the files. For more information, see [“Excluding a File or Folder from the Open Image” on page 739](#).
- **Exclude individual files and folders from the image:** In doing this, you create file sets of the image by specifying which of ten possible sets to exclude a given file or folder from. The file sets exist merely as internal attributes of the same image archive. For more information, see [“Purging Files and Folders Marked for Deletion from the Open Image” on page 740](#).

IMPORTANT: Do not exclude BPB files from a base image or the workstation won't be able to boot the new operating system after receiving the image.

- **Add files and folders to the image:** By default, any file or folder you add is included in all file sets. To change this, you must explicitly exclude the file or folder from one or more file sets. For more information, see [“Adding a File or Folder to an Open Image” on page 739](#).
- **Add Windows registry (.reg) files:** The registry settings contained in the .reg files that you add are applied after the image is put down and the target workstation reboots to Windows, if the ZENworks Imaging Windows Agent is installed on the workstation.

As with any other file or folder that you add, a .reg file is included in all file sets of the image unless you explicitly exclude it from one or more file sets. For more information, see [“Adding Specific Windows Registry Settings That Are to Be Applied After the Open Image Is Laid Down” on page 739](#).

To start Image Explorer as a Windows standalone utility:

- 1 Double-click the `imgexp.exe` file located on the ZENworks Imaging server at:

- **Linux:** `/opt/novell/zenworks/zdm/winutils/nls/language`

The Image Explorer utility must be run on a Windows device. You need Samba running on the Linux ZENworks Imaging server where the utility file is located in order for the Windows machine to have access to it.

- **NetWare:** `sys:\public\zenworks\imaging`

The Image Explorer utility must be run on a Windows device. You need a drive mapped to the NetWare server where the utility file is located in order for the Windows machine to have access to it.

- **Windows:** `zenworks\imaging`

or

To start the utility from Novell ConsoleOne[®] from the server, click *Tools > ZENworks Utilities > Imaging > Image Explorer*.

59.4 Making an Image Available for Automatic Imaging

When you boot a workstation from an imaging method and allow the boot process to proceed in auto-imaging mode, the imaging operation that is performed on the workstation is determined by policies and settings that you define in eDirectory.

In order to make an image available to such operations, you must expose it as a Workstation Image object in eDirectory. Otherwise, when you define imaging policies and settings in eDirectory, you won't have any way to refer to the image.

Creating a Workstation Image object also allows you to combine a base image and one or more add-on images into a single entity that can be put down on target workstations. You can specify a standard image file to put down, or you can create a script to further customize your imaging operation. You can also specify that a particular file set of an image be used.

The sections that follow give instructions for performing these tasks:

- [Section 59.4.1, “Creating a Workstation Image Object,” on page 706](#)
- [Section 59.4.2, “Associating an Add-On Image with a Base Image,” on page 707](#)
- [Section 59.4.3, “Using a File Set of an Image,” on page 708](#)

59.4.1 Creating a Workstation Image Object

- 1 Create the base image that the Workstation Image object will refer to.

For more information, see [Section 59.1, “Creating a Workstation \(Base\) Image,” on page 703](#).

Although it isn't typical, you can create a Workstation Image object that refers only to one or more add-on images. However, if you want a base image to be put down in the same operation as the add-on images, you should include both types of images in the Workstation Image object.

- 2 Copy the image file to a ZENworks Imaging server that is accessible as a server object in your eDirectory tree.
- 3 In ConsoleOne, open the eDirectory tree and browse to the container where you want to create the Workstation Image object.
- 4 Right-click the container, click *New*, click *Object*, select *Workstation Image* from the list of object classes, then click *OK*.

- 5 Specify a name for the new object.

Example: Dell Image

- 6 Click *Define Additional Properties*, then click *OK*.

- 7 Click *Use Standard Imaging*.

or

Click *Use Scripted Imaging*, then specify the script you want to use. See the F1 help for examples of how you can use scripts. Skip to **Step 10**.

You can perform scripted imaging operations from the bash prompt by using the `imaging.s` command.

- 8 Under *Base Image File*, click the browse button next to the field, select the ZENworks Imaging server where the image resides, select or specify the path and filename of the image, then click *OK*.

For details on selecting or specifying the path and filename, click *Help* in the Image File Location dialog box.

If the Workstation Image object consists only of add-on images, leave the *Base Image File* field blank, and skip to **Step 5** of “**Associating an Add-On Image with a Base Image**” on page 707.

- 9 (Conditional) If you are using Preboot Services but formerly booted from ZENworks partitions on workstations, you can delete the ZENworks partition at the same time you put down an image. To do so, select the *Delete the ZENworks Imaging Partition, If It Exists, When Bringing Down The Base Image* check box. You can delete the ZENworks partition only when the workstation is booted from an imaging boot device or method other than the ZENworks partition.

IMPORTANT: After you have deleted the ZENworks partition, you need to make sure that the image you put on the workstation was made on a workstation without a ZENworks partition. Otherwise, the wrong MBR (Master Boot Record) is restored, and the workstation fails to boot. In addition, if you remove the ZENworks partition from a Windows 2000/XP machine, Windows cannot boot. You should only remove the ZENworks partition if you are going to restore an image to the workstation.

- 10 Click *OK* to save the Workstation Imaging object.

59.4.2 Associating an Add-On Image with a Base Image

- 1 Create the add-on image to associate with the base image. For more information, see **Section 59.2, “Creating an Add-On Image,”** on page 704.
- 2 Copy the image file to a ZENworks Imaging server that is accessible as a server object in your eDirectory tree.
You might want to copy the add-on image to the same location as the base image.
- 3 In ConsoleOne, open the eDirectory tree and browse to the Workstation Image object that refers to the base image. If you haven’t created this object yet, do so as instructed in “**Creating a Workstation Image Object**” on page 706.
- 4 Right-click the object, then click *Properties*.

- 5 Under *Add-on Image Files*, click the *Add* button, select the ZENworks Imaging server where the add-on image resides, select or specify the path and filename of the image, then click *OK*.

For details on selecting or specifying the path and filename, click *Help* in the Image File Location dialog box.

You can associate more than one add-on image with a base image. The add-on images are put down after the base image in the order listed on this page.

- 6 Click *OK* to save the Workstation Imaging object.

59.4.3 Using a File Set of an Image

As explained in [Section 59.3, “Using Image Explorer to Customize an Image,” on page 704](#), you can exclude individual files and folders from any of 10 possible file sets of an image. The file sets exist merely as internal attributes of the same image archive.

Because creating an image of a workstation can take time, it is more efficient in some cases to just create an image of a few workstations and customize those images to get all of the file sets you need. Even though the file sets do not all exist as separate, physical image files, you can access them as though they are. How you do this depends on whether you are performing a manual or automated imaging operation, as explained below.

Table 59-1 *File Sets for Imaging Operations*

Type of imaging operation	How to specify the file set to use
Automatic (eDirectory-based)	<p>In the Workstation Image object, specify the number of the file set in the <i>Use File Set</i> field. All eDirectory policies and settings that specify that the Workstation Image object use the specified file set.</p> <p>You can create multiple Workstation Image objects that point to the same base image but to different file sets.</p>
Manual (commandline or menu)	<p>Use the <i>s</i> parameter on the <i>img restore</i> command. For example, to specify file set number 3:</p> <pre>img restore1 dellnt4.zmg s3</pre> <p>or</p> <p>Enter <i>img</i> at the bash prompt to display a menu, select <i>Restore an Image</i>, then select <i>Local Image</i>. Specify <i>sfileset</i> (for example, <i>s3</i>) in the <i>Advanced Parameters</i> field.</p> <p>For details, see “ZENworks Imaging Engine Commands” on page 773.</p>

59.5 Performing an Automatic Imaging Creation or Restoration

The following procedure explains how to use ConsoleOne to set a flag in the Workstation object that indicates to take or put an image on the workstation the next time it is booted, and then verify that the imaging operation occurs as expected.

- 1 If the imaging operation that you want to trigger is to put an image on the workstation, do the following. Otherwise, skip this step.
 - 1a If you haven't already done so, create the image to be put on the workstation. Make sure to store it on your ZENworks Imaging server. For more information, see [Section 60.1, "Manually Taking an Image of a Workstation,"](#) on page 711.
 - 1b In ConsoleOne, create a Workstation Image object in your eDirectory tree. Configure the object to point to the image file that is to be put on the workstation. For more information, see ["Creating a Workstation Image Object"](#) on page 706. For details on pointing to the image file, click *Help* in the Image File Location dialog box.
- 2 In ConsoleOne, right-click the Workstation object, then click *Properties*.
- 3 On the ZENworks Imaging Configuration page, do either of the following:
 - To take an image of the workstation the next time it boots, select the first check box, click the browse button next to the available field, select your ZENworks Imaging server and the path and filename under which to store the new image, select the *Use Compression* check box and select a compression option if you want to use compression (click *Help* for details), then click *OK*.
 - To put an image on the workstation the next time it boots, select the *Put an Image on This Workstation on Next Boot* check box, select the box that says to use an image other than the effective policy image or multicast session, click the browse button next to the available field, select the Workstation Image object you created in [Step 1b](#), then click *OK*.

IMPORTANT: Be sure that the ZENworks Imaging server storing the image or the workstation receiving the image has enough disk space for the image. Otherwise, you receive a "Failed to write to proxy" error.

- 4 Click *OK* to save the imaging configuration settings.

After the imaging operation has been performed on the workstation, Desktop Management clears these imaging configuration settings automatically so that the imaging operation won't keep recurring.

- 5 Verify that the imaging operation occurs as expected when you reboot the workstation.

When you put a base image and its add-on images on a workstation, if you abort the process after the base image is put down, or if one of the add-on images fails, the ZENworks Imaging Engine reports a "successful image" to Linux.

For example, suppose the base image containing the new OS is successfully laid down and one or more of the add-on images fails. In order for the workstation to reboot to the new OS, the ZENworks Imaging server must report to Linux that the image was successful.

If any add-on images are not successfully laid down, the job is not marked as complete in ConsoleOne. You can see the last base image and the last add-on images that are successfully laid down by looking at the workstation object's properties in ConsoleOne (right-click the Workstation object, click the down-arrow on the *ZENworks Imaging* tab, then click *History*).

Performing Manual Imaging Operations

60

The following sections provide instructions for these basic imaging operations:

- [Section 60.1, “Manually Taking an Image of a Workstation,” on page 711](#)
- [Section 60.2, “Manually Putting an Image on a Workstation,” on page 715](#)

These instructions assume that you have already prepared the ZENworks Imaging server (see [Chapter 54, “Preparing a ZENworks Imaging Server,” on page 629](#)), prepared workstations for imaging (see [Chapter 57, “Setting Up Workstations for Imaging,” on page 693](#)), and set up imaging policies ([Chapter 58, “Setting Up Imaging Policies,” on page 697](#)).

Desktop Management Imaging supports devices that physically connect to the network and that meet the minimum requirements for workstations. For more information, see “[User Workstation Hardware Requirements](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*. Desktop Management Imaging does not support imaging operations (creating or restoring images) using wireless connectivity.

60.1 Manually Taking an Image of a Workstation

This section explains how to take an image of a workstation by booting from an imaging method and entering a particular imaging command. The image is stored on your ZENworks Imaging server.

If you want to store an image locally rather than on an ZENworks Imaging server, see [Section 61.1, “Using a CD or DVD for Disconnected Imaging Operations,” on page 719](#) and [Section 61.2, “Using a Hard Disk or Jaz Drive for Disconnected Imaging Operations,” on page 721](#).

Make sure that your ZENworks Imaging server has enough disk space for the image. Otherwise, you receive a “Failed to write to proxy” error.

- [Section 60.1.1, “Using the Bash Prompt to Manually Take an Image of a Workstation,” on page 711](#)
- [Section 60.1.2, “Using the ZENworks Imaging Engine Menu to Manually Take an Image of a Workstation,” on page 713](#)

60.1.1 Using the Bash Prompt to Manually Take an Image of a Workstation

1 Boot the workstation using one of the following methods:

- If the workstation is PXE-enabled, boot it from the ZENworks Imaging server. For more information, see [Section 55.1, “Using Preboot Services \(PXE\),” on page 631](#).
- Boot the workstation using an Imaging boot CD or DVD. For more information, see [Section 55.2, “Preparing Imaging Boot CDs or DVDs,” on page 632](#).
- Boot the workstation from the Imaging hard-disk partition. For more information, see [Section 55.4, “Creating an Imaging Hard-Disk Partition,” on page 635](#).

- 2 Enter `manual` at the boot prompt.

or

Select *Start ZENworks Imaging in Maintenance Mode* from the PXE menu.

- 3 (Optional) At the bash prompt, type `img dump`, then press Enter.

This displays a list of the partition slots on the workstation. For your reference, note the number and type of partitions and which one is active.

- 4 Enter a command at the bash prompt using one of the following formats:

- To create an image and store it on the ZENworks Imaging server, enter:

```
img makep serverIPAddr_or_DNSname //uncpath/newimg.zmg  
[comp=comp level]
```

The `makep` parameter stands for “make on proxy,” or in other words, create an image and store it on the imaging (proxy) server.

The IP address or DNS name should be that of your ZENworks Imaging server. This can be any server running the Imaging Proxy service.

The `.zmg` filename extension is case-sensitive and must be all lowercase.

The UNC path to the image file to retrieve, including image filename and `.zmg` extension. The format of this UNC path is as follows:

```
//servername/volume_or_share/path_to_stored_images/  
imagename.zmg
```

When `img makep` is executed at the command line, the *servername* portion of this path is replaced with the value in the address portion of the path.

For OES Linux, the path to the image file must be from root (/). For example, the path might look like:

```
//servername/media/nss/NSS_volume/path_to_image/  
imagefilename.zmg
```

The directories in the path must exist. You can use the following characters in the path and filename:

- Letters: a through z (uppercase and lowercase)
- Numbers
- Special Characters: \$ % ' - _ @ { } ~ ` ! # ()

comp level is the amount of compression used when creating the image. Specify any number from 0-9. 0 means no compression. 1 is the same as Optimize for Speed and is used by default if you do not specify this parameter. 6 is the same as Balanced. 9 is the same as Optimize for Space. (Optimize for Speed takes the least amount of time but creates the largest image file. Optimize for Space creates the smallest image file but might take a significant amount of time. Balanced is a compromise between compression time and image file size.)

For example:

```
img makep 137.65.95.127 //xyz_srv/sys/imgs/cpqnt.zmg comp=6
```

- To create an image and store it locally: enter:

```
img makel filepath [comp=comp level]
```

The `makel` parameter stands for “make locally,” or in other words, create an image and store it on a local (writable) device, such as a hard disk or Jaz drive.

Unless you mount a drive before using the `makel` command, the image is created in RAM and is lost during a reboot of the workstation.

filepath is the image filename, including the `.zmg` extension (case-sensitive) and the complete path from the root of the partition.

The directories in the path must exist. You can use the following characters in the path and filename:

- Letters: a through z (uppercase and lowercase)
- Numbers
- Special Characters: \$ % ' - _ @ { } ~ ` ! # ()

comp level is the amount of compression used when creating the image. Specify any number from 0-9. 0 means no compression. 1 is the same as Optimize for Speed and is used by default if you do not specify this parameter. 6 is the same as Balanced. 9 is the same as Optimize for Space. (Optimize for Speed takes the least amount of time but creates the largest image file. Optimize for Space creates the smallest image file but might take a significant amount of time. Balanced is a compromise between compression time and image file size.)

For example:

```
img makel /imgs/dellnt.zmg comp=6
```

IMPORTANT: Make sure to use forward slashes in the UNC path as shown above. Backslashes aren't recognized by Linux. Alternatively, you can use backslashes and enclose the entire UNC path in quotes. The path you specify must exist on your ZENworks Imaging server.

For more information on the parameters you can use and usage examples, see [Section 64.3, "Make Mode \(img make\)," on page 775](#).

Depending on the amount of data on the hard disk, the image might take several minutes to create. If the screen goes blank, just press any key. (Linux enters a screen-saving mode after a few minutes.)

- 5 After the image is created and the bash prompt is displayed, Remove any CD or DVD from the drive and reboot the workstation.
- 6 (Optional) Verify that the image file was created on your ZENworks Imaging server. You might also want to check its size.

60.1.2 Using the ZENworks Imaging Engine Menu to Manually Take an Image of a Workstation

- 1 Boot the workstation using one of the following methods:
 - If the workstation is PXE-enabled, boot it from the ZENworks Imaging server. For more information, see [Section 55.1, "Using Preboot Services \(PXE\)," on page 631](#).
 - Boot the workstation using an Imaging boot CD or DVD. For more information, see [Section 55.2, "Preparing Imaging Boot CDs or DVDs," on page 632](#).
 - Boot the workstation from the Imaging hard-disk partition. For more information, see [Section 55.4, "Creating an Imaging Hard-Disk Partition," on page 635](#).

- 2 Enter `manual` at the boot prompt.
or
Select *Start ZENworks Imaging in Maintenance Mode* from the PXE menu.
- 3 Enter `img` to display the ZENworks® Imaging Engine menu.
- 4 (Optional) Click *System Information*, then click *Drive Information* to display a list of the partition slots on the workstation.
For your reference, note the number and type of partitions and which one is active.
- 5 Click *Imaging*, then click *Make Image*.
- 6 In the Make Image Wizard window, specify the destination where the image is to be stored (Local or Server), then click *Next*.
The directories in the path must exist. You can use the following characters in the path and filename:
 - Letters: a through z (uppercase and lowercase)
 - Numbers
 - Special Characters: \$ % ' - _ @ { } ~ ` ! # ()
- 7 Browse to and specify the path to the image archive.
- 8 Select the partitions that you want to include in the image.
- 9 Select a compression option.
None: No compression is used.
Speed: Takes the least amount of time to compress but creates the largest compressed image file. This option is used by default when an image is created.
Balanced: Represents a compromise between compression time and image file size.
Size: Creates the smallest image file but takes longer to compress.
- 10 Click *Next*.
- 11 (Optional) Fill in the fields:
Author: The name of the person creating this image.
Computer: The name of the computer being imaged.
Image Description: A description of the image.
Comments: Any additional comments about the image.
- 12 Click *Next*.
Depending on the amount of data on the hard disk, the image might take several minutes to create. If the screen goes blank, just press any key. (Linux enters a screen-saving mode after a few minutes.)
- 13 After the image is created, exit from the ZENworks Imaging Engine menu, remove any CD or DVD from the drive, then reboot the workstation.
- 14 (Optional) Verify that the image file was created on your ZENworks Imaging server. You might also want to check its size.

60.2 Manually Putting an Image on a Workstation

The section explains how to put an image on the workstation by booting from an imaging method and entering a particular imaging command. The image is retrieved from your ZENworks Imaging server.

Make sure that the workstation receiving a new image has enough disk space for the image. Otherwise, you receive a “Failed to write to proxy” error.

- [Section 60.2.1, “Using the Bash Prompt to Manually Put an Image on a Workstation,” on page 715](#)
- [Section 60.2.2, “Using the ZENworks Imaging Engine Menu to Manually Put an Image on a Workstation,” on page 717](#)

60.2.1 Using the Bash Prompt to Manually Put an Image on a Workstation

- 1 If you haven’t already done so, create the image to put on the workstation, as instructed in [Section 60.1, “Manually Taking an Image of a Workstation,” on page 711](#).

Make sure that the image is of the same type of workstation (same hardware configuration) and is stored on your ZENworks Imaging server. You can use a previous image of the same workstation.

IMPORTANT: If you are putting an image on a workstation without a ZENworks partition, make sure the image was made on a workstation without a ZENworks partition. Otherwise, the wrong MBR (Master Boot Record) is restored, and the workstation fails to boot.

- 2 (Optional) Boot the workstation from a Windows startup disk and run FDISK to remove all partitions from the hard disk.

Running FDISK is not required, but it is recommended for purposes of comparing the workstation’s partitions before and after the imaging operation.

- 3 Boot the workstation using one of the following methods:

- If the workstation is PXE-enabled, boot it from the ZENworks Imaging server. For more information, see [Section 55.1, “Using Preboot Services \(PXE\),” on page 631](#).
- Boot the workstation using an Imaging boot CD or DVD. For more information, see [Section 55.2, “Preparing Imaging Boot CDs or DVDs,” on page 632](#).
- Boot the workstation from the Imaging hard-disk partition. For more information, see [Section 55.4, “Creating an Imaging Hard-Disk Partition,” on page 635](#).

- 4 Enter `manual` at the boot prompt.

- 5 (Optional) At the bash prompt, type `img dump`, then press Enter to display a list of the partition slots on the workstation.

For your reference, note the number and type of partitions and which one is active. If you removed all partitions using FDISK, each slot should be empty and none should be active.

6 Enter a command at the bash prompt using one of the following formats:

- To restore an image from the ZENworks Imaging server and put it down on a workstation, enter:

```
img restorep serverIPaddr_or_DNSname //uncpath/newimg.zmg
```

The `restorep` parameter stands for “restore from proxy,” or in other words, retrieve an image from the Imaging (proxy) server and put it on this workstation. The IP address or DNS name should be that of your ZENworks Imaging server, and the UNC path specifies the location and filename where the image is to be retrieved from.

For example:

```
img restorep 137.65.95.127 //xyz_srv/sys/imgs/cpqnt.zmg
```

- To retrieve an image from a local device and put it down on a workstation:

```
img restorel filepath
```

The `restorel` parameter stands for “restore from local,” or in other words, retrieve an image from a local device and put it on this workstation. *filepath* represents the filename of the image to retrieve, including the `.zmg` extension (case-sensitive) and the complete path from the root of the partition.

IMPORTANT: Make sure to use *forward slashes* in the UNC path as shown above. Backslashes aren’t recognized by Linux. Alternatively, you can use backslashes and enclose the entire UNC path in quotes. The server portion of the path must be the name of your ZENworks Imaging server.

If you want to manually restore an image from a directory that uses extended or double-byte characters in its name, you should perform an automatic image restoration using Novell® ConsoleOne®. For more information, see [Section 59.5, “Performing an Automatic Imaging Creation or Restoration,” on page 709](#).

For more information on the parameters you can use and usage examples, see [Section 64.4, “Restore Mode \(img restore\),” on page 778](#).

Depending on the size of the image, it might take several minutes to put the image down. Images actually take slightly longer to put down than they do to take. If the screen goes blank, just press any key. (Linux enters a screen-saving mode after a few minutes.)

7 (Optional) After the image is put down and the bash prompt is displayed, type `img dump`, then press Enter.

As before, this displays a list of the partition slots on the workstation. You should now see information about the new partitions that are created and activated by the image that you just put down.

8 At the bash prompt, type `lilo.s`, then press Enter.

9 Remove any CD or DVD from the drive and reboot the workstation and verify that it boots to the operating system that was installed by the new image.

60.2.2 Using the ZENworks Imaging Engine Menu to Manually Put an Image on a Workstation

- 1 If you haven't already done so, create the image to put on the workstation, as instructed in [Section 60.1, "Manually Taking an Image of a Workstation," on page 711](#).

Make sure that the image is of the same type of workstation (same hardware configuration) and is stored on your ZENworks Imaging server. You can use a previous image of the same workstation.

IMPORTANT: If you are putting an image on a workstation without a ZENworks partition, make sure the image was made on a workstation without a ZENworks partition. Otherwise, the wrong MBR (Master Boot Record) is restored, and the workstation fails to boot.

- 2 (Optional) Boot the workstation from a Windows startup disk and run FDISK to remove all partitions from the hard disk.

Running FDISK is not required, but it is recommended for purposes of comparing the workstation's partitions before and after the imaging operation.

- 3 Boot the workstation using one of the following methods:

- If the workstation is PXE-enabled, boot it from the ZENworks Imaging server. For more information, see [Section 55.1, "Using Preboot Services \(PXE\)," on page 631](#).
- Boot the workstation using an Imaging boot CD or DVD. For more information, see [Section 55.2, "Preparing Imaging Boot CDs or DVDs," on page 632](#).
- Boot the workstation from the Imaging hard-disk partition. For more information, see [Section 55.4, "Creating an Imaging Hard-Disk Partition," on page 635](#).

- 4 Enter `manual` at the boot prompt.

or

Select *Start ZENworks Imaging in Maintenance Mode* from the PXE menu.

- 5 Enter `img` to display the ZENworks Imaging Engine menu.

- 6 (Optional) Click *System Information*, then click *Drive Information* to display a list of the partition slots on the workstation.

For your reference, note the number and type of partitions and which one is active. If you removed all partitions using FDISK, each slot should be empty and none should be active.

- 7 Click *Imaging*, then click *Restore Image*.

- 8 In the Restore Image Wizard window, specify the source location of the image (Local or Server), then click *Next*.

- 9 Browse to and specify the path to the image archive.

- 10 (Optional) Specify a file set.

- 11 (Optional) Specify any advanced options, such as `sfileset` or `apartition:ppartition`.

For details on this and other related `img` command parameters, see [Chapter 64, "ZENworks Imaging Engine Commands," on page 773](#).

- 12 Click *Next*.

Depending on the size of the image, it might take several minutes to put the image down. Images actually take slightly longer to put down than they do to take. If the screen goes blank, just press any key. (Linux enters a screen-saving mode after a few minutes.)

- 13** (Optional) Click *System Information*, then click *Drive Information* to display a list of the partition slots on the workstation.

As before, this displays a list of the partition slots on the workstation. You should now see information about the new partitions that are created and activated by the image that you just put down.

- 14** Exit the ZENworks Imaging Engine menu.
- 15** Run `lilo.s` from the bash prompt.
- 16** Remove any CD or DVD from the drive and reboot the workstation. Verify that it boots to the operating system that was installed by the new image.

Setting Up Disconnected Imaging Operations

61

Disconnected imaging operations are inherently manual in the sense that they don't involve the network and thus can't be automated through Novell® eDirectory™.

To perform a disconnected imaging operation on a workstation, you must have a storage device to hold the image to be created or put down, and that storage device must be locally accessible to the ZENworks® Imaging Engine (in Linux) when you boot the workstation from the imaging device. The following sections explain how to set up and perform disconnected operations using several different storage devices:

- [Section 61.1, “Using a CD or DVD for Disconnected Imaging Operations,” on page 719](#)
- [Section 61.2, “Using a Hard Disk or Jaz Drive for Disconnected Imaging Operations,” on page 721](#)

You can also use other storage devices providing that they are locally accessible to the ZENworks Imaging Engine (in Linux).

61.1 Using a CD or DVD for Disconnected Imaging Operations

Using Desktop Management, you can use CDs and DVDs only as the storage medium for an image to be put down, not for an image to be created.

You can put down an image from a bootable or non-bootable Imaging CD or DVD using either the bash prompt or using the ZENworks Imaging Engine menu.

- [Section 61.1.1, “Using the Bash Prompt to Put Down an Image,” on page 719](#)
- [Section 61.1.2, “Using the ZENworks Imaging Engine Menu to Put Down an Image,” on page 720](#)

61.1.1 Using the Bash Prompt to Put Down an Image

- 1 Use your CD- or DVD-burning software to burn the source image onto a CD or DVD.
- 2 Boot the workstation using one of the following methods:
 - If the workstation is PXE-enabled, boot it from the ZENworks Imaging server. For more information, see [Section 55.1, “Using Preboot Services \(PXE\),” on page 631](#).
 - Boot the workstation using an Imaging boot CD or DVD. For more information, see [Section 55.2, “Preparing Imaging Boot CDs or DVDs,” on page 632](#).
 - Boot the workstation from the Imaging hard-disk partition. For more information, see [Section 55.4, “Creating an Imaging Hard-Disk Partition,” on page 635](#).
- 3 Enter `manual` from the boot prompt.
- 4 Insert the CD or DVD that contains the source image.

- 5 At the Linux prompt, enter `cdrom.s` to mount the CD or DVD.

This mounts the CD or DVD to `/mnt/cdrom`.

- 6 Enter a command of the following format:

```
img restore1 /mnt/cdrom/path/image.zmg
```

where *path* and *image* are the path and filename of the image relative to the root of the CD or DVD.

- 7 After the imaging is done, remove the imaging device (if applicable) and do the following to boot the workstation with the new image:

- 7a At the Linux prompt, type `lilo.s`, then press Enter.

- 7b Press Ctrl+Alt+Delete.

If the workstation doesn't boot to the new operating system (that is, if the Linux prompt is displayed), enter the `lilo.s` command again and reboot the workstation a second time.

61.1.2 Using the ZENworks Imaging Engine Menu to Put Down an Image

- 1 Use your CD- or DVD-burning software to burn the source image onto a CD or DVD.
- 2 Boot the workstation using one of the following methods:
 - If the workstation is PXE-enabled, boot it from the ZENworks Imaging server. For more information, see [Section 55.1, "Using Preboot Services \(PXE\)," on page 631](#).
 - Boot the workstation using an Imaging boot CD or DVD. For more information, see [Section 55.2, "Preparing Imaging Boot CDs or DVDs," on page 632](#).
 - Boot the workstation from the Imaging hard-disk partition. For more information, see [Section 55.4, "Creating an Imaging Hard-Disk Partition," on page 635](#).

- 3 Enter `manual` from the boot prompt.

- 4 Insert the CD or DVD that contains the source image.

- 5 At the Linux prompt, enter `cdrom.s` to mount the CD or DVD.

This mounts the CD or DVD to `/mnt/cdrom`.

- 6 Enter `img` to display the ZENworks Imaging Engine menu.

- 7 Click *Imaging*, then click *Restore Image*.

- 8 Click *Local*, then click *Next*.

- 9 Browse to and specify the path to the image archive.

- 10 (Optional) Specify a file set.

- 11 (Optional) Specify any advanced options, such as `sfileset` or `apartition:ppartition`.

For details on this and other related `img` command parameters, see [Chapter 64, "ZENworks Imaging Engine Commands," on page 773](#).

- 12 Click *Next*.

Depending on the size of the image, it might take several minutes to put the image down. Images actually take slightly longer to put down than they do to take. If the screen goes blank, just press any key. (Linux enters a screen-saving mode after a few minutes.)

13 After the imaging is done, remove the imaging device (if applicable) and do the following to boot the workstation with the new image:

13a At the Linux prompt, type `lilo.s`, then press Enter.

13b Press Ctrl+Alt+Delete.

If the workstation doesn't boot to the new operating system (that is, if the Linux prompt is displayed), enter the `lilo.s` command again and reboot the workstation a second time.

61.2 Using a Hard Disk or Jaz Drive for Disconnected Imaging Operations

When you boot a workstation from a Desktop Management Workstation Imaging device, you can create an image on, or put down an image from, any primary FAT16, FAT32, EXT2, or EXT3 partition on an IDE or SCSI hard drive or Iomega* Jaz drive. You can also use the local ZENworks partition if one is installed. Any target partition must have sufficient space.

When you create an image, the partition where you store the image is itself excluded from the image. When you put down an image, the source partition is not altered.

- [Section 61.2.1, “Creating an Image on a Hard Disk or Jaz Drive,” on page 721](#)
- [Section 61.2.2, “Putting Down an Image from a Hard Disk or Jaz Drive,” on page 723](#)

61.2.1 Creating an Image on a Hard Disk or Jaz Drive

You can create an image on a hard disk or Jaz drive using either the bash prompt or using the ZENworks Imaging Engine menu.

- [“Using the Bash Prompt to Create an Image” on page 721](#)
- [“Using the ZENworks Imaging Engine Menu to Create an Image” on page 722](#)

Using the Bash Prompt to Create an Image

1 Boot the workstation using one of the following methods:

- If the workstation is PXE-enabled, boot it from the ZENworks Imaging server. For more information, see [Section 55.1, “Using Preboot Services \(PXE\),” on page 631](#).
- Boot the workstation using an Imaging boot CD or DVD. For more information, see [Section 55.2, “Preparing Imaging Boot CDs or DVDs,” on page 632](#).
- Boot the workstation from the Imaging hard-disk partition. For more information, see [Section 55.4, “Creating an Imaging Hard-Disk Partition,” on page 635](#).

2 Enter `manual` from the boot prompt.

3 At the Linux prompt, enter `img dump` to view the available partitions.

Note the number of the FAT partition where you'll store the new image.

4 Enter a command of the following format:

```
img make1[pNumber] /path/image.zmg [comp=comp_level]
```

where *pNumber* is the number of the partition to store the image in, and *comp_level* is the amount of compression used when creating the image. Specify any number from 0-9. 0 means no compression. 1 is the same as Optimize for Speed. 6 is the same as Balanced and is used by default if you do not specify this parameter. 9 is the same as Optimize for Space. (Optimize for

Speed takes the least amount of time but creates the largest image file. Optimize for Space creates the smallest image file but might take a significant amount of time. Balanced is a compromise between compression time and image file size.) *Path* and *image* are the path and filename of the new image relative to the partition root. If you omit the partition number, the local ZENworks partition is used.

For details on other related `img` command parameters, see “ZENworks Imaging Engine Commands” on page 773.

Using the ZENworks Imaging Engine Menu to Create an Image

- 1 Boot the workstation using one of the following methods:
 - If the workstation is PXE-enabled, boot it from the ZENworks Imaging server. For more information, see [Section 55.1, “Using Preboot Services \(PXE\),” on page 631](#).
 - Boot the workstation using an Imaging boot CD or DVD. For more information, see [Section 55.2, “Preparing Imaging Boot CDs or DVDs,” on page 632](#).
 - Boot the workstation from the Imaging hard-disk partition. For more information, see [Section 55.4, “Creating an Imaging Hard-Disk Partition,” on page 635](#).
- 2 Enter `manual` from the boot prompt.
- 3 Enter `img` to display the ZENworks Imaging Engine menu.
- 4 (Optional) Click *System Information*, then click *Drive Information* to display a list of the partition slots on the workstation.

For your information, note the number of the FAT partition where you’ll store the new image.

- 5 Click *Imaging*, then click *Make Image*.
- 6 In the Make Image Wizard window, click *Local*, then click *Next*.
- 7 Browse to and specify the path to the image archive.
- 8 Select the partitions that you want to include in the image.
- 9 Select a compression option.

None: No compression is used.

Speed: Takes the least amount of time to compress but creates the largest compressed image file. This option is used by default when an image is created.

Balanced: Represents a compromise between compression time and image file size.

Size: Creates the smallest image file but takes longer to compress.

- 10 Click *Next*.
- 11 (Optional) Fill in the fields:
 - Author:** The name of the person creating this image.
 - Computer:** The name of the computer being imaged.
 - Image Description:** A description of the image.
 - Comments:** Any additional comments about the image.

- 12 Click *Next*.

Depending on the amount of data on the hard disk, the image might take several minutes to create. If the screen goes blank, just press any key. (Linux enters a screen-saving mode after a few minutes.)

- 13 After the image is created, exit from the ZENworks Imaging Engine menu, remove any CD or DVD from the drive, then reboot the workstation.
- 14 (Optional) Verify that the image file was created. You might also want to check its size.

61.2.2 Putting Down an Image from a Hard Disk or Jaz Drive

You can put down an image from a hard disk or Jaz drive using either the bash prompt or using the ZENworks Imaging Engine menu.

- [“Using the Bash Prompt to Put Down an Image” on page 723](#)
- [“Using the ZENworks Imaging Engine Menu to Put Down an Image” on page 723](#)

Using the Bash Prompt to Put Down an Image

- 1 Boot the workstation using one of the following methods:
 - If the workstation is PXE-enabled, boot it from the ZENworks Imaging server. For more information, see [Section 55.1, “Using Preboot Services \(PXE\),” on page 631](#).
 - Boot the workstation using an Imaging boot CD or DVD. For more information, see [Section 55.2, “Preparing Imaging Boot CDs or DVDs,” on page 632](#).
 - Boot the workstation from the Imaging hard-disk partition. For more information, see [Section 55.4, “Creating an Imaging Hard-Disk Partition,” on page 635](#).

2 Enter `manual` from the boot prompt.

3 (Optional) At the Linux prompt, enter `img dump` to view the available partitions.

For your information, note the number of the FAT partition where the source image is stored.

4 Enter a command of the following format:

```
img restore1[pNumber] /path/image.zmg
```

where *pNumber* is the number of the partition where the source image is stored, and *path* and *image* are the image path and filename relative to the partition root. If you omit the partition number, the local ZENworks partition is used.

For details on other related `img` command parameters, see [“ZENworks Imaging Engine Commands” on page 773](#).

5 After the imaging is done, remove the imaging device (if applicable) and do the following to boot the workstation with the new image:

5a At the Linux prompt, type `lilo.s`, then press Enter.

5b Press Ctrl+Alt+Delete.

If the workstation doesn't boot to the new operating system (that is, if the Linux prompt is displayed), enter the `lilo.s` command again and reboot the workstation a second time.

Using the ZENworks Imaging Engine Menu to Put Down an Image

- 1 Boot the workstation using one of the following methods:
 - If the workstation is PXE-enabled, boot it from the ZENworks Imaging server. For more information, see [Section 55.1, “Using Preboot Services \(PXE\),” on page 631](#).
 - Boot the workstation using an Imaging boot CD or DVD. For more information, see [Section 55.2, “Preparing Imaging Boot CDs or DVDs,” on page 632](#).

- Boot the workstation from the Imaging hard-disk partition. For more information, see [Section 55.4, “Creating an Imaging Hard-Disk Partition,” on page 635](#).

- 2 Enter `manual` from the boot prompt.
- 3 Enter `img` to display the ZENworks Imaging Engine menu.
- 4 (Optional) Click *System Information*, then click *Drive Information* to display a list of the partition slots on the workstation.

For your reference, note the number of the FAT partition where the source image is stored.

- 5 Click *Imaging*, then click *Restore Image*.
- 6 Click *Local*, then click *Next*.
- 7 Browse to and specify the path to the image archive.
- 8 (Optional) Specify a file set.
- 9 (Optional) Specify any advanced options, such as *sfileset* or *apartition:ppartition*.

For details on this and other related `img` command parameters, see [Chapter 64, “ZENworks Imaging Engine Commands,” on page 773](#).

- 10 Click *Next*.

Depending on the size of the image, it might take several minutes to put the image down. Images actually take slightly longer to put down than they do to take. If the screen goes blank, just press any key. (Linux enters a screen-saving mode after a few minutes.)

- 11 After the imaging is done, remove the imaging device (if applicable) and do the following to boot the workstation with the new image:

11a At the Linux prompt, type `lilo.s`, then press Enter.

11b Press Ctrl+Alt+Delete.

If the workstation doesn't boot to the new operating system (that is, if the Linux prompt is displayed), enter the `lilo.s` command again and reboot the workstation a second time.

Novell® ZENworks® Desktop Management Imaging software includes an imaging multicast capability. The following sections explain what this is, why you might want to use it, and the overall procedures for using it.

- [Section 62.1, “Understanding Multicasting,” on page 725](#)
- [Section 62.2, “Performing a Multicast Session,” on page 726](#)

62.1 Understanding Multicasting

To multicast an image is to take an image of one workstation (the master), immediately send it over the network to multiple other workstations (the participants), and put it down simultaneously on those workstations. You can specify a workstation as the session master, or you can specify an image file that you have previously saved and customized.

If the session master is a workstation, a base image is taken of all partitions on the hard disks and other storage devices (such as Jaz drives) of that workstation.

Before the image is put down on the participating workstations, all existing partitions are removed from the hard disks and writable storage devices of those workstations.

For multicasting to work properly, the routers and switches on the network must have multicast features configured. Otherwise, multicast packets might not be routed properly.

In versions of ZENworks for Desktops prior to 3.2, the master had to be a Linux workstation, which formerly restricted multicasting to exact “cloning” of the workstation.

- [Section 62.1.1, “Benefits of Multicasting Images,” on page 725](#)
- [Section 62.1.2, “Limitations of Multicasting Images,” on page 726](#)

62.1.1 Benefits of Multicasting Images

Multicasting is the way to use ZENworks Desktop Management Imaging services for mass re-imaging with the least amount of overhead. It is useful if you have one workstation with a clean software configuration that you want to duplicate on several other machines, or if you have a single image that you want to set up on multiple machines.

With multicasting, all you need is a physical network with modern routers and switches.

If you are setting up multicasting by visiting each workstation, you also need an imaging boot CD or DVD, or the workstations must be PXE-enabled. For more information, see [Chapter 55, “Preparing an Imaging Boot Method,” on page 631](#).

The workstations to be imaged must be physically connected to the network. They can be workstations with existing operating systems of any kind, or they can be new workstations with no operating system installed.

62.1.2 Limitations of Multicasting Images

One significant limitation of using multicast without installing any ZENworks Desktop Management software is that it results in a set of workstations that have duplicate network identities. The IP addresses, Computer (NETBIOS) names, Workgroup memberships, and Security Identifiers (Windows 2000/XP only) are all the same and can cause conflicts if deployed on the network without change.

For multicasting with a handful of workstations, this might not be a problem. But for a larger number, if the workstations have Windows, you should install the ZENworks Imaging Windows Agent on them before doing the multicast. (See [Step 3 of Section 57.2, “Enabling a Windows Workstation for Auto-Imaging Operations,” on page 694](#).) The ZENworks Imaging Windows Agent saves the workstation’s network identity settings before the multicast session and restores them afterwards.

62.2 Performing a Multicast Session

- [Section 62.2.1, “Initiating an Automatic Multicast Session in ConsoleOne,” on page 726](#)
- [Section 62.2.2, “Performing a Manual Multicast Session,” on page 729](#)

62.2.1 Initiating an Automatic Multicast Session in ConsoleOne

When you initiate an automatic multicast session in Novell ConsoleOne[®], you do not need to start the session from the ZENworks Imaging server or physically visit each participating workstation. You name the session, define the master image source (an image file or workstation), and then add Workstation objects to include in the multicast session or define rules to include workstations that meet specific criteria you set.

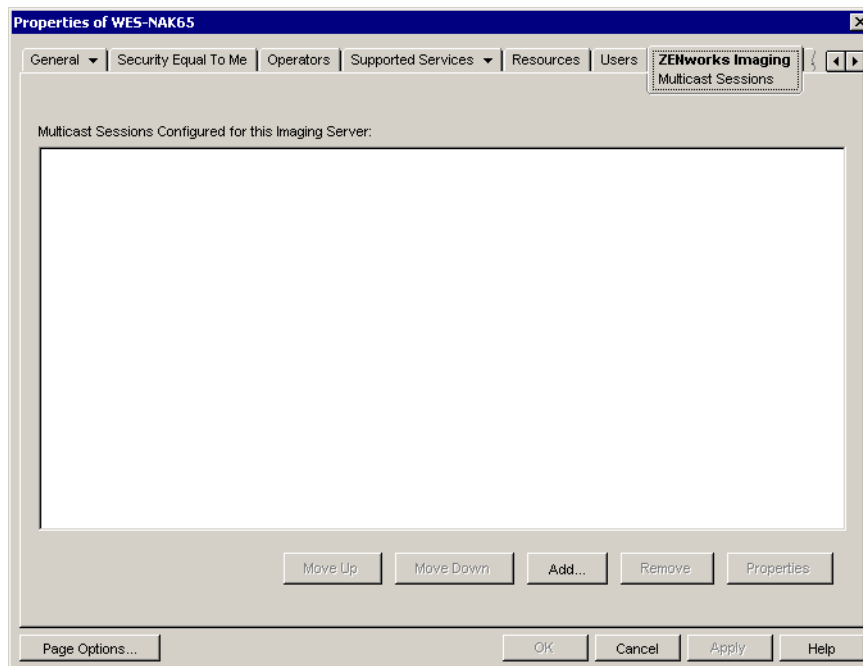
To initiate an automatic multicast session in ConsoleOne:

- 1 (Optional) Install the ZENworks Imaging Windows Agent on each of the participating workstations.

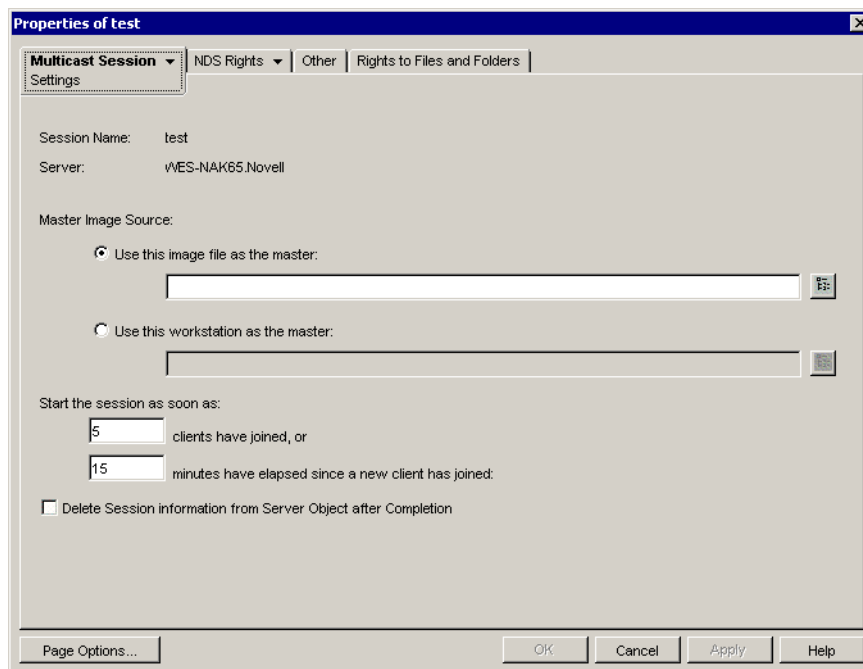
IMPORTANT: If you do not install the ZENworks Imaging Windows Agent on each participating machine, those machines will have duplicate network identities. For more information, see [“Limitations of Multicasting Images” on page 726](#).

- 2 In ConsoleOne, right-click the server object, click *Properties*, then click the *ZENworks Imaging* tab.

If you do not see the *ZENworks Imaging* tab, click the right-arrow on the right side of the displayed tabs until it is displayed.



- 3 Click *Add*, enter a name for the multicast session, then click *OK*.



- 4 Specify the *Master Image Source*.

You can specify an image file or a master workstation.

A workstation cannot be the master if it is being used as a master in another multicast session or if it explicitly participates in any other session.

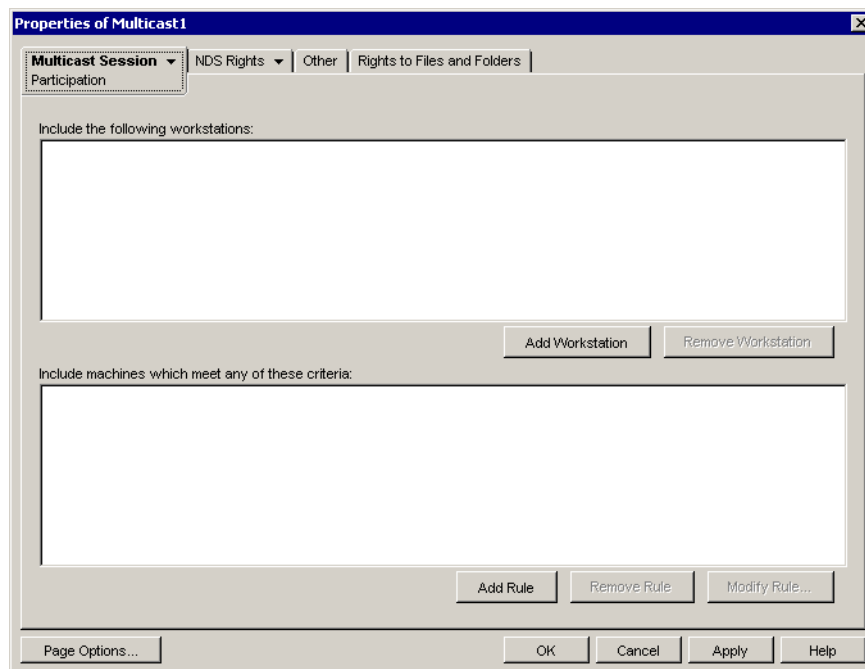
- 5 Decide how many participating workstations you want to have booted up before the multicast session begins. Specify this number in the *Clients Have Joined* text box.

The default if you do not specify a number is 5 workstations.

- 6 If not enough workstations have booted up to fulfill the Clients Have Joined requirement, the multicast session begins if a participating workstation boots up and a certain amount of time passes without another participating workstation booting. Specify this amount of time in the *Minutes Have Elapsed Since a New Client Has Joined* text box.

The default if you do not specify a time is 15 minutes.

- 7 (Optional) To delete the session after it has finished, select the last check box.
- 8 Click the down-arrow on *Multicast Session* tab, then click *Participation*.



- 9 Click *Add Workstation* under *Include the Following Workstations* to explicitly add the workstation objects that you want to include in this multicast session.

or

To create rules to select the workstations you want to participate in this multicast session, click *Add Rule* under *Include Machines Which Meet Any of These Criteria*.

The screenshot shows a 'New Rule' dialog box. It contains a list of criteria for including machines, each with a dropdown menu (all set to 'CPU'), a dropdown menu (all set to 'contains'), and a text input field. Below this is a 'Rule Description:' section with a text area containing 'CPU contains ""'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Click *Help* on the Participation page for more information.

- 10 Click *OK* to return to the ZENworks Imaging Multicast Sessions page.
- 11 The check box next to the multicast session name is automatically selected, showing that the session is enabled. If you want to disable a multicast session, deselect the check box next to the session name.
- 12 (Optional) If you want to change the position of a session in the list, select the multicast session name, then click *Move Up* or *Move Down*.

If multiple multicast sessions are defined that use rules to select participating workstations, it is possible that a workstation could qualify to participate in more than one session. If this occurs, the first enabled session in this list for which the workstation qualifies takes precedence over the other enabled sessions.

- 13 Click *OK*.

62.2.2 Performing a Manual Multicast Session

If you want to perform a manual multicast session, you need to start the multicast session from the ZENworks Imaging server (Linux, NetWare®, or Windows) and physically visit each participating workstation. Performing a manual multicast session is particularly useful in a lab environment in which a small number of workstations participate.

The following sections contain step-by-step information about performing a manual multicast session:

- “Initiating a Multicast Session from the ZENworks Imaging Server” on page 730
- “Initiating a Multicast Session from Each Client” on page 734

To perform a manual multicast session, you must perform the steps in both sections; however, the order in which you perform the tasks does not matter.

Initiating a Multicast Session from the ZENworks Imaging Server

You can use any ZENworks Imaging server to initiate a multicast session.

- “Initiating a Multicast Session from a Linux ZENworks Imaging Server” on page 730
- “Initiating a Multicast Session from a NetWare ZENworks Imaging Server” on page 732
- “Initiating a Multicast Session from a Windows ZENworks Imaging Server” on page 733

Initiating a Multicast Session from a Linux ZENworks Imaging Server

On the Linux ZENworks Imaging server, do the following to initiate the multicast session:

- 1 In the shell console, enter the following command to enable a multicast session:

```
/opt/novell/zenworks/preboot/bin/novell-zmgmcast -mcast arguments
```

where *arguments* represents the following:

Argument	Description
<i>session_name</i>	(Required) The session name is any string that uniquely identifies this multicast session from other multicast sessions that might be in progress on the network.
<i>-p path</i>	(Required) The path to the image to be multicast, which is located on the ZENworks Imaging server. This must be the full path.
<i>-i IP_address</i>	(Optional) The IP address of the ZENworks Imaging server.

Argument	Description
<code>-f file_set_number</code>	<p>(Optional) File sets are assigned to the current ZENworks image using this information. File sets are defined on the ZENworks Imaging server from the base image using the Image Explorer utility, which can be run on a Windows device from a Linux server running Samba. The Image Explorer utility is located at <code>/opt/novell/zenworks/zdm/imaging/winutils/ImgExp.exe</code> on the Linux server.</p> <p>When you define a file set using Image Explorer, you specify files and directories to be excluded from the image. Thus, a file set is a subset of the original image that excludes the files you select in Image Explorer. A separate image file is not created for the file set; instead, a file set contains internal attributes representing the excluded information. Therefore, even though a file set does not exist as a separate, physical image file, it is accessed as though it is, placing the image on the receiving device, minus the excluded files.</p> <p>For example, <code>deviceimage.zmg</code> is the image file on your ZENworks Imaging server. You use Image Explorer to determine which data to exclude and assign this to a file set number, such as 2. When a device associated with this ZENworks image boots, it is imaged with the smaller version (file set 2) of <code>deviceimage.zmg</code>.</p> <p>File sets provide an advantage because you can create a base image and modify it slightly for various devices, instead of creating separate, somewhat different base images for each device. However, because file sets only concern excluded files, if you add files to the base image using Image Explorer, all file sets include those additional files. If you don't want them included in a file set, you must use Image Explorer to exclude these new files from that file set.</p> <p>There are a maximum of 10 file sets. Each of the ten file set numbers represents the original base image, until you use Image Explorer and assign the results to a file set number.</p> <hr/> <p>IMPORTANT: If you create 10 different file sets, then the original image can be lost. If you want to maintain the original image's information, do not use Image Explorer to assign exclusions to file set 1, which is the default file set if you don't select a file set when using this wizard.</p> <hr/>
<code>-t time_wait</code>	<p>(Optional) If not enough devices have booted to fulfill the Client Count requirement, the multicast session begins if a participating device boots and a certain amount of time passes without another participating device booting. Specify this amount of time. The default is 5 minutes.</p>
<code>-c client_count</code>	<p>(Optional) The number of participating devices you want to have booted before the multicast session begins. If you do not specify a number, the default is 1.</p>

IMPORTANT: The image is sent to and put down on each participating device only after you initiate the multicast session from each participating client.

2 To view the status of the multicast session, enter:

```
/opt/novell/zenworks/preboot/bin/novell-zmgmcast -status -i
proxy_IP_address
```

The `-i` argument is optional.

- 3** To view the list of multicast sessions, enter:

```
/opt/novell/zenworks/preboot/bin/novell-zmgmcast -list -i  
proxy_IP_address
```

The `-i` argument is optional.

- 4** To stop a multicast session, enter:

```
/opt/novell/zenworks/preboot/bin/novell-zmgmcast -stop  
session_name -i proxy_IP_address
```

The `session_name` is required and the `-i` argument is optional.

- 5** Continue with **“Initiating a Multicast Session from Each Client” on page 734.**

Initiating a Multicast Session from a NetWare ZENworks Imaging Server

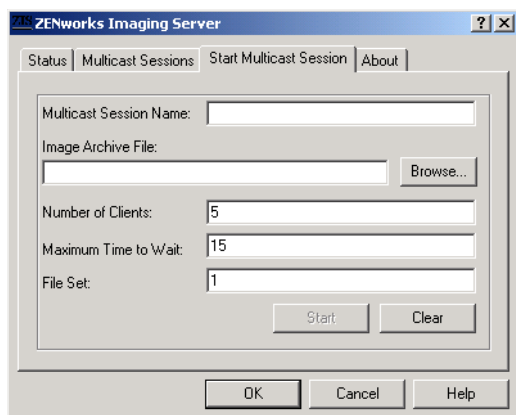
- 1** From the Netware server, load the ZENworks Imaging server (`imgserv.nlm`).
- 2** From the Main Menu, select *Manually Start Multicast*.
- 3** Specify the path to the image archive.
You can either enter the full path to the image file you want to use, or you can press Insert to browse for the image file.
- 4** Specify the name for the multicast session.
- 5** Decide how many participating workstations you want to have booted up before the multicast session begins and specify this number in the *Number of Clients* field.
The default if you do not specify a number is 1 workstation.
- 6** If not enough workstations have booted up to fulfill the Number of Clients requirement, the multicast session begins if a participating workstation boots up and a certain amount of time passes without another participating workstation booting. Specify this amount of time in the *Maximum Time to Wait* field.
The default if you do not specify a time is 5 minutes.
- 7** (Optional) Specify a file set.
- 8** Press Esc, then select *Yes* to start the multicast session.
- 9** (Conditional) If you have not done so, proceed with the steps under **“Initiating a Multicast Session from Each Client” on page 734.**

After you initiate the multicast session from each participating client, the image is sent to and put down on each participating workstation.

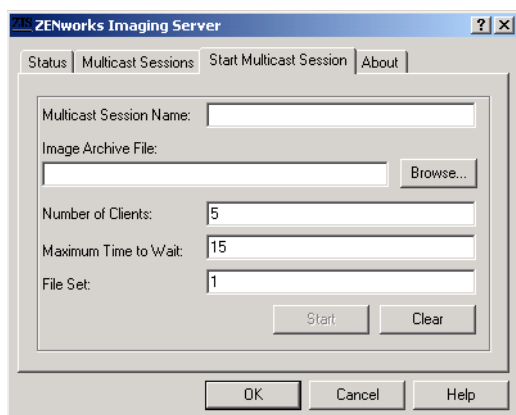
At the Main Menu, select *Multicast Sessions* to see how many clients have registered and how many the session is still waiting for. For example, 3/2 means 3 clients have registered and 2 more need to register before the session can begin. You can delete any session listed, even if it is in progress, by selecting the session name, then pressing Delete.

Initiating a Multicast Session from a Windows ZENworks Imaging Server

- 1 From the Windows taskbar, click the *ZIS* icon to start the ZENworks Imaging server software.



- 2 Click the *Start Multicast Session* tab.



- 3 Specify the name for the multicast session.
- 4 Browse to and specify the image archive file.
- 5 Decide how many participating workstations you want to have booted up before the multicast session begins. Specify this in the *Number of Clients* text box.
The default if you do not specify a number is 5 workstations.
- 6 If not enough workstations have booted up to fulfill the Number of Clients requirement, the multicast session begins if a participating workstation boots up and a certain amount of time passes without another participating workstation booting. Specify this amount of time in the *Maximum Time to Wait* text box.
The default if you do not specify a time is 15 minutes.
- 7 (Optional) Specify a file set.
- 8 Click *Start*.
- 9 (Conditional) If you have not done so, proceed with the steps under “Initiating a Multicast Session from Each Client” on page 734.

You can click the *Status* tab to see how many Update Requests have been received, how many images have been sent or received, and the number of client referrals.

You can click the *Multicast Sessions* tab to view current multicast sessions. You can also delete any session listed, even if it is in progress, by selecting the session name, then clicking *Delete*. You can refresh a session by selecting the session name, then clicking *Refresh*.

Initiating a Multicast Session from Each Client

You can use the bash prompt or the ZENworks Imaging Engine menu to perform the multicast session as you physically visit each workstation.

- [“Using the Bash Prompt to Perform the Multicast Session” on page 734](#)
- [“Using the ZENworks Imaging Engine Menu to Perform the Multicast Session” on page 735](#)

Using the Bash Prompt to Perform the Multicast Session

- 1 (Optional) Install the ZENworks Imaging Windows Agent on each of the participating workstations.

If you do not install the ZENworks Imaging Windows Agent on each participating machine, the machines will have duplicate network identities. For more information, see [“Limitations of Multicasting Images” on page 726](#).

- 2 Create an imaging boot CD or DVD for each person who assists with the multicast session, or enable PXE on the participating workstations.

If you don’t know how to do this, see [“Preparing an Imaging Boot Method” on page 631](#).

- 3 At each workstation, including the master workstation (unless you are starting the multicast session from the ZENworks Imaging server), access a Linux prompt by using the imaging boot CD or DVD, or if it is PXE-enabled, boot it.

- 4 Enter `manual` at the boot prompt.

- 5 To identify each participating workstation in the multicast session, enter the following command at the bash prompt of every workstation:

```
img session name
```

where *name* is any string that uniquely identifies this multicast session from other multicast sessions that might be in progress on the network. Use the same session name on each of the participating workstations in this multicast session. You can specify any multicast session, including one that originates from the ZENworks Imaging server (as long as you specify the session name used by the ZENworks Imaging server).

Example: `img session mcast01`

The `img session` command can take other parameters that allow you to designate the master workstation and the imaging start time beforehand. See [Chapter 64, “ZENworks Imaging Engine Commands,” on page 773](#) for details.

- 6 (Conditional) If you have not already done so, start the multicast session from the master workstation or from the ZENworks Imaging server.

Master Workstation: To start the multicast session from the master workstation, after all of the other workstations have registered as participants, click *Start Session*.

If you start the session from the master workstation, the session master must be a workstation. If you start the session from the ZENworks Imaging server, the session master must be a previously saved image file.

The ZENworks Imaging Engine begins creating the image of the master workstation and the image is sent to and put down on each participating workstation. Any problems are reported and displayed on the master workstation.

Imaging Server: To start the multicast session from the ZENworks Imaging server, follow the steps under [“Initiating a Multicast Session from the ZENworks Imaging Server” on page 730](#).

- 7 At each participating workstation, when the imaging is done, do the following to boot the workstation with the new operating system:

7a At the Linux prompt, type `lilo.s`, then press Enter.

7b Press Ctrl+Alt+Delete.

If the workstation doesn't boot to the new operating system (that is, if the Linux prompt is displayed), enter the `lilo.s` command again and reboot the workstation a second time.

Using the ZENworks Imaging Engine Menu to Perform the Multicast Session

- 1 (Optional) Install the ZENworks Imaging Windows Agent on each of the participating workstations.

If you do not install the ZENworks Imaging Windows Agent on each participating machine, the machines will have duplicate network identities. For more information, see [“Limitations of Multicasting Images” on page 726](#).

- 2 Create an imaging boot CD or DVD for each person who assists with the multicast session, or enable PXE on the participating workstations.

If you don't know how to do this, see [“Preparing an Imaging Boot Method” on page 631](#).

- 3 At each workstation, including the master workstation (unless you are starting the multicast session from the ZENworks Imaging server), access a Linux prompt by using the imaging boot CD or DVD, or if it is PXE-enabled, boot it.

- 4 Enter `manual` at the boot prompt.

or

Select *Start ZENworks Imaging in Maintenance Mode* from the PXE menu.

- 5 To identify each participating workstation in the multicast session, type `img` at the bash prompt to display the ZENworks Imaging Engine menu.

- 6 Click *Imaging*, then click *Multicast Session*.

- 7 Enter a session name.

The session name is any string that uniquely identifies this multicast session from other multicast sessions that might be in progress on the network. Use the same session name on each of the participating workstations in this multicast session. You can specify any multicast session, including one that originates from the ZENworks Imaging server (as long as you specify the session name used by the ZENworks Imaging server).

- 8 Select a *Session Role* option:

Master: Select this option if this is the session master.

Client: Select this option if this is a participating workstation.

9 (Optional) If you chose *Master* in **Step 8**, specify any additional options:

- **Compression Level:** Specify the compression level you want to use for this multicast session:
 - **None:** No data compression is used. Data is sent immediately across the network to participating workstations. You might use this option if the master workstation has a slow CPU; the amount of time to compress the data is eliminated and the data is immediately sent across the network. Using this option, however, the multicast session creates more network traffic than if you selected one of the other compression levels (*Speed*, *Balanced*, or *Size*).
 - **Speed:** Takes the least amount of time to compress the data before the data is sent across the network to participating workstations. You might use this option if the master workstation has a slow CPU; the amount of time to compress the data is reduced before the data is sent across the network. With this option, however, the multicast session creates more network traffic than if you selected either the *Balanced* or *Size* compression level.
 - **Balanced:** Represents a compromise between data compression and the amount of network traffic that the multicast session creates.
 - **Size:** Takes the most amount of time to compress the data before sending it across the network to participating workstations. You might use this option if the master workstation has a fast CPU. Using this option requires the most CPU resources to compress the data but creates less network traffic to transfer the data to the participating workstations.
- **Automated Session:** Click *Enabled* to specify the number of participating workstations (clients) that must register before starting the automated multicast session and to specify the amount of time, in minutes, that can expire without the number of participating workstations to register before starting the automated multicast session. If you do not select the *Enabled* check box, you must manually start the multicast session.

10 Click *Next*, then click *Start Session*.

11 At each participating workstation, when the imaging is done, do the following to boot the workstation with the new operating system:

11a At the Linux prompt, type `lilo.s`, then press Enter.

11b Press Ctrl+Alt+Delete.

If the workstation doesn't boot to the new operating system (that is, if the Linux prompt is displayed), enter the `lilo.s` command again and reboot the workstation a second time.

The following sections provide reference information on Novell® ZENworks® Desktop Management imaging utilities, commands, configuration settings, and log formats.

- [Section 63.1, “Image Explorer \(imgexp.exe\),” on page 737](#)
- [Section 63.2, “ZENworks Imaging Windows Agent \(Ziswin.exe\),” on page 743](#)
- [Section 63.3, “Image-Safe Data Viewer and Editor \(Zisview and Zisedit\),” on page 754](#)
- [Section 63.4, “Imaging Floppy Boot Disk Creator \(zimboot.exe\),” on page 758](#)
- [Section 63.5, “Imaging Configuration Parameters \(Settings.txt\),” on page 758](#)
- [Section 63.6, “Imaging Boot Parameters,” on page 761](#)
- [Section 63.7, “Imaging Server \(Imgserv.nlm or .dll or .dlm, or Linux Daemons\),” on page 761](#)
- [Section 63.8, “Imaging Server Log \(Zimglog.xml\),” on page 770](#)

63.1 Image Explorer (imgexp.exe)

Use the Image Explorer utility at a Windows workstation to view or modify workstation images, create add-on images, compress image files, and split images.

Non-Windows partitions, such as NetWare® partitions, are visible when you open an image, but their contents are not.

Although the ZENworks Imaging Explorer looks, and in most situations, functions like the Microsoft Windows Explorer, the two programs are different and some functionality differences exist:

- **Replacing Files in an Image:** During the life cycle of an image, files might be deleted or updated using Image Explorer. When you replace an existing file in an image by using Image Explorer, the original file is not deleted from the image. Image Explorer purges only deleted files; it does not purge files that have been updated.

When files are added to an image where the file already exists, Image Explorer appends the entry to the end of the image. When images are restored, all files that have been previously updated (but not deleted) are sequentially restored.

To avoid performance problems, you should manually delete and purge each instance of duplicate files in order to have them purged from the image. In Windows Explorer, replaced files are automatically deleted.

- **Dragging Files from Image Explorer:** You cannot drag files from Image Explorer in order to extract them, which you can do in Windows Explorer. However, you can drag and drop files and folders into an image by using Image Explorer.

IMPORTANT: Do not exclude BPB files from a base image or the workstation won't be able to boot the new operating system after receiving the image.

The following sections describe the tasks that you can perform using the Image Explorer:

- Section 63.1.1, “Starting Image Explorer (Imgexp.exe),” on page 738
- Section 63.1.2, “Opening an Image,” on page 739
- Section 63.1.3, “Adding a File or Folder to an Open Image,” on page 739
- Section 63.1.4, “Creating a Folder in an Open Image,” on page 739
- Section 63.1.5, “Adding Specific Windows Registry Settings That Are to Be Applied After the Open Image Is Laid Down,” on page 739
- Section 63.1.6, “Excluding a File or Folder from the Open Image,” on page 739
- Section 63.1.7, “Marking a File or Folder for Deletion in the Open Image,” on page 739
- Section 63.1.8, “Purging Files and Folders Marked for Deletion from the Open Image,” on page 740
- Section 63.1.9, “Extracting a File or Directory from the Open Image to a Folder,” on page 740
- Section 63.1.10, “Extracting a File or Directory from the Open Image as an Add-On Image,” on page 740
- Section 63.1.11, “Viewing a File from the Open Image in its Associated Application,” on page 740
- Section 63.1.12, “Saving Your Changes to the Open Image,” on page 740
- Section 63.1.13, “Creating a Workstation Add-On Image,” on page 740
- Section 63.1.14, “Adding a Partition to a New Add-On Image,” on page 741
- Section 63.1.15, “Compressing an Image,” on page 741
- Section 63.1.16, “Splitting an Image,” on page 742
- Section 63.1.17, “Resizing a Partition in an Image,” on page 742

63.1.1 Starting Image Explorer (Imgexp.exe)

There are no command line parameters for the Image Explorer utility.

- 1 To start the Image Explorer as a Windows standalone utility, double-click the `imgexp.exe` file located on the ZENworks Imaging server at:

- **Linux:** `/opt/novell/zenworks/zdm/winutils/nls/language`

The Image Explorer utility must be run on a Windows device. You need Samba running on the Linux ZENworks Imaging server where the utility file is located in order for the Windows machine to have access to it.

- **NetWare:** `sys:\public\zenworks\imaging`


The Image Explorer utility must be run on a Windows device. You need a drive mapped to the NetWare server where the utility file is located in order for the Windows machine to have access to it.

- **Windows:** `zenworks\imaging`



or

To start the utility from Novell ConsoleOne® from the server, click *Tools > ZENworks Utilities > Imaging > Image Explorer*.


63.1.2 Opening an Image

- 1 Open **Image Explorer** (`imgexp.exe`).
- 2 Click  on the toolbar, browse for and select the image (`.zmg`) file, then click *Open*.
Large image files might take a few moments to open.

63.1.3 Adding a File or Folder to an Open Image

- 1 Open **Image Explorer** (`imgexp.exe`).
- 2 In the left pane, browse to the partition or directory where you want to add the file or folder.
- 3 Click  or  on the toolbar, browse to the file or folder, then click *Add* or *OK*.

63.1.4 Creating a Folder in an Open Image

- 1 Open **Image Explorer** (`imgexp.exe`).
- 2 In the left pane, browse to the partition or directory where you want to create the folder, click , enter the name of the folder, then click *OK*.

63.1.5 Adding Specific Windows Registry Settings That Are to Be Applied After the Open Image Is Laid Down

This only applies to Windows machines being imaged.

- 1 Open **Image Explorer** (`imgexp.exe`).
- 2 Select a partition in the left pane, click *Image*, then click *Add Registry File*.
- 3 Select the registry (`.reg`) file that contains the settings, then click *Add*.

The registry file is added to a fixed, known area of the partition and is applied when the workstation reboots after receiving the image.

63.1.6 Excluding a File or Folder from the Open Image

- 1 Open **Image Explorer** (`imgexp.exe`).
- 2 Select the file or folder, click *Edit*, click *File Sets*, then select the file sets that you want the file or folder to be excluded from.

This image has 10 possible file sets, labeled Set 1, Set 2, and so on. The files and folders that you selected in the main window are excluded only from the file sets that you select in this dialog box.

63.1.7 Marking a File or Folder for Deletion in the Open Image

- 1 Open **Image Explorer** (`imgexp.exe`).
- 2 Select the file or folder, click *Image*, then click *Delete*.

IMPORTANT: Deleting a file in the Image Explorer merely marks it for deletion; it can still be retrieved. A file marked as deleted is not removed from the image until the image is purged; files and folders marked as deleted are not restored during imaging.

63.1.8 Purging Files and Folders Marked for Deletion from the Open Image

- 1 Open **Image Explorer** (imgexp.exe).
- 2 Make sure that the open image is saved, click *File*, then click *Purge Deleted Files*.
- 3 Browse to the image filename or specify a new image filename, then click *Save*

63.1.9 Extracting a File or Directory from the Open Image to a Folder

- 1 Open **Image Explorer** (imgexp.exe).
- 2 Click the file or directory, click *File > Extract > As Files*, browse to and select a folder, then click *OK*.


63.1.10 Extracting a File or Directory from the Open Image as an Add-On Image

- 1 Open **Image Explorer** (imgexp.exe).
- 2 Click the file or directory, click *File > Extract > As Add-on Image*, enter the name of the new add-on image, then click *OK*.


63.1.11 Viewing a File from the Open Image in its Associated Application

- 1 Open **Image Explorer** (imgexp.exe).
- 2 Click the file, then click *File > Extract and View*.


63.1.12 Saving Your Changes to the Open Image

- 1 Open **Image Explorer** (imgexp.exe).
- 2 Click  on the toolbar.

63.1.13 Creating a Workstation Add-On Image

- 1 Open **Image Explorer** (imgexp.exe).
- 2 Click  on the toolbar, open Windows Explorer, browse to the files and folders you want the add-on image to contain, drag the files and folders into the right pane from Windows Explorer, then click *Save*.

63.1.14 Adding a Partition to a New Add-On Image

- 1 Open **Image Explorer** (`imgexp.exe`).
- 2 Click  on the toolbar, click the root of the image, click *Image*, then click *Create Partition*.

You cannot add a partition to an existing add-on image or to any base image.

63.1.15 Compressing an Image

You can set compression options so that it takes less time to restore the image file and less space to store the file on your ZENworks Imaging server. You can compress an uncompressed image (including images created by previous versions of ZENworks Desktop Management) to 40 to 60 percent of the original file size.

The ZENworks Desktop Management Image Explorer provides the following types of image compression:

- “Compressing an Open Image” on page 741
- “Compressing Any Image without Waiting for the File to Fully Load into Image Explorer” on page 741

Compressing an Open Image

- 1 Open **Image Explorer** (`imgexp.exe`).
- 2 Browse for the image (`.zmg`) file, then click *Open*.
Large image files might take a few moments to open.
- 3 Click *File > Compress Image*.
- 4 Browse to a directory, specify a new image filename, then select a compression option:
 - **Optimize for Speed:** Takes the least amount of time to compress but creates the largest compressed image file.
 - **Balanced (Recommended):** Represents a compromise between compression time and image file size. This option is used by default when an image is created.
 - **Optimize for Space:** Creates the smallest image file but takes longer to compress.
- 5 Click *Compress*.

Files marked for deletion in the image are removed during the compression operation.

Compressing Any Image without Waiting for the File to Fully Load into Image Explorer

You can set compression options to quickly compress an image file without waiting for the file to fully load into Image Explorer.

- 1 Open **Image Explorer** (`imgexp.exe`).
- 2 Click *Tools > QuickCompress*.
- 3 Browse to the image file, browse to a directory, specify a new image filename, select a compression option:
 - **Optimize for Speed:** Takes the least amount of time to compress but creates the largest compressed image file.

- **Balanced (Recommended):** Represents a compromise between compression time and image file size. This option is used by default when an image is created.
- **Optimize for Space:** Creates the smallest image file, but takes longer to compress.

4 Click *Compress*.

Files marked for deletion in the image are removed during the compression operation.

63.1.16 Splitting an Image

You can split an image file into separate files so that you can span the entire image across several CDs or DVDs.

When you split a workstation image and span it across several CDs or DVDs, you are essentially creating a base image on the first CD or DVD. The remaining CDs or DVDs are add-on images.

To restore a workstation image that is spanned across several CDs or DVDs, you should restore the first CD or DVD before restoring the remaining CDs or DVDs containing the add-on images. For more information, see [Section 60.2, “Manually Putting an Image on a Workstation,” on page 715](#).

Restoring split images is a manual task and can only be automated by scripted imaging. For more information, see [Step 7 on page 707](#).

To split an image:

- 1 Open **Image Explorer** (`imgexp.exe`).
- 2 Click *Tools > Image Split*.
- 3 Specify an existing base image file to split, specify the directory in which to store the split images, then specify the maximum file size of each split-image file.
Because images are split by placing individual files into different images, an image cannot be split if it contains any single file that is larger than the specified maximum file size.
- 4 Click *Split*.

63.1.17 Resizing a Partition in an Image

For base images, you can edit the value in the *Original Size* text box to allow you to change how big the ZENworks Imaging Engine makes the partition when the image is restored.

For example, suppose you create a base image of a workstation with a 20 GB hard drive and you want to then put that image on a new workstation with a 60 GB hard drive. If you do not increase the size of the partition, the partition will be 20 GB, thus making the remaining 40 GB unusable.

However, if you increase the number in the *Original Size* text box to match the size of the new hard drive, the ZENworks Imaging Engine expands the partition when the image is restored so that you can use the entire drive.

To resize a partition:

- 1 Open **Image Explorer** (`imgexp.exe`).
- 2 Right-click a partition in the left frame, then click *Properties*.

- 3 Increase or decrease the value in the *Original Size* text box.

You cannot decrease the number in the *Original Size* text box to a smaller value than what is in the *Minimum Size* text box.

The *Original Size* field is not applicable for add-on images and cannot be modified.

63.2 ZENworks Imaging Windows Agent (Ziswin.exe)

When you install the ZENworks Imaging Windows Agent (`ziswin.exe`) on an existing Windows workstation, it saves certain workstation-unique data (IP address, computer name, etc.) to an area on the hard disk that is safe from reimaging.

WARNING: When running `ziswin.exe` in the service mode, its **restoration submodule** removes **image-safe data**. This only applies to images created with previous versions of ZENworks. For more information, see “**Preserving Image-Safe Data**” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

The following sections contain additional information:

- Section 63.2.1, “Understanding the ZENworks Imaging Windows Agent,” on page 743
- Section 63.2.2, “Running the ZENworks Imaging Windows Agent in Interactive Mode,” on page 745
- Section 63.2.3, “Running the ZENworks Imaging Windows Agent in Service Mode,” on page 750
- Section 63.2.4, “Running the ZENworks Imaging Windows Agent in Installation Mode,” on page 753
- Section 63.2.5, “Running the ZENworks Imaging Windows Agent in Uninstallation Mode,” on page 753

63.2.1 Understanding the ZENworks Imaging Windows Agent

The ZENworks Imaging Windows Agent is an extension to the Windows boot procedure on a workstation.

The ZENworks Imaging Windows Agent (`ziswin.exe`) is installed on each workstation when you install the Desktop Management Agent. On Windows 98 workstations, the default location is `windows\system\ziswin.exe`. On Windows 2000/XP workstations, the default location is `windows\system32\ziswin.exe`. During installation of the Desktop Management Agent, you must select the *Workstation Imaging* feature on the Select Features page. For more information, see “**Installing and Configuring the Desktop Management Agent**” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

If you want to run the ZENworks Imaging Windows Agent on a workstation without the Desktop Management Agent installed, you can install it manually. For more information, see “**Manually Installing the ZENworks Imaging Windows Agent**” on page 745.

The ZENworks Imaging Windows Agent is also installed on the ZENworks Imaging server (`sys:public\zenworks\imaging\ziswin.exe`, by default).

The ZENworks Imaging Windows Agent runs before any network communications are established. It enables you to:

- Make an existing Windows workstation safe for reimaging

When you install the ZENworks Imaging Windows Agent on an existing Windows workstation, it saves certain workstation-unique data (such as the IP address and Computer name) to an area on the hard disk that is safe from reimaging. After the workstation is reimaged and Windows reboots, the agent restores the data from the image-safe area so the workstation can use the same network identity as before.

- Automatically assign a network identity to a brand new workstation

A new workstation (with no Windows operating system) doesn't have a network identity established yet. You can define network identity information for such a workstation in a Novell eDirectory™ policy and apply it when the workstation receives its first Windows image. In this scenario, the Windows image is put down (including the ZENworks Imaging Windows Agent) on the workstation and the identity information from the eDirectory policy is written to the image-safe area on the hard disk. When the workstation reboots, the agent reads the data from the image-safe area and applies it to the Windows installation, thus establishing the workstation's network identity.

The data that the ZENworks Imaging Windows Agent saves to (or restores from) the image-safe area includes the following:

- Whether a static IP address or DHCP is used
- If a static IP address is used:
 - IP address
 - Subnet mask
 - Default gateway (router)
- Computer (NETBIOS) name
- Workgroup that the workstation belongs to, if any
- Workstation Security ID (SID)
- If the workstation is registered in eDirectory:
 - Distinguished name of the Workstation object
 - Context of the Workstation object
 - eDirectory tree that the Workstation object belongs to
- DNS settings
 - DNS suffix
 - DNS hostname
 - DNS servers

On a workstation that has just received a new Windows 2000/XP base image, in addition to restoring the above data, the agent also locates and modifies all instances of the Security Identifier (SID). This ensures that the workstation has a SID that is unique from other workstations that might receive the same image.

IMPORTANT: The ZENworks Imaging Windows Agent does not save or restore any Windows2000/XP Domain information. If you change a workstation's domain and then restore an image, the workstation receives whatever domain is embedded in the new image.

Manually Installing the ZENworks Imaging Windows Agent

The ZENworks Imaging Windows Agent is installed on each workstation when you install the Desktop Management Agent. You can also run the ZENworks Imaging Windows Agent on a workstation without the Desktop Management Agent installed.

- “Manually Installing Ziswin.exe on a Windows 98 Workstation:” on page 745
- “Manually Installing Ziswin.exe on a Windows 2000/XP Workstation:” on page 745

Manually Installing Ziswin.exe on a Windows 98 Workstation:

- 1 From the `windows\system` directory on the ZENworks Imaging server, copy the following files to the `windows\system` directory on the workstation:
 - `ziswin.exe`
 - `zislib16.dll`
 - `zislib32.dll`
- 2 From the command prompt, run `ziswin -install`.

Manually Installing Ziswin.exe on a Windows 2000/XP Workstation:

- 1 From the `windows\system` directory on the ZENworks Imaging server, copy the `ziswin.exe` file to the `windows\system32` directory on the workstation.
- 2 From the command prompt, run `ziswin -install`.

63.2.2 Running the ZENworks Imaging Windows Agent in Interactive Mode

You can use the ZENworks Imaging Windows Agent (`ziswin.exe`) in interactive mode to view and edit a workstation's image-safe data using a graphical user interface rather than from the command line or `regedit`. The ZENworks Imaging Windows Agent combines the capabilities of the **Image-Safe Data Viewer** (`zisview`) to let you view a workstation's image-safe data and the **Image-Safe Data Editor** (`zisedit`) to let you edit this data.

IMPORTANT: Image-safe data is not supported on Linux workstations.

The following sections describe the tasks that you can perform using the ZENworks Imaging Windows Agent in interactive mode:

- “Starting the ZENworks Imaging Windows Agent in Interactive Mode” on page 746
- “Reloading a Workstation's Image-Safe Data” on page 746
- “Saving a Workstation's Unique Data to the Image-Safe Data Store” on page 746
- “Exporting a Workstation's Image-Safe Data to a File” on page 746
- “Importing a Workstation's Image-Safe Data from a File” on page 746

- “Modifying a Workstation’s Image-Safe Data” on page 747
- “Clearing a Workstation’s Image-Safe Data” on page 748
- “Viewing the Contents of a Workstation’s Image-Safe Data” on page 748
- “Modifying a Workstation’s Image-Safe Options” on page 748
- “Viewing a Workstation’s Image-Safe Data History” on page 750

Starting the ZENworks Imaging Windows Agent in Interactive Mode

- 1 To run the ZENworks Imaging Windows Agent in interactive mode, manually run `ziswin.exe` from your preferred location, such as from the command line prompt, Windows Explorer, or the *Windows > Start > Run* command.

The ZENworks Imaging Windows Agent (`ziswin.exe`), is installed on each workstation during installation of the Desktop Management Agent (if you selected the *Desktop Imaging* feature). For Windows 98 workstations, the default location is `windows\system\ziswin.exe`. For Windows 2000\XP workstations, the default location is `windows\system32\ziswin.exe`. For more information, see “[Installing and Configuring the Desktop Management Agent](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

If the ZENworks Imaging Windows Agent is started as part of a boot sequence, it is automatically started in **service mode**. If the ZENworks Imaging Windows Agent is started manually, it is automatically started in interactive mode.

Reloading a Workstation’s Image-Safe Data

- 1 **Open the ZENworks Imaging Windows Agent** (`ziswin.exe`) in interactive mode.
- 2 Click *File > Reload Image-Safe Data*.

Saving a Workstation’s Unique Data to the Image-Safe Data Store

- 1 **Open the ZENworks Imaging Windows Agent** (`ziswin.exe`) in interactive mode.
- 2 Click *File > Save Image-Safe Data > Save*.

Exporting a Workstation’s Image-Safe Data to a File

- 1 **Open the ZENworks Imaging Windows Agent** (`ziswin.exe`) in interactive mode.
- 2 Click *File*, then click *Export to File*.
- 3 Browse to the location in which you want to save the file, then enter the filename.
- 4 Click *Save*.

Importing a Workstation’s Image-Safe Data from a File

- 1 **Open the ZENworks Imaging Windows Agent** (`ziswin.exe`) in interactive mode.
- 2 Click *File*, then click *Import from File*.
- 3 Browse to and select the `.zis` file you want to import data from, then click *Open* to apply the imported image-safe data to the workstation.

Modifying a Workstation's Image-Safe Data

- 1 **Open the ZENworks Imaging Windows Agent** (`ziswin.exe`) in interactive mode.
- 2 Click *Edit*, then click *Modify Image-Safe Data*.
- 3 In the Modify Image-Safe Data dialog box, modify the desired data on the *Imaging* tab:

Just Imaged Flag: If this option is selected, the ZENworks Imaging Windows Agent (`ziswin.exe`) reads data from the image-safe data store and writes it to the Windows registry. If this option is not selected, the ZENworks Imaging Windows Agent reads data from the Windows registry and writes it to the image-safe data store.

Last Base Image: Displays information about the last base image that was restored to this workstation. The ZENworks Imaging Engine uses this information to prevent the same image from being restored to the workstation, unless you specify in ConsoleOne that the same image be restored.

- **Filename:** The last base image that was restored to the workstation.
- **File Time:** The time stamp of the last base image that was restored to the workstation.
- **File Size:** The size of the last base image that was restored to the workstation.

Scripted Image: Indicates whether or not the last imaging operation was a scripted image.

- **Scripted Image Flag:** If this option is selected, the last imaging operation was a scripted image. If this option is not selected, the last imaging operation was not a scripted image.
- **Script Checksum:** Displays the checksum value representing the last script run. The ZENworks Imaging Engine uses the checksum to prevent the same script from re-running on the workstation unless you specify in ConsoleOne that you want to rerun the same script.

- 4 Click the *Identity* tab in the Modify Image-Safe Data dialog box, then modify the desired data:

Object Name: The name of the eDirectory Workstation object for this workstation.

Tree Name: The eDirectory tree that contains the Workstation object for this workstation.

Object ID: The ZENworks Object ID for this workstation, which together with the workstation DN, uniquely identifies this workstation.

- 5 Click the *Windows* tab in the Modify Image-Safe Data dialog box, then modify the desired data:

NETBIOS Name: Displays the Windows NETBIOS name for this workstation. For Windows 2000/XP workstations, the computer name and the NETBIOS name are not necessarily the same. For these workstations, the ZENworks Imaging Windows Agent uses the *DNS Hostname* field in the image-safe data as the computer name, which takes precedence over the NETBIOS name entered here.

Workgroup: Displays the network workgroup that this workstation belongs to, if any. A workgroup is a group of users who work on a common project and share information on interconnected computers, often over a LAN.

Workstation SID: Displays the workstation's Security ID (SID), a unique number that identifies this workstation in Windows.

Clear SID: Clears this workstation's SID. If you clear the workstation's SID, the ZENworks Imaging Windows Agent generates a new SID if the agent is run in Enabled mode. To specify that the agent run in Enabled mode, click *Edit*, click *Options*, then click *Enabled* on the *Mode* tab. You must also set the Just Imaged flag (click *Edit*, click *Modify Image-Safe Data*, then click *Just Imaged Flag* on the *Imaging* tab).

- 6 Click the *IP Settings* tab in the Modify Image-Safe Data dialog box, then modify the desired data to configure the IP settings stored in the image-safe data area of this workstation:

Uses DHCP to Get an IP Address: Indicates that this workstation uses DHCP to obtain its IP address.

Uses a Static IP Address: Indicates that this workstation uses a static IP address.

- **IP Address:** Displays the static IP address that this workstation uses.
- **Subnet Mask:** Displays the subnet mask that this workstation uses.
- **Gateway:** Displays the gateway that this workstation uses.

- 7 Click the *DNS* tab in the Modify Image-Safe Data dialog box, then modify the desired data to configure the DNS settings stored in the image-safe data area of this workstation:

DNS Suffix: Displays the DNS context of the workstation.

DNS Hostname: Displays the DNS local hostname of the workstation. For Windows 2000/XP, this is the Computer name plus the first 15 characters of the NETBIOS name.

DNS Servers: Displays the names of DNS servers used for DNS name resolution. You can use the drop-down list to select another DNS server or you can use the browse button to enter additional DNS servers for this workstation.

- 8 Click *OK*.

Clearing a Workstation's Image-Safe Data

- 1 Open the **ZENworks Imaging Windows Agent** (`ziswin.exe`) in interactive mode.
- 2 Click *Edit > Clear Image-Safe Data*.

Viewing the Contents of a Workstation's Image-Safe Data

- 1 Open the **ZENworks Imaging Windows Agent** (`ziswin.exe`) in interactive mode.
- 2 Click *Edit > Copy to Clipboard*.

Modifying a Workstation's Image-Safe Options

- 1 Open the **ZENworks Imaging Windows Agent** (`ziswin.exe`) in interactive mode.
- 2 Click *Edit > Options*.
- 3 In the ZENworks Imaging Windows Agent Options dialog box, modify the desired data on the *Mode* tab to select the mode for the ZENworks Imaging Windows Agent (`ziswin.exe`) to run during the boot process:

Enabled: If this option is selected and the *Just Imaged Flag* is set (*File > Edit > Modify Image-safe Data > Imaging*), the ZENworks Imaging Windows Agent reads data from the image-safe data store and write it to the Windows registry.

If this option is selected but the *Just Imaged Flag* is not set, the ZENworks Imaging Windows Agent reads data from the Windows registry and writes it to the image-safe data store.

Disabled: If this option is selected, the ZENworks Imaging Windows Agent runs automatically during the boot process, but exits without doing any work.

- **Re-enable After _ Boot:** Enable this option and specify the number of boot cycles to take place before the ZENworks Imaging Windows Agent returns to an enabled state.

Uninstalled: If this option is enabled, the ZENworks Imaging Windows Agent does not automatically run during the boot process.

- 4 Click the *Logging* tab in the ZENworks Imaging Windows Agent Options dialog box, then modify the desired data to specify history log and debug logging setting for the ZENworks Imaging Windows Agent (*ziswin.exe*):

History Logging: Use the options in this group box to specify the location of the history log file and how many entries you want the log file to contain before discarding the oldest entries.

- **History Log File:** Click the browse button to specify the location in which you want to store the history log file (*ziswin.hst*).
- **Maximum History Log Entries:** Specify the maximum number of log entries that you want the history log file to contain. After the number of entries you enter in this field is reached, each new entry causes the oldest entry to be discarded.

Debug Logging: The debug log file, *ziswin.log*, is located in the system *\temp* directory if the ZENworks Imaging Windows Agent is run in service mode. The ZENworks Imaging Windows Agent runs, by default, in service mode during each Windows boot process when the workstation is started. When you run the *ziswin.exe* executable file, by default, the agent is started in interactive mode and *ziswin.log* is located in the interactive user's user *\temp* directory.

- **Disabled:** Turns off debug logging.
- **Single Log File:** Enables debug logging and specifies that the current debug log file be overwritten during each boot process.
- **Multiple Log Files:** Enables debug logging and specifies that a new debug log file is created during each boot process. Each new log file is given a unique name (*ziswinx.log*, where *x* represents a number that identifies each log file). Although these log files are small, you might want to periodically delete older files that you no longer need.

- 5 Click the *Restore Mask* tab in the ZENworks Imaging Windows Agent Options dialog box, then use this tab to prevent restoration of certain image-safe data components to the workstation when the ZENworks Imaging Windows Agent (*ziswin.exe*) restores image-safe data.

To prevent image-safe data from being restored to the workstation, select the box next to the desired component.

If the check box is enabled (a check mark is displayed next to an item), that information is not restored to the workstation from the image-safe data.

If the check box is not enabled (a check mark does not display next to an item), that information is restored to the workstation from the image-safe data.

- 6 Click the *Collection Mask* tab in the ZENworks Imaging Windows Agent Options dialog box, then use this tab to prevent certain items from being overwritten in the image-safe data store when the ZENworks Imaging Windows Agent (*ziswin.exe*) collects data from Windows.

To prevent image-safe data from being overwritten, select the box next to the desired component.

If the check box is enabled (a check mark is displayed next to an item), that information is not written to the workstation's image-safe data. Any corresponding existing image-safe data is not overwritten.

If the check box is not enabled (a check mark does not display next to an item), that information is collected from the workstation and stored with the workstation's image-safe data. Any corresponding existing image-safe data is overwritten.

7 Click *OK*.

Viewing a Workstation's Image-Safe Data History

- 1 Open the **ZENworks Imaging Windows Agent** (`ziswin.exe`) in interactive mode.
- 2 Click *View > View History*.

From the ZENworks Imaging Windows Agent History dialog box, you can view the image-safe data's history, load a history file from another location, clear the workstation's image-safe data history, and view a specific history entry's details, including the image-safe data that was loaded when booting and saved during shutdown. To view a specific history entry's data, select the entry in the ZENworks Imaging Windows Agent History dialog box, then click *Details*.

63.2.3 Running the ZENworks Imaging Windows Agent in Service Mode

WARNING: When you run `ziswin.exe` in the service mode, its **restoration submode** removes image-safe data. This only applies to images created with previous versions of ZENworks. For more information, see “**Preserving Image-Safe Data**” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

The ZENworks Imaging Windows Agent (`ziswin.exe`) runs in service mode when no parameters are given on the command line. This is always the mode when the ZENworks Imaging Windows Agent is run automatically by Windows during the boot process (because of the registry entries made during the installation mode install process.) When it is in service mode, the ZENworks Imaging Windows Agent reads the registry to determine if it should be disabled or inactive. If the ZENworks Imaging Windows Agent is not disabled and not inactive, it reads the image-safe data to determine whether to run in restoration or collection submode. If the Just-Imaged flag in the image-safe data is set, the ZENworks Imaging Windows Agent runs in the restoration submode. If the Just-Imaged flag in the image-safe data is not set, or if image-safe data does not exist on the machine, the ZENworks Imaging Windows Agent runs in collection submode.

IMPORTANT: Image-safe data is not supported on Linux workstations.

- “**Disabled Submode**” on page 750
- “**Inactive Submode**” on page 751
- “**Collection Submode**” on page 751
- “**Restoration Submode**” on page 752

Disabled Submode

To run the ZENworks Imaging Windows Agent in the disabled submode of service mode, edit the workstation's `HKEY_LOCAL_MACHINE\SOFTWARE\NOVELL\ZENWORKS\ZISWIN` Disabled registry setting.

When this string value is set to 1, the ZENworks Imaging Windows Agent exits without doing any work.

Inactive Submode

You can set a registry value to cause the ZENworks Imaging Windows Agent to consider itself inactivated for a certain number of executions.

To run the ZENworks Imaging Windows Agent in the inactive submode of service mode, edit the workstation's `HKEY_LOCAL_MACHINE\SOFTWARE\NOVELL\ZENWORKS\ZISWIN` `Inactive` setting. You can set this value at anything greater than zero.

When the ZENworks Imaging Windows Agent runs in service mode and determines that this registry value is set, the agent decrements the inactive count by one and then exits. When the inactive count reaches zero, the ZENworks Imaging Windows Agent reactivates itself and performs its normal collection or restoration work.

Collection Submode

The ZENworks Imaging Windows Agent gathers Windows registry information necessary to populate the image-safe data store and writes that information to an area on the workstation's hard disk that is safe from reimaging. In so doing, the ZENworks Imaging Windows Agent does not collect information for any image-safe data components that are specified in the Do Not Collect entry in the registry. This functionality provides a means for administrators to prevent certain components in the image-safe data store from being overwritten with new data.

You can also edit the edit the workstation's `HKEY_LOCAL_MACHINE\SOFTWARE\NOVELL\ZENWORKS\ZISWIN` `Do Not Collect Mask` to specify which components you do not want the ZENworks Imaging Windows Agent to collect inside of the image-safe data store. This value is interpreted as a mask (as seen in [Table 63-1](#)), with each component receiving one bit in the mask. To stop the collection of one item, specify its corresponding mask as the value in the registry. To stop the collection of multiple items, add the masks together and the sum is the value defined in the registry.

You can use the following values for the `ZISWIN` `Do Not Collect Mask`:

Table 63-1 *The Ziswin Do Not Collect Mask Values*

Component	Value
Workstation Distinguished Name	0x00000001
Workstation Tree	0x00000002
NetBios Name	0x00000004
Workgroup	0x00000008
IP Address	0x00000010
SID	0x00000020
DNS	0x00000100
Workstation ID	0x00000200

Restoration Submode

The ZENworks Imaging Windows Agent reads the information stored in the image-safe data store and restores that information into the Windows registry.

WARNING: When running `ziswin.exe` in the service mode, this restoration submode removes image-safe data. This only applies to images created with previous versions of ZENworks. For more information, see “**Preserving Image-Safe Data**” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

You can also edit the workstation’s `HKEY_LOCAL_MACHINE\SOFTWARE\NOVELL\ZENWORKS\ZISWIN Do Not Restore Mask` to specify image-safe data components that you do not want the ZENworks Imaging Windows Agent to restore to the Windows registry upon successful completion of an image. This value is interpreted as a mask (as seen in [Table 63-2](#)), with each component receiving one bit in the mask. To stop the restoration of one item, specify its corresponding mask as the value in the registry. To stop the restoration of multiple items, add the masks together and the sum is the value defined in the registry.

You can use the following values for the `ZISWIN Do Not Restore Mask`:

Table 63-2 *The Ziswin Do Not Restore Mask Values*

Component	Value
Workstation Distinguished Name	0x00000001
Workstation Tree	0x00000002
NetBios Name	0x00000004
Workgroup	0x00000008
IP Address	0x00000010
SID	0x00000020
DNS	0x00000100
Workstation ID	0x00000200

Following are common scenarios and example usages of the `ZISWIN Do Not Restore Mask`:

Windows Domain Environment: The ZENworks Imaging Windows Agent does not currently add workstations to the domain. However, you can use sysprep to add the workstation to the domain. In this scenario, you can specify that the ZENworks Imaging Windows Agent restore everything but the Workgroup. To do this, set the value of this registry key to 0x00000008.

DHCP Environment: Administrators who push IP and DNS configuration through DHCP do not need the ZENworks Imaging Windows Agent to restore this information from image-safe data store. To not restore these two components, the value of this registry key is 0x00000110.

Sysprep Naming Environment: Administrators can have a process (running during the mini-setup that sysprep performs) that names the NetBios name of the computer. Because the ZENworks Imaging Windows Agent runs after sysprep, there could be a case where the ZENworks Imaging Windows Agent is renaming the workstation (to its original name) after the proper name was

determined during the sysprep routine. To have the ZENworks Imaging Windows Agent not restore the NetBios name of a workstation, set the value of this registry key to 0x00000004.

If your environment has all three of the configurations mentioned above, add the four components' mask values. The resulting registry value is 0x0000011C.

If your environment needs only the Workstation Object, Workstation ID, and Workstation Tree to be restored after imaging, add up all of the other components' mask values. The resulting registry value is then 0x0000013C.

If your environment does not need anything restored by the ZENworks Imaging Windows Agent, the registry value can be set to 0xFFFFFFFF.

NOTE: You can use the registry REG_SZ value in HKEY_LOCAL_MACHINE\SOFTWARE\NOVELL\ZENWORKS\ZISWIN Prevent Reboot=1 to prevent the ZENworks Imaging Windows Agent from causing the workstation to reboot after performing work in restoration mode.

63.2.4 Running the ZENworks Imaging Windows Agent in Installation Mode

To install the ZENworks Imaging Windows Agent so that it runs automatically each time Windows starts, follow the instructions in [Chapter 57, “Setting Up Workstations for Imaging,” on page 693](#).

To run the ZENworks Imaging Windows Agent in installation mode, enter the following on the workstation's command line:

```
ziswin -install
```

The `ziswin.exe` file must be located in the workstation's `windows\system32` directory for Windows 2000/XP workstations. For Windows 98 workstations, `ziswin.exe` must be located in the workstation's `windows\system` directory.

When you run `ziswin.exe` with the `-install` switch, the ZENworks Imaging Windows Agent creates the registry entries necessary for it to run automatically during subsequent boot cycles of the workstation. This switch adds the String Value System with a Value Data of ZISWIN.EXE to the registry location so that `ziswin.exe` executes during subsequent boot sequences. On Windows 2000/XP workstations, this location is

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON. On Windows 98 workstations, this location is HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENT VERSION\RUN SERVICES.

63.2.5 Running the ZENworks Imaging Windows Agent in Uninstallation Mode

The ZENworks Imaging Windows Agent (`ziswin.exe`) is uninstalled if you uninstall the ZENworks Imaging Windows Agent from the workstation.

If you want to uninstall only the ZENworks Imaging Windows Agent, you can run `ziswin -remove` from the workstation's command line. Running `ziswin -remove` removes the registry entries that

cause `ziswin.exe` to be executed during the boot cycle; however, the `ziswin.exe` file is not removed from the workstation.

63.3 Image-Safe Data Viewer and Editor (Zisview and Zisedit)

After booting a workstation from an imaging boot medium (PXE, CD, DVD, or ZENworks partition), you can enter `zisedit` or `zisview` at the Linux bash prompt to edit and view the image-safe data for that workstation.

IMPORTANT: Image-safe data is not supported on Linux workstations.

- [Section 63.3.1, “Information Displayed by the Image-Safe Data Viewer,” on page 755](#)
- [Section 63.3.2, “Image-Safe Data Viewer,” on page 756](#)
- [Section 63.3.3, “Image-Safe Data Editor,” on page 757](#)

NOTE: You can also use the ZENworks Imaging Windows Agent (`ziswin.exe`) to view and edit a workstation’s image-safe data. The ZENworks Imaging Windows Agent combines the capabilities of the Image-Safe Data Viewer (`zisview`) to let you view a workstation’s image-safe data and the Image-Safe Data Editor (`zisedit`) to let you edit this data. For more information, see [Section 63.2, “ZENworks Imaging Windows Agent \(Ziswin.exe\),” on page 743](#).

63.3.1 Information Displayed by the Image-Safe Data Viewer

After booting a workstation from an imaging device, you can enter `zisview` at the Linux bash prompt to view the image-safe data for that workstation.

The image-safe data viewer (`zisview`) displays the following information about the workstation:

Table 63-3 *Zisview Information*

Category	Information
Image-safe Data	<ul style="list-style-type: none">• Version: The version number of the ZENworks Imaging Windows Agent (<code>ziswin</code>).• Just Imaged Flag: If this is set to False, the ZENworks Imaging Windows Agent (<code>ziswin.exe</code>) reads data from the Windows registry and writes it to the image-safe data store. If this is set to True, the ZENworks Imaging Windows Agent reads data from the image-safe data store and writes it to the Windows registry.• Last Base Image: The last base image that was restored to the workstation.• Last Base Image Time: The time stamp of the last base image that was restored to the workstation.• Last Base Image Size: The size of the last base image that was restored to the workstation.• Scripted Image Flag: If this option is set to True, the last imaging operation was a scripted image. If this option is set to False, the last imaging operation was not a scripted image.• Script Checksum: Displays the checksum value representing the last script run. The ZENworks Imaging Engine uses the checksum to prevent the same script from re-running on the workstation unless you specify in ConsoleOne that you want to rerun the same script.
Workstation Identity Information	<ul style="list-style-type: none">• Workstation Tree: The eDirectory tree that contains the Workstation object for this workstation.• Workstation Object: The distinguished name of this computer's workstation.• Workstation ID: The workstation identification number.• Win 9x Computer Name: The computer name for the workstation. This is only used for changing the computer name of Windows 9.x workstations. To change the computer name of Windows 2000 or XP workstations, use DNS Hostname.• Windows Workgroup: The Microsoft network workgroup of the workstation.• Windows SID: The Windows Security ID of the workstation, which is a unique number that identifies this workstation in Windows.

Category	Information
Network Information	<ul style="list-style-type: none"> • DHCP: Displays whether this workstation uses DHCP to obtain its IP address. • IP Address: Displays the static IP address that this workstation uses. • Subnet Mask: Displays the subnet mask that this workstation uses. • Gateway: Displays the gateway that this workstation uses. • DNS Servers: The number of DNS name servers used for DNS name resolution. • DNS Suffix: The DNS context of the workstation. • DNS Hostname: The DNS local hostname of the workstation. This is also used for changing the computer name of Windows 2000 or XP workstations.

63.3.2 Image-Safe Data Viewer

To use zisview, enter any of the following commands at the Linux bash prompt:

Table 63-4 *Zisview Bash Commands*

Command	Explanation
<code>zisview</code>	Displays all image-safe data.
<code>zisview -z field</code>	<p>Displays information about a specific field or fields. <i>field</i> is one or more field names separated by a space. <i>field</i> is not case-sensitive.</p> <p>All of the following are valid field names. The corresponding minimum names that can also be entered on the command line follow each field name in parenthesis.</p> <p>JustImaged (J) ScriptedImage (SC) LastBaselImage (L) Tree (T) ObjectDN (ObjectDN) NetBIOSName (N) WorkGroup (WorkG) SID (SI) WorkstationID (Works) DHCP (DH) IP (I) Gateway (Gateway) Mask (M) DNSServerCount (DNSServerC) DNSServer (DNSServer) DNSSuffix (DNSSu) DNSHostName (DNSH)</p>
<code>zisview -s</code>	Creates a script that can be used to generate environment variables that contain all of the image-safe data fields.
<code>zisview -h</code>	Displays help for zisview.

63.3.3 Image-Safe Data Editor

After booting a workstation from an imaging device, you can enter `zisedit` at the Linux bash prompt to change, clear, or remove information the image-safe data for that workstation.

To use `zisedit`, enter any of the following commands at the Linux bash prompt:

Table 63-5 *Zisedit Bash Commands*

Command	Explanation
<code>zisedit</code>	Displays a screen showing all of the image-safe data fields. You can add or change any of the information in the fields.
<code>zisedit field=new_information</code>	<p>You can change the information for one field using this syntax, where <i>field</i> is any valid field name and <i>new_information</i> is the information you want this field to contain. <i>field</i> is not case sensitive.</p> <p>For example, enter <code>zisedit Mask=255.255.252.0</code> to enter this information in the <i>Subnet Mask</i> field.</p> <p>All of the following are valid field names. The corresponding minimum names that can also be entered on the command line are shown in parenthesis after each field name.</p> <p>JustImaged (J) ScriptedImage (SC) LastBaseImage (L) Tree (T) ObjectDN (ObjectDN) NetBIOSName (N) WorkGroup (WorkG) SID (SI) WorkstationID (Works) DHCP (DH) IP (I) Gateway (Gateway) Mask (M) DNSServerCount (DNSServerC) DNSServer1 (DNSServer1) DNSSuffix (DNSSu) DNSHostName (DNSH) PXESWorkRevision (PXESWorkR) PXESWorkObject (PXESWorkO) PXETaskID (PXETaskI) PXETaskState (PXETaskS) PXETaskRetCode (PXETaskR)</p>
<code>zisedit -c</code>	Clears all image-safe data fields.
<code>zisedit -r</code>	Removes the image-safe data store.
<code>zisedit -h</code>	Displays help for <code>zisedit</code> .

63.4 Imaging Floppy Boot Disk Creator (zimboot.exe)

Use the ZENworks Imaging Floppy Boot Disk Creator at a Windows workstation to:

- Create or update the `settings.txt` file so that you can boot workstations to perform imaging tasks
- Create a CD boot diskette for workstations that cannot be booted using a CD or DVD
- Create a PXE boot disk to be used with a workstation that cannot be PXE enabled

`Zimboot.exe` is located in the `sys:public\zenworks\imaging` directory in your ZENworks Desktop Management installation (on the ZENworks Imaging server). It is also accessible from the Tools menu of ConsoleOne.

For more information, see [Section 55.3, “Using the ZENworks Imaging Floppy Boot Disk Creator,” on page 633](#).

63.5 Imaging Configuration Parameters (Settings.txt)

The `settings.txt` file contains parameters that control how the imaging boot-up process occurs.

You should maintain the working copy of `settings.txt` at the root of the imaging boot device (CD or DVD, or ZENworks partition).

`Settings.txt` is a plain text file that contains various parameters, each on a separate line. Each parameter has the general format of `PARAMETER=value`. Lines that begin with a pound sign (#) are comments and are ignored during the imaging boot process.

You can edit this file manually in a text editor, manually using the *Load Settings from Disk* option in the `zimboot.exe` utility, or by making configuration changes in the `zimboot.exe` utility.

The format and function of each parameter in the `settings.txt` file are described in [Table 63-6](#):

Table 63-6 *Settings.txt Parameters*

Parameter	Description
MANUALREBOOT	<p>Specifies whether to access the bash prompt to reboot a workstation manually after it was booted from the imaging device in automatic mode. (If the workstation was booted from the imaging device in manual mode, you must always reboot the workstation manually.)</p> <p>If you boot a workstation from the imaging device and you let the boot process proceed in automatic mode, the ZENworks Imaging Engine starts and checks the ZENworks Imaging server to see if an imaging operation should be performed on the workstation. If so, it performs the imaging operation and then quits. If not, it quits without doing anything.</p> <p>What happens next depends on how you set this parameter. If you leave it commented out or set it to <i>No</i>, you are prompted to remove the imaging device (such as the CD or diskette, if necessary) and press any key to reboot the workstation to the native operating system. If you set this parameter to <i>Yes</i>, the workstation doesn't reboot automatically but instead displays the Linux prompt, allowing you to perform additional imaging-related tasks using the Linux menu or at the command line. This is helpful if you want to do things like check the current partition information or the image-safe data before booting to the native operating system.</p> <p>Example: <code>MANUALREBOOT=YES</code></p>
PARTITIONSIZE	<p>The number of megabytes to allocate to the ZENworks partition if you choose to create one locally on a workstation when you boot the workstation from the imaging device. The default size is 150 MB. The minimum partition size is 50 MB. The maximum size allowed is 2048 MB (2 GB). If you plan to store an image in the ZENworks partition, for example to enable the workstation to be restored to a certain state without connecting to the network, you might want to specify a larger size for this parameter.</p> <p>Example: <code>PARTITIONSIZE=500</code></p>
netsetup	<p>If you are using DHCP, keep this option enabled. If you are using a specific IP address, replace "dhcp" with "1" and uncomment and configure the other three IP address lines (HostIP, NETMASK, and GATEWAY).</p> <p>Example: <code>netsetup=dhcp</code></p>
HostIP	<p>The IP address used by a device to communicate on the network when you boot the device from the imaging device, if a static IP address is needed.</p> <p>Example: <code>HostIP=137.65.95.126</code></p> <p>If you want DHCP to be used, leave this and the next two parameters commented.</p>
NETMASK	<p>The subnet mask to be used by the workstation, if the workstation is using a static IP address.</p> <p>Example: <code>NETMASK=255.255.252.0</code></p> <p>If DHCP is being used, leave this parameter commented.</p>

Parameter	Description
GATEWAY	<p>The IP address of the gateway (router) to be used by the workstation, if the workstation is using a static IP address.</p> <p>Example: GATEWAY=137.65.95.254</p> <p>If DHCP is being used, leave this parameter commented.</p>
NAMESERVER	<p>The list of DNS name servers, by IP address, to use for resolving DNS domain names used on this workstation. Use a space to separate entries.</p> <p>Example: NAMESERVER=123.45.6.7 123.45.6.9</p> <p>If DHCP is being used, leave this parameter commented.</p>
DOMAIN	<p>The list of DNS domain suffixes to be used to identify connections used by this workstation. Use a space to separate entries.</p> <p>Example: DOMAIN=example.novell.com example.xyz.org</p> <p>If DHCP is being used, leave this parameter commented.</p>
PROXYADDR	<p>The IP address or full DNS name of the imaging (proxy) server to connect to when you boot a workstation from the imaging device in auto-imaging mode.</p> <p>Examples:</p> <p>PROXYADDR=137.65.95.127 PROXYADDR=imaging.xyz.com</p> <p>This parameter is used to set the PROXYADDR environment variable in Linux when the workstation is booted from the imaging device. The ZENworks Imaging Engine then reads this variable to determine which server to contact if it's running in automatic mode. Whether it's running in automatic or manual mode, the ZENworks Imaging Engine attempts to log the imaging results to the server specified in this variable.</p>
export PS1="\`pwd \`#"	Configures the string used by the bash shell. You can change the string by editing the text after the = symbol. The ' character is not a single quote mark, but is from the ~ key.
export IMGCMD	Use this parameter to alter the behavior of automated imaging. If this variable is defined as a script (or a series of commands), then that script (or those commands) are executed instead of the usual img auto command (see <code>/bin/imaging.s</code>).
netdevice=eth0	Selects a specific network adapter. If necessary, replace eth0 with the correct interface.

63.6 Imaging Boot Parameters

ZENworks Imaging, by default, loads PCMCIA, SCSI, and USB drivers. When performing imaging work using CDs or DVDs, some computers, particularly laptops, with PCMCIA, SCSI, or USB cards can hang during the boot process. Although loading these drivers does not normally cause problems, you can use command line parameters to prevent these drivers from loading. Also, if you have computers that use PCMCIA cards, you can choose to have the PCMCIA driver load earlier in the boot process if these computers experience problems loading the driver during a normal boot process.

You can use the following parameters at the command prompt:

Table 63-7 *Imaging Boot Parameters*

Parameter	Description
PCMCIA	Whether to load a PCMCIA device during the boot process. Example: manual PCMCIA=NO
PCMCIABOOT	Whether to load a PCMCIA device earlier during the boot process (for example, a PCMCIA CDROM device). Example: manual PCMCIABOOT=YES
SCSI	Whether to load a SCSI device during the boot process. Example: manual SCSI=NO
USB	Whether to load a USB device during the boot process. Example: manual USB=NO

63.7 Imaging Server (Imgserv.nlm or .dll or .dlm, or Linux Daemons)

The ZENworks Imaging server is a software component of the Desktop Management server. It enables imaging clients (workstations that are booted from an imaging device) to connect with the network to receive imaging services, including:

- Storage or retrieval of an image on a server
- Automatic imaging based on an eDirectory policy or setting
- Logging the results of an imaging operation
- A multicast imaging session

Use the ZENworks Imaging server to do the following:

- [Section 63.7.1, “Initiating the Imaging Processes on Linux Imaging Servers,” on page 762](#)
- [Section 63.7.2, “Initiating the Imaging Processes on Windows or NetWare Imaging Servers,” on page 769](#)
- [Section 63.7.3, “Viewing Information About Imaging Requests,” on page 769](#)
- [Section 63.7.4, “Starting a Manual Multicast Session,” on page 770](#)

63.7.1 Initiating the Imaging Processes on Linux Imaging Servers

An imaging server daemon is initiated by running the script at the Linux terminal program command line, which in turn calls the executable and uses the configuration set in the corresponding `.conf` file. Because the scripts do not normally accept parameters, but only arguments (such as `start`), you can configure parameters in their corresponding `.conf` files.

The following Linux daemons and library file run the imaging server processes:

- [“libzmgserv.so” on page 762](#)
- [“novell-proxydhcp” on page 762](#)
- [“novell-tftp” on page 764](#)
- [“novell-zmgprebootpolicy” on page 766](#)
- [“Understanding Script Arguments” on page 768](#)

libzmgserv.so

The `libzmgserv.so` library file is used by eDirectory to provide imaging services to the devices.

This library file is used automatically by eDirectory when installing ZENworks Linux Management, or when rebooting the server.

novell-proxydhcp

The `novell-proxydhcp` daemon provides PXE devices with the information that they require in order to connect to the ZENworks Preboot Services system.

This daemon is not started automatically when installing ZENworks Linux Management.

- [“Understanding the novell-proxydhcp Components” on page 762](#)
- [“Configuring novell-proxydhcp” on page 763](#)

Understanding the novell-proxydhcp Components

To initiate the `novell-proxydhcp` daemon, enter the following command listed for Script Location on the Linux command line in a terminal program:

```
/etc/init.d/novell-proxydhcp
```

This command executes `/opt/novell/bin/novell-proxydhcpd`.

The following script arguments are available for the `novell-proxydhcp` command:

<code>start</code>	<code>restart</code>	<code>status</code>	<code>install</code>
<code>stop</code>	<code>force-reload</code>	<code>showpid</code>	

For descriptions of these arguments, see [“Understanding Script Arguments” on page 768](#).

Configuring novell-proxydhcp

The novell-proxydhcp configuration file (`/etc/opt/novell/novell-proxydhcp.conf`), contains the following parameters:

Table 63-8 *Novell-proxydhcp Parameters*

Parameter	Description
LocalDHCPFlag = 0	<p>Indicates whether the DHCP server for this subnet resides on the same server as novell-proxydhcp.</p> <p>0 (the default) means novell-proxydhcp is not running on the same server as the DHCP service. 1 means they are running on the same server.</p> <p>The Proxy DHCP server needs to behave slightly differently if it is loaded on the same server as the DHCP service.</p>
LocalInterface = 10.0.0.1	<p>Indicates the IP address to be used by the Proxy DHCP server. This setting is intended only for use on servers with multiple LAN interfaces. The IP address must be valid on the server.</p> <p>By default, this parameter is commented out.</p>
NovellPolicyEngine = 10.0.0.1	<p>The IP address of the server where a Novell Preboot policy engine is running. Most often, this is a ZENworks imaging daemon. If no value is specified, the Proxy DHCP assumes that the daemon is running on the same server.</p> <p>By default, this parameter is commented out.</p>
NBPx86 = nvlnbp.sys	<p>The name of the boot file this service suggests for all x86 computers, such as <code>nvlnbp.sys</code>.</p>
MenuTimeout = 2	<p>The number of seconds the F8 menu is displayed before automatically choosing the first option, which is always this server and its default NBP. The default is 2 seconds.</p>
ProxyLogLevel = 2	<p>The value assigned here determines which events are entered in <code>novell-proxydhcp.log</code>. Specifying a high level in an active system can quickly fill the log. Valid values are 0, 1, 2, 3, and 4. The default is 2.</p> <p>Each message from the Proxy DHCP server is assigned a priority level. If <i>ProxyLogLevel</i> is set to a value equal to or greater than a message's priority level, that message is entered in <code>novell-proxydhcp.log</code>. All other messages are ignored.</p> <p>Priority meaning:</p> <ul style="list-style-type: none">0: Critical information. Service start, stop, and critical events are logged.1: Warning information. Additionally, warning information is logged.2: Transaction information. All completed client transactions are logged.3: Request information. All client requests and Proxy DHCP requests received are logged, including ignored requests. If a request is ignored, the reason for ignoring it is also logged.4: Debugging information. All DHCP packets received and accepted are decoded and logged.

Parameter	Description
ProxyLogFile = /var/opt/novell/log/novell-proxydhcp.log	<p>The file where all log file entries are placed. It is located at /var/opt/novell/log/novell-proxydhcp.log.</p> <p>By default, this parameter is commented out.</p>
ProxyLogFileSize = 15	<p>The size of the ProxyLogFile file is controlled by the value of ProxyLogFileSize, where 15 is the default (in MB).</p> <p>When the log file exceeds the ProxyLogFileSize value, it is deleted and restarted.</p>

Parameters that are not commented out, but contain no values, are given a default value.

The novell-proxydhcp daemon is compliant with the following RFCs:

RFC 2131: Dynamic Host Configuration Protocol

RFC 2132: DHCP Options and BOOTP Vendor Extensions

The novell-proxydhcp daemon is compliant with the Preboot eXecution Environment (PXE) Specification v2.1 industry specification, published by Intel.

novell-tftp

The novell-tftp daemon provides TFTP services to imaging clients.

This daemon is started automatically when installing ZENworks Linux Management, or when rebooting the server.

- [“Understanding the novell-tftp Components” on page 764](#)
- [“Configuring novell-tftp” on page 765](#)

Understanding the novell-tftp Components

To initiate the novell-tftp daemon, enter the following command (listed under Script Location) on the Linux command line in a terminal program:

```
/etc/init.d/novell-tftp
```

This command executes /opt/novell/bin/novell-tftpd.

The following script arguments are available for the novell-tftp command:

start	restart	status
stop	force-reload	showpid

For descriptions of these arguments, see [“Understanding Script Arguments” on page 768](#).

Configuring novell-tftp

The novell-tftp configuration file (`/etc/opt/novell/novell-tftp.conf`), contains the following parameters for the Novell TFTP server:

Table 63-9 *Novell-tftp Parameters*

Parameter	Description
TFTPInterface = 10.0.0.1	<p>The IP address that is used for all TFTP communications. If a value is not given here, the service tries to detect one.</p> <p>This value is most useful for multihomed servers.</p> <p>By default, this parameter is commented out.</p>
TransferBlockSize = 1428	<p>This value determines the size of the data block used by the TFTP server to transmit and receive data to and from a client. Valid values are between 512 and 4428.</p> <p>For Ethernet networks, this value should be 1428.</p> <p>For token ring networks, this value can be 4428, but only if you are sure there are no Ethernet segments; otherwise, use 1428.</p> <p>Older TFTP clients might be restricted to 512 bytes, which is the original transfer block size before the adoption of RFC 2348. The Novell TFTP server is compatible with these clients.</p> <p>By default, this parameter is commented out.</p>
TimeoutInterval = 1	<p>This is the amount of time (in seconds) that the TFTP server waits for a client to acknowledge before resending a packet. However, because the TFTP server uses an adaptive algorithm to calculate the actual timeout interval, this value is only used as an initial value. It can increase or decrease, depending on the performance of the network.</p> <p>This value is only a default. It can be changed at the request of a client. See RFC 2349.</p> <p>Valid values are 1 through 60.</p> <p>By default, this parameter is commented out.</p>
Linux -- TFTPDirectory = /srv/tftp	<p>TFTPDirectory is the directory where the TFTP server can store and retrieve files. All paths submitted to the TFTP server by clients are assumed to be relative to this directory.</p> <p>Because TFTP has no security, it is suggested that you not place files with sensitive information in this directory, and that you place a space quota on it.</p> <p>The TFTP server does not load if this directory does not exist.</p> <p>By default, this parameter is commented out.</p>
TFTPAllowWrites = 1	<p>This variable tells the TFTP server whether to allow users to place new files on the server. Setting this variable to 0 makes the TFTP server more secure by not allowing users to place new files on the server. The other option is 1 (the default), which allows users to place new files on the server.</p>

Parameter	Description
TFTPLogLevel = 2	<p>The value assigned here determines which events are entered in <code>novell-tftp.log</code>. Specifying a high level in an active system can quickly fill the log. Valid values are 0, 1, 2, 3, and 4. The default is 2.</p> <p>Each message from the TFTP server is assigned a priority level. If TFTPLogLevel is set to a value equal to or greater than a message's priority level, that message is entered in <code>novell-tftp.log</code>. All other messages are ignored.</p> <p>Priority meaning:</p> <p>0: Critical information. Service start, stop, and critical events are logged.</p> <p>1: Warning information. Only failed client transactions are logged.</p> <p>2: Transaction information. All completed client transactions are logged.</p> <p>3: Request information. All client requests and TFTP options are logged.</p> <p>4: Debugging information. All server events, including each packet received, are logged.</p> <p>By default, this parameter is commented out.</p>
TFTPLogFile = /var/opt/novell/log/novell-tftp.log	<p>The file where all log file entries are placed.</p> <p>By default, this parameter is commented out.</p>
TFTPLogFileSize = 15	<p>The size of the log file is controlled by the value of TFTPLogFileSize, where 15 is the default (in MB).</p> <p>When the log file exceeds the TFTPLogFileSize value, it is deleted and restarted.</p> <p>By default, this parameter is commented out.</p>

Parameters that are not commented out, but contain no values, are given a default value.

The novell-tftp daemon is compliant with the following RFCs:

- RFC 1350: THE TFTP PROTOCOL (REVISION2)
- RFC 2347: TFTP Option Extension
- RFC 2348: TFTP Blocksize Option
- RFC 2349: TFTP Timeout Interval and Transfer Size Options

novell-zmgprebootpolicy

The novell-zmgprebootpolicy daemon allows PXE devices to query the ZENworks Linux Management system for work to do and for Preboot Menu policies.

This daemon is started automatically when installing ZENworks Linux Management, or when rebooting the server.

- [“Understanding the novell-zmgprebootpolicy Components” on page 767](#)
- [“Configuring novell-zmgprebootpolicy” on page 767](#)

Understanding the novell-zmgprebootpolicy Components

To initiate the novell-zmgprebootpolicy daemon, enter the following command (listed under Script Location) on the Linux command line in a terminal program:

```
/etc/init.d/novell-zmgprebootpolicy
```

This command executes /opt/novell/zenworks/preboot/bin/novell-zmgprebootpolicyd.

The following script arguments are available for the novell-zmgprebootpolicy command:

- start
- restart
- status
- stop
- force-reload
- showpid

For descriptions of these arguments, see “Understanding Script Arguments” on page 768.

Configuring novell-zmgprebootpolicy

The novell-zmgprebootpolicy configuration file (/etc/opt/novell/zenworks/preboot/novell-zmgprebootpolicy.conf), contains the following parameters:

Table 63-10 Novell-zmgprebootpolicy Parameters

Parameter	Description
LocalInterface = 10.0.0.1	<p>The IP address that is used by the policy server.</p> <p>This setting is intended only for use on servers with multiple LAN interfaces. The address must be valid on the server.</p> <p>By default, this parameter is commented out.</p>
PolicyLogLevel = 1	<p>The value assigned here determines which events are entered in novell-zenprebootpolicy.log. Specifying a high level in an active system can quickly fill the log. Valid values are 0, 1, 2, 3, and 4. The default is 2.</p> <p>Each message from the novell-zmgprebootpolicy server is assigned a priority level. If PolicyLogLevel is set to a value equal to or greater than a message's priority level, that message is entered in novell-zenprebootpolicy.log. All other messages are ignored.</p> <p>Priority meaning:</p> <p>0: Critical information. Service start, stop, and critical events are logged.</p> <p>1: Warning information. Only failed client transactions are logged.</p> <p>2: Transaction information. All completed client transactions are logged.</p> <p>3: Request information. All client requests are logged.</p> <p>4: Debugging information. All server events, including each packet received, are logged.</p> <p>By default, this parameter is commented out.</p>

Parameter	Description
PolicyLogFile = /var/opt/novell/log/zenworks/preboot/novell-zenprebootpolicy.log	The file where all log file entries are placed. By default, this parameter is commented out.
PolicyLogFileSize = 15	The size of the log file is controlled by the value of PolicyLogFileSize, where 15 is the default (in MB). When the log file exceeds the PolicyLogFileSize value, it is deleted and restarted.
PrebootServer = 10.0.0.5	This field contains the address of the ZENworks Imaging server that should be used to resolve policies. By default, this parameter is commented out.

Parameters that are not commented out, but contain no values, are given a default value.

Understanding Script Arguments

The following arguments are available for each of the Preboot Services daemons described above:

Table 63-11 *Script Arguments*

Argument	Function
start	Starts the daemon. Because novell-proxydhcp is optional, use this argument to start this daemon. However, this daemon does not automatically start when the server reboots. (See install below.)
stop	Stops the daemon.
restart	Stops and restarts the daemon if it is already running.
force-reload	Causes the daemon's configuration file to be reloaded.
status	Displays the current status of the daemon. For example, if you enter <code>/etc/inid.d/novell-proxydhcp status</code> , information similar to the following is returned: Novell ZENworks Proxy DHCP Service running
showpid	Displays the daemon's process ID. For example, if you enter <code>/etc/inid.d/novell-proxydhcp showpid</code> , information similar to the following is returned: Novell ZENworks Proxy DHCP Service running 10211
install	For novell-proxydhcp only, causes the daemon to be automatically loaded when the server boots.

63.7.2 Initiating the Imaging Processes on Windows or NetWare Imaging Servers

The ZENworks Imaging server modules are located on a NetWare server in `sys:\system` or on a Windows server in the directory where eDirectory is installed (such as `c:\novell\nds`).

In most environments, the ZENworks Imaging server starts automatically when you reboot the server after installing Desktop Management. With eDirectory 8.5 on Windows, you must start the ZENworks Imaging server manually as follows: from the directory where eDirectory is installed, double-click `ndscons.exe`, select the `imgsrv.dlm` service, then click *Start*. You might also want to click *Startup* to configure the service to start automatically each time the server reboots.

You can use the following parameters with the ZENworks Imaging server:

Table 63-12 ZENworks Imaging Server Parameters

Parameter	Description
<code>-i:ip_address</code>	Used in a clustering environment to specify the IP address of the virtual server. This parameter is automatically set during installation in a clustering environment. You can also use this parameter in a multiple-NIC environment to bind the ZENworks Imaging server to a specific IP address.
<code>-s:DN</code>	Used in a clustering environment to specify the DN of the virtual server. If the DN contains spaces, enclose the DN in quotation marks. This parameter is automatically set during installation in a clustering environment.

63.7.3 Viewing Information About Imaging Requests

After the ZENworks Imaging server has started, you can view information about the status and results of the imaging requests that it has received from imaging clients. A statistical summary of these requests is shown on the NetWare server console, in a window accessible from the Windows taskbar, or on the Linux server's terminal program command line. The statistics shown on this screen are explained below. All statistics are reset to zero when you restart the ZENworks Imaging server.

Table 63-13 Imaging Request Statistics

Statistic	Specifies
Update Requests	The number of imaging requests of any kind that have been received by the ZENworks Imaging server since it was started. This includes requests that failed, were denied, or were referred to other Imaging servers (see Client Referrals below). Information about each of these requests is logged on the ZENworks Imaging server, including the source, type, date/time, and results, as explained in Section 63.8, "Imaging Server Log (Zimglog.xml)," on page 770 .
Images Sent	The number of images that the ZENworks Imaging server has sent to imaging clients since the ZENworks Imaging server was started. This includes only images that are retrieved from this ZENworks Imaging server. See Client Referrals below for more information.

Statistic	Specifies
Images Received	The number of new images that have been received and stored on the ZENworks Imaging server since it was started. This includes images that were received through client referrals (see Client Referrals below).
Client Referrals	The number of client requests that have been referred (redirected) by the ZENworks Imaging server to other ZENworks Imaging servers since this ZENworks Imaging server was started. Such referrals are made only when the client is running in auto-imaging mode and the ZENworks Imaging server determines from eDirectory that the image to be created or retrieved is on a different ZENworks Imaging server.
IMPORTANT: If a client is running in manual imaging mode and it requests to store or retrieve an image on a different ZENworks Imaging server, the request is denied and an error is returned to the client. Referrals are currently supported only when the client is running in auto-imaging mode.	

63.7.4 Starting a Manual Multicast Session

On the server console (NetWare) or in a window accessible from the system tray (Windows), you can start a manual multicast session, see any sessions in progress, and delete sessions. For more information, see [“Initiating a Multicast Session from Each Client”](#) on page 734 in [Chapter 62](#), [“Multicasting Images,”](#) on page 725.

63.8 Imaging Server Log (Zimglog.xml)

Zimglog.xml is a chronological record of all imaging requests that have been received by the ZENworks Imaging server since it was installed and first started, including requests merely to log information about imaging operations serviced elsewhere. For each imaging request, the ZENworks Imaging server logs information such as the source, type, date/time, and results of the request.

Zimglog.xml is created on a NetWare server in `sys:\system`, or on a Windows server at the root of the drive where eDirectory is installed (such as `c:\`). It is not created on a Linux server.

Zimglog.xml is an XML file. The oldest imaging request is logged at the top of the file and the most recent at the bottom. The file continues to grow unless you trim it manually (using a text editor) or delete it. It isn't cleared if you restart the ZENworks Imaging server.

Each imaging operation is entered in the log as a group of lines. For example, the log file shown below has two entries: one describing a successful *upload* operation and another describing a failed *download* operation. (An *upload* is the taking of a client image and storing it on the ZENworks Imaging server or other available (local) medium. A *download* is the retrieval of a client image from the ZENworks Imaging server or local medium and putting it down on the client.)

```
<ZENImageLog>

<CN=CV7PB00:C0:4F:DC:2A:B5.O=sales>
<Tree>XYZ</Tree>
<Status>Success</Status>
<Operation>Upload</Operation>
<ImageType>Base Image</ImageType>
<ImagePath>\\XYZ_SERVER\sys\imgs\dell_nt.zmg</ImagePath>
```

```

<Timestamp>Thur Nov 22 13:10:05 2001
</Timestamp>
</CN=CV7PB00:C0:4F:DC:2A:B5.O=sales>

<CN=CV7PB00:C0:4F:DC:2A:B5.O=sales>
<Tree>XYZ</Tree>
<Status>Failure</Status>
<ErrorMessage>Unable to find an image to download</ErrorMessage>
<Operation>Download</Operation>
<Timestamp>Thur Nov 22 13:13:17 2001
</Timestamp>
</CN=CV7PB00:C0:4F:DC:2A:B5.O=sales>

</ZENImageLog>

```

Table 63-14 describes the various XML elements that comprise the log entries shown above. Each element has an opening and closing tag, such as `<tree>` and `</tree>`. The outermost element contains all of the other elements in the entry.

Table 63-14 XML Elements for the *Zimglog.xml* Log Entries

XML Element	Specifies
<i>outermost_container</i>	The distinguished eDirectory name of the workstation that requested the imaging operation. This name is read by the ZENworks Imaging Engine from the workstation's image-safe data . If the workstation name isn't found (for example, if the workstation hasn't been registered as an object in eDirectory), the name of the ZENworks Imaging server that serviced the request is given instead (for example, XYZ_SERVER).
Tree	The eDirectory tree containing the workstation or server specified in the <i>Outermost_Container</i> element.
Status	Whether the requested imaging operation succeeded or failed.
ErrorMessage	The reason why the requested imaging operation failed, if applicable.
Operation	Whether the requested imaging operation was an upload or download attempt. An upload is the taking of a client image and storing it on the ZENworks Imaging server or other available (local) medium. A download is the retrieval of a client image from the ZENworks Imaging server or local medium and putting it down on the client. NOTE: Occasionally, you might see an entry in the log that omits the Operation element. Such an entry is typically a follow-up to the previous operation. For example, you might see an entry indicating that a download operation was successful, but the next entry (time-stamped a few seconds later and specifying no operation) might indicate that the ZENworks Imaging server failed to get image-safe data from eDirectory. In this case you could assume that the client that just received the download didn't have its own image-safe data , and so the ZENworks Imaging server was trying to get that data from eDirectory to apply it to the client.

XML Element	Specifies
ImageType	Whether the image that was created or retrieved is a base image or an add-on image. With a base image, all existing partitions and data are removed before the image is put down. With an add-on image, the existing partitions are left intact and are merely augmented with additional data.
ImagePath	The full path and filename of the image that was created, retrieved, or requested.
Timestamp	The time when the results of the requested imaging operation were logged by the ZENworks Imaging server, including the week day, month, date, 24-hour time (including seconds), and year.

ZENworks Imaging Engine Commands

64

After booting a workstation from an imaging device, you can use the `img` command at the Linux bash prompt or the ZENworks® Imaging Engine menu to do any of the following:

- Take an image of the workstation's hard disks
- Put down an image on the workstation's hard disks
- View or manipulate the workstation's hard-disk partitions
- View the workstation's hardware configuration or image-safe data
- Display a menu from which you can also perform all of these tasks

The ZENworks Imaging Engine is installed to the `/bin` directory on the imaging boot device. If the imaging boot device is a CD or DVD, the `/bin` directory is actually archived in the `root.tgz` file, which is expanded during the imaging boot process. If the imaging boot method is Preboot Services, the ZENworks Imaging Engine is downloaded to the workstation when booting.

Because the ZENworks Imaging Engine is a Linux application, the command syntax is case sensitive. The overall syntax is:

```
img [mode]
```

where *mode* is any of the modes described in the sections below.

NOTE: Each mode can be abbreviated to the first letter of its name. For example, `img dump` can be abbreviated `img d`.

- [Section 64.1, “Help Mode \(img help\),” on page 774](#)
- [Section 64.2, “Auto Mode \(img auto\),” on page 774](#)
- [Section 64.3, “Make Mode \(img make\),” on page 775](#)
- [Section 64.4, “Restore Mode \(img restore\),” on page 778](#)
- [Section 64.5, “Session \(Multicast\) Mode \(img session\),” on page 782](#)
- [Section 64.6, “Partition Mode \(img p\),” on page 784](#)
- [Section 64.7, “ZENPartition Mode \(img zenPartition\),” on page 786](#)
- [Section 64.8, “Dump Mode \(img dump\),” on page 786](#)
- [Section 64.9, “Information Mode \(img info\),” on page 787](#)

To access the ZENworks Imaging Engine menu from which to perform all of these tasks, enter `img` with no parameters.

64.1 Help Mode (img help)

Use Help mode to get information about the `img` command if you don't have documentation available.

To use the Help mode:

- 1 Do one of the following:

- Enter:

```
img [help [mode]]
```

where *mode* is the mode whose command syntax you want help with.

Examples:

Example	Explanation
<code>img help</code>	Displays a short description of each mode.
<code>img help m</code>	Displays information on how to use the Make mode.
<code>img help p</code>	Displays information on how to use the Partition mode.

- Enter `img` to display the ZENworks Imaging Engine menu, select *Help*, then select a mode name.

64.2 Auto Mode (img auto)

Use Auto mode to image the workstation automatically, based on any applicable Novell® eDirectory™ policies and settings. The ZENworks Imaging Engine runs in this mode if you let the imaging boot process proceed without interruption, or if you enter the command listed below at the Linux prompt.

To use the Auto mode, do any of the following at the bash prompt:

- Enter:

```
img auto
```

- To display the ZENworks Imaging Engine menu, enter:

```
img
```

and on the menu bar, click *Imaging*, then click *Query for work*.

- To display the ZENworks Imaging Engine menu, enter:

```
img
```

then click *F9 Query for work* on the taskbar.

- To display the ZENworks Imaging Engine menu, enter:

```
img
```

then press *F9*.

In this mode, the ZENworks Imaging Engine queries the ZENworks Imaging server specified in the `PROXYADDR` environment variable for any work to do. The ZENworks Imaging server checks the relevant eDirectory policies and settings to determine what imaging tasks should be performed (if

any), such as taking or putting down an image. It then instructs the ZENworks Imaging Engine to perform those tasks. If any tasks involve storing or retrieving images on other ZENworks Imaging servers, the ZENworks Imaging server refers the ZENworks Imaging Engine to those servers to complete those tasks. After the ZENworks Imaging Engine has completed its work, it communicates the results to the original ZENworks Imaging server, and the results are logged on that server.

For information on configuring the eDirectory policies and settings that control what happens in this mode, see [Chapter 58, “Setting Up Imaging Policies,” on page 697](#).

64.3 Make Mode (img make)

Use the Make mode to take an image of the workstation and store it in a specified location. Normally, all partitions on hard disks and other storage devices (such as Jaz drives) are included in the image, but there are some exceptions noted in [Table 64-1 on page 776](#).

You can take an image of a workstation using either the bash prompt or using the ZENworks Imaging Engine menu. For step-by-step instructions, see [Section 60.1, “Manually Taking an Image of a Workstation,” on page 711](#). You can also use the Make Locally mode to take an image of the workstation and store it in a partition on a local (writable) device, such as a hard disk or Jaz drive. For step-by-step instructions, see [Chapter 61, “Setting Up Disconnected Imaging Operations,” on page 719](#).

The image size is about the size of the data in the Windows partitions plus the entire size of any non-Windows partitions (such as NetWare[®] partitions). ZENworks partitions and Compaq configuration partitions are always excluded. The data from Windows partitions is stored in an intelligent, file-by-file format so you can customize it later using the [Image Explorer \(imgexp.exe\)](#) utility. Non-Windows partitions are stored in a raw, bit-by-bit format that cannot be customized.

The syntax of this mode depends on whether you store the image locally or on an Imaging (proxy) server.

The following sections contain additional information:

- [Section 64.3.1, “Make Locally \(img makel\),” on page 776](#)
- [Section 64.3.2, “Make on Proxy \(img makep\),” on page 777](#)

64.3.1 Make Locally (img makel)

Using the bash prompt, the following example explains the syntax and available parameters that you can use with the makel “make locally” parameter:

```
img makel [pNumber] filepath [comp=comp level] [xpartition]
```

Commands

Table 64-1 *Img Makel Parameters*

Parameter	Description
<code>makel[pNumber]</code>	<p>The partition number (as displayed by <code>img dump</code>) of the local partition to store the image in. It must be a primary FAT16 or FAT32 partition. This partition is excluded from the image that's created.</p> <p>If you omit the partition number from this parameter, the image is stored in the local ZENworks partition.</p>
<code>filepath</code>	The image filename, including a <code>.zmg</code> extension (case-sensitive) and the complete path from the root of the partition. The directories in the path must exist. If the file already exists, it is overwritten.
<code>[comp=comp level]</code>	<code>comp level</code> is the amount of compression used when creating the image. Specify any number from 0-9. 0 means no compression. 1 is the same as Optimize for Speed. 6 is the same as Balanced and is used by default if you do not specify this parameter. 9 is the same as Optimize for Space.
<code>xpartition</code>	<p>The partition number (as displayed by <code>img dump</code>) of a local partition to exclude from the image. You can repeat this parameter as needed to exclude multiple partitions.</p> <p>If you omit this parameter, all partitions are included in the image except the one where the image is stored.</p>

Examples

Table 64-2 *Img Makel Examples*

Example	Explanation
<code>img makel8 /imgs/dellnt.zmg</code>	Takes an image of all partitions except the one in slot 8 and saves the image to <code>imgs/dellnt.zmg</code> in the partition in slot 8. (This example assumes that slot 8 contains a primary FAT16 or FAT32 partition.)
<code>img makel /imgs/dellnt.zmg</code>	Takes an image of all partitions and saves it to <code>imgs/dellnt.zmg</code> in the ZENworks partition. (This example assumes that the ZENworks partition is installed.)
<code>img makel /imgs/dellnt.zmg x2 x3</code>	Takes an image of all partitions except those in slots 2 and 3 and saves the image to <code>imgs/dellnt.zmg</code> in the ZENworks partition. (This example assumes that the ZENworks partition is installed.)

64.3.2 Make on Proxy (img makep)

Using the bash prompt, the following example explains the syntax and available parameters that you can use with the makep “make on proxy” parameter:

```
img makep address filepath [comp=comp level] [xpartition]
```

Commands

Table 64-3 *Img Makep Parameters*

Parameter	Description
address	The IP address or DNS name of the ZENworks Imaging server where the image is stored. This can be any server running the Imaging Proxy service.
filepath	<p>The UNC path to the new image file being created, including the image filename and the .zmg extension (case-sensitive). The format of the UNC path is as follows:</p> <pre>//servername/volume_or_share/path_to_store_images/ imagename.zmg</pre> <p>For OES Linux, the path to the image file must be from root (/). For example, the path might look like:</p> <pre>//servername/media/nss/NSS_volume/path_to_image/ imagefilename.zmg</pre> <p>Upon execution of <code>img makep</code> at the command line, the <i>servername</i> portion of this path is replaced with the value in the address portion of this syntax.</p> <p>The image filename, including a .zmg extension (case-sensitive) and the complete path in UNC style. The directories in the path must exist. If the file already exists, the ZENworks Imaging server won't overwrite it unless you enable it to do so in the ZENworks Imaging server's policy in eDirectory. (See Section 58.3, “Allowing Overwriting Filenames and Restricting the Save Location of Image Files (Imaging Server Settings),” on page 701.) If no directories are specified in the path, the image is created at the root of the volume or drive where the ZENworks Imaging server software is installed.</p> <p>IMPORTANT: Because Linux doesn't recognize backslashes, you must use forward slashes in the UNC path or enclose the entire path in quotes.</p>
[comp=comp level]	<i>comp level</i> is the amount of compression used when creating the image. Specify any number from 0-9. 0 means no compression. 1 is the same as Optimize for Speed. 6 is the same as Balanced and is used by default if you do not specify this parameter. 9 is the same as Optimize for Space.
xpartition	<p>The partition number (as displayed by <code>img dump</code>) of a local partition to exclude from the image. You can repeat this parameter as needed to exclude multiple partitions.</p> <p>If you omit this parameter, all partitions are included in the image.</p>

Examples

Table 64-4 *Img Makep Examples*

Example	Explanation
<code>img makep 137.65.95.127 /xyz_server/sys/imgs/dellnt.zmg</code>	Takes an image of all partitions and saves it to <code>sys/imgs/dellnt.zmg</code> on <code>xyz_server</code> . (This example assumes that 137.65.95.127 is the IP address of <code>xyz_server</code> .)
<code>img makep img.xyz.com //xyz_server/sys/imgs/dellnt.zmg x2 x3</code>	Takes an image of all partitions except those in slots 2 and 3 and saves the image to <code>sys/imgs/dellnt.zmg</code> on <code>xyz_server</code> . (This example assumes that <code>img.xyz.com</code> is the DNS name of <code>xyz_server</code> .)
<code>img makep img.xyz.com //bogus/sys/imgs/dellnt.zmg</code>	Takes an image of all partitions and saves the image to <code>sys/imgs/dellnt.zmg</code> on <code>img.xyz.com</code> . (This example assumes that <code>img.xyz.com</code> is the DNS name of a server running the Imaging Proxy service).
	Because the servername inside the UNC path is replaced by the address value defined earlier in the cmd line, <code>//bogus</code> becomes <code>//img.xyz.com</code>

64.4 Restore Mode (img restore)

Use the Restore mode to retrieve an image from a specified location and put it down on a workstation.

You can restore an image of a workstation using either the bash prompt or using the ZENworks Imaging Engine menu. For step-by-step instructions, see [Section 60.2, “Manually Putting an Image on a Workstation,” on page 715](#). You can also use the Restore mode to restore an image from a partition on a local (writable) device, such as a hard disk or Jaz drive. For step-by-step instructions, see [Chapter 61, “Setting Up Disconnected Imaging Operations,” on page 719](#).

Normally, if the image to be put down is a base image (one created previously by the ZENworks Imaging Engine), all existing partitions except ZENworks Linux and Compaq configuration partitions are removed from all local writable devices (such as hard disks and Jaz drives) before the new image is put down. When the image is put down, the sizes of the original partitions from which the image was taken are preserved if possible. If there is insufficient space, the last partition is sized to fit unless it results in data loss, in which case the ZENworks Imaging Engine denies the requested operation. If there is extra space left after all partitions in the image have been restored to their original sizes, that space is left unpartitioned.

If the image to be put down is an add-on image (one produced from an Application object or created by the **Image Explorer (imgexp.exe)** utility), or if it's a base image and you specify the `apartition:ppartition` parameter, none of the existing physical partitions are removed. Instead, the appropriate partitions are updated with the files from the image. The update process does not remove any existing files or overwrite any existing files of the same names if they are newer.

Restoring add-on images over 4 GB in size is not supported by Desktop Management imaging.

The syntax of this mode depends on whether you retrieve the image from a local device or from an Imaging (proxy) server, as explained in the subsections below:

- [Section 64.4.1, “Restore from Local \(img restore\),” on page 779](#)
- [Section 64.4.2, “Restore from Proxy \(img restorep\),” on page 780](#)

64.4.1 Restore from Local (img restore)

Use the Restore from Local mode to retrieve an image from a local device and put it down on the workstation. For more information, see [Chapter 61, “Setting Up Disconnected Imaging Operations,” on page 719](#).

Using the bash prompt, the following example explains the syntax and available parameters that you can use with the restore “restore from local” parameter:

```
img restorel[pNumber] filepath [sfileset] [apartition:ppartition]
```

Commands

Table 64-5 *Img Restore Parameters*

Parameter	Description
restorel[pNumber]	<p>The partition number (as displayed by <code>img dump</code>) of the local partition to retrieve the image from. It must be a primary FAT16 or FAT32 partition. This partition is not changed by the imaging operation.</p> <p>If you omit the partition number from this parameter, the image is retrieved from the local ZENworks partition.</p>
filepath	The filename of the image to retrieve, including the <code>.zmg</code> extension (case-sensitive) and the complete path from the root of the partition.
sfileset	<p>The number of the image file set to put down. Valid values are 1 through 10. For information on creating file sets of an image, see Chapter 59, “Creating and Restoring Images,” on page 703.</p> <p>If you omit this parameter, file set 1 is used.</p>
apartition:ppartition	<p>A mapping between a partition in the image archive (<i>apartition</i>) and a target physical partition on the local machine (<i>ppartition</i>). Use this parameter to selectively restore a specific part of the image to a specific local partition.</p> <hr/> <p>IMPORTANT: If you use this parameter, none of the existing local partitions are removed, and only the target local partition is updated. The update process does not remove any existing files; however, any existing files of the same names are overwritten. If you want to remove all existing files from the target partition before updating it, first use <code>img pd</code> and <code>img pc</code> to delete and re-create the partition.</p> <hr/> <p>For <i>apartition</i>, use the partition number displayed for the source partition in the Image Explorer (imgexp.exe) utility. For <i>ppartition</i>, use the partition number displayed by <code>img dump</code> for the target partition. The target partition must be a Windows partition. You can repeat this parameter as needed to request multiple selective restorations in a single operation. In doing so, you can apply multiple parts of the image to a single local partition, but you can't apply the same part of an image to multiple local partitions in a single operation.</p>

Examples

Table 64-6 *Img Restorl Examples*

Example	Explanation
<code>img restore18 /imgs/dellnt.zmg</code>	Removes all existing local partitions except the one in slot 8, retrieves the image from <code>imgs/dellnt.zmg</code> in slot 8, and puts down the partitions and contents of that image on the available local writable devices. (This example assumes that there is sufficient local space and that slot 8 contains a primary FAT16 or FAT32 partition.)
<code>img restore1 /imgs/dellnt.zmg</code>	Removes all existing local partitions, retrieves the image from <code>imgs/dellnt.zmg</code> in the ZENworks partition, and puts down the partitions and contents of that image on the available local writable devices, if there is sufficient space.
<code>img restore1 /imgs/dellnt.zmg s2</code>	Removes all existing local partitions, retrieves the image from <code>imgs/dellnt.zmg</code> in the ZENworks partition, and puts down the partitions and contents of file set 2 of that image on the available local writable devices, if there is sufficient space.
<code>img restore1 /imgs/dellnt.zmg a2:p1 a3:p1</code>	Retrieves the image from <code>imgs/dellnt.zmg</code> in the ZENworks partition, updates local partition 1 with the data from partitions 2 and 3 of that image, and leaves the other local partitions unchanged, if there is sufficient space in local partition 1.

64.4.2 Restore from Proxy (img restorep)

Use the Restore from Proxy mode to retrieve an image from an Imaging (proxy) server and put it down on the workstation. For more information, see [Section 60.2, “Manually Putting an Image on a Workstation,” on page 715](#).

Using the bash prompt, the following example explains the syntax and available parameters that you can use with the restorep “restore from proxy” parameter:

```
img restorep address filepath [sfileset] [apartition:ppartition]
```

Commands

Table 64-7 *Img Restorp Parameters*

Parameter	Description
<code>address</code>	The IP address or DNS name of the ZENworks Imaging server to retrieve the image from. This can be any server running the Imaging Proxy service.

Parameter	Description
<i>filepath</i>	<p>The UNC path to the image file to retrieve, including the image filename and the .zmg extension (case-sensitive). The format of the UNC path is as follows:</p> <pre>//servername/volume_or_share/path_to_store_images/ imagename.zmg</pre> <p>For OES Linux, the path to the image file must be from root (/). For example, the path might look like:</p> <pre>//servername/media/nss/NSS_volume/path_to_image/ imagefilename.zmg</pre> <p>Upon execution of <code>img restorep</code> at the cmd line, the <i>servername</i> portion of this path is replaced with the value in the address portion of this syntax.</p> <hr/> <p>IMPORTANT: Because Linux doesn't recognize backslashes, you must use forward slashes in the UNC path or enclose the entire path in quotes.</p>
<i>sfileset</i>	<p>The number of the image file set to put down. Valid values are 1 through 10. For information on creating file sets of an image, see Chapter 59, "Creating and Restoring Images," on page 703.</p> <p>If you omit this parameter, file set 1 is used.</p>
<i>apartition:ppartition</i>	<p>A mapping between a partition in the image archive (<i>apartition</i>) and a target physical partition on the local machine (<i>ppartition</i>). Use this parameter to selectively restore a specific part of the image to a specific local partition.</p> <hr/> <p>IMPORTANT: If you use this parameter, none of the existing local partitions are removed, and only the target local partition is updated. The update process does not remove any existing files or overwrite any existing files of the same names if they are newer. If you want to remove all existing files from the target partition before updating it, first use the Partition Mode (img p) to delete and re-create the partition.</p> <hr/> <p>For <i>apartition</i>, use the partition number displayed for the source partition in the Image Explorer (imgexp.exe) utility. For <i>ppartition</i>, use the partition number displayed by <code>img dump</code> for the target partition. The target partition must be a Windows partition. You can repeat this parameter as needed to request multiple selective restorations in a single operation. In doing so, you can apply multiple parts of the image to a single local partition, but you can't apply the same part of an image to multiple local partitions in a single operation.</p>

Examples

Table 64-8 *Img Restorp Examples*

Example	Explanation
<pre>img restorep 137.65.95.127 // xyz_server/sys/imgs/ dellnt.zmg</pre>	<p>Removes all existing local partitions, retrieves the image from <code>sys/imgs/dellnt.zmg</code> on <code>xyz_server</code>, and puts down the partitions and contents of that image on the available local writable devices. (This example assumes that there is sufficient local space and that 137.65.95.127 is the IP address of <code>xyz_server</code>.)</p>

Example	Explanation
<code>img restorep img.xyz.com //xyz_server/sys/imgs/dellnt.zmg s2</code>	Removes all existing local partitions, retrieves the image from <code>sys/imgs/dellnt.zmg</code> on <code>xyz_server</code> , and puts down the partitions and contents of file set 2 of that image on the available local writable devices. (This example assumes that there is sufficient local space and that <code>img.xyz.com</code> is the DNS name of <code>xyz_server</code> .)
<code>img restorep img.xyz.com //xyz_server/sys/imgs/dellnt.zmg a2:p1</code>	Retrieves the image from <code>sys/imgs/dellnt.zmg</code> on <code>xyz_server</code> , updates local partition 1 with the data from partition 2 of that image, and leaves the other local partitions unchanged. (This example assumes that there is sufficient space in local partition 1 and that <code>img.xyz.com</code> is the DNS name of <code>xyz_server</code> .)
<code>img restorep img.xyz.com //bogus/sys/imgs/dellnt.zmg</code>	Removes all existing local partitions, retrieves the image from <code>sys/imgs/dellnt.zmg</code> on <code>img.xyz.com</code> , and puts down the partitions and contents of that image on the available local writable devices. (This example assumes that there is sufficient local space, and that <code>img.xyz.com</code> is the DNS name of a server running the Imaging Proxy). Because the servername inside the UNC path is replaced by the address value defined earlier in the cmd line, <code>//bogus</code> becomes <code>//img.xyz.com</code>

64.5 Session (Multicast) Mode (img session)

Use the Session (Multicast) mode to take an image of one workstation and put it down on multiple other workstations simultaneously over the network in a single operation.

IMPORTANT: For multicasting to work properly, the routers and switches on the network must have multicast features configured. Otherwise, multicast packets might not be routed properly.

For step-by-step instructions of the different ways you can perform multicast sessions, see the following sections:

- [“Initiating an Automatic Multicast Session in ConsoleOne” on page 726](#)
- [“Using the Bash Prompt to Perform the Multicast Session” on page 734](#)
- [“Using the ZENworks Imaging Engine Menu to Perform the Multicast Session” on page 735](#)

For multicasting to work, each participating workstation must boot from an imaging device and run the ZENworks Imaging Engine in this mode, as explained below. The workstation from which the image is taken is called the *master*, and the workstations that receive the image are called *participants*.

Starting in ZENworks for Desktops 4, you can start the multicast session from the ZENworks Imaging server. If you start the session this way, you specify an image file for multicasting rather than a workstation as the session master.

Using the bash prompt, the following example explains the syntax and available parameters that you can use with the session parameter:

```
img session name [master|client] [clients=count [t=minutes]]
```

Commands

Table 64-9 *Img Session Parameters*

Parameter	Description
<i>name</i>	<p>The name of the multicast session. Each workstation joining the session uses the same value for this parameter.</p> <p>NOTE: The name must be unique among concurrent multicast sessions. It is hashed by the ZENworks Imaging Engine to produce a Class D IP address for the multicast session. To facilitate troubleshooting (wire sniffing), all Desktop Management Workstation Imaging multicast addresses start with 231. For example, the session name mcast01 produces the multicast address 231.139.79.72.</p>
master client	<p>That this workstation is the session master or a session client.</p> <p>If you omit this parameter, the ZENworks Imaging Engine waits for a user on one of the workstations to press m to designate that workstation as the master, or for the imaging session to be started from the ZENworks Imaging server by selecting <i>Manually Start Multicast</i>, providing the required information, then selecting <i>Yes</i>.</p>
clients= <i>count</i>	<p>The number of participating workstations that must register with the master before imaging begins. The option applies only for session masters.</p> <p>If you omit this parameter, the ZENworks Imaging Engine waits for the master user to press g. After imaging has begun, any participating workstations attempting to register are denied.</p>
time= <i>minutes</i>	<p>The number of minutes the master workstation waits for the next participant to register before starting the imaging process without reaching <i>count</i> registered participants. The option only applies for session masters.</p> <p>If you omit this parameter, the imaging process won't start until <i>count</i> is reached or the master user presses g. After that, any participants attempting to register are denied.</p>

Examples

Table 64-10 *Img Session Examples*

Example	Explanation
<code>img session mcast01</code>	Starts a multicast session named mcast01. Each successive workstation that issues this same command before the imaging begins joins the session. Imaging doesn't start until one of the users presses m to designate himself as master and presses g to start the imaging, or the imaging session is started from the ZENworks Imaging server by selecting <i>Manually Start Multicast</i> , providing the required information, then selecting <i>Yes</i> .
<code>img session mcast01 m</code>	Starts a multicast session named mcast01 and designates this workstation as the master. Each successive workstation that issues <code>img session mcast01</code> before the imaging begins joins the session as a participant. Imaging doesn't start until the master user presses g.

Example	Explanation
<code>img session mcast01</code> <code>master clients=5</code>	Starts a multicast session named mcast01. Each successive workstation that issues <code>img session mcast01</code> before the imaging begins joins the session. Imaging doesn't start until one of the users presses <code>m</code> to designate himself as master, or until the imaging session is started from the ZENworks Imaging server by selecting <i>Manually Start Multicast</i> , providing the required information, then selecting <i>Yes</i> . Five other workstations must also register as participants before the session begins.
<code>img session mcast01</code> <code>master clients=5 time=20</code>	Starts a multicast session named mcast01. Each successive workstation that issues <code>img session mcast01</code> before the imaging begins joins the session. Imaging doesn't start until one of the users presses <code>m</code> to designate himself as master, or until the imaging session is started from the ZENworks Imaging server by selecting <i>Manually Start Multicast</i> , providing the required information, then selecting <i>Yes</i> . Either five other workstations must register as participants or more than 20 minutes must elapse between any consecutive participant registrations, whichever occurs first, and then the session begins.

64.6 Partition Mode (img p)

Use the Partition mode to activate (make bootable), add, or delete a partition on the workstation.

You can activate, add, or delete a partition using either ZENworks Imaging Engine menu or the bash prompt.

The Partition mode can be used in two ways:

- [Section 64.6.1, “Using the ZENworks Imaging Engine Menu,” on page 784](#)
- [Section 64.6.2, “Using the Bash Prompt,” on page 785](#)

64.6.1 Using the ZENworks Imaging Engine Menu

- 1 Enter `img` to display the ZENworks Imaging Engine menu, then click *Partitioning*.
- 2 Click *Modify Partitions*, then click an option.

Active: Select a partition that you want to activate (make bootable), then click *Active*.

Add: Opens the Create New Partition window. Click a partition type, partition size, and cluster size, then click *OK*.

Delete: Select a partition, then click *Delete*.

For more information, see the table in [Section 64.6.2, “Using the Bash Prompt,” on page 785](#).

64.6.2 Using the Bash Prompt

To use the Partition mode from the bash prompt:

- 1 From the bash prompt, enter:

```
img poperation
```

where *operation* is one of the following:

Operation	Description
<i>pcpNumber type</i> [<i>size</i>] [<i>cluster=clusterSize</i>]	<p>Create a new partition, where:</p> <ul style="list-style-type: none">• <i>pNumber</i> is the number of the partition slot (as displayed by <code>img dump</code>) in which to create the partition• <i>type</i> is a keyword, FAT12, FAT16, FAT32, NTFS, or Extended, or a numerical value for the partition type, for example 0x0C (hexadecimal) or 11 (decimal) <p>If you are creating an extended partition, you can create a logical drive inside of the extended partition. See the next table for an example.</p> • <i>size</i> is a valid size for the partition type in MB <p>If you omit this parameter, the largest valid size for the partition type is used, given the available unpartitioned space on the drive.</p> • <i>clusterSize</i> is the cluster size for an NTFS partition. This parameter is not valid for any other partition type. <p>Don't use this parameter unless you have a specific reason to do so. It must be a power of 2 (2, 4, 8, 16, ...128). If you omit this parameter, the ZENworks Imaging Engine uses a reasonable cluster size for the NTFS partition size.</p> <p>The new partition is recognizable by other operating systems, but must be formatted or have a base image restored to it before you can store files in it.</p>
<i>pdpNumber</i>	Delete the partition from slot number <i>pNumber</i> . Use <code>img dump</code> to get the slot number.
<i>papNumber</i>	Activate (make bootable) the partition in slot number <i>pNumber</i> . Use <code>img dump</code> to get the slot number.

The following are examples:

Example	Explanation
<code>img pc1 fat16</code>	Creates a FAT16 partition in slot 1 using all of the available unpartitioned space on the drive.
<code>img pc5 fat32 5671</code>	Creates a FAT32 partition in slot 5 using 5,671 MB on the drive.
<code>img pd3</code>	Deletes the partition from slot 3.
<code>img pa5</code>	Activates (makes bootable) the partition in slot 5. (This assumes that a partition exists in that slot.)

Example	Explanation
<code>img pc2 extended 2500</code>	Creates an extended partition with a 2000 NTFS logical drive and a 500 MB FAT16 logical drive.
<code>img pc2 NTFS 2000</code> <code>cluster=1</code>	
<code>img pc2 fat16 500</code>	

64.7 ZENPartition Mode (img zenPartition)

Use the ZENPartition mode to enable, disable, or remove the installed ZENworks Workstation Imaging (Linux) partition.

1 Do one of the following:

- From the bash prompt, enter the following:

```
img zenPartition operation
```

where *operation* is enable, disable, or remove.

- Enter `img` to display the ZENworks Imaging Engine menu, click *Partitioning*, then click one of the following:

Disable ZENworks partition

Enable ZENworks partition

Remove ZENworks partition

2 Enter `lilo.s` to make this change effective.

IMPORTANT: If you remove an installed ZENworks partition, you must immediately restore a base image with a valid non-LILO MBR (Master Boot Record). If you do not, the workstation is not able to boot properly.

64.8 Dump Mode (img dump)

Use the Dump mode to view information about the storage devices and partitions on the workstation.

1 Do one of the following:

- Enter `img` to display the ZENworks Imaging Engine menu, click *System information*, then click *Drive information*.

- Enter the following:

```
img dump [geo]
```

where:

Parameter	Action
<code>dump</code>	Lists the existing partitions on all local hard drives. For each partition, the type, size, and slot number of the partition are given. The ZENworks partition and Dell or Compaq configuration partitions are not listed.

Parameter	Action
geo	Displays additional information about the geometry (cylinders, heads, and sectors) and capacity of each hard drive.
Examples:	
Example	Explanation
img dump	Lists the current partitions on all local writable devices.
img dump geo	Lists all hard drives, their geometry and capacity, and the current partitions on the writable devices.

64.9 Information Mode (img info)

Use the Information mode to view the following:

- The data currently stored in the image-safe area on the workstation

This data is saved by the ZENworks Imaging Windows Agent during each Windows session to ensure that it can be restored after the workstation is reimaged. If the workstation is new and doesn't have Windows yet, an initial set of data is supplied from an eDirectory policy via the ZENworks Imaging server to the ZENworks Imaging Engine when the first base Windows image is put down. (For more information, see [Section 58.1, “Defining an Imaging Policy for Unregistered Workstations \(Server Policy\),”](#) on page 697.)

- Information about the hardware devices on the workstation

This information is detected during the imaging boot process. If the ZENworks Imaging Engine runs in auto-imaging mode, this information is sent to the ZENworks Imaging server to help determine which image to put on the workstation, if necessary.

- Name of the base image that was last put down on the workstation

To use the Information mode:

- 1 Enter `img` to display the ZENworks Imaging Engine menu, click *System Information*, then click *Image-Safe Data* or *Detected Hardware* (see the table below for details).

or

Enter the following from the bash prompt:

```
img info [zisd]
```

IMPORTANT: Image-safe data is not supported on Linux workstations.

Menu Item or Parameter	Description
<i>System Information > Detected Hardware</i> or info from the bash prompt	Lists the detected hardware devices on the workstation, including: <ul style="list-style-type: none"> • CPU chipset • BIOS asset tag • BIOS serial number • Video adapter • Network adapter • MAC address • Sound card • Hard drive controller • Hard disk capacity • Detected RAM • Boot media
<i>System Information > Image-Safe Data</i> or zisd from the bash prompt	Lists the data currently stored in the image-safe area on the workstation. The items that comprise this data are listed in Section 63.2, “ZENworks Imaging Windows Agent (Ziswin.exe),” on page 743. In addition to the image-safe data , the last base image that was put down on the workstation is also listed.
Example	Explanation
<code>img info</code>	Lists the detected hardware devices on the workstation.
<code>img info zisd</code>	Lists the Desktop Management image-safe data currently stored on the workstation and the last base image that was put down.

Updating ZENworks Imaging Resource Files

65

In Novell® ZENworks® 7 Desktop Management, you can manually update ZENworks imaging resource files.

The following sections provide concepts and instructions for adding Linux drivers into an image resource file:

- [Section 65.1, “The Linux Distribution for Imaging,” on page 789](#)
- [Section 65.2, “Understanding Device Boot Processes in a ZENworks Imaging Environment,” on page 790](#)
- [Section 65.3, “Understanding ZENworks Partitions and Command Line Parameters,” on page 792](#)
- [Section 65.4, “Modifying ZENworks Imaging Resource Files,” on page 793](#)
- [Section 65.5, “Adding or Updating LAN Drivers,” on page 796](#)
- [Section 65.6, “Using Uname,” on page 798](#)
- [Section 65.7, “Variables and Parameters,” on page 799](#)
- [Section 65.8, “Troubleshooting Linux Driver Problems,” on page 801](#)

65.1 The Linux Distribution for Imaging

ZENworks Imaging uses a small Linux distribution on the client device to perform imaging operations. The distribution shipping with ZENworks 7 is based on the SUSE® installation system, where SUSE Linux or SUSE Linux Enterprise Server (SLES) boot to a small distribution to perform a YaST installation. ZENworks Imaging uses the same installation system found in SLES, but instead of starting a YaST installation, it starts a ZENworks Imaging session.

In ZENworks 6.5 SP1 and earlier, Linux kernel 2.4.x is used in the customized distribution; in ZENworks 6.5 SP2 the kernel is updated to 2.6 and is a SLES-based distribution.

Using a stable Linux distribution based on SLES gives customers a distribution with the broadest range of stable drivers available. The hardware industry is continually introducing new and updated network and disk drivers, so it's not always possible to provide the latest drivers in its software releases.

This section covers how to update Linux drivers using the new distribution. It deals with the Imaging resource files that are based on the SLES distribution and ZENworks Preboot Services processing.

NOTE: The PXE (Preboot Execution Environment) environment provided by PreWorX, used in ZENworks 6.5 SP1 and earlier for Windows and NetWare® servers, has been modified for ZENworks 7 to support the SLES-based ZENworks Imaging distribution. Linux servers use Novell's internally-developed PXE solution.

The PXE process based on PreWorX files differs from Novell's solution. For example, PreWorX uses a combination of Caldera DOS, the linld Linux loader program, and .cmd configuration files

for passing parameters to the Linux kernel. Novell's PXE solution is based on the pxelinux boot loader and .cfg configuration files. PreWorX-specific information is not included in this imaging resource files section.

65.2 Understanding Device Boot Processes in a ZENworks Imaging Environment

The following provides a high-level overview of a Linux boot process and how ZENworks 7 imaging affects it:

1. A boot loader program loads the Linux kernel and `initrd` (initial RAM drive) into memory.

The SLES-based imaging distribution uses `isolinux` as the boot loader for imaging CDs, a modified `pxelinux` for booting using PXE, or `linld.com` when using a single diskette with the CD. If you have a ZENworks partition installed, it uses the `lilo` program to boot alternately between the ZENworks partition and the installed operating system.

The following provides the current paths and filenames and a historical comparison:

Files	ZENworks 6.5 SP1 and Earlier	ZENworks 7 NetWare and Windows Servers ¹	ZENworks 7 Linux Servers ²
Preboot Loader	Does the following: <ul style="list-style-type: none">• Loads DOS• Runs <code>loadlin</code>	CD boot: <code>isolinux</code> PXE boot: <code>linld.com</code>	CD boot: <code>isolinux</code> PXE boot: <code>linld.com</code>
Linux Kernel Name	CD boot: <code>kernel</code> PXE boot: <code>linux.1</code> Diskette: <code>kernel.zen</code>	CD boot: <code>\boot\loader\linux</code> PXE boot: <code>\tftp\boot\linux</code>	/boot/loader/CD boot: <code>linux</code> PXE boot: <code>/srv/tftp/boot/linux</code>
Initrd Filename	CD boot: <code>initrd.gz</code> PXE boot: <code>linux.2</code> Diskette: <code>initrd</code> (on the second diskette)	CD boot: <code>\boot\loader\initrd</code> PXE boot: <code>\tftp\boot\initrd</code>	CD boot: <code>/boot/loader/initrd</code> PXE boot: <code>/srv/tftp/boot/initrd</code>

¹ The same as ZENworks 6.5 SP2.

² The same as ZENworks 7 Linux Management.

2. The Linux kernel starts running, does some device driver setup, then mounts the `initrd` file system.

Regardless of which boot loader method is used, the main purpose is to set up the `initrd` file as a RAM drive, load the Linux kernel into memory, then turn control over to it with an indication to the Linux kernel of where to find `initrd`.

3. The Linux kernel turns control over to `linuxrc` for performing initial hardware detection. When finished, control is returned to the Linux kernel.

NOTE: ZENworks 6.5 SP1 and earlier imaging contains a `linuxrc` script file that performs some initial setup, but not the hardware detection.

4. The Linux kernel starts a background process (`/sbin/init`).

After control is passed to the `linuxrc` program, control is never returned to the Linux kernel or passed on to the `init` process.

NOTE: ZENworks 6.5 SP1 and earlier use the `init` process to perform the imaging. All ZENworks imaging processing is performed within the `linuxrc` process. For this reason, some of the standard processes you are familiar with do not work or exist in ZENworks 7 imaging.

For example, the `halt` and `reboot` commands are different. In a fully-installed Linux system, `reboot` actually performs an `init 6` call. Because `init` is not running during the ZENworks 7 imaging process, an `init 6` call cannot be made. Therefore, `reboot` has been aliased to `reboot -r`, which forces a reboot without trying to call `init`.

Most other commands do run from the bash prompt, because `bash` is running.

For more information on `linuxrc` and `zenworks.s`, review the following sections:

- [Section 65.2.1, “linuxrc,” on page 791](#)
- [Section 65.2.2, “zenworks.s,” on page 792](#)

65.2.1 linuxrc

When control is turned over to `linuxrc`, there are several processes it performs to get the system ready for the imaging process. `Linuxrc` is initially configured from the `/linuxrc.config` file, which is located in the `initrd` file system. Additional configuration information for `linuxrc` can be placed in the `/info` file (located in the `initrd` file system), but ZENworks does not normally use this information.

`Linuxrc` also loads a `root` file system, which is combined with the `initrd` file system that is set up by the boot loader. The `root` file system is located on an imaging CD as the file `/boot/root`. For PXE booting, the `root` file system is stored on the ZENworks Imaging server as:

- **NetWare/Windows servers:** `\tftp\boot\root`
- **Linux servers:** `/srv/tftp/boot/root`

`Linuxrc` attempts to locate and load the `settings.txt` file, either on the root of the imaging CD, or on the ZENworks Imaging server in the TFTP directory. From `settings.txt`, `linuxrc` reads and processes any parameters that pertain to itself, then copies `settings.txt` to the root (`/`) of the file system.

`Linuxrc` then also attempts to locate and load a file named `driverupdate`. It is usually located in the same directory as `root`. This file is used to update drivers and other files in the imaging distribution.

The `driverupdate` file is based on standard SUSE technology during a PXE boot. Because the network must be operating normally in order to obtain `driverupdate`, this file cannot update drivers for the active network device. However, other files and drivers can be updated by using the `driverupdate` file. For more information, see [Section 65.4.3, “Using the Driverupdate File Method,” on page 796](#).

65.2.2 zenworks.s

A normal SUSE installation for SUSE Linux or SLES boots to a small distribution to perform a YaST installation. ZENworks Imaging boots with the same installation system, but instead of starting a YaST installation, it starts the ZENworks Imaging process. Control is turned over to the ZENworks script `/bin/zenworks.s`, which is the main script file for ZENworks imaging processing. The script performs a certain number of setup tasks, then gives control to the appropriate script for the selected imaging process. For more information on the imaging process, see [Section 56.1, “Understanding Desktop Management Preboot Services,” on page 637](#).

One of the setup tasks is to apply any update files. When booting from a CD, `zenworks.s` copies the `/addfiles` directory structure to the Linux file system. For more information, see [Section 65.4.1, “Adding Files to an Imaging Boot CD,” on page 794](#).

65.3 Understanding ZENworks Partitions and Command Line Parameters

The following sections provide an understanding of the ZENworks partition and imaging commands that are used when updating Linux drivers:

- [Section 65.3.1, “The ZENworks Partition,” on page 792](#)
- [Section 65.3.2, “Command Line Parameters and Variables,” on page 792](#)

65.3.1 The ZENworks Partition

The ZENworks partition is used to store the files required to load Linux into RAM, making the result similar to using a CD or PXE boot method. The ZENworks partition has a similar boot media layout as an imaging CD.

NOTE: To provide additional imaging functionality, ZENworks has changed the way it uses the ZENworks partition. In ZENworks 7, the partition is no longer mounted as the `root` file system and has a minimum size of 150 MB. In ZENworks 6.5 SP1 and earlier, the partition is mounted and used as the Linux `root` file system with a minimum size of 100 MB.

The files stored on the ZENworks partition are `/boot/loader/linux`, `/boot/loader/initrd`, and `/boot/root`, which are the same directories as on the imaging CD. In ZENworks 7, the boot loader continues to be lilo, which loads Linux as described under [Section 65.2, “Understanding Device Boot Processes in a ZENworks Imaging Environment,” on page 790](#). The `driverupdate` and `settings.txt` files are searched for and loaded from the ZENworks partition.

If you need to modify the Linux files, you must modify the `initrd` or `root` file sets the same way as you would for other boot methods. For information, see [Section 65.4.2, “Adding Files to the Initrd or Root File Systems,” on page 794](#).

65.3.2 Command Line Parameters and Variables

There are four types of command line parameters that can be used with the ZENworks imaging process. They are entered manually on the command line when booting from a CD or they can be placed in the `isolinux.cfg` file located in the `/boot/loader` directory. The commands are

also located in the *.cfg files for PXE and are located in the /srv/tftp directory on the ZENworks Imaging server.

- **Kernel parameters:** The valid parameters for the Linux kernel are found in the / Documentation/kernel-parameters.txt file that is installed with the kernel source.

Some devices have a faulty BIOS, where you must turn off ACPI processing for the kernel to load properly. To do this, use the kernel parameter acpi=off. For more information, see [Novell Support \(http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=10099330&sliceId=&dialogID=1284337&stateId=1%200%20548668\)](http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=10099330&sliceId=&dialogID=1284337&stateId=1%200%20548668).

- **Linuxrc parameters:** These parameters affect the way linuxrc detects hardware or sets hardware settings. They are described briefly in the /usr/share/doc/packages/linuxrc/linuxrc.html file in a Linux system.

Linuxrc parameters can be found in the /linuxrc.config or /info files that reside in the initrd file system. Some parameters can be placed in the settings.txt file that is located on the root of the imaging CD or ZENworks partition, or in the /srv/tftp/boot file for PXE booting.

Parameters that can be placed in the settings.txt file (the easiest file to edit) are limited. During PXE booting, parameters that affect the network are not processed from settings.txt, because by the time linuxrc loads the settings.txt file, the network is already set up. Network settings can be placed in the settings.txt file when booting from an imaging CD, because it is loaded early enough in the process to take effect.

- **ZENworks variables:** Some environment variables affect the way imaging performs. They can be configured in any file, but should normally be configured in the settings.txt file.

If you add variables to the settings.txt file that were not originally defined there, you must export the variable. For example, in the settings.txt file, enter:

```
export IMGCMD="myscript"
```

A list of all image engine or script variables is listed under [Section 65.7, “Variables and Parameters,” on page 799](#).

- **Other variables:** Environment variables that you might want in your script can be added in the same manner as described for the ZENworks variables.

65.4 Modifying ZENworks Imaging Resource Files

From time to time you might want to modify an imaging distribution by adding your own files. These can be additional programs, scripts, data files, or updated Linux drivers.

You can use the following methods to update imaging resource files:

- The easiest method is to edit the settings.txt file, which is located on the root of the imaging CD or in /srv/tftp/boot on the ZENworks Imaging server for PXE booting.
- Where you are using a ZENworks partition, you can boot to the manual or maintenance mode, mount the ZENworks partition, then copy the modified settings.txt and the files in initrd or root to the mounted ZENworks partition.

- Another easy method is to edit the `.cfg` files located in `/srv/tftp` on the ZENworks Imaging server for PXE booting. This method is only available for Linux imaging servers, because the configuration files are provided by Novell's version of PXE.
- You can modify files in the `initrd` or `root` file systems, but you need a Linux environment for performing the modification process. Files required during the initial setup (during `linuxrc` processing time), such as LAN drivers, must be placed in the `initrd` file system. Other files that are not needed until the `zenworks.s` script file takes control can be placed in the `root` file system (for example, an imaging script), or you can use the `driverupdate` file.

This method is discussed in this section.

The following sections provide various methods for modifying imaging resource files:

- [Section 65.4.1, “Adding Files to an Imaging Boot CD,” on page 794](#)
- [Section 65.4.2, “Adding Files to the Initrd or Root File Systems,” on page 794](#)
- [Section 65.4.3, “Using the Driverupdate File Method,” on page 796](#)

65.4.1 Adding Files to an Imaging Boot CD

If you have files to add to an imaging boot CD so they can be available for use when you get to the actual imaging process (such as scripts, but normally not driver modules), you can copy the files to the `/addfiles` directory on the imaging CD. This is an easy way to insert your script or other files into the distribution without **modifying the `initrd` or `root` file systems**. However, these files are not available during the boot and module loading phases.

The imaging boot CD has a directory named `/addfiles` where you can add files. They should be placed below this directory in their proper directory names. They are then available in this directory structure during the imaging process.

An example of how you can add files:

- 1 If you want to execute your own script instead of the normal imaging process, create a script file named `myscript.s` and place it on the boot CD. For example, `/addfiles/bin/myscript.s`.

IMPORTANT: The script file must have proper LF line terminators that Linux requires, not the DOS CR and LF end-of-line characters. In other words, you cannot use `Notepad.exe` to create the script; you must use a text editor compatible with Linux or UNIX, such as `TextPad`.

- 2 To place the following line in the `settings.txt` file, enter:

```
export IMGCMD=/bin/myscript.s
```

When imaging is run, it runs `/bin/myscript.s` instead of using the normal `img auto` command.

65.4.2 Adding Files to the Initrd or Root File Systems

This is the preferred method for updating imaging resource files, and must be performed in a Linux environment.

Before performing the procedure given below, make sure you have created backup copies of any files you plan to change, specifically the `/srv/tftp/boot/initrd` file. If you want to change

the files on an imaging CD, you need a program such as winiso, or some other process for extracting and replacing the file in the `bootcd.iso` image file.

IMPORTANT: When updating or adding files and Linux drivers in the `initrd` or `root` file systems, document the changes you make. When you receive updated resource files from Novell, they do not contain your customized changes. If the kernel version has changed with the newer resource files from Novell, previously added drivers must be updated either by obtaining a new version from the manufacturer or recompiling the driver using the correct Linux kernel version source.

You can use the following procedure for the `root` file system by simply replacing “`initrd`” with “`root`” in the steps. However, Linux drivers should always be placed in the `initrd` file system, not the `root` file system.

To add files to the `root` file system, you can also use the `driverupdate` method described in [Section 65.4.3, “Using the Driverupdate File Method,” on page 796](#).

To modify the `initrd` or `root` file system:

- 1 Using a Linux machine, create a working directory and change to that directory.
- 2 To copy `initrd` from the PXE server or the boot CD to the new working directory:
 - For PXE, copy `\tftp\boot\initrd` to the Linux workstation’s working directory.
 - For the CD, extract `initrd` from the `\boot\loader` directory on the boot CD, then copy the extracted `initrd` to the Linux workstation’s working directory.
- 3 To rename `initrd` to `initrd.gz`, enter:

```
cp initrd initrd.gz
```
- 4 To unzip the `initrd.gz` file, enter:

```
gunzip initrd.gz
```
- 5 To create another working directory for use as a mount point in the subsequent steps, enter:

```
mkdir work
```
- 6 To mount the `initrd` file system to the `/work` directory, enter:

```
mount -o loop initrd work
```
- 7 To copy your files or updated driver to the mounted `initrd` file system, enter:

```
cp /your_path/module.ko work/lib/modules/2.6.5-override-default/initrd
```

where `your_path` is the path to the `module.ko` file and `module` is the name of the module.
Other files to be included in the `initrd` file system should be copied to the appropriate directory.
- 8 To unmount the `initrd` file system, enter:

```
umount work
```
- 9 To zip the new `initrd` file, enter:

```
gzip -v9c initrd > initrd.gz
```
- 10 To rename `initrd.gz` back to `initrd`, enter:

```
cp initrd.gz initrd
```

11 To copy the file back:

- For PXE, copy the updated `initrd` to the `\tftp\boot` directory on the PXE server.
- For the CD, copy the updated `initrd` to the `\boot\loader` directory on the boot CD.

65.4.3 Using the Driverupdate File Method

For information on using the `driverupdate` file method with Linux servers, see “[Using the Driverupdate File Method](#)” in the *Novell ZENworks 7 Linux Management Administration Guide*. This particular method is not used for the NetWare and Windows platforms.

65.5 Adding or Updating LAN Drivers

As LAN card manufacturers develop and release new LAN adapters, they usually release new or updated drivers as well. Sometimes the new LAN card functions properly with an earlier driver, and sometimes the earlier driver does not recognize the new LAN card and refuses to load. Occasionally, the older driver does load, but the LAN card exhibits serious performance problems. To obtain the full performance capabilities of a new LAN card, you should use the new driver.

The following sections explain how to obtain or compile drivers:

- [Section 65.5.1, “Obtaining Drivers,” on page 796](#)
- [Section 65.5.2, “Building Drivers,” on page 796](#)
- [Section 65.5.3, “Loading Drivers with Parameters,” on page 798](#)

If you need to load your drivers with specific parameters, see [Section 65.5.3, “Loading Drivers with Parameters,” on page 798](#).

65.5.1 Obtaining Drivers

New LAN drivers should be obtained from the manufacturer. Most LAN card manufacturers have drivers available for free downloading from their Web site. Some drivers are available from www.scyld.com/network, and the source to the Broadcom BCM5700 driver can be downloaded from <http://www.broadcom.com/drivers/downloaddrivers.php>.

If a manufacturer has a binary driver compiled specifically for the kernel version used by ZENworks, you can obtain the driver and use one of the update methods to add the driver. ZENworks 7 is based on SLES 9 SP2, kernel version 2.6.5-7.191. If the driver is not for this specific version, you must obtain the source and compile it for this version. For more information, see [Section 65.5.2, “Building Drivers,” on page 796](#).

65.5.2 Building Drivers

Nearly all Linux drivers are distributed in source code form and need to be compiled before they can be used. Follow the manufacturer’s instructions included with the new driver to build the driver module. Many drivers can be built in such a way that they are built into the kernel itself; however, we recommend that LAN drivers be built as external kernel modules.

When building your LAN drivers, make sure that your build machine uses the same kernel as the imaging environment. If you have a LAN driver that doesn’t load in your imaging environment, it

usually means that you have a mismatch between your build environment and the imaging environment.

You can find the current kernel version of your Linux environment by using the following command:

```
uname -r
```

However, you might need to modify the results from the `uname` command to get your kernel versions to match. For more information, see [Section 65.6, “Using Uname,” on page 798](#).

To build your drivers:

- [“Obtaining the Linux Source Code Tree” on page 797](#)
- [“Compiling the Module” on page 798](#)

Obtaining the Linux Source Code Tree

To compile a module, you need the Linux source code tree that contains the configuration matching the ZENworks kernel. To obtain the necessary source code, see TID 10091818 in the [Novell Support Knowledgebase \(http://support.novell.com/search/kb_index.jsp\)](#).

To use the Linux source code tree:

- 1 Unzip the file and install the source code tree in the `/usr/src` directory.

For example, the tar file creates the following directories:

```
/usr/src/linux-2.6.5-7.191
/usr/src/linux-2.6.5-7.191-obj
```

- 2 Obtain the proper configuration file from one of the following locations:
 - A running ZENworks imaging distribution file (`/proc/config.gz`)
 - TID 10091818 in the [Novell Support Knowledgebase \(http://support.novell.com/search/kb_index.jsp\)](#)
- 3 Copy this configuration file to the directory created in [Step 1](#).

For example, `/usr/src/linux-2.6.5-7.191`.

- 4 To create a link to the source tree:

4a

To change to the `/usr/src` directory, enter:

```
cd /usr/src
```

- 4b If there is a Linux soft link in the directory, delete it.

- 4c Create the Linux soft link, such as:

```
ln -s linux-2.6.5-7.191 linux
```

You now have the Linux kernel source tree and soft link ready for compiling the module. Continue with [“Compiling the Module” on page 798](#).

Compiling the Module

- 1 Install the source.

Follow the instructions supplied from the manufacturer to install the source.

Normally, the module source is in a directory under `/usr/src`. Module source files usually come in the form of a gzipped tar file (`.tar.gz` or `.tgz`). The file might also be a bzipped file (`.bz2`).

- 2 To compile the source:

- 2a Change directories to the source.

- 2b If you **modified** `uname` to change to the proper kernel version, issue a `make` command.

- 3 When you have your module compiled for ZENworks, take the generated `.ko` module file (make sure you select the proper module name and not a work `.ko` file) and install it by using the **driver update method** or **placing it in the `initrd` file system**.

65.5.3 Loading Drivers with Parameters

If there is a module that you want to load during the `linuxrc` processing time, and if `linuxrc` does not recognize that it needs to be loaded or you want to specify the load parameters, you can enter a line in the `linuxrc.config` or `/info` file. This file then needs to be updated in the `initrd` file system.

You might need to load a LAN driver module with specific parameters. You can do this with a line like:

```
insmod="moduleName parm=xxx"
```

This type of line is most commonly used to load a LAN driver with specific parameters, such as full duplex or specific speed.

65.6 Using Uname

The `uname` command enables you to find the current kernel version of your Linux environment. However, you might need to modify the results from the `uname` command to get your kernel versions to match.

The following steps modify the `uname` command to provide the value you need:

- 1 To obtain your current kernel version, enter:

```
uname -r
```

Write down the version number so you can use it in **Step 4**. This example uses version 2.6.13-15-smp from a SLES 9 SP2 installation.

- 2 To create a new directory, enter:

```
mkdir /bin/orig
```

- 3 To move the `uname` binary to the `/bin/orig` directory that you just created, enter:

```
mv /bin/uname /bin/orig/uname
```

- 4 Use a Linux editor (such as vi) to create the `/bin/uname` file that contains the following lines:

```
#!/bin/sh
#uname
if [ $KRNVERSION"a" = "a" ] ; then
    if [ $(/bin/orig/uname -r) = "2.6.13-15-smp" ] ; then
        export KRNVERSION=2.6.13-15-smp
    else
        export KRNVERSION=2.4.31
    fi
fi
if [ $1"a" = "-ra" ] ; then
    echo $KRNVERSION
else
    /bin/orig/uname $*
fi
```

IMPORTANT: Replace the string “2.6.13-15-smp” with the version you found in Step 1.

- 5 To make the new `uname` command script executable, enter:

```
chmod +x /bin/uname
```

- 6 Enter the following to cause the `uname -r` command to return a specific version, such as when compiling a module:

```
export KRNVERSION="2.6.5-7.191"
```

- 7 Following the manufacturer’s directions, compile the module using the appropriate `make` command.

- 8 Reset `uname` so that it returns actual values:

```
unset KRNVERSION
```

65.7 Variables and Parameters

The following sections describe the variables and parameters used in updating resource files:

- [Section 65.7.1, “Imaging Script Variables,” on page 800](#)
- [Section 65.7.2, “Linuxrc Parameters Specified in Settings.txt,” on page 800](#)
- [Section 65.7.3, “Image Engine Variables,” on page 801](#)

65.7.1 Imaging Script Variables

The following environment variables are used in imaging scripts and must not be modified:

Table 65-1 *Imaging Script Variables*

Variable	Definition
ACTIVEPARTITION	Device of the active OS partition.
CDBOOT	YES = Booted from a CD.
DISABLEZEN	1 = Disable the ZENworks partition.
ENABLEZEN	1 = Re-enable the ZENworks partition.
ZENDEVICE	Device name of the ZENworks partition.
ZENPARTBOOT	YES = Booted from ZENworks partition.

The following environment variables can be modified or set in the `settings.txt` file:

Table 65-2 *Environment Variables*

Variable	Definition
HDPARM	NO = Do not set hdparm parameters.
IMGCMD	Imaging command to run instead of the <code>img a</code> command.
MANUALREBOOT	YES = Do not automatically reboot.
PARTITIONSIZE	Size in MB to create the ZENworks partition.
PROXYADDR	IP/DNS address of the ZENworks Imaging server.
PROMPT	Go to the bash prompt after imaging is complete.

65.7.2 Linuxrc Parameters Specified in Settings.txt

Table 65-3 *Linuxrc Parameters*

Variable	Definition
netsetup	dhcp = Use DHCP. 1 = Static IP.
HostIP	Static IP address to use.
NetMask	Network mask.
Gateway	Network gateway.
HostName	Host name to assign.

Variable	Definition
Nameserver	DNS name server.
Domain	Domain suffix.
NetDevice	ethx = Define which network device to configure.

65.7.3 Image Engine Variables

Table 65-4 *Image Engine Variables*

Variable	Definition
DEVELOPER_LOG	"A" creates a verbose <code>imglog</code> debug file.
ZENIMGLOG	"A" creates a less verbose <code>imglog</code> debug file.
ZEN_IGNORE_GEO_MISMATCH	Ignore geometry device mismatches when restoring raw image formats.
NOABORTBUTTON	If defined, do not display the Abort button during imaging.

65.8 Troubleshooting Linux Driver Problems

- [Section 65.8.1, "Troubleshooting During the Boot Process," on page 801](#)
- [Section 65.8.2, "Troubleshooting at the Bash Prompt," on page 802](#)

65.8.1 Troubleshooting During the Boot Process

While booting ZENworks imaging, there are several things that you can do to help troubleshoot if there is a problem:

- Press Esc to see the kernel messages. Usually, messages are shown for failures.
- Screen 3 (press Alt+F3) is used to show the progress of the `linuxrc` process. It lists progress results, what `linuxrc` is doing, which modules are loaded, and so on.
- Screen 4 (press Alt+F4) is used to show output from the modules during the `linuxrc` process.
- Screens 1 (press Alt+F1), 3, and 4 can be used to help determine which part of the process is failing or causing a problem.
- Screens 3 and 4 indicate which drivers are loaded.
- If a drive is loaded properly but fails in some way, view screen 4 to see if there is an outdated driver.

If the boot process fails, the first command line parameter to use is `acpi=off`.

65.8.2 Troubleshooting at the Bash Prompt

When the bash prompt is displayed, there are a few tools that you can use to gather information about the hardware:

- **hwinfo:** This utility is used by linuxrc to load hardware. You can use `hwinfo -pci` to determine exactly what hardware was recognized.

Pipe to “less,” because `hwinfo` can create a lot of output. For example, `hwinfo -pci | less`.

If you need to contact Novell Support for help, you should capture the output from `hwinfo -pci` to a file for their use. You can gather the most information with this command:

```
hwinfo -pci -log /logfilename
```

where *logfilename* is the name of the file that you should send.

You can then mount a device, such as a thumb drive or other USB device, and save the output file for later use. You might also be able to use FTP to save the file where it can be available.

- **ethtool:** This is a valuable tool (contained in a ZENworks distribution) that can be used to change the configuration on most Ethernet network devices. See the online help for information on using the `ethtool` utility.

Supported Ethernet Cards

66

Novell® ZENworks® 7 Desktop Management provides the Ethernet card drivers contained in the Linux kernel (2.6) that ships with ZENworks 7.

To determine which Linux kernel you are using, enter `uname -r` at the bash prompt.

If your workstation or laptop computer uses a different card that is not supported, you must supply your own Ethernet driver.

Accessing IP Addresses for Devices Running Dual NICs

67

To automatically obtain an IP address for a device running dual NICs, you can modify the `/srv/tftp/z_auto.cfg` or the `/srv/tftp/z_maint.cfg` file (or both) by adding the following line at the end of the *Append* command:

```
netdevice=eth0
```

This eliminates the need to manually select a NIC's IP address.

Documentation Updates

K

This section contains information on documentation content changes that were made in this *Administration Guide* after the initial release of Novell® ZENworks® 7 Desktop Management. The information can help you to keep current on updates to the documentation.

All changes that are noted in this section are also made in the documentation. The documentation is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the documentation changes listed in this section.

The documentation update information is grouped according to the date the changes are published. Within a dated section, the changes are alphabetically listed by the names of the main table of contents sections in the guide.

If you need to know whether a copy of the PDF documentation you are using is the most recent, the PDF document contains its publish date on the front title page.

The documentation was updated on the following dates:

- [Section K.1, “July 14, 2006 \(Support Pack 1\),” on page 807](#)
- [Section K.2, “December 9, 2005,” on page 810](#)

K.1 July 14, 2006 (Support Pack 1)

Many updates too numerous to mention here concerning the use of Linux servers in Preboot Services imaging are made to the [Workstation and Server Imaging](#) section of this *Administration Guide*. The following sections detail some of those changes.

Updates are made to the following guide sections:

- [Imaging Utilities and Components](#)
- [Multicasting Images](#)
- [Preparing an Imaging Boot Method](#)
- [Preparing a ZENworks Imaging Server](#)
- [Server Imaging](#)
- [Updating ZENworks Imaging Resource Files](#)
- [Using ZENworks Desktop Management Preboot Services](#)

K.1.1 Imaging Utilities and Components

The following changes are made in this section:

Location	Change
Section 63.5, “Imaging Configuration Parameters (Settings.txt),” on page 758	<p>Removed the following information from the end of this section and replaced it with the new information contained in Chapter 67, “Accessing IP Addresses for Devices Running Dual NICs,” on page 805:</p> <p>If you have problems obtaining an IP address for a workstation running dual NICs, put the following line in the <code>settings.txt</code> file:</p> <pre>export VALIDATE_NIC=\$PROXYADDR</pre> <p>This line in the <code>settings.txt</code> file validates the NICs; you might notice a small performance decrease in the time it takes to obtain an IP address for the workstation.</p>
Section 63.7.1, “Initiating the Imaging Processes on Linux Imaging Servers,” on page 762	Added this section.

K.1.2 Multicasting Images

The following changes are made in this section:

Location	Change
“Initiating a Multicast Session from a Linux ZENworks Imaging Server” on page 730	Added this section.

K.1.3 Preparing an Imaging Boot Method

The following changes are made in this section:

Location	Change
Section 55.3, “Using the ZENworks Imaging Floppy Boot Disk Creator,” on page 633	Updated this section.
Section 55.4, “Creating an Imaging Hard-Disk Partition,” on page 635	Updated this section.

K.1.4 Preparing a ZENworks Imaging Server

The following changes are made in this section:

Location	Change
Section 54.1, "Imaging Server Prerequisites," on page 629	<p>Added the following bullet:</p> <ul style="list-style-type: none">• Proxy DHCP server (Linux imaging servers only): To avoid confusion, the Proxy DHCP daemon (novell-proxydhcp) is installed, but not enabled. For PXE devices to be able to communicate with Preboot Services, this daemon must be started manually on at least one server on each network segment. <p>Exactly how many servers and which specific servers should run this daemon is dictated by your network topology. As a rule of thumb, for every DHCP server deployed in your network, you should have a corresponding Proxy DHCP server.</p>

K.1.5 Server Imaging

The following changes are made in this section:

Location	Change
"Workstation and Server Imaging" on page 623	Deleted the "Server Imaging" section, updating and moving its information into the main introduction for ZENworks imaging.

K.1.6 Updating ZENworks Imaging Resource Files

The following changes are made in this section:

Location	Change
"Obtaining the Linux Source Code Tree" on page 797	Changed the method for obtaining the necessary source code and config.gz file to TID 10091818 in the Novell Support Knowledgebase (http://support.novell.com/search/kb_index.jsp) .

K.1.7 Using ZENworks Desktop Management Preboot Services

The following changes are made in this section:

Location	Change
Section 56.1.3, "Illustrating the Preboot Services Processes for Linux Imaging Servers," on page 639	Added this section.

Location	Change
"Preboot Services Components for Linux Imaging Servers" on page 650	Added this section.
"Checking the Setup on a Linux Server" on page 651	Added this section.
"Linux DHCP Server" on page 653	Added this section.
"Linux Server Configuration" on page 655	Added this section.
Section 56.4.2, "Network Configuration," on page 657	Updated this section.
Section 56.6.1, "Configuring Preboot Services Servers in Linux," on page 670	Added this section.

K.2 December 9, 2005

Page design is reformatted to comply with revised Novell documentation standards.

Updates are made to the following guide sections:

- [Updating ZENworks Imaging Resource Files](#)

K.2.1 Updating ZENworks Imaging Resource Files

The following changes are made in this section:

Location	Change
Chapter 65, "Updating ZENworks Imaging Resource Files," on page 789	This is a new section. This includes documentation on adding Linux drivers.

Remote Management

VII

The Remote Management component of Novell® ZENworks® 7 Desktop Management gives you the ability to manage remote workstations from the management console. Remote Management allows you to:

- Remotely wake up a powered-off managed workstation
- Remotely control the managed workstation
- Remotely run executables found on the managed workstation with system rights, even if the logged-in user is not a member of the local Administration Group
- Transfer files between the remote management console and the managed workstation
- Display information to diagnose problems on the managed workstation
- Log audit record information about the Remote Management sessions running on the managed workstation
- Blank the managed workstation screen during a Remote Control session
- Lock the keyboard and mouse controls at the managed workstation during a Remote Control session

IMPORTANT: You can also use the Remote Management functionality on servers. For more information, see the [ZENworks 7 Server Management documentation \(http://www.novell.com/documentation/zenworks7\)](http://www.novell.com/documentation/zenworks7).

Remote Management can save you and your organization time and money. For example, you or your organization's help desk can analyze and remote fix workstation problems without visiting the user's workstation, which reduces problem resolution times and increases productivity.

The following sections can help you understand and use Remote Management:

- [Chapter 68, "Understanding Remote Management," on page 813](#)
- [Chapter 69, "Setting Up Remote Management," on page 817](#)
- [Chapter 70, "Managing Remote Workstations," on page 833](#)
- [Chapter 71, "Viewing the Diagnostic Information," on page 857](#)
- [Appendix L, "Documentation Updates," on page 869](#)

Understanding Remote Management

68

You can use Novell® ZENworks® 7 Desktop Management to remotely manage Windows 98 and Windows 2000/XP workstations from the management console.

The following sections provide information to help you understand the functionality of Remote Management components:

- [Section 68.1, “Remote Management Terminology,” on page 813](#)
- [Section 68.2, “Understanding the Remote Management Components,” on page 814](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

68.1 Remote Management Terminology

The following brief glossary provides basic definitions of Remote Management terms:

Managed workstation: A workstation that you want to remotely manage. To remotely manage a workstation, you must install the ZENworks 7 Remote Management Agent on it.

Management server: A server where ZENworks 7 Desktop Management server is installed.

Management console: A Windows machine running Novell ConsoleOne®. The management console provides the interface to manage and administer your machines.

Remote operator: A user who can remotely manages workstations from management console.

Administrator: A person who has the rights to install Remote Management. All administrators are remote operators but all remote operators are not administrators.

Remote Management Agent: A Desktop Management component that is installed on a managed workstation, which enables the remote operator to remotely manage that workstation. The Remote Management Agent starts automatically when the managed workstation boots up. It verifies whether the Remote Operator is authorized to perform operations on the workstation before the Remote Management session proceeds.

Viewing window: A representation of the managed workstation desktop. It is displayed on the management console when the remote operator initiates a Remote Management session.

Registered workstation: A workstation that is registered in eDirectory and imported as an eDirectory Workstation object.

68.2 Understanding the Remote Management Components

The following sections provide information to help you understand the functionality of Remote Management components. You must install the Remote Management Agent on the managed workstation to perform the Remote Management operations.

- [“Understanding Remote Control” on page 814](#)
- [“Understanding Remote View” on page 814](#)
- [“Understanding Remote Execute” on page 814](#)
- [“Understanding Remote Diagnostics” on page 815](#)
- [“Understanding File Transfer” on page 815](#)
- [“Understanding Remote Management Auditing” on page 815](#)
- [“Understanding the Remote Management Events using Windows Event Viewer” on page 815](#)
- [“Understanding Remote Wake Up” on page 816](#)

68.2.1 Understanding Remote Control

Remote Control lets you control a managed workstation from the management console to provide user assistance and to help resolve workstation problems.

Remote Control establishes a connection between the management console and the managed workstation. With remote control connections, the remote operator can go beyond viewing the managed workstation to taking control of it. For more information, see [Section 70.2, “Managing a Remote Control Session,” on page 836](#).

68.2.2 Understanding Remote View

Remote View lets you connect with a managed workstation so you can view the managed workstation instead of controlling it. This helps you troubleshoot problems that the user encountered. For example, you can observe how the user at a managed workstation performs certain tasks to make sure that the user performs a task correctly. For more information, see [Section 70.1, “Managing a Remote View Session,” on page 833](#).

68.2.3 Understanding Remote Execute

Remote Execute lets you run any executable on the managed workstation from the management console. An application can be remote executed by specifying its executable name in the Remote Execute window (if the program is in the path of the managed workstation) or by entering the complete path of the application (if it is not in the path of the managed workstation). For more information, see [Section 70.3, “Managing a Remote Execute Session,” on page 842](#).

You can determine the path information from the Environment window launched from the Diagnostic feature. For more information, see [Section 71.3, “Environment Information,” on page 860](#).

68.2.4 Understanding Remote Diagnostics

Remote Diagnostics helps you shorten problem resolution times and assist users without requiring a technician to physically visit the problem workstation. This increases user productivity by keeping desktops up and running. For more information, see [“Viewing the Diagnostic Information” on page 857](#).

Diagnostics provide real-time information so the remote operator can diagnose workstation problems. Following is a list of the diagnostic information that is available on Windows 2000/XP managed workstations:

- Windows Memory
- Environment
- Network Protocols
- Name Space Provider
- Event Log
- Device Drivers
- Services

68.2.5 Understanding File Transfer

File Transfer lets you perform file operations between the management console and a managed workstation.

Using File Transfer, you can move or copy files between the management console and a managed workstation. You can also rename and delete files, and create directories on the management console and on the managed workstation. From the File Transfer window, you can view the properties of files and directories on the management console and the managed workstation. File Transfer also lets you open files with the associated application on the management console. For more information, see [Section 70.4, “Managing a File Transfer Session,” on page 842](#).

IMPORTANT: The File Transfer program does not allow access to non-fixed drives on the managed workstation.

68.2.6 Understanding Remote Management Auditing

Remote Management Auditing generates audit records for every Remote Management session running on the managed workstation. The managed workstation where the Remote Management Agent is installed maintains this log information as an audit log. For more information, see [Section 70.8, “Managing a Remote Management Audit Session,” on page 850](#).

68.2.7 Understanding the Remote Management Events using Windows Event Viewer

The Windows 2000/XP event logging mechanism allows applications running on the managed workstation to record events as log files. You can use the Event Viewer to view the event logs. The Event Viewer maintains Application, Security, and System log files. The events for Remote Management sessions are stored in the Application log file. For more information, see [Section 70.6](#),

“Viewing the Audit Log of Remote Management Sessions Using the Windows Event Viewer,” on page 846.

68.2.8 Understanding Remote Wake Up

Remote Wake Up lets you remote power up a single node or a group of powered-down nodes in your network (provided the network card on the node is Wake on LAN enabled). This feature lets the remote operator manage nodes during off-hours to minimize the downtime users experience for system maintenance and upgrades. It also facilitates saving power while keeping systems available for maintenance. For more information, see [Section 70.1, “Managing a Remote View Session,” on page 833](#).

Setting Up Remote Management

69

The following sections provide information on deploying the Remote Management component of Novell® ZENworks® 7 Desktops Management in a production environment

- [Section 69.1, “Remote Management Deployment Strategies,” on page 817](#)
- [Section 69.2, “Configuring the Remote Management Policy for the Registered Workstations,” on page 819](#)
- [Section 69.3, “Configuring the Remote Management Policy for Non-Registered Workstations,” on page 822](#)
- [Section 69.4, “Setting Up the Remote Management Agent Password,” on page 822](#)
- [Section 69.5, “Assigning Rights to the Remote Operator,” on page 822](#)
- [Section 69.6, “Operating with Windows XP Service Pack 2,” on page 823](#)
- [Section 69.7, “Starting Remote Management Operations Using ConsoleOne,” on page 824](#)
- [Section 69.8, “Starting Remote Management Operations Without Using ConsoleOne,” on page 827](#)
- [Section 69.9, “Configuring Remote Management Ports,” on page 830](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

69.1 Remote Management Deployment Strategies

The Remote Management Agent must be installed on a managed workstation so the remote operator can remotely manage that workstation.

Remote Management Agent is a ZENworks Desktop Management component installed on a managed workstation. The agent enables the remote operator to remotely manage the workstation. The Remote Management Agent starts automatically when the managed workstation boots up. It verifies whether the Remote Operator is authorized to perform operations on the workstation before the Remote Management session proceeds.

Following are the modes of Remote Management authentication:

- [“Password-Based Remote Management” on page 817](#)
- [“Directory-Based Remote Management” on page 818](#)

69.1.1 Password-Based Remote Management

In this type of Remote Management deployment, you can initiate a Remote Management session with the managed workstation whether or not the managed workstation is imported as an eDirectory™ Workstation object.

Password-Based Remote Management is a secured means of Remote Management authentication. As a result, the remote operator can automatically initiate Remote Management operations, without re-entering password or authentication information each time.

To deploy Password-Based Remote Management:

- 1 Install the Remote Management server-side components of ZENworks 7 Desktop Management. For more information, see the *Novell ZENworks 7 Desktop Management Installation Guide*.
- 2 During the Agent installation, choose to install the Remote Management Agent component only on the workstations that you want to remotely manage.

IMPORTANT: To remotely manage registered workstations, you must choose to install Workstation Manager along with the Remote Management Agent.

- 3 Set the Remote Management Agent password at the managed workstation.
For more information, see [Section 69.4, “Setting Up the Remote Management Agent Password,” on page 822](#).
Usually, the Remote Management Agent password is set by the user at the managed workstation.
- 4 To remotely manage registered workstations, configure the Remote Management policy.
For more information, see [Section 69.2, “Configuring the Remote Management Policy for the Registered Workstations,” on page 819](#).

69.1.2 Directory-Based Remote Management

In this type of Remote Management deployment, for the Remote Management Agent to accept a Remote Management request, the managed workstation must be registered in eDirectory and imported as an eDirectory Workstation object.

The Remote Management Agent uses eDirectory based authentication to verify whether the remote operator requesting to remotely manage the workstation is authorized to do so. The effective policy settings based on which the remote operator performs Remote Management sessions on the managed workstation are computed from the Remote Control policy for the eDirectory Workstation object and the User object of the user logged in to the managed workstation.

To deploy Directory-Based Remote Management:

- 1 Register the workstation in eDirectory and import it as an eDirectory Workstation object.
For more information, see the *Novell ZENworks 7 Desktop Management Installation Guide*.
- 2 Install the ZENworks Desktop Management server-side components.
For more information, see the *Novell ZENworks 7 Desktop Management Installation Guide*.
- 3 During the Agent installation, choose to install Remote Management Agent and Workstation Manager.
- 4 Configure the Remote Management policy.
For more information, see [Section 69.2, “Configuring the Remote Management Policy for the Registered Workstations,” on page 819](#).

69.2 Configuring the Remote Management Policy for the Registered Workstations

The Remote Management policy is an eDirectory object in a policy package. Policy packages are eDirectory objects that contain policies grouped according to the object type. Object types can be Workstation object, Workstation Group, User object, User Group, or Container object.

The Remote Management policy enables the administrator to specify security settings for various Remote Management sessions. The administrator can use the ZENworks Policy wizard to create a policy package or use an existing Remote Management policy for an object. The policy packages are categorized into Workstation Policy Packages and User Policy Packages. The Workstation Policy Package and the User Policy Package are further categorized based on the operating system of the workstation or the operating system that the user is logged in to. Each policy package has a set of default policies that you can use. By default, the Remote Management policy is available from all the listed User and Workstation policy packages provided by Desktop Management, including:

- General
- Windows 9x
- Windows NT-2000-XP
- Windows NT
- Windows 2000
- Windows XP

The default values are provided for parameters in each page of the Remote Management policy. You can change the default values to suit your requirements.

To change the default values:

- 1 In Novell ConsoleOne[®], create a Workstation policy package.

For more information about how to create the policy packages, see the *Novell ZENworks 7 Desktop Management Installation Guide*.

- 2 Right-click the Workstation policy package, click *Properties* and select the *Policies* tab.
- 3 Select the check box under the *Enabled* column for the Remote Control Policy.
- 4 Click *Properties*, then click *Remote Management*.
- 5 Click the remote session tab for which you want to change settings, then select the options that you want to use.

The following table provides a description of options available in the Remote Management policy:

Tab	Options	Description
<i>General</i>	<i>Enable Diagnostics</i>	Allows the remote operator to diagnose the managed workstation.
	<i>Enable Password-Based Remote Management</i>	Allows the remote operator to establish a Remote Management session with the managed workstation using the password mode of authentication after the workstation was imported.

Tab	Options	Description
	<i>Enable Session Encryption</i>	<p>If this option is enabled, the Remote Control and Remote View sessions is encrypted. The Remote Operator cannot change this to an unencrypted mode. When the option is disabled, the remote sessions are unencrypted by default. In this case, the Remote Operator has an option to switch over to the encrypted mode from the Console. An encrypted session slightly impacts the performance of remote sessions over fast links.</p> <hr/> <p>IMPORTANT: This option does not work with Novell ZENworks for Desktops 4.x and older versions of Agent.</p> <hr/>
	<i>Allow User to Request Remote Session</i>	<p>If this option is enabled, the user at the managed workstation can request the Remote Operator on the management console to perform a remote session.</p> <hr/> <p>IMPORTANT: This option does not work for ZENworks for Desktops 4.x and older versions of the agent.</p> <hr/>
	<i>Terminate Session When Workstation User Logs In Requires To Be Prompted for Permission</i>	<p>Terminates any ongoing Remote Management session when a new eDirectory user, whose permission for initiating any Remote Management operation is required, logs into the managed workstation.</p>
	<i>Accept Connections across NAT/Proxy</i>	<p>Enables the Remote Management Agent to accept connection with the management console across NAT or Proxy. This is applicable for connections initiated through the Directory-based authentication only.</p>
	<i>Prompt User for Permission to Accept Connections across NAT/Proxy</i>	<p>Allows the user at the managed workstation to accept or reject connections across NAT or Proxy. This is applicable for connections initiated through the Directory-based authentication only.</p>
	<i>Display Remote Management Agent Icon to Users</i>	<p>Displays the <i>Remote Management Agent</i> icon in the taskbar of the Windows 98 and Windows 2000/XP managed workstation on which the Remote Management Agent is running.</p>
Control	<i>Enable Remote Control</i>	<p>Allows the remote operator to remotely control the managed workstation.</p>
	<i>Prompt User for Permission to Remote Control</i>	<p>Allows the user at the managed workstation to either accept or reject the Remote Control session initiated by the remote operator.</p>

Tab	Options	Description
View	<i>Give User Audible Signal when Remote Controlled</i>	Generates an audible signal on the managed workstation every time the remote operator remotely controls the managed workstation. You can modify the time interval for when the audible signal should be generated.
	<i>Give User Visible Signal when Remote Controlled</i>	Displays a visible signal with the name of the remote operator on the managed workstation every time the remote operator remote controls the managed workstation. You can modify the time interval as to when the name should be displayed.
	<i>Allow Blanking User's Screen</i>	Allows the remote operator to blank the screen of the managed workstation during a remote control session and also lock the mouse and the keyboard controls.
	<i>Allow Locking User's Keyboard Mouse</i>	Allows the remote operator to lock the mouse and keyboard controls of the managed workstation during a remote control session.
	<i>Enable Remote View</i>	Allows the remote operator to remotely view the desktop of the managed workstation.
	<i>Prompt User for Permission to Remote View</i>	Allows the user at the managed workstation to either accept or reject the Remote View session initiated by the remote operator.
	<i>Give User Audible Signal when Remote Viewed</i>	Enables the management console to send an audible signal to the managed workstation every time the remote operator remotely views the managed workstation.
	<i>Give User Visible Signal when Remote Viewed</i>	Enables the management console to send a visible signal to the managed workstation every time the remote operator remotely views the managed workstation.
File Transfer	<i>Enable File Transfer</i>	Allows the remote operator to transfer files between the management console and the managed workstation.
	<i>Prompt User for Permission to Transfer Files</i>	Allows the user at the managed workstation to either accept or reject the File Transfer session initiated by the remote operator.
Remote Execute	<i>Enable Remote Execute</i>	Allows the remote operator to execute applications or files on the managed workstation.
	<i>Prompt User for Permission to Remote Execute</i>	Allows the user at the managed workstation to either accept or reject the Remote Execute session initiated by the remote operator.

The administrator can change the default settings on any page of the Remote Management policy. If you change the *Remote Management Agent* icon setting, you must restart the Remote

Management Agent for the changes to take effect. The new settings are applied for all subsequent Remote Management sessions.

NOTE: To traverse the options of the Remote Operations button, press Ctrl+Up or Ctrl+Down.

- 6 Click the *Associations* tab, then click *Add*.
- 7 Browse to and select the container object where the workstations are registered, then click *OK*.
- 8 Click *Apply*, then click *Close*.

69.3 Configuring the Remote Management Policy for Non-Registered Workstations

You can change the security settings on the non-registered managed workstations by modifying the [Remote Management Policy] section in the `ZENworks_agent_directory\remotemanagement\rmagent\rmcfg.ini` file.

69.4 Setting Up the Remote Management Agent Password

The user at the managed workstation must set a password for the Remote Management Agent and communicate the password to the remote operator.

- 1 Right-click the *Remote Management Agent* icon.
- 2 Click *Security*, then click *Set Password*

Use a password of ten or fewer ASCII characters. The password is case-sensitive and cannot be blank.

NOTE: The password is stored in an encrypted form in `HKLM\software\novell\zenworks\remote management\rmagent.password`. It is encrypted in the registry with a non-machine specific hash. This means you can use NAL to distribute a standard password.

69.5 Assigning Rights to the Remote Operator

You can use the Manage Remote Operators wizard to set up the required rights for a management console user or a set of users to manage a workstation. Alternatively, you can use the Remote Operators tab in the properties of a workstation to add a user as a remote operator while providing the appropriate Remote Management rights.

69.5.1 Assigning Rights Using the Remote Operator Wizard

The Remote Operator Wizard is a utility that runs on the NDS[®] namespace.

To assign the required rights using the Remote Operator Wizard:

- 1 In ConsoleOne, select an eDirectory tree in the NDS namespace.
- 2 Click *Tools*, then click *Manage Remote Operator*.

- 3 Click *Add* to browse and select the container or the workstation you want to manage from the list of containers and workstations.

If you want to remove any of the container or the workstation, select the container or the workstation, then click *Remove*.

- 4 Select the check box to inherit the properties for the workstations that you want to import into the container.

If you choose to select the check box, the properties are also inherited to workstations that you add later to the container.

- 5 Click *Next*.

- 6 In the Remote Management Operations list, you must assign at least one Rights option. By default all the operations are indicated by ☒.

To assign Remote Management operation rights, click the button until the symbol is ☒.

To remove Remote Management operation rights, click the button until the symbol is ☐.

- 7 Click *Next*.

- 8 Click *Add* to browse and select the container or the user to whom you want to assign the rights.

To disassociate a container or a user, select the container or the user, then click *Remove*.

- 9 Click *Next*.

A summary of the selected container or workstation, remote management rights that are assigned or removed, and names of the affected remote operators is displayed.

- 10 Click *Finish*.

69.5.2 Assigning Rights Using the Remote Operators Tab

- 1 In ConsoleOne, right-click the workstation object.

- 2 Click *Properties* > the *Remote Operators* tab > *Add*.

- 3 In the Select Objects dialog box, do the following:

- 3a Select an object type from the *Object Type* drop-down list.

- 3b To list the contents of a higher container, select the container from the *Look in* drop-down list.

- 3c Select an object, then click *OK*.

- 4 Click *Apply*, then click *OK*.

NOTE: To remove an object from the list of remote operators, select the object, then click *Remove*.

69.6 Operating with Windows XP Service Pack 2

Windows XP Service Pack 2 (SP2) comes with a firewall enabled by default. As a result, the Remote Management Agent and Remote Control Listener running on Windows XP SP2 does not receive connections initiated by the Remote Management Console and the Remote Management Agent, respectively.

You must configure the firewall settings to allow the Remote Management Agent and the Remote Control Listener to receive connections.

By default, the Remote Management Agent and the Remote Control Listener bind to TCP ports 1761 and 1762. In order to change the ports, refer to [Section 69.9, “Configuring Remote Management Ports,”](#) on page 830.

69.7 Starting Remote Management Operations Using ConsoleOne

The Remote Management Agent starts automatically when the managed workstation boots up. The remote operator can initiate a Remote Management session in any of the following ways:

- [“Initiating a Directory-Based Remote Management Session”](#) on page 824
- [“Initiating a Password-Based Remote Management Session”](#) on page 825
- [Section 69.7.3, “Initiating Remote Management Session from the Remote Management Agent,”](#) on page 827

69.7.1 Initiating a Directory-Based Remote Management Session

NOTE: The selected user must be logged into at least one managed workstation before Directory-Based Remote Management is initiated.

You can initiate directory-based Remote Management using either of the following methods:

- [“From the Workstation Object”](#) on page 824
- [“From the User Object”](#) on page 824

From the Workstation Object

The following table lists the directions for initiating a Remote Management session.

Table 69-1 *Initiating a Remote Management Session*

Remote Management Session	To Initiate
Remote Control	Right-click the managed workstation, then click <i>Actions > Remote Control</i> .
Remote View	Right-click the managed workstation, then click <i>Actions > Remote View</i> .
File Transfer	Right-click the managed workstation, then click <i>Actions > File Transfer</i> .
Remote Execute	Right-click the managed workstation, then click <i>Actions > Remote Execute</i> .
Diagnostics	Right-click the managed workstation, then click <i>Actions > Diagnostics</i> .
Remote Wake Up	Right-click the managed workstation, then click <i>Actions > Remote Wake Up</i> .
Remote Audit	Right-click the managed workstation, then click <i>Actions > Remote Audit</i> .

From the User Object

- 1 In ConsoleOne, right-click a user object.

The selected user must be logged in to at least one managed workstation before Directory-Based Remote Management is initiated.

2 Click *Remote Management*.

3 In the Remote Management dialog box:

3a Select the IP address of the managed workstation which you want to remotely manage.

If the user has logged into the eDirectory through the Middle Tier, the list of IP addresses contains the IP address of the Middle Tier. To filter this address, in the `ConsoleOne_installation_directory\1.2\bin\drishtitype.ini` file, add the `XTierServerAddresses` property and specify the Middle Tier IP addresses. For example, `XTierServerAddresses = Middle_Tier_IP_address1, Middle_Tier_IP_address2, ...`

3b Select a Remote Management operation which you want to perform on the selected managed workstation.

3c Select *Directory-Based*, then click *OK*.

69.7.2 Initiating a Password-Based Remote Management Session

NOTE: The selected user must be logged into at least one managed workstation before Directory-Based Remote Management is initiated.

Before initiating the Password-based Remote Management, make sure that the following prerequisites are met:

Table 69-2 Prerequisites to Initiate a Password-based Remote Management

Is the managed workstation registered in eDirectory and imported as an eDirectory workstation object?	Has an eDirectory user logged at the managed workstation?	To initiate a Password-Based Remote Management Session
Yes	Yes	<ul style="list-style-type: none">• The <i>Enable Password-Based Remote Management</i> option in the Remote Control policy of the managed workstation object must be enabled.• The <i>Enable Password-Based Remote Management</i> option in the user object's Remote Management property page must be enabled.• The workstation user must have a password set on the managed workstation.
Yes	No	<ul style="list-style-type: none">• The <i>Enable Password-Based Remote Management</i> option in the Remote Control policy of the managed workstation object must be enabled.• The workstation user must have a password set on the managed workstation.

Is the managed workstation registered in eDirectory and imported as an eDirectory workstation object?	Has an eDirectory user logged at the managed workstation?	To initiate a Password-Based Remote Management Session
No	Yes	<ul style="list-style-type: none"> The workstation user must have a password set on the managed workstation.
No	No	<ul style="list-style-type: none"> The workstation user must have a password set on the managed workstation.

You can initiate Password-Based Remote Management using either of the following methods:

- “From the ConsoleOne Menu” on page 826
- “From the User Object” on page 826

From the ConsoleOne Menu

- 1 In ConsoleOne, click *Tools > Remote Management > Windows*.
- 2 In the Remote Management dialog box:
 - 2a Enter or select the IP address or DNS name of the managed workstation with which you want to initiate a Remote Management session.
 - 2b Enter the password set by the workstation user on the managed workstation.
 - 2c Select a Remote Management operation that you want to perform on the selected managed workstation.

From the User Object

- 1 In ConsoleOne, right-click a user object.

The selected user must be logged in to at least one managed workstation before Password-Based Remote Management is initiated.
- 2 Click *Remote Management*.
- 3 In the Remote Management dialog box:
 - 3a Select the IP address of the managed workstation which you want to remotely manage.

If the user has logged into the eDirectory through the Middle Tier, the list of IP addresses contains the IP address of the Middle Tier. To filter this address, in the `ConsoleOne_installation_directory\1.2\bin\drishtitype.ini` file, add the `XTierServerAddresses` property and specify the Middle Tier IP addresses. For example, `XTierServerAddresses = Middle_Tier_IP_address1, Middle_Tier_IP_address2, ...`
 - 3b Select a Remote Management operation that you want to perform on the selected managed workstation.
 - 3c Click *Password*.
 - 3d Enter the password set by the workstation user on the managed workstation.
 - 3e Click *OK*.

69.7.3 Initiating Remote Management Session from the Remote Management Agent

If the managed workstation is configured behind dynamic NAT, the managed workstation cannot be accessed from the management console but the management console can be accessed from the managed workstation. To resolve this problem:

- 1 The user at the managed workstation must initiate a request for a Remote Management session to the remote operator by using the Request Session option.

IMPORTANT: Before initiating a Remote Management session from the Remote Management Agent, the remote operator must make sure that ConsoleOne is running on the management console.

To request a session, the user at the managed workstation must do the following:

- 1a Right-click the *Remote Management Agent* icon.
- 1b Select *Request Session*.
- 1c Specify the IP address or the DNS name of the management console.
- 1d Select the *Remote Control* or *Remote View* operation from the drop-down list.
- 1e Click *OK*.
- 2 The Remote Management Listener listens to the request and notifies the remote operator about it. The remote operator must accept the request and provide the following credentials for the request in the Select Authentication Mode dialog box:
 - 2a Select the *Directory* option for directory-based authentication.
 - or
 - Select the *Password* option for password-based authentication.
 - 2b If the password-based authentication is selected, enter the password for authentication.
 - 2c Click *OK*.

Operating in the Terminal Server Environment

The first instance of ConsoleOne receives the request when a session request is initiated from a managed server to the management console running on a terminal server. None of the ConsoleOne instances receive the session request until all ConsoleOne instances on the session where ConsoleOne was launched for the first time are closed. To receive the session request, ConsoleOne must be launched again on any terminal session.

69.8 Starting Remote Management Operations Without Using ConsoleOne

The `desktop4.exe` application that ships with ZENworks 7 Desktop Management allows you to start the following Remote Management operations without using ConsoleOne: Remote Control, Remote View, Remote Execute, File Transfer, Remote Wake Up, and Remote Diagnostics.

You can install `desktop4.exe` using either of the following methods:

- Install the ZENworks 7 Desktop Management ConsoleOne snap-ins. This automatically installs `desktop4.exe`. `Desktop4.exe` is located in the `ConsoleOne_installation_directory\consoleone_version\bin` directory.
- From the desktop directory in the *ZENworks 7 Companion 2* CD, extract `desktop.zip` to a temporary directory on your machine. Copy the contents of `temporary_directory\desktop` to the `ConsoleOne_installation_location` directory.

Before you can run `desktop4.exe`, you must perform the following tasks.

- 1 For Password-Based Remote Management, enter the following details in the `ConsoleOne_installation_directory\bin\remagent.ini` file:

Agent IP address: IP address of the managed workstation.

Agent Password: Remote Management Agent password.

Authentication Mode: PASSWORD.

Protocol: Enter TCPIP.

A sample `remagent.ini` file is as follows:

```
# Novell Inc.  
AGENT_IPADDRESS=164.99.149.37  
AGENT_PASSWORD=novell  
AUTHENTICATION_MODE=PASSWORD  
PROTOCOL=TCPIP
```

- 2 If you want to perform the Remote Management operation using the Directory mode of authentication, you must log into the eDirectory tree to which the Managed workstation is imported. For Directory-Based Remote Management, make sure that the `AUTHENTICATION_MODE` in `ConsoleOne_installation_directory\bin\remagent.ini` file is DS.
- 3 You can run `desktop4.exe` from the MS-DOS prompt or by using a `.bat` file. You must specify valid values for the following parameters

- **-w:** Fully qualified Distinguished Name (DN) of the managed workstation
- **-n:** eDirectory tree name
- **-c:** Remote Management operation to be performed on the managed workstation.

To do a file transfer, enter `-c"File Transfer"`

To perform diagnostics, enter `-c"Diagnostics"`

To use remote control, enter `-c"RemoteControl"`

To use remote view, enter `-c"RemoteView"`

To remotely execute a file, enter `-c"Remote Execute"`

To do a remote wake-up, enter `-c"Remote Wakeup"`

For example, you can perform Remote control using either of the following methods:

- At the MS-DOS prompt, enter the following command:

```
Desktop4 -w"CN=WINXP-R1B164_99_151_48.OU=WsProm.O=novell" -  
n"INDYPROM-TREE" -c"RemoteControl"
```

where Desktop4 is the name of the application; "CN=WINXP-R1B164_99_151_48.OU=WsProm.O=novell" is the DN of the managed workstation; "INDYPROM-TREE" is the eDirectory tree name; and "Remote Control" is the Remote Management operation to be performed on the managed workstation.

NOTE: You need to make sure that the remagent.ini file is updated with the specific details before you execute the desktop4.exe at the MS-DOS prompt.

- Using a .bat file.

- 1 Create a .bat file in the same directory as desktop4.exe with the following contents:

```
Desktop4 -w"CN=WINXP-R1B164_99_151_48.OU=WsProm.O=novell" -  
n"INDYPROM-TREE" -c"RemoteControl"
```

where Desktop4 is the name of the application; "CN=WINXP-R1B164_99_151_48.OU=WsProm.O=novell" is the DN of the managed workstation; "INDYPROM-TREE" is the tree name; and "RemoteControl" is the Remote Management operation to be performed on the managed workstation.

- 2 Run the .bat file.

Depending upon the operation that you have specified, the Remote Management session starts.

Desktop4.exe is a back-end utility that can be leveraged by developing user-friendly interface to launch desktop4.exe.

Using desktop4.exe, you can also view Inventory information of the inventoried workstations. For more information, see [Section 77.3, "Viewing Inventory Information Without Using ConsoleOne," on page 1145](#).

69.8.1 Launching User-Based Remote Management Using Desktop4.exe

You can launch Remote Management from desktop4.exe in both Password-Based or Directory-Based authentication mode.

To launch Remote Management from desktop4.exe:

- 1 Run the desktop.exe, then specify -w.
- 2 Populate the IP address of the managed workstation in which the user has logged in the `ConsoleOne_installation_directory\bin\remagent.ini` file.

69.9 Configuring Remote Management Ports

The Remote Management Agent and Remote Control Listener bind to TCP ports 1761 and 1762, respectively. In case there is a conflict of port numbers with some application, you can change the port numbers to which they bind as follows:

- [Section 69.9.1, “Configuring the Remote Management Agent Port,” on page 830](#)
- [Section 69.9.2, “Configuring the Remote Control Listener Port,” on page 830](#)
- [Section 69.9.3, “Customizing the Permission Message,” on page 831](#)

69.9.1 Configuring the Remote Management Agent Port

The Remote Management Agent port binds to TCP port 1761 by default. You might configure it to run on a different TCP port by following the steps mentioned below:

- 1 Open the `ZENworks_agent_directory\remotemanagement\rmagent\rmcfg.ini` file.
- 2 Under the *Remote Management Agent Port* section, set the *DefaultCommPort* to the desired port number.
- 3 Restart the Novell ZENworks Remote Management service.

To initiate a remote session to a managed workstation where the Remote Management Agent is running on any port other than 1761, the following modifications need to be done on the management console:

- 1 Open the `ConsoleOne_directory\1.2\bin\rmports.ini` file.
- 2 Under the *Remote Management Agent Ports* section, add the port number.

NOTE: If the Remote Management Agents are running on different ports on different managed workstations, you might mention the port numbers one below the other under the *Remote Management Agent Ports* section.

69.9.2 Configuring the Remote Control Listener Port

The Remote Control Listener port binds to TCP port 1762 by default when ConsoleOne is started. You might configure it to run on a different TCP port by following the steps mentioned below:

- 1 Open the `ConsoleOne_directory\1.2\bin\rmports.ini` file.
- 2 Under the *Remote Control Listener Port* section, set the *DefaultCommPort* to the desired port number.
- 3 Restart ConsoleOne.

To initiate a remote session request to a management console, where the Remote Control Listener is running on any port other than 1762, the following modifications need to be done on the managed workstations:

- 1 Open the `ZENworks_agent_directory\remotemanagement\rmagent\rmcfg.ini` file.
- 2 Under the *Remote Control Listener Ports* section, add the port number.

NOTE: If the Remote Control Listeners are running on different ports on different management consoles, you might mention the port numbers one below the other under the *Remote Control Listener Ports* section.

69.9.3 Customizing the Permission Message

If the *Ask for user permission* option is selected in the Remote Management policy, the Request for Permission dialog box is displayed with the following default message:

```
Do you want to allow console user to perform remote management
operation?
```

ZENworks 7 with Support Pack 1 allows you to customize the default message displayed in the Request for Permission dialog box.

- 1 To customize the default message, do the following on the managed server:
 - 1 Open the Registry Editor.
 - 2 Traverse to HKEY_LOCAL_MACHINE\Software\Novell\ZENworks\RemoteManagement\RMAgent and create a registry string in the name “PermissionMessage”.
 - 3 Enter the message that should be displayed in the Request for Permission dialog box as the value of the registry string created in the previous step.
 - 4 (Optional) In the registry string value, you can use the following parameters that will be dynamically replaced by valid information in the message:

Table 69-3 Parameters Used to Customize the Message of the Request for Permission dialog box

Parameter	Information Displayed
%a or %A	Displays the Remote console user name.
%i or %I	Displays the IP address of the management console.
%r or %R	Displays the Remote Management operation initiated by Remote Operator.

A sample registry string with parameters is as follows:

```
Do you want to allow %a to %r from the remote machine, %i?
```

The registry string is displayed as the following message in the Request for Permission dialog box:

```
Do you want to allow admin.novell to Remote Control from the remote
machine,10.0.0.0?
```


Managing Remote Workstations

70

The following sections provide information to help you effectively manage the Remote Management sessions of Novell® ZENworks® 7 Desktop Management:

- [Section 70.1, “Managing a Remote View Session,” on page 833](#)
- [Section 70.2, “Managing a Remote Control Session,” on page 836](#)
- [Section 70.3, “Managing a Remote Execute Session,” on page 842](#)
- [Section 70.4, “Managing a File Transfer Session,” on page 842](#)
- [Section 70.5, “Managing a Remote Wake Up Session,” on page 844](#)
- [Section 70.6, “Viewing the Audit Log of Remote Management Sessions Using the Windows Event Viewer,” on page 846](#)
- [Section 70.7, “Remote Operator Identification Display,” on page 849](#)
- [Section 70.8, “Managing a Remote Management Audit Session,” on page 850](#)
- [Section 70.9, “Generating Remote Management Reports,” on page 851](#)
- [Section 70.10, “Improving the Remote Management Performance,” on page 853](#)
- [Section 70.11, “Using the Remote Management Agents,” on page 854](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

70.1 Managing a Remote View Session

You can use ZENworks 7 to remotely view the managed workstation.

The following sections explain the tasks you can perform to effectively manage a Remote View session:

- [“Controlling the Display of the Viewing Window” on page 833](#)
- [“Using the Viewing Window Accelerator Keys” on page 834](#)
- [“Defining a Custom Accelerator Key Sequence” on page 836](#)

70.1.1 Controlling the Display of the Viewing Window

To enable the control options:

- 1 Click the *Remote Management Agent* icon, located at the top left corner of the Viewing window.
- 2 Click *Configure*.

Option	Description
<i>Enable High Quality Scaling</i>	Enhances the quality of images in the Scale To Fit Mode.

Option	Description
<i>Enable Accelerator Keys</i>	Allows you to enable or disable the default accelerator keys sequences.
<i>Enable Encryption</i>	<p>Encryption is an optional feature and is effective per session. If the saved configuration has enabled encryption, the session is encrypted from the start of the session.</p> <p>Encrypting a whole session provides greater security as the data transferred over the wire is encrypted and it is difficult to decipher anything meaningful even after the data over the wire is captured. However, it impacts performance slightly and is recommended when the security requirement is very stringent.</p>
<i>Hide Wallpaper</i>	Suppresses any wallpaper displayed on the managed workstation. This option is enabled by default. If you want to display the wallpaper on the managed workstation during a Remote View session, disable this option.
<i>Color Quality</i>	<p>By default, on a fast Link, the color quality is set to <i>Normal</i> and on a slow link the color quality is set to 256 colors. You can change the color quality of the slow link or the fast link to one of the following:</p> <ul style="list-style-type: none"> • 16 Colors: Forces the use of 16-color palette on the managed workstation during a Remote Management session. This enhances the Remote Management performance particularly over a slow link. • 256 Colors: Forces the use of 256-color palette on the managed workstation during a Remote Management session. This enhances the Remote Management performance over a slow link. • Normal: The color is not altered and the setting is the same on the managed workstation during a Remote Management session.
<i>Network Type</i>	<p>If the managed workstation is connected by a LAN, select the <i>Fast Links</i> option to enhance the Remote Management performance.</p> <p>If the managed workstation is connected over a dial-up link or by WAN, select the <i>Slow Links</i> option to enhance the Remote Management performance.</p>

- 3 To save the Control Parameter settings, click the *Save on Exit* check box.

The saved settings are implemented in the next Remote View session.

- 4 Click *OK*.

70.1.2 Using the Viewing Window Accelerator Keys

You can use accelerator keys to control the display of the Viewing window. Default accelerator key sequences are assigned to each accelerator key option. The Accelerator Keys dialog box displays the

default key sequence in the edit field of each accelerator key option. You can define a custom accelerator key sequence to change the default sequence. For more information, see [“Defining a Custom Accelerator Key Sequence” on page 836](#).

To enable the Accelerator Keys option:

- 1 Click the *Remote Management Agent* icon, located at the top left corner of the Viewing window.
- 2 Click *Configure*.
- 3 Select *Enable Accelerator Keys*.
- 4 Click *OK*.

To open the Accelerator Keys dialog box:

- 1 Click the *Remote Management Agent* icon, located at the top left corner of the Viewing window.
- 2 Click *Accelerator Keys*.

The following table explains the Accelerator Key options you can use during the Remote View session:

Table 70-1 Accelerator Key Options available during a Remote View Session

Option	Default Keystroke	Description
<i>Toggle Full Screen</i>	Ctrl+Alt+M	Applicable only if the color resolution settings on the management console and managed workstation are the same. Sizes the Viewing window to the size of your screen without window borders.
<i>Refresh Screen</i>	Ctrl+Alt+R	Refreshes the Viewing window.
<i>Restart Session</i>	Ctrl+Alt+T	Re-establishes the connection with the managed workstation.
<i>Enable Accelerator Keys</i>	Ctrl+Alt+A	Allows you to enable or disable the default accelerator key sequences.
<i>Stop Viewing</i>	Left-Shift+Esc	Closes the Viewing window.
<i>Configure Dialog</i>	Alt+M	Opens the Control Parameters dialog box.
<i>Accelerator Keys Dialog</i>	Alt+A	Opens the Accelerator Keys dialog box.
<i>Poll Full Screen</i>	Alt + L	Scans and renders the information of the entire screen of the managed workstation continuously.
<i>Scale To Fit</i>	Ctrl+Alt+G	Hides the scroll bars and scales the Remote Management window to fit your screen.

70.1.3 Defining a Custom Accelerator Key Sequence

Default keystrokes assigned to the accelerator key option are displayed in the edit field to the right of each accelerator key option in the Accelerator Keys dialog box. You can change the accelerator key sequence and define a custom accelerator key sequence if you do not want to use the default.

To define a custom accelerator key sequence:

- 1 Click the *Remote Management Agent* icon, located at the top left corner of the Viewing window.
- 2 Click *Accelerator Keys*.
- 3 Click the edit field of the accelerator key option where you want to define a custom accelerator key sequence.
- 4 Press the new accelerator key sequence.
- 5 Click *OK*.

IMPORTANT: The shift keys are left-right sensitive, and are indicated in the Control Options dialog box as LShift and RShift. Avoid the use of standard key sequences like Ctrl+C, Ctrl+V, and Shift+Del.

70.2 Managing a Remote Control Session

Remote Management lets you remote control a managed workstation. You can use Remote Control to provide user assistance and to help resolve workstation problems. With remote control connections, the remote operator can go beyond viewing the managed workstation to taking control of it.

You can effectively manage a Remote Control session by performing the following tasks:

- [“Controlling the Display of the Viewing Window” on page 836](#)
- [“Using the Viewing Window Accelerator Keys” on page 838](#)
- [“Using the Toolbar Buttons on the Viewing Window” on page 839](#)
- [“Enabling the Wallpaper on the Managed Workstation” on page 840](#)
- [“Obtaining Information About Remote Management Sessions” on page 841](#)

70.2.1 Controlling the Display of the Viewing Window

You can control the display of the managed workstation by using the Viewing window control options.

To enable the control options:

- 1 Click the *Remote Management Agent* icon, located at the top left corner of the Viewing window.
- 2 Click *Configure*.
- 3 Select the control options you want to enable for the remote session.

Option	Description
<i>Blocks Mouse Movements to Agent</i>	To reduce network bandwidth consumption, blocks all the mouse movements to the Agent.
<i>Enable High Quality Scaling</i>	Enhances the quality of images in the Scale To Fit mode.
<i>Enable Accelerator Keys</i>	Enables the accelerator keys on the management console so that you can change the default accelerator key sequences during the remote session.
<i>Enable Encryption</i>	<p>Encryption is an optional feature and is effective per session. If the saved configuration has enabled encryption, the session is encrypted from the start of the session.</p> <p>Encrypting a whole session provides greater security because the data transferred over the wire is encrypted and it is difficult to decipher anything meaningful even after the data over the wire is captured. However, it impacts performance slightly and is recommended when the security requirement is very stringent.</p>
<i>System Key Pass</i>	<p>Passes Alt-key sequences from the management console to the managed workstation.</p> <hr/> <p>NOTE: During a Remote View session, the <i>System Key Pass-Through</i> option is not enabled.</p> <hr/>
<i>Hide Wallpaper</i>	Suppresses any wallpaper displayed on the managed workstation. This option is enabled by default. If you want to display the wallpaper on the managed workstation during a Remote Control or Remote View session, disable this option.
<i>Color Quality</i>	<p>By default, on a fast Link, the color quality is set to Normal and on a slow link the color quality is set to 256 colors. You can change the color quality of the slow link or the fast link to one of the following:</p> <ul style="list-style-type: none"> • 16 Colors: Forces the use of 16-color palette on the managed workstation during a Remote Management session. This enhances the Remote Management performance particularly over a slow-link. • 256 Colors: Forces the use of 256-color palette on the managed workstation during a Remote Management session. This enhances the Remote Management performance over a slow-link. • Normal: The color is not altered and the setting is the same on the managed workstation during a Remote Management session.
<i>Network Type</i>	<p>If the managed workstation is connected by a LAN, select the <i>Fast Links</i> option to enhance the Remote Management performance.</p> <p>If the managed workstation is connected over a dial-up link or by WAN, select the <i>Slow Links</i> option to enhance the Remote Management performance.</p> <hr/>

- 4 To save the Control Parameter settings, click the *Save on Exit* check box.
- The saved settings are implemented in the next Remote Control session.

70.2.2 Using the Viewing Window Accelerator Keys

You can use accelerator keys to control the display of the Viewing window. Default accelerator key sequences are assigned to each accelerator key option. The Accelerator Keys dialog box displays the default key sequence in the edit field of each accelerator key option. You can define a custom accelerator key sequence to change the default sequence. For more information, see [“Defining a Custom Accelerator Key Sequence” on page 836](#).

To enable the Accelerator Keys option:

- 1 Click the *Remote Management Agent* icon, located at the top left corner of the Viewing window.
- 2 Click *Configure*.
- 3 Select *Enable Accelerator Keys*.

To open the Accelerator Keys dialog box:

- 1 Click the *Remote Management Agent* icon, located at the top left corner of the Viewing window.
- 2 Click *Accelerator Keys*.

Table 70-2 Viewing Window Accelerator Keys





Option	Default Keystroke	Description
<i>Toggle Full Screen</i>	Ctrl+Alt+M	Applicable only if the resolution settings on the management console and managed workstation are same. Sizes the Viewing window to the size of your screen without window borders.
<i>Refresh Screen</i>	Ctrl+Alt+R	Refreshes the Viewing window.
<i>Restart Session</i>	Ctrl+Alt+T	Re-establishes the connection with the managed workstation.
<i>Enable Accelerator Keys</i>	Ctrl+Alt+A	Enables you to change the default accelerator key sequences.
<i>Stop Viewing</i>	Left-Shift+Esc	Closes the Viewing window.
<i>Configure Dialog</i>	Alt+M	Opens the Control Parameters dialog box.
<i>Accelerator Keys Dialog</i>	Alt+A	Opens the Accelerator Keys dialog box.
<i>Poll Full Screen</i>	Alt + L	Scans and renders the information of the entire screen of the managed workstation continuously.
<i>Scale To Fit</i>	Ctrl+Alt+G	Hides the scroll bars and scale the Remote Management window to fit your screen.
<i>System Key Pass</i>	Ctrl+Alt+S	Passes Alt-key sequences on the management console to the managed workstation.
<i>Mouse/Keyboard Lock</i>	Ctrl+L	Locks the keyboard and mouse controls at the managed workstation.







Option	Default Keystroke	Description
<i>Blank Screen</i>	Ctrl+Alt+B	Blanks the screen at the managed workstation.
<i>Reboot</i>	Ctrl+Alt+D	Sends the Ctrl+Alt+Del keystroke to the managed workstation. Invokes the Security window on Windows 2000/XP managed workstation. Invokes the reboot confirmation dialog on Windows 98 managed workstation.
<i>Start</i>	Alt+R	Invokes the start menu on the managed workstation.
<i>Switch Applications</i>	Ctrl+T	Switches applications on managed workstations.

70.2.3 Using the Toolbar Buttons on the Viewing Window

The following table describes the toolbar options in the Viewing window:

Table 70-3 *Toolbar Options in the Viewing Window*

Button	Default Keystroke	Key Function
<i>Screen Blanking</i> 	Ctrl+Alt+B	<p>Enabled only if the <i>Allow Blanking User's Screen</i> option is enabled in the effective Remote Control policy of the managed workstation.</p> <p>Blanks the screen at the managed workstation. When the remote operator selects this option, the screen of the managed workstation is blacked out and the operations performed by the remote operator on the managed workstation are not visible to the user at the managed workstation.</p> <p>Not supported over certain display adapters. Refer to the ZENworks 7 Desktop Management Readme (http://www.novell.com/documentation/zenworks7) for the list of display adapters that do not support this feature.</p>
<i>Mouse and Keyboard Lock</i> 	Ctrl+L	Locks the keyboard and mouse controls at the managed workstation. When the remote operator selects this option, the user at the managed workstation is not able to use the keyboard and mouse controls of the managed workstation.
<i>System Start</i> 	Alt+R	Invokes the <i>Start</i> menu on the managed workstations.
<i>Application Switcher</i> 	Ctrl+T	<p>Sends the Alt-tab key sequences to the managed workstation.</p> <p>Switches applications on managed workstations. If you use the toolbar button, you must click it continuously to traverse through the applications and then press Tab to select the desired application. If you use the Ctrl+T accelerator key, you must use it as you would use the Alt+Tab sequence to switch between applications.</p>

Button	Default Keystroke	Key Function
<i>System Key Pass Through</i> 	Ctrl+Alt+S	Sets the system key pass to On or Off. Passes Alt-key sequences on the management console to the managed workstation.
<i>Reboot</i> 	Ctrl+Alt+D	Sends the Ctrl+Alt+Del keystroke to the managed workstation. Displays the Security window on Windows 2000/XP managed workstation. Displays the reboot confirmation dialog on Windows 98 managed workstation.
<i>Refresh</i> 	Ctrl+Alt+R	Refreshes the viewing window.
<i>Full Screen Polling</i> 	Alt+L	Scans and renders the information of the entire screen of the managed workstation continuously.
<i>Scale To Fit</i> 	Ctrl+Alt+G	Hides the scroll bars and scales the Remote Management window to fit your screen.
<i>Session Encryption</i> 		Encryption is an optional feature and is effective per session. If the saved configuration has the option enabled, the session is encrypted from the start of the session. Encrypting a whole session provides greater security because the data transferred over the wire is encrypted and it is difficult to decipher anything meaningful even after the data over the wire is captured. However, it impacts performance slightly and is recommended when the security requirement is very stringent.

You can define a custom key sequence if you do not want to use the default key sequence. For more information, see [“Defining a Custom Accelerator Key Sequence” on page 836](#).

70.2.4 Enabling the Wallpaper on the Managed Workstation

When the remote operator initiates a Remote Control session, any wallpaper displayed on the desktop of the managed workstation is suppressed. This feature reduces the response time from the managed workstation for requests from the management console because less traffic is generated over the network while the wallpaper is suppressed.

You can configure the control parameter for this option to change the default settings and enable the display of the wallpaper on the managed workstation. When you terminate the Remote Control session, the suppressed wallpaper is restored.

To enable the display of suppressed wallpaper on the managed workstation:

- 1 Click the *Remote Management Agent* icon, located at the top left corner of the Viewing window, then *Configure*.
- 2 Deselect the *Hide Wallpaper* option.

70.2.5 Obtaining Information About Remote Management Sessions

Using the Information window, the user at the managed workstation can view details about the session, such as the name of the remote operator who is remotely managing the workstation, the security settings, and the protocol in use for the remote session.

To view information about remote sessions:

- 1 Right-click the *Remote Management Agent* icon located in the system tray of the managed workstation.
- 2 Click *Information*.
- 3 Click the *General* tab to view the general information and the *Security* tab to view the security information.

See the following sections for details:

- “Obtaining General Information” on page 841
- “Obtaining Security Information” on page 841

70.2.6 Obtaining General Information

The following table explains the general information you can obtain about Remote Management sessions from the Information window:

Table 70-4 General Information of Remote Management Sessions that can be obtained from the Information Window

Parameter	Description
RM Operation	Lists the ongoing Remote Management sessions.
RM Information > Initiator	Displays the name of the remote operator.
RM Information > Protocol	Displays the protocol that the Remote Management Agent uses to communicate with the management console during a remote session.
Optimization Status > RC/RV Optimization	Displays if the optimization driver is enabled or disabled for the Remote Management session. The remote session performance is enhanced if the optimization driver is enabled.

70.2.7 Obtaining Security Information

The Security Information dialog box displays information based on the following categories of remote sessions:

- Remote Control
- Remote View
- File Transfer
- Remote Execute
- Others

70.3 Managing a Remote Execute Session

You can remotely run executables found on the managed workstation with system rights, even if the logged-in user is not a member of the local Administrator Group.

To execute an application program on a managed workstation, launch Remote Execute Window:

- 1 Enter the command line in the Remote Execute window.

Specify the complete path of the application if the application is not in the path of the managed workstation.

If you do not specify the extension of the file you want to execute at the managed workstation, Remote Execute appends the `.exe` extension.

- 2 Click *Execute*.

Enter the name of the application or the parameter within double quotes if the application or parameter has a space character. Following are a few examples:

```
"My Wordpad"
```

```
"C:\Program Files\Accessories\My Wordpad"
```

```
"C:\Program Files\Accessories\My Wordpad" "C:\myfile.txt"
```

```
"C:\Program Files\Accessories\My Wordpad" C:\myfile.txt"
```

```
"Wordpad"
```

70.4 Managing a File Transfer Session

ZENworks 7 Desktop Management enables you to transfer files between the management console and a managed workstation. Right-click the file or folder to view the list of available menu options.













NOTE: Transferring larger files (by launching file transfer from ConsoleOne®) might block the usage of ConsoleOne. In this case, launch the file transfer from `desktop4.exe`.

The following section explains how you can use File Transfer and the options that are available for working with files from the File Transfer window.

70.4.1 Using File Transfer Window Controls

The left pane of the File Transfer window shows the files in the current folder on the management console and the right pane shows the files on the managed workstation. The following table explains the function of the File Transfer controls:

Table 70-5 *File Transfer Window Controls*

Menu Option	Toolbar Option	Description
<i>File > Open</i>		Opens the selected file in its associated application at the management console.
<i>File > Open with</i>		Opens the folder with the list of files at the management console. Opens a dialog box that lists the applications, which are installed on the managed workstation. You can choose the application in which the file must open.
<i>File > New Folder</i>		Creates the folder with the specified name.
<i>File > Delete</i>		Deletes the selected files. Deletes the folder if the folder selected from the management console is empty.
<i>File > Rename</i>		Renames the selected file.
<i>File > Properties</i>		Displays the properties of a selected file or folder, such as size of the file and the date and time of last modification.
<i>File > Upload</i>		Moves files from the management console to the managed workstation.
<i>File > Download</i>		Moves files from the managed workstation to the management console.
<i>File > Exit</i>		Closes the File Transfer window.
<i>Edit > Cut</i>		Transfers the selected files to the Clipboard.
<i>Edit > Copy</i>		Copies the selected files to the Clipboard.
<i>Edit > Paste</i>		Pastes the selected files from the Clipboard to the current location.
<i>Edit > Select All</i>		Selects all the files in the current pane.
<i>Edit > Cancel All</i>		Deselects all the files in the current pane.
<i>View Refresh</i>		Updates the display in the Operator Station pane and Target Station pane
<i>Help</i>		Displays help for this window.
Up One Level Folder button		Moves one level up in the directory tree. Right-click the file or folder to view the list of available menu options.
<i>Operator Station Pane</i>		The left pane of the File Transfer window shows the files in the current folder on the management console.
<i>Target Station Pane</i>		The right pane of the File Transfer window shows the files in the current folder on the managed workstation.

70.5 Managing a Remote Wake Up Session

The Remote Wake Up feature supports Magic Packet* technology. When a powered off node that is enabled for Wake on LAN receives the magic packet, the system boots up.

This section provides information on the following topics:

- [Section 70.5.1, “Prerequisites,” on page 844](#)
- [Section 70.5.2, “Remotely Waking Up the Managed Workstations,” on page 844](#)
- [Section 70.5.3, “Setting Up a Scheduled Remote Wake Up Using the Wake-on-LAN Policy,” on page 844](#)
- [Section 70.5.4, “Starting and Stopping the Wake-on-LAN Service,” on page 845](#)

70.5.1 Prerequisites

Before waking up the managed workstations, the following requirements must be fulfilled:

- ☐ Make sure that the managed workstation has a network card that supports Wake on LAN. Additionally, make sure that you have enabled the Wake on LAN option in the BIOS setup of the managed workstation.
- ☐ Make sure that the managed workstation is registered to Novell eDirectory™.
- ☐ Make sure that the remote node is in a soft-off power state. In the soft-off state, the CPU is powered off and a minimal amount of power is utilized by its network interface card. Unlike the hard-off state, in the soft-off state the power connection to the machine remains switched on when the machine is shut down.
- ☐ Make sure that the routers connecting the management console and the remote node are configured to forward subnet-oriented broadcasts

70.5.2 Remotely Waking Up the Managed Workstations

You can perform Remote Wake Up without configuring the Wake-on-LAN policy and service. To perform a Remote Wake Up:

- 1 In Novell ConsoleOne, right-click a managed workstation, a group of managed workstations, a container, or a group of containers.
- 2 Click *Actions > Remote Wake Up*.

70.5.3 Setting Up a Scheduled Remote Wake Up Using the Wake-on-LAN Policy

Remote Management Wake-on-LAN service allows you to wake up a managed workstation or a set of managed workstations automatically by configuring the Wake-on-LAN policy.

To schedule the wake up of a managed workstation or a set of managed workstations automatically through the Wake-on-LAN service, you must perform the following tasks in the order listed:

- [“Configuring the Wake-on-LAN Service Object” on page 845](#)
- [“Configuring the Server Package for the Wake-on-LAN Service” on page 845](#)

Configuring the Wake-on-LAN Service Object

- 1 In ConsoleOne, right-click the Wake-on-LAN service object (WOLService_*servername*), then click *Properties > Look Up Schedule*.
- 2 Modify the schedule to read the Wake-on-LAN policy.
- 3 Click *OK*.

IMPORTANT: If you modify the Wake-on-LAN schedule after starting the Wake-on-LAN service, you need to restart the Wake-on-LAN service. For more information, see [“Starting the Wake-on-LAN Service on NetWare and Windows Servers” on page 845](#).

Configuring the Server Package for the Wake-on-LAN Service

- 1 In the ConsoleOne, right-click the Server package, then click *Properties > Policies > General*.
- 2 Click the *Add* button.
- 3 Select the Wake-on-LAN policy type and enter a name for the Wake-on-LAN policy.
- 4 Select the check box under the *Enabled* column for the Wake-on-LAN policy, then click *Properties > Target List* tab.
- 5 Click *Add*.
- 6 Select the workstations or the workstation container, then click *OK*.
- 7 Click the *Policy Schedule* tab.
- 8 Modify the policy schedule.
- 9 Click *Apply*, then click *Close*.
- 10 Click the *Associations* tab.
- 11 Browse to select the server object or the container where ZENworks 7 Desktop Management is installed, then click *OK*, then click *OK* again.

NOTE: You can create different policies for different target lists.

70.5.4 Starting and Stopping the Wake-on-LAN Service

- [“Starting and Stopping the Wake-on-LAN Services on NetWare and Windows Servers” on page 845](#)
- [“Starting and Stopping the Wake-on-LAN Services on Linux Servers” on page 846](#)

Starting and Stopping the Wake-on-LAN Services on NetWare and Windows Servers

- [“Starting the Wake-on-LAN Service on NetWare and Windows Servers” on page 845](#)
- [“Stopping the Wake-on-LAN Service on NetWare and Windows Servers” on page 846](#)

Starting the Wake-on-LAN Service on NetWare and Windows Servers

To load the Wake-on-LAN service on NetWare server, enter `startwol` at the console prompt.

To start the Wake-on-LAN service on Windows server:

- 1 From the Control Panel, double-click *Administrative Tools*.

- 2 Double-click *Services*.
- 3 Select *Novell ZENworks Wake-on-LAN Service*.
- 4 Click *Start*.

Stopping the Wake-on-LAN Service on NetWare and Windows Servers

To stop the Wake-on-LAN service on NetWare server, enter `stopwol` at the console prompt.

To stop the Wake-on-LAN service on Windows server:

- 1 From the Control Panel, double-click *Administrative Tools*.
- 2 Double-click *Services*.
- 3 Select *Novell ZENworks Wake-on-LAN Service*.
- 4 Click *Stop*.

You can also obtain the information about the Wake-on-LAN operations from the `wolstatus.log` file in the `sys:\` directory on NetWare servers or `ZENworks_installation_path\remmgmt\server\bin\` directory on Windows servers.

Starting and Stopping the Wake-on-LAN Services on Linux Servers

- “Starting the Wake-on-LAN Service on Linux Servers” on page 846
- “Stopping the Wake-on-LAN Service on Linux Servers” on page 846

Starting the Wake-on-LAN Service on Linux Servers

To start the Wake-on-LAN service on Linux server, enter `/etc/init.d novell-zdm-wol start` at the command prompt.

Stopping the Wake-on-LAN Service on Linux Servers

To stop the Wake-on-LAN service on Linux server, enter `/etc/init.d novell-zdm-wol stop` at the command prompt.

You can also obtain the information about the Wake-on-LAN operations from the `novell-zdm-wol.log` file in the `/var/opt/novell/log/zenworks/rm` directory.

70.6 Viewing the Audit Log of Remote Management Sessions Using the Windows Event Viewer

ZENworks 7 Desktop Management records log information on a Windows 2000/XP managed workstation.

To view the audit log of Remote Management sessions:

- 1 Click *Start > Programs > Administrative Tools > Event Viewer*.
- 2 Click *Log > Application*.
- 3 Double-click the event associated with the source Remote Management Agent.

NOTE: To view only the events pertinent to the Remote Management Agent, choose Remote Management Agent from the Source drop-down list in the Filter dialog box.

Desktop Management provides remote diagnostics of workstations. Remote diagnostics displays the event log information of Windows 2000/XP managed workstations. You can also view the audit log for Remote Management using the Event Log window. For more information, see [Section 71.4, “Event Log Information,” on page 861](#).

70.6.1 Understanding the Audit Log

The Windows 2000/XP event logging mechanism allows applications running on the managed workstation to record events as log files. You can use the Event Viewer to view the event logs. The Event Viewer maintains Application, Security, and System log files. The events for Remote Management sessions are stored in the Application log file. The managed workstation where the Remote Management Agent is installed maintains this log information as an audit log. For more information, see [Section 70.6, “Viewing the Audit Log of Remote Management Sessions Using the Windows Event Viewer,” on page 846](#).

The audit log maintains the list of events for each Remote Management session and stores the following details:

- The success or failure of the authentication process
- The start time or end time of Remote Management sessions
- The name of the user attempting to remote manage the workstation
- The domain name and address of the management console accessing the managed workstation
- The remote operation performed on the managed workstation
- The name of the user logged in to the managed workstation
- The event success or failure status, and details for the failure

The following sections contain additional information:

- [“Details of Events in the Audit Log” on page 847](#)
- [“Event Log Messages for Remote Management Sessions” on page 848](#)

Details of Events in the Audit Log

The following table explains the information stored by each event during a Remote Management session:

Table 70-6 *Details of Events in the Audit Log*

Parameter	Description
Date	Date of the event occurrence.
Time	Time stamp of the event occurrence.
Computer	Name of the computer on which the event occurred.
Event ID	Unique ID assigned to the event.

Parameter	Description
Source	The source name for the Remote Management audit log is Remote Management Agent.
Type	The type of the event indicates if the particular event was a success, failure, information, warning, or error.
Category	<p>The category lists the different events for the application. The details of an event are in the detailed message for the event. The events for Remote Management Agent are:</p> <ul style="list-style-type: none"> • Authentication Event • Session Start Event • Session Terminate Event
Operation	<p>The various operations that a management console user can perform on the managed workstation are:</p> <ul style="list-style-type: none"> • Remote Control • Remote View • Remote Diagnostics • File Transfer • Remote Execute <p>All events record the domain name of the remote operator who is remote accessing the managed workstation.</p>
Console Address	IP address of the workstation that the remote operator uses to remote access the managed workstation.
Console DN	Domain name of the workstation that the remote operator uses to remote access the managed workstation.
Local User	Domain name of the user logged in to the managed workstation.
Event Message	The message for the event.

Event Log Messages for Remote Management Sessions

Informational and error messages are recorded for the following events during a Remote Management session:

- [“Authentication Event” on page 848](#)
- [“Session Start Event” on page 849](#)
- [“Session Terminate Event” on page 849](#)

You can view the details of events that occurred during a Remote Management session from the Description box in the Event Detail window. For more information about event details, see [Section 70.6, “Viewing the Audit Log of Remote Management Sessions Using the Windows Event Viewer,” on page 846](#).

Authentication Event

The Authentication event records whether the Remote Management Agent could authenticate the remote user for that operation. The following table describes the Authentication Event messages:

Table 70-7 *Authentication Event Messages*

Type	Message
Success	<ul style="list-style-type: none">• Authentication was successful.• The password is successfully set for this workstation.• The password is successfully reset for this workstation.
Failure	<ul style="list-style-type: none">• Authentication failed.

Session Start Event

The Session Start event records the time when a particular session was started. The following table describes the Session Start Event messages:

Table 70-8 *Session Start Event Messages*

Type	Message
Information	Session started.

Session Terminate Event

The Session Terminate event details the time when the session was disconnected, and the reason for terminating the session. The following table describes the Session Terminate Event messages:

Table 70-9 *Session Terminate Event Messages*

Type	Message
Information	Session terminated normally.

70.7 Remote Operator Identification Display

The Remote Management Agent displays the identification of the remote operator in the following dialog boxes on the managed workstation:

- Permission dialog box
- Visible signal dialog box

The information displayed can be one of the following (listed in the order):

- 1 If the managed workstation is imported to a ZENworks tree, and the remote operator has logged in to the ZENworks tree:
 - If the Fullname attribute of the remote operator's user object has been populated, then the full name of the remote operator is displayed, for example, "Network Administrator." If it has not been populated, then the typeless name of the object is displayed. For example, "user.novell."

- If the Fullname attribute of the remote operator's user object has not been populated, then the typeless name of the remote operator's user object is displayed. For example, user.novell.
- 2 If the managed workstation is not imported to a ZENworks tree, then the *Console_machine_name\console_windows_username* is displayed.

70.8 Managing a Remote Management Audit Session

The Remote Management Auditing mechanism allows you to store information about the Remote Management sessions running on the managed workstations as log files.

The Remote Management Audit session is launched automatically as soon as the management console initiates a Remote Management session with the managed workstation.

The Remote Management sessions are logged as audit records. The managed workstation where the Remote Management Agent is installed logs the audit records into the `auditlog.txt` file. The `auditlog.txt` file is created and updated only when there are no Remote Management sessions in progress. The audit session information is recorded from the fourth line in the `auditlog.txt` file. You can find the `auditlog.txt` file in the system directory of the managed workstation:

The following table explains the information stored by each event during a Remote Management session:

Table 70-10 *Information Stored by Events During a Remote Management Session*

Parameter	Description
Start Time	Start time of the event occurrence.
Duration	Duration of the Remote Management session.
Console DN	Distinguished name of the workstation that the remote operator uses to remote access the managed workstation.
Console user DN	Distinguished name of the remote operator.
Operation Code	The various operations that a management console user can perform on the managed workstation are: <ul style="list-style-type: none"> • Remote Control, indicated by 1 • Remote View, indicated by 2 • File Transfer, indicated by 3 • Remote Execute, indicated by 5 • Remote Diagnostics, indicated by 6
Operation Status	The status of the event indicates if the particular event was a success or failure. 1 indicates that the Remote Management operation was successful and 0 indicates that the Remote Management operation was unsuccessful.

A sample entry is as follows:

```
1005572546000 1000 rajwin2ktestpc admin.novell 1 0
```

All the parameters in an audit record are separated by spaces. Each record is logged in a new line. The `auditlog.txt` file can store a maximum of one hundred records and is saved in the system directory.

70.8.1 Viewing the Audit Logs from a Centralized Database

You can store the audit records of all the managed workstations in a database in a centralized location. To store the `auditlog.txt` files in a database, you must install the Workstation Inventory Agent on every managed workstation. For information on installing the Workstation Inventory Agent, see the *Novell ZENworks 7 Desktop Management Installation Guide*.

The Inventory Scanner collects the audit records and stores them as scan data files in the scan directory at the Inventory server. The Inventory Storer stores the files in the Inventory database.

NOTE: If the Inventory Server rolls up scan data across servers, the audit records are not rolled up after the data stored for the first time.

You can configure the number of audit records per workstation that can be stored in the Inventory database using the RM Audit property page.

To configure the RM Audit property page:

- 1 In ConsoleOne, right-click the Inventory database object, then click *Properties*.
- 2 Click the *RM Audit* tab.
- 3 Specify the maximum number of records per workstation that can be stored in the Inventory database.
- 4 Specify the life span of the audit records.

If the Inventory database has enough space to store new records, the audit records are not deleted from the `auditlog.txt` file even after their expiry time. But if the Inventory database doesn't have enough space to store new records, the oldest audit records are deleted even before their expiry time.

70.9 Generating Remote Management Reports

You can run reports to gather Remote Management information from the Inventory database.

The Remote Management information is taken from the Inventory database you configure.

You can print or export the report as desired. Remember that any reports you generate are empty if you have not configured ZENworks 7 Desktop Management to start populating the Inventory database with the data you want.

This section covers the following sections:

- “Prerequisites for Generating Remote Management Reports” on page 852
- “Generating a Remote Management Report” on page 852
- “Printing a Remote Management Report” on page 853
- “Exporting a Remote Management Report to a File” on page 853

70.9.1 Prerequisites for Generating Remote Management Reports

Before running the inventory reports you must perform the following tasks:

- Configure the Inventory database. For more information, see [Section 77.1.1, “Configuring the Inventory Database,” on page 1096](#).

The Remote Management reports always use the Inventory database you configured as the data source for your reports unless you change it later as described in [Section 77.1.1, “Configuring the Inventory Database,” on page 1096](#).

- Before running the inventory reports you must make sure that the appropriate ODBC client for Sybase, Oracle, or MS SQL is installed on the machine running ConsoleOne. The ODBC driver is automatically configured on the machine when you invoke the Inventory report. For more information on how to configure the ODBC client, see “[Installing the ODBC Drivers](#)” in “[Post-Installation](#)” in the *Novell ZENworks 7 Desktop Management Installation Guide*.

70.9.2 Generating a Remote Management Report

- 1 In ConsoleOne, configure the database through *Tools > ZENworks Inventory > Configure DB*.
- 2 Click *Tools > ZENworks Reports*.
- 3 From the Available Reports list, double-click *RM Audit Reports*, then click *Remote Management Report*.

The description for the report is displayed on the right side of the screen.

- 4 Specify the selection criteria.

Date of Operation: Specify a date when the Remote Management operation occurred. All the records of the Remote Management operation subsequent to the specified date are listed.

Console DN: Specify the Distinguished Name (DN) of the workstation that the remote operator uses to remote access the managed workstation.

Console User DN: Specify the DN of the remote operator.

Target Workstation DN: Specify the DN of the managed workstation.

Operation: Select the Remote Management operation for which you want to generate the report.

Operation Status: Select the status of the selected Remote Management operation.

In the Reporting dialog box, you can use an asterisk (*) as a wildcard. The wildcard character can be used for character data only.

The following table lists examples of wildcards.

Example	Specifies to Include
*	All items
wNT*	All items starting with “wNT”
wNTcpq.xcorp	The single named item, in this case a workstation

- 5 Click *Run Selected Report*.

A status box appears displaying the progress of the report generation. When the report is generated, it appears in the viewer. Use the buttons on the toolbar to page through, print, or export the report.

70.9.3 Printing a Remote Management Report

- 1 Generate and view the report.
- 2 To change the default settings of the Printer, click the *Printer Setup* icon and modify the settings.
- 3 Click the *Printer* icon.

70.9.4 Exporting a Remote Management Report to a File

- 1 Generate and view the report.
- 2 On the toolbar, click the *Export Report* icon.
- 3 In the dialog box, specify the location and file format, then click *OK*.
- 4 Browse for and select the directory where you want to save the exported file.
- 5 Click *OK*.

70.10 Improving the Remote Management Performance

The Remote Management performance, especially over a slow link, has been enhanced through using improved compression.

The performance during a Remote Management session over a slow link or a fast link varies depending on the network traffic. For better response time, try one or more of the following strategies:

On the Management Console

- Select the *Hide Wallpaper* option on the managed workstation in the Control Parameters dialog box.
- Assign color settings on the management console higher than the managed workstation or assign the same color settings for the management console and the managed workstation.
- Select *16 Colors* or *256 Colors* mode in the Control Parameters dialog box to enhance the Remote Management performance.
- The speed of the management console depends upon the processing power of the client machine. We recommended that you to use single-processor client with a Pentium III, 500MHz (or later).

On the Managed Workstation

- Deselect the *Enable Pointer Shadow* option before starting the Remote Control or Remote View session.

To disable *Enable Pointer Shadow*:

1. From the Windows desktop, click *Start*, click *Settings*, click *Control Panel*, then double-click *Mouse*.
 2. Click *Pointers*.
 3. Deselect *Enable Pointer Shadow*.
 4. Click *Apply*, then click *OK*.
- At the managed workstation, use a plain background. Do not set a wallpaper pattern.
 - If the Task manager is opened at the target machine, you should minimize it or close it if possible.
 - Make sure that the scrolling texts (such as the debug windows) and animations are not active on the managed workstation.
 - Make sure to minimize or close the dialog boxes that are not in use.
 - To perform any operations at the managed workstation, if possible, use the toolbar options instead of menu options.
 - To maximize the Remote Management performance over WAN, configure the following settings in the Control Parameters dialog box at the managed workstation:
 - Set the color mode of the managed workstation to 16 Color.
 - Select the *Slow Link* option.

70.11 Using the Remote Management Agents

You can access and remote control the managed workstations if you have installed the Remote Management Agent on the managed workstations.

The following sections explain how you can use the Remote Management Agent during remote sessions:

- “Shutting Down the Remote Management Agent” on page 854
- “Restarting the Remote Management Agent” on page 855
- Section 70.11.3, “Using the Remote Management Agent Icon,” on page 855

70.11.1 Shutting Down the Remote Management Agent

You can shut down the Remote Management Agent during a remote session. When you shut down the Remote Management Agent, the remote session stops. To start another remote session, you need to reload the Remote Management Agent. For more information, see “Restarting the Remote Management Agent” on page 855.

To shut down the Remote Management Agent on a Windows 2000/XP managed workstation:

- 1 From the Control Panel, double-click *Administrative Tools*.
- 2 Double-click *Services*.
- 3 Select *Novell ZENworks Remote Management* service.
- 4 Click *Stop*.

To shut down the Remote Management Agent on a Windows 98 managed workstation:

- 1 Right-click the *Remote Management Agent* icon in the system tray.

- 2 Click *Shutdown Agent*.

IMPORTANT: You can stop the Remote Management Agent on Windows 2000/XP workstation only if you have the rights to stop the Windows service.

70.11.2 Restarting the Remote Management Agent

During the ZENworks 7 Desktop Management installation, the Remote Management Agent is installed on the managed workstation and started automatically when the managed workstation starts up. If you shut down the Remote Management Agent during a remote session, the remote session stops. To start another remote session, you need to restart the Remote Management Agent on the managed workstation.

To restart the Remote Management Agent on a Windows 2000/XP managed workstation:

- 1 From the Control Panel, double-click *Administrative Tools*.
- 2 Double-click *Services*.
- 3 Select *Novell ZENworks Remote Management* service.
- 4 Click *Start*.

To restart the Remote Management Agent on a Windows 98 managed workstation:

- 1 Go to the
`ZENworks_agent_installation_directory\remotemanagement\rmagent`
directory.
- 2 Double-click `zenrem32.exe`.

IMPORTANT: You can start the Remote Management Agent on Windows 2000/XP workstation only if you have the rights to start the Windows service.

70.11.3 Using the Remote Management Agent Icon

By default, the *Remote Management Agent* icon is displayed in the system tray of the managed workstations. This icon indicates that the Remote Management Agent is loaded on the managed workstation.

If the Remote Management Agent is loaded and the *Remote Management Agent* icon is not displayed in the system tray, it indicates that you have disabled the display option in the Remote Control Policy settings.

The user at the managed workstation can right-click the *Remote Management Agent* icon and choose from the following options:

Table 70-11 *Remote Management Agent Options*

Option	Description
<i>Terminate RC/RV Session</i>	Disconnects and closes the remote session on the managed workstation and displays a message on the management console indicating that the remote session is closed.

Option	Description
<i>Security</i>	Allows the user at the managed workstation to set or clear the password for the workstation
<i>Information</i>	<p>Displays information such as who is accessing the managed workstation for the remote session, security settings, and the protocol in use for the remote session.</p> <p>For details, see “Obtaining Information About Remote Management Sessions” on page 841.</p> <p>You can right-click or double-click the Remote Management Agent icon to view the Information window.</p>
<i>Shutdown Agent</i>	Allows the user logged into the Windows 98 managed workstation to shutdown the Remote Management Agent. This option is not applicable for Windows 2000/XP managed workstations. To shut down the Remote Management Agent on Windows 2000/XP managed workstations, the user must go to the Service Control Panel and stop the “Novell ZENworks Remote Management” service.
<i>Request Session</i>	Enables the user at the managed workstation to request a remote operator to perform remote session.
<i>Help</i>	Displays the Remote Management Agent help.

Viewing the Diagnostic Information

71

You can diagnose the managed workstation and obtain information to help you analyze problems at the managed workstation.

You can view real-time managed workstation diagnostic information from the management console. For more information, see [Section 71.1, “Viewing Diagnostic Information for a Managed Workstation,” on page 858](#).

Before you begin to obtain the diagnostic information, make sure that the Remote Management Agent is installed on the managed workstation. During the Remote Management Agent installation, the Diagnostic Agent is also installed on the managed workstation, which runs automatically when the managed workstation boots up. When the management console user requests diagnostic information from the managed workstation, the Diagnostic Agent on the managed workstation procures the requested information and provides it to the Remote Management Agent, which then makes it available to the management console.

- [Section 71.1, “Viewing Diagnostic Information for a Managed Workstation,” on page 858](#)
- [Section 71.2, “Windows Memory Information,” on page 860](#)
- [Section 71.3, “Environment Information,” on page 860](#)
- [Section 71.4, “Event Log Information,” on page 861](#)
- [Section 71.5, “Device Drivers Information,” on page 862](#)
- [Section 71.6, “Services Information,” on page 862](#)
- [Section 71.7, “WIN32 Process Information,” on page 862](#)
- [Section 71.8, “WIN32 Modules Information,” on page 863](#)
- [Section 71.9, “NetWare Connections Information,” on page 863](#)
- [Section 71.10, “Novell Client Information,” on page 864](#)
- [Section 71.11, “Network Protocols Information,” on page 864](#)
- [Section 71.12, “Name Space Providers Information,” on page 865](#)
- [Section 71.13, “Network Drives Information,” on page 865](#)
- [Section 71.14, “Network Open Files Information,” on page 866](#)
- [Section 71.15, “Print Capture Information,” on page 867](#)

71.1 Viewing Diagnostic Information for a Managed Workstation

You can view diagnostic information that helps you analyze problems at the managed workstation.

IMPORTANT: If you have not installed the Novell® Client™ on the managed workstation, you cannot view the information about NetWare Connections, Novell Client, Network Drives, Network Open files, and Print Capture.

To view diagnostic information:

- 1 Right-click the managed workstation from the management console.
- 2 Click *Actions > Diagnostics*.

The following table explains the steps you need to take to view various diagnostic windows.

Table 71-1 *Diagnostic Information*

Window Name	Instructions for Viewing
Windows Memory	Expand the <i>Diagnostics</i> folder > <i>Operating System</i> folder > <i>Memory</i> folder, then click <i>Windows Memory</i> . For more information, see Section 71.2, "Windows Memory Information," on page 860 .
Environment	Expand the <i>Diagnostics</i> folder > <i>Operating System</i> folder, then click <i>Environment</i> . For more information, see Section 71.3, "Environment Information," on page 860 .
Event Log	Expand the <i>Diagnostics</i> folder > <i>Operating System</i> folder, then click <i>Event Log > Security, System, or Application</i> . Click an event row in the Event Log table to view a description of the event. For more information, see Section 71.4, "Event Log Information," on page 861 .
Device Drivers	Expand the <i>Diagnostics</i> folder > <i>Operating System</i> folder, then click <i>Device Drivers</i> . For more information, see Section 71.5, "Device Drivers Information," on page 862 .
Services	Expand the <i>Diagnostics</i> folder > <i>Operating System</i> folder, then click <i>Services</i> . For more information, see Section 71.6, "Services Information," on page 862 .
WIN32 Processes	Expand the <i>Diagnostics</i> folder > <i>Operating System</i> folder, then click <i>WIN32 Processes</i> . For more information, see Section 71.7, "WIN32 Process Information," on page 862 .

Window Name	Instructions for Viewing
WIN32 Modules	<p>Expand the <i>Diagnostics</i> folder > <i>Operating System</i> folder, then click <i>WIN32 Modules</i>.</p> <p>For more information, see Section 71.8, “WIN32 Modules Information,” on page 863.</p>
NetWare Connections	<p>Expand the <i>Diagnostics</i> folder > <i>Network</i> folder, then click <i>NetWare Connections</i>.</p> <p>For more information, see Section 71.9, “NetWare Connections Information,” on page 863.</p>
Novell Client	<p>Expand the <i>Diagnostics</i> folder > <i>Network</i> folder, then click <i>Novell Client</i>.</p> <p>For more information, see Section 71.10, “Novell Client Information,” on page 864.</p>
Network Protocols	<p>Expand the <i>Diagnostics</i> folder > <i>Network</i> folder, then click <i>Network Protocols</i>.</p> <p>For more information, see Section 71.11, “Network Protocols Information,” on page 864.</p>
Name Space Providers	<p>Expand the <i>Diagnostics</i> folder > <i>Network</i> folder, then click <i>Name Space Providers</i>.</p> <p>For more information, see Section 71.12, “Name Space Providers Information,” on page 865.</p>
Network Drives	<p>Expand the <i>Diagnostics</i> folder > <i>Network</i> folder, then click <i>Network Drives</i>.</p> <p>For more information, see Section 71.13, “Network Drives Information,” on page 865.</p>
Network Open Files	<p>Expand the <i>Diagnostics</i> folder > <i>Network</i> folder, then click <i>Network Open Files</i>.</p> <p>For more information, see Section 71.14, “Network Open Files Information,” on page 866.</p>
Print Capture	<p>Expand the <i>Diagnostics</i> folder > <i>Network</i> folder, then click <i>Print Capture</i>.</p> <p>For more information, see Section 71.15, “Print Capture Information,” on page 867.</p>

You can use the *Edit* menu options to copy all or selected diagnostic information from the diagnostics window to a text editor for later analysis.

71.2 Windows Memory Information

On Windows 2000/XP managed workstations, the Windows Memory window displays the percentage of memory in use, physical memory, paging details, and free space details.

The following table describes the fields in the Windows Memory window:

Table 71-2 *Windows Memory Information*

Field	Description
<i>Memory Load (%)</i>	Percentage of memory utilization. Zero percentage memory indicates memory usage is nil; 100% indicates that all the available memory is in use.
<i>Total Physical Memory (MB)</i>	Total physical memory in MB.
<i>Free Physical Memory (MB)</i>	Amount of available physical memory in MB.
<i>Total Paging File Size (MB)</i>	Total number of MB that can be stored in the paging file. This number does not indicate the actual physical size of the paging file on the managed workstation.
<i>Free Space in Paging File (MB)</i>	Number of MB available in the paging file.
<i>Total Address Space (MB)</i>	Total number of MB described in the user mode portion of the virtual address space of the calling process.
<i>Free User Bytes (MB)</i>	Number of MB in unreserved and uncommitted memory of the user address space of the calling process.

71.3 Environment Information

The Environment window displays the variables set at the managed workstation. You can view the Environment information on Windows 2000/XP managed workstations.

The following table describes the fields in the Environment window:

Table 71-3 *Environment Information*

Field	Description
<i>Variables</i>	Environment variable name.
<i>Value</i>	Value of the variable or the path.

71.4 Event Log Information

Event logging in Windows 2000/XP provides a standard, centralized way for applications and the operating system to record important software and hardware events. Event logging provides a means to merge events from various sources into a single informative story. The event log diagnostics help the remote operator view the System, Security, and Application event logs. You can view the Event Log Information on Windows 2000/XP managed workstations.

The following table describes the fields in the Event Log window:

Table 71-4 *Event Log Information*

Field	Description
<i>Event Generated Date</i>	Date when the entry was submitted (MM/DD/YYYY).
<i>Event Generated Time</i>	Time when the entry was submitted (HH:MM:SS).
<i>Event ID</i>	Identifies the event specific to the source that generated the event log entry.
<i>Event Generated Type</i>	Classification of the type as Error, Warning, Information, Success, or Failure.
<i>Event Generated Category</i>	<p>Subcategory for the event. This subcategory is source specific.</p> <hr/> <p>NOTE: Every application registering for a Windows Event log needs to specify a message resource file for Event Category. Event Category is application specific and is defined in the message file. Diagnostics reads this information from HKLM\system\CurrentControlSet\Services\EventLog\<application>, maps the category to message and fetches the category.</p> <p>Some applications do not specify a message resource file for Event Description and Event Category. In this case, Windows assigns arbitrary numbers for the event category. Also, there is no way to get this arbitrary number (because it is not stored in the registry). The Diagnostics reports it as None.</p> <hr/>
<i>Source Name</i>	Name of the source (application, service, driver, subsystem) that generated the entry.
<i>Description</i>	Details of the event.
<i>Computer Name</i>	Name of the computer that generated the event.

71.5 Device Drivers Information

The Device Drivers window displays information about the device drivers installed on Windows 2000/XP managed workstations. You can use the information in this window to determine whether the workstation has the required drivers loaded and their status.

The following table describes the fields in the Device Driver window for Windows 2000/XP managed workstations:

Table 71-5 *Device Drivers Information*

Field	Description
<i>Name</i>	Name of the device driver.
<i>State</i>	Indicates if the device driver is Stopped or Running.

71.6 Services Information

The Services window indicates which services are available on Windows 2000/XP managed workstations, and lists the state of each service.

The following table describes the fields in the Services window:

Table 71-6 *Services Information*

Item	Description
<i>Service Name</i>	List of services available on the workstation.
<i>State</i>	Indicates if the service is Stopped or Running.

71.7 WIN32 Process Information

Diagnostic information about processes is available on Windows 98 managed workstations.

To view the WIN32 modules associated for a particular Windows 32-bit process, double-click the row entry in the WIN32 Processes window.

The following table describes the fields in the WIN32 Processes window:

Table 71-7 *Win32 Process Information*

Field	Description
<i>Path</i>	Path and filename of the executable file for the process.
<i>PID</i>	Processor identifier.
<i>PPID</i>	Parent processor identifier.
<i>No. of threads</i>	Number of execution threads started by the process.

Field	Description
<i>Usage Count</i>	Number of references to the process. A process exists as long as its usage count is non-zero. When the usage count becomes zero, the process terminates.

71.8 WIN32 Modules Information

The WIN32 Modules window displays the list of modules associated with a specified process on Windows 98 managed workstations.

The following table describes the fields in the WIN32 Modules window:

Table 71-8 *Win32 Modules Information*

Field	Description
<i>Module ID</i>	Module identifier in the context of the owning process.
<i>Global Usage Count</i>	Global usage count on the module.
<i>Process Usage Count</i>	Module usage count in the context of the owning process.
<i>Module Path</i>	Location of the module.
<i>Module Size (KB)</i>	Size of the module in KB.

71.9 NetWare Connections Information

The NetWare Connections window displays information about all current connections for the Novell Client. It also indicates the current server and current tree.

The following table describes the fields in NetWare Connections window:

Table 71-9 *NetWare Connections Information*

Field	Description
<i>Server Name</i>	Names of the servers and trees the workstation is connected to.
<i>User Name</i>	Username for each connection.
<i>Connection Number</i>	User's connection number on the server.
<i>Authentication State</i>	Connections are either NDS [®] or bindery connection.
<i>NDS Tree</i>	NDS Directory tree for each connection to a server that is running NetWare [®] 4 or later.
<i>Transport Type</i>	The transit protocol in use between the server and the workstation.
<i>Address</i>	The internal address of the server.
<i>Resource Type</i>	Identifies the primary server.

71.10 Novell Client Information

The Novell Client window displays the information about the installed Novell Client and its settings.

The following table describes the fields in the Novell Client window:

Table 71-10 *Novell Client Information*

Field	Description
<i>Preferred Server</i>	NetWare server that is used for NDS authentication of the user when the Novell Client for Windows workstation software is started.
<i>Preferred Tree</i>	Directory tree that the client first attaches to when the Novell Client for Windows software is started.
<i>Name Context</i>	The current position or context in the NDS tree structure. This setting is applicable only to client workstations connecting to a NetWare 4 or NetWare 5 network.
<i>First Network Drive</i>	Network drive that is selected when you connect to a NetWare server.
<i>Client Version</i>	Novell Client32™ version number.

71.11 Network Protocols Information

The Network Protocols window displays the information about the active network protocols on a managed workstation using WinSock. The WinSock architecture also allows for simultaneous access to multiple transport protocols. WinSock contains the Windows Open System Architecture (WOSA) compliant architecture, which allows applications to access protocols including TCP/IP.

The following table describes the fields in the Network Protocols window:

Table 71-11 *Network Protocols Information*

Field	Description
<i>Properties</i>	Specifies characteristics of the protocol.
<i>Address Family</i>	Defines the structure of protocol addresses that are in use by the protocol.
<i>Socket Type</i>	Represents the different socket types for the BSD socket interface. It can have the following values: <ul style="list-style-type: none">• Stream• Datagram• Raw Socket• Seq. Packet• RDM Socket• Unknown
<i>Protocol ID</i>	Protocols identifier.

Field	Description
<i>Message Size (Bytes)</i>	Specifies the maximum message size (in bytes) supported by the protocol. This is the maximum size of a message that can be sent from or received by the host. For protocols that do not support message framing, the actual maximum size of a message that can be sent to a given address might be less than this value. If the protocol is stream-oriented, the concept of message size is not relevant. If the protocol is message-oriented, there is no maximum message size.
<i>Protocol Name</i>	Name of the protocol that is supported, such as TCP/IP, UDP/IP, or IPX™.

71.12 Name Space Providers Information

The Name Space Providers window displays information about the name space provider registered with WinSock Name Resolution and Registration APIs. WinSock 2 includes a new set of API functions that standardize how the applications access and use the various network naming services. This information is not displayed for workstations with WinSock 1.1.

The following table describes the fields in the Name Space Providers Information window:

Table 71-12 *Name Space Provides Information*

Field	Description
<i>Name space</i>	Specifies the name space (SAP, DNS, SLP).
<i>Connected</i>	Displays whether the name space provider is enabled on the workstation.
<i>Version</i>	The name space version identifier.
<i>Service Provider</i>	Displays the string for the name space provider.

71.13 Network Drives Information

The Network Drives window displays information about mapped drives, drive capacity, volume label, file system information, sector size, and cluster size. The following table describes the fields in the Network Drives window:

Table 71-13 *Network Drives Information*

Field	Description
<i>Drive Letter</i>	Mapped drive letter.
<i>Path</i>	NetWare path of the volume or directory to which the drive is mapped. For example, if the <code>zenworks</code> directory on the <code>sys:</code> volume of server <code>zen_kyoto</code> is mapped to drive Q, the path displays <code>zen_kyoto\sys:zenworks</code> .
<i>File System</i>	File system type for the mapped NetWare directory or volume.

Field	Description
<i>Effective Rights</i>	<ul style="list-style-type: none"> • Read For a folder, grants the right to open files in the folder and read the contents or run the programs. For a file, grants the right to open and read the file. • Write For a folder, grants the right to open and change the contents of files in the folder. For a file, grants the right to open and write to the file. • Create For a folder, grants the right to create new files and folders in the folder. For a file, grants the right to create a file and to salvage a file after it has been deleted. • Delete Grants the right to delete the folder or file. • Modify Grants the right to change the attributes or name of the folder or file, but does not grant the right to change its contents. Changing the contents requires the Write right. • File Scan Grants the rights to see the folder or file with the DIR or NDIR command. • Ownership Grants the ownership rights of the file, folder, or volume. If the corresponding rights are not given to the user, Effective Rights displays a hyphen (-).
<i>Long Name Size (Bytes)</i>	Maximum length in characters of a filename component supported by the specified file system. For example, for a FAT file system supporting long names, the value is 255. The value for a DOS file system is 11.
<i>Sector Size (Bytes)</i>	Sector size in bytes.
<i>Sectors Per Cluster</i>	Number of sectors per cluster.
<i>Total Clusters</i>	Size of the volume in clusters.
<i>Free Clusters</i>	Number of clusters currently free for allocation. This number includes the space that is reclaimed from the sub-allocation file system and also clusters freed from deleted files.

71.14 Network Open Files Information

The Open Files window displays the names of files open on a NetWare server corresponding to the connection ID from the mapped drives of managed workstation.

The following table describes the fields in the Network Open Files window:

Table 71-14 *Network Open Files Information*

Field	Description
<i>File Name</i>	Name of the file.

Field	Description
<i>Volume Name</i>	Name of the volume.
<i>Server Name</i>	Name of the file server.
<i>User</i>	The NetWare name under which the user's workstation is logged in to the file server.
<i>Connection ID</i>	Connection ID on which the file is opened.

71.15 Print Capture Information

The Print Capture window displays information about the captured queues, print options for each parallel port on the managed workstation, and current status of each port.

The following table describes the fields in the Print Capture window:

Table 71-15 *Print Capture Information*

Field	Description
<i>Printer Device Name</i>	LPT device. Number of LPT ports for which captures can be managed.
<i>Port State</i>	Specifies whether the LPT device is captured.
<i>Captured Queues</i>	Captured print queue name.

Documentation Updates



This section contains information on documentation content changes that have been made in the *Administration* guide for Remote Management since the initial release of Novell® ZENworks® 7 Desktop Management. The information will help you to keep current on updates to the documentation.

All changes that are noted in this section were also made in the documentation. The documentation is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the documentation changes listed in this section.

The documentation update information is grouped according to the date the changes were published. Within a dated section, the changes are alphabetically listed by the names of the main table of contents sections for Remote Management.

If you need to know whether a copy of the PDF documentation you are using is the most recent, the PDF document contains the date it was published on the front title page.

The documentation was updated on the following date:

- [Section L.1, “July 14, 2006 \(Support Pack 1\),” on page 869](#)
- [Section L.2, “December 9, 2005,” on page 870](#)

L.1 July 14, 2006 (Support Pack 1)

The following changes were made to this guide with the release of Support Pack 1:

- The following note was added to each section of the guide:

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

Other updates were made to the following sections. The changes are explained below.

- [Section L.1.1, “Setting Up Remote Management,” on page 869](#)

L.1.1 Setting Up Remote Management

The following changes were made in this section:

Location	Change
Section 69.9.3, “Customizing the Permission Message,” on page 831	Added this section for Support Pack 1.

L.2 December 9, 2005

Page design of the entire guide was reformatted to comply with revised Novell documentation standards.

Workstation Inventory

VIII

The Workstation Inventory component of Novell® ZENworks® 7 Desktop Management enables you to collect hardware and software inventory information from local and remote workstations of your enterprise. This inventory information is scanned and stored in a database that can be accessed by the ZENworks administrator.

From Novell ConsoleOne®, you can view the complete hardware and software inventory of the servers. You can also query the centralized database of the servers.

The following sections provide information on the features and tasks of Workstation Inventory:

- [Chapter 72, “Understanding Workstation Inventory,” on page 873](#)
- [Chapter 73, “Setting Up Workstation Inventory,” on page 887](#)
- [Chapter 74, “Understanding Workstation Inventory Components,” on page 965](#)
- [Chapter 75, “Understanding the Inventory Database Schema,” on page 987](#)
- [Chapter 76, “Managing Your Inventory System,” on page 1021](#)
- [Chapter 77, “Viewing Inventory Information,” on page 1095](#)
- [Chapter 78, “Monitoring Workstation Inventory Using Status Logs,” on page 1177](#)
- [Appendix M, “Performance Tips,” on page 1185](#)
- [Appendix N, “Hardware Information Collected by the Inventory Scanners,” on page 1199](#)
- [Appendix O, “ZENworks 7 Desktop Management Inventory Attributes,” on page 1211](#)
- [Appendix P, “Enumeration Values,” on page 1237](#)
- [Appendix Q, “Documentation Updates,” on page 1247](#)

Understanding Workstation Inventory

72

The Workstation Inventory component of Novell® ZENworks® 7 Desktop Management gathers hardware and software inventory information from the workstations in your enterprise. ZENworks 7 Desktop Management collects, stores, and reports inventory information of the workstations on your network.

The inventory information can be useful to help you make business decisions on how to manage workstations. The following are some of the business decisions that you can make once you have obtained the inventory information:

- Workstations that need new applications
- Workstations that need updated hardware and drivers
- Workstations that should receive an application object
- Workstations that conform to the corporate hardware and software standard

This section provides a basic overview of ZENworks 7 Desktop Management Workstation Inventory. It contains the following information:

- [Section 72.1, “Workstation Inventory Terminology,” on page 873](#)
- [Section 72.2, “Overview of Inventory Components,” on page 874](#)
- [Section 72.3, “Understanding Inventory Scanning Cycle,” on page 876](#)
- [Section 72.4, “Understanding the Inventory Server Roles,” on page 876](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

72.1 Workstation Inventory Terminology

The following brief glossary provides basic definitions of Workstation Inventory terms:

Inventoried workstation: A Windows workstation whose hardware and software information you want to scan and maintain in a central repository. To gather complete hardware and software inventory for a workstation, you must install the Inventory Agent (ZENworks 7 Desktop Management Agent) on that workstation.

Inventory server: A NetWare®, Linux, or Windows ZENworks 7 Desktop Management server where you run the Inventory service. This server can also run any other ZENworks 7 Desktop Management services. The Inventory server collects the inventory information from associated inventoried workstations and stores it into the Inventory database.

Inventory database: A repository of inventory information of all the inventoried workstations.

Database server: A server running Sybase, Oracle*, or MS SQL where your Inventory database is mounted. The database can run on an Inventory server or on a different server.

Management console: A Windows workstation or server running Novell ConsoleOne® with ZENworks 7 Desktop Management Workstation Inventory ConsoleOne snap-ins installed. The management console provides the interface to administer the inventory system.

eDirectory Tree: The Novell eDirectory™ tree with eDirectory objects such as multiple levels of organizational units, users, groups, and other network resources. This hierarchical structure is referred to as the eDirectory tree in this document. For more information, see the [Novell eDirectory documentation Web site \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Inventory Tree: A logical tree depicting the transmission of the inventory information from the inventoried workstations and the Inventory servers to the centralized enterprise Inventory database.

Standalone Server: An Inventory server that has an Inventory database and inventoried workstations attached to it.

Leaf Server: The lowest-level Inventory server in the inventory tree hierarchy. This server has one or more inventoried workstations attached to it and can have an Inventory database attached to it. This Inventory server collects the inventory information from the inventoried workstations attached to it and moves the information to the next-level Inventory server.

Intermediate Server: The Inventory server for moving the information from the lower-level Inventory servers up the Inventory server hierarchy. This server can have either inventoried workstations or an Inventory database, or both attached to it.

Root Server: The highest-level Inventory server in the inventory tree hierarchy. This server has the Inventory database that contains the inventory information of all the lower-level Inventory servers. At the Root Server level, you can view complete inventory information for the entire enterprise. This server can have inventoried workstations attached to it.

Site: A site is typically a geographical location. There can be multiple sites in your enterprise.

Software Dictionary or Dictionary: The Software Dictionary contains a list of software identifiers and rules. Each software identifier identifies a particular software installed on an inventoried workstation.

Software Identifiers: An entry that identifies an item of software is called as a software identifier. Each software identifier has a set of file matching attributes and corresponding software information attributes. During the Inventory scan, the scanner reads the attributes from the file headers, and if these attributes match the attributes configured in the dictionary, the information in the corresponding software information attributes is stored in the Inventory database.

Software Dictionary Rule: A software dictionary rule represents a set of conditions that control the scope of scanning process.

Unidentified Software: The software dictionary might not identify all the software products installed in your network. The software not listed in the dictionary is called Unidentified software.

72.2 Overview of Inventory Components

Before setting up Workstation Inventory, you should understand the inventory components, which interact together to perform inventory functions.

The following sections provide a brief overview of the Workstation Inventory components:

- “Inventory Scanners” on page 875

- [“Inventory Components on Servers” on page 875](#)
- [“Inventory Database” on page 876](#)
- [“Management Console” on page 876](#)

72.2.1 Inventory Scanners

Platform-dependent scanners determine the hardware and software configurations of workstations. These Inventory scanners are located at the inventoried workstations. When executed on the inventoried workstations, the scanner collects the inventory information for the inventoried workstations. The inventory information is subsequently transferred to the Inventory server and processed.

Using the Workstation Inventory policy, you can configure the scan settings for scheduling the scan on the workstations and customize hardware scanning. From the Inventory Service object (Inventory Service_*server_name*), you can specify the location of the inventory information and also customize software scanning using the Software Dictionary snap-ins.

For more information about the Inventory scanner, see [Section 74.3, “Understanding the Inventory Scanner,” on page 968](#).

72.2.2 Inventory Components on Servers

The Inventory server components process the inventory information. The following components are Java programs that work identically on Inventory servers:

- Selector

The Selector processes the inventory information and places the information in appropriate directories. For more information, see [Section 74.6, “Understanding the Selector,” on page 979](#).

- Sender and Receiver

The Sender on the Inventory server compresses the inventory information and then transfers it from the lower-level Inventory server to the Receiver on the higher-level Inventory servers. By using the Roll-Up policy, you can configure the next level destination Inventory server for roll-up, and also schedule the roll-up time. For more information, see [Section 74.4, “Understanding the Sender and Receiver,” on page 974](#).

- Storer

The Storer stores the collected inventory information in the Inventory database. By using the Database Location policy, you can configure the properties of the Inventory Database object (Inventory database_*server_name*) and associate the database object to an Inventory server. For more information, see [Section 74.7, “Understanding the Storer,” on page 981](#).

- STR Converter

The STR Converter converts the ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management inventory information to the format required by ZENworks 7 Desktop Management. For more information about the STR Converter, see [Section 74.8, “Understanding the Str Converter,” on page 981](#).

- TCP Receiver

The TCP Receiver receives the roll-up inventory information from the ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management Inventory servers connected to it and converts the

information to a format required by ZENworks 7 Desktop Management. For more information, see [Section 74.5, “Understanding the TCP Receiver,” on page 978](#).

- Dictionary Provider and Dictionary Consumer

All Inventory servers run the Dictionary Provider and Dictionary Consumer services. The Dictionary Consumer downloads the dictionary updates from the Dictionary Provider. For more information, see [Section 74.10, “Understanding Dictionary Provider and Dictionary Consumer,” on page 983](#).

72.2.3 Inventory Database

The Inventory database is a repository of inventory information of the inventoried workstations. In Desktop Management, the database is a Common Information Model-based database and is implemented in Relational Database Management System (RDBMS). It is maintained in Sybase, Oracle, or MS SQL. For more information, see [Section 73.2, “Setting Up the Inventory Database,” on page 929](#).

72.2.4 Management Console

The management console is the Novell ConsoleOne. This is a Java-based console that includes snap-ins for Workstation Inventory management operations.

72.3 Understanding Inventory Scanning Cycle

The Inventory scanning cycle is as follows:

1. The Inventory scanner checks whether an updated dictionary is available at its Inventory server and downloads the updated dictionary.
2. The Inventory scanner sends hardware and software information from the inventoried workstations to the Inventory server as per the scan schedule.
3. The Inventory server stores the inventory information in the Inventory database.
4. At the management console, you can view and retrieve the inventory information from the Inventory database using Inventory tools such as Reporting, Summary, etc.

72.4 Understanding the Inventory Server Roles

This section describes the following roles that you assign for an Inventory server:

- [“Root Server” on page 877](#)
- [“Root Server with Inventoried Workstations” on page 878](#)
- [“Intermediate Server” on page 878](#)
- [“Intermediate Server with Database” on page 879](#)
- [“Intermediate Server with Inventoried Workstations” on page 880](#)
- [“Intermediate Server with Database and Inventoried Workstations” on page 881](#)
- [“Leaf Server” on page 882](#)
- [“Leaf Server with Database” on page 883](#)
- [“Standalone Server” on page 884](#)

For a quick reference table of the Inventory Server roles, see [Section 72.4.10, “Quick Reference Table of the Inventory Server Roles,”](#) on page 885.

72.4.1 Root Server

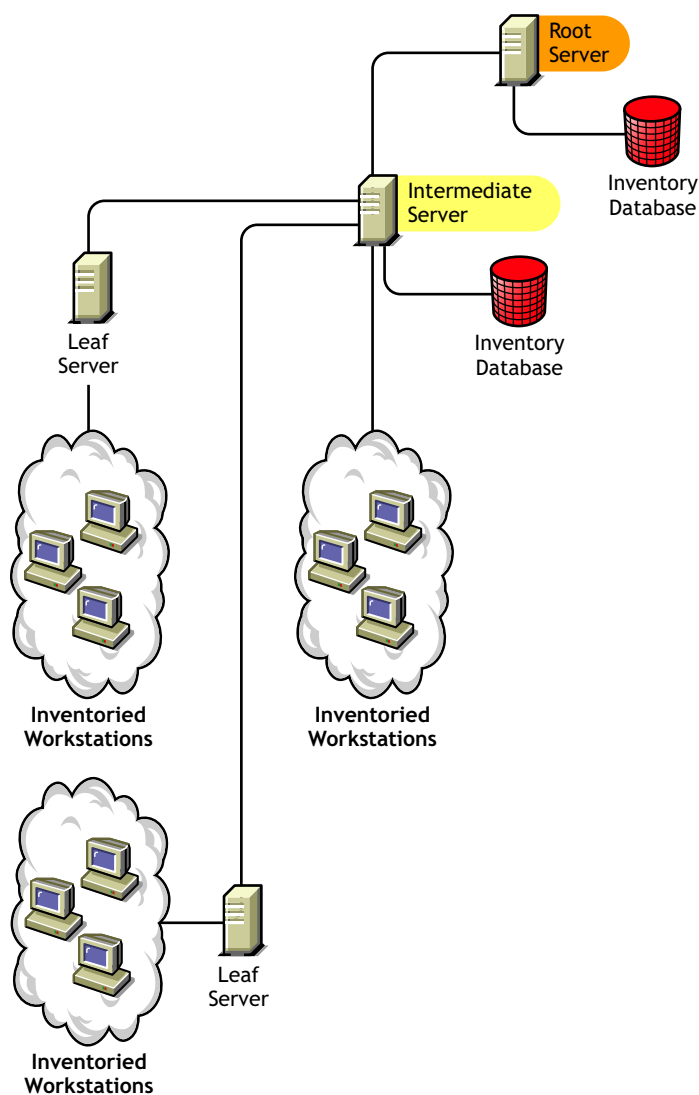
The Root Server has the following characteristics:

- This server is the topmost Inventory server in the inventory tree hierarchy.
- This server has an Inventory database attached to it.

Choose Root Server to store the inventory information for your enterprise in a centralized database. The Inventory database at the Root Server contains the inventory information for all lower-level Inventory servers.

The following illustration depicts Leaf Servers connected to the Intermediate Server with Database. The Intermediate Server is attached to the Root Server.

Figure 72-1 Root Server



72.4.2 Root Server with Inventoried Workstations

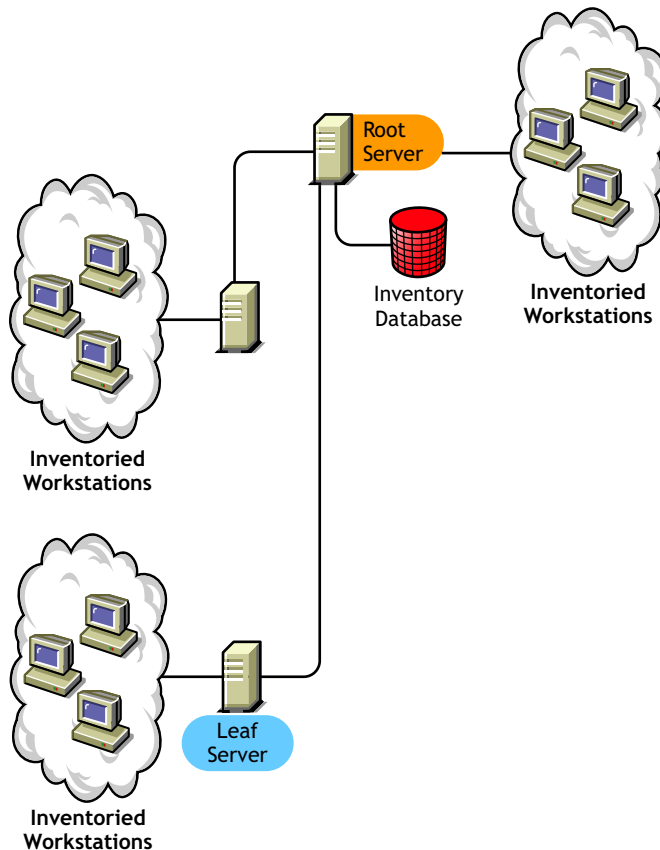
The Root Server with Inventoried Workstations has the following characteristics:

- This server is the topmost Inventory server in the inventory tree hierarchy.
- This server has an Inventory database and inventoried workstations attached to it. We recommend that you deploy these inventoried workstations in a LAN.

Choose Root Server with Inventoried Workstations if you want to store the inventory information of your enterprise in a centralized database and if you have inventoried workstations in the same site as the Root Server. You can directly send the inventory information from these workstations to the Root Server. The Inventory database at the Root Server with Inventoried Workstations contains the inventory information for all these inventoried workstations as well as for all the lower-level Inventory servers.

The following illustration depicts a Root Server with inventoried workstations and Inventory database attached to it. The Leaf Servers are connected to the Root Server.

Figure 72-2 Root Server with Inventoried Workstations



72.4.3 Intermediate Server

The Intermediate Server has the following characteristics:

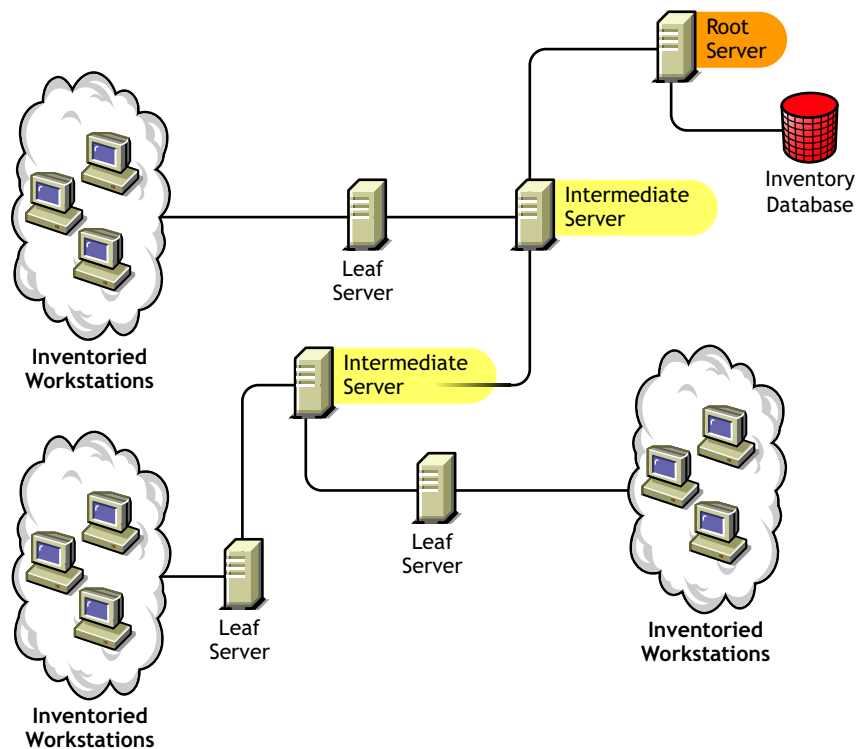
- This Inventory server acts as a staging server for the lower-level Leaf Servers.
- The server moves the inventory information to the next-level Inventory server.

- This server does not have inventoried workstations or an Inventory database attached to it.
- There can be one or more Intermediate Servers in your enterprise.

Place Intermediate Servers on sites where the link parameters change substantially. The Intermediate Server stores the scan files to the disk to make up for the difference in bandwidth and reliability.

The following illustration depicts an Intermediate Server connected to Root Server. Two Leaf Servers roll up the inventory information to the Intermediate Server. This Intermediate Server rolls up the inventory information to another Intermediate Server that is connected to the Root Server.

Figure 72-3 *Intermediate Server*



In the illustration, there are many Leaf Servers and Intermediate Servers at different levels. The Intermediate Server is a staging server for uploading the scan information to the next-level server. The last Intermediate Server is attached to the topmost Root Server. This scenario is typical if there are many Leaf Servers in different geographical locations. All the Leaf Servers move the inventory information to the Intermediate Server.

In some scenarios, the Leaf Server connects to the Intermediate Server over a WAN.

72.4.4 Intermediate Server with Database

The Intermediate Server with Database has the following characteristics:

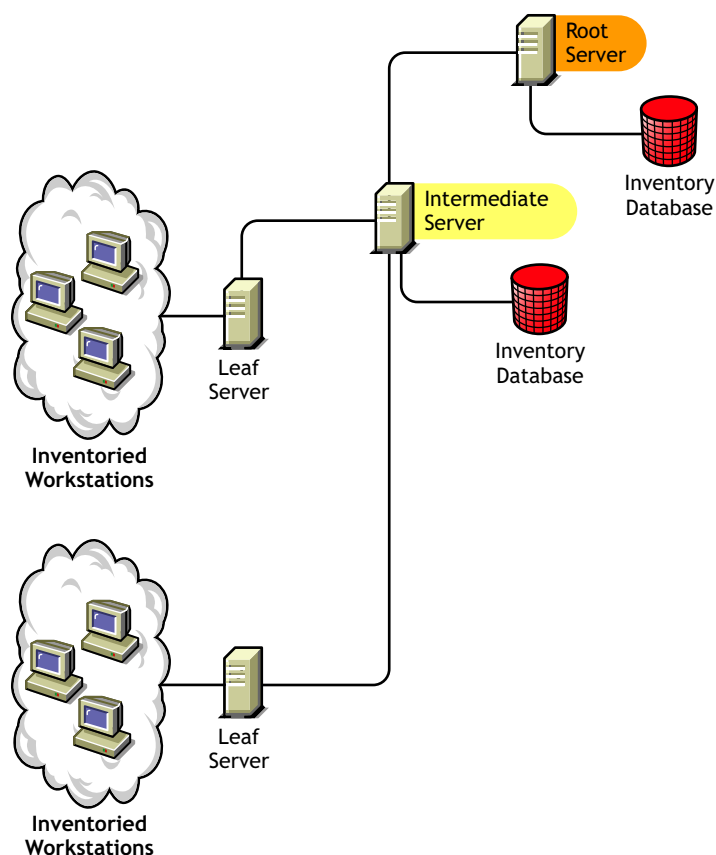
- This Inventory server acts as a staging server for the lower-level Leaf Servers.
- The server moves the inventory information to the next-level Inventory server.
- This server has an Inventory database attached to it.

- There can be one or more Intermediate Servers with Database in your enterprise.

Choose Intermediate Server with Database if you want to administer an intermediate site by generating Inventory reports. The inventory information that is rolled up to this Inventory server is stored in the local Inventory database and also rolled up to the next-level Inventory server.

The following illustration depicts two Leaf Servers attached to the Intermediate Server. A consolidated inventory information of all Leaf Servers is available at the Intermediate Server level.

Figure 72-4 *Intermediate Server with Database*



72.4.5 Intermediate Server with Inventoried Workstations

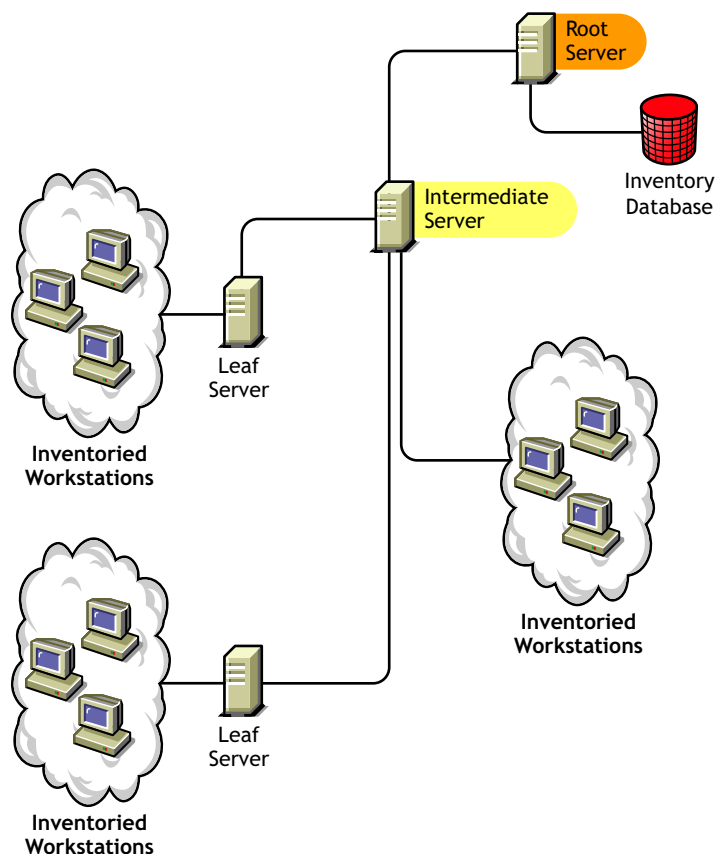
The Intermediate Server with Inventoried Workstations has the following characteristics:

- This Inventory server acts as an intermediate server for the lower-level Leaf Servers.
- This server moves the inventory information to the next-level Inventory server.
- This server has inventoried workstations attached to it
- The server does not have an Inventory database attached to it.
- There can be one or more Intermediate Servers with Inventoried Workstations in your enterprise.

Choose Intermediate Server with Inventoried Workstations if you want an Intermediate Server and the site having the Intermediate Server has inventoried workstations, whose inventory information you want to store it at the Root Server.

The following illustration depicts two Leaf Servers attached to the Intermediate Server. This Intermediate Server also has inventoried workstations attached to it.

Figure 72-5 *Intermediate Server with Inventoried Workstations*



72.4.6 Intermediate Server with Database and Inventoried Workstations

The Intermediate Server with Database and Inventoried Workstations has the following characteristics:

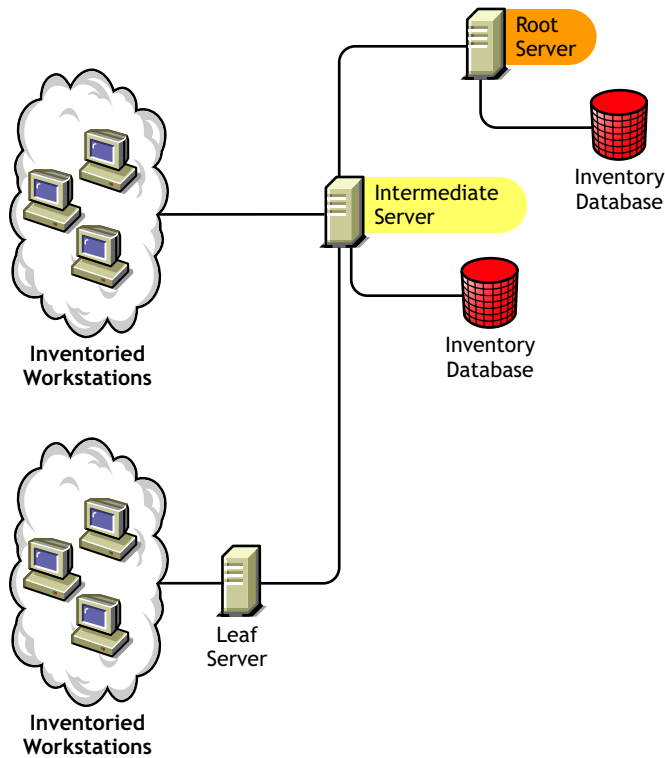
- This Inventory server acts as a staging server for the lower-level Leaf Servers.
- This server moves the inventory information to the next-level Inventory server.
- This server has inventoried workstations attached to it.
- This server has an Inventory database attached to it.
- There can be one or more Intermediate Servers with Database and Inventoried Workstations in your enterprise.

Choose Intermediate Server with Database and Inventoried Workstations if you want the functionalities of **Intermediate Server with Database** and **Intermediate Server with Inventoried Workstations** available on the site.

The following illustration depicts two Leaf Servers attached to the Intermediate Server. The Intermediate Server has inventoried workstations attached to it. A consolidated Inventory database

of all Leaf Servers and the inventoried workstations that are directly connected to the Intermediate Server is available at the Intermediate Server level.

Figure 72-6 *Intermediate Server with Database and Inventoried Workstations*



72.4.7 Leaf Server

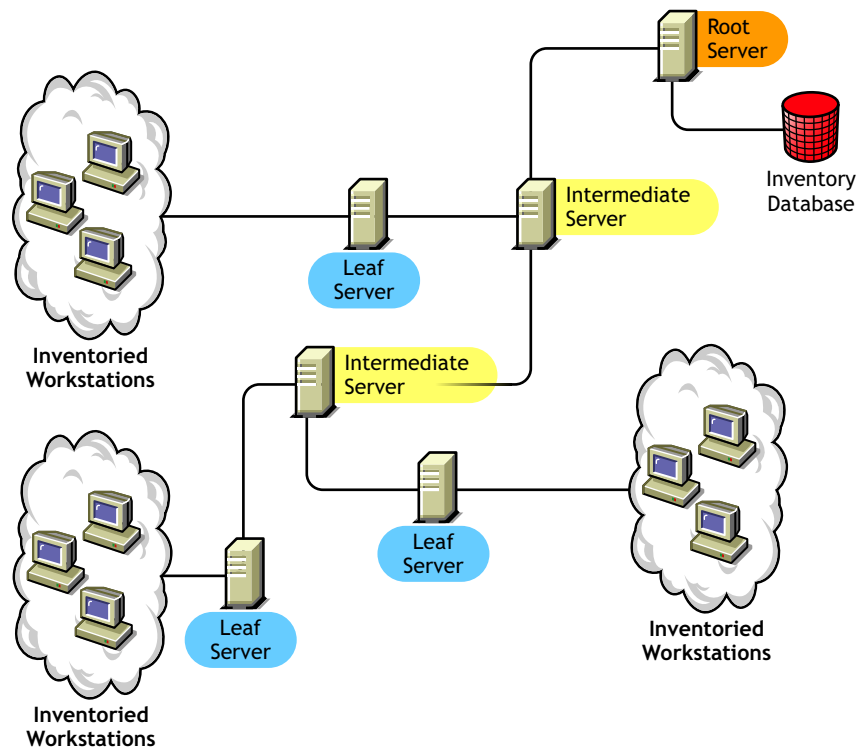
The Leaf Server has the following characteristics:

- This Inventory server is at the lowest level in the inventory tree hierarchy.
- This server has inventoried workstations attached to it.
- This server moves the inventory information to the next-level Inventory server
- A simple Leaf Server does not have an Inventory database. An Inventory database is not required because there might be only few inventoried workstations attached to the Leaf server.

Choose Leaf Server if you have inventoried workstations at remote sites, and you want to obtain and store the inventory information from these inventoried workstations in a centralized database.

The following illustration depicts many Leaf Servers attached to the Intermediate Server. The Intermediate Server is connected to Root Server. A consolidated Inventory database of all Leaf Servers is available at the Root Server level.

Figure 72-7 Leaf Server



72.4.8 Leaf Server with Database

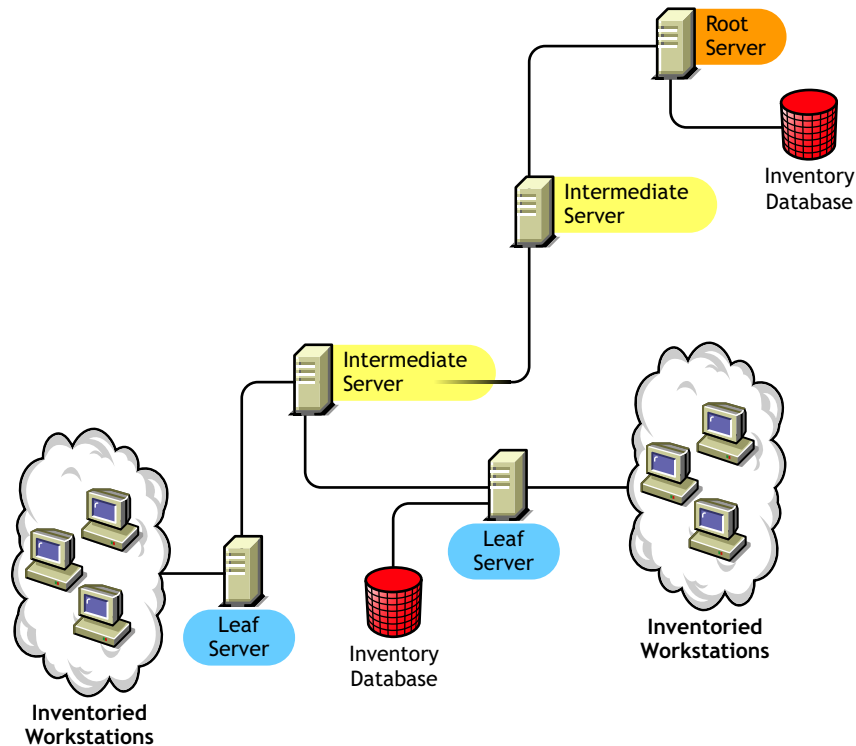
The Leaf Server with Database has the following characteristics:

- This Inventory server is at the lowest level in the inventory tree hierarchy.
- This server has inventoried workstations attached to it.
- This server moves the inventory information to the next-level Inventory server.
- This server has an Inventory database attached to it. You can assign a server as a Leaf Server with Database to maintain the inventory information for the inventoried workstations specific to the site.

Choose Leaf Server with Database if you want the functionalities of a **Leaf Server** as well as administer the site by generating Inventory reports.

The following illustration depicts two Leaf Servers attached to the Intermediate Server. One Leaf Server has an Inventory database attached to it. This database contains a consolidated inventory of all inventoried workstations attached to this Leaf Server.

Figure 72-8 *Leaf Server with Database*



72.4.9 Standalone Server

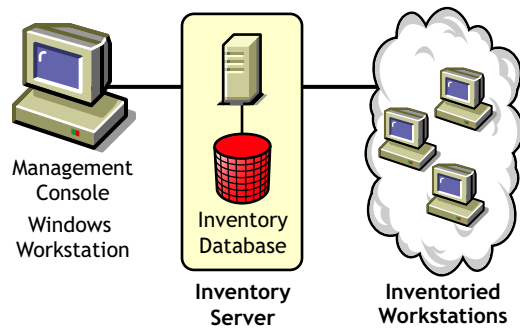
The Standalone Server has the following characteristics:

- This Inventory server has inventoried workstations attached to it.
- This server has an Inventory database attached to it.
- There is no roll-up of scan information and there are no requirements for Intermediate Servers and a Root Server.

Use a Standalone Server if your network is made up of a single site and you want to administer that site.

The following illustration depicts Standalone Server.

Figure 72-9 *Standalone Server*



72.4.10 Quick Reference Table of the Inventory Server Roles

Table 72-1 *Inventory Server Roles*

Inventory Server	Is the Inventory Database Attached to the Inventory Server?	Are Inventoried Workstations Attached to the Inventory Server?
Root Server	Yes	No
Root Server with Inventoried Workstations	Yes	Yes
Intermediate Server	No	No
Intermediate Server with Database	Yes	No
Intermediate Server with Inventoried Workstations	No	Yes
Intermediate Server with Database and Inventoried Workstations	Yes	Yes
Leaf Server	No	Yes
Leaf Server with Database	Yes	Yes
Standalone Server	Yes	Yes

Setting Up Workstation Inventory

73

Before you install Novell® ZENworks® 7 Workstation Inventory in your working environment, you must plan and decide the hierarchy of the Inventory server tree for your enterprise. You should organize your inventory deployment based on your network constraints and information requirements.

The following sections contain detailed information to help you deploy Workstation Inventory in your enterprise:

- [Section 73.1, “Deploying Workstation Inventory,” on page 887](#)
- [Section 73.2, “Setting Up the Inventory Database,” on page 929](#)
- [Section 73.3, “Configuring the Inventory Service Object,” on page 955](#)
- [Section 73.5, “Configuring the Database Location Policy,” on page 957](#)
- [Section 73.6, “Configuring the Workstation Inventory Policy,” on page 958](#)
- [Section 73.7, “Configuring the Roll-Up Policy,” on page 960](#)
- [Section 73.8, “Configuring the Dictionary Update Policy,” on page 961](#)
- [Section 73.9, “Setting Up Distribution of Dictionary,” on page 962](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

73.1 Deploying Workstation Inventory

The following sections help you to deploy Workstation Inventory:

- [Section 73.1.1, “Simple Deployment,” on page 887](#)
- [Section 73.1.2, “Advanced Deployment,” on page 890](#)

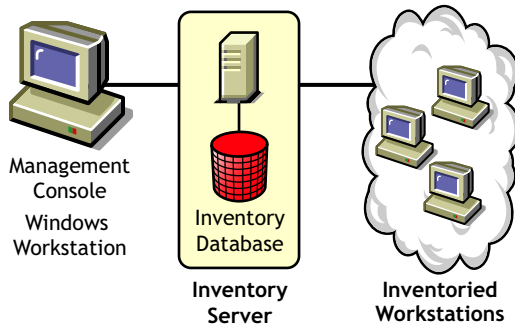
IMPORTANT: The recommendations discussed in the scenarios are generic. Based on the topology of your enterprise, further refinements might become necessary.

73.1.1 Simple Deployment

In the example scenario, the network consists of a single site and up to 5000 inventoried workstations. The Inventory server components and the database are located on a Standalone Server, and the inventoried workstations send scans to the Standalone server.

This scenario is illustrated in the following figure.

Figure 73-1 *Simple Workstation Inventory Deployment*



The following sections contain detailed information to help you deploy Workstation Inventory in a single site:

1. [“Deployment Options for Inventory Agent” on page 888](#)
2. [“Recommendations for Deployment” on page 888](#)
3. [“Installing Workstation Inventory” on page 889](#)
4. [“Understanding the Effects of Workstation Inventory Installation” on page 889](#)
5. [“Configuring the Required Policy” on page 889](#)
6. [“Starting the Inventory Service” on page 889](#)
7. [“Updating the Software Dictionary” on page 889](#)
8. [“Understanding the Inventory Scanning Cycle in the Standalone Scenario with Novell Client Installed on Inventoried Workstations” on page 889](#)

Deployment Options for Inventory Agent

Before installing the Inventory Agent on your workstation, you must deploy the Inventory servers to receive workstation scans. For more information about the deployment options for Inventory Agent, see [“Deploying the Inventory Agent” on page 910](#).

Recommendations for Deployment

- The minimum base Inventory server configuration includes 512 MB RAM and a database cache of 128 MB.
- The transmission of inventory information to the Inventory server and storage of the inventory information into the Inventory database is an ongoing back end process that can take several hours or even more than a day.
- If many inventoried workstations are attached to the same Inventory server, we recommend that you do not schedule the scan of all inventoried workstations at the same time, because this stresses Novell eDirectory™ and the Inventory services.
- Make sure that the eDirectory time synchronization radius is set within 2 seconds.
- The optimal database cache size requirement for the server could vary because of the server environment. Determine the database cache size that needs to be set by trying a range of cache sizes in the runtime environment. The default Sybase database cache size is 128 MB. For more

information about improving the database performance, see [Appendix M, “Performance Tips,” on page 1185](#).

Installing Workstation Inventory

During the Workstation Inventory installation, configure the Inventory Standalone Configuration settings. For detailed information, see the *Novell ZENworks 7 Desktop Management Installation Guide*.

Understanding the Effects of Workstation Inventory Installation

For detailed information on the effects of Workstation Inventory installation, see [Section 73.1.4, “Understanding the Effects of Workstation Inventory Installation,” on page 913](#).

Configuring the Required Policy

Configure the [Workstation Inventory Policy](#).

Starting the Inventory Service

After installing ZENworks 7 Desktop Management, the Inventory service is automatically started.

Updating the Software Dictionary

You must manually download the latest version of the dictionary from TID 10093255 in the [Novell Support Knowledgebase \(http://novell.com/support/\)](#) and update the software dictionary.

NOTE: The dictionary is updated and published once in every three months in this TID.

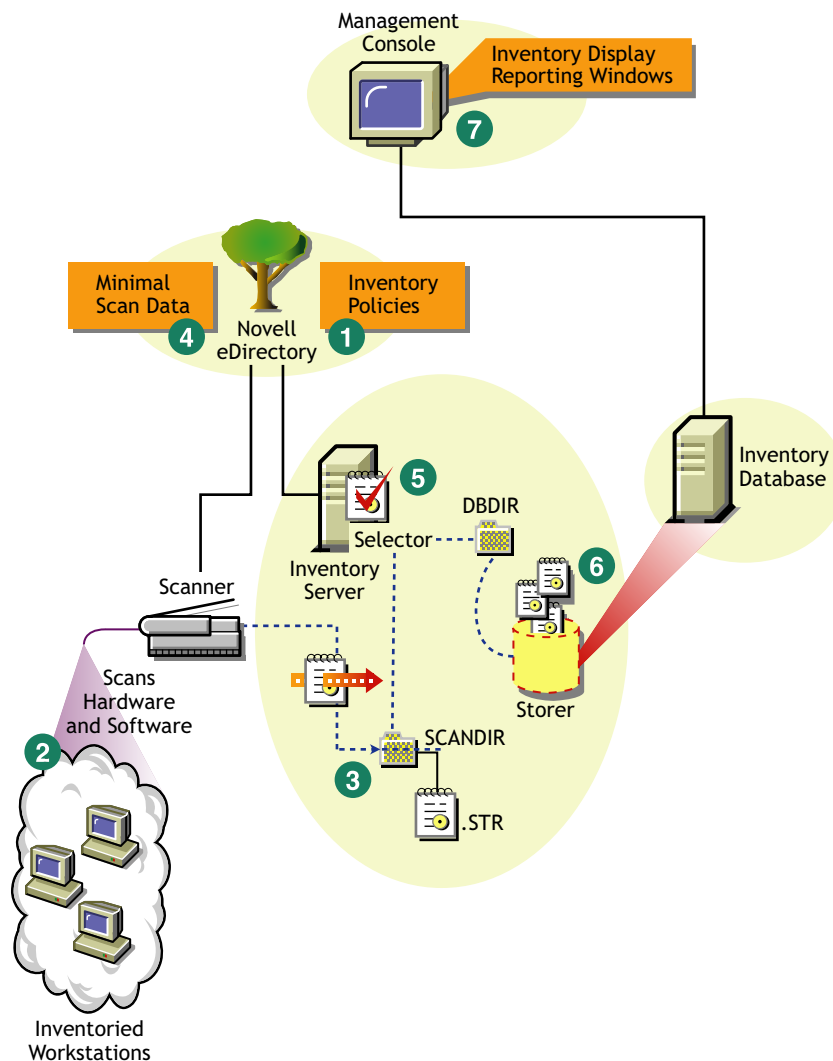
Understanding the Inventory Scanning Cycle in the Standalone Scenario with Novell Client Installed on Inventoried Workstations

The inventory scanning cycle is as follows:

1. The Inventory policies in eDirectory define the inventory settings, such as scanning time and the location of the scan directory. These settings can be customized.
2. The scanner reads the inventory policies and collects the workstation inventory information. The Inventory scanner also checks whether an updated dictionary is available at its Inventory server and downloads the updated dictionary.
3. The scanner stores the inventory information of each inventoried workstation at the Inventory server.
4. The scanner stores the minimal inventory information of the inventoried workstation in the respective workstation objects in the eDirectory.
5. The Selector validates the inventory information and places the information in the Inventory database.
6. The Storer updates the database with the inventory information.
7. The ZENworks administrator views the inventory information.

The following illustrations depict the inventory scanning cycle in the Standalone scenario with Novell Client installed.

Figure 73-2 *Inventory Scanning cycle in the Standalone scenario with Novell Client installed*



73.1.2 Advanced Deployment

- “Deploying Inventory in a Single Site with More than 5,000 Inventoried Workstations” on page 890
- “Deploying Inventory in Multiple or Enterprise Sites” on page 894

Deploying Inventory in a Single Site with More than 5,000 Inventoried Workstations

In this example scenario, the network consists of a single site with more than 5000 workstations. The inventory configuration consists of two or more Standalone Servers, each server receiving scans from up to 5,000 inventoried workstations. All the Standalone Servers store the inventory data to a single database.

The following sections contain detailed information to help you deploy Workstation Inventory on a single site:

1. [“Deployment Options for Inventory Agent” on page 891](#)
2. [“Recommendations for Deployment” on page 891](#)
3. [“Installing Workstation Inventory” on page 891](#)
4. [“Understanding the Effects of Workstation Inventory Installation” on page 891](#)
5. [“Configuring the Required Policy” on page 892](#)
6. [“Starting the Inventory Service” on page 892](#)
7. [“Updating the Software Dictionary” on page 892](#)
8. [“Understanding the Inventory Scanning Cycle in the Standalone Scenario” on page 892](#)

Deployment Options for Inventory Agent

Before installing the Inventory Agent on your workstation, you must deploy the Inventory servers to receive inventory scans. For more information about the deployment options for Inventory Agent, see [“Deploying the Inventory Agent” on page 910](#).

Recommendations for Deployment

- The minimum base Inventory server configuration includes 512 MB RAM and a database cache of 128 MB.
- All inventoried workstations should send the inventory information to the nearest Inventory server on the LAN; policies must be created based on this information.
- The transmission of inventory information to the Inventory server and storage of the inventory information into the Inventory database is an ongoing back end process that can take several hours or even more than a day.
- If many inventoried workstations are attached to the same Inventory server, we recommend that you do not schedule the scan of all inventoried workstations at the same time, because this stresses Novell eDirectory™ and the Inventory services.
- Make sure that the eDirectory time synchronization radius is set within 2 seconds.
- The optimal database cache size requirement for the server could vary because of the server environment. Determine the database cache size that needs to be set by trying a range of cache sizes in the runtime environment. The default Sybase database cache size is 128 MB. For more information about improving the database performance, see [Appendix M, “Performance Tips,” on page 1185](#).

Installing Workstation Inventory

During the Workstation Inventory installation, configure the Inventory Standalone Configuration settings. For detail information on installing Workstation Inventory, see [Novell ZENworks 7 Desktop Management Installation Guide](#).

Understanding the Effects of Workstation Inventory Installation

For detail information on the effects of Workstation Inventory installation, see [Section 73.1.4, “Understanding the Effects of Workstation Inventory Installation,” on page 913](#).

Configuring the Required Policy

Configure the **Workstation Inventory Policy**.

Starting the Inventory Service

After installing ZENworks 7 Desktop Management, the Inventory service is automatically started.

Updating the Software Dictionary

You can update the software dictionary in any one of the following ways:

- On each Inventory server, manually download the latest version of the dictionary from TID 10093255 in the [Novell Support Knowledgebase \(http://novell.com/support/\)](http://novell.com/support/) and update the software dictionary.
- Manually download the latest version of the dictionary from TID 10093255 in the [Novell Support Knowledgebase \(http://www.novell.com/support\)](http://www.novell.com/support) on one of the Standalone Servers and automatically distribute the dictionary from this server to all other Standalone Servers in your setup by “**Configuring the Dictionary Update Policy**” on page 961. For more information, see **Section 73.9, “Setting Up Distribution of Dictionary,”** on page 962.

NOTE: The dictionary is updated and published once in every three months in this TID.

Understanding the Inventory Scanning Cycle in the Standalone Scenario

The inventory scanning cycle is as follows:

1. The Inventory policies in eDirectory define the inventory settings, such as scanning time and the location of the scan directory. These settings can be customized.
2. The scanner reads the inventory policies and collects the workstation inventory information. The Inventory scanner also checks whether an updated dictionary is available at its Inventory server and downloads the updated dictionary.

If the Novell Client is not installed on the inventoried workstation, the Scanner accesses eDirectory through the ZENworks 7 Desktop Management Middle Tier Server.

3. The scanner stores the inventory information of each inventoried workstation at the Inventory server.

If the Novell Client is not installed on the inventoried workstation, the Scanner sends the inventory information of each inventoried workstation to the Inventory server through the ZENworks 7 Desktop Management Middle Tier Server.

4. The scanner stores the minimal inventory information of the inventoried workstation in the respective workstation objects in the eDirectory.

If the Novell Client is not installed on the inventoried workstation, the Scanner accesses eDirectory through the ZENworks 7 Desktop Management Middle Tier Server.

5. The Selector validates the inventory information and places the information in the Inventory database.
6. The Storer updates the database with the inventory information.
7. The ZENworks administrator views the inventory information.

Figure 73-3 *Inventory Scanning Cycle in the Standalone scenario with the Novell Client installed*

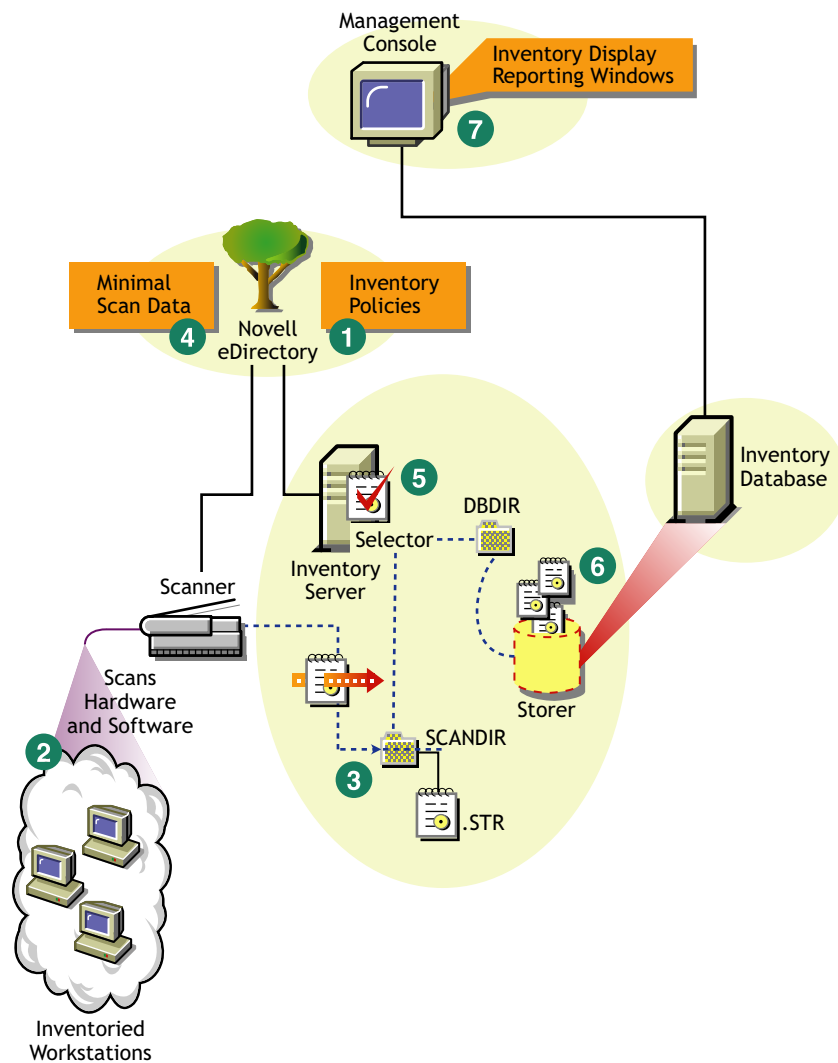
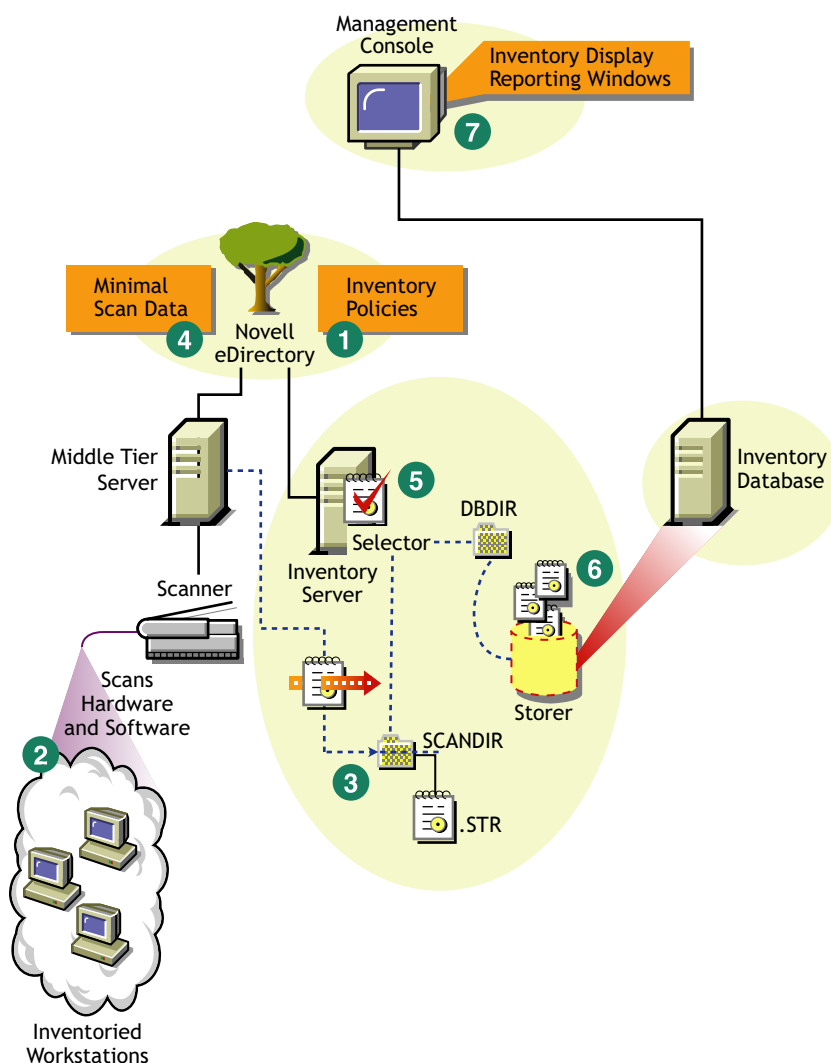


Figure 73-4 Inventory Scanning Cycle in the Standalone Server without the Novell Client installed



Deploying Inventory in Multiple or Enterprise Sites

The following sections contain detailed information to help you deploy Workstation Inventory in multiple or enterprise sites:

1. [“Designing the Inventory Tree” on page 895](#)
2. [“Deployment Options for Inventory Server and Inventory Database” on page 900](#)
3. [“Deployment Options for Inventory Agent” on page 905](#)
4. [“Recommendations for Deployment” on page 905](#)
5. [“Installing Workstation Inventory” on page 905](#)
6. [“Understanding the Effects of Workstation Inventory Installation” on page 906](#)
7. [“Configuring the Required Policies” on page 906](#)
8. [“Starting the Inventory Service” on page 907](#)
9. [“Updating the Software Dictionary” on page 907](#)

10. “Understanding Rolling Up Inventory Information Across Servers” on page 908

Designing the Inventory Tree

In an enterprise or multiple site, complete the following tasks to design the inventory tree:

- “1. List the sites in the enterprise” on page 895
- “2. What is the ideal place for the Root Server?” on page 896
- “3. Is any other database needed?” on page 897
- “Optional step: If another database is needed” on page 897
- “4. Identify the route for Inventory information” on page 897
- “5. Identify servers on each site to act as Inventory and Database Servers” on page 898
- “6. Create the tree of servers for enterprise Inventory collection” on page 898
- “7. Create an implementation plan” on page 899
- “8. Start the actual deployment” on page 899

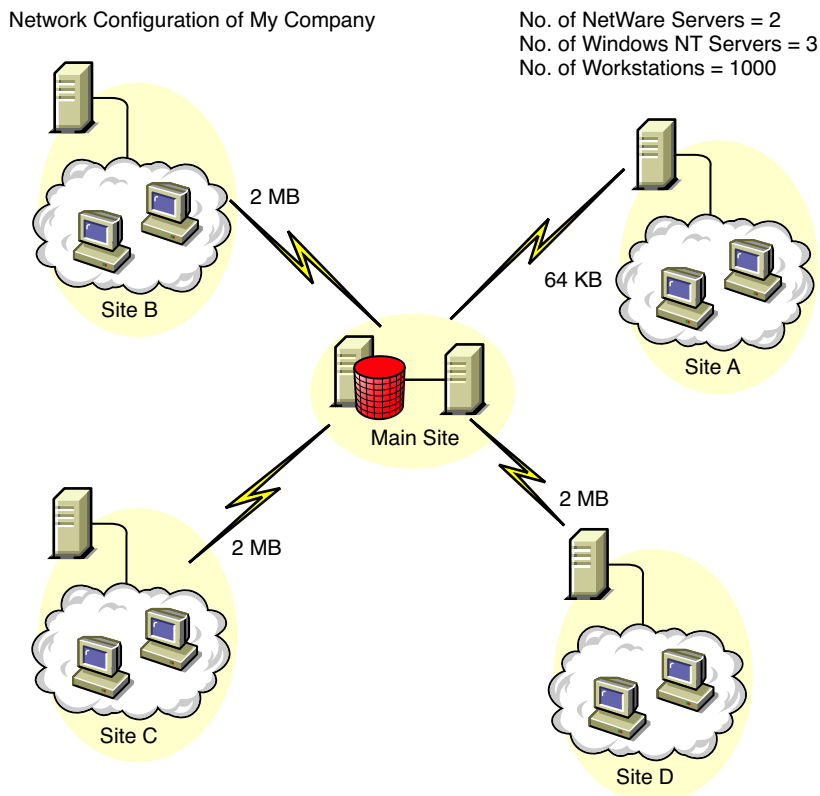
1. List the sites in the enterprise

Describe the entire network of your enterprise.

- List the various sites in your enterprise.
- List the physical links between the various sites.
- Identify the type of links in terms of bandwidth and reliability.

The following figure illustrates the network organization of an enterprise with servers in different locations.

Figure 73-5 *Network organization of an enterprise*



This illustration depicts four sites (Site A, Site B, Site C, and Site D) connected to a central site. It depicts the physical links between the sites and the type of links in terms of bandwidth.

2. What is the ideal place for the Root Server?

The Root Server in the inventory tree is the highest-level server. Necessarily, an Inventory database is attached to the Root Server.

The inventory information available from the Inventory database of the Root Server consists of all information from lower-level sites on the network and from the Root Server site.

Factors that you must consider include:

- There must be high-speed links between the Root Server and the management console.
- We recommend that there should be high-speed links between the site having the Root Server and the sites having the lower-level Inventory servers.
- Using the management console, the administrator can collect the inventory information from any of the sites connected on high-speed links from the Root Server, or from the Root Server level site.
- A database server of suitable configuration should be provided for the Inventory server.

3. Is any other database needed?

In addition to the database at the Root Server, you can maintain database servers at different sites.

You might want to maintain additional databases if there are sites or subtrees that are managed for inventory at different locations, and these sites are connected to the network over a slow link.

You should also determine if there are specific reasons to have a separate database for a single site or a set of sites. There might be some organizational needs for your enterprise to have the database server on different sites, even if there is no product deployment need to have any other database.

NOTE: For a majority of enterprises, there could be no need to have any other database besides the enterprise-wide single database.

Optional step: If another database is needed

- If you decide to have additional database servers, identify the sites that need a database. Additionally, you need to examine whether the database caters to the local site or a site with many subsites. Also, identify the sites that require information in each Inventory database.
- All the sites served by a single database should typically access this database instead of the database at the Root Server for inventory management. This reduces the load on the database at Root Server.
- Database administrators should be available for these sites.

4. Identify the route for Inventory information

Identify the routes for inventory information for all Inventory servers to the nearest database.

To devise a route plan:

- Each route can have an Intermediate Server at a staging site. The Intermediate Server receives and transmits the information to the next destination. These are application-layer-level routes for inventory information. There can be various network-layer-level routes between two adjacent servers, which is determined and managed by the routers in the network.
- The route provides information indicating how inventory information travels from a particular site to its final destination, which is the database at the Root Server.
- There can be multiple routes. Choose the fastest and most reliable route. To determine the route, consider the physical network links.
- Routes identified and made operational can be changed later, although there might be some cost in terms of management and traffic generation. If there is no intermediate database involved, you can change the route by changing the eDirectory-based policy.
- Put Intermediate Servers on sites where the link parameters change substantially. Criteria to consider are difference in bandwidth, difference in reliability of the links, and the need for roll up of inventory information.
- Availability of Inventory servers on the intermediate site for staging the inventory information should be considered while deciding the sites for Intermediate Servers. Make sure that there is enough disk space on these servers to store all the inventory information on the disk until the Sender sends it to the next destination.

5. Identify servers on each site to act as Inventory and Database Servers

In ZENworks 7 Desktop Management, you choose the role for each Inventory server. For more information, see [Section 72.4, “Understanding the Inventory Server Roles,”](#) on page 876.

The number of inventoried workstations attached to an Inventory server also determines the load. The following table lists the disk space requirements for the server:

Table 73-1 *Disk Requirements for a ZENworks Inventory Server*

Server Type	Disk Space Requirements
Leaf Server	$(n1 \times s) + (n1 \times z)$
Leaf Server with Database	$(n1 \times s \times 2) + \{(n1 \times dbg)\}$
Intermediate Server	$n2 \times z$
Intermediate Server with Database	$(n2 \times z) + (n2 \times s) + \{(n2 \times dbg)\}$
Intermediate Server with Inventoried Workstations	$(n1 \times s \times 2) + (n2 \times z)$
Intermediate Server with Database and Inventoried Workstations	$(n1 \times s \times 2) + (n2 \times z) + (n2 \times s) + \{(n1 \times dbg) + (n2 \times dbg)\}$
Root Server	$(n2 \times z) + (n2 \times s) + \{(n2 \times dbg)\}$
Root Server with Inventoried Workstations	$(n1 \times s \times 2) + (n2 \times z) + (n2 \times s) + \{(n1 \times dbg) + (n2 \times dbg)\}$
Standalone Server	$(n1 \times s \times 1) + \{(n1 \times dbg)\}$

In the table, $n1$ is the number of inventoried workstations attached to the server.

s is the size of the scan data files. This file size varies depending on the data collected. Calculate 400 KB scan data from each inventoried workstation to calculate the load.

dbg is the storage space of the inventory information in the database.

$n2$ is the number of inventoried workstations rolled up to the Inventory server.

z is the size of the compressed scan data file per inventoried workstation. The average compression ratio is 80-90% of the STR file size.

$\{ \}$ denotes the disk space of the database server, depending on whether the database is on the same Inventory server or if it is connected to the Inventory server. If the database is on the same Inventory server, calculate the total disk space including the database space for the Inventory server. For example, if the Leaf Server with Database has the Inventory database on the same server, calculate the requirements for storage of inventory information, including the database disk space.

6. Create the tree of servers for enterprise Inventory collection

Make sure that the inventory tree you design follows these guidelines:

- The root of the tree is the Root Server.
- At least one Inventory server per site is recommended.

- Each site has inventoried workstations to be scanned.
- Optionally, there are databases and Intermediate Servers on different sites.

7. Create an implementation plan

After you design the inventory tree, you should develop an implementation plan to cover the phased deployment plan for the network. Use the top-down deployment of the Workstation Inventory installation. Always begin the installation at the topmost level server (Root Server) and proceed with the next lower-level servers.

8. Start the actual deployment

After your implementation plan is finalized, start the actual deployment according to the plan.

Follow these steps:

1. Install the Inventory servers on the sites. For more information, see [“Installing Workstation Inventory” on page 905](#).
2. Create and configure the policies applicable to Inventory server and inventoried workstations. For more information, see [“Configuring the Required Policies” on page 906](#).

Adding a Database Server to an Existing Inventory Setup

If you have already configured the servers for inventory setup, and you need to add another database server, follow these instructions:

- 1 Run the installation program to install the Inventory database on the server.

The installation program installs the Sybase database. If you are maintaining the database in Oracle, make sure that the Oracle database exists. For more information, see [“Setting Up the Sybase Inventory Database” on page 929](#). If you are maintaining the database in MS SQL, make sure that the MS SQL database exists. For more information, see [“Setting Up the MS SQL Server 2000 or MS SQL Server 2005 Inventory Database” on page 945](#).

- 2 Shut down the Inventory services. For more information, see [Section 73.1.5, “Starting and Stopping the Inventory Service,” on page 915](#).
- 3 Based on the database you select, make sure that you configure the database. For more information, see [Section 73.5, “Configuring the Database Location Policy,” on page 957](#).
- 4 If you want to attach a new database to an existing Inventory server that does not have a database attached, you must change the role of the Inventory server in its Inventory Service object (Inventory Service_server_name). For example, if you attach an Inventory database to an existing Leaf Server, you must change the server role from Leaf Server to Leaf Server with Database in the Inventory Service object of the Leaf Server.

If you want to attach an Inventory database to a freshly installed Inventory server, you must choose an appropriate server role for the Inventory server.

To change the role of an Inventory server:

- 4a In ConsoleOne, right-click the Inventory Service object, click *Properties*, then click the *Inventory Service Object Properties* tab.

- 4a1 Choose the new role of the Inventory Service object, then click *Apply*.

Follow the actions that you need to change the role. For more information, see [Section 73.1.7, “Changing the Role of the Inventory Server,” on page 917](#).

- 5 Make sure that you enforce Full Scan for the Inventory Service object.
 - 5a In ConsoleOne, right-click the Inventory Service object, click *Properties*, then click the *Inventory Service Object Properties* tab.
 - 5b Select the *Enable Scan option*, then click *OK*.
- 6 Bring up the Inventory service. For more information, see [Section 73.1.5, “Starting and Stopping the Inventory Service,”](#) on page 915.

Deployment Options for Inventory Server and Inventory Database

This section covers these scenarios:

- [“Scenario 1: Inventory Deployment without Intermediate Servers in a WAN”](#) on page 900
- [“Scenario 2: Inventory Deployment with Intermediate Servers in a WAN”](#) on page 901
- [“Scenario 3: Roll Up of the Inventory Information Across eDirectory Trees”](#) on page 903
- [“Scenario 4: Merging eDirectory Trees”](#) on page 903
- [“Scenario 5: Deploying Inventory Server Across a Firewall”](#) on page 904

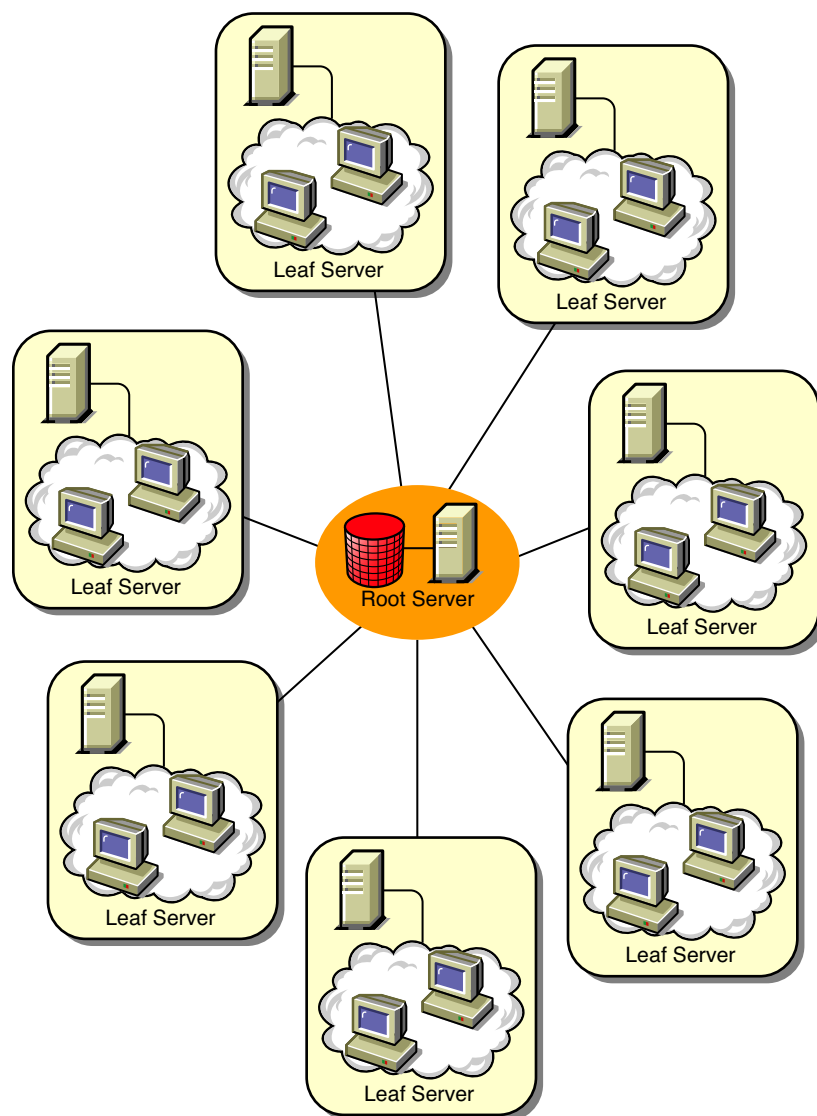
Scenario 1: Inventory Deployment without Intermediate Servers in a WAN

In this scenario, the network consists of many remote sites connected to a Central Site over a WAN. Each remote site has a Leaf Server that collects inventory information from workstations located in the same site, and rolls up the inventory information to the Root Server located at the central site. The remote sites are administered from the Central Site because the Leaf Servers do have Inventory database attached to it.

TIP: To locally administer the remote sites, you must have the Inventory database attached to Leaf Servers and change the role of the Inventory server to Leaf Server with Database. For more information on how to change the role of an Inventory server, see [Section 73.1.7, “Changing the Role of the Inventory Server,”](#) on page 917.

This scenario is illustrated in the following figure.

Figure 73-6 *Inventory Deployment without Intermediate Servers in a WAN*

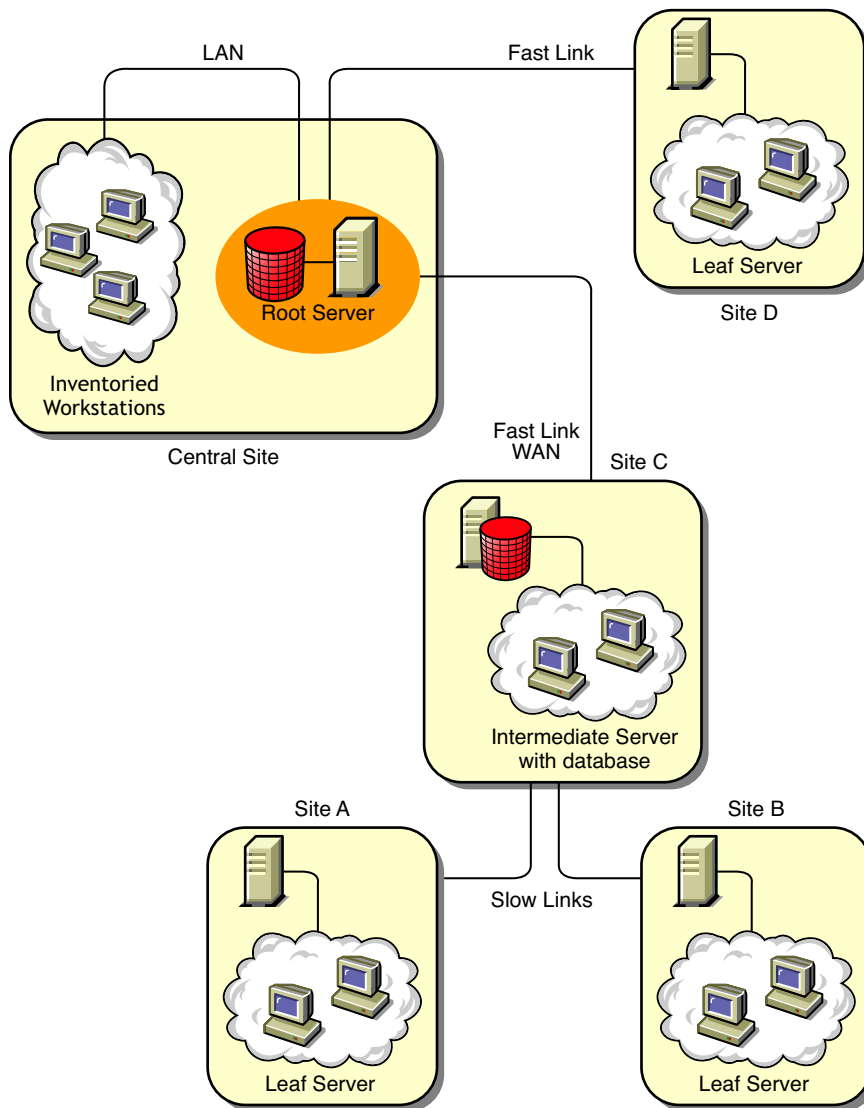


Scenario 2: Inventory Deployment with Intermediate Servers in a WAN

In this scenario, the network consists of four remote sites (A, B, C, and D), and a Central Site. Sites A and B are connected to Site C over slow links and are not directly connected to the Central Site. Site C is connected to the Central Site over a fast WAN link. Site D is directly connected to the Central Site over a fast link. Sites A, B and C are administered at Site C.

This scenario is illustrated in the following figure.

Figure 73-7 Inventory Deployment with Intermediate Servers in a WAN



To administer the enterprise from the Central Site, and also administer Sites A and B from Site C, do the following:

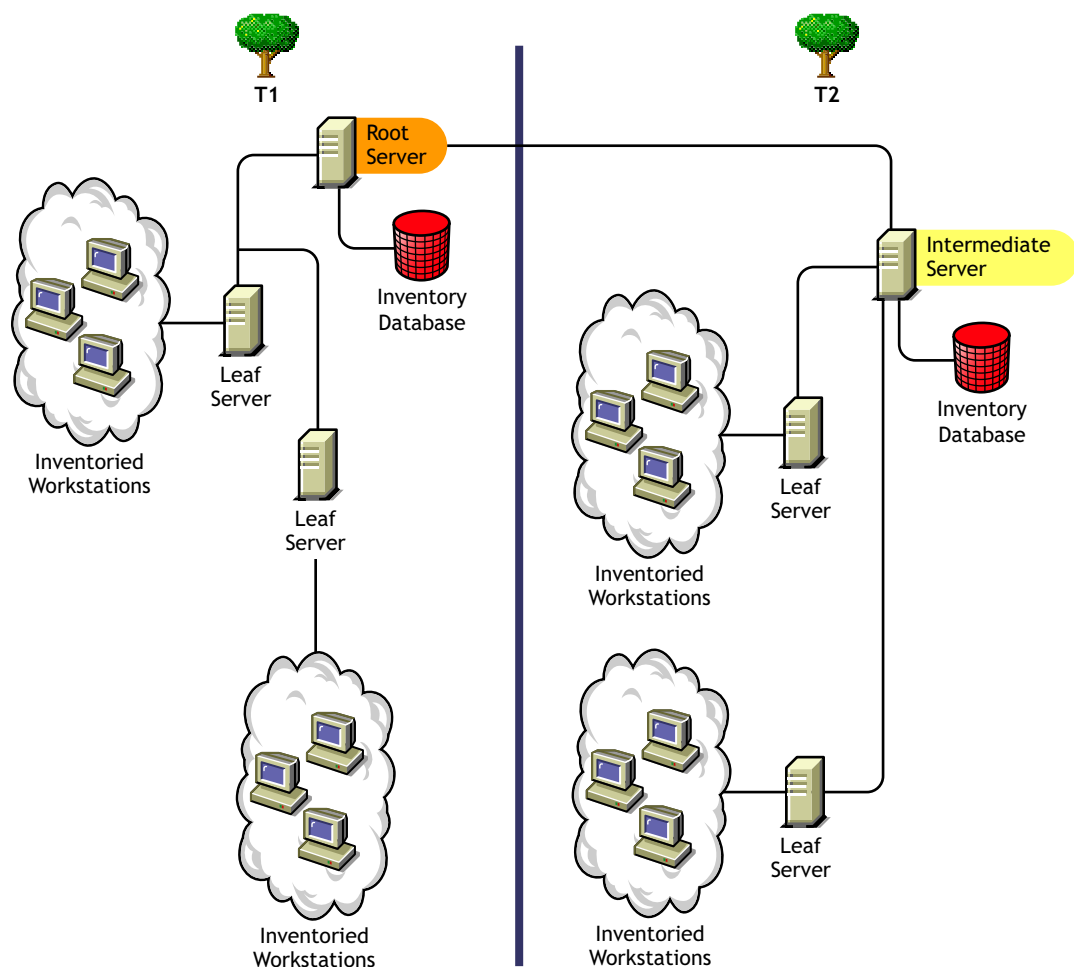
1. Install Leaf Servers at Sites A, B, and D.
2. Install Intermediate Servers with Database at Site C.
3. Configure Leaf Servers at Sites A and B to roll up the inventory information to the Intermediate Server with Database at Site C.
4. Configure the Intermediate Server with Database at Site C to roll up the inventory information to Root Server at the Central Site.
5. Configure the Leaf Server at Site D to roll up the inventory information to Root Server at the Central Site.

Scenario 3: Roll Up of the Inventory Information Across eDirectory Trees

In this configuration, you can deploy any of the previous scenarios. The highest-level Inventory server of one eDirectory tree rolls up the inventory information to an Inventory server located on the other eDirectory tree.

The following illustration depicts a sample scenario where you can deploy this inventory configuration.

Figure 73-8 Roll Up of the Inventory Information across eDirectory Trees



There are two organizations: A and B. Each organization has its own eDirectory tree and inventory tree. Organization A has two Leaf Servers and a Root Server in its inventory tree. Organization B also has two Leaf Servers and a Root Server in its inventory tree. A decision is taken to merge both the organizations and both the inventory trees but to retain the eDirectory trees. After the merger, the role of the Root Server on the eDirectory tree T2 is changed to Intermediate Server with Database and the inventory information is rolled up from the Intermediate Server to the Root Server residing on the eDirectory tree T1.

Scenario 4: Merging eDirectory Trees

In this configuration, you can merge the inventory trees and the eDirectory trees. After you merge the eDirectory trees, you must manually change the eDirectory tree name and (optionally) the

Inventory Service DN in the *Inventory_server_installation_drive or volume\zenworks\inv\server\wminv\properties\config.properties* file before starting the Inventory service. For more information on merging the eDirectory trees, see the [Novell eDirectory documentation Web site \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

To merge the inventory trees, you must change the role of the Root Server of one inventory tree to roll up to an Inventory server in the other inventory tree.

To change the eDirectory tree name and the DN of an Inventory server, edit the following entries of the *config.properties* file:

```
NDSTree=Target_eDirectory_tree_name
```

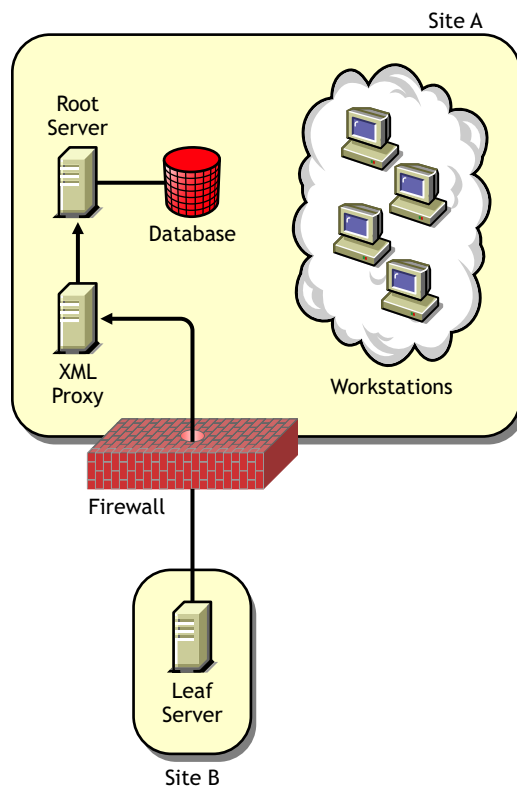
```
InventoryServiceDN=New_DN_of_the_Inventory_server
```

Scenario 5: Deploying Inventory Server Across a Firewall

There are two sites; Site A and Site B connected through a WAN link. The Inventory server of Site A rolls up to an Inventory server in Site B. All communication from Site A to Site B flows through the firewall at Site B.

The following illustration depicts a sample scenario where you can deploy this inventory configuration:

Figure 73-9 Deploying Inventory Server across a Firewall



To enable the roll-up:

- Install an XML proxy at Site A. For more information about installing the proxy, see the *Novell ZENworks 7 Desktop Management Installation Guide*.

- You must have at least one XML proxy/site installed. One proxy server can handle requests for multiple Inventory servers.
- You can configure the port that the proxy listens to during the ZENworks 7 Desktop Management installation. For more information, see the *Novell ZENworks 7 Desktop Management Installation Guide*.

You must allow requests to the proxy server on this port at the firewall. You can configure the XML proxy to listen to standard ports allowed by your firewall.

The XML proxy does not support any commercial Web server. You must make sure that the port number assigned to the XML proxy is not used by any other service on the same server.

You must also configure the Roll-Up policy with the XML proxy server's address and port number.

Deployment Options for Inventory Agent

Before installing the Inventory Agent on your workstation, you must deploy the Inventory servers to receive workstation scans. For more information about the deployment options for Inventory Agent, see *"Deploying the Inventory Agent" on page 910*.

Recommendations for Deployment

- When you configure the inventory scanning of inventoried workstations, we recommend staggering the inventory scanning to scan at different times or to scan a group of inventoried workstations at a time.
- If many inventoried workstations are attached to the same Inventory server, we recommend that you do not schedule the scan of all inventoried workstations at the same time, because this stresses eDirectory and the Inventory service.
- You can attach inventoried workstations to the server as determined by the number of connections supported by Inventory servers up to a maximum of 5,000 inventoried workstations.
- When you schedule the roll-up of information in the Inventory policies, we recommend the roll-up frequency should be at least one day. If the roll-up of inventory information is scheduled too frequently, for example less than one hour, there might be some performance degradation of the Inventory server.
- Use top-down deployment for Inventory installation. Always begin the installation at the topmost level server and proceed with the next lower-level servers. For example, in an inventory setup with a Root Server and a Leaf Server, complete the inventory installation at the Root Server, and then run the installation for the Leaf Server.
- If an Inventory server must receive Inventory scans either directly from the Inventory servers or through roll-up, you must install ZENworks 7 Desktop Management on this server.
- We recommend that you configure DNS for your Inventory and database servers. If you have not configured DNS, choose the IP address in the Roll-Up and Database Location policies. Scheduling the frequency of information gathering and roll-up must be fine-tuned based on the Root Server. Make sure that the Root Server is able to handle the load of the `.str` files.

Installing Workstation Inventory

For detailed information on installing Workstation Inventory, see the *Novell ZENworks 7 Desktop Management Installation Guide*.

Understanding the Effects of Workstation Inventory Installation

For detailed information on the effects of Workstation Inventory installation, see [Section 73.1.4, “Understanding the Effects of Workstation Inventory Installation,”](#) on page 913.

Configuring the Required Policies

The following table lists the actions that you should follow to set up the server for Workstation Inventory:

Table 73-2 *Policies Required to set up an Inventory Server*

To set up this type of server:	Do this:
Standalone Server	<ol style="list-style-type: none">1. Follow the steps in Section 73.5, “Configuring the Database Location Policy,” on page 9572. Follow the steps in Section 73.6, “Configuring the Workstation Inventory Policy,” on page 958
Root Server	<ol style="list-style-type: none">1. Follow the steps in Section 73.3, “Configuring the Inventory Service Object,” on page 9552. Follow the steps in Section 73.5, “Configuring the Database Location Policy,” on page 957
Root Server with Inventoried Workstations	<ol style="list-style-type: none">1. Follow the steps in Section 73.3, “Configuring the Inventory Service Object,” on page 9552. Follow the steps in Section 73.6, “Configuring the Workstation Inventory Policy,” on page 958.3. Follow the steps in Section 73.5, “Configuring the Database Location Policy,” on page 957
Intermediate Server	<ol style="list-style-type: none">1. Follow the steps in Section 73.3, “Configuring the Inventory Service Object,” on page 955.2. Follow the steps in Section 73.7, “Configuring the Roll-Up Policy,” on page 960.
Intermediate Server with Database	<ol style="list-style-type: none">1. Follow the steps in Section 73.3, “Configuring the Inventory Service Object,” on page 955.2. Follow the steps in Section 73.7, “Configuring the Roll-Up Policy,” on page 960.3. Follow the steps in Section 73.5, “Configuring the Database Location Policy,” on page 957.
Intermediate Server with Inventoried Workstations	<ol style="list-style-type: none">1. Follow the steps in Section 73.3, “Configuring the Inventory Service Object,” on page 955.2. Follow the steps in Section 73.6, “Configuring the Workstation Inventory Policy,” on page 958.3. Follow the steps in Section 73.7, “Configuring the Roll-Up Policy,” on page 960.

To set up this type of server:	Do this:
Intermediate Server with Database and Inventoried Workstations	<ol style="list-style-type: none"> 1. Follow the steps in Section 73.3, “Configuring the Inventory Service Object,” on page 955. 2. Follow the steps in Section 73.6, “Configuring the Workstation Inventory Policy,” on page 958. 3. Follow the steps in Section 73.7, “Configuring the Roll-Up Policy,” on page 960. 4. Follow the steps in Section 73.5, “Configuring the Database Location Policy,” on page 957.
Leaf Server	<ol style="list-style-type: none"> 1. Follow the steps in Section 73.3, “Configuring the Inventory Service Object,” on page 955. 2. Follow the steps in Section 73.6, “Configuring the Workstation Inventory Policy,” on page 958. 3. Follow the steps in Section 73.7, “Configuring the Roll-Up Policy,” on page 960.
Leaf Server with Database	<ol style="list-style-type: none"> 1. Follow the steps in Section 73.3, “Configuring the Inventory Service Object,” on page 955. 2. Follow the steps in Section 73.6, “Configuring the Workstation Inventory Policy,” on page 958. 3. Follow the steps in Section 73.7, “Configuring the Roll-Up Policy,” on page 960. 4. Follow the steps in Section 73.5, “Configuring the Database Location Policy,” on page 957.

Starting the Inventory Service

After installing ZENworks 7 Desktop Management, the Inventory service is automatically started only if you have configured the Inventory Standalone Configuration settings during the installation.

To manually start the Inventory service, see [Section 73.1.5, “Starting and Stopping the Inventory Service,”](#) on page 915.

Updating the Software Dictionary

You can update the software dictionary in any one of the following ways:

- On each Inventory server, manually download the latest version of the dictionary from TID 10093255 in the [Novell Support Knowledgebase](http://www.novell.com/support) (<http://www.novell.com/support>) and update the software dictionary.
- Manually download the latest version of the dictionary from TID 10093255 in the [Novell Support Knowledgebase](http://www.novell.com/support) (<http://www.novell.com/support>) on an Inventory server (preferably, the Root Server) and automatically distribute the dictionary to all servers in your setup by configuring the [Section 73.8, “Configuring the Dictionary Update Policy,”](#) on page 961. For more information, see [Section 73.9, “Setting Up Distribution of Dictionary,”](#) on page 962.

NOTE: The dictionary is updated and published once in every three months in this TID.

Understanding Rolling Up Inventory Information Across Servers

If the inventory deployment rolls up inventory information across servers, the process of scanning is as follows:

1. The Inventory policies in eDirectory define the inventory settings, such as scanning time and the location of the scan directory. These settings can be customized.
2. The Scanner reads the Inventory policies and collects the workstation inventory information. The Inventory scanner also checks whether an updated dictionary is available at its Inventory server and downloads the updated dictionary.

If the Novell Client is not installed on the inventoried workstation, the Scanner accesses eDirectory through the ZENworks 7 Desktop Management Middle Tier Server.

3. The Scanner stores the inventory information of each inventoried workstation as a scan data file in the scan directory at the Inventory server.

If the Novell Client is not installed on the inventoried workstation, the Scanner sends the inventory information of each inventoried workstation to the Inventory server through the ZENworks 7 Desktop Management Middle Tier Server.

4. The Scanner stores the minimal inventory information of the inventoried workstation in the respective workstation objects in the respective workstation objects in eDirectory.

If the Novell Client is not installed on the inventoried workstation, the Scanner accesses eDirectory through the ZENworks 7 Desktop Management Middle Tier Server.

5. The Selector validates the `.str` file and places the file in the enterprise merge directory for roll-up of inventory information. If there is a database attached, the Selector places the files in the database directory also.
6. The Sender on the server has a Roll-Up policy to identify the server to which it transmits the inventory information and the Roll-Up Schedule specifies a time for roll-up of information. The Sender compresses the `.str` files as a `.zip` file and places the `.zip` file in the enterprise push directory (`entpushdir`). The Sender then sends the `.zip` file to the Receiver on the next-level server.
7. The Receiver on the next-level server receives the `.zip` file.

NOTE: The next-level Inventory server can be located on the same eDirectory tree or on a different eDirectory tree or across firewalls.

On the Intermediate Server, the Receiver copies the file in the enterprise push directory. On the Intermediate Server with Database, or the Intermediate Server with Database and Inventoried Workstations, the Receiver copies the file in `entpushdir` and copies the file in the Database Directory.

On the Root Server, or the Root Server with Inventoried Workstations, the Receiver copies the file in `dbdir` only.

8. The Storer extracts the `.zip` file containing the `.str` files in to a temp directory (`dbdir\temp`) and updates the database with the inventory information of the inventoried workstation `.str` file.
9. The ZENworks administrator views the inventory information, queries the database, generates inventory reports, and performs other Inventory based tasks in ConsoleOne.

The following illustrations depict the inventory scanning cycle in the Roll-Up scenario, both with and without the Novell Client installed.

Figure 73-10 Inventory scanning cycle in the Roll-Up scenario with the Novell Client installed

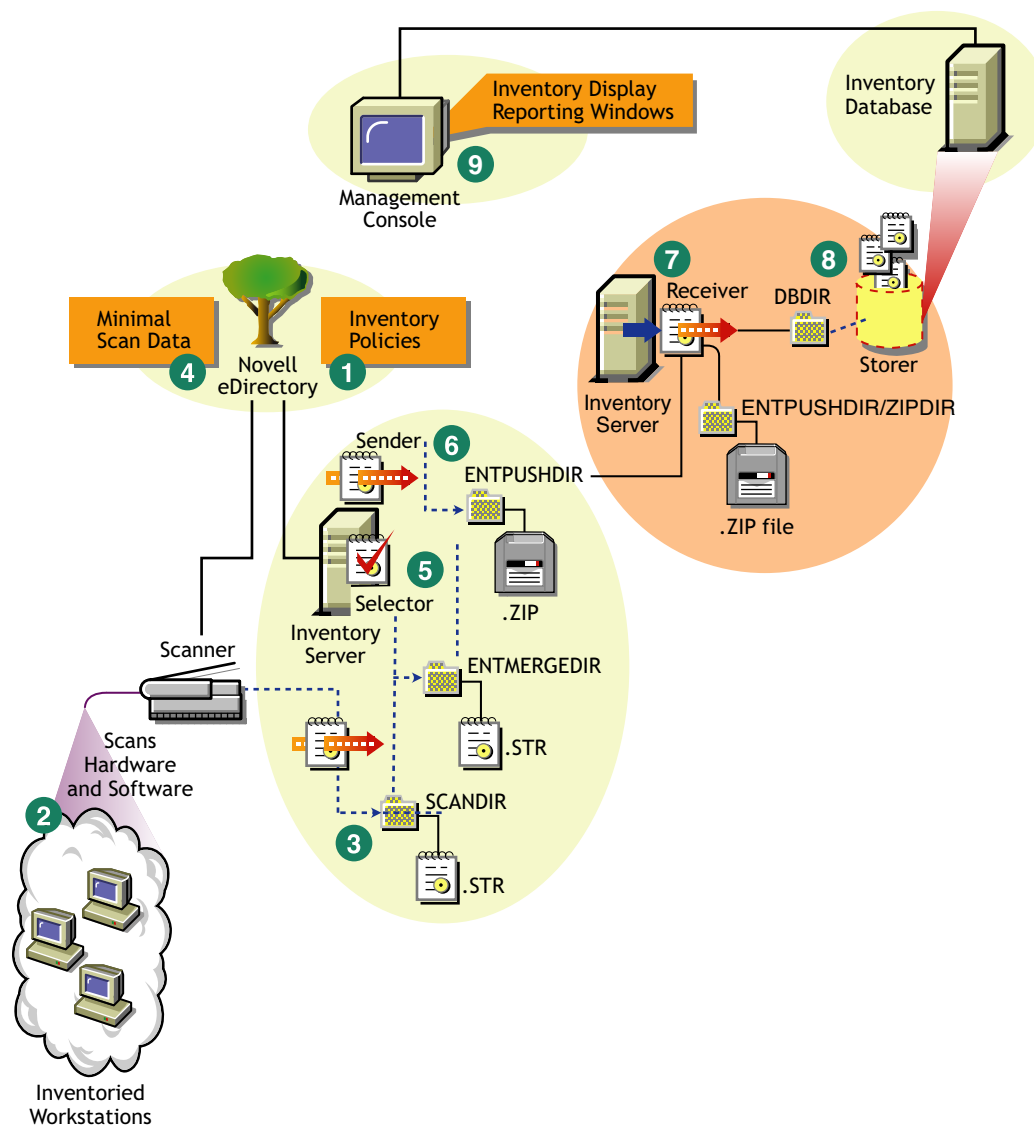
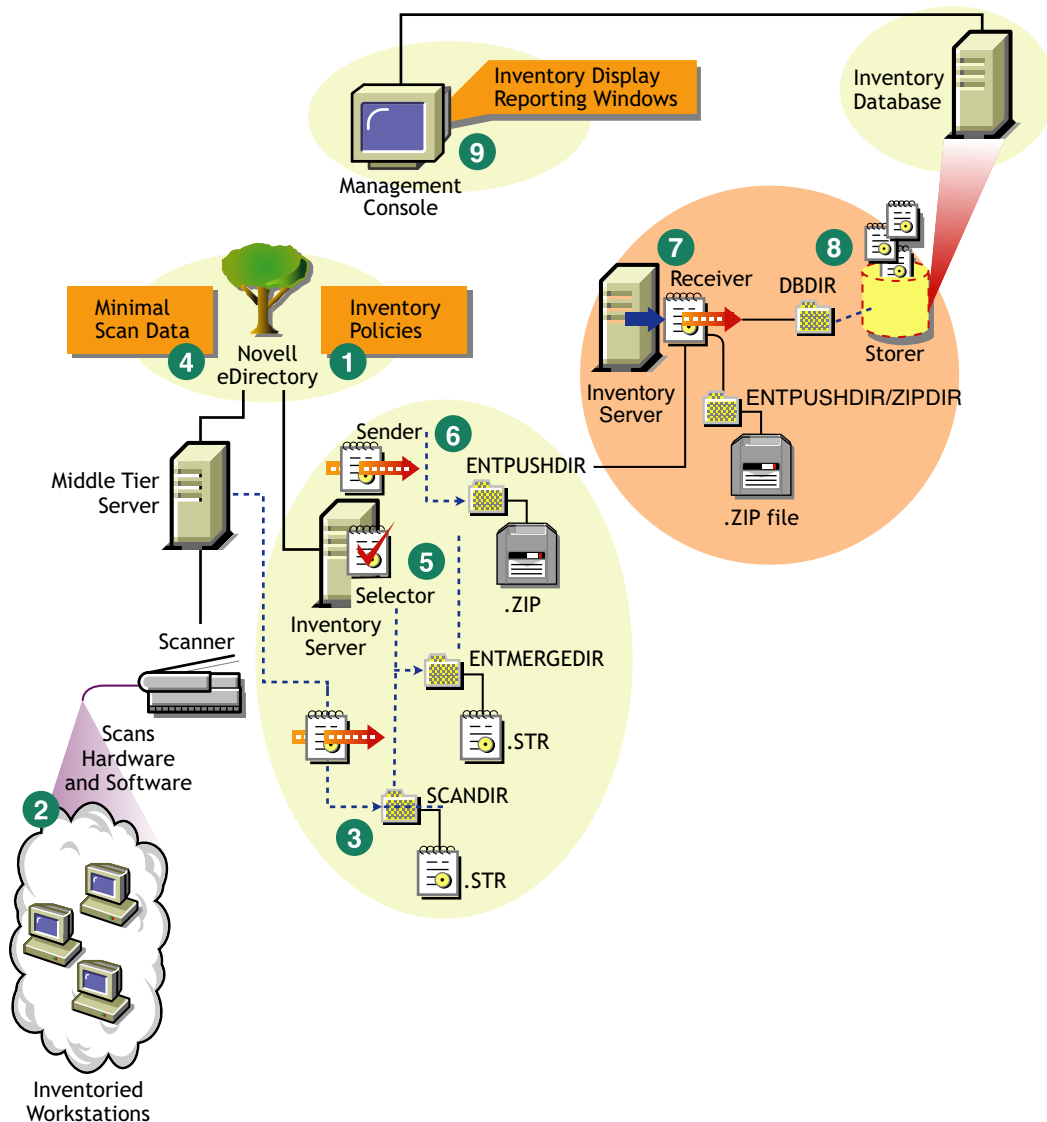


Figure 73-11 Inventory scanning cycle in the Roll-Up scenario without the Novell Client installed



73.1.3 Deploying the Inventory Agent

Before installing the Inventory Agent on your workstations, you must deploy the Inventory servers to receive workstation scans.

IMPORTANT: Before deploying Inventory Agent, we recommend that you customize your software scan rules to create a base-line configuration. For more information, see [Section 76.2, "Customizing the Hardware Inventory Information To Be Scanned,"](#) on page 1022.

You can deploy the Inventory Agent in the following scenarios:

- "Scenario 1: Deploying the Inventory Agent on Workstations that are in the Same LAN as the Inventory Server" on page 911

- “Scenario 2: Deploying the Inventory Agent on Workstations that Send Scans over a WAN across the Firewall” on page 911
- “Scenario 3: Deploying Inventory Agent on Workstations that Are Periodically Connected to the Network” on page 912
- “Scenario 4: Deploying Inventory Agent on Workstations that Are Never Connected to the Network” on page 913

Scenario 1: Deploying the Inventory Agent on Workstations that are in the Same LAN as the Inventory Server

In this scenario, the inventoried workstations and the Inventory server are in the same LAN environment.

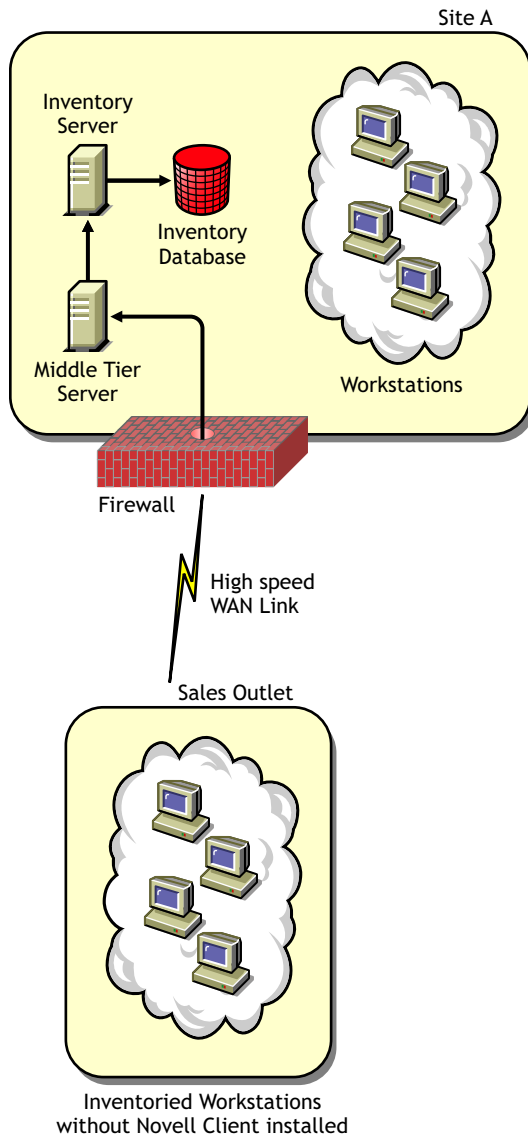
- If the Novell Client is installed on inventoried workstations or if you plan to install the Novell Client on inventoried workstations before installing the ZENworks 7 Desktop Management - Inventory Agent:
 - Install the ZENworks 7 Desktop Management Inventory Agent on inventoried workstations. For more information, see the *Novell ZENworks 7 Desktop Management Installation Guide*.
The Inventory Agent directly sends the scans to the Inventory server.
 - You can configure a maximum of 5000 inventoried workstations to send scans to an Inventory server.
- If the Novell Client is not installed on inventoried workstations or if you do not plan to install the Novell Client on inventoried workstations before installing the ZENworks 7 Desktop Management Inventory Agent:
 - Install the ZENworks 7 Desktop Management Inventory Agent, which works in the clientless mode. The Inventory Agent routes the requests through the Middle Tier. For more information, see the *Novell ZENworks 7 Desktop Management Installation Guide*.
 - You must have one ZENworks 7 Desktop Management Middle Tier Server for each site. For more information, see the *Novell ZENworks 7 Desktop Management Installation Guide*.
 - You can configure a maximum of 5000 workstations to send scans to an Inventory server.

Scenario 2: Deploying the Inventory Agent on Workstations that Send Scans over a WAN across the Firewall

Consider a scenario where there are two sites, A and B, that are connected via a WAN link. All communication from Site B to Site A goes through the firewall at Site A. Site B has five workstations with the Inventory Agent installed, and they do not have the Novell Client installed. The five workstations must be inventoried and the scan must be sent directly to the Inventory server at Site A. You must install the Middle Tier Server at Site A. For more information, see the *Novell ZENworks 7 Desktop Management Installation Guide*. Site B must be connected to Site A through a fast WAN link. This should have sufficient bandwidth to handle traffic generated by the workstations when accessing policies in the eDirectory and sending scans to the Inventory server.

The following illustration depicts a sample scenario where you can deploy this inventory configuration

Figure 73-12 Deploying the Inventory Agent on Workstations that send scans over a WAN across the Firewall



Scenario 3: Deploying Inventory Agent on Workstations that Are Periodically Connected to the Network

In this scenario, the Inventory Agent is installed on workstations that periodically connect to the network.

The inventoried workstations are connected periodically to the network. The workstation policies are refreshed when the inventoried workstation connects to the network. If the scan schedule expires, the Inventory Agent defers scanning the inventoried workstation until the workstation is connected to the network.

We recommend that you set your scan schedule to match when the inventoried workstation connects to the network.

For more information, see [Section 76.5, “Scanning for Workstations That Are Periodically Connected to the Network,”](#) on page 1081.

Scenario 4: Deploying Inventory Agent on Workstations that Are Never Connected to the Network

In this scenario, the Inventory Agent is installed on workstations that are never connected to the network. For more information, see [“Collecting Inventory for Workstations That Are Not Connected to the Network”](#) on page 1082.

73.1.4 Understanding the Effects of Workstation Inventory Installation

On the Inventory servers, the Workstation Inventory installation program does the following:

On NetWare Inventory Servers

- Copies the Workstation Inventory related files to the *installation_volume*.
- Copies the Workstation Inventory snap-ins to the ConsoleOne[®] directory.
- Creates an Inventory Service object (Inventory Service_ *server_name*) in eDirectory for each server on which Inventory server is installed. This object is populated with the following attributes: *zeninvRole* (role of the server), *zeninvScanFilePath* (path to the *scandir* directory), *zeninvHostServer* (DN of the server on which Inventory server is installed), and *zeninvDictionarypath* (Path to the dictionary directory).
- If the Inventory Service object already exists, the object is validated and re-created again if it is invalid.
- During installation, the Inventory Service object is made a trustee of the NCP[™] server with Compare and Read rights.
- Assigns the Inventory Service object as trustee to itself.
- Creates the scan directory with the subdirectories in the specified volume on the Inventory server. [Root] is granted the Create rights to this directory.
- Creates a dictionary directory (*dictdir*), and copies the files of general dictionary and private dictionary. [Root] is granted the Read and Write rights to this directory.
- Creates the *zenworks.properties* file in *sys:\system*. This file contains the installation path of the Inventory server and the ZEN Web server.
- During the Workstation Inventory installation, if you have configured Inventory Standalone Configuration settings, then the Inventory Service Manager is automatically started.
- Installs the ZEN Web server on the Inventory server, if it is not installed already.
- If Workstation Inventory is reinstalled in the same directory as the previous installation, the *config.properties* and *directory.properties* files are backed up and re-created.

On Windows Inventory Servers

- Copies the Workstation Inventory related files to the *installation_directory*.
- Copies the Workstation Inventory snap-in component to the ConsoleOne directory.
- Creates the scan directory with the subdirectories in the specified directory on the Inventory server, and creates a share with Create rights to this directory for all users.

- Creates a dictionary directory (`dictdir`), copies the files of general dictionary and private dictionary, and grants Read and Write rights to this directory for all users.
- Creates an Inventory Service object (Inventory Service *server_name*) in eDirectory for each server on which Inventory server is installed. This object is populated with the following attributes: `zeninvRole` (role of the server), `zeninvScanFilePath` (path to the `scandir` directory), `zeninvHostServer` (DN of the server on which Inventory server is installed) and `zeninvDictionarypath` (Path to the dictionary directory).
- If the Inventory Service object (Inventory Service *server_name*) already exists, the object is validated and re-created again if it is invalid.
- During installation, the Inventory Service object is made a trustee of the NCP server with Compare and Read rights.
- Assigns the Inventory Service object as trustee to itself.
- The Inventory Service Manager is created as a service.
- Edits the Registry settings to add the installation path of the Inventory server and the ZEN Web server.
- On the Inventory server, the ZENworks Service Management is created as a service.
- If the Workstation Inventory is reinstalled in the previous installation directory, the `config.properties` and `directory.properties` files are backed up and re-created.

On Linux Inventory Servers

- Copies the Workstation Inventory related files through the `novell-zenworks-invserver` and `novell-zenworks-invrcommon` RPMs.
- Creates an inventory user in the inventory and zenworks groups.
- Creates a scan directory (`/opt/novell/zenworks/inv/ScanDir`) with the subdirectories, assigns read and execute permissions for all the directories in the path of `ScanDir` and creates a samba share with Create rights to this directory for all users.
- Creates a dictionary directory (`/opt/novell/zenworks/inv/server/DictDir`), copies the files of general directory and private dictionary, and grants Read and Write rights to this for all users.
- Creates an Inventory Service object (Inventory Service *server_name*) in eDirectory for each server on which Inventory server is installed. This object is populated with the following attributes: `zeninvRole` (role of the server), `zeninvScanFilePath` (path to the `scandir` directory), `zeninvHostServer` (DN of the server on which Inventory server is installed) and `zeninvDictionarypath` (Path to the dictionary directory).
- Creates the NCP shares for the `ScanDir` and `DictDir` volumes of OES.
- Creates the Inventory server as a daemon in `/etc/init.d/novell-zdm-inv`, and adds it to be started when the server boots.

On Database Servers

- Installs the Sybase database on the server you specify.
- At server startup time, the database is loaded.
- On NetWare, the `mgmt.db` entries are added to the `sys:\system\mgmt.dbs.ncf` file. On Windows, the `mgmt.db` entries are added to the registry.

- Creates two database objects (Inventory database_ *server_name* and Desktop Management database_ *server_name*_) for Sybase and configures the properties of the object.
- If the database server is installed in the previous installation directory, the database files are re-created if they were found invalid or non-existing.
- If Sybase is already installed, only the database files are copied.

73.1.5 Starting and Stopping the Inventory Service

The section provides information on:

- “Starting the Inventory Service on a NetWare Inventory Server” on page 915
- “Stopping the Inventory Service on a NetWare Inventory Server” on page 915
- “Starting the Inventory Service on a Windows Inventory Server” on page 915
- “Stopping the Inventory Service on a Windows Inventory Server” on page 916
- “Starting the Inventory Service on a Linux Inventory Server” on page 916
- “Stopping the Inventory Service on a Linux Inventory Server” on page 917

For more information about the various Inventory services, see [Section 74.1, “Understanding the Inventory Service Manager,” on page 965](#).

Starting the Inventory Service on a NetWare Inventory Server

Before you start the Inventory service, make sure that the Inventory database is up and running. The Inventory database is automatically started after the installation.

To start the Inventory service on the NetWare Inventory server, enter `startinv` at the server console prompt.

To start an Inventory service, enter `startser inventory_service_name` at the server console prompt. For more information about different Inventory services, see [“List of Services” on page 966](#).

After starting the Inventory service, make sure that the Inventory services are up and running. To list all services, enter `listser *` at the server console prompt. To list an Inventory service, enter `listser inventory_service_name` at the server console prompt.

If the services are not up and running, check the Server Status log. For more information on the Server Status log, see [Section 78.4, “Viewing the Status of Inventory Components on a Server,” on page 1179](#).

Stopping the Inventory Service on a NetWare Inventory Server

To stop an Inventory service, enter `stopser inventory_service_name` at the server console prompt.

To stop all the Inventory services, enter `stopser *` at the server console prompt.

Starting the Inventory Service on a Windows Inventory Server

Before you start the Inventory service, make sure that the Inventory database is up and running. The Inventory database is automatically started after the installation.

To start the Inventory services on the Windows 2000/2003 Inventory server:

- 1 In the Control Panel, double-click Administrative Tools.
- 2 Double-click Services.
- 3 Select Novell Inventory Service, then click Start.

To start an Inventoryservice from the console prompt:

- 1 Go to the `installation_directory\inv\server\wminv\bin` directory.
- 2 At the prompt, enter `startser inventory_service_name`.

After starting the Inventory service, make sure that the Inventory services are up and running. To list all services, enter `listser "*"` at the server console prompt. To list an Inventory service from the console prompt:

- 1 Go to the `installation_directory\inv\server\wminv\bin` directory.
- 2 At the prompt, enter `listser inventory_service_name`.

If the services are not up and running, check the Server Status log. For more information on the Server Status log, see [Section 78.4, “Viewing the Status of Inventory Components on a Server,” on page 1179](#).

Stopping the Inventory Service on a Windows Inventory Server

To stop the Inventory services on a Windows 2000/2003 Inventory server:

- 1 In the Control Panel, double-click Administrative Tools.
- 2 Double-click Services.
- 3 Select Novell Inventory Service, then click Stop.

To stop an Inventory service on a Windows Inventory server from the console prompt:

- 1 Go to the `installation_directory\inv\server\wminv\bin` directory.
- 2 Enter `stopser inventory_service_name`.

Starting the Inventory Service on a Linux Inventory Server

- To start all Inventory services, do any of the following ways:

1. At the Linux server prompt, go to `/etc/init.d`.
2. Enter `./novell-zdm-inv start`.

Or

To start all Inventory services from any directory on Linux, enter

```
/etc/init.d/novell-zdm-inv start
```

- To start a specific Inventory service:

1. At the Linux server prompt, go to `/opt/novell/bin`.
2. Enter `StartSer Inventory_service`.

Stopping the Inventory Service on a Linux Inventory Server

- To stop all Inventory services, do any of the following ways:

1. At the Linux server prompt, go to `/etc/init.d`.
2. Enter `./novell-zdm-inv stop`.

Or

To stop all Inventory services from any directory on Linux, enter

```
/etc/init.d/novell-zdm-inv stop
```

- To stop a specific Inventory service:

1. At the Linux server prompt, go to `/opt/novell/bin`.
2. Enter `StopSer Inventory_service`.

73.1.6 Checking the Status of the Workstation Inventory Components Installed on Linux

The following table lists the Workstation Inventory components installed on Linux whose status you can check by executing commands at the Linux console prompt.

Table 73-3 *Commands to check the status of Workstation Inventory components installed on Linux*

Workstation Inventory Component	Command To Be Entered At the Linux Console Prompt
Inventory server daemon	<code>/etc/init.d/novell-zdm-inv status</code>
Sybase daemon	<code>/etc/init.d/novell-zdm-sybase status</code>
Inventory Proxy daemon	<code>/etc/init.d/novell-zen-zws status</code>

73.1.7 Changing the Role of the Inventory Server

When you install ZENworks 7 Desktop Management, by default, the role of the Inventory server is that of a Standalone. By configuring the Inventory Service object, you can assign specific roles to the Inventory server based on your inventory deployment.

For example, if the deployment plan identifies three servers, such as a Root Server, an Intermediate Server with Database, and a Leaf Server for inventory deployment, you install Workstation Inventory on these servers, and choose the role for the server. Later, if you want to make changes in the inventory deployment, such as attaching the inventoried workstations to the existing Root Server, you need to change the role of the Inventory Service object from Root Server to Root Server with Inventoried Workstations. Additionally, depending on the new role, there are some policies you need to configure.

To change the role for any Inventory server:

- 1 Plan the change of roles carefully because the changes impact the existing inventory deployment. Also, consider the disk space requirements and make sure that you have the required configurations for Inventory.

- 2 In ConsoleOne, right-click the Inventory Service object (Inventory Service_<server_name>), click *Properties*, then click the *Inventory Service Object Properties* tab.
 - 3 Choose the new role of the Inventory Service object, then click *Apply*.
 - 4 Bring down the services running on the changed server, follow the actions that you need to change the role, and then bring up the server.
- For detailed information about how to stop and restart the Inventory service, see [Section 73.1.5, “Starting and Stopping the Inventory Service,”](#) on page 915.

The following sections contain information to help you change the role of the Inventory Service object:

- [“Changing the Role of the Root Server”](#) on page 918
- [“Changing the Role of the Root Server with Inventoried Workstations”](#) on page 919
- [“Changing the Role of the Intermediate Server”](#) on page 920
- [“Changing the Role of the Intermediate Server with Database”](#) on page 922
- [“Changing the Role of the Intermediate Server with Database and Inventoried Workstations”](#) on page 922
- [“Changing the Role of the Intermediate Server with Inventoried Workstations”](#) on page 923
- [“Changing the Role of the Leaf Server”](#) on page 925
- [“Changing the Role of the Leaf Server with Database”](#) on page 926
- [“Changing the Role of the Standalone Server”](#) on page 927

Changing the Role of the Root Server

To change the role of the Root Server to a different role, perform the actions specified in the following table:

Table 73-4 Tasks to be performed to change the role of the Root Server

To change the role of the Root Server to ...	Tasks:
Root Server with Inventoried Workstations	<p>Perform the following tasks after changing the role:</p> <ol style="list-style-type: none"> 1. Configure the Workstation Inventory Policy so that the inventoried workstations that you have attached to the Root Server with Inventoried Workstations are scanned for. 2. Make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server. This setting ensures that a complete scan of the inventoried workstations attached to is done.
Intermediate Server	<p>Perform the following tasks:</p> <ol style="list-style-type: none"> 1. Before changing the role, remove the Database Location policy associated with the Root Server. 2. After changing the role, configure the Roll-Up policy to specify the next-destination server for roll-up of information from this server.

To change the role of the Root Server to ...	Tasks:
Intermediate Server with Database	<p>Perform the following task:</p> <ol style="list-style-type: none"> 1. After changing the role, configure the Roll-Up policy to specify the next-destination server for roll-up of information from this server.
Intermediate Server with Database and Inventoried Workstations	<p>Perform the following tasks after changing the role:</p> <ol style="list-style-type: none"> 1. Configure the Workstation Inventory Policy so that the inventoried workstations that you have attached are scanned for. 2. Make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server. This setting ensures that a complete scan of the inventoried workstations is done. 3. Configure the Roll-Up policy to specify the next-destination server for roll-up of information from this server.
Intermediate Server with Inventoried Workstations	<p>Perform the following tasks:</p> <ol style="list-style-type: none"> 1. Before changing the role, remove the Database Location policy associated with the Root Server. 2. After changing the role, configure the Workstation Inventory Policy so that the inventoried workstations that you have attached are scanned for. 3. After changing the role, make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server. This setting ensures that a complete scan of the inventoried workstations is done. 4. After changing the role, configure the Roll-Up policy to specify the next-destination server for roll-up of information from this server.
Leaf Server, Leaf Server with Database, or Standalone Server	<p>Workstation Inventory does not allow you to change the Root Server to these servers because these changes affect the complete inventory system. If you want to assign these roles, you must uninstall Workstation Inventory, and then reinstall the Workstation Inventory component.</p>

Changing the Role of the Root Server with Inventoried Workstations

Perform the actions specified in the following table:

Table 73-5 Tasks to be performed to change the role of the Root Server with Inventoried Workstations

To Change the Role of the Root Server with Inventoried Workstations to ...	Tasks:
Root Server	<p>Perform the following task before changing the role:</p> <ol style="list-style-type: none"> 1. Remove the Workstation Inventory policy associated with the Root Server with Inventoried Workstations.

To Change the Role of the Root Server with Inventoried Workstations to ...**Tasks:**

Intermediate Server

Perform the following tasks:

1. Before changing the role, remove the Database Location policy associated with the Root Server with Inventoried Workstations.
2. Before changing the role, if the Workstation Inventory policy is associated with the Root Server with Inventoried Workstations, remove the policy for those inventoried workstations attached to this server.
3. After changing the role, configure the **Roll-Up policy** to specify the next-destination server for roll-up of information from this server.

Intermediate Server with Database

Perform the following tasks:

1. Before changing the role, if the Workstation Inventory policy is associated with the Root Server with Inventoried Workstations, remove the policy for those inventoried workstations attached to this server.
2. After changing the role, configure the **Roll-Up policy** to specify the next-destination server for roll-up of information from this server.

Intermediate Server with Database and Inventoried Workstations

Perform the following tasks after changing the role:

1. Make sure that you enable the Full Scan setting in the **Inventory Service Object property page** for the server. This setting ensures that a complete scan of the inventoried workstations is done.
2. Configure the **Roll-Up policy** to specify the next-destination server for roll-up of information from this server.

Intermediate Server with Inventoried Workstations

Perform the following task before changing the role:

1. Remove the Database Location policy associated with the Root Server with Inventoried Workstations.

Leaf Server, Leaf Server with Database, or Standalone server

Workstation Inventory does not allow you to change the Root Server to these servers because these changes affect the complete inventory system. If you want to assign these roles, you must uninstall Workstation Inventory, and then reinstall the Workstation Inventory component.

Changing the Role of the Intermediate Server

Perform the actions specified in the following table:

Table 73-6 Tasks to be performed to change the role of the Intermediate Server

To Change the Role of the Intermediate Server to ...	Tasks:
Root Server	<p>Perform the following tasks:</p> <ol style="list-style-type: none"> 1. Before changing the role, remove the Roll-Up policy associated with the Intermediate Server. 2. After changing the role, configure the Database Location policy. 3. After changing the role, make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server.
Root Server with Inventoried Workstations	<p>Perform the following tasks:</p> <ol style="list-style-type: none"> 1. Before changing the role, remove the Roll-Up policy associated with the Intermediate Server. 2. After changing the role, configure the Workstation Inventory Policy for those workstations attached to this server. 3. After changing the role, configure the Database Location policy. 4. After changing the role, make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server.
Intermediate Server with Database	<p>Perform the following tasks after changing the role:</p> <ol style="list-style-type: none"> 1. Configure the Database Location policy for the server. 2. Make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server
Intermediate Server with Database and Inventoried Workstations	<p>Perform the following tasks after changing the role:</p> <ol style="list-style-type: none"> 1. Configure the Workstation Inventory Policy so that all the inventoried workstations associated to this Inventory Service object are scanned for. 2. Configure the Database Location policy. 3. Make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server.
Intermediate Server with Inventoried Workstations	<p>Perform the following task after changing the role:</p> <ol style="list-style-type: none"> 1. Configure the Workstation Inventory Policy so that the inventoried workstations that you have attached are scanned for.
Leaf Server, Leaf Server with Database, or Standalone server	<p>Workstation Inventory does not allow you to change the Intermediate Server to these servers because these changes affect the complete inventory system. If you want to assign these roles, you must uninstall Workstation Inventory, and then reinstall the Workstation Inventory component.</p>

Changing the Role of the Intermediate Server with Database

Perform the actions specified in the following table:

Table 73-7 Tasks to be performed to change the role of the Intermediate Server with Database

To Change the Role of the Intermediate Server with Database to ...	Tasks:
Root Server	Perform the following task before changing the role: 1. Remove the Roll-Up policy associated with the Intermediated Server with Database.
Root Server with Inventoried Workstations	Perform the following tasks: 1. Before changing the role, remove the Roll-Up policy associated with the Intermediated Server with Database. 2. After changing the role, configure the Workstation Inventory Policy so that the inventoried workstations that you have attached are scanned for.
Intermediate Server	Perform the following task before changing the role: 1. Remove the Database Location policy associated with the Intermediate Server with Database.
Intermediate Server with Database and Inventoried Workstations	Perform the following task after changing the role: 1. Configure the Workstation Inventory Policy so that the inventoried workstations attached are scanned for.
Intermediate Server with Inventoried Workstations	Perform the following tasks: 1. Before changing the role, remove the Database Location policy associated with the Intermediate Server with Database. 2. After changing the role, configure the Workstation Inventory Policy so that the inventoried workstations that you have attached are scanned for.
Leaf Server, Leaf Server with Database, or Standalone server	Workstation Inventory does not allow you to change the Intermediate Server to these servers because these changes affect the complete inventory system. If you want to assign these roles, you must uninstall Workstation Inventory, and then reinstall the Workstation Inventory component.

Changing the Role of the Intermediate Server with Database and Inventoried Workstations

Perform the actions specified in the following table:

Table 73-8 Tasks to be performed to change the role of the Intermediate Server with Database and Inventoried Workstations

To Change the Role of the Intermediate Server with Database and Inventoried Workstations to ...	Tasks:
Root Server	<p>Perform the following tasks before changing the role:</p> <ol style="list-style-type: none"> 1. Remove the Roll-Up policy associated with the Intermediate Server with Database and Inventoried Workstations. 2. Remove the Workstation Inventory policy associated with the server so that the inventoried workstations do not send the scan files to this server.
Root Server with Inventoried Workstations	<p>Perform the following task before changing the role:</p> <ol style="list-style-type: none"> 1. Remove the Roll-Up policy associated with the Intermediate Server with Database and Inventoried Workstations.
Intermediate Server	<p>Perform the following tasks before changing the role:</p> <ol style="list-style-type: none"> 1. Remove the Workstation Inventory policy associated with the lower-level servers that roll up to the Intermediate Server with Database and Inventoried Workstations server. 2. Remove the Database Location policy associated with the Intermediate Server with Database and Inventoried Workstations.
Intermediate Server with Database	<p>Perform the following task before changing the role:</p> <ol style="list-style-type: none"> 1. Remove the Workstation Inventory policy of the Intermediate Server with Database.
Intermediate Server with Inventoried Workstations	<p>Perform the following task before changing the role:</p> <ol style="list-style-type: none"> 1. Remove the Database Location policy associated with the Intermediate Server with Database and Inventoried Workstations.
Leaf Server, Leaf Server with Database, or Standalone Server	<p>Workstation Inventory does not allow you to change the Intermediate Server to these servers because these changes affect the complete inventory system. If you want to assign these roles, you must uninstall Workstation Inventory, and then reinstall the Workstation Inventory component.</p>

Changing the Role of the Intermediate Server with Inventoried Workstations

Perform the actions specified in the following table:

Table 73-9 Tasks to be performed to change the role of the Intermediate Server with Inventoried Workstations

To Change the Role of the Intermediate Server with Inventoried Workstations to ...	Tasks:
Root Server	<p>Perform the following tasks:</p> <ol style="list-style-type: none"> 1. Before changing the role, remove the Roll-Up policy associated with the Intermediate Server with Inventoried Workstations. 2. After changing the role, configure the Database Location policy for the server. 3. After changing the role, make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server.
Root Server with Inventoried Workstations	<p>Perform the following tasks:</p> <ol style="list-style-type: none"> 1. Before changing the role, remove the Roll-Up policy associated with the Intermediate Server with Inventoried Workstations 2. After changing the role, configure the Workstation Inventory Policy for those inventoried workstations attached to the lower-level server that roll up to this server. 3. After changing the role, configure the Database Location policy. 4. After changing the role, make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server.
Intermediate Server	<p>Perform the following task before changing the role:</p> <ol style="list-style-type: none"> 1. Remove the Workstation Inventory policy.
Intermediate Server with Database	<p>Perform the following tasks:</p> <ol style="list-style-type: none"> 1. Before changing the role, remove the Workstation Inventory policy associated to the server attached to this Inventory Service object. 2. After changing the role, configure the Database Location policy for the server. 3. After changing the role, make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server.
Intermediate Server with Database and Inventoried Workstations	<p>Perform the following tasks after changing the role:</p> <ol style="list-style-type: none"> 1. Configure the Database Location policy for the server. 2. Make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server.
Leaf Server, Leaf Server with Database, or Standalone Server	<p>Workstation Inventory does not allow you to change the Intermediate Server to these servers because these changes affect the complete inventory system. If you want to assign these roles, you must uninstall Workstation Inventory, and reinstall the Workstation Inventory component.</p>

Changing the Role of the Leaf Server

Perform the actions specified in the following table:

Table 73-10 Tasks to be performed to change the role of the Leaf Server

To Change the Role of the Leaf Server to ...	Tasks:
Root Server	<p>Perform the following tasks:</p> <ol style="list-style-type: none">1. Before changing the role, remove the Roll-Up policy associated with the Leaf Server.2. Before changing the role, remove the Workstation Inventory policy associated with the server.3. After changing the role, configure the Database Location policy for the Root Server.4. After changing the role, make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server.
Root Server with Inventoried Workstations	<p>Perform the following tasks:</p> <ol style="list-style-type: none">1. Before changing this role, remove the Roll-Up policy associated with the Leaf Server.2. After changing the role, configure the Database Location policy.3. After changing the role, make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server.
Intermediate Server	<p>Perform the following tasks:</p> <ol style="list-style-type: none">1. Before changing the role, remove the Workstation Inventory policy for those inventoried workstations associated with the server or reconfigure.
Intermediate Server with Database	<p>Perform the following tasks:</p> <ol style="list-style-type: none">1. Before changing the role, remove the Workstation Inventory policy for those inventoried workstations associated with the server or reconfigure the policies to send the scans to another Inventory server.2. After changing the role, configure the Database Location policy for the server.3. After changing the role, make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server.
Intermediate Server with Database and Inventoried Workstations	<p>Perform the following tasks after changing the role:</p> <ol style="list-style-type: none">1. Configure the Database Location policy for the server.2. Make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server.

To Change the Role of the Leaf Server to ...	Tasks:
Intermediate Server with Inventoried Workstations	This change of role does not require any specific policy modifications.
Leaf Server with Database	Perform the following tasks after changing the role: <ol style="list-style-type: none"> 1. Configure the Database Location policy for the server. 2. Make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server.
Standalone Server	Perform the following tasks: <ol style="list-style-type: none"> 1. Before changing the role, remove the Roll-Up policy associated with the Leaf Server. 2. After changing the role, configure the Database Location policy for the server.

Changing the Role of the Leaf Server with Database

Perform the actions specified in the following table:

Table 73-11 Tasks to be performed to change the role of the Leaf Server with Database

To Change the Role of the Leaf Server with Database to ...	Tasks:
Root Server	Perform the following tasks: <ol style="list-style-type: none"> 1. Before changing the role, remove the Workstation Inventory policy associated with the Leaf Server with Database. 2. Before changing the role, remove the Roll-Up policy associated with Leaf Server with Database. 3. After changing the role, make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server.
Root Server with Inventoried Workstations	Perform the following tasks: <ol style="list-style-type: none"> 1. Before changing the role, remove the Roll-Up policy associated with the Leaf Server with Database. 2. After changing the role, make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server.
Intermediate Server	Perform the following task: <ol style="list-style-type: none"> 1. Before changing the role, remove the Workstation Inventory policy and the Database Location policy associated with the Leaf Server with Database.

To Change the Role of the Leaf Server with Database to ...	Tasks:
Intermediate Server with Database	Perform the following tasks: <ol style="list-style-type: none"> 1. Before changing the role, remove the Workstation Inventory policy associated with the Leaf Server with Database. 2. After changing the role, make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server.
Intermediate Server with Database and Inventoried Workstations	Perform the following task after changing the role: <ol style="list-style-type: none"> 1. After changing the role, make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server.
Intermediate Server with Inventoried Workstations	Perform the following task before changing the role: <ol style="list-style-type: none"> 1. Remove the Database Location policy associated with the Leaf Server with Database.
Leaf Server	Perform the following task before changing the role: <ol style="list-style-type: none"> 1. Remove the Database Location policy associated with the Leaf Server with Database.
Standalone Server	Perform the following task before changing the role: <ol style="list-style-type: none"> 1. Remove the Roll-Up policy.

Changing the Role of the Standalone Server

Perform the actions specified in the following table:

Table 73-12 Tasks to be performed to change the role of the Standalone Server

To Change the Role of the Standalone Server to ...	Tasks:
Root Server	Perform the following tasks: <ol style="list-style-type: none"> 1. Before changing the role, remove the Workstation Inventory policy associated with the Standalone Server. 2. After changing the role, make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server.
Root Server with Inventoried Workstations	Perform the following task after changing the role: <ol style="list-style-type: none"> 1. After changing the role, make sure that you enable the Full Scan setting in the Inventory Service Object property page for the server.

To Change the Role of the Standalone Server to ...**Tasks:**

Intermediate Server

Perform the following tasks:

1. Before changing the role, remove the Workstation Inventory policy and the Database Location policy associated with the Standalone Server.
2. After changing the role, configure the **Roll-Up policy**.
3. After changing the role, make sure that you enable the Full Scan setting in the **Inventory Service Object property page** for the server.

Intermediate Server with Database

Perform the following tasks:

1. Before changing the role, remove the Workstation Inventory policy associated with the Standalone Server.
2. After changing the role, configure the **Roll-Up policy** to specify the next-destination server for roll-up of information from the Intermediate Server with Database.
3. After changing the role, make sure that you enable the Full Scan setting in the **Inventory Service Object property page** for the server.

Intermediate Server with Database and Inventoried Workstations

Perform the following tasks after changing the role:

1. Configure the **Roll-Up policy** to specify the next-destination server for roll-up of information from the Intermediate Server with Database and Inventoried Workstations.
2. Make sure that you enable the Full Scan setting in the **Inventory Service Object property page** for the server

Intermediate Server with Inventoried Workstations

Perform the following tasks:

1. Before changing the role, remove the Database Location policy associated with the Standalone Server.
2. After changing the role, configure the **Roll-Up policy** to specify the next-destination server for roll-up of information from the Intermediate Server with Workstations.

Leaf Server

Perform the following tasks:

1. Before changing the role, remove the Database Location policy associated with the Standalone Server.
2. After changing the role, configure the **Roll-Up policy** to specify the next-destination server for roll-up of information from the Leaf Server.

Leaf Server with Database

Perform the following task after changing the role:

1. Configure the **Roll-Up policy** to specify the next-destination server for roll-up of information from the Leaf Server with Database.
-

73.2 Setting Up the Inventory Database

This section provides information on the following topics:

- [Section 73.2.1, “Setting Up the Sybase Inventory Database,” on page 929](#)
- [Section 73.2.2, “Setting Up the Oracle Inventory Database,” on page 935](#)
- [Section 73.2.3, “Setting Up the MS SQL Server 2000 or MS SQL Server 2005 Inventory Database,” on page 945](#)

If you want to replace the Inventory database, always stop the Inventory services before replacing the database. Replace the database and restart the Inventory services. For more information, see [Section 73.1.5, “Starting and Stopping the Inventory Service,” on page 915](#).

73.2.1 Setting Up the Sybase Inventory Database

This section provides information on the following topics:

- [“Adding Non-English Enumerated Values for Inventory Attributes into the Inventory Database” on page 929](#)
- [“Manually Creating the Sybase Inventory Database Object” on page 930](#)
- [“Organizing the Sybase Database Spaces on NetWare, Windows, or Linux Servers \(AlterDBSpace Tool\)” on page 931](#)
- [“Understanding the Sybase Database Startup Parameters” on page 933](#)
- [“Backing Up the Sybase Inventory Database” on page 933](#)

Adding Non-English Enumerated Values for Inventory Attributes into the Inventory Database

You need to add the non-English enumerated values so the Inventory report can display the enum value for the inventory attributes in internationalized versions. The non-English enum values must be available in English version of the product so that the rolled-up inventory information from non-English sites can be properly captured at the high-level servers where only English versions are installed.

For more information about the list of attributes that contains enumerated values, see [Appendix P, “Enumeration Values,” on page 1237](#).

To add the non-English enum values:

- 1 Specify the JDBC connection settings in the `connection.prop` to connect to the Sybase database. The file is located in the following directory:

- **On NetWare or Windows:** `zenworks_directory\inv\server\wminv\properties`
- **On Linux:** `/etc/opt/novell/zenworks/inv`

You can do this by copying the template property settings for Sybase specified in the comments section in the `connection.prop` file. Specify the IP address, port number, and Database SID in the JDBC URL string that matches your Sybase server configuration.

- 2 At the server prompt, enter `AddEnums`
`directory_name_containing_connection.prop`

On the Inventory server, run the above command from the following directory:

- **On NetWare or Windows:** `zenworks_directory\inv\server\wminv\bin`
- **On Linux:** `/opt/novell/bin`

After executing the command, the a message indicating that the non-English enums have been successfully inserted is displayed on the console prompt.

Manually Creating the Sybase Inventory Database Object

- 1 In ConsoleOne, right-click in the eDirectory tree where you want to create the database object, click *New*, click *Object*, click *ZENworks Database*, then click *OK*.
- 2 Enter a name for the database object, then click *OK*.
- 3 Configure the Database server options of the Database object.

3a In ConsoleOne, right-click the database object, click *Properties*, then click the *ZENworks Database* tab.

3b Select the database server object using any of the following methods:

- If eDirectory is installed on the database server, in the *Server DN* field, browse for and select the Server object for the server where the database is physically installed and running.

The server's IP address is automatically populated to the *Server IP Address or DNS Name* drop-down list. If the selected server object has more than one IP address, select the appropriate IP address.

To clear the value set in the *Server DN* field, type the IP address of another database server or browse and select another server object.

- If eDirectory is not installed on the database server, enter the server's IP address or the DNS name in the *Server IP Address or DNS Name* field.

3c Type the values for the following options:

- **Database (Read-Write) User Name:** `MW_DBA`
- **Database (Read-Write) Password:** `novell`
- **Database (Read Only) User Name:** `MW_READER`
- **Database (Read Only) Password:** `novell`
- **Database (Write Only) User Name:** `MW_UPDATER`
- **Database (Write Only) Password:** `novell`

IMPORTANT: All Inventory components use the username and password the configured in the database object. By default, "novell" is the password for all options. But you can change it in the database, and update the same here.

3d Click *Apply*.

3e To configure the JDBC Driver properties, click the *JDBC Driver Information* tab.

3f Select *Sybase*, then click *Default Settings*.

This populates the fields with default JDBC driver information.

The database settings for Sybase are:

- **Driver:** `com.sybase.jdbc.SybDriver`

- **Protocol:** *jdbc:*
- **SubProtocol:** *sybase:*
- **SubName:** *Tds:*
- **Port:** 2638
- **Flags:** ?ServiceName=mgmtdb&JCONNECT_VERSION=4
- **Database Service Name:** *the database name specified against the -n Sybase startup parameter while invoking Sybase.*

By default, the value of the *-n* switch is the IP address of the database server. If you retain this switch value, you must enter the same IP address as the database service name.

3g Click *Apply*, then click *Close*.

Organizing the Sybase Database Spaces on NetWare, Windows, or Linux Servers (AlterDBSpace Tool)

If there are more volumes or drives on the multiple physical disks of the database server, placing the Sybase database spaces files on separate volumes or drives improves the performance while accessing the database.

If you install the Sybase database component of ZENworks 7 Desktop Management, the system database file and the database spaces files are installed in the location on the database server you specify. On loading the Inventory database server, the system database file (*mgmtdb.db*) is loaded. this *mgmtdb.db* file references the inventory information in the database spaces files. the database spaces files (*mgmtdb1.db*, *mgmtdb2.db*, *mgmtdb3.db*, *mgmtdb4.db*, *mgmtdb5.db*, *mgmtdb6.db*, *mgmtdb7.db*, *mgmtdb8.db*, *mgmtdb9.db*, *mgmtdb10.db*, and *mgmtdb11.db*) contain the inventory information.

The *alterdb.props* file is installed on the database server in the following location:

- **On Windows:** *inventory_server_installation_directory\wminv\properties*
- **On Linux:** */etc/opt/novell/zenworks/inv*

You can modify the sections in the file to specify the location of the database spaces on the volumes or drives.

The contents of the *alterdb.props* file are as follows:

```
#Database Space Properties
count=11

mgmtdb1=location_of_mgmtdb1
mgmtdb2=location_of_mgmtdb2
mgmtdb3=location_of_mgmtdb3
mgmtdb4=location_of_mgmtdb4
mgmtdb5=location_of_mgmtdb5
mgmtdb6=location_of_mgmtdb6
```

```
mgmtdb7=location_of_mgmtdb7
mgmtdb8=location_of_mgmtdb8
mgmtdb9=location_of_mgmtdb9
mgmtdb10=location_of_mgmtdb10
mgmtdb11=location_of_mgmtdb11
.....
```

To organize the database spaces:

- 1 Make sure that the database is not loaded.
- 2 Make sure that the Inventory Service Manager is not running on the Inventory server.
- 3 Manually move the database spaces files on the Inventory server.

Arrange the database space files in the following way for better performance:

- mgmtdb1 and mgmtdb2 in the same location
- mgmtdb3 and mgmtdb6 in the same location
- mgmtdb5 and mgmtdb7 in the same location
- mgmtdb8 and mgmtdb4 in the same location
- mgmtdb9 and mgmtdb10 in the same location
- mgmtdb11 in a location

IMPORTANT: If you want to move mgmtdb.db to another directory or volume on a network server, update the `sys:\system\mgmt dbs.ncf` file with the new location of the mgmtdb.db.

If you want to move mgmtdb.db to another directory or volume on a Windows server, run the `ntdbconfig.exe` located in the `zenworks\database\dbengine` directory. In the NTDBCONFIG dialog box, enter the new path of mgmtdb.db.

- 4 Modify the location of the eleven database space files in the `alterdb.props` file.

For example,

- On NetWare, enter `mgmtdb3=SYS: \ZENWORKS \ INV \ DB`
- On Windows, enter `mgmtdb3=C: \ZENWORKS \ INV \ DB`
- On Linux, enter `mgmtdb3=/opt/sybase/zenworks/inv/db`

- 5 Load the database.

- On NetWare, enter `mgmt dbs.`
- On Windows, run the database service.
- On Linux, enter `/etc/init.d/novell-zdm-sybase start.`

Ignore the error messages displayed on the console. These messages are displayed because the database spaces files are not loaded.

- 6 Make sure that the Database Location policy has been configured.

7 On the Inventory server console, run the AlterDBSpace service by entering the following command at the server prompt:

- On NetWare or Windows: Enter `StartSer AlterDBSpace`.
- On Linux: Go to `/opt/novell/bin`, then enter `StartSer AlterDBSpace`.

On the Inventory server, the AlterDBSpace tool runs as a service.

You will see a message that the database is adjusted.

8 Exit the database and then load the database.

Make sure that while loading the database there are no errors. Errors indicate that the specified location of the database space files is incorrect or does not exist. Make sure that the path of the database spaces is correct in the `alterdb.props` file and repeat the procedure to organize the database spaces.

IMPORTANT: If you place the database spaces in different volumes or drives, the log file should be placed in the same volume or drive as the System database file (`mgmtdb.db`).

Understanding the Sybase Database Startup Parameters

The startup parameters of the Sybase database are as follows:

- **-c:** Sets the initial memory reserves for caching database pages and other server information. For example, `-c 32M` reserves 32 MB cache size.
- **-gc:** Sets the maximum length of time in minutes that the database server runs without doing a checkpoint on each database. The default value is 60 minutes. For example, `-gc 120` sets the checkpoint time as 120 minutes.
- **-gn:** Sets the number of execution threads to be used in the database server.
- **-m:** Deletes the transaction log when a checkpoint is done, either at shutdown or as a result of a checkpoint scheduled by the server.
- **-n:** Specifies the host name of the database server. For example, `-n IP_address`.
- **-ti:** Disconnects the connections that have not submitted a request for a certain number of minutes. The default is 240 (4 hours). A client machine in the middle of the database transaction locks until the transaction ends or the connection terminates. The `-ti` option is provided to disconnect inactive connections and to free their locks. For example, specify `-ti 400`.
- **-x:** Specifies a communication link. For example, `-x tcpip` indicates a TCP/IP link.
- **-ct:** Enables character set translation by converting strings between character sets that represent the same characters but at different values. This is useful when the client machine and the database use different character sets.
- **-gss:** Sets the stack size per internal execution thread in the server.
- **database_installation_path:** Specifies the installation path of the Inventory database. For example, `c:\zenworks\inv\db\mgmtdb.db`.

Backing Up the Sybase Inventory Database

Workstation Inventory provides a utility, Database Backup, to back up the Sybase Inventory database from the server. We recommend that you back up the database on a weekly basis. However, if you are tracking the inventory of workstations frequently, increase the frequency of backup.

You can back up the database files and the transaction log to the location relative to the SCANDIR path.

You can run Database Backup either from the server console or ConsoleOne.

This section provides information on the following topics:

- [“Running Database Backup from the Server Console” on page 934](#)
- [“Running Database Backup from ConsoleOne” on page 934](#)
- [“Restoring the Inventory Database” on page 935](#)

Running Database Backup from the Server Console

Before running Database Backup from the server console, fulfill the following prerequisites:

- ❑ You can run Database Backup only on an Inventory server to which you have associated a database server. If you deployed more than one database server, you must run Database Backup for each database server.
- ❑ Ensure that the database you have to back up is configured in the Database Location policy. For more information on how to access the Database Location policy, see [Section 73.5, “Configuring the Database Location Policy,” on page 957](#).
- ❑ In the [DBBackup Service] section of the server property file, you must modify the location of the backup destination in the ARGUMENTS parameter. The backup files are relative to the SCANDIR path. For example, if the SCANDIR path is `sys:\zenworks\inv\scandir`, the database is backed up in `sys:\zenworks\inv\database\directory_you_specify`. You must modify the server property file located on the server on which you are running Database Backup. Modify the server property file corresponding to the role of the server. For example, if you are running Database Backup on the Leaf Server with Database, modify the server property file, `leaf_db_wks.properties`.
- ❑ Ensure that the Service Manager is loaded when you run Database Backup.

To run Database Backup from the server console:

- 1 At the Inventory server console, enter `StartSer DBBACKUP`
- 2 View the status of the backup in the backup log file. The database will be copied to `zenworks_installation_path\zenworks\inv\db\directory_you_specify`

Database Backup creates a log file, `bacstatus.txt`, located in the `zenworks\inv\database` directory on NetWare and Windows 2000 servers. The log records the status of the backup operation. Open this text file to view the status of the backup. This file increases in size for every backup operation. Remove the existing contents of the file if you do not require the details.

Running Database Backup from ConsoleOne

- 1 In ConsoleOne, click *Tools*, click *ZENworks Inventory*, then click *Database Backup*.

If you want to back up the latest information in the Inventory database, right-click the database object, click *ZENworks Inventory*, then click *Database Backup*.

- 2 Enter the path to the directory where the database backup will be saved

WARNING: Do not use double-byte characters in the directory name. If you do so, Sybase interprets the double-byte characters as a different name, and backs up the database in the directory with the interpreted name.

If the Inventory database is running on a NetWare server, you can either enter the path or click Browse to browse for and select a directory. If you enter the database backup directory name without specifying the complete path, the backup directory will be created in the `sys:` directory.

If the Inventory database is running on a Windows or Linux machine, you must manually enter the backup directory path. If you enter the database backup directory name without specifying the complete path, the backup directory is created in the `\winnt\system32` directory on Windows, and in the `root` directory on Linux.

NOTE: If you want to back up the database to a non-existent directory, only one level of the new directory will be created. To back up the database to a subdirectory, ensure that the primary directory already exists. For example, if you want to back up the database to a new `c:\backup` directory, the `\backup` directory will be created and the database will be backed up. But if you want to back up the database to a new `\database` directory, located under `c:\backup`, the `\backup` directory must already exist.

3 Click *Start Backup*.

This backs up the database to the specified directory on the server running the database and overwrites any existing files without prompting about the overwrite.

Database Backup creates a log file, `bacstatus.txt`, located in the `ConsoleOne_installation_directory\1.2\bin` directory. The log records the status of the backup operation. Open this text file to view the status of the backup. This file increases in size for every backup operation. Remove the existing contents of the file if you do not require the details.

Restoring the Inventory Database

- 1 If the Inventory database server is up, stop the Storer service. At the database server console, enter `StopSer Storer`.
- 2 Exit the Sybase database.
 - On NetWare servers: At the database server prompt, enter `q` to stop the Sybase database.
 - On Windows 2000: In the Windows Control Panel, double-click *Administrative Tools*, double-click *Services*, select *Novell Database - Sybase*, then click *Stop*.
- 3 Copy the backup files, overwriting the working database files.
- 4 Restart the database server.

73.2.2 Setting Up the Oracle Inventory Database

The following sections explain how to set up the Inventory database for Oracle9i and Oracle10g:

- “Creating the Oracle9i Inventory Database on a Windows Server” on page 936
- “Creating the Oracle9i Inventory Database on a UNIX Server” on page 937
- “Creating the Oracle10g Inventory Database on a Windows Server” on page 939
- “Creating the Oracle10g Inventory Database on a UNIX Server” on page 941

- “Manually Creating the Oracle Inventory Database Object” on page 943
- “Configuring and Running Multiple Oracle Database Instances on a Windows Server” on page 945

IMPORTANT: In this setup, the Inventory database is not mounted with any other version or instances of Oracle databases.

Creating the Oracle9i Inventory Database on a Windows Server

Make sure that the following prerequisites are met:

- ☐ Oracle 9.2.0.6 must be installed on the server before configuring the Inventory database.
- ☐ To maintain the Inventory database on Oracle, Workstation Inventory requires that you have a minimum of 25 user licenses.

You must manually create the Inventory database for Oracle on Windows servers by following the procedure below:

- 1 Create a directory `c:\schema` and copy all the files in the following directories from the *ZENworks 7 Companion 2 CD* to the schema directory:


```
database\oracle9i\common
database\oracle9i\winntspecific
```
- 2 By default, `_create.sql`, `init.ora`, `_start.sql` are Read-only files. Make the files writable.
- 3 Create the `user_specified_path\zenworks\inventory\oracle\database\trace` directory structure.
- 4 In `c:\schema_create.sql`, replace all instances of `d:` with `user_specified_path`.
- 5 In `c:\schema\init.ora`, replace all instances of `d:` with `user_specified_path`.
- 6 In `c:\schema_start.sql`, replace all instances of `d:` with `user_specified_path`.
If `d:` is not found, check and correct the path of `init.ora` in the database directory.
- 7 Copy `c:\schema\init.ora` to `user_specified_path\zenworks\inventory\oracle\ database`.
- 8 Copy `c:\schema_start.sql` to `user_specified_path\zenworks`.
- 9 Make sure that Oracle services are loaded correctly and the database is not mounted.
- 10 At the command prompt, enter `sqlplus /nolog` to load the Oracle server manager.
- 11 At the Oracle Server Manager prompt (sqlplus prompt), enter `@c:\schema\schema.sql`.
Review the `c:\schema\inv.log` file to make sure that the database has been created successfully. If the database has not been successfully created, `inv.log` contains the following error messages: Oracle not available, Out of space, Compilation error.
- 12 Add non-English enumerated (enum) values for certain Inventory attributes into the Inventory database.

IMPORTANT: You must perform this step on the English version of the product also.

You need to add the non-English enumerated values so the Inventory ConsoleOne utilities such as Inventory Report can display the enum value for the inventory attributes in internationalized versions. The non-English enum values must be available in English version of the product so that the rolled-up inventory information from non-English sites can be properly captured at the high-level servers where only English versions are installed.

For more information about the list of attributes that contains enumerated values, see [Appendix P, “Enumeration Values,” on page 1237](#).

To add the non-English enum values:

12a Specify the JDBC connection settings in the

`zenworks_directory\inv\server\wminv\properties\connection.prop` file to connect to the Oracle database.

You can do this by copying the template property settings for Oracle specified in the comments section in the `connection.prop` file. Specify the IP address, port number, and Database SID in the JDBC URL string that matches your Oracle server configuration.

12b At the server prompt, enter `AddEnums`

`directory_name_containing_connection.prop`

If your Inventory server is running on a Windows machine, run the above command from `zenworks_directory\inv\server\wminv\bin`.

12c Execute the following SQL statement at the `sqlplus` prompt to make sure that the localized enumerated values are added correctly:

- To display the enumerated values in French: `connect mw_dba/password` and `SELECT * FROM cim.ostype_fr`
- To display the enumerated values in Spanish: `connect mw_dba/password` and `SELECT * FROM cim.ostype_es;`
- To display the enumerated values in German: `connect mw_dba/password` and `SELECT * FROM cim.ostype_de;`
- To display the enumerated values in Brazilian-Portuguese: `connect mw_dba/password` and `SELECT * FROM cim.ostype_pt_BR;`

13 At the `sqlplus` prompt, enter `@c:\schema\schemal.sql`.

Review the `c:\schema\inv1.log` file to make sure that the database has been created successfully. If the database has not been successfully created, `inv1.log` contains the following error messages: Oracle not available, Out of space, Compilation error.

14 At the `sqlplus` prompt, enter `connect / as sysdba` to login as DBA.

15 At the `sqlplus` prompt, enter `shutdown immediate`.

16 At the `sqlplus` prompt, enter `@path\zenworks_start.sql` to start the Inventory database.

17 Continue with [“Manually Creating the Oracle Inventory Database Object” on page 943](#).

Creating the Oracle9i Inventory Database on a UNIX Server

Make sure that the following prerequisites are met:

- ☐ Oracle 9.2.0.6 must be installed must be installed on Linux or Solaris versions supported by Oracle9i.
- ☐ Hard disk free space: 4 GB or above.

- ❑ Primary memory: 1 GB or above.
- ❑ To maintain the Inventory database on Oracle, Workstation Inventory requires that you have a minimum of 25 user licenses.

You must manually create the Inventory database for Oracle on UNIX servers by following the procedure below:

- 1 Log in as an Oracle user.
- 2 Create a `/schema` directory in the Oracle installation directory (by default, Oracle is installed in the `/opt/oracle` directory), and copy all the files in the following directories from the *ZENworks 7 Companion 2 CD* to the schema directory:


```
database\oracle9i\common
database\oracle9i\unixspecific
```
- 3 By default, `_create.sql`, `init.ora`, `_start.sql` are Read-only files. Make the files writable.
- 4 Create the `user_specified_directory_path/zenworks/inventory/oracle/database/trace` directory structure in `/opt/oracle`.
- 5 In `schema/init.ora`, replace all instances of `$HOME` with `user_specified_directory_path`.
- 6 In `schema/_start.sql`, replace all instances of `$HOME` with `user_specified_directory_path`.
- 7 In `schema/_create.sql`, replace all instances of `$HOME` with `user_specified_directory_path`.
- 8 In `schema/schema.sql`, replace all instances of `$HOME` with the `schema` directory created in **Step 2**.
- 9 In `schema/schema1.sql`, replace all instances of `$HOME` with the `schema` directory created in **Step 2**.
- 10 Copy `schema/init.ora` to `user_specified_directory_path/zenworks/inventory/oracle/database`.
- 11 Copy `schema/_start.sql` to `user_specified_directory_path`.
- 12 Make sure the Oracle services are up and running and no database is mounted.
- 13 At the command prompt, enter `sqlplus /nolog` to load the Oracle Server Manager.
- 14 At the Oracle Server Manager prompt, enter `@$HOME/schema/schema.sql`, where `$HOME` is the schema directory created in **Step 2**.
- 15 Review the `schema/inv.log` file to make sure that the database has been created successfully. If the database has not been successfully created, `inv.log` will contain the following error messages: Oracle not available, Out of space, Compilation error.
- 16 Add non-English enumerated (enum) values for certain Inventory attributes into the Inventory database.

IMPORTANT: You must perform this step on the English version of the product also.

You need to add the non-English enumerated values so the Inventory ConsoleOne utilities such as Inventory Report can display the enum value for the inventory attributes in internationalized versions. The non-English enum values must be available in English version of the product so

that the rolled-up inventory information from non-English sites can be properly captured at the high-level servers where only English versions are installed.

To add the non-English enum values:

16a On the Inventory Server machine, Specify the JDBC connection settings in the `zenworks_directory\inv\server\wminv\properties\connection.prop` file to connect to the Oracle database.

You can do this by copying the template property settings for Oracle specified in the comments section in the `connection.prop` file. Specify the IP address, port number, and Database SID in the JDBC URL string that matches your Oracle server configuration.

16b At the server prompt, enter `AddEnums`
`directory_name_containing_connection.prop`.

If your Inventory server is running on a Windows machine, run the above command from `zenworks_directory\inv\server\wminv\bin`.

16c Execute the following SQL statement at the sqlplus prompt to make sure that the localized enumerated values are added correctly:

- To display the enumerated values in French: `connect mw_dba/password` and `SELECT * FROM cim.ostype_fr`
- To display the enumerated values in Spanish: `connect mw_dba/password` and `SELECT * FROM cim.ostype_es;`
- To display the enumerated values in German: `connect mw_dba/password` and `SELECT * FROM cim.ostype_de;`
- To display the enumerated values in Brazilian-Portuguese: `connect mw_dba/password` and `SELECT * FROM cim.ostype_pt_BR;`
- To display the enumerated values in Japanese: `connect mw_dba/password` and `SELECT * FROM cim.ostype_ja;`

17 At the sqlplus prompt, enter `@$HOME/schema/schema1.sql`, where `$HOME` is schema directory created in [Step 2](#).

Review the `schema/inv1.log` file to make sure that the database has been created successfully. If the database has not been successfully created, `inv1.log` contains the following error messages: Oracle not available, Out of space, Compilation error.

18 At the sqlplus prompt, enter `connect / as sysdba` to login as DBA.

19 At the sqlplus prompt, enter `shutdown immediate`.

20 At the Oracle Server Manager prompt, enter `@user_specified_directory_path/zenworks/_start.sql` to start the Inventory database.

Creating the Oracle10g Inventory Database on a Windows Server

Make sure that the following prerequisites are met:

- ☐ Oracle10g R1 or Oracle10g R2 must be installed on the server before configuring the Inventory database.
- ☐ To maintain the Inventory database on Oracle, Server Inventory requires that you have a minimum of 25 user licenses.

You must manually create the Inventory database for Oracle on Windows servers by following the procedure below:

- 1 Create a directory `c:\schema`.
- 2 (Conditional) To create the Oracle10g R1 Inventory database, copy all the files in the following directories from the *ZENworks 7 Companion 2 CD* to the `c:\schema` directory:

`database\oracle10gR1\common`
`database\oracle10gR1\winntspecific`
- 3 (Conditional) To create the Oracle10g R2 Inventory database, copy all the files in the following directories from the *ZENworks 7 Companion 2 CD* to the `c:\schema` directory:

`database\oracle10gR2\common`
`database\oracle10gR2\winntspecific`
- 4 By default, `_create.sql`, `init.ora`, `_start.sql` are Read-only files. Make the files writable.
- 5 Create the `user_specified_path\zenworks\inventory\oracle\database\trace` directory structure.
- 6 In `c:\schema_create.sql`, replace all instances of `d:` with `user_specified_path`.
- 7 In `c:\schema\init.ora`, replace all instances of `d:` with `user_specified_path`.
- 8 In `c:\schema_start.sql`, replace all instances of `d:` with `user_specified_path`.
If `d:` is not found, check and correct the path of `init.ora` in the database directory.
- 9 Copy `c:\schema\init.ora` to `user_specified_path\zenworks\inventory\oracle\database`.
- 10 Copy `c:\schema_start.sql` to `user_specified_path\zenworks`.
- 11 Make sure that Oracle services are loaded correctly and the database is not mounted.
- 12 At the command prompt, enter `sqlplus /nolog` to load the Oracle server manager.
- 13 At the Oracle Server Manager prompt (sqlplus prompt), enter `@c:\schema\schema.sql`.
Review the `c:\schema\inv.log` file to make sure that the database has been created successfully. If the database has not been successfully created, `inv.log` contains the following error messages: Oracle not available, Out of space, Compilation error.
- 14 Add non-English enumerated (enum) values for certain Inventory attributes into the Inventory database.

IMPORTANT: You must perform this step on the English version of the product also.

You need to add the non-English enumerated values so the Inventory ConsoleOne utilities such as Inventory Report can display the enum value for the inventory attributes in internationalized versions. The non-English enum values must be available in English version of the product so that the rolled-up inventory information from non-English sites can be properly captured at the high-level servers where only English versions are installed.

For more information about the list of attributes that contains enumerated values, see [Appendix P, "Enumeration Values," on page 1237](#).

To add the non-English enum values:

14a Specify the JDBC connection settings in the `zenworks_directory\inv\server\wminv\properties\connection.prop` file to connect to the Oracle database.

You can do this by copying the template property settings for Oracle specified in the comments section in the `connection.prop` file. Specify the IP address, port number, and Database SID in the JDBC URL string that matches your Oracle server configuration.

14b At the server prompt, enter `AddEnums`
`directory_name_containing_connection.prop`

If your Inventory server is running on a Windows machine, run the above command from `zenworks_directory\inv\server\wminv\bin`.

14c Execute the following SQL statement at the sqlplus prompt to make sure that the localized enumerated values are added correctly:

- To display the enumerated values in French: `connect mw_dba/password` and `SELECT * FROM cim.ostype_fr`
- To display the enumerated values in Spanish: `connect mw_dba/password` and `SELECT * FROM cim.ostype_es;`
- To display the enumerated values in German: `connect mw_dba/password` and `SELECT * FROM cim.ostype_de;`
- To display the enumerated values in Brazilian-Portuguese: `connect mw_dba/password` and `SELECT * FROM cim.ostype_pt_BR;`

15 At the sqlplus prompt, enter `@c:\schema\schemal.sql`.

Review the `c:\schema\inv1.log` file to make sure that the database has been created successfully. If the database has not been successfully created, `inv1.log` contains the following error messages: Oracle not available, Out of space, Compilation error.

16 At the sqlplus prompt, enter `connect / as sysdba` to login as DBA.

17 At the sqlplus prompt, enter `shutdown immediate`.

18 At the sqlplus prompt, enter `@path\zenworks_start.sql` to start the Inventory database.

19 Continue with [“Manually Creating the Oracle Inventory Database Object” on page 943](#).

Creating the Oracle10g Inventory Database on a UNIX Server

NOTE: Information about Oracle 10g R2 is applicable only for ZENworks 7 with Support Pack 1

Make sure that the following prerequisites are met:

- ☐ Oracle10g R1 must be installed must be installed on Linux or Solaris versions supported by Oracle10g.
- ☐ Hard disk free space: 4 GB or above.
- ☐ Primary memory: 1 GB or above.
- ☐ To maintain the Inventory database on Oracle, Workstation Inventory requires that you have a minimum of 25 user licenses.

You must manually create the Inventory database for Oracle on UNIX servers by following the procedure below:

- 1 Log in as an Oracle user.
- 2 Create a `/schema` directory in the Oracle installation directory (by default, Oracle is installed in the `/opt/oracle` directory).
- 3 (Conditional) To create the Oracle10g R1 Inventory database, copy all the files in the following directories from the *ZENworks 7 Companion 2 CD* to the `schema` directory:

```
Database\Oracle10gR1\Common  
Database\Oracle10gR1\unixSpecific
```

- 4 (Conditional) To create the Oracle10g R2 Inventory database, copy all the files in the following directories from the *ZENworks 7 Companion 2 CD* to the `schema` directory:

```
Database\Oracle10gR2\Common  
Database\Oracle10gR2\unixSpecific
```

- 5 By default, `_create.sql`, `init.ora`, `_start.sql` are Read-only files. Make the files writable.
- 6 Create the `user_specified_directory_path/zenworks/inventory/oracle/database/trace` directory structure in `/opt/oracle`.
- 7 In `schema/init.ora`, replace all instances of `$HOME` with `user_specified_directory_path`.
- 8 In `schema/_start.sql`, replace all instances of `$HOME` with `user_specified_directory_path`.
- 9 In `schema/_create.sql`, replace all instances of `$HOME` with `user_specified_directory_path`.
- 10 In `schema/schema.sql`, replace all instances of `$HOME` with the `schema` directory created in **Step 2**.
- 11 In `schema/schema1.sql`, replace all instances of `$HOME` with the `schema` directory created in **Step 2**.
- 12 Copy `schema/init.ora` to `user_specified_directory_path/zenworks/inventory/oracle/database`.
- 13 Copy `schema/_start.sql` to `user_specified_directory_path`.
- 14 Make sure the Oracle services are up and running and no database is mounted.
- 15 At the command prompt, enter `sqlplus /nolog` to load the Oracle Server Manager.
- 16 At the Oracle Server Manager prompt, enter `@$HOME/schema/schema.sql`, where `$HOME` is the `schema` directory created in **Step 2**.
- 17 Review the `schema/inv.log` file to make sure that the database has been created successfully. If the database has not been successfully created, `inv.log` contains the following error messages: Oracle not available, Out of space, Compilation error.
- 18 Add non-English enumerated (enum) values for certain Inventory attributes into the Inventory database.

IMPORTANT: You must perform this step on the English version of the product also.

You need to add the non-English enumerated values so the Inventory ConsoleOne utilities such as Inventory Report can display the enum value for the inventory attributes in internationalized versions. The non-English enum values must be available in English version of the product so that the rolled-up inventory information from non-English sites can be properly captured at the high-level servers where only English versions are installed.

To add the non-English enum values:

18a On the Inventory Server machine, Specify the JDBC connection settings in the `zenworks_directory\inv\server\wminv\properties\connection.prop` file to connect to the Oracle database.

You can do this by copying the template property settings for Oracle specified in the comments section in the `connection.prop` file. Specify the IP address, port number, and Database SID in the JDBC URL string that matches your Oracle server configuration.

18b At the server prompt, enter `AddEnums`
`directory_name_containing_connection.prop`.

If your Inventory server is running on a Windows machine, run the above command from `zenworks_directory\inv\server\wminv\bin`.

18c Execute the following SQL statement at the sqlplus prompt to make sure that the localized enumerated values are added correctly:

- To display the enumerated values in French: `connect mw_dba/password` and `SELECT * FROM cim.ostype_fr`
- To display the enumerated values in Spanish: `connect mw_dba/password` and `SELECT * FROM cim.ostype_es;`
- To display the enumerated values in German: `connect mw_dba/password` and `SELECT * FROM cim.ostype_de;`
- To display the enumerated values in Brazilian-Portuguese: `connect mw_dba/password` and `SELECT * FROM cim.ostype_pt_BR;`
- To display the enumerated values in Japanese: `connect mw_dba/password` and `SELECT * FROM cim.ostype_ja;`

19 At the sqlplus prompt, enter `@$HOME/schema/schema1.sql`, where `$HOME` is schema directory created in [Step 2](#).

Review the `schema/inv1.log` file to make sure that the database has been created successfully. If the database has not been successfully created, `inv1.log` contains the following error messages: Oracle not available, Out of space, Compilation error.

20 At the sqlplus prompt, enter `connect / as sysdba` to login as DBA.

21 At the sqlplus prompt, enter `shutdown immediate`.

22 At the Oracle Server Manager prompt, enter `@user_specified_directory_path/zenworks/_start.sql` to start the Inventory database.

Manually Creating the Oracle Inventory Database Object

- 1 In ConsoleOne, right-click a location in the Novell eDirectory tree for the database object, then click *New*, click *Object*, click *ZENworks Database*, then click *OK*.
- 2 Type a name for the database object, then click *OK*.
- 3 Configure the database server options of the database object.

3a In ConsoleOne, right-click the database object (Inventory database_ *server_name*), then click *Properties*, then click the *ZENworks Database* tab.

3b Select the database server object by using either of the following methods:

- If eDirectory is installed on the database server, then in the *Server DN* field, browse for and select the Server object of the server where the database is physically installed and running.

The server's IP address is automatically populated to the *Server IP Address or DNS Name* drop-down list. If the selected server object has more than one IP address, select the appropriate IP address.

IMPORTANT: Make sure that the DNS name of the database server configured for the database object is valid. If the DNS name is invalid, you must select an appropriate database server IP address in the Database object property page.

To clear the value set in the *Server DN* field, type the IP address of another database server or browse and select another server object.

- If eDirectory is not installed on the database server, then specify the server IP address or the DNS name in the *Server IP Address or DNS Name* field.

3c Specify the following values:

- **Database (Read-Write) User Name:** *MW_DBA*
- **Database (Read-Write) Password:** *novell*
- **Database (Read Only) User Name:** *MWO_READER*
- **Database (Read Only) Password:** *novell*
- **Database (Write Only) User Name:** *MWO_UPDATER*
- **Database (Write Only) Password:** *novell*

IMPORTANT: All Inventory components use the username and password the configured in the database object. By default, "novell" is the password for all options. But you can change it in the database, and update the same here.

3d Click *Apply*.

3e To configure the JDBC Driver properties, click the *JDBC Driver Information* tab.

3f Select *Oracle*, then click the *Default Settings* button.

This populates the fields with default JDBC driver information.

The database settings for Oracle are:

- **Driver:** *oracle.jdbc.driver.OracleDriver*
- **Protocol:** *jdbc:*
- **SubProtocol:** *oracle:*
- **SubName:** *thin:@*
- **Port:** *1521*
- **Flags:** This field is not applicable for Oracle
- **Database Service Name:** *orcl* (The value for the SID is the same as assigned for the database instance.)

3g Click *Apply*, then click *Close*.

Configuring and Running Multiple Oracle Database Instances on a Windows Server

Make sure that the following prerequisites are met:

- ☐ The ZENworks supported Oracle version must be installed on the Windows Inventory server.
- ☐ To maintain the Inventory database in Oracle, Workstation Inventory requires that you have a minimum of 25 user licenses.
- ☐ You have already set up the Inventory database.

To configure and run Oracle instances:

- 1 At the database server, from the desktop *Start* menu, click *Programs*, click *Oracle*, click *Database Administration*, then click *Oracle Database Configuration Assistant*.
- 2 Click *Create a Database*, click *Next*, click *Typical*, click *Next*, click *Copy Existing Database Files from the CD*, then click *Next*.
- 3 Enter the following details:
 - **Global Database Alias:** `mgmtdb.your_windows_nt/2000_name`
 - **SID:** By default, the value is `mgmtdb`.

- 4 Click *Finish*.

This process takes a significant amount of time and creates the Oracle database.

Make sure that the OracleServiceMGMTDB service is created and started.

- 5 Load the Inventory database.

From the desktop *Start* menu, click *Run*, then click *SQLPLUS* to run the Oracle Server Manager.

Enter the following commands:

```
set instance mgmtdb
connect internal/password_for_administrator
```

73.2.3 Setting Up the MS SQL Server 2000 or MS SQL Server 2005 Inventory Database

This section provides information on the following topics:

- “Configuring the MS SQL Server 2000 Inventory Database” on page 945
- “Configuring the MS SQL Server 2005 Inventory Database” on page 948
- “Manually Creating the Inventory Database Object for MS SQL 2000 or MS SQL 2005” on page 951
- “Connecting the Inventory Server and ConsoleOne to the MS SQL 2000 or MS SQL 2005 Inventory Database” on page 953

Configuring the MS SQL Server 2000 Inventory Database

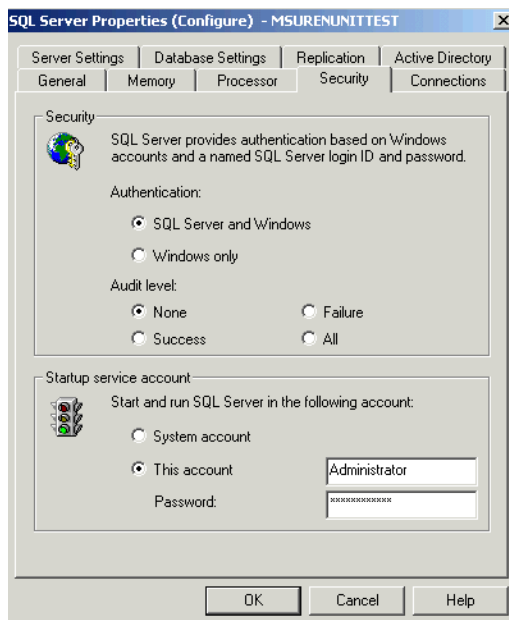
Prerequisites for configuring the database include the following:

- ☐ Microsoft SQL Server 2000 installed on the Windows server.
- ☐ Minimum free disk space of 50 MB to extract the `plmssqlinvdb.zip` file.

- ❑ Make sure that you have sufficient disk space to store the inventory information on the server that has the Inventory database.

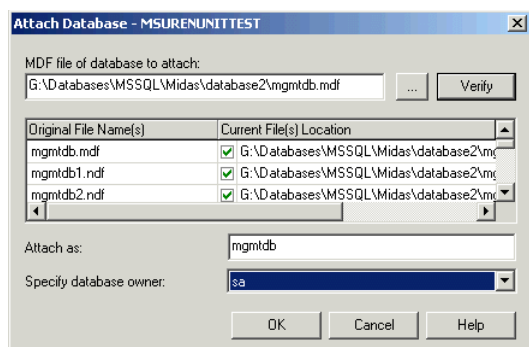
To configure the Inventory database for MS SQL Server 2000:

- 1 Copy the `plmssqlinvdb.zip` file from the *ZENworks 7 Companion 2* CD\database\mssql directory to *path_of_inventory_database_directory_on_the_database_server*.
- 2 Extract `plmssqlinvdb.zip`.
- 3 From the MS SQL server desktop *Start* menu, click *Programs*, click *Microsoft SQL Server*, then click *Enterprise Manager*.
- 4 In the SQL Server Enterprise Manager, browse to Console Root/Microsoft SQL Servers/SQL Server Group/*machine_name_running_Inventory_database*.
- 5 Right -click *machine_name_running_Inventory_database*, then click *Properties*.
- 6 In the SQL Server Properties dialog box, click the *Security* tab and make sure that the authentication is set to SQL Server and Windows.



- 7 Click *OK*.
- 8 Browse to *machine_name_running_Inventory_database/Databases* and right-click *Databases*, click *All Tasks*, then double-click *Attach Database*.
- 9 In the Attach Database dialog box, do the following:
 - 9a Click the *Browse* button to browse to and select `mgmtdb.mdf` as the `.mdf` database file to be attached.
 - 9b Make sure that the value of the *Attach As* field is `mgmtdb`.
 - 9c Select *sa* from the *Specify Database Owner* drop-down list.
 - 9d Click *OK*.

The ZENworks Inventory database (mgmtdb) is attached to the Databases server group.



10 Select *mgmtdb*, then click the *Tools* menu, then click *SQL Query Analyzer*.

11 In the SQL Query Analyzer, do the following:

11a Make sure that *mgmtdb* is selected in the drop-down list.

11b Click *File*, then click *Open*.

11c Select the `createloginnames.sql` query file from *ZENworks 7 Companion 2* CD\database\mssql directory.

11d Click *Query*, then click *Execute*.

On successful execution, the following message is displayed in the Message pane:

New Login Created

11e Login as MW_DBA in the SQL Query Analyzer and execute the following drop trigger sqls:

```
drop trigger cim.x$scim$component
go
drop trigger cim.x$scim$dependency
go
drop trigger managewise.x$managewise$designates
go
drop trigger managewise.x$managewise$currentloginuser
go
drop trigger managewise.x$managewise$lastloginuser
go
drop trigger cim.x$scim$installedsoftwareelement
go
```

During the execution of the drop trigger sqls, the following error message might be displayed on the console, “Cannot drop the trigger '*trigger_name*', because it does not exist in the system catalog”. Ignore the error message.

12 (Optional) Add non-English enumerated (enum) values for certain Inventory attributes into the Inventory database.

You need to add the non-English enumerated values so the Inventory ConsoleOne utilities such as Inventory Report can display the enum value for the inventory attributes in internationalized

versions. The non-English enum values must be available in English version of the product so that the rolled-up inventory information from non-English sites can be properly captured at the high-level servers where only English versions are installed.

For more information about the list of attributes that contains enumerated values, see [Appendix P, “Enumeration Values,” on page 1237](#).

To add the non-English enum values:

12a Specify the JDBC connection settings in the

`zenworks_directory\inv\server\wminv\properties\connection.prop` file to connect to the MS SQL database.

You can do this by copying the template property settings for MS SQL specified in the comments section in the `connection.prop` file. Specify the IP address, port number, and Database SID in the JDBC URL string that matches your MS SQL server configuration.

12b At the server prompt, enter `AddEnums`

`directory_name_containing_connection.prop`

If your Inventory server is running on a Windows machine, run the above command from `zenworks_directory\inv\server\wminv\bin`.

After executing the command, the a message indicating that the non-English enums have been successfully inserted is displayed on the console prompt.

13 Continue with [“Manually Creating the Inventory Database Object for MS SQL 2000 or MS SQL 2005” on page 951](#).

Configuring the MS SQL Server 2005 Inventory Database

NOTE: Information about MS SQL 2005 is applicable only for ZENworks 7 with Support Pack 1.

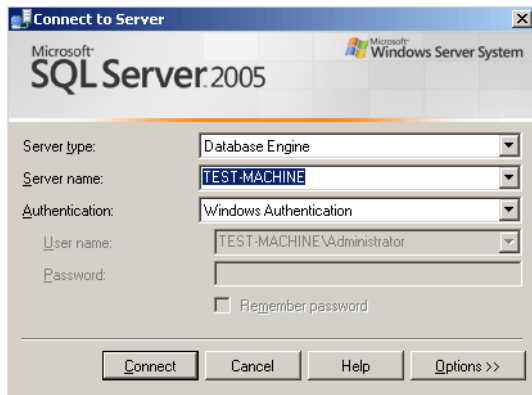
Prerequisites for configuring the database include the following:

- ☐ Microsoft SQL Server 2005 installed on the Windows server.
- ☐ Minimum free disk space of 50 MB to extract the `plmssqlinvdb.zip` file.
- ☐ Make sure that you have sufficient disk space to store the inventory information on the server that has the Inventory database.

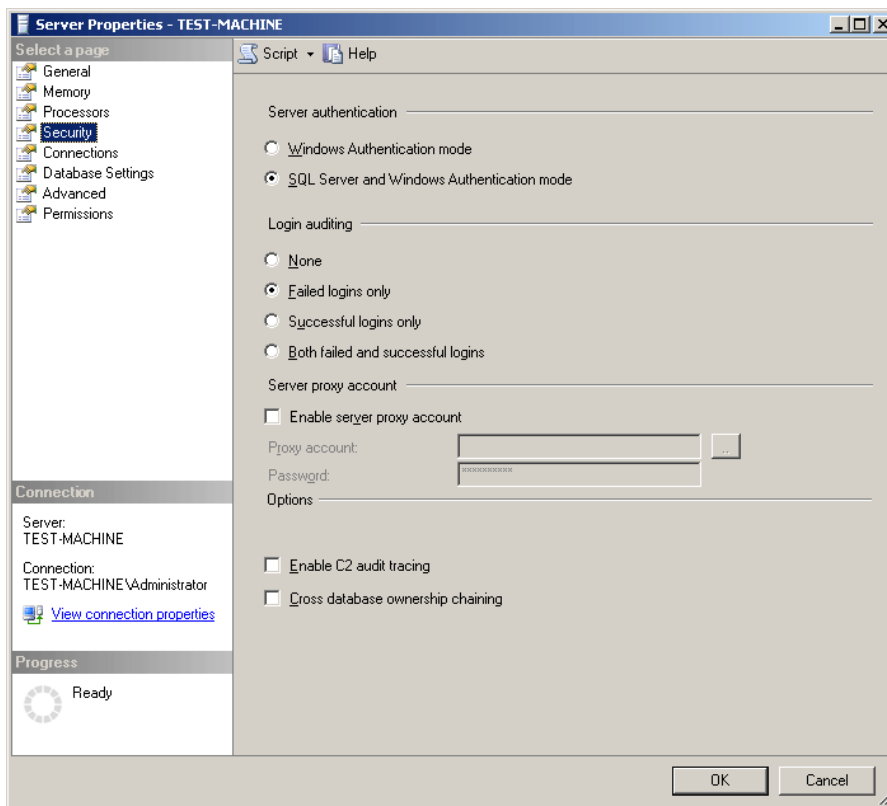
To configure the Inventory database for MS SQL Server 2005:

- 1** Copy the `plmssqlinvdb.zip` file from the *ZENworks 7 Companion 2* `CD\database\mssql` directory to `path_of_inventory_database_directory_on_the_database_server`.
- 2** Extract `plmssqlinvdb.zip`.
- 3** From the MS SQL server desktop *Start* menu, click *Programs*, click *Microsoft SQL Server 2005*, then click *SQL Server Management Studio*.

- 4 In the SQL Server Management Studio, connect to the Database Engine of the MSSQL Server by clicking on File->Connect Object Explorer and setting the properties.



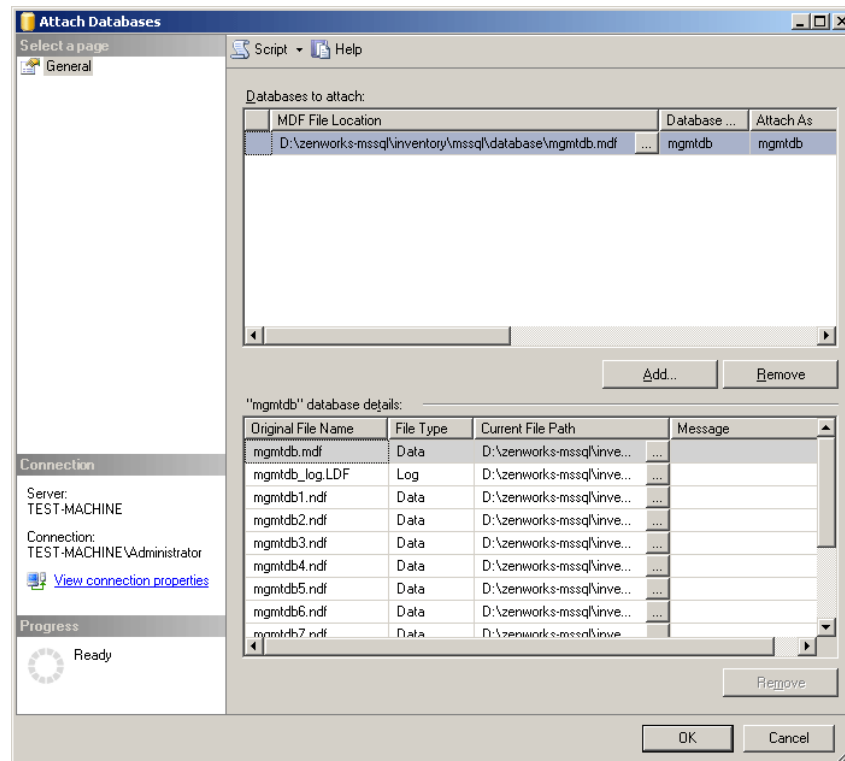
- 5 Browse to *machine_name_running_Inventory_database* in the Object Explorer, and right-click *machine_name_running_Inventory_database*, then click Properties.
- 6 In the SQL Server Properties dialog box, click the Security tab and make sure that the authentication is set to SQL Server and Windows.



- 7 Click OK.
- 8 Browse to *machine_name_running_Inventory_database/Database*, and right-click Databases, click All Tasks, then double-click Attach Database.
- 9 In the Attach Database dialog box, do the following:

- 9a** Click the *Add* button to browse to and select `mgmtdb.mdf` as the `.mdf` database file to be attached.
- 9b** Make sure that the value of the *Attach As* field is `mgmtdb`.
- 9c** Click *OK*.

The ZENworks Inventory database (`mgmtdb`) is attached to the Databases server group.



- 9d** Right-click *mgmtdb*, then select *New Query*.
- 10** In the SQL Query Analyzer, do the following:
 - 1001** Select the `createloginnames.sql` query file from *ZENworks 7 Companion 2* CD\database\mssql directory. Either drag and drop it on the opened query window or copy the contents of the sql file to the query window.
 - 1002** Click *Execute*.

On successful execution, the following message is displayed in the Message pane:

New Login Created

- 10a** Login as `MW_DBA` in the SQL Query Analyzer and execute the following drop trigger sqls:

```
drop trigger cim.x$cim$component
go
drop trigger cim.x$cim$dependency
go
drop trigger managewise.x$managewise$designates
go
```

```
drop trigger managewise.x$managewise$currentloginuser
go
drop trigger managewise.x$managewise$lastloginuser
go
drop trigger cim.x$cim$installedsoftwareelement
go
```

During the execution of the drop trigger sqls, the following error message might be displayed on the console, “Cannot drop the trigger '*trigger_name*', because it does not exist in the system catalog”. Ignore the error message.

- 11 Continue with “[Manually Creating the Inventory Database Object for MS SQL 2000 or MS SQL 2005](#)” on page 951

Manually Creating the Inventory Database Object for MS SQL 2000 or MS SQL 2005

NOTE: Information about MS SQL 2005 is applicable only for ZENworks 7 with Support Pack 1.

- 1 In ConsoleOne, right-click a location in the Novell eDirectory tree for the database object, then click *New*, click *Object*, click *ZENworks Database*, then click *OK*.
- 2 Type a name for the database object, then click *OK*.
- 3 Configure the database server options of the database object.

3a In ConsoleOne, right-click the database object (Inventory database_*server_name*), then click *Properties*, then click the *ZENworks Database* tab.

3b Select the database server object by using either of the following methods:

- If eDirectory is installed on the database server, then in the *Server DN* field, browse for and select the Server object of the server where the database is physically installed and running.

The server’s IP address is automatically populated to the *Server IP Address or DNS Name* drop-down list. If the selected server object has more than one IP address, select the appropriate IP address.

IMPORTANT: Make sure that the DNS name of the database server configured for the database object is valid. If the DNS name is invalid, you must select an appropriate database server IP address in the Database object property page.

To clear the value set in the *Server DN* field, type the IP address of another database server or browse and select another server object.

- If eDirectory is not installed on the database server, then specify the server IP address or the DNS name in the *Server IP Address or DNS Name* field.

3c Specify the following values:

- **Database (Read-Write) User Name:** *MW_DBA*
- **Database (Read-Write) Password:** *novell*
- **Database (Read Only) User Name:** *MWM_READER*
- **Database (Read Only) Password:** *novell*
- **Database (Write Only) User Name:** *MWM_UPDATER*

- **Database (Write Only) Password:** *novell*

IMPORTANT: All Inventory components use the username and password the configured in the database object. By default, “novell” is the password for all options. But you can change it in the database, and update the same here.

3d Click *Apply*.

3e To configure the JDBC Driver properties, click the *JDBC Driver Information* tab.

3f If you have installed ZENworks 7 Desktop Management, select *MSSQL*, then click the *Default Settings* button.

This populates the fields with default JDBC driver information.

The database settings for MS SQL 2000 are:

- **Driver:** *com.microsoft.jdbc.sqlserver.SQLServerDriver*
- **Protocol:** *jdbc:*
- **SubProtocol:** *microsoft:*
- **SubName:** *sqlserver://*
- **Port:** *1433*
- **Flags:** This field is not applicable for MS SQL 2000.
- **Database Service Name:** This field is not applicable for MS SQL 2000.

3g If you have installed ZENworks 7 Desktop Management and MS SQL 2000, select *MSSQL (2000)*, then click the *Default Settings* button.

This populates the fields with default JDBC driver information.

The database settings for MS SQL 2000 are:

- **Driver:** *com.microsoft.jdbc.sqlserver.SQLServerDriver*
- **Protocol:** *jdbc:*
- **SubProtocol:** *microsoft:*
- **SubName:** *sqlserver://*
- **Port:** *1433*
- **Flags:** This field is not applicable for MS SQL 2000.
- **Database Service Name:** This field is not applicable for MS SQL 2000.

3h If you have installed ZENworks 7 Desktop Management with Support Pack 1 and MS SQL 2005, select *MSSQL (2005)*, then click the *Default Settings* button.

This populates the fields with default JDBC driver information.

The database settings for MS SQL 2005 are:

- **Driver:** *com.microsoft.jdbc.sqlserver.SQLServerDriver*
- **Protocol:** *jdbc:*
- **SubProtocol:** This field is not applicable for MS SQL 2005.
- **SubName:** *sqlserver://*
- **Port:** *1433*
- **Flags:** This field is not applicable for MS SQL 2005.
- **Database Service Name:** This field is not applicable for MS SQL 2005.

- 3i Click *Apply*, then click *Close*.
- 4 Continue with “Connecting the Inventory Server and ConsoleOne to the MS SQL 2000 or MS SQL 2005 Inventory Database” on page 953.

Connecting the Inventory Server and ConsoleOne to the MS SQL 2000 or MS SQL 2005 Inventory Database

The Inventory server components and the ConsoleOne use Microsoft JDBC driver to connect to the Inventory database on MS SQL 2000. You must install and configure Microsoft SQL Server 2000 driver for JDBC driver with the Inventory system.

To configure the Microsoft SQL Server 2000 driver for JDBC to access the Inventory database running on MS SQL 2000:

- 1 Download the Windows English version of Microsoft JDBC driver from the [Microsoft SQL Server Web site](http://www.microsoft.com/downloads/details.aspx?FamilyID=9f1874b6-f8e1-4bd6-947c-0fc5bf05bf71&DisplayLang=en) (<http://www.microsoft.com/downloads/details.aspx?FamilyID=9f1874b6-f8e1-4bd6-947c-0fc5bf05bf71&DisplayLang=en>).

NOTE: Skip to Step 5, if you have MS SQL 2005 as the database.

- 2 On a Windows Inventory server, do the following and then skip to **Step 4**:
- 2a Install the driver.
- 2b Copy the `msbase.jar`, `msutil.jar`, and `mssqlserver.jar` files to `inventory_server_installation_directory\inv\server\lib` directory.
- 3 On a Linux Inventory server, do the following and continue with **Step 4**:
- 3a Extract `msbase.jar`, `msutil.jar`, and `mssqlserver.jar` from the downloaded Microsoft JDBC driver.
- 3b Copy the `msbase.jar`, `msutil.jar`, and `mssqlserver.jar` files to the `/opt/novell/zenworks/java/lib/common` directory.
- 4 On the machine, running ConsoleOne with ZENworks 7 Inventory snap-ins, copy the `msbase.jar`, `msutil.jar`, and `mssqlserver.jar` files to the `consoleone_installation_directory\lib\zen` directory.
- 5 In ConsoleOne, create a database object in the same container where Inventory server is installed.
- 5a Right-click the container.
- 5b Click *New*, click *Object*, select *ZENworks Database* from the list of objects, then click *OK*.
- 5c Enter a name for the database object, then click *OK*.
- 6 Configure the Database server options of the Database object.
- 6a In ConsoleOne, right-click the database object, click *Properties*, then click the *ZENworks Database* tab.
- 6b Select the database server object using any of the following methods:
- If eDirectory is installed on the database server, in the *Server DN* field, browse for and select the Server object for the server where the database is physically installed and running.

The server's IP address is automatically populated to the *Server IP Address or DNS Name* drop-down list. If the selected server object has more than one IP address, select the appropriate IP address.

IMPORTANT: Make sure that the DNS name of the database server configured for the database object is valid. If the DNS name is invalid, you must select an appropriate database server IP address in the Database object property page.

To clear the value set in the *Server DN* field, type the IP address of another database server or browse and select another server object.

- If eDirectory is not installed on the database server, then enter the server's IP address or the DNS name in the *Server IP Address or DNS Name* field.

6c Type the values for the following options:

- **Database (Read-Write) User Name:** *MW_DBA*
- **Database (Read-Write) Password:** *novell*
- **Database (Read Only) User Name:** *MWM_READER*
- **Database (Read Only) Password:** *novell*
- **Database (Write Only) User Name:** *MWM_UPDATER*
- **Database (Write Only) Password:** *novell*

6d Click *Apply*.

6e To configure the JDBC Driver properties, click the *JDBC Driver Information* tab.

6f Select *MS SQL*, then click *Default Settings*.

This populates the fields with default JDBC driver information.

Modify the database settings based on the configuration of your MS SQL Server. The database settings for MS SQL are:

- **Driver:** *com.microsoft.jdbc.sqlserver.SQLServerDriver*
- **Protocol:** *jdbc:*
- **SubProtocol:** *microsoft:*
- **SubName:** *sqlserver://*
- **Port:** *1433*
- **Flags:** Not applicable for MS SQL
- **Database Service Name:** Not applicable for MS SQL

6g For MS SQL 2005, select *MS SQL (2005)*, then click *Default Settings*.

This populates the fields with default JDBC driver information.

Modify the database settings based on the configuration of your MS SQL Server. The database settings for MS SQL are:

- **Driver:** *com.microsoft.jdbc.sqlserver.SQLServerDriver*
- **Protocol:** *jdbc:*
- **SubProtocol:** Not applicable for MS SQL 20005
- **SubName:** *sqlserver://*
- **Port:** *1433*
- **Flags:** Not applicable for MS SQL 2005

- **Database Service Name:** Not applicable for MS SQL 2005

6h Click *Apply*, then click *Close*.

For more information on Performance tips, see [Section M.1, “Database Parameter Tuning Tips,” on page 1185](#).

73.3 Configuring the Inventory Service Object

The Inventory Service object settings configure scanning for the associated inventoried workstations.

To configure the Inventory Service object:

- 1 In ConsoleOne, right-click the Inventory Service object (Inventory Service_*server_name*), then click *Properties* to display the Inventory Service Object Properties page.
- 2 Modify the following settings:

Inventory Server Role: Based on the servers that you have deployed for scanning inventory, you must specify the role of the server. For more information, see [Section 72.4, “Understanding the Inventory Server Roles,” on page 876](#).

Based on the new role you select, you will see a list of actions to be followed. For example, if you change the role of the Root Server to Root Server with Inventoried Workstations, you must configure the Workstation Inventory policy for the inventoried workstations that you have attached. Similarly, to change the role to any other server, follow the actions to make the new role change effective. For more information, see [Section 73.1.7, “Changing the Role of the Inventory Server,” on page 917](#).

Plan the change of roles carefully because these changes impact the existing inventory deployment.

Discard Scan Data Time: Select the date and time. Any scan data files (.zip files) that have scan information collected before the Discard Scan Data Time that you specify in the Inventory Service Object property page are discarded.

Scan Directory Path: Select the name of the volume on the Inventory server where you want to store the scan data files.

The Scan directory (`scandir`) path is the location on the Inventory server that stores the scan data files. The format of the Scan directory path is as follows:

inventory_server_name\volume_of_the_server_directory.

For a NetWare server, you cannot modify the Inventory server name specified in the Scan directory path. To modify the directory name, click *Browse* and select an existing directory.

For a Windows server, you cannot modify the Inventory server name specified in the Scan directory path. To modify the directory name, you must manually type it.

For a Linux server, you cannot modify the Inventory server name or the directory path specified in the Scan directory path of this property page. However, you can change the directory path using the `zeninvshares` script. For more information, see [Section 73.4, “Changing the ScanDir Path for a Linux Inventory Server,” on page 956](#).

Enable Scan of Machines: Select this option to specify hardware and software scanning of the inventoried workstations associated with this Inventory Service object. The scanners collect inventory information only if this option is enabled. By default, the scanners collect only hardware information for the inventoried workstations.

Start Full Scan: When scanning the inventoried workstation for the first time, the Scanner collects the complete inventory of the inventoried workstation. A complete inventory scan of the inventoried workstation is referred as a *full scan*. After the inventoried workstation is scanned, the next time the Scanner compares the current inventory information to the history data that it maintains. If there are any changes to the inventoried workstation, the Scanner creates a *delta scan*, which collects the changes in inventory since the last scan was done. The delta scan setting is the default scan operation for each successive scan after the first scanning of the inventoried workstation. If the Status Log reported by the inventory component indicates the scanning on the inventoried workstation is not successful, you can enforce a full scan. This policy setting is applicable for all inventoried workstations associated with it. To override the policy, set this option for an individual inventoried workstation. For more information about the Workstation object settings, see [Section 73.6, “Configuring the Workstation Inventory Policy,” on page 958](#).

NOTE: Using the Workstation Inventory policy, you can configure the Scheduled Full scan to send a full scan after a certain number of delta scans. The value must be between 5 and 65535. If you do not want the Scheduled Full scan, set the value to 65535

- 3 To configure the software dictionary rules, click the *Software Inventory Configuration* tab. For more information on how to configure the software dictionary rules, see [Section 76.3, “Customizing the Software Inventory Information To Be Scanned For ZENworks 7 Inventoried Workstations,” on page 1035](#).
- 4 Click OK.

NOTE: If you are modifying the Inventory policies or configuring the objects, always stop the Inventory services. Configure the policies and properties of the objects. Restart the Inventory services again. For more information on how to start the inventory service, see [Section 73.1.5, “Starting and Stopping the Inventory Service,” on page 915](#).

73.4 Changing the ScanDir Path for a Linux Inventory Server

You can change the scandir path for a Linux Inventory server using the zeninvshares script.

To change the scandir path:

- 1 At the Linux Inventory server prompt, execute the zeninvshares script by entering `/opt/novell/bin/zeninvshares`.
- 2 Enter the new scandir path.

NOTE: Do not choose a directory that might contain privileged information because this script grants everyone Read and Execute permissions to all the directories in the `scandir` path.

- 3 (Conditional) On the OES Linux Inventory server, you are prompted to enter the eDirectory administrator's name and password to assign the rights to the NCP shares.

After changing the scandir path, if your Linux Inventory server is running on OES, ensure that the following entry exists in `/etc/opt/novell/ncpserv.conf`:

```
VOLUME sys /usr/novell/sys
```


If the entry does not exist, you must manually add it to the file, and restart Novell eDirectory by entering `/etc/init.d/ndsd restart` at the Linux server prompt.

73.5 Configuring the Database Location Policy

The Database Location policy contains the location of the Inventory database. You can associate the Database Location policy with a container under which the Inventory Service object (Inventory Service_ *server_name*) is located through using the Service Location Package or with an Inventory server through using the Server Package.

NOTE: If you configure the Service Location Package and the Server Package, the Server Package settings override the Service Location Package settings.

To associate the Database object with a container under which the Inventory Service object is located:

- 1 In ConsoleOne, right-click the *Service Location Package*, then click *Properties* to display the *Policies* page.
- 2 Select the check box under the *Enabled* column for the ZENworks Database policy.
- 3 Click *Properties* to display the *Inventory Management* page.
- 4 Browse to the DN of the Inventory Database object (Inventory database_ *server_name*), then click *OK*.

For a Sybase database, the database object is automatically created during the Workstation Inventory installation unless you are installing on a Windows server without eDirectory installed. To manually create the database object, see [“Manually Creating the Sybase Inventory Database Object” on page 930](#).

For an Oracle database, you must create the database object and configure the object. For more information, see [“Setting Up the Oracle Inventory Database” on page 935](#).

For an MS SQL database, you must configure the database object. For more information, see [“Setting Up the MS SQL Server 2000 or MS SQL Server 2005 Inventory Database” on page 945](#).

- 5 Click *OK*.
- 6 Click the *Associations* tab, then click *Add*.
- 7 Browse to select the container under which the Inventory Service object (Inventory Service_ *server_name*) is located, then click *OK*.
- 8 Click *Apply*, then click *Close*.

To associate the Database object with an Inventory server:

- 1 In ConsoleOne, right-click the *Server Package*, then click *Properties* to display the *Policies* page.
- 2 Select the check box under the *Enabled* column for the ZENworks Database policy.
- 3 Click *Properties* to display the *Inventory Management* page.
- 4 Browse to the DN of the Inventory Database object (Inventory database_ *server_name*), then click *OK*.

For a Sybase database, the database object is automatically created during the Workstation Inventory installation unless you are installing on a Windows server without eDirectory

installed. To manually create the database object, see [“Manually Creating the Sybase Inventory Database Object” on page 930](#).

For an Oracle database, you must create the database object and configure the object. For more information, see [“Setting Up the Oracle Inventory Database” on page 935](#).

For an MS SQL database, you must configure the database object. For more information, see [“Setting Up the MS SQL Server 2000 or MS SQL Server 2005 Inventory Database” on page 945](#).

- 5 Click *OK*.
- 6 Click the *Associations* tab, then click *Add*.
- 7 Browse to select an NCP server object of an Inventory server, then click *OK*.
- 8 Click *Apply*, then click *Close*.

NOTE: If you are modifying the Inventory policies or configuring the objects, always stop the Inventory services. Configure the policies and properties of the objects. Restart the Inventory services again. For more information on how to start the inventory service, see [Section 73.1.5, “Starting and Stopping the Inventory Service,” on page 915](#).

73.6 Configuring the Workstation Inventory Policy

- 1 In ConsoleOne, right-click the Workstation package, then click *Properties* to display the *Policies* page.
- 2 Click the *Policies* tab, and then select a specific platform from the drop-down list to configure and enable the policy for that platform. The available platforms include: *Windows 9x*, *WinNT-2000-XP*, *Windows NT*, *Windows 2000*, or *Windows XP*.
- 3 Select the check box under the *Enabled* column for the Workstation Inventory Policy.
- 4 Click *Properties* to display the Workstation Inventory Policy page.
- 5 In the *General* page, configure the following settings:
 - 5a Browse to and select the DN of the Inventory Service object (Inventory Service_server_name).
 - 5b Specify the number of delta scans after which a full scan is required.
- 6 (Optional) Customize the Inventory scan.
 - 6a Click the *Hardware Scan* tab to specify the following settings:

Enable DMI Scan: Select this option to include scanning of hardware information from Desktop Management Interface (DMI) on the inventoried workstations.

Enable WMI Scan: Select this option to include WMI scanning of hardware information from Microsoft's Windows Management Instrumentation (WMI) on the inventoried workstations.

Enable Custom Scanning: Select this option to include Custom scanning of the inventoried workstations. You need to enter the name of the Custom Scan executable that should be run for custom scanning.

Custom Attribute Editor: Click this button to specify the list of custom attributes. Modify the list if necessary.

- 6b** To customize the software scan settings for the Windows inventoried workstations where ZENworks for Desktops 4 or ZENworks for Desktops 4.0.1 is installed, click the *Software Scan* tab and configure the following settings. For more information, see [Section 76.4, “Customizing the Software Inventory Information To Be Scanned For ZENworks for Desktops 4.x and Earlier Versions of Inventoried Workstations,”](#) on page 1081.

IMPORTANT: Do not configure the settings for the inventoried workstations that have ZENworks 7 Desktop Management installed. To customize software scanning for workstations having ZENworks 7 Desktop Management installed, see [Section 76.3, “Customizing the Software Inventory Information To Be Scanned For ZENworks 7 Inventoried Workstations,”](#) on page 1035.

Enable Software Scan: Enables software scanning for the inventoried workstations associated with the Inventory policy. The scan program collects software information for the inventoried workstations and stores it in the Inventory database.

Custom Scan Editor: Enables you to customize the list of application details to scan for at the inventoried workstations. The Inventory scanner scans for the details of the applications listed in the Custom Scan Editor.

For example, specify the following details in the Custom Scan Editor: Vendor Name=Microsoft; Product Name=Microsoft Office; Product Version=10.0; FileName=winword.exe; File Size=1 MB. The Inventory scanner scans for the winword.exe file having a size of 1 MB on the inventoried workstations. If the file is found, the scanner stores “Microsoft;Microsoft Office;10.0” for “winword.exe;1 MB” in the Inventory database.

Product Identification Number: Enables you to scan for the product identification number of the Microsoft applications installed on the inventoried workstations.

Product Location: Enables you to scan for the full path of the applications installed on the inventoried workstations.

Perform only Custom Scanning: Enables you to scan only the customized software applications that are selected in the Custom Scan Editor.

- 6c** Click the *Configuration Editor* tab. If required, modify the settings of the following .ini files.

- **SWRules:** Configure the SWRules file for the Windows inventoried workstations on which ZENworks for Desktops 4 or ZENworks for Desktops 4.0.1 is installed. Do not configure the file for the inventoried workstations that have ZENworks 7 Desktop Management installed.

Use the SWRules file to customize the software scanning information of vendors and products. For more information on how to configure this file, see [Section 76.4, “Customizing the Software Inventory Information To Be Scanned For ZENworks for Desktops 4.x and Earlier Versions of Inventoried Workstations,”](#) on page 1081.

- **Asset Information:** Use this file to scan for vendor-specific information from the Desktop Management Interface (DMI). For more information how to configure this file, see [“Scanning for Vendor-Specific Asset Information from DMI”](#) on page 1032.
- **Zippered Names:** Use this file to customize the hardware scanning of Jaz and Zip drives. For more information how to configure this file, see [“Customizing the Hardware Scanning Information of Jaz, Zip, and Floppy Drive Vendors”](#) on page 1031.

- **IBM Names:** Use this file to scan for IBM computer models. For more information how to configure this file, see “[Scanning for IBM Computer Models](#)” on page 1030.
- **HWRules:** Use this file to customize the information on nominal size of monitors. For more information on how to configure the `hwrules.ini` file, see [Section 76.2.5, “Customizing the Hardware Information for Monitor Size,”](#) on page 1033.

- 7 Click *Apply*.
- 8 Click the *Policy Schedule* tab.
- 9 Modify the settings for scheduling the scan of the inventoried workstations, click *Apply*, then click *Close*.
- 10 Click the *Associations* tab, then click *Add*.
- 11 Browse to and select the container object where the inventoried workstations are registered, then click *OK*.
- 12 Click *Apply*, then click *Close*.
- 13 In ConsoleOne, right-click the Inventory Service object (Inventory Service_*server_name*), click *Properties*, then click the *Inventory Service object* tab.
- 14 Make sure *Enable Scan of Machines* is selected, then click *OK*.

73.7 Configuring the Roll-Up Policy

The Roll-Up policy configures the Inventory server for roll-up of scan information. The settings in the Roll-Up policy identify the next-level Inventory server (DN of the Inventory Service object) for moving the inventory information from the selected Inventory server. These settings are stored in eDirectory and are associated with the Inventory server object.

To configure the Roll-Up policy:

- 1 In ConsoleOne, right-click the *Server Package*, click *Properties*, click *Policies*, then select the appropriate suboption. If you want this policy to be applied on all servers, select the *General* suboption.
- 2 Select the check box under the *Enabled* column for the Inventory Rollup Policy.
- 3 Click *Properties* to display the Roll-Up Policy page.
- 4 Browse to and select the DN of the Inventory Service object (Inventory Service_*server_name*).

Destination Server Object: You must specify the DN of the Inventory Service object at the next level Inventory server for moving the inventory information from the selected Inventory server. The server that you specify must be another Intermediate Server, Intermediate Server with Database, Intermediate Server with Database and Inventoried Workstations, Intermediate Server with Inventoried Workstations, Root Server, or Root Server with Inventoried Workstations.

NOTE: Make sure that the specified Inventory server is a different server, because the roll-up of information cannot happen on the same Inventory server. Also, the higher level roll-up Inventory server cannot specify the lower-level Inventory server as the next-destination server for roll-up of information.

If you want to roll up to an Inventory server in a different eDirectory tree, click the *Set Context* button, enter the tree name, and select the Inventory Service object of the next-level server.

- 5 By default, the DNS name or the IP address (if a DNS name is not configured) of the next-level server is populated in the field. If the next-level server has multiple IP addresses, select the preferred address.

IMPORTANT: Make sure that the DNS name of the next-level server is valid. If the DNS name is invalid, you must select an appropriate server IP address.

- 6 If the roll-up is to an Inventory server that is across the firewall, specify the IP address or the DNS name and the port number of the proxy server.
- 7 Click *Apply*.
- 8 Click the *Roll-Up Policy* tab, then click *Roll-Up Schedule*.
- 9 Modify the settings for scheduling the roll-up time, then click *Apply*.

When you schedule the roll-up of information in the Inventory policies, we recommend the roll-up frequency should be at least one day. It is likely that if the roll-up of inventory information is scheduled too frequently, for example less than one hour, there might be some performance degradation of the Inventory server.

- 10 (Conditional) If you have not yet associated the Server Package, you are prompted to associate it with an Inventory server or a container. The policy you configured and enabled earlier will not be in effect until you associate this policy package with an Inventory server or a container.

To associate the policy package:

10a Click the *Associations* tab, then click *Add*.

10b Browse for and select the Inventory server or the container that you want to associate the Roll-Up policy to.

10c Click *OK*, then click *OK*.

- 11 Click *Apply*, then click *Close*.

NOTE: If you are modifying the Inventory policies or configuring the objects, always stop the Inventory services. Configure the policies and properties of the objects. Restart the Inventory services again. For more information, see [Section 73.1.5, “Starting and Stopping the Inventory Service,” on page 915](#).

73.8 Configuring the Dictionary Update Policy

The Dictionary Update policy configures the Inventory server to receive the software dictionary updates from other Inventory servers. You must manually download the dictionary updates to at least one Inventory server in your network. This Inventory server can then act as the source of dictionary updates to other Inventory servers.

- 1 In ConsoleOne, right-click the *Server Package*, click *Properties*, click *Policies*, then select the appropriate suboption. If you want this policy to be applied on all servers, select the *General* suboption.
- 2 Select the check box under the *Enabled* column for the Dictionary Update policy.
- 3 Click *Properties* to display the Dictionary Update Policy page.
- 4 Configure the following settings:

- 4a** (Recommended) Select the *Use the Roll-Up Server as the Update Source* check box if you want the Dictionary Update Service to use the Inventory server configured in the Roll-Up policy as the source for dictionary updates.

If you select this check box, continue with [Step 9 on page 962](#). If you do not select this option, the Dictionary Update Service uses the following settings configured in this policy (Dictionary Update Policy); continue with [Step 4b on page 962](#).

NOTE: Do not select this option for a Standalone Server and a Root Server. You must manually configure the settings of the policy.

- 4b** In the *Source Service Object* field, browse to select the DN of the Inventory server, which provides the dictionary updates.
- 4c** Select the IP address or the DNS name of the Inventory server, which provides the dictionary updates.
- 4d** If the source Inventory server is across the firewall, specify the IP address or the DNS name and the port number of the XML proxy server.
- 4e** Click *Apply*.
- 5** Click the *Dictionary Update Policy* tab, then click the *Dictionary Update Schedule* suboption.
- 6** Configure the Dictionary Update Schedule page to establish the schedule for running the Dictionary Consumer.
- We recommend that you configure the Weekly schedule.
- 7** Click *Apply*.
- 8** (Conditional) If you have not yet associated the Server Package, you are prompted to associate it with an Inventory server or a container. The policy you configured and enabled earlier will not be in effect until you associate this policy package with an Inventory server or a container. To associate the policy package:
- 8a** Click the *Associations* tab, then click *Add*.
- 8b** Browse for and select the Inventory server or the container that you want to associate the Dictionary Update policy to.
- 8c** Click *OK*, then click *OK*.
- 9** Click *Apply*, then click *Close*.

NOTE: If you want to modify the Dictionary Update policy settings, you need not stop the Inventory services.

73.9 Setting Up Distribution of Dictionary

A software dictionary can be updated in the following ways:

- Manually download the latest version of the dictionary from TID 10093255 in the [Novell Support Knowledgebase \(http://www.novell.com/support\)](#) to each Inventory server.

NOTE: The dictionary is updated and published once in every three months in this TID.

- Manually download the dictionary from the [Novell Support \(http://www.novell.com/support\)](#) web site to one Inventory server (preferably, the Root Server) and automatically distribute the dictionary to all servers in your setup by configuring the Dictionary Update policy.

An Inventory server can receive dictionary updates from any other Inventory server, irrespective of the server's role. The role of the Inventory server indicates whether the server receives the inventory information, stores the information into a local Inventory database, or rolls up the inventory information.

To update and distribute the software dictionary between Inventory servers:

- 1 Manually download the dictionary from the [Novell Support Web site \(http://www.novell.com/support\)](http://www.novell.com/support) and save it in the `zenworks_installation_directory\zenworks\inv\server\dictdir` directory on the Inventory server.
- 2 Configure the Dictionary Update policy. For more information see, [Section 73.8, “Configuring the Dictionary Update Policy,” on page 961.](#)

All Inventory servers have Dictionary Provider and Dictionary Consumer services that are automatically installed during the Workstation Inventory installation.

When an Inventory server is started, the Dictionary Consumer reads the Dictionary Update policy and contacts the Dictionary Provider (running on another Inventory server) specified in the policy.

Subsequently, the Dictionary Consumer checks for the dictionary updates based on the schedule set in the Dictionary Update policy. It compares the date of the dictionary file on the Dictionary Provider with the file that has been locally stored. If the file on the Dictionary Provider is newer, then the Dictionary Consumer downloads the file from the Dictionary Provider using XML-RPC as per the schedule.

The user-defined rules in the downloaded dictionary file are merged with the rules present in the local dictionary. If the merge yields a different set of rules from those locally present, the consolidated set of rules is written to the local dictionary. During the merge process, conflicts might arise, which are resolved on the basis of the following considerations:

- The rules in the downloaded dictionary always override the rules in the local dictionary.
- If a conflict arises between the software identifiers, the conflicting identifiers in the local dictionary are removed from the final (merged) dictionary.
- For a software dictionary rule, the final result is obtained by first writing the downloaded rules and then the local rules into the final dictionary; eliminating the duplicates during the process. This ensures that the downloaded software rules precede the local rules.

The following scenario illustrates the distribution of the software dictionary among the Inventory servers.

In this scenario, there is an Inventory tree consisting of one Root Server (R1), one Leaf Server (L1), and two Standalone servers (S1 and S2). L1 rolls up the inventory information to R1.

Follow the below procedure to update the software dictionary on all the Inventory servers.

1. Manually download the dictionary on R1 from the [Novell Support Web site \(http://www.novell.com/support\)](http://www.novell.com/support).
2. Create and configure a Dictionary Update policy by specifying R1 as the Dictionary Provider, and associate the policy to L1. For more information on how to configure the Dictionary Update policy, see [Section 73.8, “Configuring the Dictionary Update Policy,” on page 961.](#)

3. For S1 and S2, you can either manually download the dictionary from the [Novell Support Web site \(http://www.novell.com/support\)](http://www.novell.com/support) or configure the Inventory servers to automatically receive the latest version of the dictionary from R1.

For S1 and S2 to automatically receive the latest version of the dictionary from R1, create and configure a Dictionary Update policy by specifying R1 as the Dictionary Provider, and associate the policy to S1 and S2. For more information on how to configure the Dictionary Update policy, see [Section 73.8, “Configuring the Dictionary Update Policy,” on page 961](#).

Understanding Workstation Inventory Components

74

The following sections describe the Novell® ZENworks® 7 Workstation Inventory components and processes:

- [Section 74.1, “Understanding the Inventory Service Manager,” on page 965](#)
- [Section 74.2, “Understanding the Server Configuration Service,” on page 968](#)
- [Section 74.3, “Understanding the Inventory Scanner,” on page 968](#)
- [Section 74.4, “Understanding the Sender and Receiver,” on page 974](#)
- [Section 74.5, “Understanding the TCP Receiver,” on page 978](#)
- [Section 74.6, “Understanding the Selector,” on page 979](#)
- [Section 74.7, “Understanding the Storer,” on page 981](#)
- [Section 74.8, “Understanding the Str Converter,” on page 981](#)
- [Section 74.9, “Understanding the Inventory Sync Service,” on page 982](#)
- [Section 74.10, “Understanding Dictionary Provider and Dictionary Consumer,” on page 983](#)
- [Section 76.7, “Removing Redundant Inventoried Workstations from the Inventory Database,” on page 1084](#)
- [Section 74.11, “Understanding the Upgrade Service,” on page 983](#)
- [Section 74.12, “An Overview of the Inventory Components on an Inventory Server,” on page 985](#)
- [Section 74.13, “Understanding the Inventory Database,” on page 986](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

74.1 Understanding the Inventory Service Manager

The Inventory Service Manager loads the inventory components on the Inventory server, based on the configuration parameters specified in the Inventory server properties file.

This sections contains the following:

- [“List of Services” on page 966](#)
- [“Services on NetWare Inventory Servers” on page 966](#)
- [“Services on Windows Servers” on page 967](#)
- [Section 74.1.4, “Services on Linux Inventory Servers,” on page 967](#)

74.1.1 List of Services

The Service Manager loads the following important services. You can obtain the list of services that the Service Manager loads from the property file in

inventory_server_installation_directory_or_volume\zenworks\inv\server\wminv\properties.

Server Configuration Service

Inventory Scheduler Service

Inventory Scheduler Service

Selector Service

Receiver Service

Sender Service

Storer Service

Str Converter Service

Upgrade Service

Dictionary Consumer Service

Dictionary Provider Service

You can use these service names to list, start, and stop the respective services.

The Inventory Service Manager reads the server property file (*config.properties*) and the role-based property file in the

inventory_server_installation_directory_or_volume\zenworks\inv\server\wminv\properties directory, and loads the required services and server components.

IMPORTANT: Do not modify the property files because the updates might fail to load the services or the Service Manager.

74.1.2 Services on NetWare Inventory Servers

To start the Inventory server on a Novell NetWare® Inventory server, run *startinv.ncf* at the server console prompt.

You can start, stop, or list the services, if the Inventory Service Manager is already loaded.

- To check if the Inventory Service Manager is loaded, enter *java -show* at the Inventory server prompt

This displays the following message:

```
com.novell.zenworks.inventory.servercommonZENWorksInventoryService
Manager
```

- To start an Inventory service, enter *StartSer service_name* at the Inventory server prompt. *service_name* refers to any of the listed services. Follow the service naming syntax when you modify the *service_name*.

For example, to start the Storer, enter *StartSer Storer*

- To stop an Inventory service, enter *StopSer service_name* at the Inventory server prompt. *service_name* refers to any of the listed services. Follow the service naming syntax when you modify the *service_name*

For example, to stop the Storer, enter `StopSer Storer`

- To stop all Inventory services, enter `StopSer *` at the console prompt.
- To list an Inventory service, enter `ListSer service_name` at the Inventory server prompt. *service_name* refers to any of the listed services. Follow the service naming syntax when you modify the *service_name*.
- To list all Inventory services, enter `ListSer *` at the console prompt.

74.1.3 Services on Windows Servers

You can start, stop, or list the services, if the Inventory Service Manager is already loaded. In the Control Panel, double-click *Services*, and check the status of the Inventory service.

- To start the Inventory service on a Windows 2000/2003 Inventory server:
 1. In the Control Panel, double-click *Administrative Tools*.
 2. Double-click *Services*.
 3. Select *Novell Inventory Service*, then click *Start*.
- To start an Inventory service, go to the `installation_directory\inv\server\wminv\bin` directory, and enter `StartSer service_name` at the command prompt. *service_name* refers to any of the listed services. Follow the service naming syntax when you modify the *service_name*.

For example, to start the Storer, enter `StartSer Storer`

- To stop an Inventory service, go to the `installation_directory\inv\server\wminv\bin` directory, and enter `StopSer service_name` at the command prompt. *service_name* refers to any of the listed services. Follow the service naming syntax when you modify the *service_name*.

For example, to stop the Storer, enter `StopSer Storer`

- To list an Inventory service, go to the `installation_directory\inv\server\wminv\bin` directory, and enter `ListSer service_name` at the command prompt. *service_name* refers to any of the listed services. Follow the service naming syntax when you modify the *service_name*.

To list all Inventory services, enter `ListSer "*"`

- To stop the Inventory services on a Windows 2000/2003 Inventory server:
 1. In the Control Panel, double-click *Administrative Tools*.
 2. Double-click *Services*.
 3. Select *Novell Inventory Service*, then click *Stop*.

74.1.4 Services on Linux Inventory Servers

- To start all Inventory services, do any of the following ways:
 1. At the Linux server prompt, go to `/etc/init.d`.
 2. Enter `./novell-zdm-inv start`.

Or

To start all Inventory services from any directory on Linux, enter

```
/etc/init.d/novell-zdm-inv start
```

- To start a specific Inventory service:
 1. At the Linux server prompt, go to `/opt/novell/bin`.
 2. Enter `StartSer Inventory_service`.
- To stop all Inventory services, do any of the following ways:
 1. At the Linux server prompt, go to `/etc/init.d`.
 2. Enter `./novell-zdm-inv stop`.

Or

To stop all Inventory services from any directory on Linux, enter

```
/etc/init.d/novell-zdm-inv stop
```

- To stop a specific Inventory service:
 1. At the Linux server prompt, go to `/opt/novell/bin`.
 2. Enter `StopSer Inventory_service`.

The following table lists the Workstation Inventory components installed on Linux whose status you can check by executing commands at the Linux console prompt.

Table 74-1 *Commands to check the status of the Workstation Inventory components installed on Linux*

Workstation Inventory Component	Command To Be Entered At the Linux Console Prompt
Inventory server daemon	<code>/etc/init.d/novell-zdm-inv status</code>
Sybase daemon	<code>/etc/init.d/novell-zdm-sybase status</code>
Inventory Proxy daemon	<code>/etc/init.d/novell-zen-zws status</code>

74.2 Understanding the Server Configuration Service

The Server Configuration Service performs the following tasks:

- Reads the policy information from the Novell eDirectory™ and passes it to other Inventory components.
- Validates the policies to ensure that the policies are correctly configured.
- Validates the Inventory database engine version.

74.3 Understanding the Inventory Scanner

ZENworks 7 Desktop Management uses the Scanner to collect hardware and software information from Windows inventoried workstations.

The Scanner collects hardware details such as: floppy disk drive, hard disk drive, BIOS, bus, mouse, keyboard, display adapters, network adapter cards, modems, Jaz drives, Zip drives, sound cards, memory cards, serial ports, parallel ports, processors, and modems. The software scanning includes

checking for applications on the inventoried workstations and reporting the information about the scanned software, such as the vendor name, the product name and version, etc.

The following sections contain detailed information about the Inventory Scanners:

- [“Inventory Scanning Process” on page 969](#)
- [Section 74.3.2, “Types of Scan,” on page 969](#)
- [Section 74.3.3, “Scanning for the Hardware Inventory Information,” on page 970](#)
- [Section 74.3.4, “Scanning for the Software Inventory Information,” on page 971](#)
- [“Inventory Scanner Log Files” on page 974](#)

You can customize the hardware and the software information to be scanned. For more information, see [Section 76.2, “Customizing the Hardware Inventory Information To Be Scanned,” on page 1022](#) and [Section 76.3, “Customizing the Software Inventory Information To Be Scanned For ZENworks 7 Inventoried Workstations,” on page 1035](#).

74.3.1 Inventory Scanning Process

1. The Workstation Inventory policy lets you configure the Scheduler to adjust scanning times at the inventoried workstations. You can set different actions to run the scanners on one or more inventoried workstations.
2. The Inventory scanner checks whether an updated dictionary is available at its Inventory server and downloads the updated dictionary.
3. The scanner scans for the hardware and software information.
4. The scan information collected by the scanners is stored as scan data files (`.str`). The files are sent to the Inventory server.

74.3.2 Types of Scan

You can perform the following types of scans:

- **Full Scan:** The Scanner enforces a complete scanning of the inventoried workstation. This setting overrides the option set in the Inventory Service Object property page associated with the inventoried workstation. When scanning the inventoried workstation for the first time, the Scanner collects the complete hardware and software inventory of the inventoried workstation.
- **Delta Scan:** After the inventoried workstation is scanned, on subsequent scans, the Scanner compares the current inventory information to the history data that it maintains. If there are any changes to the inventoried workstation, the Scanner reports the delta scan data, which contains only the changes in inventory since the last scan was reported. The Delta Scan setting is the default scan operation for each successive scan after the first scanning of the inventoried workstation.
- **Scheduled Full Scan:** After a specified number of delta scans, the Scanner enforces a full scan of the inventoried workstations, associated with the Workstation Inventory policy. The Scheduled Full scan can contain full and delta inventory information based on the Workstation Inventory policy settings. By default, one Scheduled full scan happens after every five delta scans.

74.3.3 Scanning for the Hardware Inventory Information

Following are the sources on the inventoried workstations from where the hardware inventory information is scanned:

- “Desktop Management Interface (DMI)” on page 970
- “Windows Management Instrumentation (WMI)” on page 970
- “Probe” on page 971

For more information about the hardware information collected by the Inventory scanner, see [Appendix N, “Hardware Information Collected by the Inventory Scanners,” on page 1199](#).

Desktop Management Interface (DMI)

The scanners for scanning the inventoried workstations (Windows 98, Windows 2000, and Windows XP) also include scanning based on the industry-standard Desktop Management Interface (DMI) specification 2.0. These programs use the Management Interface (MI) of DMI to look for the hardware components installed on the inventoried workstation. The scanners scan for specific components that are instrumented on the inventoried workstation through DMI. The scanners query the DMI service layer to retrieve this information.

The MI allows the DMI-compliant scanners to probe the Service Provider within the Service Layer. The Service Provider collects information from the manageable components and stores the collected information in the Management Information Format database. The Component Interface (CI) communicates with the manageable components and the Service layer. The following figure shows the scanner interaction with DMI.

For more information on DMI standards, see the [DMTF Web site \(http://www.dmtf.org\)](http://www.dmtf.org).

NOTE: If the inventoried workstations are DMI compliant and if the Enable DMI Scan check box is selected in the Workstation Inventory policy, the scanners collect hardware information by querying the DMI Service Layer. Otherwise, the scanners probe for the hardware.

We recommend that you instrument DMI and also install DMI components that are supplied by the vendors.

For example, if you have a Compaq* Family Deskpro* EN Model-SFF6500 workstation running under Windows 98, download the Management Product software - Compaq Insight Management Desktop Agents software for Windows 98 from the Compaq Web site.

For Dell* workstations, access the DM/Desktop Management Utilities software from the Dell Web site.

Windows Management Instrumentation (WMI)

The scanners collect hardware information from Windows inventoried workstations based on Microsoft Windows Management Instrumentation (WMI) specification.

WMI is the Microsoft implementation of Web-Based Enterprise Management (WBEM) that enables accessing management information in an enterprise environment. WMI 1.5 is fully compliant with Common Information Model (CIM) schema, which is an industry standard. For more information, see [Microsoft WMI Web site \(http://www.microsoft.com/hwdev/driver/WMI\)](http://www.microsoft.com/hwdev/driver/WMI). WMI also works with existing management standards, such as DMI and SNMP.

The scanners use WMI to look for the hardware components installed on the inventoried workstation. The scanners also scan for specific components that are instrumented on the inventoried workstation through WMI.

WMI-compliant scanners are supported on Windows 98, Windows XP, and Windows 2000 inventoried workstations only.

You can view the WMI information of the inventoried workstations in the Workstation Inventory.

To obtain WMI information from the inventoried workstation, you must first download Microsoft's Windows Management Instrumentation - Core Software Installation from [Microsoft WMI Web site](http://msdn.microsoft.com/downloads/default.asp?url=/downloads/sample.asp?url=/msdn-files/027/001/576/msdncompositedoc.xml) (<http://msdn.microsoft.com/downloads/default.asp?url=/downloads/sample.asp?url=/msdn-files/027/001/576/msdncompositedoc.xml>), and then install WMI Core Software on Windows 98 workstations

IMPORTANT: Only the WMI Core Software Installation download is required to instrument an inventoried workstation for WMI. To troubleshoot any WMI related problems, you can use the WMI SDK download. Also, on Windows 2000/XP workstations, the WMI Core Software is already installed.

By default, both DMI and WMI scanning are enabled. To disable either DMI or WMI scanning, deselect the *Enable DMI* or *Enable WMI* check box in the Inventory policy window.

Probe

Probe is a special built-in algorithm in the Inventory scanner, which is used to collect hardware information.

74.3.4 Scanning for the Software Inventory Information

The Inventory scanner scans for the following software inventory information on the Windows inventoried workstations:

- “Installed Software Information” on page 971
- “Disk Usage” on page 972
- “File Information” on page 972
- “AntiVirus Definition Files” on page 973

Installed Software Information

The scanner collects software information from the following sources on the inventoried workstation:

MSI: Includes software that is installed on the inventoried workstations using the Microsoft Installer.

Add-Remove Programs: Includes software that is listed in the Add/Remove Programs window.

Dictionary-based scan: Includes software that is collected based on the software dictionary rules. For more information, see [Section 76.3, “Customizing the Software Inventory Information To Be Scanned For ZENworks 7 Inventoried Workstations,” on page 1035.](#)

Probe: Probe is a special built-in algorithm in the Inventory scanner. It is used to collect software information about Windows operating system, Internet Explorer, Media Player, Outlook* Express, Microsoft Office and its installed components, Novell Client™ and its installed components, and the ZENworks suite and its installed components.

The following table shows the software information collected by the scanner from the various sources:

Table 74-2 *Software Information collected by the Inventory Scanner*

Scanned Attributes	MSI	Add/Remove Programs	Dictionary-based scan	Probe
Product Name	Yes	Yes	Yes	Yes
Vendor Name	Yes	No	Yes	Yes
Product Version	Yes	Yes	Yes	Yes
Product Identifier	Yes	Yes	No	No
Product Install Location	Yes	Yes	Yes	Yes
Category	No	No	Yes	No
Description	No	No	Yes	No
Help Link	Yes	Yes	No	No
MSI Package GUID	Yes	Yes	No	Yes
Display/Internal Version	Yes	Yes	Yes	Yes
Language	Yes	Yes	No	Yes
UnInstall String	Yes	Yes	No	No
Installation Source	Yes	Yes	No	No
Display Name	Yes	Yes	No	Yes
Support Pack	No	No	No	Yes
Product Edition	No	No	No	Yes
Last Execution Time	No	Yes	No	No
Usage Count	No	Yes	No	No

Disk Usage

The scanner collects the total disk usage information for the file extensions that are configured in the Software Dictionary editor. For more information, see [Section 76.3, “Customizing the Software Inventory Information To Be Scanned For ZENworks 7 Inventoried Workstations,”](#) on page 1035.

File Information

The scanner reports certain information for the files that match with the dictionary entries, and the files that belong to the unidentified software list, which is configured using the software dictionary rules. For more information, see [Section 76.3.10, “Configuring the Software Dictionary Rules,”](#) on page 1045

The scanner reports the following file attributes: FileName, FileSize, LastModifiedTime, InternalName, FileVersion, ProductName, ProductVersion, CompanyName, Language, DirectoryPath, and SoftwareDictionaryID.

AntiVirus Definition Files

The scanner collects information about the latest virus definition date and version that is installed on the inventoried workstations for the following product versions:

Symantec* AntiVirus Corporate Edition 8.0
Symantec* AntiVirus Corporate Edition 9.0
Symantec* AntiVirus Corporate Edition 10.0
Norton AntiVirus* Corporate Edition for Windows 7.0
Norton AntiVirus Corporate Edition 7.6.1.0000
Symantec Norton AntiVirus 2000
Symantec Norton Internet Security 2002
Symantec Norton AntiVirus 2003 (9.00)
Symantec Norton AntiVirus 2003 Professional Edition (9.00)
Symantec Norton AntiVirus 2004 (10.00)
Symantec Norton Internet Security 2004 (10.00)
Symantec Norton AntiVirus 2004 Professional (10.00)
Symantec Norton Internet Security 2004 Professional (10.00)
Symantec Norton AntiVirus 2005 Professional (11.00)
Symantec Norton Internet Security 2005 Professional (11.00)
Network Associates McAfee* VirusScan* 4.0.3 (Windows 9x)
Network Associates McAfee VirusScan NT 4.0.3a (Windows NT)
Network Associates McAfee NetShield 4.5.0
Network Associates McAfee VirusScan 4.5.0
Network Associates McAfee VirusScan 4.5.1
Network Associates McAfee VirusScan (McAfee Security Center) 8.0
Network Associates McAfee VirusScan ASaP
Network Associates McAfee VirusScan Enterprise 7.1
Network Associates McAfee VirusScan Enterprise 8.0
Central Command Vexira AntiVirus Guard for Windows XP (2000 + NT) 2.10
Central Command Vexira AntiVirus Windows 95/98
Central Command Vexira AntiVirus NT/2000 Servers
Central Command Vexira AntiVirus Server Edition (6.26.xx.xx)
Sophos Anti-Virus - Windows NT/2000/XP/2003
Sophos Anti-Virus - Windows 95/98
Trend Micro PC-cillin 2002 (9.x)
Trend Micro PC-cillin 2003 (10.x)
Trend Micro Internet Security 11.x (PC-cillin)
Trend Micro Internet Security 2005 12.x (PC-cillin)
Trend Micro Server Protect 5.xx
Trend Micro OfficeScan 5.xx - Client for Windows NT/2000/XP
Trend Micro OfficeScan 5.xx - Client for Windows 9x

74.3.5 Inventory Scanner Log Files

Table 74-3 Location and brief description of the Inventory Scanner log files

Filename	Location	Description
inventory.xml	windows_installation_drive /zenworks	Contains complete hardware and software information after the scan.
inventorydata.xml	windows_installation_drive /zenworks	Contains delta scan information.
zenererrors.log	windows_installation_drive /zenworks	Contains the error and status information for the latest scan of the inventoried workstation.

74.4 Understanding the Sender and Receiver

The Sender and the Receiver on the Inventory servers transfer the scan files from the lower-level servers to the higher-level servers. The following sections contain more information:

- “Understanding the Sender” on page 975
- “Understanding the Receiver” on page 975
- “Understanding the Compressed Scan Data File” on page 976
- “Sender-Receiver Directories” on page 976
- Section 74.8, “Understanding the Str Converter,” on page 981

The processing done by the Sender-Receiver is as follows:

1. The Service Manager starts the Sender-Receiver component.
2. The Roll-Up Scheduler activates the Sender at the specified roll-up time.
3. The Sender moves the scan data files (.str) from the enterprise merge directory (entmergedir) to the enterprise push directory (entpushdir) and compresses the files as a .zip file.
4. Each .zip file is again compressed with the .prp file into a .zip file. The .prp file is an internal file containing information about the .zip file.
5. The Sender sends the .zip file from the entpushdir directory to the Receiver on the next-level Inventory server.
6. The Receiver places the .zip files to the entpushdir\zipdir directory.
7. The Receiver copies the .zip files to the entpushdir directory and deletes the .zip files from the entpushdir\zipdir directory.
8. The Receiver copies the .zip files to the database directory (dbdir) if a database is attached to the server.
9. The Sender-Receiver logs the status in eDirectory.

74.4.1 Understanding the Sender

The Sender is a Java component that runs on any Leaf Server or on the Intermediate Server. The Sender is a service loaded by the Service Manager. See [Section 74.12, “An Overview of the Inventory Components on an Inventory Server,” on page 985](#) for a quick reference table of server components.

The flow of information from the Sender in the roll-up of inventory information is as follows:

1. The Service Manager starts the Sender on the Inventory server. At the specified time scheduled in the Roll-Up Schedule, the Sender moves the scan data files (`.str`) from the enterprise merge directory (`entmergedir`) to the enterprise push directory (`entpushdir`).

The Sender compresses these `.str` files in the `entpushdir` directory of the server as a `.zip` file and then deletes the `.str` files. This `.zip` file is again compressed with the `.prp` file into a `.zip` file. The `.prp` file is an internal file containing information about the `.zip` file. For more information, see [“Understanding the Compressed Scan Data File” on page 976](#).

2. The Sender creates a new record in the `zeninvRollUpLog` attribute of the Inventory Service object in eDirectory with the following details: server on which the Sender compresses the `.str` files and the name and size of the `.zip` file.
3. Based on the Discard Scan Data Time in the Inventory Service object properties of the Receiver, the Sender deletes the compressed `.zip` files in the `entpushdir` directory that have been created earlier than the specified discard scan data time. This removes unwanted scan information being sent in the roll-up.
4. The Sender sends the compressed `.zip` files to the Receiver, with the oldest compressed files sent first.
5. The Sender, after transferring the `.zip` files, deletes the compressed files in the `entpushdir` directory.
6. After the roll-up of information, the Sender updates the `zeninvRollUpLog` attribute of the server on which the compressed file was created with the following details: server from which the Sender transmitted the file, name of the `.zip` file, time of transmission, total time taken to transmit the files, and the server to which it was sent.

The status information for all actions of the Sender is logged in the Roll-Up Log and Server Status log. For more information, see [“Monitoring Workstation Inventory Using Status Logs” on page 1177](#).

If the Sender is unable to connect to the Receiver, the Sender retries to connect after 10 seconds. The time interval increases exponentially by a factor of 2. After 14 retries, the Sender stops trying to connect to the Receiver. The Sender retries for approximately 23 hours before it discontinues trying. The Sender does not process any other information while it is establishing the connection.

74.4.2 Understanding the Receiver

The Receiver is a Java component that runs on the Intermediate Server or on the Root Server. The Receiver is a service loaded by the Service Manager. See [Section 74.12, “An Overview of the Inventory Components on an Inventory Server,” on page 985](#) for a quick reference table of server components.

On a Standalone Server, the Receiver is not loaded.

The processing done by the Receiver is as follows:

1. The Receiver receives the scan .zip file from the Sender. The file is placed in the `entpushdir\zipdir` directory.
2. The Receiver copies the .zip file to the `entpushdir` directory and deletes the .zip files from the `entpushdir\zipdir` directory.
On an Intermediate Server, the file is copied to `entpushdir`. On an Intermediate Server with Database, or an Intermediate Server with Database and Inventoried Workstations, the file is copied to `\entpushdir` and copied to the Database Directory (`\dbdir`).
3. The Receiver on the Root Server or the Root Server with Inventoried Workstations receives the .zip files from the Senders and places the .zip files in the `entpushdir\zipdir` directory. It copies the files to the DBDIR directory on the server.
4. The Receiver logs the status information in the Roll-Up log. For more information, see [“Monitoring Workstation Inventory Using Status Logs” on page 1177](#).

74.4.3 Understanding the Compressed Scan Data File

The Sender compresses the scan data files (.str) into a .zip file. This .zip file is again compressed with the .prp file into a .zip file. The .zip file (containing the .zip files and .prp) is named using the following naming conventions:

scheduledtime_inventoryservername_treename_storedstatus.zip

where *scheduledtime* refers to the date and time when the .zip file is created, *inventoryservername* refers to the Inventory server on which the .zip file was compressed, *treename* refers to the unique tree name in which the .zip file is currently located, *storedstatus* refers to the storage status of the .zip file, and *zip* is the file extension for the compressed files.

The *storedstatus* is represented by 0, 1, or 2. 0 indicates the .zip file has not yet been stored. 1 indicates the .zip file will be stored for the first time in the server. 2 indicates the .zip file has already been stored once.

The .zip filename changes depending on if the database is attached to the server.

The .zip file contains the .zip files and a property file. The property file is named using the following conventions:

scheduledtime_inventoryservername.prp

The property file contains the scheduled time, Inventory server name, and signature. The signature helps to authenticate the .zip file.

Each .zip file can contain a maximum of 50 .str files.

74.4.4 Sender-Receiver Directories

The following table provides a quick reference of the directories that the Sender-Receiver uses:

Table 74-4 List of directories used by Sender and Receiver

Server	Sender	Receiver	ENTMERGDIR	ENTPUSHDIR ZIPDIR	ENTPUSHDIR	DBDIR
Leaf Server, Leaf Server with Database	Runs on this Inventory server	--	Sender moves the .str files to the entpushdir .	--	Sender compresses the .str files as a .zip file. Sender deletes the .str files. Sends the .zip file to the next-level Inventory server.	--
Intermediate Server	Runs on this Inventory server	Runs on this Inventory server	--	Receiver receives the .zip files from the lower-level server in this directory.	Receiver copies the .zip files from the lower-level Inventory server in this directory. Sender sends the .zip files to the next-level Inventory server.	--
Intermediate Server with Inventoried Workstations	Runs on this Inventory server	Runs on this Inventory server	Sender moves the .str files to the entpushdir.	Receiver receives the .zip files from the lower-level Inventory server in this directory.	Receiver copies the .zip files from ZIPDIR into this directory. Sender sends the .zip files to the next-level Inventory server. Sender compresses the .str files in to .zip files. Sender deletes the .str files.	--
Intermediate Server with Database	Runs on this Inventory server	Runs on this Inventory server	--	Receiver receives the .zip files from the lower-level server in this directory.	Receiver copies the .zip files from ZIPDIR into this directory. Sender sends the .zip file to the next-level Inventory server.	Receiver copies the file in this directory.

Server	Sender	Receiver	ENTMERGDIR	ENTPUSHDIR ZIPDIR	ENTPUSHDIR	DBDIR
Intermediate Server with Database and Workstations	Runs on this Inventory server	Runs on this Inventory server	Sender moves the .str files to the entpushdir.	Receiver receives the .zip files from the lower-level Inventory server in this directory.	Receiver copies the .zip files from ZIPDIR into this directory. Sender compresses the .str files as a .zip file. Sender deletes the .str files. Sender sends the .zip file to the next-level Inventory server.	Receiver copies the file in this directory.
Root Server, Root Server with Inventoried Workstations	--	Runs on this Inventory server	--	Receiver receives the .zip files from the lower-level Inventory server in this directory.	--	Receiver copies the .zip files from the lower-level Inventory server in this directory.

74.5 Understanding the TCP Receiver

The TCP Receiver is a Java component on the Inventory server that converts ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management residual .str and .zip files on the server and the .zip files received from lower-level ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management Inventory servers to the format required by the ZENworks 7 Desktop Management Inventory server. See [Section 74.12, “An Overview of the Inventory Components on an Inventory Server,” on page 985](#) for a quick reference table of server components.

The processing done by the TCP Receiver is as follows:

1. The Service Manager starts the TCP Receiver on the Inventory server.
2. The TCP Receiver receives the scan .zip file from the ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management Sender and places the file in the Receiver Conversion directory (entpushdir\recvconv).
3. The TCP Receiver converts the following ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management files into the format required by ZENworks 7 Desktop Management components:

Residual .zip files in \dbdir
 .str and .prp files in dbdir\temp
 Residual .zip files in \entpushdir
 Residual .str files in \entpushdir
 Residual .str files in \entmergedir

.zip files

After conversion, these .zip files are copied to entpushdir\zipdir directory for further processing by the Receiver.

4. The Receiver logs the status information in the Roll-Up log. For more information, see [“Monitoring Workstation Inventory Using Status Logs” on page 1177](#).

The TCP Receiver uses the following directories:

- The TCP Receiver receives the ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management .zip files in \entpushdir\recvconv directory. The .zip files are converted to the ZENworks 7 Desktop Management format and copied to \entpushdir\zipdir directory. The Upgrade service copies the ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management residual .zip files in the \dbdir directory to the \entpushdir\dbdirconv directory. The .zip files are converted to the ZENworks 7 Desktop Management format and copied to the \dbdir directory.
- The Upgrade service copies the residual .str and .prp files in the dbdir\temp directory to the \entpushdir\dbdirconv directory. The .str and .prp files are converted to the ZENworks 7 Desktop Management format and copied to the \dbdir directory.
- The Upgrade service copies the residual .zip files in entpushdir directory to the \entpushdir\entpushzipconv directory. The .zip files are converted to the ZENworks 7 Desktop Management format and copied to the \entpushdir directory.
- The Upgrade service copies the residual .str files in the entpushdir directory to the \entpushdir\entpushstrconv directory. The .str files are converted to the ZENworks 7 Desktop Management format and copied to the \entpushdir directory.
- The Upgrade service copies residual .str files in the entmergedir to the \entpushdir\entmergeconv directory. The .str files are converted to the ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management format and copied to the \entmergedir directory.

74.6 Understanding the Selector

The Selector is a Java component on the server that receives the inventory information from the inventoried workstations. These servers can be any of the following: Leaf Server, Leaf Server with Database, Intermediate Server with Database and Inventoried Workstations, Intermediate Server with Inventoried Workstations, Root Server with Inventoried Workstations, and Standalone Server. See [Section 74.12, “An Overview of the Inventory Components on an Inventory Server,” on page 985](#) for a quick reference table of server components.

The processing done by the Selector is as follows:

1. While scanning the inventoried workstation, the Scanner creates a scan data file (.str) in the scan directory (\scandir) at the server for each scan done on the inventoried workstation. The location of \scandir is obtained from the Inventory Service object. The Selector processes the .str files placed by the Scanner in the \scandir directory.

The Selector also detects the .str files generated by the ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management Scanners and moves the .str files to the \scandir\conv directory for the Str Converter to process these files.

The Selector processes the following types of `.str` files.

- **Full:** Contains complete hardware and software inventory information of the inventoried workstation.
- **Delta:** Contains only the changes in the inventory since the last scan.
- **Delete:** Contains the information needed for the Storer to delete the inventoried workstation object from the database. This `.str` file is created when the inventoried workstation object is deleted from the eDirectory.
- **Scheduled Full:** Contains full and delta scans. Depending upon the last stored status of the inventoried workstation object data, the Storer processes either the full or delta scan. The Scheduled Full `.str` file is used by the Storer to rectify the errors in the inventoried workstation inventory data that is stored in the database.

Using the **Workstation Inventory Policy**, you can configure the Scheduled Full scan to send a full scan after a certain number of delta scans. The value must be between 5 and 65535. If you do not want the Scheduled Full scan, set the value to 65535.

- The Selector checks for the following conditions to ensure that the `.str` file, generated by the Scanner, is valid.
 - If a Scheduled Full scan is done at the inventoried workstation, the `.str` file should contain both full and delta scan data. The Identification section in the Scheduled Full Str file should have `SCHEDFULL` as ScanType.
 - If delta scan is done at the inventoried workstation, the `.str` file should contain two instances of the Inventory Scanner objects.
 - The integer value logged in the `.str` file is based on the `.str` file name with the actual value of the `.str` file.
 - The actual size of the `.str` file should be in sync with the size recorded in the `.str` file.

The Selector processes only valid `.str` files. If invalid files are present in the directory, the Selector deletes them.

- Based on the role of the server, the Selector copies the individual `.str` files from the `\scandir` directory to the `dbdir\entmergedir` directory.

The following table lists the directories that the Selector copies or renames the files to:

Server	Copies the .str file to the database directory (dbdir)	Renames the .str file in the database directory (dbdir)	Renames the .str file in the enterprise merge directory (entmergedir)
Leaf Server with Database	Yes	--	Yes
Leaf Server	--	--	Yes
Intermediate Server with Database and Inventoried Workstations	Yes	--	Yes
Standalone Server	--	Yes	--
Root Server with Inventoried Workstations	--	Yes	--

- The Selector updates the sequence number of valid `.str` files in eDirectory.

The Selector determines whether to enforce a full scan if the scanning sequence number in the `.str` file is improper. If the `.str` file is invalid or if there are discrepancies in the sequence number of the `.str` file, the Selector enforces a full scan.

5. The Selector logs the status in the Server log. For more information, see [“Monitoring Workstation Inventory Using Status Logs” on page 1177](#).

The Selector removes the existing `.str` files in the `\scandir` directory.

74.7 Understanding the Storer

The Storer is a Java component on the server that has a database attached to it. These servers can be any of the following: Leaf Server with Database, Intermediate Server with Database, Intermediate Server with Database and Inventoried Workstations, Root Server, and Root Server with Inventoried Workstations. See [Section 74.12, “An Overview of the Inventory Components on an Inventory Server,” on page 985](#) for a quick reference table of server components.

The Storer runs as a service loaded by the Service Manager. It processes the files in the `dbdir` directory.

The processing done by the Storer is as follows:

1. The Storer reads the Startup configuration parameters from the Inventory Server Configuration Service.
2. The Selector places the `.str` files in `dbdir` and the Receiver places the `.zip` files in `dbdir`.
3. The Storer processes the `.str` files and `.zip` files alternately.
4. The Storer extracts the `.zip` file containing the compressed `.zip` files and the `.prp` file to a temp directory (`dbdir\temp`) and updates the database with the inventory information.
5. If the inventoried workstations are connected directly to the Inventory server or if the `.str` files are stored for the first time in the tree, the Storer forces a full scan of an inventoried workstation if there are errors in the `.str` files. However, enforcing a full scan of the inventoried workstations located in a different tree is not supported.
6. The Storer updates the status in the Workstation Status log and updates the Roll-Up log. For more information, see [“Monitoring Workstation Inventory Using Status Logs” on page 1177](#).

If the inventoried workstations are connected directly to the Inventory server or if the `.str` files are stored for the first time in the tree, the status messages are logged directly into the inventoried workstation objects and can be viewed from the Workstation Status Log.

For rolling up inventory information across trees, the roll-up status messages are logged into the first Inventory server receiving the rolled-up `.str` files in the tree.

7. The Storer processes the converted ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management `.str` files and `.zip` files similarly to how it processes the ZENworks 7 Desktop Management `.str` files. However, the Storer does not enforce a full scan if a processing error occurs during the conversion to `.str` files.

74.8 Understanding the Str Converter

The Str Converter is a Java component on the Inventory server that has workstations attached to it. The Str Converter converts the ZENworks for Desktops 4.x and ZENworks 6.5 Desktop

Management files to the ZENworks 7 Desktop Management format in order to support backward compatibility with ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management.

You can run the Str Converter on the following servers:

- Leaf Server with Inventoried Workstations
- Leaf Server with Inventoried Workstations and Database
- Intermediate Server with Inventoried Workstations
- Intermediate Server with Inventoried Workstations and Database
- Root Server with Inventoried Workstations
- Standalone Server

For a quick reference table of server components, see [Section 74.12, “An Overview of the Inventory Components on an Inventory Server,” on page 985](#).

The Str Converter runs as a service loaded by the Service Manager. It processes the files in the `scandir\conv` directory.

The Str Converter process sequence is as follows:

1. The Str Converter reads the Startup configuration parameters, such as `scandir`, from the Inventory Server Configuration Service. If the `conv` and the `convtemp` directories do not exist, they are created under the `scandir` directory.
2. The selector places the ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management `.str` files in `conv` directory.
3. The Str Converter converts the ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management `.str` files into the ZENworks for Desktops 4.x format and places the files in the `convtemp` directory.
4. The converted `.str` files from the `convtemp` directory are moved to the `scandir` directory to be retrieved again by the Selector and are processed similar to ZENworks 7 Desktop Management `.str` files.

NOTE: The status log is not updated for the Str Converter component.

74.9 Understanding the Inventory Sync Service

The Inventory Sync Service is a service loaded by the Inventory Service Manager. It runs on all the Inventory servers that have inventoried workstations attached to them and removes the inventory information of the workstations from the attached Inventory database if they have already been deleted from eDirectory.

The Inventory Sync Service schedule is not automatically created after the Workstation Inventory installation. To schedule the Inventory Sync Service:

- 1 In ConsoleOne[®], right-click the Inventory Service object (Inventory Service_*server_name*) of the designated Inventory server, click *Properties*.
- 2 Click the *Inventory Service Object* tab, select the *Inventory Service Sync Schedule* suboption.
- 3 Modify the settings for scheduling the Inventory Sync Service.
- 4 Click *Apply*, then click *Close*.

The Inventory Sync Scheduler reads the Inventory Service Sync Schedule and triggers the Inventory Sync service at the specified time. The Inventory Sync service, is started by the Inventory Service Manager, but is activated by the Inventory Service Sync Scheduler.

The processing done by the Inventory Sync service is as follows:

1. The Inventory Sync Service maintains a list of DN of all the inventoried workstations attached to that Inventory server. The Inventory Sync Service reads the list and validates whether each inventoried workstation is registered in eDirectory.
2. If the inventoried workstation is not present in eDirectory, the Inventory Sync Service creates a `delete_str` file for that inventoried workstation in the `scandir` directory.
3. The Selector validates the `delete_str` files and copies the files into the `dbdir` and `entmergedir` directories.
4. The Storer reads the `delete_str` file in the `dbdir` and deletes the inventoried workstations from the attached Inventory database.
5. If the inventory deployment rolls up the inventory information across servers, the `delete_str` file is also rolled up to the next level Inventory server.

The inventoried workstation is removed from the Inventory database at all Inventory server tree hierarchy levels.

NOTE: If you restore a backup of the Inventory database, the database will contain the workstations that you have removed from eDirectory. The Inventory service does not remove these workstations. To remove these workstations, you must use the Inventory Removal Service. For more information, see [Section 76.7, “Removing Redundant Inventoried Workstations from the Inventory Database,” on page 1084](#).

74.10 Understanding Dictionary Provider and Dictionary Consumer

All Inventory servers and inventoried workstations have Dictionary Provider and Dictionary Consumer services that are automatically installed during the Workstation Inventory installation.

When an inventoried workstation is started, the Dictionary Consumer reads the Dictionary Update policy and contacts the Dictionary Provider (running on the Inventory server) specified in the policy.

Subsequently, the Dictionary Consumer checks for the dictionary updates based on the schedule set in the Dictionary Update policy. It compares the date of the dictionary file on the Dictionary Provider with the file that has been locally stored. If the file on the Dictionary Provider is newer, then the Dictionary Consumer downloads the file from the Dictionary Provider using XML-RPC as per the schedule.

74.11 Understanding the Upgrade Service

The Upgrade service runs as a service loaded by the Service Manager and performs the following functions:

1. Migrates ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management database to ZENworks 7 Desktop Management database. For more information, see [“Inventory Database Migration” on page 984](#).

2. Converts the ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management residue .str files to ZENworks 7 Desktop Management .str files. For more information, see [“Conversion and Movement of ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management Residue Files” on page 984.](#)

The Upgrade service performs all the functions in a state-driven method. This is to make sure that the Upgrade service does not execute the same steps when one step is executed successfully. The Upgrade service runs as an uninterrupted service. Therefore, you cannot manually stop the Upgrade service. The Upgrade service stops automatically after completing all its functions.

This section contains the following:

- [“Inventory Database Migration” on page 984](#)
- [“Conversion and Movement of ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management Residue Files” on page 984](#)

74.11.1 Inventory Database Migration

The Inventory database migration consists of two phases, Schema migration and Data migration.

The Inventory database migration involves the following activities:

1. The .zip files that contains all the SQL scripts are unzipped. Before the schema migration begins, the SQL files are transformed by filling the constants from the database.
2. **Schema migration phase:** The tables, procedures, views, and other related schema objects are either altered or added in compliance with the ZENworks 7 Desktop Management schema. The grants are provided appropriately to the tables, procedures, and views.
3. **Data migration phase:** The old data in the ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management schema is migrated to the ZENworks 7 Desktop Management schema. This phase consumes some time depending upon the size of the database.
4. Post-migration corrections.

The Database migration activity is additionally traced into a migration log, which could be found in the *installation_path\zenworks\inv\server\wminv\logs\migrationlogs* directory.

74.11.2 Conversion and Movement of ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management Residue Files

The residue files are the ZENworks for Desktops 4.x and ZENworks 6.5 Desktop Management .str or .zip files that are collected before the ZENworks 7 Desktop Management Inventory services runs for the first time.

The Upgrade service performs the following functions:

- Converts the .str files in the dbdir directory to ZENworks 7 Desktop Management .str files
- Moves the .zip files in the dbdir directory to the dbdirconv directory
- Moves the .zip files in the entpush directory to the entpushzipconv directory.
- Moves the .str files in the entpush directory to the entpushstrconv directory.

- Moves the .str files in the entmerge directory to the entmergeconv directory.
- Moves the .str files and the .prp files in the dbdir\temp directory to the dbdirtempconv directory.

This is to make sure that the ZENworks 7 Desktop Management Storer and Sender-Receiver services process the residue files present in the dbdir, entpush, and entmerge directories before they process and refresh the new inventory information.

WARNING: You must not delete the residue files during or after upgrade.

Dbdirconv, entpushzipconv, entpushstrconv, entmergeconv, and dbdirtempconv are auxiliary directories created by the upgrade service to facilitate its functioning.

74.12 An Overview of the Inventory Components on an Inventory Server

Depending on the type of the Inventory server, the following inventory components exist on the Inventory server.

Table 74-5 Inventory components running on the Inventory server

Server Component	Stand alone Server	Root Server	Root Server with Inventoried Workstations	Leaf Server with Database	Leaf Server	Intermediate Server	Intermediate Server with Database and Inventoried Workstations	Intermediate Server with Database	Intermediate Server with Inventoried Workstations
Service Manager or Server Configuration	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Selector	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes
Storer	Yes	Yes	Yes	Yes	No	No	Yes	Yes	No
Sender	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Receiver	No	Yes	Yes	No	No	Yes	Yes	Yes	Yes
Str Converter	Yes	No	Yes	Yes	Yes	No	Yes	No	Yes
TCP Receiver	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Upgrade Service	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Database	Yes	Yes	Yes	Yes	No	No	Yes	Yes	No

Server Component	Stand alone Server	Root Server	Root Server with Inventoried Workstations	Leaf Server with Database	Leaf Server	Intermediate Server	Intermediate Server with Database and Inventoried Workstations	Intermediate Server with Database	Intermediate Server with Inventoried Workstations
Dictionary Consumer and Dictionary Provider	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

74.13 Understanding the Inventory Database

The Inventory database functions as a repository of the inventoried workstation hardware and software information. The Storer updates the database with the inventory information of the `.str` file. The network administrator can view the inventory information, query the database, and generate inventory reports in ConsoleOne. For more information, see [“Understanding the Inventory Database Schema” on page 987](#).

Understanding the Inventory Database Schema

75

This section describes the design of the Novell® ZENworks® 7 Inventory database schema implemented using the Common Information Model (CIM) of the Distributed Management Task Force (DMTF). To understand this section effectively, you should be familiar with terminology such as CIM and Desktop Management Interface (DMI). You should also have a solid understanding of relational database based managed systems (RDBMS) and database concepts.

The following sections provide in-depth information:

- [Section 75.1, “Overview,” on page 987](#)
- [Section 75.2, “CIM Schema,” on page 988](#)
- [Section 75.3, “Inventory Database Schema in ZENworks 7 Desktop Management,” on page 995](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

75.1 Overview

The DMTF is the industry organization leading the development, adoption, and unification of management standards and initiatives for desktop, enterprise, and Internet environments. For more information about DMTF, see the [DMTF Web site \(http://www.dmtf.org\)](http://www.dmtf.org).

The DMTF CIM is an approach to system and network management that applies the basic structuring and conceptualization techniques of the object-oriented paradigm. The approach uses a uniform modeling formalism that together with the basic repertoire of object-oriented constructs supports the cooperative development of an object-oriented schema across multiple organizations.

A management schema is provided to establish a common conceptual framework at the level of a fundamental topology, both with respect to classification and association, and to a basic set of classes intended to establish a common framework for a description of the managed environment. The management schema is divided into the following conceptual layers:

- **Core Model:** An information model that captures notions that are applicable to all areas of management.
- **Common Model:** An information model that captures notions that are common to particular management areas, but independent of a particular technology or implementation. The common areas are systems, applications, databases, networks, and devices. The information model is specific enough to provide a basis for the development of management applications. This model provides a set of base classes for extension into the area of technology-specific schema. The Core and Common models together are expressed as the CIM schema.
- **Extension Schemas:** This schema represents technology-specific extensions of the Common model. These schemas are specific to environments, such as operating systems, for example, NetWare® or Microsoft Windows.

CIM comprises a specification and a schema (see the [DMTF Web site \(http://www.dmtf.org/standards/standard_cim.php\)](http://www.dmtf.org/standards/standard_cim.php)). The specification defines the meta-schema plus a concrete representation language called Managed Object Format (MOF).

75.2 CIM Schema

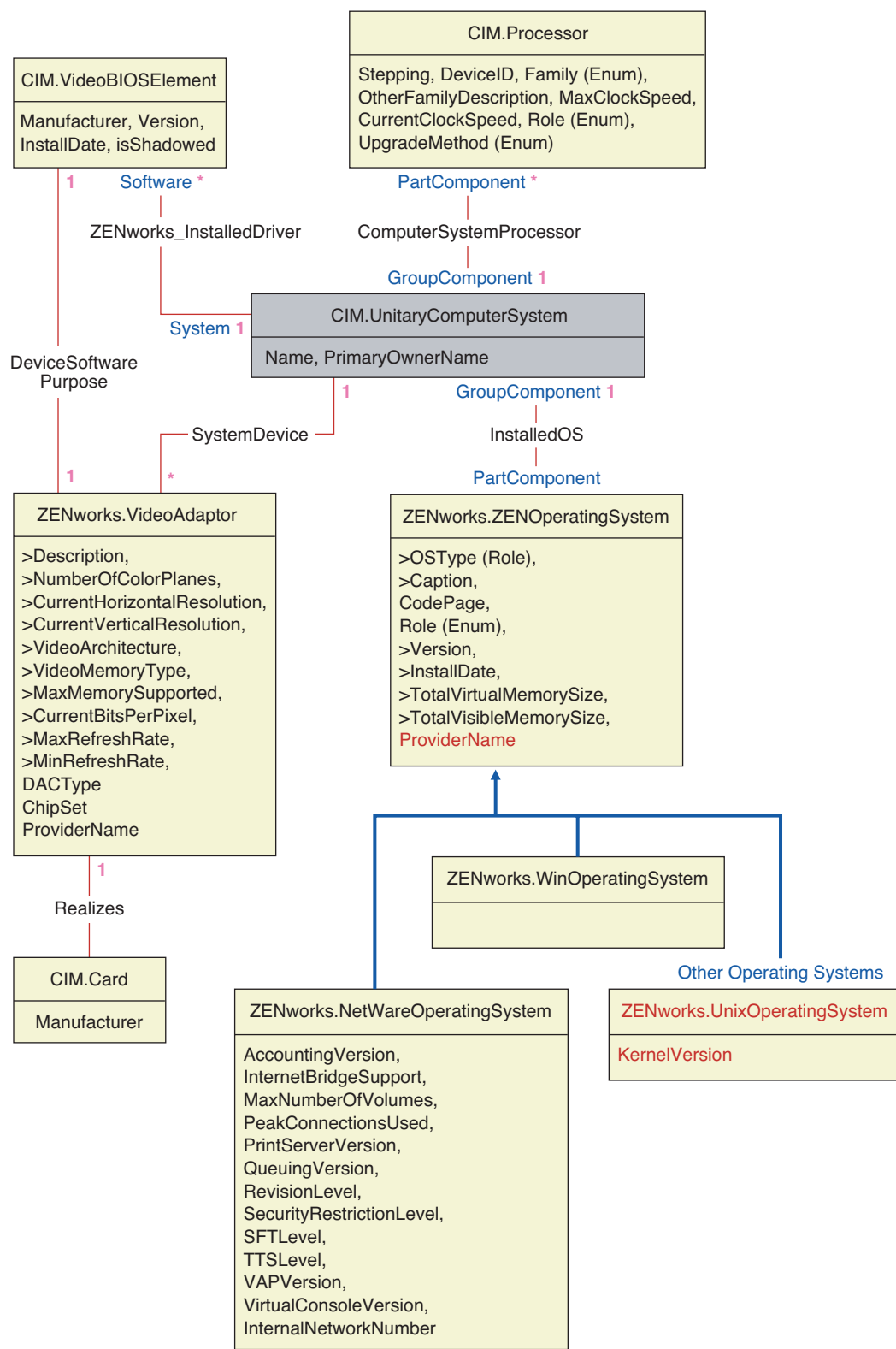
The elements of the meta-schema are classes, properties, and methods. The meta schema also supports indications and associations as types of classes and references as types of properties.

Classes can be arranged in a generalization hierarchy that represents subtype relationships between classes. The generalization hierarchy is a rooted, directed graph that does not support multiple inheritance.

A regular class can contain scalar or array properties of any intrinsic type such as Boolean, integer, string, and others. It cannot contain embedded classes or references to other classes.

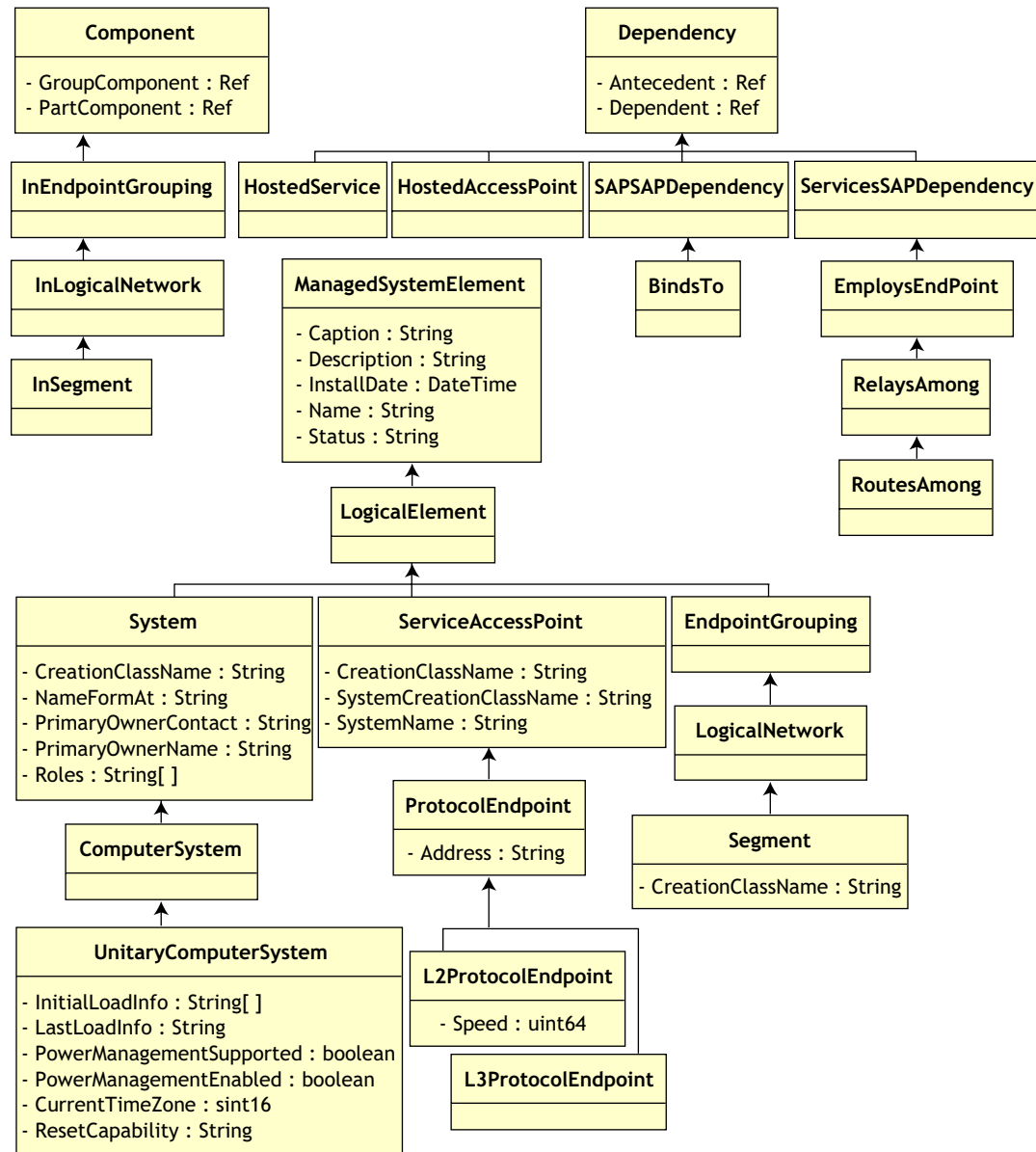
An association is a special class that contains two or more references. It represents a relationship between two or more objects. Because of the way associations are defined, it is possible to establish a relationship between classes without affecting any of the related classes. That is, addition of an association does not affect the interface of the related classes. Only associations can have references.

The schema fragment in the following illustration shows the relationships between some CIM objects that ZENworks 7 Desktop Management uses.



The illustration shows how the CIM schema maps to a relational DBMS schema. The classes are shown with the class name as the box heading. The associations are labeled within the lines between two classes.

The inheritance hierarchy of this schema fragment is shown in the following illustration of the CIM 2.2 schema. The references shown as type Ref are in bold with each association subtype narrowing the type of the reference.



75.2.1 CIM-to-Relational Mapping

CIM is an object model complete with classes, inheritance, and polymorphism. The generated mapping to a relational schema preserves these features to the maximum extent. The following two aspects are part of the relational mapping:

- **Logical Schema:** The logical schema defines how the data appears to applications, similar to an API. The goal is that the logical schema remains the same irrespective of the underlying database so that application software can run unchanged on any supported databases. Although SQL is a standard, this goal is not fully possible. Application software needs to know more about the database in use and this information can be abstracted and isolated to a small area of the application code.
- **Physical Schema:** The physical schema defines how the data is structured in the database. The schema tends to be specific to the database because of the nature of SQL and RDBMS. This document describes the physical schema in general terms only.

A table in the database represents each class in the CIM hierarchy. A column of the appropriate type in the table represents each non-inherited property in the class. Each table also has a primary key, `id$`, which is a 64-bit integer that uniquely identifies an instance. An instance of a CIM class is represented by a row in each table that corresponds to a class in its inheritance hierarchy. Each row has the same value for `id$`.

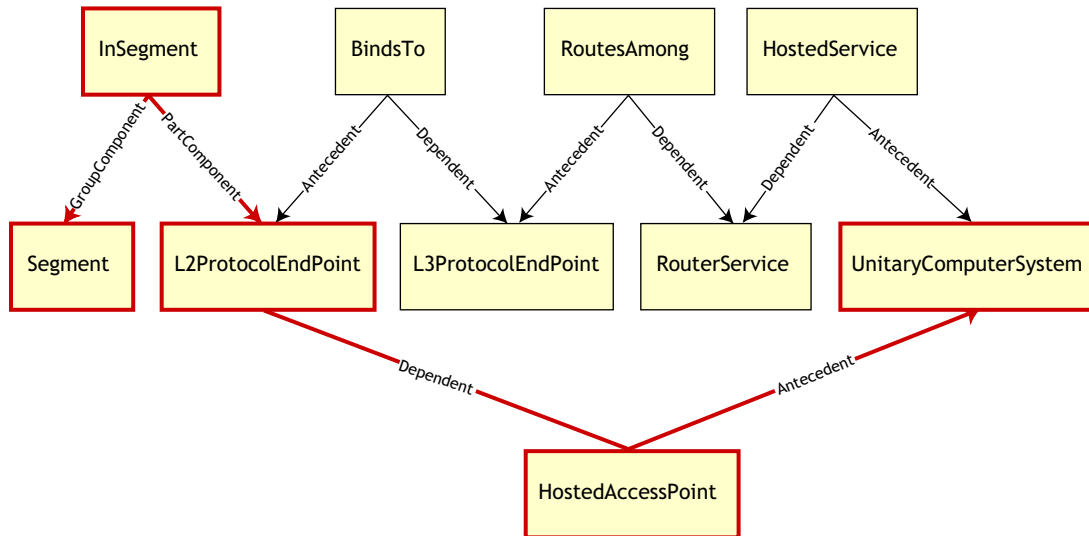
Each CIM class is also represented by a view that uses `id$` to join rows from the various tables in the inheritance hierarchy to yield a composite set of properties (inherited plus local) for an instance of that class. The view also contains an extra column, `class$`, of type integer that represents the type of the actual (leaf-most) class of the instance.

Associations are mapped in the same manner as regular classes, with a reference property being represented by a column with the `id$` field of the referenced object instance. Thus, associations can be traversed by doing a join between the reference field in the association and the `id$` field in the referenced table.

The following illustration depicts a typical query using this mapping:

Get Computers for Segment

```
SELECT CIM.UnitaryComputerSystem.*
FROM   CIM.UnitaryComputerSystem, CIM.Segment, CIM.L2ProtocolEndPoint,
       CIM.HostedAccessPoint, CIM.InSegment
WHERE  CIM.SegmentName = 'xxx'
AND    CIM.InSegment.GroupComponent = CIM.Segment.id$
AND    CIM.InSegment.PartComponent = CIM.L2ProtocolEndPoint.id$
AND    CIM.HostedAccessPoint.Dependent = CIM.L2ProtocolEndPoint.id$
AND    CIM.HostedAccessPoint.Antecedent = CIM.UnitaryComputerSystem.id$
```



This query finds all the computers attached to a given network segment. The classes and relationships involved are highlighted with borders.

The following topics describe both the schema types:

- [“Logical Schema” on page 992](#)
- [“Physical Schema” on page 994](#)

75.2.2 Logical Schema

The logical schema is the database schema as seen by users of the database and the application program. The schema consists of stored procedures and views. The underlying tables are not visible to the application.

ZENworks 7 Desktop Management Inventory components use JDBC to issue SQL statements to the RDBMS and to convert between RDBMS data types and Java data types. Using JDBC with stored procedures and views provides a level of abstraction that insulates application code from the underlying database technology and from changes to the physical schema.

The various elements of the logical schema are discussed in more detail in the following sections:

- [“Naming Schema Elements” on page 993](#)
- [“Users and Roles” on page 993](#)

- “Data Types” on page 994
- “Views” on page 994

Naming Schema Elements

We recommend that you use the CIM names unchanged in the database schema. Some problems could still ensue because of the differences in the naming schemes, such as the following:

- Names in CIM and SQL are not case sensitive.
- All databases have different sets of reserved words that must be enclosed in quotes (“”) when used as schema element names; however, in Oracle, enclosing a name in quotes makes it case sensitive.
- CIM classes avoid using SQL reserved words as names.
- CIM names are not limited in length and usually the names are long. Sybase allows up to 128 characters, but Oracle restricts the names to 30 characters.

Most of these problems are avoided during schema generation by preserving the case of CIM names, abbreviating any names longer than 30 characters, and placing quotes around any name that is in the union of the sets of reserved words.

Any name longer than 28 characters is abbreviated to a root name of 28 or fewer characters to allow a two-character prefix so that all associated SQL schema elements can use the same root name. The abbreviation algorithm shortens a name so that it is mnemonic, recognizable, and also unique within its scope. The abbreviated name is given a # character as a suffix (note that # is an illegal character in CIM) to prevent clashes with other names. If two or more names within the same scope generate the same abbreviation, an additional digit is appended to make the name unique. For example, AttributeCachingForRegularFilesMin is abbreviated to AttCacForRegularFilesMin#.

All such mangled names are written to the mangled name table so that a program can look up the real CIM name and retrieve the mangled name to use with the SQL.

Views are the schema elements that are most often manipulated by application code and queries. They use the same name as the CIM class they represent. For example, the CIM.UnitaryComputerSystem class is represented by a view named CIM.UnitaryComputerSystem.

When necessary, names for indexes and auxiliary tables are created by concatenating the class name and property name separated by a \$ character. These names are usually abbreviated. For example, NetworkAdapter\$NetworkAddresses is abbreviated to NetAdapter\$NetAddresses#. This does not have any adverse impact on ZENworks 7 Desktop Management schema users.

Users and Roles

In SQL, a user with the same name as the schema is the owner of each schema, for example, CIM, ManageWise®, ZENworks, and others.

Additionally, there is an MW_DBA user that has Database Administrator privileges and rights to all schema objects. The MW_Reader role has read-only access to all schema objects and the MW_Updater role has read-write-execute access to all schema objects.

Application programs should access the database as either MW_Reader or MW_Updater for a Sybase database, MWO_Reader or MWO_Updater for an Oracle database, and MWM_Reader or MWM_Updater for MS SQL Server database, depending on their requirements.

Data Types

CIM data types are mapped to the most appropriate data type provided by the database. Usually, the Java application does not require the type because it uses JDBC to access the data.

Java does not natively support unsigned types, so you should use classes or integer types of the next size to represent them. Also, make sure that there are no problems while reading or writing to the database. For example, reading or writing a negative number to an unsigned field in the database is likely to cause an error.

Strings in CIM and Java are Unicode, so the database is created using the UTF-8 character set. Internationalization does not pose any problems; however, it might create problems with case sensitivity in queries.

All databases preserve the case of string data stored within them, but might access the data as either case sensitive or otherwise during queries. In ZENworks 7 Desktop Management, the Inventory Query and the Data Export components are not affected because the queried data is retrieved from the database before being queried and so case sensitivity is automatically taken care of.

In CIM, strings can be specified with or without a maximum size in characters. Many strings have no specified size, which means they can be unlimited in size. For efficiency reasons, these unlimited strings are mapped to a variable string with maximum size of 254 characters. CIM strings with a maximum size are mapped to variable database strings of the same size. The size in the database is in bytes and not as characters because a Unicode character might require more than one byte for storage.

Views

Each CIM class is represented in the database by a view that contains all the local and inherited non-array properties of that class. The view is named the same as the CIM class.

Views can be queried using the SELECT statement and updated using the UPDATE statement. Because views cannot be used with the INSERT and DELETE statements, use the constructor and destructor procedures.

75.2.3 Physical Schema

The physical schema comprises elements necessary to implement the database. The physical schema differs for each database. A typical physical schema consists of:

- Table definitions 't\$xxx' Index definitions 'i\$xxx'
- Trigger definitions 'x\$xxx', 'n\$xxx' and 'u\$xxx'
- Sequence definitions (Oracle) 's\$xxx'
- Stored procedures and functions

The logical schema is layered on top of the physical schema and makes it unnecessary for users and applications to know the physical schema.

75.3 Inventory Database Schema in ZENworks 7 Desktop Management

The following section describes the database schema classes and the extensions and associations made to the CIM schema for use in ZENworks 7 Desktop Management. These extensions have ZENworks or ManageWise as their schema name. ZENworks.*classname* refers to the extended class in the ZENworks schema and ManageWise.*classname* refers to the extended class in the ManageWise schema.

The following sections help you understand the ZENworks 7 Desktop Management database schema:

- “Case Study of CIM Schema Implementation in ZENworks 7 Desktop Management” on page 995
- “Legends for Schema Diagrams” on page 997
- “Schema Diagrams of CIM and the Extension Schema in ZENworks 7 Desktop Management” on page 998
- “Custom Inventory Schema” on page 1006
- Section 75.3.6, “Sample Inventory Database Queries,” on page 1012

75.3.1 Case Study of CIM Schema Implementation in ZENworks 7 Desktop Management

The following scenario describes an inventoried workstation that has two parallel ports with a specified interrupt number.

In the following schema diagram, the CIM.UnitaryComputerSystem represents a managed inventory system.

In this illustration, class CIM.PointingDevice associates to CIM.UnitaryComputerSystem using the association CIM.SystemDevice with SystemDevice.GroupComponent pointing to CIM.UnitaryComputerSystem and SystemDevice.PartComponent pointing to CIM.PointingDevice. The relationship between the two classes is one to many. This means a computer system might have more than one pointing device.

Class CIM.IRQ associates to CIM.PointingDevice using the association CIM.AllocatedResource. Dependent pointing to CIM.PointingDevice and Antecedent pointing to CIM.IRQ.

Class ZENworks.ZENKeyboard associates to CIM.UnitaryComputerSystem using the association CIM.SystemDevice with SystemDevice.GroupComponent pointing to CIM.UnitaryComputerSystem and SystemDevice.PartComponent pointing to ZENworks.ZENKeyboard. The relationship between the two classes is one to one. This means a computer system can have only one keyboard.

Class ZENworks.BIOS associates to CIM.UnitaryComputerSystem using the association CIM.SystemBIOS with SystemDevice.GroupComponent pointing to CIM.UnitaryComputerSystem and SystemBIOS.PartComponent pointing to ZENworks.BIOS. The relationship between the two classes is one to one. This means a computer system can have only one BIOS.

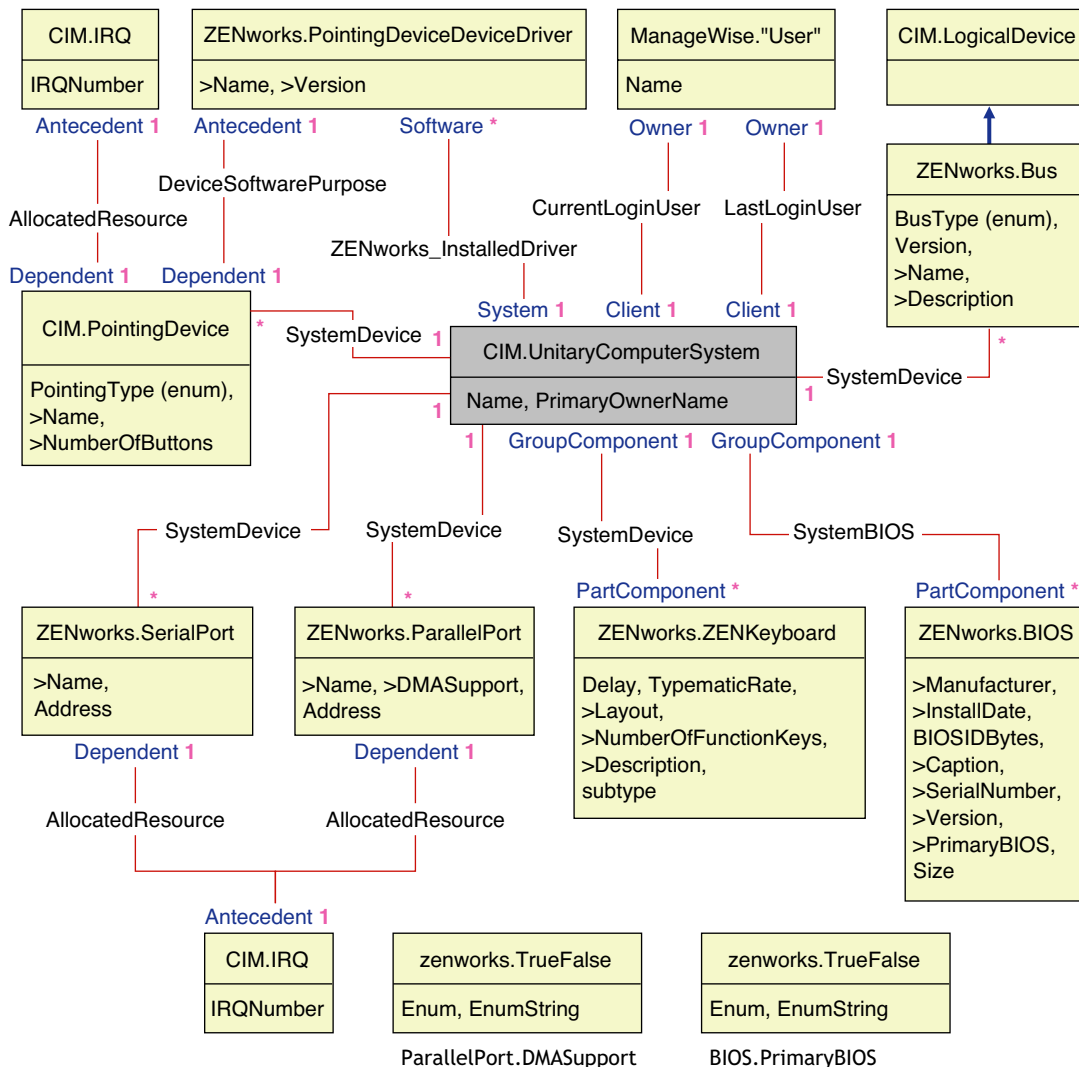
Class CIM.ZENworks.ParallelPort associates to CIM.UnitaryComputerSystem using the association CIM.SystemDevice with SystemDevice.GroupComponent pointing to

CIM.UnitaryComputerSystem and SystemDevice.PartComponent pointing to CIM.ZENworks.ParallelPort. The relationship between the two classes is one to many. This means a computer system might have more than one parallel port.

Class ZENworks.BUS associates to CIM.UnitaryComputerSystem using the association CIM.SystemDevice with SystemDevice.GroupComponent pointing to CIM.UnitaryComputerSystem and SystemDevice.PartComponent pointing to ZENworks.BUS. The relationship between the two classes is one to many. This means a computer system can have more than one bus.

Class ManageWise.User associates to CIM.UnitaryComputerSystem using CurrentLoginUser and LastLoginUser. In the CurrentLoginUser association, the specific instance of User is the one who is currently logged into the inventoried workstation. In the LastLoginUser association, the specific instance of User is the one who logged last into the inventoried workstation.

Class CIM.IRQ associates to CIM.ParallelPort using the association CIM.AllocatedResource. Dependent pointing to CIM.ParallelPort and Antecedent pointing to CIM.IRQ.



The schema diagram illustrates the following:

- All components that a computer system manages are represented as associations from the UnitaryComputerSystem class. The type of references (1..n, 1..1) between two classes are marked.
- Those associations that do not have a schema name are assumed as CIM schema.

There are three instances of ZENworks.ParallelPort associated to one instance of CIM.UnitaryComputerSystem using three instances of CIM.SystemDevice associations. CIM.SystemDevice.GroupComponent references UnitaryComputerSystem and CIM.SystemDevice.PartComponent references ParallelPort.

This is called 1 to n object reference relationship and is depicted in the illustration as 1..*. Similarly, every instance of ParallelPort has a corresponding instance of CIM.IRQ designating the port's IRQ. This is one-to-one relationship and is depicted as 1..1.

All other classes follow similar representation. For schema diagrams of other classes, see “[Schema Diagrams of CIM and the Extension Schema in ZENworks 7 Desktop Management](#)” on page 998.

75.3.2 Legends for Schema Diagrams

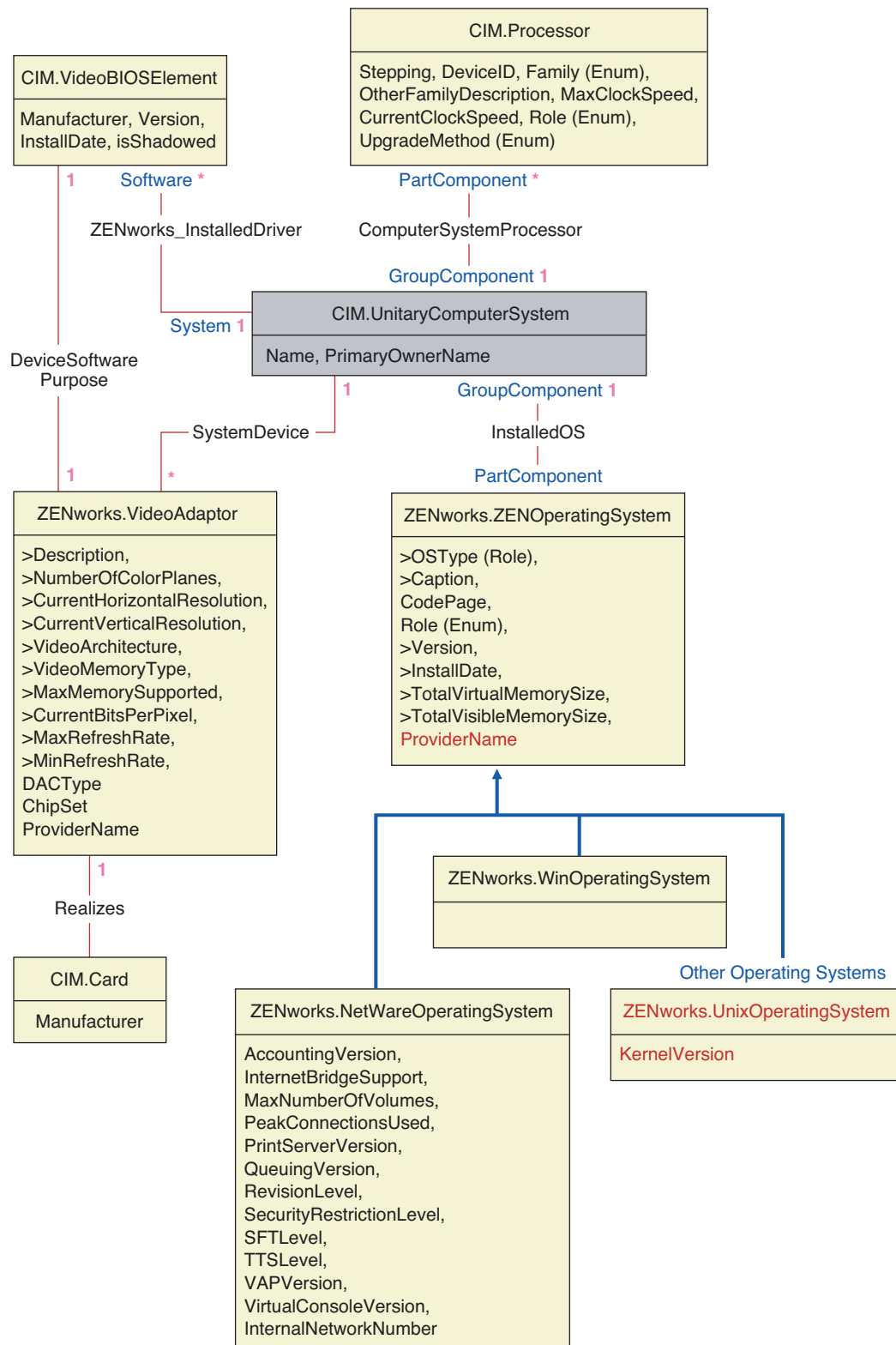
The legends for reading the schema diagrams are as follows:

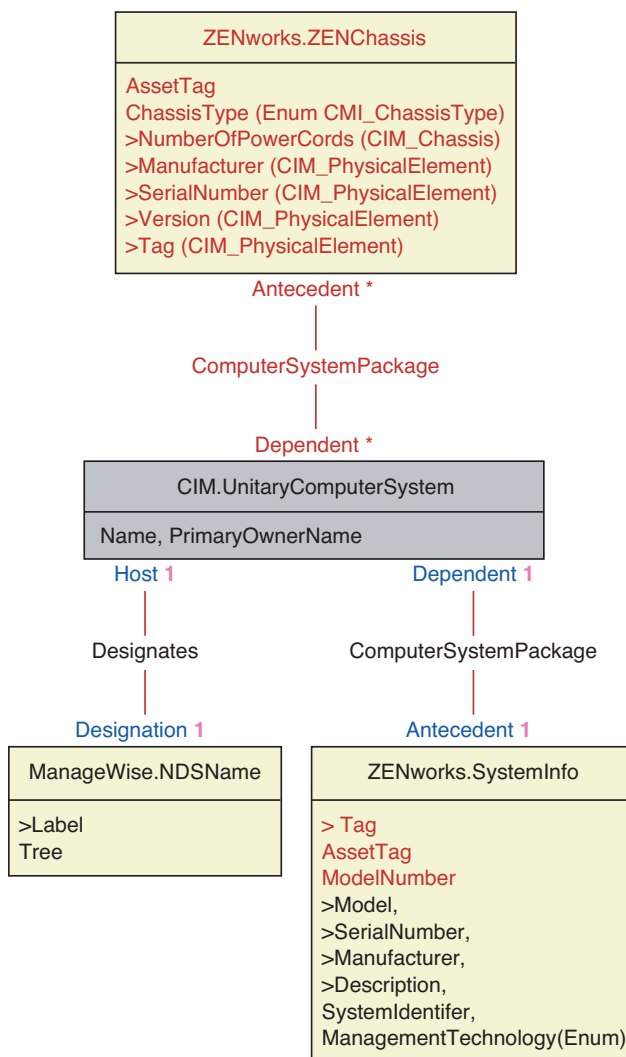
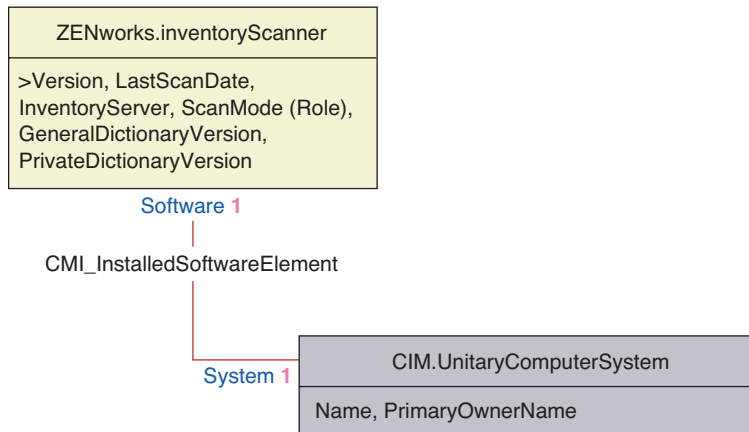
- Class names are enclosed in boxes with the class name as the heading and the attribute names within it.
- Red lines connect two classes using an association class.
- Blue lines indicate the class inheritance hierarchy. The class pointed by the arrow is the class that is being inherited from. The class from where the arrow originates is the inheriting class.
- The association class name is shown within the line joining two classes.
- References of the association class are marked on either side of the associated classes.

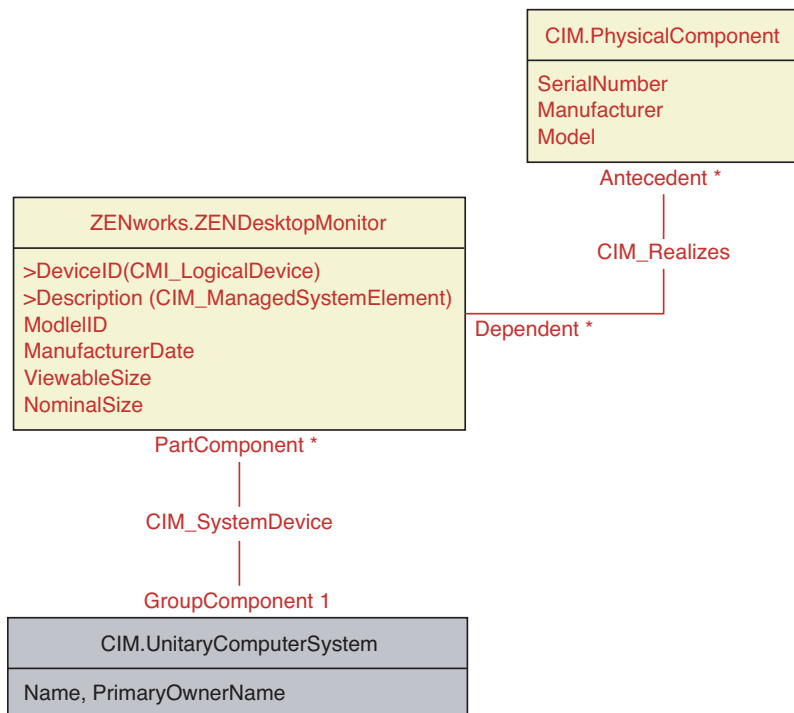
For an explanation of the CIM schema, see the CIM 2.2 schema specification on the [DMTF Web site \(http://www.dmtf.org\)](http://www.dmtf.org).

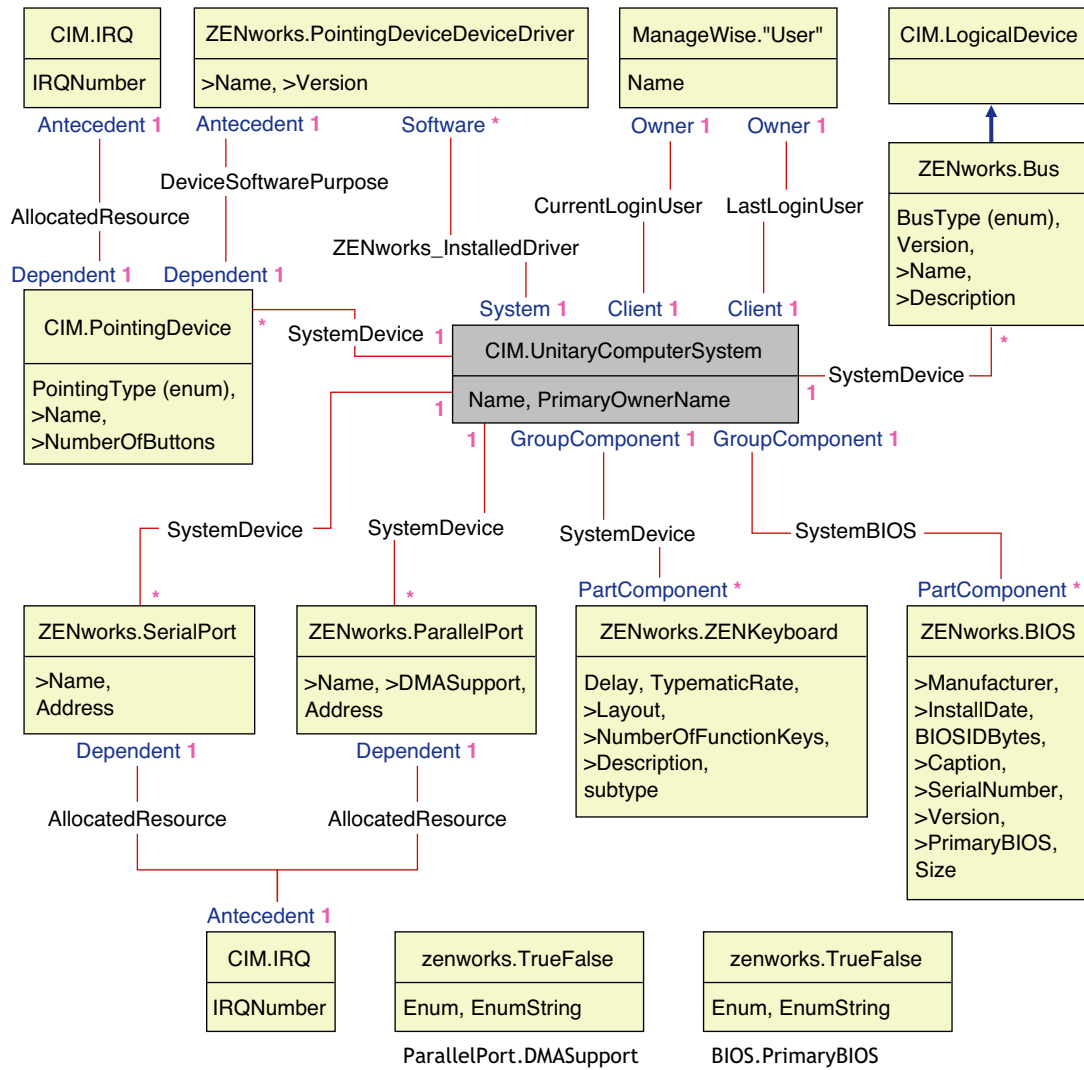
75.3.3 Schema Diagrams of CIM and the Extension Schema in ZENworks 7 Desktop Management

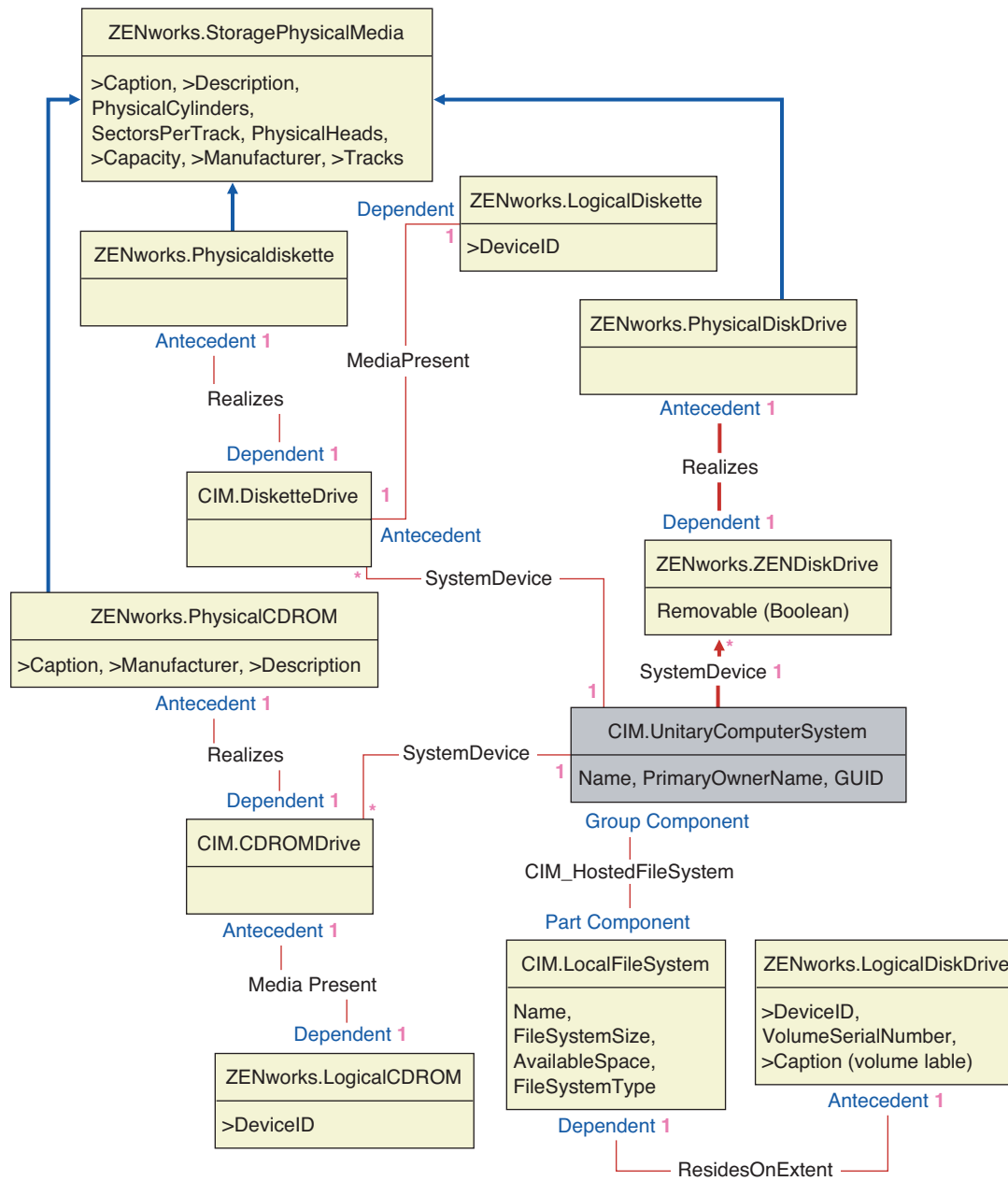
The following schema diagrams of the CIM and extension schema model the Inventory database in ZENworks 7 Desktop Management.

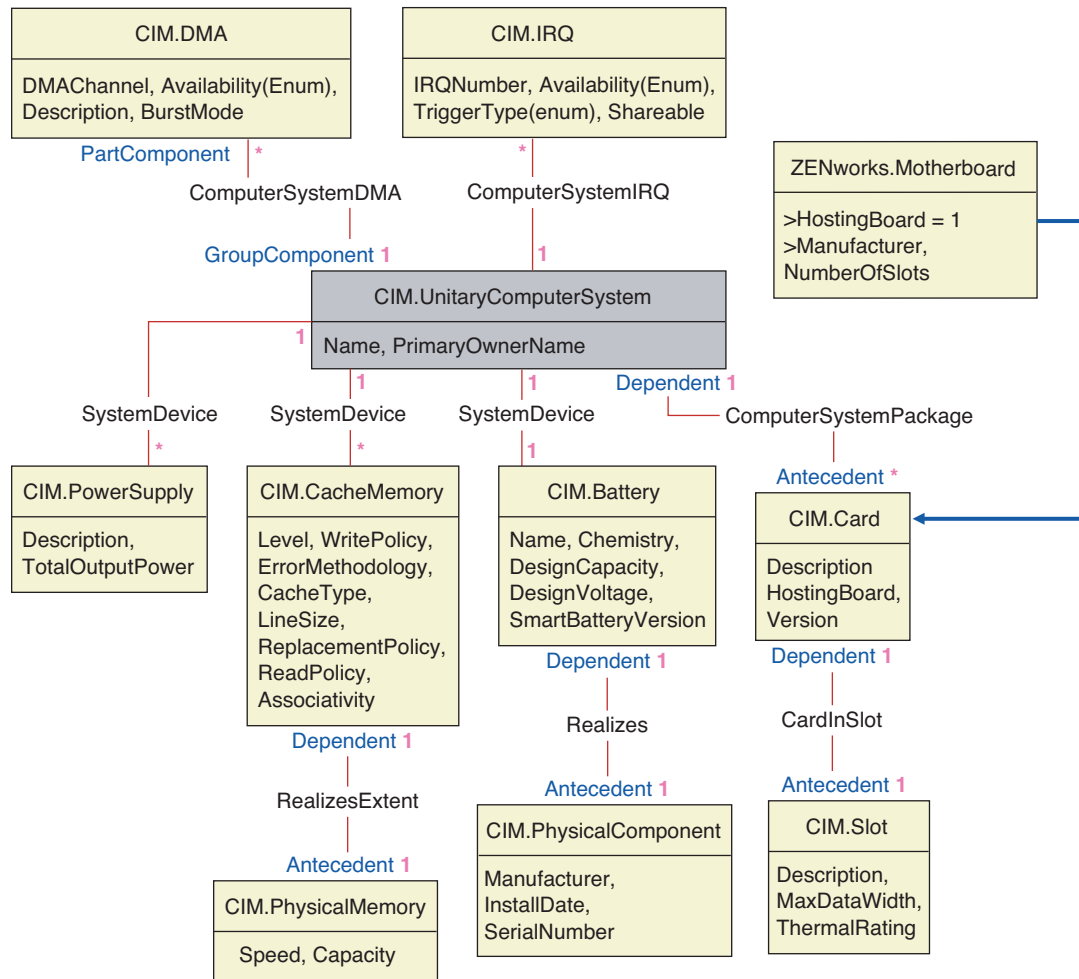


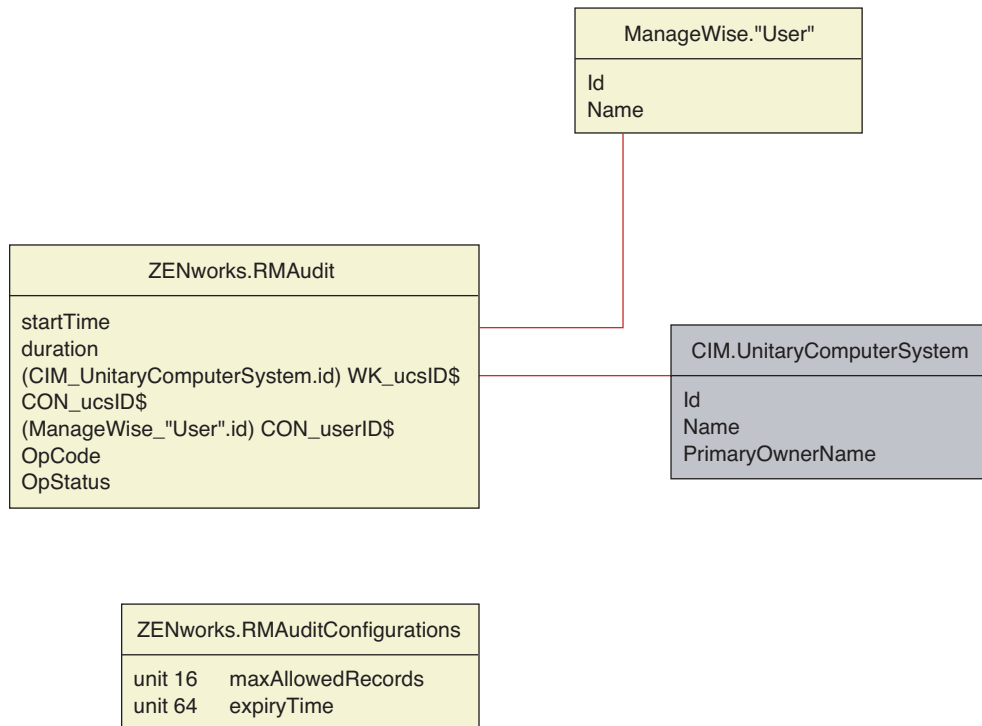










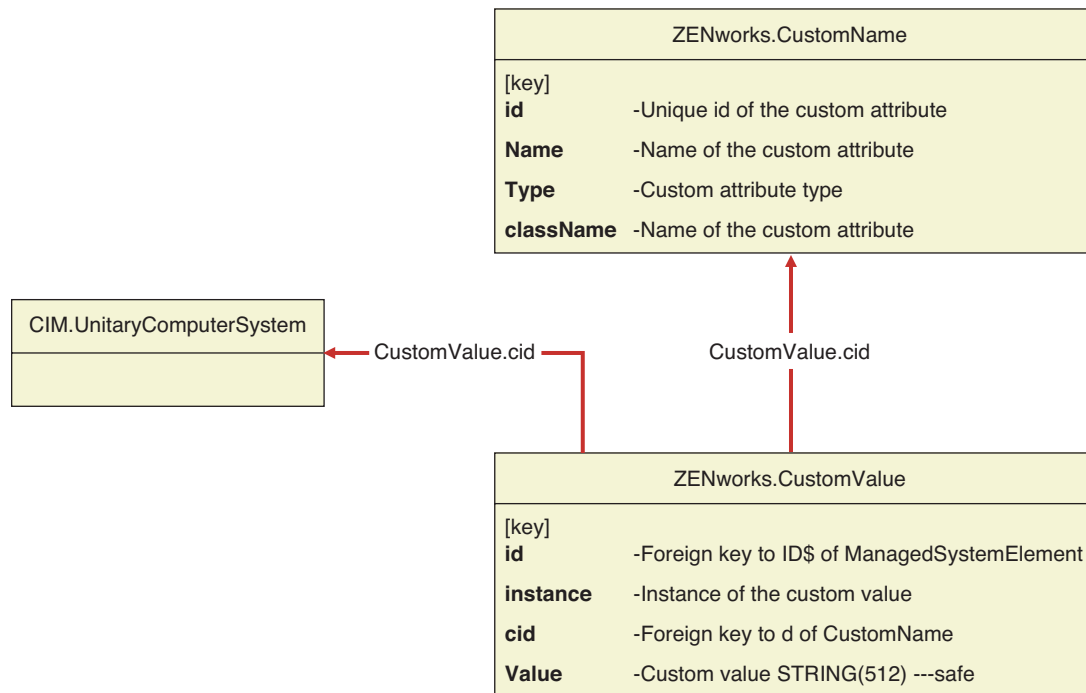


75.3.4 Custom Inventory Schema

A custom inventory attribute has the following qualifiers in the database:

Table 75-1 *Qualifiers of Custom Inventory attributes*

Qualifier	Description
Name	The name of the custom attribute
Value	The value assigned to the custom attribute
Type	The data type of the custom attribute. ZENworks 7 Desktop Management treats all custom attributes as type "String" only.
ClassName	The Inventory Class (table) to which the custom attribute is associated to.
Instance	The number of values assigned to a given custom attribute. In ZENworks 7 Desktop Management, you cannot have more than one value for a custom attribute.
ID	The id (id\$) of the Inventory object to which the custom attribute is associated.
CID	The unique ID of the custom attribute name.



The custom inventory information is stored in two tables: ZENworks.CustomName and ZENworks.CustomValue.

The ZENworks.CustomName table contains the attribute name, ID, type (not used) and the class name. The attribute ID is automatically incremented when a new custom attribute is stored.

A sample ZENworks.CustomName table is as follows:

ID	Name	Class Name
1	Cost	ZENworks.VideoAdapter
2	ProductUnit	CIM.UnitaryComputerSystem

The Zenworks.CustomValue table contains the object instance ID, the attribute value, and the reference to the associated custom attribute name. In the CustomValue table, a custom attribute can have multiple values for different instances of an inventory object but not for the same instance of the inventory object.

A sample Zenworks.CustomValue table is as follows:

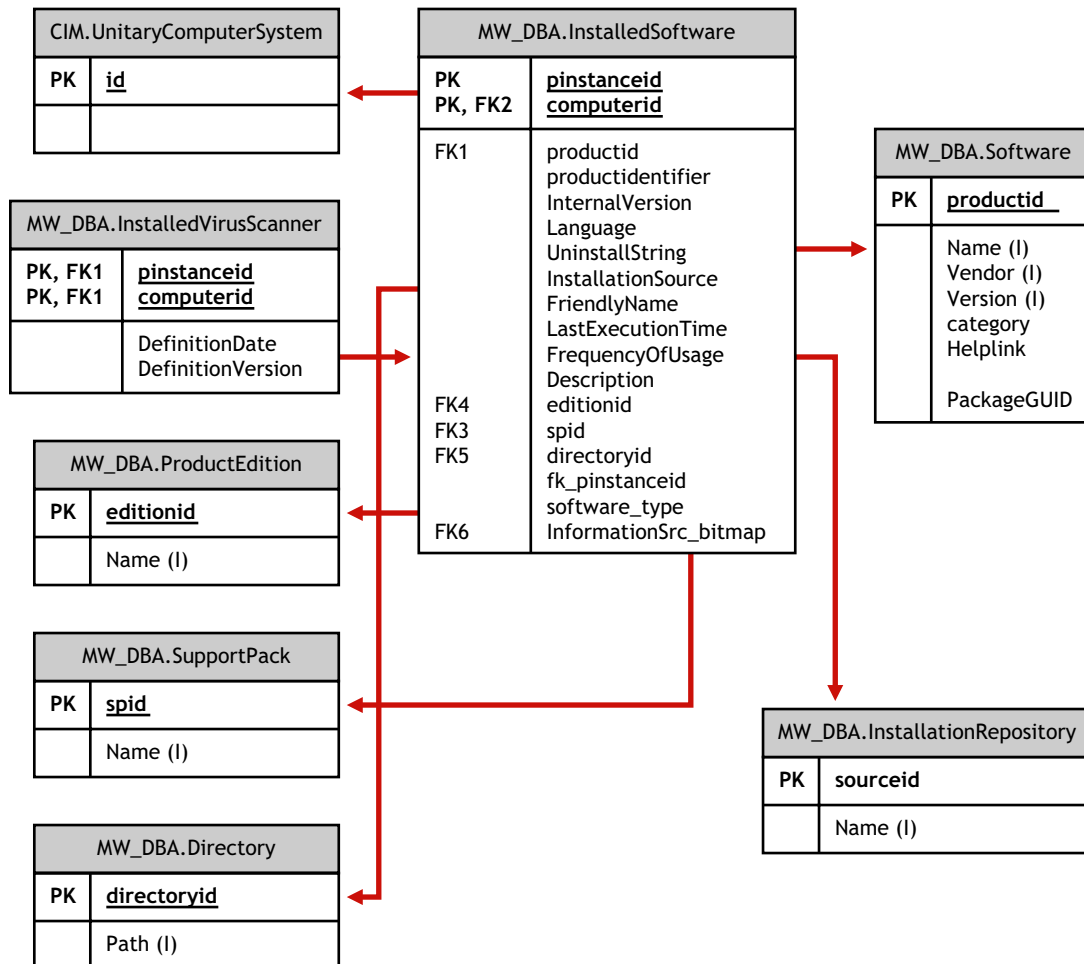
ID	Instance	CID	Value
28147497671065605	1	1	200.39
28147497671065606	1	1	345
69147497671045662	1	2	BAY-2

In the preceding example, the CustomName table has two custom attributes; Cost and ProductUnit. There are three rows in CustomValue table; two of them describe the cost of the video adapter, and the third one is the value of the ProductUnit attribute assigned directly to ComputerSystem.

75.3.5 Software Inventory Schema

The following software schema diagrams model the Inventory database in ZENworks 7 Desktop Management. In the following schema diagram, the CIM.UnitaryComputerSystem represents a managed inventory system.

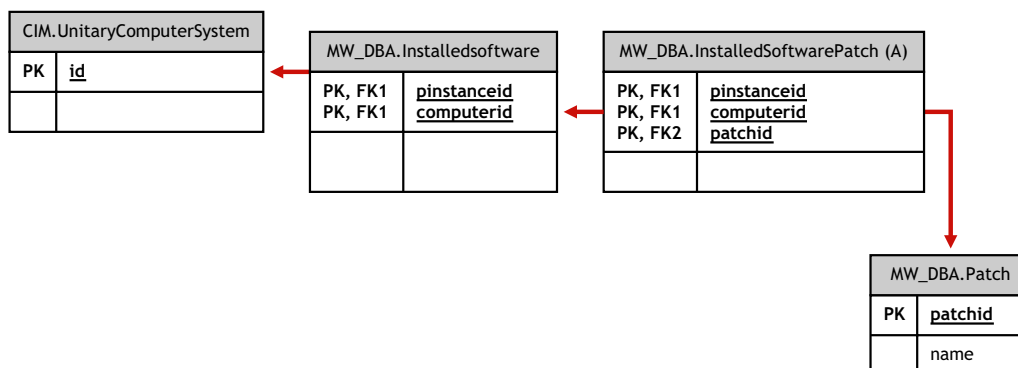
For more information about the tables, see [Appendix O, “ZENworks 7 Desktop Management Inventory Attributes,” on page 1211.](#)



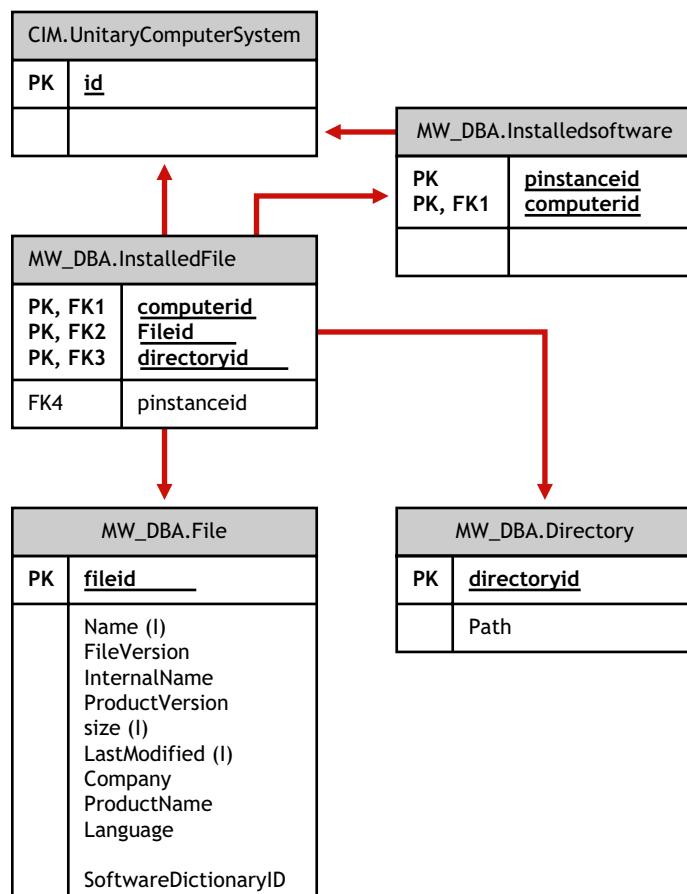
In the above illustration, class MW_DBA.Software associates to CIM.UnitaryComputerSystem using the association MW_DBA.InstalledSoftware with MW_DBA.InstalledSoftware.ComputerSystem pointing to CIM.UnitaryComputerSystem and MW_DBA.InstalledSoftware.ProductID pointing to MW_DBA.Software. The relationship between the two classes is one to many. This means a computer system might have more than one software information.

MW_DBA.InstalledSoftware association has Foreign key references to the following tables: ProductEdition, SupportPack, Directory, and Installation Repository.

MW_DBA.InstalledVirusScanner inherits the software information from MW_DBA.InstalledSoftware along with virus specific information such as Definition date and Definition version.



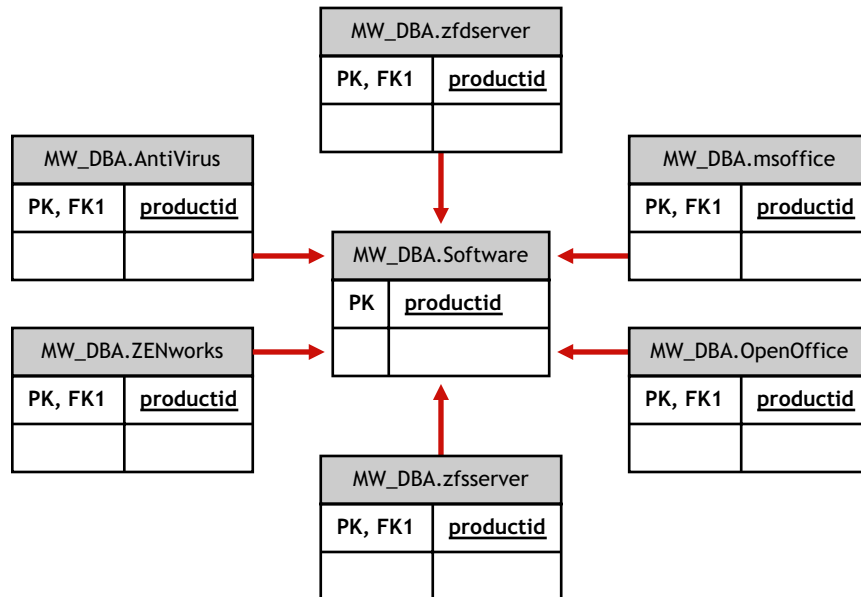
In the above illustration, class MW_DBA.Patch associates to MW_DBA.InstalledSoftware using the association MW_DBA.InstalledSoftwarePatch with MW_DBA.InstalledSoftwarePatch.pinstanceID pointing to MW_DBA.InstalledSoftware and MW_DBA.InstalledSoftwarePatch.PatchID pointing to MW_DBA.Patch. The relationship between the two classes is one to many. This means a software might have zero or more patch information.

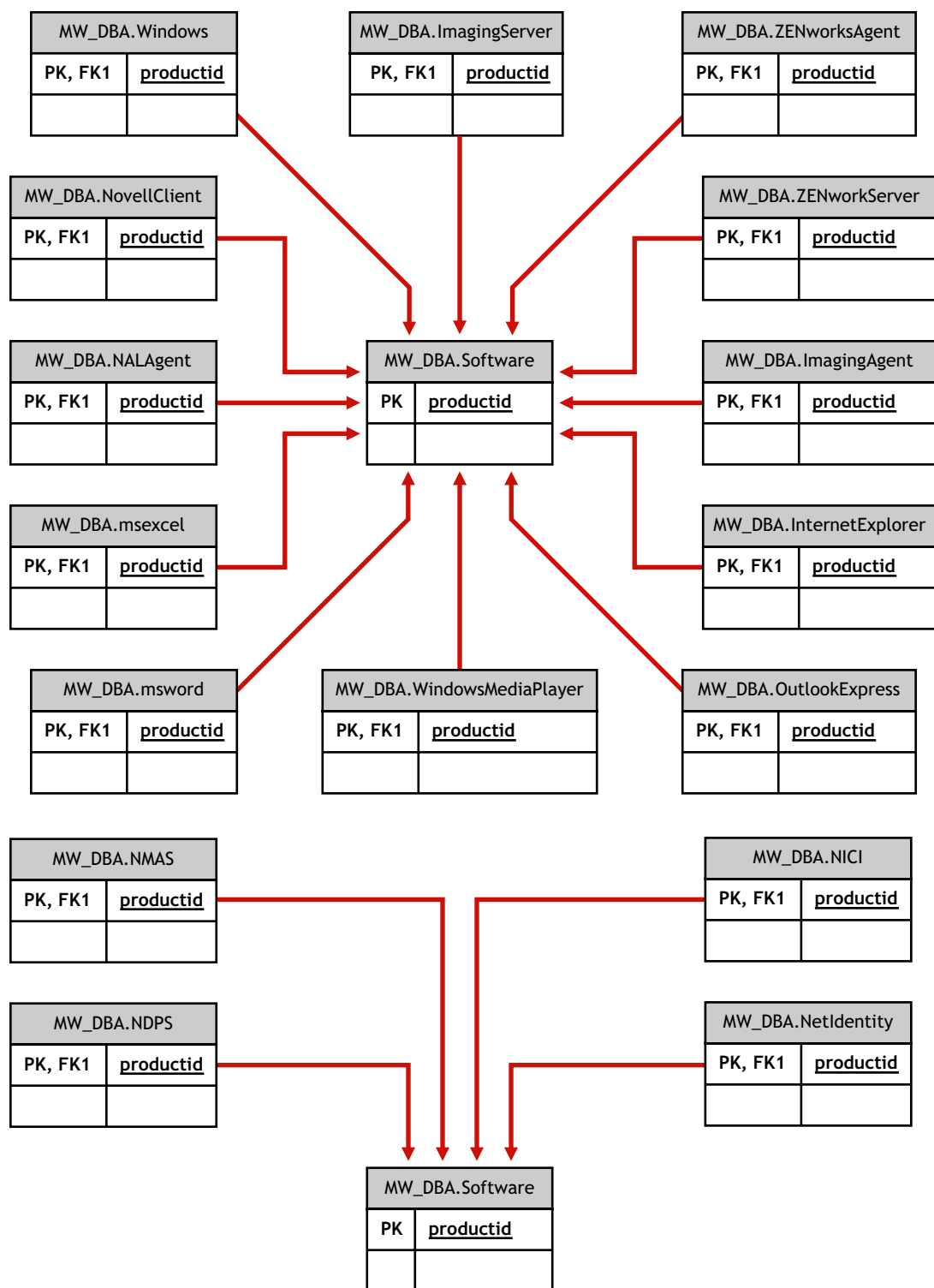


In the above illustration, class MW_DBA.File associates to MW_DBA.InstalledSoftware using the association MW_DBA.InstalledFile with MW_DBA.InstalledFile.pinstanceID pointing to

MW_DBA.InstalledSoftware and MW_DBA.InstalledFile.fileID pointing to MW_DBA.File. The relationship between the two classes is one to many. This means a software might have zero or more file information.

In this illustration, class MW_DBA.Directory associates to MW_DBA.InstalledSoftware using the association MW_DBA.InstalledFile with MW_DBA.InstalledFile.pinstanceID pointing to MW_DBA.InstalledSoftware and MW_DBA.InstalledFile.DirectoryID pointing to MW_DBA.Directory.





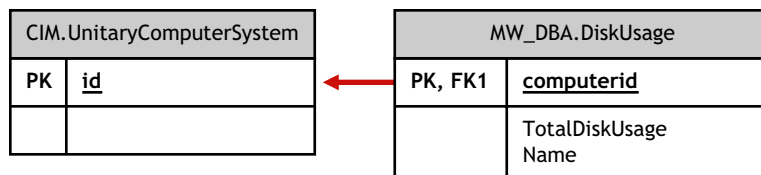
In the above illustrations, MW_DBA.MSoffice inherits the software information from MW_DBA.Software. This sub-class gets directly the MS office information. This is also applicable for the following classes:

mw_dba.zfdserver

mw_dba.zfdinventoryserver

mw_dba.zfdagent

mw_dba.zfsserver	mw_dba.zfdinventoryagent	mw_dba.zfsagent
mw_dba.zfsinventoryserver	mw_dba.mspowerpoint	mw_dba.msphotodraw
mw_dba.zfsinventoryagent	mw_dba.msoutlook	mw_dba.zfdwsmanager
mw_dba.zfsrmserver	mw_dba.msaccess	mw_dba.zfdwsimportserver
mw_dba.zfsrmagent	mw_dba.mspublisher	mw_dba.zfdinvdbserver
mw_dba.zfdrmserver	mw_dba.msfrontpage	mw_dba.zfsinvdbserver
mw_dba.zfdrmagent	mw_dba.msinfopath	mw_dba.zfdinvxmlproxyserver
mw_dba.zfsinvxmlproxyserver	mw_dba.zfdimagingagent	mw_dba.zfdimagingserver
mw_dba.zfdnalagent	mw_dba.zfdnalserver	mw_dba.zfdnaldb
mw_dba.middletier	mw_dba.zfsmmsserver	mw_dba.zfspds
mw_dba.zfspxeserver	mw_dba.zfsmmssrvmgmtagent	mw_dba.zfsmmstrafficanalysis agent
mw_dba.zfsmmsadctrendingagent	mw_dba.zfspdsdb	mw_dba.zfhserver
mw_dba.zfhaccesspoint	mw_dba.zfhdesktopsync	



In the above illustration, MW_DBA.DiskUsage has the computerID column foreign key references to the CIM.UnitaryComputerSystem.ID. The MW_DBA.DiskUsage table contains the total disk usage and the file extension name.

75.3.6 Sample Inventory Database Queries

The following are sample queries for retrieving the inventory information from the ZENworks 7 Desktop Management Inventory database.

Refer to the schema diagrams in [“Schema Diagrams of CIM and the Extension Schema in ZENworks 7 Desktop Management”](#) on page 998 to find out the associated schema classes and attribute information.

1. Retrieve the name and ID of all inventoried workstations from the database and also to the Novell eDirectory™ tree to which these workstations are registered. The query is as follows:

```
SELECT
    u.id$, u.name, m.tree
FROM
    ManageWise.NDSName m,
    CIM.UnitaryComputerSystem u,
```



```

        ManageWise.Designates s
WHERE
        s.Designation=m.id$ AND s.Host=u.id$;

```

In the above query, the tree name is part of the computer system name.

2. Retrieve the asset tag, manufacturer, and model number of all the inventoried workstations in the database. The query is as follows:

```

SELECT
        m.AssetTag,
        m.Manufacturer,
        m.ModelNumber,
        m.SerialNumber
FROM
        CIM.UnitaryComputerSystem u,
        CIM.ComputerSystemPackage s,
        ZENworks.SystemInfo m
WHERE
        s.Antecedent=m.id$ AND s.Dependent=u.id$;

```

3. Retrieve all the Microsoft applications with their versions and IDs that are installed on the inventoried workstation 'SJOHN164_99_139_79' registered under the 'NOVELL_AUS' eDirectory tree. The query is as follows:

```

SELECT
        m.Name,
        m.Version,
        im.ProductIdentifier
FROM
        CIM.UnitaryComputerSystem u,
        MW_DBA.InstalledSoftware im,
        MW_DBA.Software m
WHERE
        u.Name='SJOHN164_99_139_79.Novell_AUS' AND
        (im.computerid=u.id$ and im.productid=m.productid)
        AND m.Vendor LIKE 'Microsoft%';

```

4. Retrieve the processor information for the inventoried workstation 'SJOHN164_99_139_79.NOVELL_AUS'. The query is as follows:

```

SELECT
        procr.DeviceID,
        role.EnumString,
        family.EnumString,
        procr.OtherFamilyDescription,

```

```

        upg.EnumString,
        procr.MaxClockSpeed,
        procr.CurrentClockSpeed,
        procr.Stepping
FROM
        CIM.UnitaryComputerSystem ucs,
        CIM.ComputerSystemProcessor csp,
        CIM.Processor procr,
        CIM.Role_en_US role,
        CIM.Family_en_US family,
        CIM.UpgradeMethod_en_US upg
WHERE
        ucs.name='SJOHN164_99_139_79.Novell_AUS' AND
        csp.PartComponent=procr.id$ AND
        (
                (
                        ( procr.Role IS NOT NULL AND procr.Role=role.Enum ) OR
                        ( procr.Role IS NULL AND role.Enum=1000 )
                )
                AND
                procr.Family=family.Enum
                AND
                (
                        ( procr.UpgradeMethod IS NOT NULL AND
procr.UpgradeMethod=upg.Enum ) OR
                        ( procr.UpgradeMethod IS NULL AND upg.Enum=1000 )
                )
        )
);

```

5. Retrieve the ID of the UnitaryComputerSystem used for the inventoried workstation 'SJOHN164_99_139_79.NOVELL_AUS'. The query is as follows:

```

SELECT
        id$
FROM
        CIM.UnitaryComputerSystem
WHERE
        Name='SJOHN164_99_139_79.Novell_AUS';

```

6. Find the number of inventoried workstations in the database. The query is as follows:

```

SELECT
        count(u.id$)
FROM

```

```

    CIM.UnitaryComputerSystem u,
    CIM.InstalledSoftwareElement s,
    ZENworks.InventoryScanner m
WHERE
    m.id$=s.Software AND u.id$=s.System;

```

7. When you know the ID of the UnitaryComputerSystem for a particular inventoried workstation from the query as shown in query 5, query 4 can be modified as:

```

SELECT
    procr.DeviceID,
    role.EnumString,
    family.EnumString,
    procr.OtherFamilyDescription,
    upg.EnumString,
    procr.MaxClockSpeed,
    procr.CurrentClockSpeed,
    procr.Stepping
FROM
    CIM.UnitaryComputerSystem ucs,
    CIM.ComputerSystemProcessor csp,
    CIM.Processor procr,
    CIM.Role_en_US role,
    CIM.Family_en_US family,
    CIM.UpgradeMethod_en_US upg
WHERE
    ucs.id$ = ? AND
    csp.PartComponent=procr.id$ AND
    (
        (
            ( procr.Role IS NOT NULL AND procr.Role=role.Enum ) OR
            ( procr.Role IS NULL AND role.Enum=1000 )
        )
        AND
        procr.Family=family.Enum
        AND
        (
            ( procr.UpgradeMethod IS NOT NULL AND
procr.UpgradeMethod=upg.Enum ) OR
            ( procr.UpgradeMethod IS NULL AND upg.Enum=1000 )
        )
    );

```

Substitute the ID of the specified inventoried workstation in place of the ?, value for ucs.id\$ in the query.

8. List the IP address, IPX address, and MAC address of all workstations in the database. The query is as follows:

```
SELECT
    u.name,
    ip.Address,
    ipx.Address,
    mac.MACAddress
FROM
    CIM.UnitaryComputerSystem u,
    CIM.HostedAccessPoint s1,
    CIM.IPProtocolEndpoint ip,
    CIM.HostedAccessPoint s2,
    CIM.IPXProtocolEndpoint ipx,
    CIM.HostedAccessPoint s3,
    CIM.LANEndpoint mac
WHERE
    (s1.Dependent=ip.id$ and s1.Antecedent=u.id$) AND
    (s2.Dependent=ipx.id$ and s2.Antecedent=u.id$) AND
    (s3.Dependent=mac.id$ and s3.Antecedent=u.id$);
```

9. Retrieve the name and other properties of the drives on the hard disk of the specified inventoried workstation. The query is as follows:

```
SELECT
    n.Name,
    m.DeviceID,
    n.FileSystemSize,
    n.AvailableSpace,
    n.FileSystemType,
    m.VolumeSerialNumber,
    m.caption as VolumeLabel
FROM
    CIM.HostedFileSystem s,
    CIM.LocalFileSystem n,
    CIM.ResidesOnExtent r,
    ZENworks.LogicalDiskDrive m
WHERE
    (s.GroupComponent=? and s.PartComponent=n.id$) AND
    (r.Dependent=n.id$ and r.Antecedent=m.id$);
```

10. Retrieve all Custom attribute information stored in the database. The query is as follows:

```
SELECT * FROM ZENworks.CustomInformation;
```

11. Retrieve all Custom attribute information associated to the Class CIM.UnitaryComputerSystem. The query is as follows:

```
SELECT
    *
FROM
    ZENworks.CustomInformation
WHERE
    extractClass(id) IN
    (SELECT id FROM MW_DBA.t$Class WHERE
    ClassName='CIM. UnitaryComputerSystem')
```

12. Retrieve all the Microsoft Office installations in the enterprise. The query is as follows:

```
SELECT
    u.name,
    m.FriendlyName,
    im.InternalVersion,
    im.ProductIdentifier
FROM
    CIM.UnitaryComputerSystem u,
    MW_DBA.InstalledSoftware im,
    MW_DBA.Software m,
    MW_DBA.MSOffice mso
WHERE
    mso.id$=m.productid AND
    m.productid=im.productid AND
    im.computerid=u.id$;
```

13. Retrieve all the Internet Explorer installations in the enterprise. The query is as follows:

```
SELECT
    u.Name,
    m.Name,
    m.Version,
    im.InternalVersion,
    im.ProductIdentifier
FROM
    CIM.UnitaryComputerSystem u,
    MW_DBA.InstalledSoftware im,
    MW_DBA.Software m,
    MW_DBA.InternetExplorer ie
WHERE
    ie.id$=m.productid AND
```

```
m.productid=im.productid AND
im.computerid=u.id$;
```

NOTE: Query 12 and 13 follow nearly the same syntax except for the table relating to the component. A similar approach can be used for components such as Windows Media Player, Outlook Express, Microsoft Word, and Microsoft Excel. The complete set of these tables is available in the Schema.

14. Retrieve all the anti-virus installations in the enterprise. The query is as follows:

```
SELECT
    u.Name,
    m.Name,
    m.Version,
    im.InternalVersion,
    ivs.DefinitionVersion,
    ivs.DefinitionDate
FROM
    CIM.UnitaryComputerSystem u,
    MW_DBA.InstalledSoftware im,
    MW_DBA.Software m,
    MW_DBA.InstalledVirusScanner ivs
WHERE
    ivs.pinstanceid=im.pinstanceid AND
    m.productid=im.productid AND
    im.computerid=u.id$;
```

15. Retrieve all the applications and the details of the files associated with the application that are installed on the inventoried workstation 'SJOHN164_99_139_79.NOVELL_AUS'. The query is as follows:

```
SELECT
    u.Name,
    m.Name,
    m.Version,
    m.Category,
    zfile.company,
    zfile.productname,
    zfile.productversion,
    zfile.name,
    dir.path,
    zfile.fileversion,
    zfile."size",
    zfile.lastmodified,
    zfile.internalname,
```

```

        zfile.softwaredictionaryid
FROM
    CIM.UnitaryComputerSystem u,
    MW_DBA.InstalledSoftware iso,
        MW_DBA.Software m,
        MW_DBA.InstalledFile ifile,
        MW_DBA."file" zfile,
        MW_DBA.Directory dir
WHERE
    u.Name='SJOHN164_99_139_79.Novell_AUS' AND
    iso.computerid=u.id$ AND
    iso.productid=m.productid AND
    iso.pinstanceid=ifile.pinstanceid AND
        ifile.directoryid=dir.id AND
        ifile.fileid=zfile.id;

```

16. Retrieve all the files present on the inventoried workstation 'SJOHN164_99_139_79.NOVELL_AUS' that has not been associated with a valid software. The query is as follows:

```

SELECT
    u.Name,
    zfile.name,
    dir.path,
    zfile.fileversion,
    zfile."size",
        zfile.lastmodified,
    zfile.internalname,
    zfile.productversion,
    zfile.company,
    zfile.productname
FROM
    CIM.UnitaryComputerSystem u,
    MW_DBA.InstalledFile ifile,
        MW_DBA."file" zfile,
        MW_DBA.Directory dir
WHERE
    u.Name='SJOHN164_99_139_79.Novell_AUS' AND
        u.id$=ifile.computerid AND
        ifile.fileid=zfile.id AND
        ifile.directoryid=dir.id AND
        ifile.pinstanceid is null;

```

17. Retrieve the disk usage details of files with known extensions on each inventoried machine in the enterprise. The query is as follows:

```
SELECT
    u.Name,
    du.Name,
    du.TotalDiskUsage
FROM
    CIM.UnitaryComputerSystem u,
    MW_DBA.DiskUsage du
WHERE
    u.id$=du.Computerid AND
    du.Name is not null;
```


This section contains the following information to help you customize the way Novell® ZENworks® 7 Workstation Inventory displays information:

- [Section 76.1, “Viewing the Servers Deployed for Inventory,” on page 1021](#)
- [Section 76.2, “Customizing the Hardware Inventory Information To Be Scanned,” on page 1022](#)
- [Section 76.3, “Customizing the Software Inventory Information To Be Scanned For ZENworks 7 Inventoried Workstations,” on page 1035](#)
- [Section 76.4, “Customizing the Software Inventory Information To Be Scanned For ZENworks for Desktops 4.x and Earlier Versions of Inventoried Workstations,” on page 1081](#)
- [Section 76.5, “Scanning for Workstations That Are Periodically Connected to the Network,” on page 1081](#)
- [Section 76.6, “Scanning for Workstations That Are Never Connected to Your Network,” on page 1081](#)
- [Section 76.7, “Removing Redundant Inventoried Workstations from the Inventory Database,” on page 1084](#)
- [Section 76.8, “Removing Duplicate Workstation Objects from the Inventory Database,” on page 1086](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

76.1 Viewing the Servers Deployed for Inventory

Using ConsoleOne®, you can view the Inventory servers and databases that you configured for collecting inventory.

To get a complete Inventory tree view:

- 1 Log into all the Novell eDirectory™ trees that contain Inventory servers present in your inventory tree.
- 2 In ConsoleOne, select a container, click the *View* menu, then click *Complete Tree View*.
All the Inventory servers within the container are displayed in the *Complete Tree View*.

To view a complete tree view if your inventory deployment involves roll-up of information between Inventory servers that are situated on different Novell eDirectory trees:

- 1 In ConsoleOne, select *NDS Tree*.
- 2 Click *View*, then click *Complete Tree View*.
- 3 Select the eDirectory trees or containers within the tree that contains the Inventory servers.
- 4 Click *OK*.

To view all Inventory server from the selected Inventory server to the highest-level server:

- 1 In ConsoleOne, right-click the Inventory Service object (Inventory Service *_server_name*), click *View*, then click *Up Tree View* or double-click the Inventory Service object.

If your inventory deployment consists of a single eDirectory tree, an Up Tree View displays all the Inventory servers from the selected Inventory server up to the highest level (Root Server).

If your inventory deployment involves roll-up of inventory information across Inventory servers located on different eDirectory trees, the Up Tree View displays all the Inventory servers from the selected Inventory server up to the highest level server to which you have logged in.

NOTE: You cannot collapse the inventory tree using the shortcut keys.

76.2 Customizing the Hardware Inventory Information To Be Scanned

This section describes how to customize the inventory information.

- “Customizing the Hardware Inventory Scanning of Inventoried Workstations” on page 1022
- “Scanning for IBM Computer Models” on page 1030
- “Customizing the Hardware Scanning Information of Jaz, Zip, and Floppy Drive Vendors” on page 1031
- “Scanning for Vendor-Specific Asset Information from DMI” on page 1032
- Section 76.2.5, “Customizing the Hardware Information for Monitor Size,” on page 1033

76.2.1 Customizing the Hardware Inventory Scanning of Inventoried Workstations

ZENworks 7 Desktop Management allows you to collect information that is not part of the default hardware inventory from the inventoried workstations.

To collect information that is not part of the default inventory from the inventoried workstations, you must define attributes and their corresponding values for an Inventory class. By default, each Inventory class has its own attributes called as regular attributes and the values corresponding to the regular attributes are called as regular attribute values. The Inventory Scanner stores the user-defined attributes (called as custom attributes) and the corresponding values along with the regular attribute values of the class in the Inventory database. This process is called custom hardware inventory scanning.

For example, you can add a custom attribute named Rate to the Processor table. The Inventory Scanner scans for the regular attribute values such as the processor type and stores the values of the Rate and the Processor Type in the Inventory database.

The following table lists the Inventory class and the regular attributes.

NOTE: The * in the following table indicates that you need to specify the values in bytes. The + in the table given below indicates that you need to specify the enumerated values for these attributes. For more information on enumerated values, see [Appendix P, “Enumeration Values,” on page 1237](#).

Table 76-1 List of Inventory class and its regular attributes

Inventory Class Name as Displayed in the Custom Attribute Editor Dialog Box	Inventory Class Name in the Inventory Database	Regular Attributes
Asset	Zenworks.SystemInfo	Description, Caption, AssetTag, Model, ModelNumber, SystemIdentifier, ManagementTechnology, Serial Number, and Tag +
MAC Address	CIM.LANEndpoint	MAC Address
IP Address	CIM.IPProtocolEndpoint	Address, SubnetMask
IPX Address	CIM.IPXProtocolEndpoint	Address
Modem	Zenworks.ZENPOTSModem	Description, Name, ProviderName, DeviceID
Network Adapter	Zenworks.ZENNetworkAdapter	MaxSpeed*, Name, PermanentAddress, AdapterType, ProviderName, MACAddress
Network Adapter Driver	Zenworks.NetworkAdapterDriver	Description, Name, Version
NetWare Client	Zenworks.NetwareClient	Version
Processor	CIM.Processor	stepping, DeviceID, Family+, OtherFamilyDescription, MaxClockSpeed*, CurrentClockSpeed*, Role+, UpgradeMethod+, Description, Name
BIOS	Zenworks.BIOS	Manufacturer, InstallDate, BIOSIDBytes, Caption, SerialNumber, Version, PrimaryBios+, size*
Bus	Zenworks.Bus	BusType+, Name, Description, Version, DeviceID
IRQ	CIM.IRQ	IRQNumber, Availability+, TriggerType+, Shareable+
KeyBoard	Zenworks.ZENKeyboard	Layout, SubType, Description, NumberOfFunctionKeys, Delay*, TypeMaticRate*
Display Adapter	Zenworks.VideoAdapter	NumberOfColorPlanes, CurrentHorizontalResolution, CurrentVerticalResolution, VideoArchitecture+, VideoMemoryType+, MaxMemorySupported*, CurrentBitsPerPixel, Description, MaxRefreshRate*, MinRefreshRate*, DACType, ChipSet, ProviderName
Display Driver	CIM.VideoBIOSElement	Manufacturer, Version, InstallDate, IsShadowed+
Parallel Port	Zenworks.ParallelPort	Name, DMA Support+, Address
Serial Port	Zenworks.SerialPort	Name, Address

Inventory Class Name as Displayed in the Custom Attribute Editor Dialog Box	Inventory Class Name in the Inventory Database	Regular Attributes
Diskette Drive	Zenworks.ExtendedDiskette Drive	DisketteDeviceID, DisketteManufacture, DisketteDescription, DiskettePhysicalCylinders, DiskettePhysicalHeads, DisketteSectorsPerTrack, DisketteCapacity*
CDROM	Zenworks.ExtendedCDROM Drive	CDROMDeviceID, CDROMManufacturer, CDROMDescription, CDROMCaption
Physical Disk Drive	Zenworks.ExtendedDiskDrive	DiskRemovable+, DiskManufacturer, DiskDescription, DiskPhysicalCylinders, DiskPhysicalHeads, DiskSectorsPerTrack, DiskCapacity*
Logical Disk Drive	CIM.LocalFileSystem	Name, FileSystemType, FileSystemSize*, AvailableSpace*
Windows Operating System	Zenworks.WinOperatingSystem	OSType+, Version, CodePage, InstallDate, SizeStoredInPagingFiles*, Caption, OtherTypeDescription, TotalVirtualMemorySize*, TotalVisibleMemorySize* (specify the values in bytes), Role+
Multimedia Card	Zenworks.SoundAdapter	Description, Name, ProviderName
Cache Memory	Zenworks.ExtendedCacheMemory	CacheMemoryLevel+, CacheMemoryWritePolicy+, CacheMemoryErrorMethodology, CacheMemoryCacheType+, CacheMemoryLineSize*, CacheMemoryReplacementPolicy+, CacheMemoryReadPolicy+, CacheMemoryAssociativity+, CacheMemorySpeed*, CacheMemoryCapacity*
Mother Board	Zenworks.MotherBoard	Version, Description, NumberOfSlots, Manufacturer
Battery	CIM.Battery	Name, Chemistry+, DesignCapacity*, DesignVoltage*, SmartBatteryVersion
Power Supply	CIM.PowerSupply	Description, TotalOutputPower*
DMA	CIM.DMA	DMAChannel, Description, Availability+, BurstMode+
Computer System Information	CIM.UnitaryComputerSystem	Name, PrimaryOwnerContactID, PrimaryOwnerName
Pointing Device	CIM.PointingDevice	PointingType+, Name, NumberOfButtons
Pointing Device Driver	Zenworks.PointingDeviceDeviceDriver	Name, Version
Slot	Zenworks.ExtendedSlot	SlotDescription, SlotMaxDataWidth, SlotThermalRating*

Inventory Class Name as Displayed in the Custom Attribute Editor Dialog Box	Inventory Class Name in the Inventory Database	Regular Attributes
Monitor	Zenworks.ZENDesktopMonitor	DeviceID,Description,ManufacturerDate,ModelID,ViewableSize,NominalSize,SerialNumber,Manufacturer,Model
System Chassis	ZENworks.ZENChassis	ChassisType(+),Manufacturer,SerialNumber,AssetTag,Version,NumberOfPowerCords,Tag

The following sections give information on the tasks you need to perform to do custom scanning:

- [“Adding Custom Attributes” on page 1025](#)
- [“Using the Custom.ini File to Add Custom Attribute Values” on page 1025](#)
- [“Guidelines for Creating the CUSTOM.INI File” on page 1027](#)
- [“Viewing Custom Attributes and Custom Attribute Values” on page 1028](#)
- [“Custom Inventory Scanning Examples” on page 1028](#)

Adding Custom Attributes

To add custom attributes to an Inventory class:

- 1 In the Workstation Inventory policy, click the *Hardware Scan* tab.
- 2 Select *Enable Custom Scanning*.
- 3 Click *Custom Attribute Editor*.
- 4 In the Custom Attribute Editor dialog box, click *Add*.
- 5 From the *Class Name* drop-down list, select the class where you want to add the custom attribute. For example: Processor.
- 6 Enter the custom attribute name in the *Attribute Name* field. For example: Rate.

NOTE: If custom attributes are used in Oracle Inventory database, the custom attribute name must be less than 10 characters.

- 7 Click *OK*.
You can add more than one custom attribute for a class.
- 8 Click *OK*, click *Apply*, then click *OK*.

Using the Custom.ini File to Add Custom Attribute Values

To add values to the custom attributes, you must create the `custom.ini` file. The administrator must communicate the list of Inventory classes to which the custom attributes can be added. The Inventory Scanner uses the `custom.ini` file to get information about custom attributes and their corresponding values.

The contents of a `custom.ini` file are as follows:

```
[START_CIM_OBJECT]
Class =
Inventory_Class_Name_as_displayed_in_the_Custom_Attribute_Editor_dialo
```

```

gbox or Inventory_Class_Name_in_Inventory_database
RegularAttrs = regular_attribute_name1, regular_attribute_name2, ...,
regular_attribute_nameN
RegularVals = regular_attribute_value1, regular_attribute_value2, ...,
regular_attribute_valueN
Action = A/D
custom_attribute = custom_attribute_value
custom_attribute = custom_attribute_value
...
...
custom_attribute = custom_attribute_value
[END_CIM_OBJECT]

```

where `Class` is a predefined Inventory class name (for the list of the predefined Inventory class names, refer to the [Inventory Class Name and Regular Attributes table](#)), `RegularAttrs` indicates the list of regular attribute names, `RegularVals` indicates the corresponding regular attribute values, the `Action` value `A` indicates the specified custom attributes to be added to the database table, and the `Action` value `D` indicates the specified custom attributes to be deleted from the database table.

You can enter comments after the semicolon (;). The data after the semicolon is ignored by the Scanner.

In the `custom.ini` file, the content between `[START_CIM_OBJECT]` and `[END_CIM_OBJECT]` is called as a “section”. The first three lines within the section are called as a query.

A sample `custom.ini` file that has one regular attribute, one regular attribute value, and one custom attribute and value is as follows:

```

[START_CIM_OBJECT]
Class = Computer System Information           ;Inventory class name
RegularAttrs = Name                           ;Regular attribute name
RegularVals = John                           ;Regular attribute value
Action = A
Employee Number=BLR_5000234                   ;Custom attribute and its value
[END_CIM_OBJECT]

```

In the above query, the employee number is added to the `CIM.UnitaryComputerSystem` table if the value of the `Name` attribute is `John`.

You can create a `custom.ini` file using either of the following methods:

- Use a text editor to create a `custom.ini` file and save it in the `windows_installation_drive/zenworks` directory of the inventoried workstation.
- Develop an application to automatically generate the `custom.ini` file and place the file in the `windows_installation_drive/zenworks` directory of the inventoried workstation. You must save the application in the `windows_installation_drive/zenworks` directory of the inventoried workstation.

After developing the application, go to the Workstation Inventory policy's *Hardware Scan* tab, select the *Enable Custom Scanning* option, and specify the name of the application. For more information, see [Section 73.6, “Configuring the Workstation Inventory Policy,” on page 958](#).

This application is launched by the Scanner.

Guidelines for Creating the CUSTOM.INI File

Follow these guidelines as you work with the `custom.ini` file:

- If the Inventory class name is not specified, the custom attributes and their corresponding values are added to the CIM.UnitaryComputerSystem table.
- If the regular attribute name is not specified, the custom attributes and their corresponding values are added to the appropriate Inventory class only if one instance of the Inventory class exists in the Inventory database.

If multiple instances of the Inventory class exist, you must specify a minimum set of regular attributes and their corresponding values to distinguish the instances.

- Each regular attribute must have a corresponding value.
- If the action to be performed (addition or deletion) is not specified, the custom attribute values are added to the appropriate Inventory class.
- Do not use a semicolon (;) in a custom attribute name or custom attribute value. The data after the semicolon (;) is ignored by the Scanner.
- Use only alphanumeric characters in the custom attribute name.
- If the custom attribute value is a date, you must enter the date value in the format YYYY-MM-DD (year-month-day).
- If a query has more than one regular attribute or regular attribute value, use a comma (,) as the separator between regular attribute names and regular attribute values.
- If a regular attribute value has a comma (,) in it, precede the comma with a backslash (\).

For example, if the regular attribute value is "Novell, Ltd.", the regular attribute value should be written as follows in the `custom.ini` file:

```
Novell\, Ltd.
```

- A `custom.ini` file can have more than one section.

A sample `custom.ini` file with two sections is as follows:

```
[START_CIM_OBJECT]
Class = Computer System Information
RegularAttrs = Name, PrimaryOwnerContactID
RegularVals = John, 56
Action = D
EmployeeName= Tom
EmployeeId=568
[END_CIM_OBJECT]
[START_CIM_OBJECT]
Class = Diskette Drive
RegularAttrs = DisketteDeviceID
RegularVals = A:
Action = A
Manufacturer = Sony
[END_CIM_OBJECT]
```

- If a query returns multiple instances for regular attributes, the custom attribute and its corresponding values are not added to the Inventory database.

For example, a workstation has two floppy drives, one mapped to A: and the other to B:, and the storage capacity of both the drives is 1440 KB. If you want to add "Rate" as the custom attribute, you cannot write a query using only the DisketteCapacity regular attribute as follows:

```
[START_CIM_OBJECT]
Class = Diskette Drive
RegularAttrs = DisketteCapacity
RegularVals = 1440
Action = A
Rate = $100
[END_CIM_OBJECT]
```

The above query returns two instances. One is the floppy drive mapped to A: and the other is the floppy drive mapped to B:. The custom attribute and its value are not added to the Inventory database.

You could rewrite the `custom.ini` file as follows:

```
[START_CIM_OBJECT]
Class = Diskette Drive
RegularAttrs = DisketteDeviceID
RegularVals = A:
Action = A
Rate = $100
[END_CIM_OBJECT]
[START_CIM_OBJECT]
Class = Diskette Drive
RegularAttrs = DisketteDeviceID
RegularVals = B:
Action = A
Rate = $100
[END_CIM_OBJECT]
```

Viewing Custom Attributes and Custom Attribute Values

You can view the custom attributes and the values of all the inventoried workstations in the Workstation Inventory. For more information, see [Section 77.1.2, “Viewing the Inventory Summary of an Inventoried Workstation,” on page 1096](#).

Custom Inventory Scanning Examples

- **Example 1:** Adds the custom attributes Employee Name and Employee Code with values of XYZ and BLR_TERCH_5000234 respectively to CIM.UnitaryComputerSystem.

Using the [Custom Attribute Editor dialog box](#), add Employee Name and Employee Code to Computer System Information.

Create the `custom.ini` file with the following contents:

```
[START_CIM_OBJECT]
Employee Name = XYZ
Employee Code = BLR_TERCH_5000234
[END_CIM_OBJECT]
```

After creating the `custom.ini` file, run the Novell Desktop Management Scheduler to start the scan.

- **Example 2:** Adds the custom attributes Price and Value \$4.00 to ZENworks.ExtendedDisketteDrive if the value of the regular attribute DisketteDeviceID is A:. Also adds custom attribute Price with a Value \$8.00 to ZENworks.ExtendedDisketteDrive if the value of the regular attribute DisketteDeviceID is B:

Using the **Custom Attribute Editor dialog box**, add Price to Diskette Drive.

Create the custom.ini file with the following contents:

```
[START_CIM_OBJECT]
Class =Diskette Drive
RegularAttr = DisketteDeviceID
RegularVals = A:
Price = $4.00
[END_CIM_OBJECT]
[START_CIM_OBJECT]
Class = Diskette Drive
RegularAttr = DisketteDeviceID
RegularVals = B:
Price = $ 8.00
[END_CIM_OBJECT]
```

After creating the custom.ini file, run the Novell Desktop Management Scheduler to start the scan.

- **Example 3:** Deletes the custom attribute Employee Name from CIM.UnitaryComputerSystem.

Create the custom.ini with the following contents:

```
[START_CIM_OBJECT]
Action = D
Employee Name = XYZ
[END_CIM_OBJECT]
```

After creating the custom.ini file, run the Novell Desktop Management Scheduler to start the scan.

- **Example 4:** To reset the value of Employee Code from BLR_TERCH_5000234 to BLR_TEST_1200012 in CIM.UnitaryComputerSystem

Create the custom.ini file with the following contents:

```
[START_CIM_OBJECT]
Action = A
Employee Code = BLR_TEST_1200012
[END_CIM_OBJECT]
```

After creating the custom.ini file, run the Novell Desktop Management Scheduler to start the scan.

- **Example 5:** Adds the custom attributes Price with value \$100.00 to CIM.Processor if the values of the regular attributes Family and MaxClockSpeed are 178 and 1500 respectively. Also adds the custom attributes Price with its value \$250.00 to CIM.Processor if the values of the regular attributes Family and MaxClockSpeed are 178 and 2000 respectively.

Using the **Custom Attribute Editor dialog box**, add Price to Processor.

Create the custom.ini file with the following contents:

```
[START_CIM_OBJECT]
Class = Processor
RegularAttr = Family, MaxClockSpeed
RegularVals = 178, 1500 ; Pentium 4 with MaxClockSpeed = 1500 MHz
Price = $ 100.00
[END_CIM_OBJECT]
[START_CIM_OBJECT]
Class = Processor
```

```
RegularAttr = Family, MaxClockSpeed
RegularVals = 178, 2000 ; Pentium 4 with MaxClockSpeed = 2000 MHz
Price = $ 2500.00
[END_CIM_OBJECT]
```

After creating the `custom.ini` file, run the Novell Desktop Management Scheduler to start the scan.

76.2.2 Scanning for IBM Computer Models

The IBMNAMES information (configured using the *Configuration Editor* > the *IBMNAMES* option in the Workstation Inventory policy) is used to get information about IBM inventoried workstations running under Windows 98. The Scanner reads the model name using the machine type and model number information specified in the Configuration Editor option of the Workstation Inventory policy.

Using the IBMNAMES information is an IBM-specific method of scanning model names of IBM inventoried workstations defined by the Scanner. If you have a new IBM inventoried workstation that is not listed in the Configuration Editor, the model number of the inventoried workstation is not scanned. To add the machine type, model number, and model description of the new IBM inventoried workstation, you must edit the IBMNAMES information in the Configuration Editor using the Workstation Inventory policy. By adding this entry, you enable the Scanner to identify the new model name.

To add the IBM computer models:

- 1 In the Workstation Inventory policy, click the *Configuration Editor* tab.

For more information, see [Section 73.6, “Configuring the Workstation Inventory Policy,” on page 958](#).

- 2 Click the *IBMNAMES* suboption, then click *Set Defaults*.

The default values are displayed.

```
[Product Names]
6260-??? = IBM PC 140
6272-??? = IBM PC 300GL
6282-??? = IBM PC 300GL
6284-??? = IBM PC 300GL
...
```

The format of each entry in the section is as follows:

```
4_bytes_machine_type-3_byte_model_number=model_description
```

For example, if the model is IBM PC 140 and the machine type is 6260, specify the model description as IBM PC 140. The entry in the `ibmnames.ini` is `6260-79T = IBM PC 140`.

If you want the Scanner to scan for all IBM computer models of a particular machine type with the same model description, the *3_byte_model_number* is specified with three question marks (???) as wildcard characters.

For example, to scan all models of a 6282 machine type with same model description, the entry is as follows:

```
6282-???=IBM PC 300GL
```

The machine type and model number are printed at the rear of the laptop or on the back side of the desktop workstation. For example, the 760E Thinkpad* model has the following label:
TYPE 9546-A98.

3 Add or modify the entries.

If you specify incorrect values for the device ID entry, the device is not displayed in the Inventory windows.

4 Click *OK*.

76.2.3 Customizing the Hardware Scanning Information of Jaz, Zip, and Floppy Drive Vendors

The scan information of the vendors for devices such as backup and floppy devices is usually unavailable on the inventoried workstation. Also, if the information is available, the vendor information does not usually contain the details. You can customize and update information about the vendors of these devices in Workstation Inventory policy > *Configuration Editor* > *Zipped Names*. The Scanners read this information during the hardware scanning process for these devices.

To customize and update the vendor information for display:

1 In the Workstation Inventory policy, click the *Configuration Editor* tab.

For more information, see [Section 73.6, “Configuring the Workstation Inventory Policy,” on page 958](#).

2 Click the *ZIPPED NAMES* suboption, then click *Set Defaults*.

The default values are displayed.

```
[Identifier]
iomega ZIP 100=Iomega 100MB Backup Device
iomega jaz 1GB=Iomega 1GB Backup Device
IOMEGA ZIP 100          D.13=Iomega Corporation
IOMEGA ZIP 1GB          D.13=Iomega Corporation
...
```

The format of each entry in the section is as follows:

```
[Identifier]
device_id=vendor_display_name_you_specify
```

where *device_id* is the unique ID generated and updated in the registry by the vendor during the installation of the device on the inventoried workstation.

For example, the contents of the section are as follows:

```
[Identifier]
iomega ZIP 100=Iomega 100MB Backup Device
```

This entry is for a 100 MB Zip drive installed on the inventoried workstation.

3 Add or modify the entries.

If you specify incorrect values for the device ID entry, the device is not displayed in the Inventory windows.

4 Click *OK*.

76.2.4 Scanning for Vendor-Specific Asset Information from DMI

- 1 In the Workstation Inventory policy, click the *Configuration Editor* tab.

For more information, see [Section 73.6, “Configuring the Workstation Inventory Policy,”](#) on [page 958](#).

- 2 Click the *Asset Information* suboption, then click *Set Defaults*.

The following entries are populated.

```
[ASSETTAG]
DMI1_CLASSNAME=
DMI1_ATTRIBUTEID=
DMI2_CLASSNAME=
DMI2_ATTRIBUTEID=
[SERIALNUMBER]
DMI1_CLASSNAME=
DMI1_ATTRIBUTEID=
DMI2_CLASSNAME=
DMI2_ATTRIBUTEID=
[MODEL]
DMI1_CLASSNAME=
DMI1_ATTRIBUTEID=
DMI2_CLASSNAME=
DMI2_ATTRIBUTEID=
[COMPUTERTYPE] DMI1_CLASSNAME=DMI1_ATTRIBUTEID=
[MODELNUMBER] DMI1_CLASSNAME=DMI1_ATTRIBUTEID=
```

- 3 Specify the values.

The Asset Information contains the following sections:

- Contains Asset Tag in the section [ASSETTAG]
- Contains Serial Number in the section [SERIALNUMBER]
- Contains Computer Model in the section [MODEL]
- Contains Computer Type [COMPUTERTYPE]
- Contains Computer Model Number [MODELNUMBER]

Each section contains the particular DMI Class name and DMI Class Attribute ID.

The format of Asset Information is as follows:

```
[ASSETTAG]
DMI1_CLASSNAME=DMI_class_name_for_asset_tag
DMI1_ATTRIBUTEID=DMI_attribute_ID_for_asset_tag
[SERIALNUMBER]
DMI1_CLASSNAME=DMI_class_name_for_serial_number
```

DMI1_ATTRIBUTEID=*DMI_attribute_ID_for_serial_number*

[MODEL]

DMI1_CLASSNAME=*DMI_class_name_for_computer_model*

DMI1_ATTRIBUTEID=*DMI_attribute_ID_for_computer_model*

The value of the Asset Information sections can have a maximum string length of 64 characters.

A DMI Class name can be any DMI class other than DMTF|COMPONENTID|00x.

If there is more than one DMI vendor implementing different custom DMI classes, you can specify multiple DMI classes. A maximum of five classes can be specified in these sections. For example, the asset information for five classes is as follows:

[ASSETTAG]

DMI1_CLASSNAME=*DMI_class_name_for_asset_tag*

DMI1_ATTRIBUTEID=*DMI_attribute_ID_for_asset_tag*

DMI2_CLASSNAME=*DMI_class_name_for_asset_tag*

DMI2_ATTRIBUTEID=*DMI_attribute_ID_for_asset_tag*

DMI3_CLASSNAME=*DMI_class_name_for_asset_tag*

DMI3_ATTRIBUTEID=*DMI_attribute_ID_for_asset_tag*

DMI4_CLASSNAME=*DMI_class_name_for_asset_tag*

DMI4_ATTRIBUTEID=*DMI_attribute_ID_for_asset_tag*

DMI5_CLASSNAME=*DMI_class_name_for_asset_tag*

DMI5_ATTRIBUTEID=*DMI_attribute_ID_for_asset_tag*

The Scanner processes DMI1 and if the values of DMI1 are valid, the Scanner does not process the remaining DMI classes.

4 Click *OK*.

5 Run the scans on the inventoried workstations.

Verify that the inventory information is in eDirectory Minimal Information and the Workstation Summary window.

76.2.5 Customizing the Hardware Information for Monitor Size

The attributes scanned for a monitor includes the following:

Nominal Size: A number representing the diagonal width of the monitor (the distance from one corner of the screen to the opposite corner of the screen). For example, 17”.

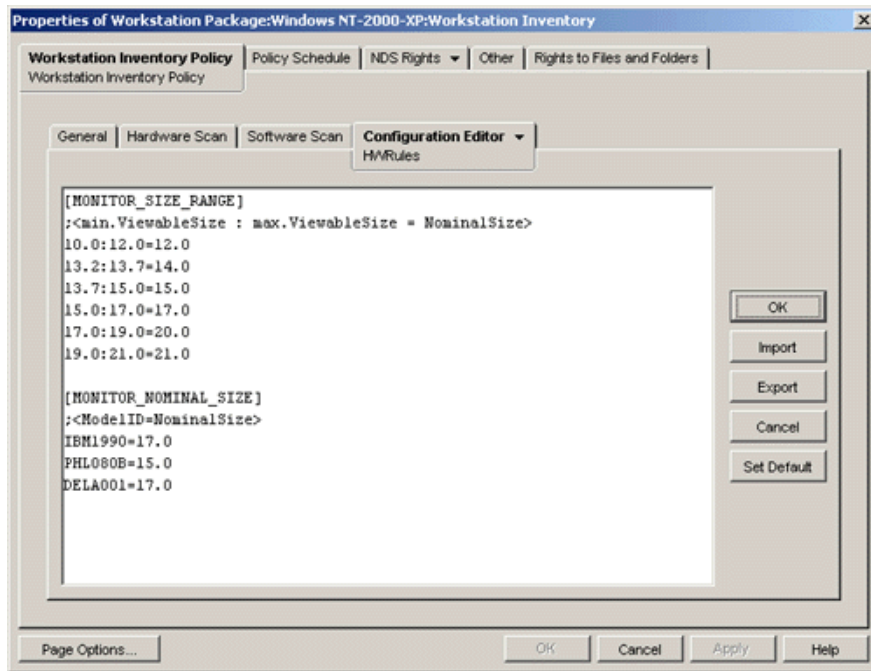
Viewable Size: A number representing the diagonal width of the screen image excluding the black borders around the image's edge. For example, 15.8”.

The Inventory scanner automatically scans for the viewable size of the monitor of Windows inventoried workstations. Using the Workstation Inventory policy, you can customize the nominal size of the monitor to be reported.

IMPORTANT: The Inventory scanner reports inventory information for the monitors that are manufactured only after 1997.

To customize the scan of the nominal size of the monitor:

- 1 In the Workstation Inventory policy, click the *Configuration Editor* tab, then click the *HWRules* suboption.



- 2 Click *Set Default*.

The default values are displayed in the Configuration Editor box.

- 3 Add or modify the entries.

The format of `hwrules.ini` is as follows:

```
[MONITOR_SIZE_RANGE]
minimum_viewable_size_you_specify:
maximum_viewable_size_you_specify = nominal_size_you_specify
[MONITOR_NOMINAL_SIZE]
model_ID_reported_by_scanner = nominal_size_you_specify
```

In the [MONITOR_SIZE_RANGE] section, specify the minimum and maximum range of the viewable size, and the corresponding nominal size of the monitor. The Inventory scanner scans for the model ID of the monitor and reports the nominal size configured in the [MONITOR_NOMINAL_SIZE] section of the `hwrules.ini` file.

In the [MONITOR_NOMINAL_SIZE] section, specify the model ID and its corresponding nominal size as reported by the Inventory scanner. This information is available in the Inventory Summary dialog box under the Hardware/Software Inventory > Hardware > Monitor attribute.

If the scanned model ID is not listed in [MONITOR_NOMINAL_SIZE], then the scanner scans the viewable size of the monitors. On the basis the viewable size, the scanner reports the nominal size configured in the [MONITOR_SIZE_RANGE] section of the `hwrules.ini` file.

For example, the contents of the `hwrules.ini` file could be as follows:

```
[MONITOR_SIZE_RANGE]
10.0:12.0=12.0
13.2:13.7=14.0
[MONITOR_NOMINAL_SIZE]
IBM1990=17.0
PHL080B=15.0
```

4 Click *OK* to save the contents to the Workstation Inventory policy.

76.3 Customizing the Software Inventory Information To Be Scanned For ZENworks 7 Inventoried Workstations

The Inventory scanner has been enhanced with the following features that enable you to control the scanning process more effectively and efficiently for inventoried workstations having ZENworks 7 Workstation Inventory:

- It supports scanning for the following software inventory information:
 - Windows operating system and its patches
 - Internet Explorer and its patches
 - Windows Media Player and its patches
 - Outlook Express and its patches
 - Novell Client32™ and its installed components
 - The ZENworks suite and its installed components
 - Microsoft Office and its installed applications
 - Antivirus products such as Symantec Antivirus Corporate Edition and McAfee Antivirus
 - Virus definition date and version for the antivirus products such as Symantec Antivirus Corporate Edition and McAfee Antivirus
- It supports scanning for the products listed in the Windows Add/Remove Programs and the MSI database.
- It includes dictionary of software titles to provide more accurate report of Installed software.
- It provides rules to control the scope of software scan.
- It reports total disk usage against configured file extensions.

This section provides information on the following topics:

- [Section 76.3.1, “What is the ZENworks Software Dictionary?,” on page 1036](#)
- [Section 76.3.2, “What is a Software Dictionary Rule?,” on page 1036](#)
- [Section 76.3.3, “What is a Software Identifier?,” on page 1036](#)
- [Section 76.3.4, “What is a Key Identifier?,” on page 1037](#)
- [Section 76.3.5, “What is Unidentified Software?,” on page 1037](#)
- [Section 76.3.6, “What is an Inherited Rule?,” on page 1037](#)
- [Section 76.3.7, “What is an Overriding Rule?,” on page 1037](#)

- [Section 76.3.8, “Understanding the Usage and Precedence of ZENworks Software Dictionary Rules,” on page 1037](#)
- [Section 76.3.9, “Understanding the Software Dictionary Pattern Types,” on page 1044](#)
- [Section 76.3.10, “Configuring the Software Dictionary Rules,” on page 1045](#)
- [Section 76.3.29, “Disabling File Scan,” on page 1077](#)
- [Section 76.3.30, “Base-Lining the Software Dictionary Deployment,” on page 1078](#)
- [Section 76.3.31, “Viewing Software Information in the Inventory Summary,” on page 1079](#)
- [Section 76.3.32, “Generating Software Inventory Reports,” on page 1079](#)

76.3.1 What is the ZENworks Software Dictionary?

The ZENworks software dictionary contains a list of software identifiers and rules. Each software identifier identifies a particular product installed on an inventoried workstation. The rules control the scope of the scanning process.

The ZENworks software dictionary is automatically installed on an Inventory Server and inventoried workstations when you install the Workstation Inventory software. After you configure the required policies and start the Inventory service, the Inventory scanner reports the software information on the basis of the software dictionary.

There are two types of software dictionary: the General dictionary and the Private dictionary.

General Dictionary: The General dictionary is the part of the software dictionary that contains predefined software identifiers. On the basis of this dictionary, the Inventory scanner reports whether a particular product is installed on an inventoried workstation.

Private Dictionary: The private dictionary is the part of the software dictionary that contains user-defined software identifiers and rules that enable you to define the scope of Inventory scan and customize the software information. You can configure the rules. For more information on how to configure the rules, [Section 76.3.10, “Configuring the Software Dictionary Rules,” on page 1045](#).

IMPORTANT: The rules that you define in the private dictionary override the predefined rules in the general dictionary.

76.3.2 What is a Software Dictionary Rule?

A software dictionary rule represents a set of conditions that control the scope of the scanning process.

76.3.3 What is a Software Identifier?

An entry that identifies a software product is called as software identifier. Each software identifier has a set of file matching attributes and corresponding software information attributes. During the Inventory scan, the scanner reads the attributes from the file headers, and if these attributes match the attributes configured in the dictionary, the information in the corresponding software information attributes is stored in the Inventory database.

76.3.4 What is a Key Identifier?

A software product might be identified through more than one software identifier in the dictionary. In such a scenario, the inventory scanner arbitrarily selects the software information from one of these software identifiers. A key identifier identifies the software identifier from which the inventory scanner should select the software information. The key identifier is useful when the different software identifiers have marginal differences between the values of the attributes (such as Description) and you want the inventory scanner to select the information from a specific software identifier.

76.3.5 What is Unidentified Software?

An unidentified software has the following characteristics.

- It is installed on the inventoried workstations.
- It is configured in the [Report Files with These File Extensions As Unidentified Software](#) rule in ZENworks software dictionary.
- It is not configured in the [Software Dictionary](#) table.

76.3.6 What is an Inherited Rule?

An inherited rule is an entry in the software dictionary that is obtained from another Inventory server through the dictionary distribution. You cannot edit or delete these rules. These rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

76.3.7 What is an Overriding Rule?

The default software identifier in the General dictionary cannot be modified. If you want to modify a default software identifier, you must create a new software identifier that overrides the default identifier. The inventory scanner ignores the default the default identifier in favor of the overridden entry.

To create a software identifier that overrides a default identifier, you must specify the same values for all the matching attributes defined in the default identifier and provide new values for the software information attributes.

76.3.8 Understanding the Usage and Precedence of ZENworks Software Dictionary Rules

The ZENworks software dictionary rules follow a precedence order. Some guidelines are applicable to all the software dictionary rules and some guidelines are applicable to certain categories of software dictionary rules. For more information, review the following sections:

- [“Guidelines Applicable to All Software Dictionary Rules” on page 1038](#)
- [“Precedence between Report Only Maximum Software Version and Report All Software Versions” on page 1038](#)
- [“Precedence of Software Dictionary Rules in the Software Scanning Category” on page 1038](#)
- [“Precedence of Software Dictionary Rules in the Disk Usage Scanning Category” on page 1041](#)

Guidelines Applicable to All Software Dictionary Rules

The following guidelines are applicable to all the software dictionary rules that you configure:

- All software dictionary rules are applied at the inventoried workstations by the inventory scanner.
- You can change the settings of the software dictionary rules using the software dictionary ConsoleOne snap-ins. For more information on how to configure the software dictionary rules, see [Section 76.3.10, “Configuring the Software Dictionary Rules,” on page 1045](#).
- Every inventory scan contains the version of dictionary files used for that scan. This information is stored in the inventory database.
- The user-defined software identifier overrides the default software identifier present in the software dictionary but only one user-defined software identifier can be used at a time to override a default software identifier.

Precedence between Report Only Maximum Software Version and Report All Software Versions

By default, the scanner reports only the highest version of the software installed. If a rule in “Report All Software Versions” conflicts with a rule in “Report Only Maximum Software Version”, then the rule in “Report Only Maximum Software Version” overrides the rule in “Report All Software Versions”.

Precedence of Software Dictionary Rules in the Software Scanning Category

The software dictionary rules in the Software Scanning category control the scope of scanning for the files on the local file systems.

The Software Scanning category includes the following software dictionary rules:

- [“Scan File Extensions” on page 1063](#)
- [“Ignore File Extensions” on page 1063](#)
- [“Scan Directories” on page 1061](#)
- [“Ignore Directories” on page 1060](#)
- [“Scan Drives” on page 1059](#)
- [“Ignore Drives” on page 1059](#)
- [Section 76.3.20, “Software Scanning Filters - Software,” on page 1065](#)
- [Section 76.3.19, “Software Scanning Filters - Files,” on page 1064](#)

If you do not configure any of the rules mentioned above, the Inventory scanner scans for all files on the hard disk of the inventoried workstations. If the files have matching software identifiers in the software dictionary, the files are reported as identified software. Otherwise, they are reported as unidentified software.

If you configure the rules mentioned above, they take precedence in the following descending order:

- Software Scanning Filters - Files
- Software Scanning Filters - Software
- Scan File Extensions

- Ignore File Extensions
- Scan Directories
- Ignore Directories
- Scan Drives
- Ignore Drives

The following flowcharts illustrate the precedence of these rules.

Figure 76-1 *Precedence of Software Dictionary rules in the Software Scanning category*

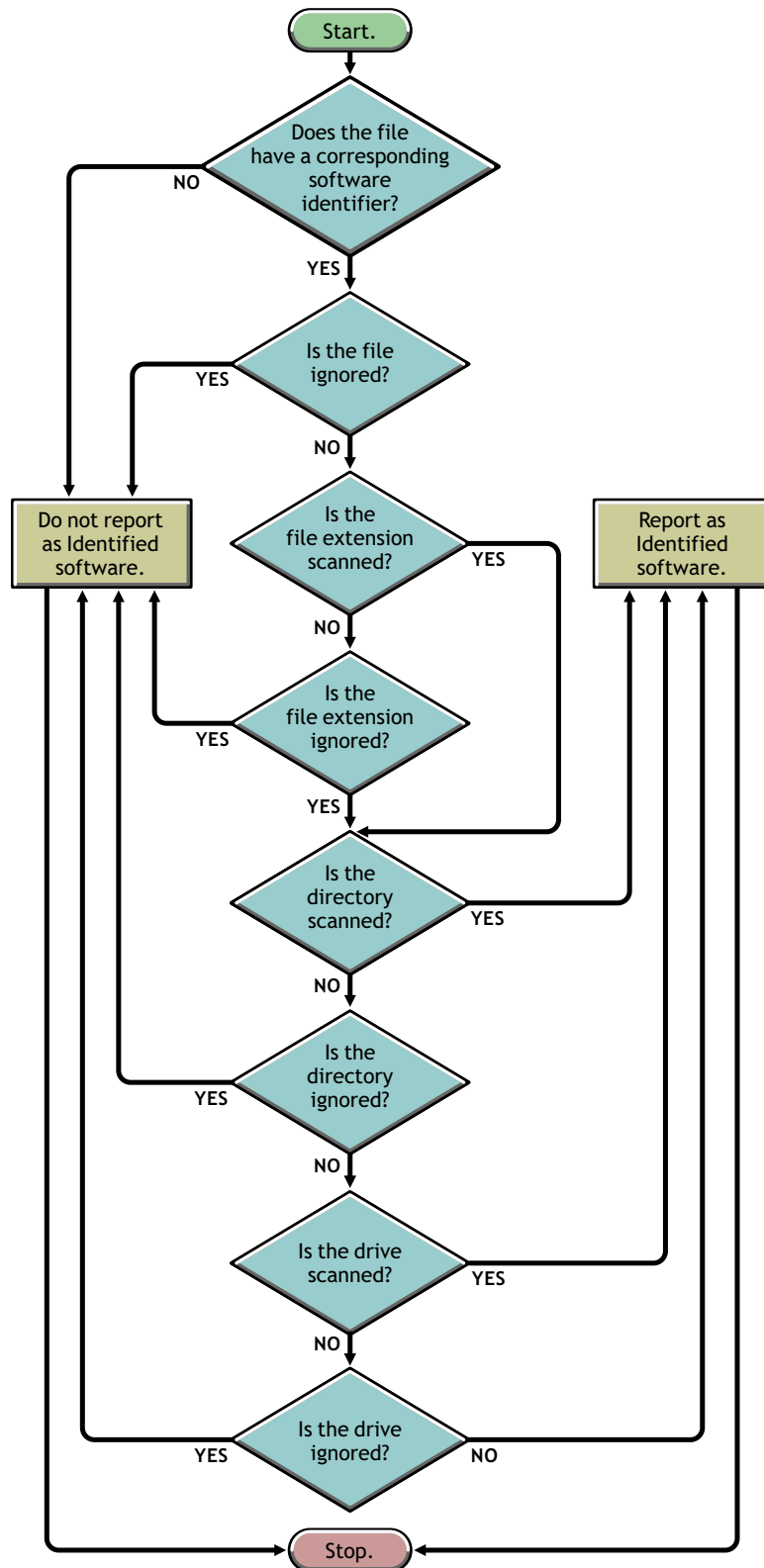
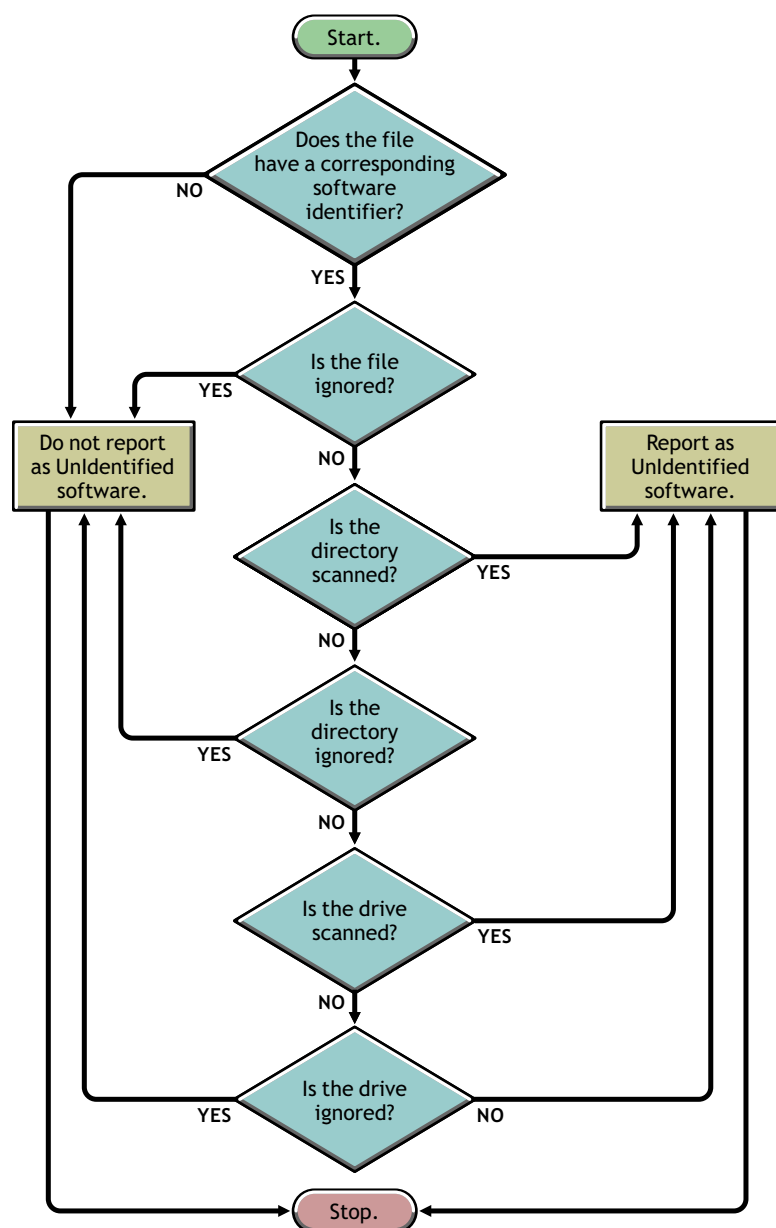


Figure 76-2 *Precedence of Software Dictionary rules in the Software Scanning category*



Precedence of Software Dictionary Rules in the Disk Usage Scanning Category

The software dictionary rules in the Disk Usage Scanning category determine whether a file should be considered for disk usage scan.

The Disk Usage Scanning category includes the following software dictionary rules:

- [Section 76.3.16, “Report Disk Space Used by File Extensions,” on page 1056](#)
- [Section 76.3.22, “Disk Usage Scanning Filters - Files,” on page 1071](#)
- [“Scan Directories” on page 1070](#)
- [“Ignore Directories” on page 1069](#)

- “Scan Drives” on page 1068
- “Ignore Drives” on page 1068

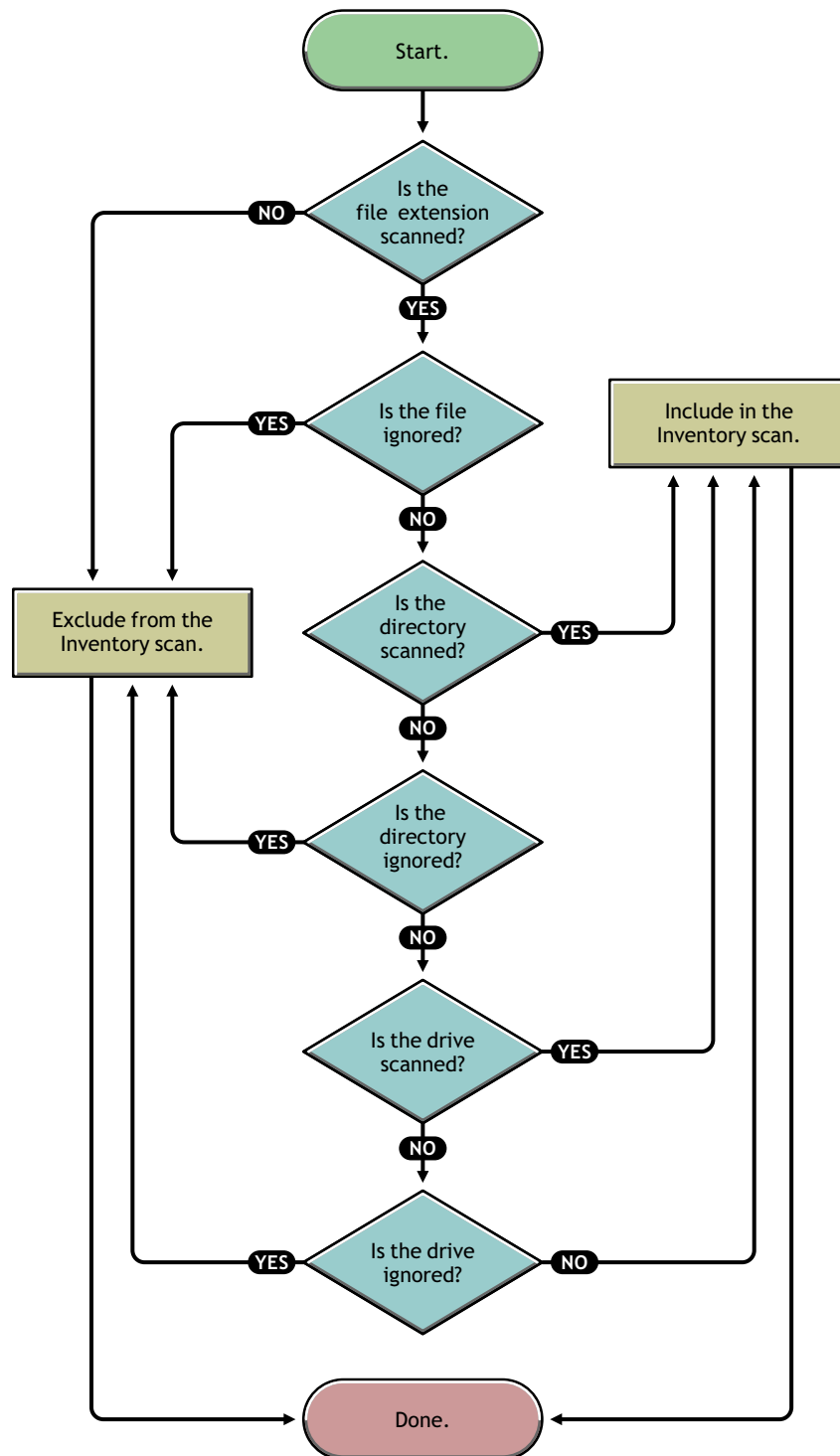
For a file to be considered for the disk usage scan, its file extension must be listed in the “Report Disk Space Used by File Extensions” rule and it should not be excluded from inventory scan in the other Disk Usage Scanning rules.

The following list indicates the precedence of rules in the descending order:

- Report Disk Space Used by File Extensions
- Disk Usage Scanning Filters - Files
- Scan Directories
- Ignore Directories
- Scan Drives
- Ignore Drives

The following flowchart illustrates the precedence of these rules.

Figure 76-3 *Precedence of Software Dictionary rules in the Disk Usage Scanning category*



76.3.9 Understanding the Software Dictionary Pattern Types

Before configuring the software dictionary rules, you must be aware of the following software dictionary pattern types that are supported in ZENworks 7:

- “Regular Expression” on page 1044
- “Expandable Expression” on page 1044
- “System Expandable Expression” on page 1044

Regular Expression

A Regular Expression refers to the POSIX* regular expressions. For more information on regexp (regular expressions), see [The Open Group Base Specifications Issue 6 Web site \(http://www.opengroup.org/onlinepubs/007904975/basedefs/xbd_chap09.html\)](http://www.opengroup.org/onlinepubs/007904975/basedefs/xbd_chap09.html).

Examples of Regular Expression usage:

- To find all vendor names starting with “Novell,” specify `Novell.*`
- To find executables, specify `[exe|EXE]`
- To find files with name containing 6 characters, starting with “r” and ending with “t”, specify `[r....t]`
- To find files with a name starting from A to C, and ending with E, specify `[A-C].*[E]`
- To find files whose name do not contain any uppercase letters, specify `[^A-Z]+`

NOTE: To use meta characters such as `[, \, ^, $, ., |, ?, (,), *, and +` as characters, you must prefix them with a backslash (`\`). For example, to specify `c:\windows` as a regular expression, specify it as `c:\\windows`.

Expandable Expression

An Expandable Expression contains displayable characters and the asterisk (*) wildcard character.

“*” matches to zero or more displayable characters.

Examples of Expandable Expression usage:

- To find all instances of the vendor name beginning with “Microsoft,” specify `Microsoft*`.
- To find files with the extension “.exe” in the scan, specify `exe`.

System Expandable Expression

- **On NetWare:** A System Expandable Expression contains displayable characters or references to environmental variables.

Example of an environmental variable: `$sysdir`

- **On Windows:** A System Expandable Expression contains displayable characters, references to environmental variables, or the asterisk (*) wildcard character.

“*” matches to zero or more displayable characters.

Example of an environmental variable: `%temp%`

IMPORTANT: A System Expandable Expression can contain a combination of displayable characters, references to environmental variables, or the asterisk (*) wildcard character, however, if it contains an environmental variable, you must specify it at the beginning of the expression. For example, %temp%/*

Examples of System Expandable Expression usage:

- To find the disk usage of the C drive, specify C.
- To find files in the c:\program files directory, specify c:\program files.
- To find files with the extensions, “.com”, specify com.

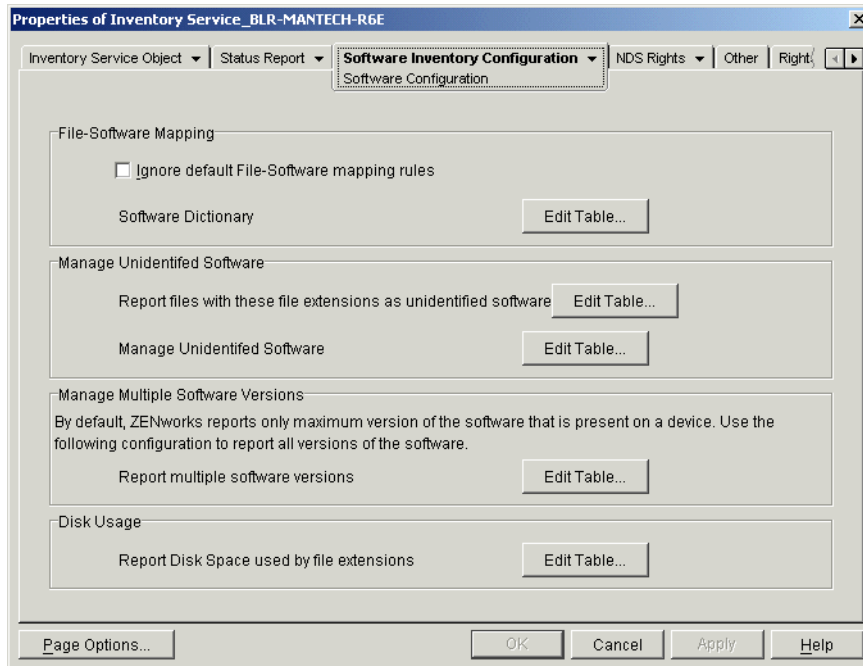
76.3.10 Configuring the Software Dictionary Rules

- 1 In ConsoleOne, right-click the Inventory Service object (Inventory Service_*server_name*), then click *Properties*.
- 2 Click the *Software Inventory Configuration* tab. The Software Configuration page is displayed by default.

You can configure the following settings to scan the software inventory information:

- **File - Software Mapping:** Includes the following rules:
 - [Section 76.3.11, “Ignore Default File-Software Mapping Rules,” on page 1048](#)
 - [Section 76.3.12, “Software Dictionary,” on page 1048](#)
- **Manage Unidentified Software:** Includes the following rules:
 - [Section 76.3.13, “Report Files with These File Extensions As Unidentified Software,” on page 1052](#)
 - [Section 76.3.14, “Manage Unidentified Software,” on page 1053](#)
- **Manage Multiple Software Versions:** Includes the following rule:
 - [Section 76.3.15, “Report Multiple Software Versions,” on page 1054](#)
- **Disk Usage:** Includes the following rule:
 - [Section 76.3.16, “Report Disk Space Used by File Extensions,” on page 1056](#)

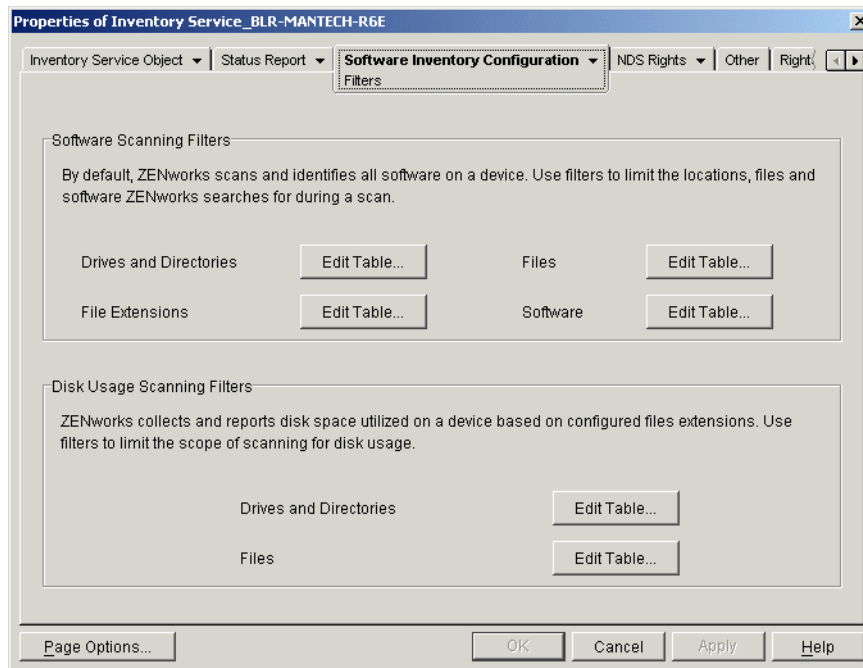
IMPORTANT: Before configuring any ZENworks software dictionary rules, you must be aware of how to use these rules. For detailed information, see [Section 76.3.8, “Understanding the Usage and Precedence of ZENworks Software Dictionary Rules,” on page 1037](#).



3 To control the scope of scanning for files, click the *Filters* page and configure the following settings:

- **Software Scanning Filters:** Includes the following filters:
 - [Section 76.3.17, “Software Scanning Filters - Drives and Directories,”](#) on page 1057
 - [Section 76.3.18, “Software Scanning Filters - File Extensions,”](#) on page 1062
 - [Section 76.3.19, “Software Scanning Filters - Files,”](#) on page 1064
 - [Section 76.3.20, “Software Scanning Filters - Software,”](#) on page 1065
- **Disk Usage Scanning Filters:** Includes the following filters:
 - [Section 76.3.21, “Disk Usage Scanning Filters - Drives and Directories,”](#) on page 1067
 - [Section 76.3.22, “Disk Usage Scanning Filters - Files,”](#) on page 1071

IMPORTANT: Before configuring any ZENworks software dictionary rules, you must be aware of how to use these rules. For detailed information, see [Section 76.3.8, “Understanding the Usage and Precedence of ZENworks Software Dictionary Rules,”](#) on page 1037



4 Click the *Aliases* page to configure the following options:

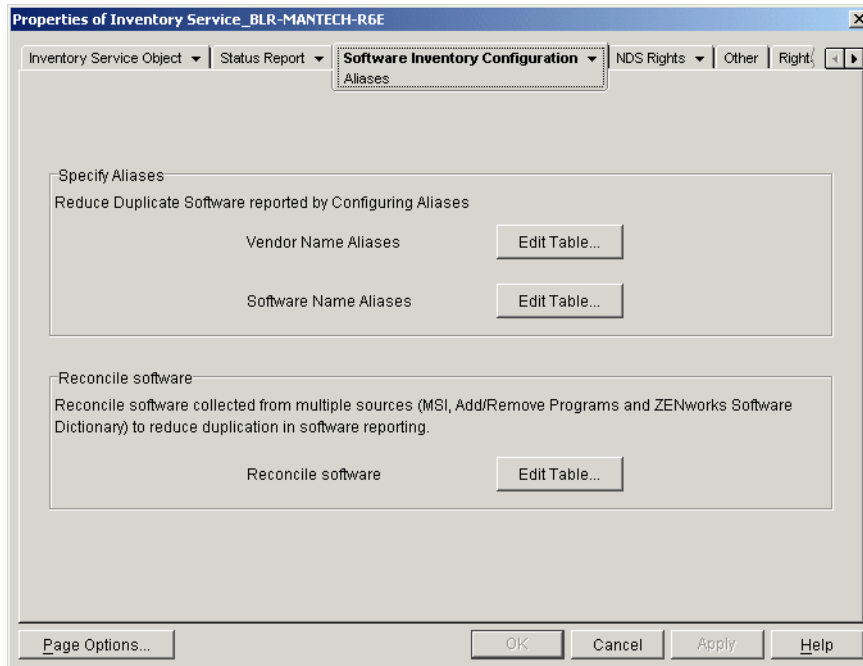
- **Specify Aliases:** Allows you to configure aliases for vendor and software names.

By default, the software information is categorized by vendor name in the Inventory ConsoleOne utilities. The software from the same vendor might sometimes have differing vendor names or product names. In this scenario, the Inventory ConsoleOne utilities display the software information under different sections.

However, you can merge the software information by specifying aliases. You customize these settings in the following software dictionary rules:

- [Section 76.3.23, “Vendor Name Aliases,” on page 1072](#)
 - [Section 76.3.24, “Software Name Aliases,” on page 1074](#)
- **Reconcile Software:** Allows you to merge the software identified through Add/Remove Programs or the MSI, and the software identified through the ZENworks software dictionary. For more information, see [Section 76.3.25, “Reconcile Software,” on page 1075](#).

IMPORTANT: Before configuring any ZENworks software dictionary rules, you must be aware of how to use these rules. For detailed information, see [Section 76.3.8, “Understanding the Usage and Precedence of ZENworks Software Dictionary Rules,” on page 1037](#).



5 Click *Apply*, then click *Close*.

76.3.11 Ignore Default File-Software Mapping Rules

In the Software Configuration property page, select the *Ignore Default File-Software Mapping Rules* check box if you do not want the Inventory scanner to use the default File-Software mapping rules that are configured in the ZENworks software dictionary for scanning software inventory information.

IMPORTANT: This option is not available for selection if the software dictionary is updated from another Inventory server.

76.3.12 Software Dictionary

The *Software Dictionary* option allows you to configure software identifiers in the ZENworks software dictionary.

By default, the ZENworks software dictionary contains predefined software identifiers. You can create new software identifiers in the ZENworks software dictionary by editing the predefined software identifiers or by creating a new software identifier.

To configure rules in the ZENworks software dictionary:

- 1 In the Software Configuration property page, click the *Edit Table* option of *Software Dictionary*.

The Software Dictionary table is displayed.

Dictionary ...	Key identifier	Filename	File Last Modified Time...	Minimum file size	Maximu...	Softw:
33823	No	MVREAD...	2003-07-14 15:25	2460160	2460160	Reader
33822	No	NETSONI...	2000-12-18 12:56	3000096	3000096	Netsonic
33821	No	MSHOW...	2003-10-29 11:37	639056	639056	Mshow
33820	No	PCBODY...	2003-01-20 18:06	942080	942080	PC Body
33819	No	AGMAIL.E...	2004-01-19 23:29	1511424	1511424	Group M
33818	No	NOTETA...	2002-08-26 17:26	1725440	1725440	NoteTab
33817	No	CITYDES...	2002-08-08 17:21	3891200	3891200	CityDesk
33816	No	EEBED9...	2003-08-17 22:22	294912	294912	Executab
33815	No	EXEAPI1...	2003-08-17 22:31	17120	17120	Executab
33814	No	PIM.EXE	2002-12-02 19:01	1646592	1646592	Mp3 Play
33813	No	2020.EXE	2001-05-08 16:21	2085376	2085376	20/20
33812	No	BSERAS...	2003-09-22 11:18	208896	208896	Erase
33811	No	ACU.EXE	2003-09-26 11:29	1339392	1339392	ACU
33810	No	PCARMD...	2002-04-18 01:17	45056	45056	AMBIT W
33809	No	MAINCTR...	2003-08-06 08:32	327680	327680	Silence I
33808	No	KILLAD.E...	2000-01-27 16:00	30720	30720	KillAd
33807	No	IPHOTON...	2003-11-30 23:00	1458176	1458176	Newsgro
33806	No	IPHOTO...	2003-10-28 22:50	1839104	1839104	Ipphoto

Buttons: Insert, Delete, Sort..., Filter..., OK, Cancel, Help

Right Panel: Add to (Ignore Software), Add From (Unidentified Software)

The Software Dictionary table displays the data stored in the ZENworks software dictionary. It might contain entries that are:

- **Light gray in color:** Indicates that these entries will not be considered in a scan because the table already contains entries that override these entries.
- **Dark gray in color:** These are inherited rules. For more information about inherited rules, see [Section 76.3.6, “What is an Inherited Rule?”](#) on page 1037.

2 In the Software Dictionary table, you can perform the following operations:

- [“Manually Adding Entries to the Software Dictionary”](#) on page 1049
- [“Automatically Adding Entries to the Software Dictionary”](#) on page 1051
- [“Deleting Entries from the Software Dictionary”](#) on page 1051
- [“Modifying the Values of the Software Dictionary Entries”](#) on page 1051
- [“Excluding a Software from a Scan”](#) on page 1052
- [Section 76.3.26, “Sorting Entries in the Table,”](#) on page 1076
- [Section 76.3.27, “Filtering Entries in the Table,”](#) on page 1076
- [Section 76.3.28, “Refreshing Entries in the Table,”](#) on page 1077

3 Click *OK*.

Manually Adding Entries to the Software Dictionary

1 In the Software Dictionary table, click *Insert* to add a new row.

2 Specify values for the following attributes:

Filename, File Last Modified Time (yyyy-dd-mm hours:minutes), Minimum File Size (bytes), Maximum File Size (bytes), Software Name, Support Pack, Software Version, Internal Version, Description, Vendor, Platform, and Category.

The following attributes are called “matching attributes”: Filename, File Last Modified Time, Minimum File Size, Maximum File Size, and Internal Version. The values of these matching attributes are compared with the values scanned by the Inventory scanner from the file headers on the inventoried workstations.

If the values are same, the values in the corresponding software information attributes (Software Name, Support Pack, Software Version, Description, Vendor, Platform, and Category) are stored in the Inventory database.

In the Software Dictionary table, you must specify values for the following attributes: Filename, Software Name, and Vendor. It is optional to specify values for other attributes.

When you add an entry, a unique ID called the Dictionary Identifier is automatically assigned to this entry.

For example, configure the following settings in the Software Dictionary - Row Editor table:

Filename= MSACCESS . EXE
File Last Modified Time = 1998-30-01 05:30
Minimum File Size = 299854
Maximum File Size = 400000
Software Name = Access
Software Version = 7.0
Internal Version = 7.0
Description = Microsoft Access
Vendor = Microsoft
Category = Database

If the Inventory scanner finds a file with the following values during the scan: “File Name= MSACCESS . EXE; File Last Modified Time= 1998-30-01 05:30; File Size= 300000”, then the following information is stored in the Inventory database:

Software Name = Access
Software Version = 7.0
Description = Microsoft Access
Vendor = Microsoft
Category = Database

If you do not specify a value for an attribute, then this attribute is not considered to determine the overriding entry. Also, only the matching attributes are considered to determine the overriding entry. For example, the Configure Dictionary table has the following entries for MS Word:

Filename	Minimum File Size	Maximum File Size	Software Name	Vendor
winword.exe	10000	10000	Word	Microsoft
winword.exe	0	30000	Word	Microsoft

To determine the overriding entry, only the maximum file size value is considered. Consequently, the second entry with 30000 maximum file size overrides the first entry.

3 (Optional) Select the *Key Identifier* check box for this entry.

For example, the Software Dictionary table has the following entries for MS Word:

Filename	File Last Modified Time	Minimum File Size	Maximum File Size	Software Name	Software version	Internal version	Description	Vendor
winword.exe	2004-30-10 5:30	10000	10000	Word	2002	10.0.4219	Microsoft Word	Microsoft
osa.exe	2004-30-02 16:00	10000	10000	Word	2002	10.0.4300	Microsoft Office XP Component	Microsoft

If the key identifier has not been defined, the software information for MS Word might be selected from anyone of the above entries.

To ensure that the information from the identifier corresponding to “Winword.exe” is selected, select *Key Identifier* for “Winword.exe.” If you select “Winword.exe” as the key identifier in the Configure Software Dictionary table, the Inventory scanner stores the information related to winword.exe into the Inventory database.

Automatically Adding Entries to the Software Dictionary

- 1 In the Software Dictionary table, click *Unidentified Software* located in the *Add From* pane.
- 2 In the Manage Unidentified Software table, do the following:
 - 2a Select the entry to be added to the software dictionary.
 - 2b Click *Software Dictionary* located in the *Add To* pane.
 - 2c Click *Close*.

Deleting Entries from the Software Dictionary

- 1 In the Software Dictionary table, select the entry to be deleted.
- 2 Click *Delete*.

IMPORTANT: You can delete only the non-inherited entries.

Modifying the Values of the Software Dictionary Entries

- 1 In the Software Dictionary table, double-click the entry whose values you want to modify.

You can modify only one entry at a time.

TIP: You can also invoke the Row Editor dialog box by selecting the entry you want to modify and pressing one of the following keys: Enter, Spacebar, or F2.

- 2 Modify the values.
You cannot modify the values of the Dictionary Identifier and Filename attributes.
- 3 Click *OK*.

IMPORTANT: You cannot modify the values of an inherited rule. Also, modifying a default predefined rule creates a new user-defined rule.

Excluding a Software from a Scan

- 1 In the Software Dictionary table, select the corresponding entry for the software you want to exclude from the Inventory scan.
- 2 Click *Ignore Software* located in the *Add To* pane.

The entry is added to the Ignore Software table in **Software Scanning Filters - Software**.

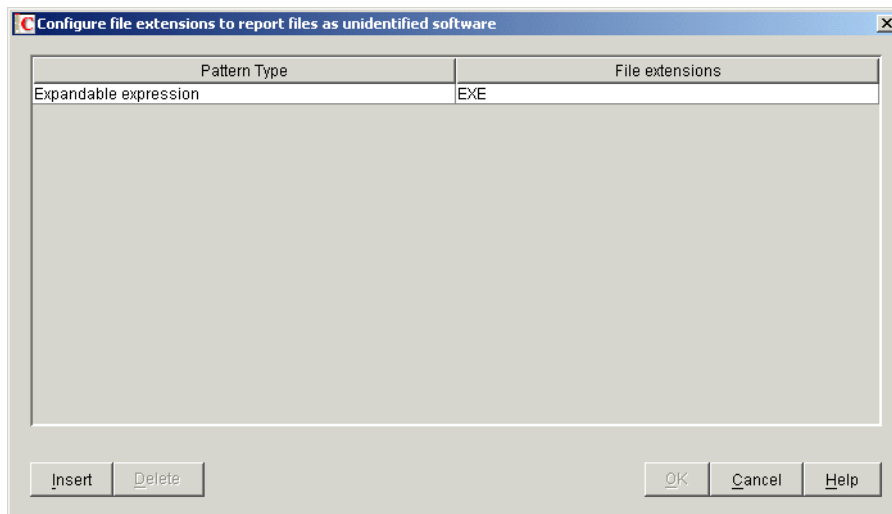
76.3.13 Report Files with These File Extensions As Unidentified Software

The “Report Files with These File Extensions As Unidentified Software” rule allows you to configure file extension of files that must be reported as unidentified software.

To configure the rule:

- 1 In the Software Configuration property page, click the *Edit Table* option of *Report Files with These File Extensions As Unidentified Software*.

The “Configure File Extensions to Report Files as Unidentified Software” table is displayed.



- 2 Click *Insert* to add a new row.
- 3 In the *Pattern Type* drop-down list, select *Expandable Expression* or *Regular Expression*.
- 4 Specify a file extension.
- 5 Click *OK*.

For example, if you want the Inventory scanner to report the software with the “.exe” extension as Unidentified software, configure the following settings in the table:

Pattern Type = Expandable Expression

File Extensions = exe

IMPORTANT: The table might contain **inherited rules**. You can edit or delete these rules only in the software dictionary of the inventory server configured in the Dictionary Update policy. These

rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

To delete an entry from the table, select the entry and click *Delete*. You can delete only the non-inherited entries.

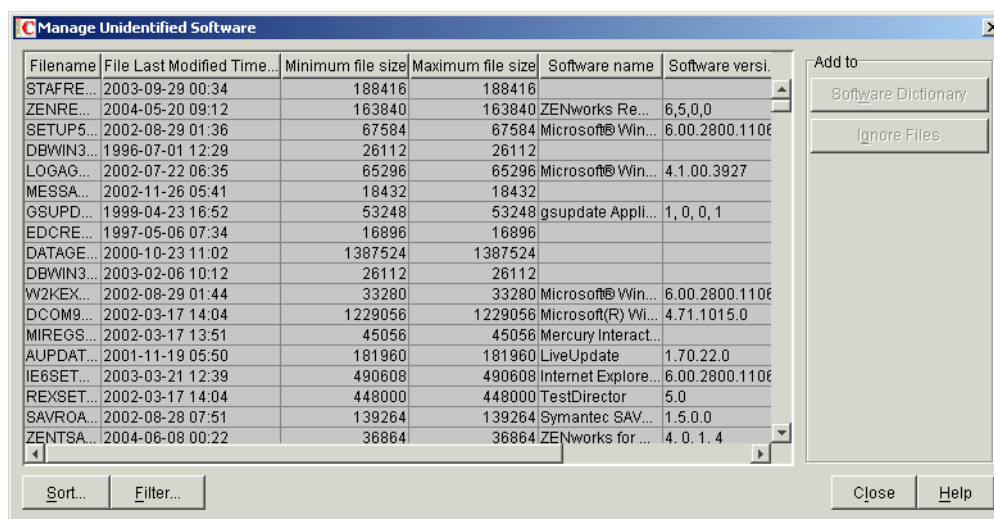
76.3.14 Manage Unidentified Software

The “Manage Unidentified Software” rule allows you to include or exclude the **unidentified software** from the inventory scan.

To configure this rule:

- 1 In the Software Configuration property page, click the *Edit Table* option of *Manage Unidentified Software*.

The Manage Unidentified Software table is displayed.



IMPORTANT: The table might contain **inherited rules**. You can edit or delete these rules only in the software dictionary of the inventory server configured in the Dictionary Update policy. These rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

- 2 In the Manage Unidentified Software table, you can perform the following operations:
 - “Including Unidentified Software in a Scan” on page 1054
 - “Excluding Unidentified Software from the Scan” on page 1054
 - Section 76.3.26, “Sorting Entries in the Table,” on page 1076
 - Section 76.3.27, “Filtering Entries in the Table,” on page 1076
 - Section 76.3.28, “Refreshing Entries in the Table,” on page 1077
- 3 Click *OK*.

Including Unidentified Software in a Scan

If you want unidentified software to be reported as a known software in subsequent scans, do the following:

- 1 Select the software entry in the Manage Unidentified Software table.
- 2 Click *Software Dictionary* located in the *Add To* pane.

The entry is automatically added to the **Software Dictionary** table.

Excluding Unidentified Software from the Scan

If you want unidentified software not to be reported in subsequent scans, do the following:

- 1 Select the software entry in the Manage Unidentified Software table.
- 2 Click *Ignore Files* located in the *Add To* pane.

The entry is automatically added to the table in **Software Scanning Filters - Files**.

76.3.15 Report Multiple Software Versions

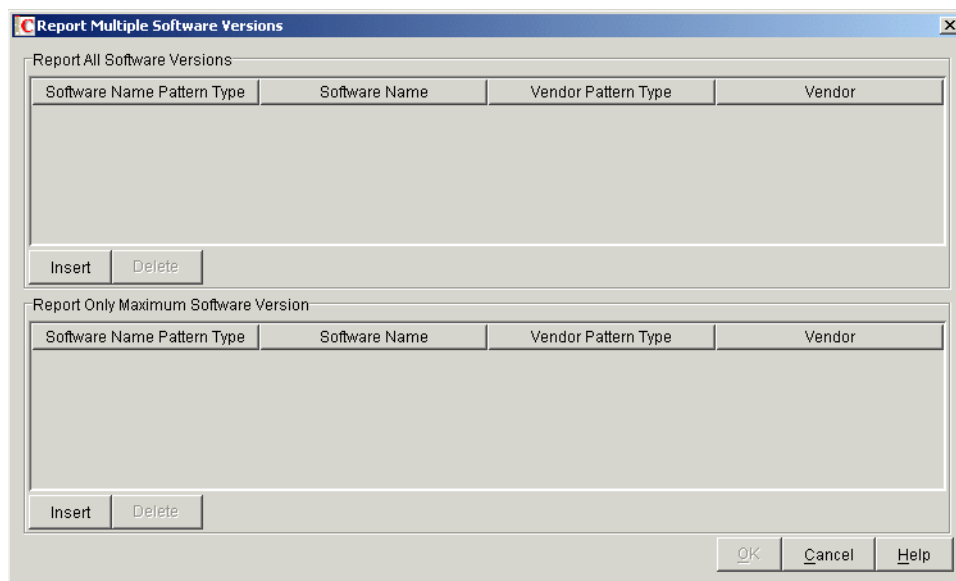
The “Report Multiple Software Versions” rule allows you to specify the software for which the Inventory scanner must report multiple versions installed on the inventoried workstation.

By default, the Inventory scanner scans for the highest version of the software installed on the inventoried workstation.

To configure this rule:

- 1 In the Software Configuration property page, click the *Edit Table* option of *Report Multiple Software Versions*.

The Report Multiple Software Versions dialog box is displayed.



- 2 If you want the Inventory scanner to report all versions of the software installed on the inventoried workstations, configure a rule in the Report All Software Versions table.

- 2a** In the Report All Software Versions table, click *Insert* to add a new row.
- 2b** In the *Software Name Pattern Type* drop-down list, select *Expandable Expression* or *Regular Expression*.
- 2c** Specify a software name.
- 2d** (Optional) In the *Vendor Pattern Type* drop-down list, select *Expandable Expression* or *Regular Expression*.
- 2e** (Optional) Specify a vendor name.

For example, if you want the Inventory scanner to report all versions of the Adobe Acrobat Reader installed on the inventoried workstation, configure the following settings in the table:

Software Name Pattern Type = Expandable Expression
Software Name = Acrobat* Reader*
Vendor Pattern Type = Expandable Expression
Vendor Name = Adobe*

If the inventoried workstation has Acrobat Reader versions 5.0 and 6.0 installed, the Inventory scanner reports both versions of Acrobat Reader (5.0 and 6.0).

IMPORTANT: The table might contain **inherited rules**. You can edit or delete these rules only in the software dictionary of the inventory server configured in the Dictionary Update policy. These rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

To delete an entry from the table, select the entry and click *Delete*. You can delete only the non-inherited entries.

- 3** If you want the Inventory scanner to report only the highest version of the software installed on the inventoried workstations, configure a rule in the Report Only Maximum Software Version table.

- 3a** In the Report Only Maximum Software Version table, click *Insert* to add a new row.
- 3b** In the *Software Name Pattern Type* drop-down list, select *Expandable Expression* or *Regular Expression*.
- 3c** Specify a software name.
- 3d** (Optional) In the *Vendor Pattern Type* drop-down list, select *Expandable Expression* or *Regular Expression*.
- 3e** (Optional) Specify a vendor name.

For example, if you want the Inventory scanner to report only the highest version of the Adobe Acrobat Reader installed on the inventoried workstation, configure the following settings in the table:

Software Name Pattern Type = Expandable Expression
Software Name = Acrobat* Reader*
Vendor Pattern Type = Expandable Expression
Vendor Name= Adobe*

If the inventoried workstation has Adobe Acrobat Reader versions 4.0 and 5.0 installed, then the Inventory scanner reports only Adobe Acrobat Reader 5.0.

IMPORTANT: The table might contain **inherited rules**. You can edit or delete these rules only in the software dictionary of the inventory server configured in the Dictionary Update policy. These rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

To delete an entry from the table, select the entry and click *Delete*. You can delete only the non-inherited entries.

4 Click *OK*.

By default, the scanner reports only the highest version of the software installed. If a rule in Report All Software Versions conflicts with a rule in Report Only Maximum Software Version, then the rule in Report Only Maximum Software Version overrides the rule of Report All Software Versions.

For example, if you want the Inventory scanner to report all versions of Microsoft software except for Microsoft Office, and also report only the highest version of Microsoft Office installed, configure the following filters as shown below:

- **Report All Software Versions:** Configure the following settings:

Software Name Pattern Type = Expandable Expression

Software Name = *

Vendor Pattern Type = Expandable Expression

Vendor Name= Microsoft*

- **Report Only Maximum Version:** Configure the following settings:

Software Name Pattern Type = Expandable Expression

Software Name = *office*

Vendor Pattern Type = Expandable Expression

Vendor Name= Microsoft*

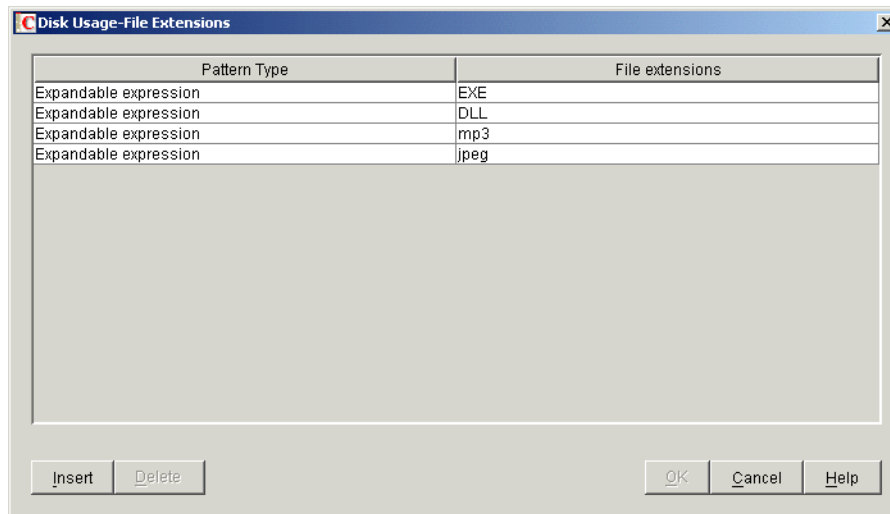
76.3.16 Report Disk Space Used by File Extensions

The “Report Disk Space Used by File Extensions” rule allows you to specify the file extension of the files whose total disk usage you want to scan.

To configure this rule:

- 1** In the Software Configuration property page, click the *Edit Table* option of *Report Disk Space Used by File Extensions*.

The Disk Usage - File Extensions table is displayed.



- 2 Click *Insert* to add a new row.
- 3 In the *Pattern Type* drop-down list, select *Expandable Expression* or *Regular Expression*.
- 4 Specify a file extension.
- 5 Click *OK*.

For example, if you want the Inventory scanner to scan for disk usage of all files with extension “.pif,” configure the following settings in the Disk Usage - File Extensions table:

Pattern Type = Expandable Expression
File Extension = pif

The Inventory scanner scans and stores only the total disk usage for all files with extension “.pif” in the Inventory database.

IMPORTANT: The table might contain **inherited rules**. You can edit or delete these rules only in the software dictionary of the inventory server configured in the Dictionary Update policy. These rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

To delete an entry from the Disk Usage - File Extensions table, select the entry and click *Delete*. You can delete only the non-inherited entries.

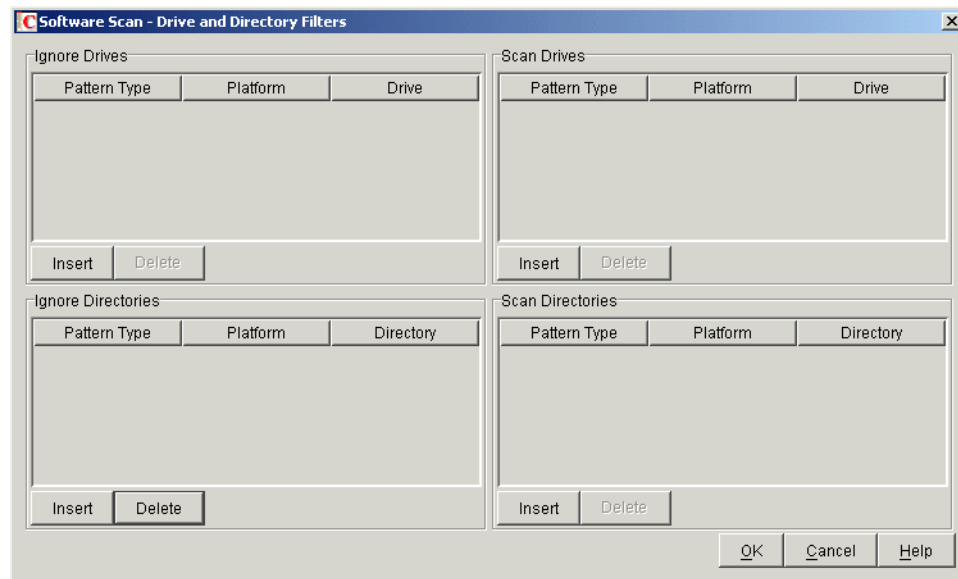
76.3.17 Software Scanning Filters - Drives and Directories

The “Drives and Directories” filter the allows you to control the scanning for software files located in specified drives and directories.

To configure this filter:

- 1 In the Filters property page, click the *Edit Table* option of *Drives and Directories* located in the *Software Scanning Filters* pane.

The Software Scan - Drive and Directory Filters dialog box is displayed.



2 Configure the following filters:

- “Ignore Drives” on page 1059
- “Scan Drives” on page 1059
- “Ignore Directories” on page 1060
- “Scan Directories” on page 1061

By default, the Inventory scanner scans all directories on the inventoried workstations. If you have configured a rule that ignores all directories during a scan by using the **Ignore Directories** filter, but now want to include a specific directory in a scan, you can identify the specific directory using the **Scan Directories** filter. The settings of the Scan Directories filter overrides the settings of the Ignore Directories and Ignore Drives filters.

For example, if you want the Inventory scanner to ignore all files and directories in C: except for the c:\program files directory on Windows inventoried workstations, configure the following filters as shown below:

- **Ignore Drives:** Configure the following settings:
Pattern Type = System Expandable Expression
Platform = Windows
Drive = C
- **Scan Directories:** Configure the following settings:
Pattern Type = System Expandable Expression
Platform = Windows
Drive = c:\program files

3 Click *OK*.

Ignore Drives

The “Ignore Drives” filter allows you to specify the drives that should not be scanned for on the inventoried workstations.

By default, the Inventory scanner scans all drives.

To configure this filter:

- 1 In the Ignore Drives table, click *Insert* to add a new row.
- 2 In the *Pattern Type* drop-down list, select *System Expandable Expression*, *Expandable Expression*, or *Regular Expression*.
- 3 (Conditional) If you select *System Expandable Expression* as the pattern type, then select *NetWare* or *Windows* in the *Platform* drop-down list, depending on the operating system of the inventoried workstations.

IMPORTANT: If you select *Expandable Expression* or *Regular Expression* as the pattern type, the corresponding value in the *Platform* column automatically changes to “Any.” You cannot change the value.

- 4 Specify a drive name.

For example, if you want the Inventory scanner not to scan the files in C drive on all the Windows inventoried workstations, configure the following settings in the Ignore Drives table:

Pattern Type = System Expandable Expression

Platform = Windows

Drive = C

The Inventory scanner does not scan the files in the C drive.

IMPORTANT: The table might contain **inherited rules**. You can edit or delete these rules only in the software dictionary of the inventory server configured in the Dictionary Update policy. These rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

To delete an entry from the Ignore Drives table, select the entry and click *Delete*. You can delete only the non-inherited entries.

Scan Drives

The “Scan Drives” filter allows you to specify the drives that should be scanned for at the inventoried workstations.

To configure this filter:

- 1 In the Scan Drives table, click *Insert* to add a new row.
- 2 In the *Pattern Type* drop-down list, select *System Expandable Expression*, *Expandable Expression*, or *Regular Expression*.
- 3 (Conditional) If you select *System Expandable Expression* as the pattern type, then select *NetWare* or *Windows* in the *Platform* drop-down list, depending on the operating system of the inventoried workstations.

IMPORTANT: If you select *Expandable Expression* or *Regular Expression* as the pattern type, the corresponding value in the *Platform* column automatically changes to “Any.” You cannot change the value.

4 Specify a drive name.

For example, if you want the Inventory scanner to scan for files in the C drive on all the Windows inventoried workstations, configure the following settings in the Scan Drives table:

Pattern Type = System Expandable Expression

Platform = Windows

Drive = C

You must also configure the following settings in the Ignore Drives table:

Pattern Type = System Expandable Expression

Platform = Windows

Drive = *

The Inventory scanner scans only the files in the C drive for the software information.

IMPORTANT: The table might contain **inherited rules**. You can edit or delete these rules only in the software dictionary of the inventory server configured in the Dictionary Update policy. These rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

To delete an entry from the Scan Drives table, select the entry and click *Delete*. You can delete only the non-inherited entries.

IMPORTANT: By default, the Inventory scanner scans all drives on the inventoried workstations. If you have configured all drives to be ignored during a scan by using the Ignore Drives filter, but now want to include a specific drive in a scan, you can identify the specific drive using the Scan Drives filter. The settings of the Scan Drives filter override the settings of the Ignore Drives filter.

Ignore Directories

The “Ignore Directories” filter allows you to specify the directories that should not be scanned for at the inventoried workstations.

By default, the Inventory scanner scans all directories.

To configure this filter:

- 1 In the Ignore Directories table, click *Insert* to add a new row.
- 2 In the *Pattern Type* drop-down list, select *System Expandable Expression*, *Expandable Expression*, or *Regular Expression*.
- 3 (Conditional) If you select *System Expandable Expression* as the pattern type, then select *NetWare* or *Windows* in the *Platform* drop-down list, depending on the operating system of the inventoried workstations.

IMPORTANT: If you select *Expandable Expression* or *Regular Expression* as the pattern type, the corresponding value in the *Platform* column automatically changes to “Any.” You cannot change the value.

4 Specify a directory name.

For example, if you do not want the Inventory scanner to scan the files in the `c:\program files` directory on all the Windows inventoried workstations, configure the following settings in the Ignore Directories table:

Pattern Type = System Expandable Expression

Platform = Windows

Directory= `C:\Program Files`

The Inventory scanner does not scan for the files in `c:\program files`.

IMPORTANT: The table might contain **inherited rules**. You can edit or delete these rules only in the software dictionary of the inventory server configured in the Dictionary Update policy. These rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

To delete an entry from the Ignore Directories table, select the entry and click *Delete*. You can delete only the non-inherited entries.

Scan Directories

The “Scan Directories” filter allows you to specify the directories that should be scanned for at the inventoried workstations.

To configure this filter:

- 1** In the Scan Directories table, click *Insert* to add a new row.
- 2** In the *Pattern Type* drop-down list, select *System Expandable Expression*, *Expandable Expression*, or *Regular Expression*.
- 3** (Conditional) If you select *System Expandable Expression* as the pattern type, then select *NetWare* or *Windows* in the *Platform* drop-down list, depending on the operating system of the inventoried workstations.

IMPORTANT: If you select *Expandable Expression* or *Regular Expression* as the pattern type, the corresponding value in the *Platform* column automatically changes to “Any.” You cannot change the value.

4 Specify a directory name.

For example, if you want the Inventory scanner to scan for files in the `c:\program files` directory on all the Windows inventoried workstations, configure the following settings in the Scan Directories table:

Pattern Type = System Expandable Expression

Platform = Windows

Directory= `C:\Program Files`

You must also configure the following settings in the Ignore Directories table:

Pattern Type = System Expandable Expression

Platform = Windows

Directory = *

The Inventory scanner scans only the files in `c:\program files` for software information.

IMPORTANT: The table might contain **inherited rules**. You can edit or delete these rules only in the software dictionary of the inventory server configured in the Dictionary Update policy. These rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

To delete an entry from the Scan Directories table, select the entry and click *Delete*. You can delete only the non-inherited entries.

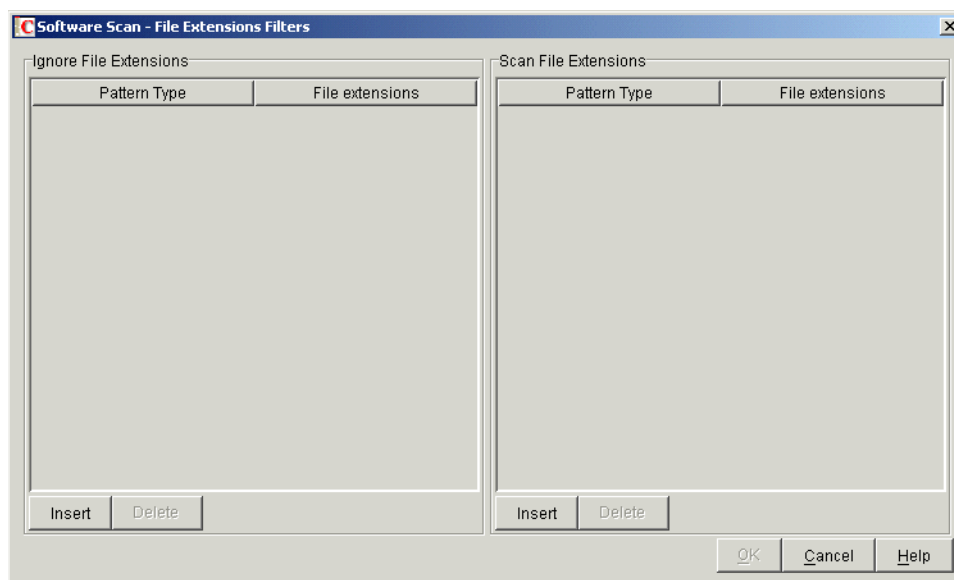
76.3.18 Software Scanning Filters - File Extensions

The “File Extensions” filter allows you to control scanning for software files with a specified extension.

To configure this filter:

- 1 In the Filters property page, click the *Edit Table* option of *File Extensions* located in the *Software Scanning Filters* pane.

The Software Scan - File Extensions Filters dialog box is displayed.



- 2 Configure the following filters:
 - “Ignore File Extensions” on page 1063
 - “Scan File Extensions” on page 1063
- 3 Click *OK*.

Ignore File Extensions

The “Ignore File Extensions” filter allows you to specify the file extensions that should not be scanned for at the inventoried workstations.

To configure this filter:

- 1 In the Ignore File Extensions table, click *Insert* to add a new row.
- 2 In the *Pattern Type* drop-down list, select *Expandable Expression* or *Regular Expression*.
- 3 Specify a file extension.

For example, if you do not want the Inventory scanner to scan for files whose extension begin with “.ex”, configure the following settings in the Ignore File Extensions table:

Pattern Type = Expandable Expression

File Extension = ex*

The Inventory scanner does not scan for the files whose extension begin with “.ex.” For example, .ex1, .ex2, .exe, and exec.

IMPORTANT: The table might contain **inherited rules**. You can edit or delete these rules only in the software dictionary of the inventory server configured in the Dictionary Update policy. These rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

To delete an entry from the Ignore File Extensions table, select the entry and click *Delete*. You can delete only the non-inherited entries.

Scan File Extensions

The “Scan File Extensions” filter allows you to specify the file extensions that should be scanned for at the inventoried workstations.

If you have excluded file extensions from scanning by using the Ignore File Extensions filter, but now want to include a specific file extension in the scan, you can identify the specific file extension using the Scan File Extensions filter. The settings of the Scan File Extensions filter override the settings of the Ignore File Extensions filter.

To configure this filter:

- 1 In the Scan File Extensions table, click *Insert* to add a new row.
- 2 In the *Pattern Type* drop-down list, select *Expandable Expression* or *Regular Expression*.
- 3 Specify a file extension.

For example, if you want the Inventory scanner to scan for all files with a “.exe” extension, configure the following settings in the Scan File Extension table:

Pattern Type = Regular Expression

File Extension = [exe|EXE]

The Inventory scanner scans and stores only the files with a “.exe” extension in the Inventory database.

IMPORTANT: The table might contain **inherited rules**. You can edit or delete these rules only in the software dictionary of the inventory server configured in the Dictionary Update policy. These rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

To delete an entry from the Scan File Extensions table, select the entry and click *Delete*. You can delete only the non-inherited entries.

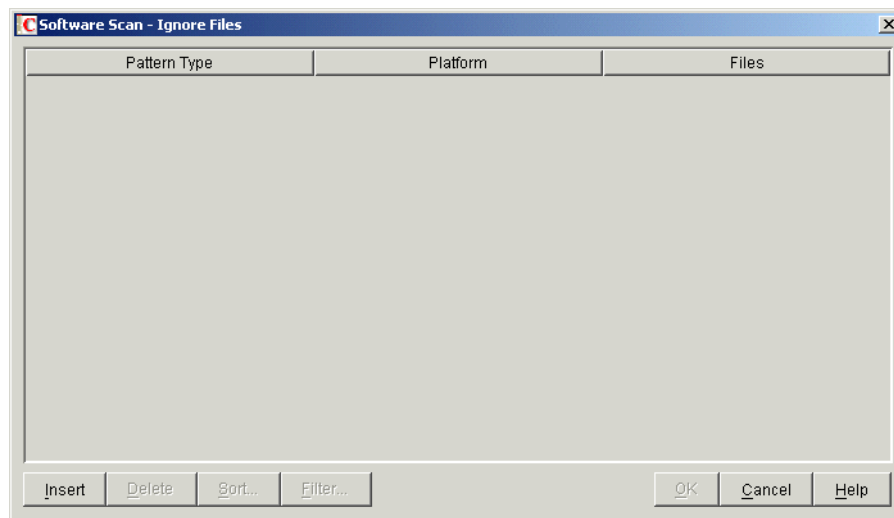
76.3.19 Software Scanning Filters - Files

The “Files” filter allows you to control scanning for specified files.

To configure this filter:

- 1 In the Filters property page, click the *Edit Table* option of *Files* located in the *Software Scanning Filters* pane.

The Software Scan - Ignore Files table is displayed.



- 2 Click *Insert* to add a new row.
- 3 In the *Pattern Type* drop-down list, select *System Expandable Expression*, *Expandable Expression*, or *Regular Expression*.
- 4 (Conditional) If you select *System Expandable Expression* as the pattern type, then select *NetWare* or *Windows* in the *Platform* drop-down list depending on the operating system of the inventoried workstations.

IMPORTANT: If you select *Expandable Expression* or *Regular Expression* as the pattern type, the corresponding value in the *Platform* column is automatically changed to “Any.” You cannot change the value.

- 5 Specify a filename.
- 6 Click *OK*.

For example, if you want the Inventory scanner to scan `notepad.exe` on all the Windows inventoried workstations, configure the following settings:

Platform = Windows

Pattern Type = System Expandable Expression

Files = notepad.exe

This table also displays files that are added from the Manage Unidentified Software table.

IMPORTANT: The table might contain **inherited rules**. You can edit or delete these rules only in the software dictionary of the inventory server configured in the Dictionary Update policy. These rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

You can also perform the following operations in the Software Scan - File Filters table:

- Deleting only the non-inherited entries.
- **Sorting Entries in the Table.**
- **Filtering Entries in the Table.**
- **Refreshing Entries in the Table.**

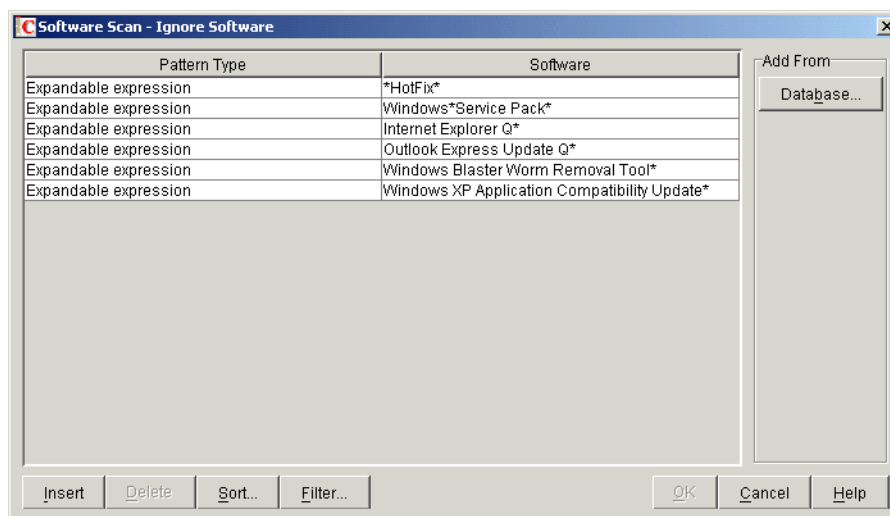
76.3.20 Software Scanning Filters - Software

The “Software” filter allows you to configure software to be excluded during the Inventory scan.

To configure this filter:

- 1 In the Filters property page, click the *Edit Table* option of *Software* located in the *Software Scanning Filters* pane.

The Software Scan - Ignore Software table is displayed.



- 2 You can add entries to the Ignore Software table either manually or automatically.

Manually Adding Entries to the Table

1. Click *Insert* to add a new row.
2. In the *Pattern Type* drop-down list, select *Expandable Expression* or *Regular Expression*.

3. Specify a software name.
4. Click *OK*.

For example, if you do not want the Inventory scanner to scan for the Adobe products, configure the following settings:

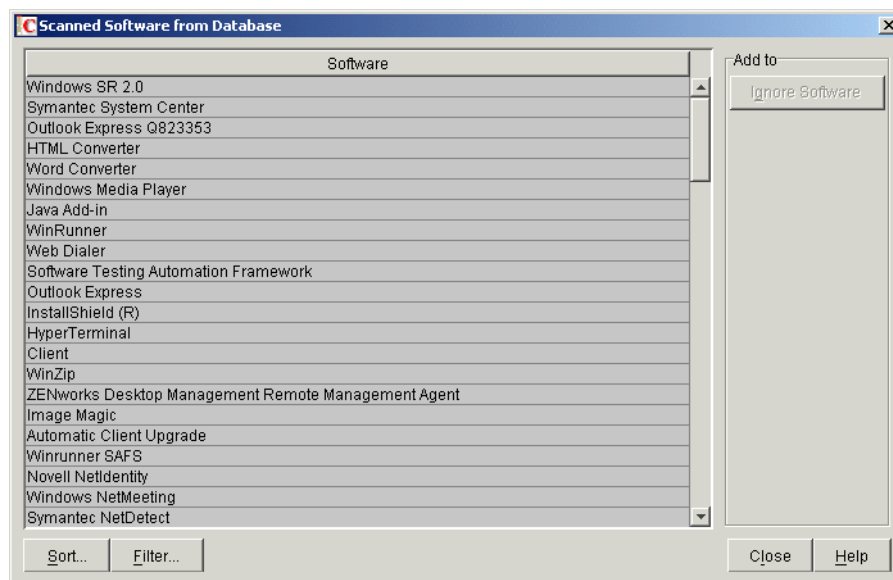
Pattern Type= Expandable Expression

Software = Adobe*

The Inventory scanner does not report the software that has names beginning with “Adobe.”

Automatically Adding Entries to the Table

1. Click *Database* located in the *Add From* pane.
The Scanned Software from Database dialog box is displayed.



2. Select the software that you want to add to the Ignore Software table.
3. Click the *Ignore Software* button located in the Add to pane.
4. Click *Close*.

IMPORTANT: The table might contain **inherited rules**. You can edit or delete these rules only in the software dictionary of the inventory server configured in the Dictionary Update policy. These rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

You can also perform the following operations in the Software Scan - Ignore Software table:

- Deleting only the non-inherited entries.
- **Sorting Entries in the Table.**
- **Filtering Entries in the Table.**
- **Refreshing Entries in the Table.**

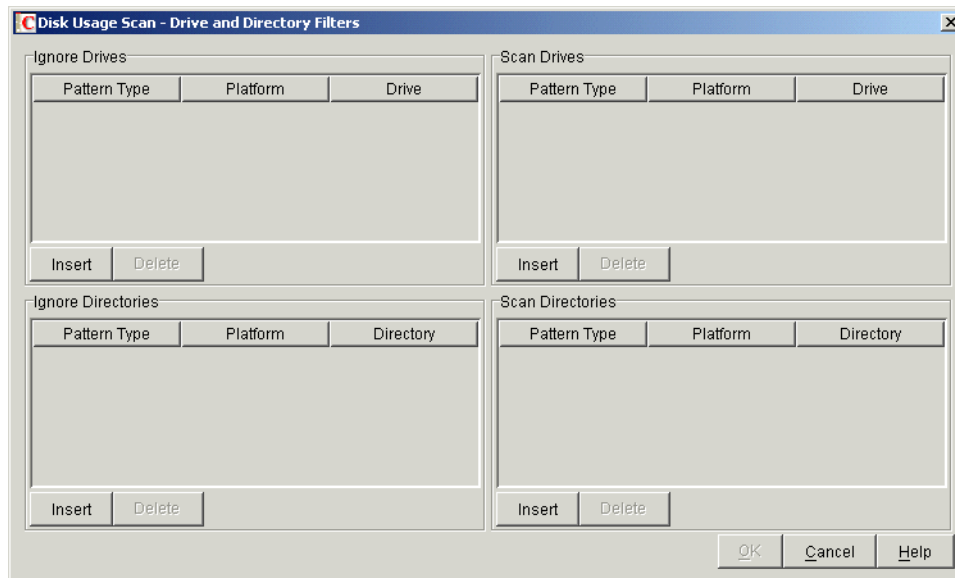
76.3.21 Disk Usage Scanning Filters - Drives and Directories

The “Drives and Directories” filter allows you to configure drives and directories to be included or excluded during the Inventory disk usage scanning.

To configure this filter:

- 1 In the Filters property page, click the *Edit Table* option of *Drives and Directories* located in the *Disk Usage Scanning Filters* pane.

The Disk Usage Scan - Drive and Directory Filters dialog box is displayed.



- 2 Configure the following filters:

- “Ignore Drives” on page 1068
- “Scan Drives” on page 1068
- “Ignore Directories” on page 1069
- “Scan Directories” on page 1070

By default, the Inventory scanner scans the disk usage of all directories on the inventoried workstations. If you have configured all directories to be ignored during a disk usage scan using the Ignore Directories filter, but now want to include a specific directory, identify the specific directory in the Scan Directories filter. The settings of the Scan Directories filter override the settings of the Ignore Directories and Ignore Drives filters.

For example, if you want the Inventory scanner to ignore the disk usage of all files and directories in C: except for the c:\program files directory on Windows inventoried workstations, configure the following filters as shown below:

- **Ignore Drives:** Configure the following settings:
Pattern Type = System Expandable Expression
Platform = Windows
Drive = C
- **Scan Directories:** Configure the following settings:

Pattern Type = System Expandable Expression

Platform = Windows

Drive = c:\program files

3 Click *OK*.

Ignore Drives

The “Ignore Drives” filter allows you to specify the drives that should not be scanned for disk usage at the inventoried workstations.

By default, the Inventory scanner scans all drives.

To configure the “Ignore Drives” filter:

- 1 In the Ignore Drives table, click *Insert* to add a new row.
- 2 In the *Pattern Type* drop-down list, select *System Expandable Expression*, *Expandable Expression*, or *Regular Expression*.
- 3 (Conditional) If you select *System Expandable Expression* as the pattern type, then select *NetWare* or *Windows* in the *Platform* drop-down list depending on the operating system of the inventoried workstations.

IMPORTANT: If you select *Expandable Expression* or *Regular Expression* as the pattern type, the corresponding value in the *Platform* column automatically changes to “Any.” You cannot change the value.

- 4 Specify a drive name.

For example, if you want the Inventory scanner not to scan for the disk usage of C drive on all the Windows* inventoried workstations, configure the following settings in the Ignore Drives table:

Pattern Type = System Expandable Expression

Platform = Windows

Drive = C

The Inventory scanner does not scan the disk usage of files on the C drive.

IMPORTANT: The table might contain **inherited rules**. You can edit or delete these rules only in the software dictionary of the inventory server configured in the Dictionary Update policy. These rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

To delete an entry from the Ignore Drives table, select the entry and click *Delete*. You can delete only the non-inherited entries.

Scan Drives

The “Scan Drives” filter allows you to specify the drives whose disk usage should be scanned for at the inventoried workstations.

To configure the “Scan Drives” filter:

- 1 In the Scan Drives table, click *Insert* to add a new row.

- 2 In the *Pattern Type* drop-down list, select *System Expandable Expression*, *Expandable Expression*, or *Regular Expression*.
- 3 (Conditional) If you select *System Expandable Expression* as the pattern type, then select *NetWare* or *Windows* in the *Platform* drop-down list depending on the operating system of the inventoried workstations.

IMPORTANT: If you select *Expandable Expression* or *Regular Expression* as the pattern type, the corresponding value in the *Platform* column automatically changes to “Any.” You cannot change the value.

- 4 Specify a drive name.

For example, if you want the Inventory scanner to scan for the disk usage of C drive on all the Windows inventoried workstations, configure the following settings in the Scan Drives table:

Pattern Type = System Expandable Expression
Platform = Windows
Drive = C

You must also configure the following settings in the Ignore Drives table:

Pattern Type = System Expandable Expression
Platform = Windows
Drive = *

The Inventory scanner scans and stores the disk usage of the files in the C drive into the Inventory database.

IMPORTANT: The table might contain **inherited rules**. You can edit or delete these rules only in the software dictionary of the inventory server configured in the Dictionary Update policy. These rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

To delete an entry from the Scan Drives table, select the entry and click *Delete*. You can delete only the non-inherited entries.

IMPORTANT: By default, the Inventory scanner scans the disk usage of all drives on the inventoried workstations. If you have configured all drives to be ignored during a disk usage scan using the Ignore Drives filter, but now want to include a specific drive in the scan, identify the specific drive in the Scan Drives filter. The settings of the Scan Drives filter override the settings of the Ignore Drives filter.

Ignore Directories

The “Ignore Directories” filter allows you to specify the directories whose disk usage should not be scanned for at the inventoried workstations.

By default, the Inventory scanner scans all directories.

To configure the “Ignore Directories” filter:

- 1 In the Ignore Directories table, click *Insert* to add a new row.

- 2 In the *Pattern Type* drop-down list, select *System Expandable Expression*, *Expandable Expression*, or *Regular Expression*.
- 3 (Conditional) If you select *System Expandable Expression* as the pattern type, then select *NetWare* or *Windows* in the *Platform* drop-down list, depending on the operating system of the inventoried workstations.

IMPORTANT: If you select *Expandable Expression* or *Regular Expression* as the pattern type, the corresponding value in the *Platform* column automatically changes to “Any.” You cannot change the value.

- 4 Specify a directory name.

For example, if you want the Inventory scanner not to scan for the disk usage of the `c:\program files` directory on all the Windows inventoried workstations, configure the following settings in the Ignore Directories table:

Pattern Type = System Expandable Expression

Platform = Windows

Directory= `c:\program files`

The Inventory scanner does not scan for the disk usage of `c:\program files`.

IMPORTANT: The table might contain **inherited rules**. You can edit or delete these rules only in the software dictionary of the inventory server configured in the Dictionary Update policy. These rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

To delete an entry from the Ignore Directories table, select the entry and click *Delete*. You can delete only the non-inherited entries.

Scan Directories

The “Scan Directories” filter allows you to specify the directories whose disk usage should be scanned for at the inventoried workstations.

To configure the “Scan Directories” filter:

- 1 In the Scan Directories table, click *Insert* to add a new row.
- 2 In the *Pattern Type* drop-down list, select *System Expandable Expression*, *Expandable Expression*, or *Regular Expression*.
- 3 (Conditional) If you select *System Expandable Expression* as the pattern type, then select *NetWare* or *Windows* in the *Platform* drop-down list depending on the operating system of the inventoried workstations.

IMPORTANT: If you select *Expandable Expression* or *Regular Expression* as the pattern type, the corresponding value in the *Platform* column automatically changes to “Any.” You cannot change the value.

- 4 Specify a directory name.

For example, if you want the Inventory scanner to scan for disk usage of the `c:\program files` directory on all the Windows inventoried workstations, configure the following settings in the Scan Directories table:

Pattern Type = System Expandable Expression

Platform = Windows

Directory = c:\program files

You must also configure the following settings in the Ignore Directories table:

Pattern Type = System Expandable Expression

Platform = Windows

Directory = *

The Inventory scanner scans and stores only disk usage of files in c:\program files into the Inventory database.

IMPORTANT: The table might contain **inherited rules**. You can edit or delete these rules only in the software dictionary of the inventory server configured in the Dictionary Update policy. These rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

To delete an entry from the Scan Directories table, select the entry and click *Delete*. You can delete only the non-inherited entries.

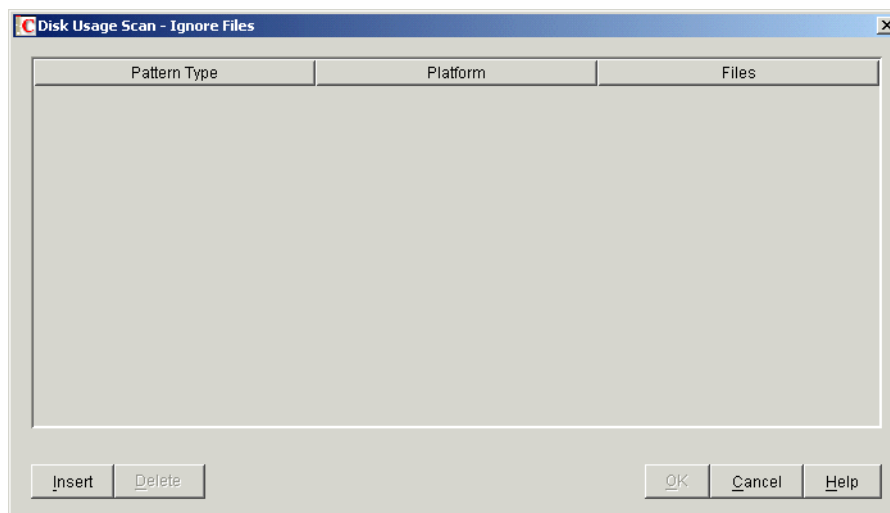
76.3.22 Disk Usage Scanning Filters - Files

The “Files” filter allows you to configure files to be excluded during the Inventory disk usage scanning.

To configure this filter:

- 1 In the Filters property page, click the *Edit Table* option of *Files* located in the *Disk Usage Scanning Filters* pane.

The Disk Usage Scan - Ignore Files dialog box is displayed.



- 2 Click *Insert* to add a new row.

- 3 In the *Pattern Type* drop-down list, select *System Expandable Expression*, *Expandable Expression*, or *Regular Expression*.
- 4 (Conditional) If you select *System Expandable Expression* as the pattern type, then select *NetWare* or *Windows* in the *Platform* drop-down list depending on the operating system of the inventoried serves.

IMPORTANT: If you select *Expandable Expression* or *Regular Expression* as the pattern type, the corresponding value in the *Platform* column automatically changes to “Any.” You cannot change the value.

- 5 Specify a file.
- 6 Click *OK*.

For example, if you want the Inventory scanner to scan for disk usage of all files with extension “.exe” except `msoffice.exe`, configure the following rules as shown below:

- **Disk Usage Scan - Ignore Files:** Configure the following settings:

Pattern Type = Expandable Expression
Files = `msoffice.exe`

- **Report Disk Space used by file extensions:** Configure the following settings:

Pattern Type = Expandable Expression
Files = `exe`

IMPORTANT: The table might contain **inherited rules**. You can edit or delete these rules only in the software dictionary of the inventory server configured in the Dictionary Update policy. These rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

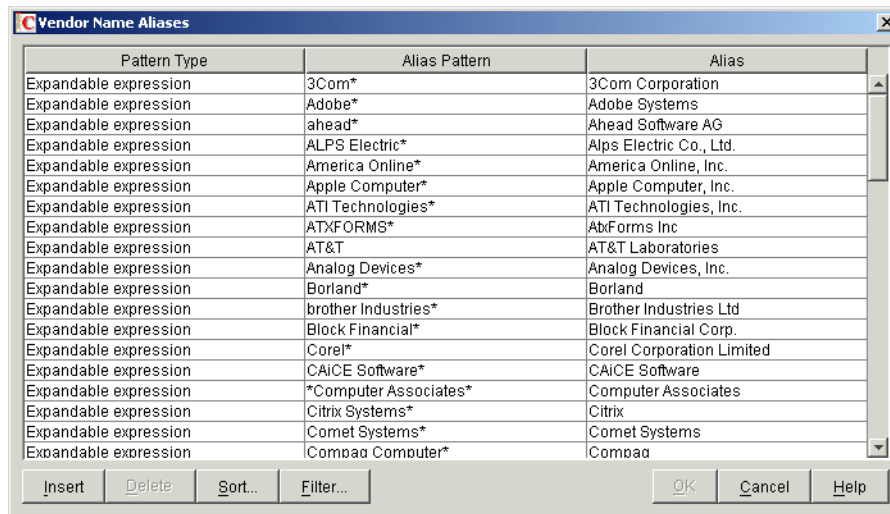
To delete an entry from the table, select the entry and click *Delete*. You can delete only the non-inherited entries.

76.3.23 Vendor Name Aliases

The “Vendor Name Aliases” rule allows you to configure aliases for vendor names.

- 1 In the Aliases property page, click the *Edit Table* option of *Vendor Name Aliases* located in the *Specify Aliases* pane.

The Vendor Name Aliases table is displayed.



Pattern Type	Alias Pattern	Alias
Expandable expression	3Com*	3Com Corporation
Expandable expression	Adobe*	Adobe Systems
Expandable expression	ahead*	Ahead Software AG
Expandable expression	ALPS Electric*	Alps Electric Co., Ltd.
Expandable expression	America Online*	America Online, Inc.
Expandable expression	Apple Computer*	Apple Computer, Inc.
Expandable expression	ATI Technologies*	ATI Technologies, Inc.
Expandable expression	ATXFORMS*	AbForms Inc
Expandable expression	AT&T	AT&T Laboratories
Expandable expression	Analog Devices*	Analog Devices, Inc.
Expandable expression	Borland*	Borland
Expandable expression	brother Industries*	Brother Industries Ltd
Expandable expression	Block Financial*	Block Financial Corp.
Expandable expression	Corel*	Corel Corporation Limited
Expandable expression	CAICE Software*	CAICE Software
Expandable expression	*Computer Associates*	Computer Associates
Expandable expression	Citrix Systems*	Citrix
Expandable expression	Comet Systems*	Comet Systems
Expandable expression	Compaq Computer*	Compaq

- 2 Click *Insert* to add a new row.
- 3 In the *Pattern Type* drop-down list, select *Expandable Expression* or *Regular Expression*.
- 4 Specify an alias pattern.
- 5 Specify an alias.
- 6 Click *OK*.

For example, if you want the Inventory scanner to report all instances of the vendor name beginning with “Microsoft” as “Microsoft Corporation” in the Inventory database, configure the following settings:

Pattern Type = Expandable Expression

Alias Pattern = Microsoft*

Alias = Microsoft Corporation

If the Inventory scanner reports Microsoft, Microsoft Inc., or Microsoft Inc. Corporation vendor names during the scan, then the name of the vendor beginning with “Microsoft” is stored as “Microsoft Corporation” in the Inventory database.

IMPORTANT: The table might contain **inherited rules**. You can edit or delete these rules only in the software dictionary of the inventory server configured in the Dictionary Update policy. These rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

You can also perform the following operations in the Vendor Name Aliases table:

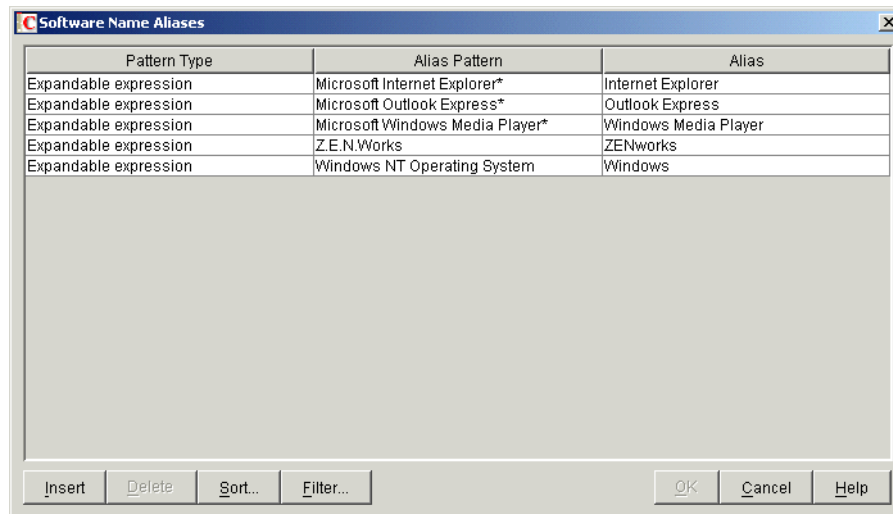
- Deleting only the non-inherited entries.
- **Sorting Entries in the Table.**
- **Filtering Entries in the Table.**
- **Refreshing Entries in the Table**

76.3.24 Software Name Aliases

The “Software Name Aliases” rule allows you to configure aliases for software names.

- 1 In the Aliases property page, click the *Edit Table* option of *Software Name Aliases* located in the *Specify Aliases* pane.

The Software Name Aliases table is displayed.



Pattern Type	Alias Pattern	Alias
Expandable expression	Microsoft Internet Explorer*	Internet Explorer
Expandable expression	Microsoft Outlook Express*	Outlook Express
Expandable expression	Microsoft Windows Media Player*	Windows Media Player
Expandable expression	Z.E.N.Works	ZENworks
Expandable expression	Windows NT Operating System	Windows

- 2 Click *Insert* to add a new row.
- 3 In the *Pattern Type* drop-down list, select *Expandable Expression* or *Regular Expression*.
- 4 Specify an alias pattern.
- 5 Specify an alias.
- 6 Click *OK*.

For example, if you want the Inventory scanner to report all instances of the product name “WinZip” as “WinZip Application” in the Inventory database, configure the following settings:

Pattern Type = Expandable Expression

Alias Pattern = WinZip

Alias = WinZip Application

If the Inventory scanner scans the WinZip, WinZip Executables, or WinZip Applications product names, then the name of the software that exactly matches “WinZip” is stored as “WinZip Application” in the Inventory database. The remaining software names are reported as scanned.

IMPORTANT: The table might contain **inherited rules**. You can edit or delete these rules only in the software dictionary of the inventory server configured in the Dictionary Update policy. These rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

You can also perform the following operations in the Software Name Aliases table:

- Deleting only the non-inherited entries.
- **Sorting Entries in the Table.**

- **Filtering Entries in the Table.**
- **Refreshing Entries in the Table.**

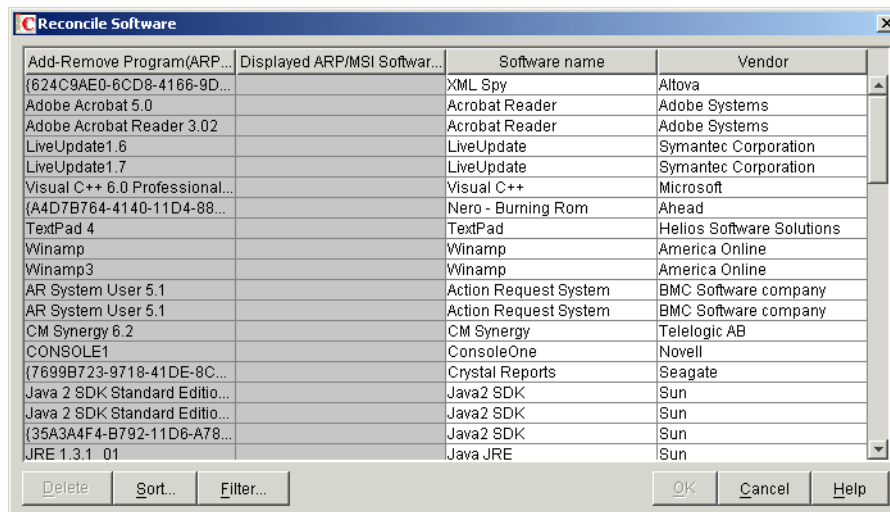
76.3.25 Reconcile Software

The “Reconcile Software” rule allows you to associate the software identified through Add/Remove Programs or the MSI, with an appropriate software and vendor identified and configured through the ZENworks software dictionary. The association might be necessary because the software entries in Add/Remove Programs or the MSI might not use the same software name and vendor as configured in the ZENworks software dictionary.

To configure the rule:

- 1 In the Aliases property page, click the *Edit Table* option of *Reconcile Software* located in the *Reconcile Software* pane.

The Reconcile Software table is displayed.



Add-Remove Program(ARP)...	Displayed ARP/MSI Softwar...	Software name	Vendor
{624C9AE0-6CD8-4166-9D...		XML Spy	Altova
Adobe Acrobat 5.0		Acrobat Reader	Adobe Systems
Adobe Acrobat Reader 3.02		Acrobat Reader	Adobe Systems
LiveUpdate1.6		LiveUpdate	Symantec Corporation
LiveUpdate1.7		LiveUpdate	Symantec Corporation
Visual C++ 6.0 Professional...		Visual C++	Microsoft
{A4D7B764-4140-11D4-88...		Nero - Burning Rom	Ahead
TextPad 4		TextPad	Helios Software Solutions
Winamp		Winamp	America Online
Winamp3		Winamp	America Online
AR System User 5.1		Action Request System	BMC Software company
AR System User 5.1		Action Request System	BMC Software company
CM Synergy 6.2		CM Synergy	Telelogic AB
CONSOLE1		ConsoleOne	Novell
{7699B723-9718-41DE-8C...		Crystal Reports	Seagate
Java 2 SDK Standard Editio...		Java2 SDK	Sun
Java 2 SDK Standard Editio...		Java2 SDK	Sun
{35A3A4F4-B792-11D6-A78...		Java2 SDK	Sun
JRE 1.3.1_01		Java JRE	Sun

By default, the Reconcile Software table displays predefined mapping of software in the Add/Remove Programs or MSI with the software configured in the software dictionary. It also displays the Add/Remove Programs or MSI software identified during the last scan for which you can configure software and vendor names. This table has the following columns:

- The Add-Remove Program (ARP) key.
You cannot edit the values of this attribute.
- The ARP /MSI name as displayed either in Add/Remove Programs or in the MSI.
The Displayed ARP/MSI Software name shows the software identified through Add/Remove Programs or the MSI and stored in the Inventory database.
You cannot edit the values of this attribute.
- The software name associated with its corresponding Add/Remove Programs or MSI name.
- The vendor name associated with its corresponding Add/Remove Programs or MSI name.

IMPORTANT: The table might contain **inherited rules**. You can edit or delete these rules only in the software dictionary of the inventory server configured in the Dictionary Update policy. These rules are displayed in dark gray color if you are accessing the software dictionary of ZENworks 7 Inventory server.

2 To reconcile software:

- Specify software and vendor names for software identified through Add/Remove Programs or the MSI but not yet been associated.
- (Optional) Change the software and vendor names for software that has already been configured in the software dictionary.

You can also perform the following operations in the Reconcile Software table:

- Deleting only the non-inherited entries.
- **Sorting Entries in the Table.**
- **Filtering Entries in the Table.**
- **Refreshing Entries in the Table.**

76.3.26 Sorting Entries in the Table

You can sort the entries in the table by one, two, or three columns.

1 Click *Sort*.

The Sort dialog box is displayed.

2 In the *Sort by* drop-down list, select the table column by which you want to sort the entries.

3 Select *Ascending* or *Descending*.

4 (Optional) To sort by either two or three columns, configure the *Then by* drop-down lists and select *Ascending* or *Descending*.

5 Click *OK*.

76.3.27 Filtering Entries in the Table

1 Click *Filter*.

The Filter dialog box is displayed.

2 In the Filter dialog box, do the following to create a query:

2a Select an attribute.

2b Select an operator. The operators displayed depend on the attribute you select in Step 2a.

2c Type a value.

2d (Optional) To create an advanced query, select one of the following logical operators and define the query:

Logical Operator	Functionality
AND	Creates a new row. The filter displays items that match the conditions in each row joined by AND.

Logical Operator	Functionality
OR	Creates a new row. The filter displays items that match the conditions in either row joined by OR.
New Row	Creates a new row to form a new query.
Delete Row	Deletes the row from the filter.
End	Closes the query expression. If you select End in a row that is followed by other rows, the subsequent rows and groups are deleted.

3 Click *OK*.

After applying the filter, the table list displays only the resulting entries. To clear the filter:

1 Click *Filter*.

The Filter dialog box is displayed.

2 Click *Clear*, then click *OK*.

76.3.28 Refreshing Entries in the Table

Use the *Refresh* option if you want to reapply the sort or filter operations. To refresh entries in the table, either click *Refresh* or press F5.

IMPORTANT: The *Refresh* button is displayed only when you apply sort or filter operations to the table.

76.3.29 Disabling File Scan

You can disable the software scanning for all software except for the following:

- Software registered in the Add/Remove Programs dialog box
- Software installed through MSI
- Software scanned by default such as Microsoft Windows, Internet Explorer, Outlook, MediaPlayer, ZENworks, Novell client, Microsoft Office and the set of Antivirus programs

To disable the file scanning:

1 In ConsoleOne, right-click the Inventory Service Object, click *Properties*.

2 Click the *Software Inventory Configuration* tab.

The Software Configuration page is displayed by default.

3 Select the *Ignore Default File-Software Mapping Rules* check box.

4 Click the *Edit Table* button of the “Report Files with These File Extensions As Unidentified Software” rule.

5 By default, the table has an entry with the EXE file extension. Delete the entry.

6 Click *OK*.

7 Click *Apply*, then click *Close*.

76.3.30 Base-Lining the Software Dictionary Deployment

When you deploy the software dictionary for the first time, the default dictionary settings are effective and the Inventory scanner reports the following information:

- Unidentified software
- Multiple instances of software installed on the same inventoried workstation
- Redundant drives and directories that do not contain software

This scan results in storing huge amount of irrelevant information in the Inventory database. It also degrades the performance of Storer and all ConsoleOne Inventory utilities such as Query and Reporting.

To avoid these problems, we recommend that you fine-tune the software dictionary according to your requirements before deploying it in your enterprise. Do the following to fine tune the software dictionary:

- 1 Deploy a small representative set of inventoried workstations in the test lab.

NOTE: This representative set should typically include all sections or departments of your enterprise that you want to collect inventory for.

- 2 Attach these inventoried workstations to a Standalone Inventory Server that is also deployed in the test lab.
- 3 In addition to defaults that are listed in the table of the **Report Files with These File Extensions As Unidentified Software** rule, you might want to scan for additional file extensions and report them as identified software. These could be extensions of application files like DLLs, etc.
- 4 Schedule the scan and wait until the inventory information is stored into the Inventory database.
- 5 Reconfigure the software dictionary based on the inventory information that is available in the database to resolve the above discussed problems. Perform the following tasks:
 - **Unidentified Software:** Based on the **Report Files with These File Extensions As Unidentified Software** settings, all the information related to the unidentified software can be viewed in the **Manage Unidentified Software** table.

The result includes the following:

- Applications that are not yet identified by the software dictionary.
- Application files that are already identified by the software dictionary.
- Application files that might be redundant such as Operating System files or DOS files.

Perform the following tasks in the Manage Unidentified Software table:

- Add the applications that are not yet identified by the software dictionary to the **Software Dictionary** table using the Software Dictionary button located in the Add To pane.
- Add the application files that are already identified by the software dictionary and application files that might be redundant to the **Software Scanning Filters - Files** table using the Ignore Files button located in the Add To pane.

The effectiveness of this exercise is based on the following assumptions:

- The representative set should not be different from the sections or departments of your enterprise, or it would amount for large number of un-identified software being scanned and reported.
 - The inventoried workstations in the enterprise are largely controlled by the enterprise administrator, who installs and copies the non-standard applications.
 - **Multiple instances of Software on the same inventoried workstation:** For an inventoried workstation, the same software can be reported twice if one entry is reported from the Add Remove Program scanning or the MSI scanning, and the other is reported based on the software dictionary configuration. The [Section 76.3.25, “Reconcile Software,” on page 1075](#) rule contains default configurations to merge these two entries but this might not be complete. In order to resolve this problem, you must manually configure the Edit Add-Remove Software rule.
 - **Redundant drives and directories that do not contain software:** Configure the rules in Software Scanning page and the Disk Usage Scanning pages of the software dictionary to eliminate these drives and directories from scan. For more information about the software dictionary rules, see [Step 3 on page 1046](#).
- 6 Re-scan all the inventoried workstations.
 - 7 After the inventory information is stored in the Inventory database, you should see that all the entries that you marked for dictionary during the earlier scan are scanned and reported as a software.
 - 8 Repeat Step 3 through Step 7 till you fine-tune the dictionary according to your requirements.

76.3.31 Viewing Software Information in the Inventory Summary

- 1 Configure the Inventory database. For more information on how to configure the Inventory database, see [Section 77.1.1, “Configuring the Inventory Database,” on page 1096](#).
- 2 Right-click an inventoried workstation object, click *Actions*, then click *Inventory*.
- 3 In the Summary dialog box, click *Inventory Information > Hardware/Software Inventory > Software > Application Vendors* to view the software inventory information.

A list of Software Groups and Software of the vendor is displayed. Software Group includes software patch and representative file information of the group. Software includes software patch and representative file information of the product.

For more information, see [Section 77.1.2, “Viewing the Inventory Summary of an Inventoried Workstation,” on page 1096](#).

76.3.32 Generating Software Inventory Reports

You can now generate the following Software Inventory reports:

- Add-Remove Programs by Application
- Add-Remove Programs by Machine
- Anti-Virus Signature Files by Machine
- Anti-Virus Signature Machine Count

- Disk Usage by Machine
- Exception List by Machine
- Installed NetWare Software by Machine
- Internet Explorer Installation Count
- Internet Explorer Patches by Machine
- Internet Explorer by Machine
- MSI Products by Application
- MSI Products by Machine
- Microsoft Office Components by Machine
- Microsoft Office Installation Count
- Microsoft Office by Machine
- Novell Client Components by Machine
- Novell Client Installation Count
- Novell Client by Machine
- Novell ZENworks Desktop Management Installed Agent Components by Machine
- Novell ZENworks Desktop Management Installed Server Components by Machine
- Novell ZENworks Handheld Management Installed Components by Machine
- Novell ZENworks Installed Components by Machine
- Novell ZENworks Installed Suites by Machine
- Novell ZENworks Server Management Installed Agent Components by Machine
- Novell ZENworks Server Management Installed Server Components by Machine
- Outlook Express Installation Count
- Outlook Express by Machine
- Software Dictionary Application Files by Machine
- Software Dictionary Applications by Machine
- Software Dictionary Versions Machine Count
- Software Dictionary Versions by Machine
- Software Installation Count
- Software Installations
- Software by Machine
- System Software Inventory Report
- Windows Components by Machine
- Windows Installation Count
- Windows Media Player Count
- Windows Media Player Patches by Machine
- Windows Media Player by Machine
- Windows Operating System by Machine
- Windows Security Patches by Machine

- Windows Security Patches by Patch

For more information about each report, see “Types of Inventory Reports” on page 1113.

76.4 Customizing the Software Inventory Information To Be Scanned For ZENworks for Desktops 4.x and Earlier Versions of Inventoried Workstations

Refer to the [ZENworks for Desktops 4.0.1 Documentation Web site \(http://www.novell.com/documentation/zdpr/index.html\)](http://www.novell.com/documentation/zdpr/index.html) to know how to customize the software inventory information for the ZENworks for Desktops 4.x inventoried workstations.

76.5 Scanning for Workstations That Are Periodically Connected to the Network

ZENworks 7 Desktop Management Inventory Scanner scans hardware and software information for all workstations that are registered to eDirectory but are temporarily disconnected from your network.

This helps the administrator to gather the inventory for the users who connect to the network less frequently but want their machines to be inventoried.

If the Inventory Scanner is scheduled to collect the inventory for an inventoried workstation that is registered to eDirectory but not connected to the network, the Inventory Scanner waits until the workstation is reconnected to the network.

The Scheduler caches the Workstation Inventory policy from eDirectory and the cache information will be available till the workstation is up and running. The Scheduler launches the Scanner. The Scanner checks whether the inventoried workstation is connected to the network.

If the inventoried workstation is connected, the Inventory Scanner collects the inventory of the workstation and will update the information to the Inventory database. If the inventoried workstation is not connected, the Scanner reports an error to the Scheduler and the Scheduler launches the Inventory Scanner after every 15 minutes until it is successful.

For more information on how to deploy this functionality in your enterprise, see “Scenario 3: Deploying Inventory Agent on Workstations that Are Periodically Connected to the Network” on page 912.

76.6 Scanning for Workstations That Are Never Connected to Your Network

ZENworks 7 Desktop Management Inventory Scanner helps you to collect the hardware and software information for workstations that are not connected to your network even at least once.

To collect the inventory for workstations that are never connected to your network, review the following sections:

- “Prerequisites” on page 1082
- “Collecting Inventory for Workstations That Are Not Connected to the Network” on page 1082

- “Limitations” on page 1084

76.6.1 Prerequisites

To collect the inventory for the workstations that are never connected to your network, make sure that the following prerequisites have been met:

- ❑ The ZENworks 7 Desktop Management Inventory Agent must be installed on the workstation
- ❑ The workstation should have at least one valid network adapter such as Ethernet, Token Ring, or FDDI installed.

76.6.2 Collecting Inventory for Workstations That Are Not Connected to the Network

To collect the inventory for the workstations that are never connected to your network:

- 1 Manually create an eDirectory workstation object for the workstation that you want to scan for.

Enter the following commands at the console prompt of an existing inventoried workstation that is connected to the network, and has ZENworks 7 Inventory agent and the recommended version of Novell Client installed:

```
zwsreg.exe -unreg
```

```
zwsreg.exe -IMPORTWS workstation_name -IMPORTSERVER NONE
```

```
zwsreg.exe -unreg
```

For more information on how to run `zwsreg.exe`, see [Section 9.3, “Using Zwsreg.exe,” on page 127](#).

- 2 Manually create the `zfdscanner.ini` file with the following contents on the workstation:

```
[ZfdScanner]
WorkstationTypedDN=complete_typed_workstation_DN
TreeName=eDirectory_tree_name
ServerName=Inventory_server_DNS_name
WMIScan=TRUE or FALSE
DMIScan=TRUE or FALSE
ScheduleFullScan=a_value_between_5_and_100
CustomHWScan=TRUE or FALSE
CustomHWScanBinaryName=name_of_binary_.exe
SoftwareScan=TRUE
```

You must enter the values for the following parameters: `WorkstationTypedDN`, `TreeName`, and `ServerName`. For the remaining parameters, if you do not specify the values or if you specify invalid values, the Inventory scanner sets the following default values:

```
WMIScan = TRUE
```

```
DMIScan=TRUE
```

```
ScheduleFullScan=5
```

CustomHWScan=FALSE

CustomHWScanBinaryName=

- 3** Using ZENworks 7 Desktop Management ConsoleOne, create the following .ini files: `asset.ini`, `zipppnames.ini`, `ibmnames.ini`, and `hwrules.ini`.

3a In ConsoleOne, right-click the Workstation package, click *Properties*, click *Policies*, then select any of the suboptions: *Win95-98*, *WinNT-2000-XP*, *WinNT*, *Win2000*, or *WinXP*.

3b Select the Workstation Inventory Policy, then click *Properties*.

3c Click *Configuration Editor* tab and do the following:

- Click the *Asset Information* suboption.

Configure Asset Information and click the *Export* button to save the file as `asset.ini` in a local directory

- Click the *Zipped Names* suboption.

To configure Zipped Names with the default values, click the *Default* button. Click the *Export* button to save the file as `zipppnames.ini` in a local directory.

- Click the *IBM Names* suboption.

To configure the IBM Names with the default values, click the *Default* button. Click the *Export* button to save the file as `ibmnames.ini` in a local directory.

- Click the *HW Rules* suboption.

To configure HW Rules with default values, click the *Default* button. Click *Export* to save the file as `hwrules.ini` in a local directory.

3d (Optional) If you want custom hardware scan functionality, create `customhwattrlist.ini`.

- In the Workstation Inventory Policy property page, click *Hardware Scan* tab.

The *Enable Custom Scanning* check box is selected by default.

- Click *Custom Attribute Editor*, then click *Export*.

- Save the file as `customhwattrlist.ini` in a local directory.

- 4** Copy the INI files created in **Step 3** to the `%SystemRoot%\zenworks` directory on the workstation that you want to scan for.

- 5** Copy `generaldictionary.xml` and `privatedictionary.xml` from `zenworks_installation_drive_or_volume\zenworks\inv\server\dictdir` on the Inventory server to the `%SystemRoot%\zenworks` directory on the workstation that you want to scan for.

- 6** Run the ZENworks 7 Desktop Management Inventory scanner on the workstation that you want to inventory. At the console prompt, enter the following command from the ZENworks Inventory installation directory:

```
zfdinvscanner.exe -d zfdscanner.ini_file_path
```

TIP: If `zfdscanner.ini` is present in the same location where the ZENworks 7 Desktop Management Scanner is running, you need not specify the `zfdscanner.ini_file_path` to run the Inventory scanner.

The Inventory scanner generates the `.str` file and saves it in the `%SystemRoot%\zenworks` directory.

- 7 Copy the `.str` file to the `Inventory_server_installation_path\zenworks\scandir` directory.

76.6.3 Limitations

You should be aware of the following limitations with collecting inventory for workstations that are never connected your network.

- The minimal information is not reported in eDirectory for disconnected workstations.
- If the `.str` file of the workstation is deleted by the Storer or the Selector, you must manually trigger a full scan on the workstation and copy the `.str` file to `inventory_server_installation_path\zenworks\scandir`.

To trigger a full scan, delete `%SystemRoot%\zenworks\hist.ini` on the workstation and run the ZENworks 7 Desktop Management scanner from the command line.

76.7 Removing Redundant Inventoried Workstations from the Inventory Database

You can remove the unwanted, redundant, or obsolete inventoried workstations from the Inventory database using the Inventory Removal service.

The Inventory Removal service is a manual service that runs on the Inventory server. The service removes the inventoried workstations from the Inventory database using the `inventoryremovallist.txt` file, which contains a list of inventoried workstations that must be removed from the Inventory database.

IMPORTANT: You must make sure that the Inventory Service Manager is loaded when you run the Inventory Removal Service.

You can run the Inventory Removal service on the Intermediate Server only if the Intermediate Server has either inventoried workstations or database attached to it.

To remove the inventoried workstations from the Inventory database:

- 1 Create `inventoryremovallist.txt` by using any of the following methods:
 - To automatically create `inventoryremovallist.txt`, use the NDS Lookup for DB utility. By default, this utility creates a lookup file, `deletewslst.txt`, that contains a list of the inventoried workstations. For more information about the NDS Lookup for DB utility, see [Section 76.7.1, “Understanding the NDS Lookup for DB Utility,” on page 1086](#).

After generating a lookup file, do the following:

- Rename the lookup file to `inventoryremovallist.txt`.
- (Optional) In the lookup file, add the DNs of any other inventoried workstations that must be removed from the Inventory database and that have not yet been listed in the lookup file.
- To manually create `inventoryremovallist.txt`, use any text editor to create the file with the following contents:

DN of the inventoried workstation (as stored in the Inventory database) to be removed from the Inventory database

DN of the *inventoried workstation* (as stored in the Inventory database) to be removed from the Inventory database

...

...

DN of the *inventoried workstation* (as stored in the Inventory database) to be removed from the Inventory database

A sample `inventoryremovallist.txt` file is as follows:

```
CN=WS1.OU=WORKSTATIONS.OU=WEST.O=XYZ.T=XYZ-TREE
CN=WS99.OU=WORKSTATIONS.OU=NORTH.O=XYZ.T=XYZ-TREE
CN=WS50.OU=WORKSTATIONS.OU=EAST.O=XYZ.T=XYZ-TREE
```

To generate the list of inventoried workstations that must be removed, you can either perform a query on a selected criteria or manually enter the names of the inventoried workstations. For more information on Query, see [Section 77.1.3, “Viewing Inventory Information by Querying the Database,”](#) on page 1109.

- 2 Copy the `inventoryremovallist.txt` file to the `ZENworks_installation_path\zenworks\inv\server\wminv\properties` directory.

For Linux, copy the `inventoryremovallist.txt` file to the `/etc/opt/novell/zenworks/inv/` directory.

- 3 In the `ZENworks_installation_path\zenworks\inv\server\wminv\properties\inventoryremoval.properties` file, make sure that the value of `FilePath` is the location of `inventoryremovallist.txt` (specified in [Step 2](#)).

For Linux, in the `/etc/opt/novell/zenworks/inv/InventoryRemoval.properties` file, make sure that the value of `FilePath` is the location of `inventoryremovallist.txt`.

NOTE: Make sure that the path separator is a forward slash (/) and not a backslash (\).

- 4 At the server console prompt, enter `StartSer RemoveInventory` to start the Inventory Removal service.

For Linux, at the server console prompt, enter `/opt/novell/bin/StartSer RemoveInventory` to start the Inventory Removal service.

The Inventory Removal service operates in the following order:

1. The Inventory Removal service reads each line of the `inventoryremovallist.txt` file and creates a `delete_str` file for each inventoried workstation that is listed in the `inventoryremovallist.txt` file.

The `delete_str` file is saved in the `scandir` directory if the Selector is running, else it will be placed in the `dbdir` or `entmergedir` directories depending on the Inventory server role.

2. The Selector validates the `delete_str` file and copies it into the `dbdir` and `entmergedir` directories.
3. The Storer reads the `delete_str` file from `dbdir` and deletes the inventoried workstation from the attached Inventory database.
4. If the inventory deployment rolls up scan data, the `delete_str` is also rolled up to the next level Inventory server.

The inventoried workstation is deleted from the Inventory database at all Inventory servers deployed at the enterprise level.

76.7.1 Understanding the NDS Lookup for DB Utility

NDS Lookup for DB automatically generates a list of inventoried workstations that are stored in the Inventory database but do not have a corresponding entry in eDirectory. By default, this lookup file is named `deletewslist.txt`.

The excess workstations in the Inventory database exist because these workstations have been deleted from eDirectory but their corresponding entries were not removed from the database.

The list generated by NDS Lookup for DB helps you in identifying the redundant workstation objects to be removed from the Inventory database by using the Inventory Removal Service.

IMPORTANT: You must run this utility only on the Inventory server to which an Inventory database is attached. Also, you must make sure that the Service Manager is loaded when you run this utility.

To run this utility:

- 1 Specify the path of the lookup file in
`inventory_server_installation_path\inv\server\wminv\properties\inventoryremoval.properties`.

For Linux, specify the path of the lookup file in `/etc/opt/novell/zenworks/inv/InventoryRemoval.properties`.

NOTE: Make sure that the path separator is a forward slash (/) and not a backslash (\).

- 2 (Optional) Configure the lookup filename in the server role property file, which can be any of the following files, depending on role of the Inventory server:
`root_db_wks.properties`, `root_db.properties`, `int_db_wks.properties`, `int_db.properties`, `leaf_db_wks.properties`, or `standalone.properties`.

The server role property file contains the [NDSLookupForDB Service] section with the lookup filename in the ARGUMENTS parameter. The default lookup filename is `deletewslist.txt`.

IMPORTANT: The lookup filename should consist of alphanumeric characters only.

- 3 At the server console prompt, enter `startser NDSLookupForDB`.

For Linux, at the server console prompt, enter `/opt/novell/bin/StartSer NDSLookupForDB`.

76.8 Removing Duplicate Workstation Objects from the Inventory Database

You can now remove the duplicate workstation objects from the Inventory database by using the Dupremove utility.

Duplicate workstation objects are workstations that have multiple entries in the Inventory database. If the Inventory database has duplicate workstation objects, it not only results in wasted database space but also reporting of duplicate information by the Inventory ConsoleOne utilities such as Query, Summary, Inventory Reports, and Data Exports.

The following sections provide more information on how to use the Dupremove utility:

- [Section 76.8.1, “Running the Dupremove Utility,” on page 1087](#)
- [Section 76.8.2, “Understanding the Dupremove Switches,” on page 1088](#)

76.8.1 Running the Dupremove Utility

- 1 Stop the Inventory service. For more information, see [Section 73.1.5, “Starting and Stopping the Inventory Service,” on page 915](#).
- 2 Make sure that the Database server is up and running.
- 3 Run the Dupremove utility.

- On a NetWare Inventory server:

Edit `sys:\system\dupremove.ncf` to configure the required parameters. Refer to `dupremove.ncf` for information about configuring the parameters. For detailed information about the parameters, see [Section 76.8.2, “Understanding the Dupremove Switches,” on page 1088](#).

After editing the file, go to `sys:\system` and enter `dupremove` from the Inventory server system console prompt.

- On a Windows Inventory server:

Edit

`Inventory_server_installation_directory\zenworks\inv\server\wminv\bin\dupremove.bat` to configure the required parameters. Refer to `dupremove.bat` for information about configuring the parameters. For detailed information about the parameters, see [Section 76.8.2, “Understanding the Dupremove Switches,” on page 1088](#).

After editing the file, go to

`Inventory_server_installation_directory\zenworks\inv\server\wminv\bin` and enter `dupremove` from the Inventory server command prompt.

- On a Linux Inventory server:

Edit `/opt/novell/bin/dupremove` to configure the required parameters. Refer to `dupremove` for information about configuring the parameters. For detailed information about the parameters, see [Section 76.8.2, “Understanding the Dupremove Switches,” on page 1088](#).

After editing the file, go to `/opt/novell/bin` and enter `./dupremove` from the Inventory server command prompt.

IMPORTANT: You must enclose the parameters within double quotes in `dupremove.ncf`, `dupremove.bat` or `dupremove` files, and there should be no spaces within double quotes. For example, “-dbtype=1”.

If you specify wrong parameters, or spaces within double quotes, the Dupremove utility retries endlessly.

To stop this process on a NetWare Inventory server, you must first procure the process ID of the Dupremove utility by entering `java -show` at the server prompt, and then enter `java -killDupremove_process_ID`.

To stop the process on a Windows or Linux Inventory server, press Ctrl+C.

- 4 Start the Inventory service. For more information, see [Section 73.1.5, “Starting and Stopping the Inventory Service,” on page 915](#).
- 5 Enforce a full scan either on all affected workstation objects or on all workstation objects that send the inventory data to this Inventory server:
 - To enforce a full scan on all workstation objects that send the inventory data to this Inventory server, enforce a full scan on the Inventory Service object. For more information, see [Section 73.3, “Configuring the Inventory Service Object,” on page 955](#).
 - To enforce a full scan on an affected workstation object:
 - 5a In ConsoleOne, right-click the workstation object, then click *Properties*.
 - 5b Click the *ZENworks Inventory* tab, then click the *Workstation Scan Configuration* suboption.
 - 5c Select *Start Full Scan*.
 - 5d Click *Apply*, then click *Close*.
 - 5e Repeat [Step 5a](#) through [Step 5d](#) for all affected workstation objects.

76.8.2 Understanding the Dupremove Switches

- [“-host” on page 1088](#)
- [“-dbtype” on page 1088](#)
- [“-sid” on page 1089](#)
- [“-port” on page 1089](#)
- [“Dupremove Functions” on page 1089](#)
- [“-user” on page 1094](#)
- [“-password” on page 1094](#)

-host

Specify the IP address of the server on which the Inventory database is running.

-dbtype

The Inventory database type. It can include any of the following values:

Table 76-2 List of Dbtype values

Inventory Database Running On	Dbtype Value
Sybase	0
Oracle	1
MS SQL	2

-sid

The service ID identifying the Inventory database. -sid is required to connect to JDBC. It can include any of the following values:

Table 76-3 *Sample sid values*

Inventory Database Running On	Sample SID Values
Sybase	mgmtdb
Oracle	orcl
MS SQL	mgmtdb

-port

The port number on which the Inventory database is running. It can include any of the following values:

Table 76-4 *Sample port values*

Inventory Database Running On	Sample Port Values
Sybase	2638
Oracle	1521
MS SQL	1433

Dupremove Functions

You must use the following Dupremove functions only one at a time in the `dupremove.bat`, `dupremove.ncf`, or `dupremove`:

IMPORTANT: The values for the Dupremove functions are case-sensitive.

Table 76-5 *Detail explanation and examples of the Dupremove functions*

Dupremove Switch	Description	Possible Values / Pattern Types	Examples
-listwsdup	Lists all workstations that have duplicate entries in the Inventory database.	---	<p>To list all the workstation objects that have duplicate entries in the Sybase Inventory database, edit the Java command in dupremove.bat, dupremove.ncf, or dupremove as follows:</p> <pre>java -Djava.compiler= com.novell.zenworks.desktop.invento ry.storer.DatabaseOperator "- host=127.0.0.1" "-listwsdup" "- dbtype=0" "-sid=mgmtldb" "- port=2638"</pre>
-listwsdirty	Lists all workstations whose scan data has not been updated in the Inventory database and that need a full scan.	--	<p>To list all the workstation objects that have duplicate entries in the Oracle Inventory database, edit the Java command in dupremove.bat, dupremove.ncf, or dupremove as follows:</p> <pre>java -Djava.compiler= com.novell.zenworks.desktop.invento ry.storer.DatabaseOperator "- host=127.0.0.1" "-listwsdirty" "- dbtype=1" "-sid=orcl" "-port=1521"</pre>

Dupremove Switch	Description	Possible Values / Pattern Types	Examples
-listwspattern	Lists workstation objects on the basis of the pattern you define.	<ul style="list-style-type: none"> Workstation names beginning with with a specific character or a string Workstation names containing a specific character or a string Workstation names ending with a specific character or a string <hr/> <p>IMPORTANT: You must enter the typed DN of the workstation.</p> <hr/>	<ul style="list-style-type: none"> To list all the workstation objects whose DN starts with "cn=ws" and that have duplicate entries in the Sybase Inventory database, edit the Java command in dupremove.bat, dupremove.ncf, or dupremove as follows: <pre>java -Djava.compiler= com.novell.zenworks.desktop.inventory.storer.DatabaseOperator" -host=127.0.0.1""- listwspattern=cn=ws%%""- dbtype=0" "-sid=mgmtldb" "- port=2638"</pre> To list all the workstation objects whose DN contains "ou=novell" and that have duplicate entries in the Oracle Inventory database, edit the Java command in dupremove.bat, dupremove.ncf, or dupremove as follows: <pre>java -Djava.compiler= com.novell.zenworks.desktop.inventory.storer.DatabaseOperator" -host=127.0.0.1""- listwspattern=%ou=novell%%""- dbtype=1" "-sid=orcl" "- port=1521"</pre> To list all the workstation objects whose DN ends with "T=novell_inc" and that have duplicate entries in the MS SQL Inventory database, edit the Java command in dupremove.bat, dupremove.ncf, or dupremove as follows: <pre>java -Djava.compiler= com.novell.zenworks.desktop.inventory.storer.DatabaseOperator" -host=127.0.0.1""- listwspattern=%T=novell_inc""- dbtype=2" "sid=mgmtldb" "- port=1433"</pre>

Dupremove Switch	Description	Possible Values / Pattern Types	Examples
-remwsdup	Removes workstation objects from the Inventory database.	<ul style="list-style-type: none"> • * (asterisk): Removes inventory information from all the workstation objects having duplicate entries in the database • <i>Typed_DN_of_a_workstation:</i> Removes inventory information of the specific workstation object having duplicate entries in the database 	<ul style="list-style-type: none"> • To remove all information from all workstation objects having duplicate entries in the MS SQL Inventory database, edit the Java command in <code>dupremove.bat</code>, <code>dupremove.ncf</code>, or <code>dupremove</code> as follows: <pre>java -Djava.compiler= com.novell.zenworks.desktop.invent ory.storer.DatabaseOperator" -host=127.0.0.1" "- remwsdup=*"-dbtype=2" "- sid=mgmtdb" "-port=1433"</pre> • To remove all information from one workstation object having a duplicate entry in the Oracle Inventory database, edit the Java command in <code>dupremove.bat</code>, <code>dupremove.ncf</code>, or <code>dupremove</code> as follows: <pre>java -Djava.compiler= com.novell.zenworks.desktop.invent ory.storer.DatabaseOperator" -host=127.0.0.1"- remwsdup=ws.novell.novell_inc"- dbtype=1" "-sid=orcl" "- port=1521"</pre>

Dupremove Switch	Description	Possible Values / Pattern Types	Examples
-remwspattern	Removes workstation objects on the basis of the pattern you define.	<ul style="list-style-type: none"> Workstation names beginning with with a specific character or a string Workstation names containing a specific character or a string Workstation names ending with a specific character or a string <hr/> <p>IMPORTANT: You must enter the typed DN of the workstation.</p> <hr/>	<ul style="list-style-type: none"> To remove all the workstation objects whose DN starts with "cn=ws" and that have duplicate entries in the Sybase Inventory database, edit the Java command in dupremove.bat, dupremove.ncf, or dupremove as follows: <pre>java -Djava.compiler= com.novell.zenworks.desktop.invent ory.storer.DatabaseOperator" -host=127.0.0.1""- remwspattern=cn=ws%""- dbtype=0" "-sid=mgmtdb" "- port=2638"</pre> To remove all the workstation objects whose DN contains "ou=novell" and that have duplicate entries in the Oracle Inventory database, edit the Java command in dupremove.bat, dupremove.ncf, or dupremove as follows: <pre>java -Djava.compiler= com.novell.zenworks.desktop.invent ory.storer.DatabaseOperator" -host=127.0.0.1""- remwspattern=%ou=novell%""- dbtype=1" "sid=orcl" "- port=1521"</pre> To remove all the workstation objects whose DN ends with "T=novell_inc" and that have duplicate entries in the MS SQL Inventory database, edit the Java command in dupremove.bat, dupremove.ncf, or dupremove as follows: <pre>java -Djava.compiler= com.novell.zenworks.desktop.invent ory.storer.DatabaseOperator" -host=127.0.0.1""- remwspattern=%T=novell_inc%""- dbtype=2" "-sid=mgmtdb" "- port=1433"</pre>

Dupremove Switch	Description	Possible Values / Pattern Types	Examples
-remwsfile	Removes the workstation objects whose names are listed in a file.	<i>Complete path of the file including the filename</i>	<ul style="list-style-type: none"> To remove all the workstation objects that have duplicate entries in the MS SQL Inventory database and are listed in c:\windows\wsname.txt: <pre>java -Djava.compiler= com.novell.zenworks.desktop.inv entory.storer.DatabaseOperator" -host=127.0.0.1""- remwsfile=c:\\windows\\wsname.t xt" "-dbtype=2" "-sid=mgmtdb""- port=1433"</pre> <p>The contents of c:\windows\wsname.txt are as follows:</p> <pre>CN=a.OU=b.O=c.T=Novell_inc CN=ws.OU=novell.T=novell_inc WS1.novell.novell_inc WS2.novell.novell_inc</pre>

-user

Provide the user name only if you have not logged into the Inventory database as the default user (mw_dba).

-password

Provide the password for the user specified in the “-user” switch.

Viewing Inventory Information

77

The following sections indicate how you can view the inventory information:

- [Section 77.1, “Viewing the Inventory Information Using ConsoleOne,” on page 1095](#)
- [Section 77.2, “Exporting the Inventory Information,” on page 1138](#)
- [Section 77.3, “Viewing Inventory Information Without Using ConsoleOne,” on page 1145](#)
- [Section 77.4, “Retrieving Inventory information from the Inventory Database Without Using the CIM Schema,” on page 1148](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

77.1 Viewing the Inventory Information Using ConsoleOne

The following sections explain the various types of information you can view using Novell® ConsoleOne®:

- You can list hardware and software components found on the inventoried workstation and any custom information you have specified for the workstation.

The Workstation Inventory window displays the inventory items for an inventoried workstation. This window displays the information from the last inventory scan for the inventoried workstation.

For more information about viewing the inventory information of an inventoried workstation, see [Section 77.1.2, “Viewing the Inventory Summary of an Inventoried Workstation,” on page 1096](#).

- You can list inventoried workstations with the inventory information from the Inventory database satisfying the criteria you specify in the Inventory Query window. You form a query by specifying the component and its attribute for the inventoried workstations within the selected database sites.

For more information about querying the Inventory database, see [Section 77.1.3, “Viewing Inventory Information by Querying the Database,” on page 1109](#).

- You can list minimal information stored in the eDirectory™ Workstation object.

For more information, see [Section 77.1.4, “Viewing the Minimal Inventory Information from an eDirectory Object,” on page 1112](#).

- You can use a list of reports that generate the inventory information from the Inventory database specific to your needs.

For more information, see [Section 77.1.5, “Running Inventory Reports,” on page 1113](#).

- You can now quickly and easily view the inventory information.

For more information, see [Section 77.1.6, “Quickly and Easily Viewing the Inventory Data Using Quick Reports,” on page 1127](#).

77.1.1 Configuring the Inventory Database

If you want to use ConsoleOne to view the inventory information stored in the database, you must configure the database. The inventory information from the Inventory database that you configure is used for generating inventory reports, viewing inventory information, and for querying the inventory information from the database.

To configure the Inventory database:

- 1 In ConsoleOne, select a container.
- 2 Invoke Configure DB.
 - To invoke Configure DB from a database object, right-click the database object, click *ZENworks Inventory*, then click *Configure DB*. This configures the database object.
 - To invoke the Configure DB dialog box from the ConsoleOne *Tools* menu, click *ZENworks Inventory*, then click *Configure DB*.
- 3 Click *Browse* to browse for and select the ZENworks Database object.

You can also select an existing ZENworks Database object from the list of Database objects. This Database object contains the database settings such as the protocol, port in use by the database, and others.
- 4 To apply this database configuration to all the sessions, select the *Apply Configuration Across Sessions* check box.
- 5 Click *OK*.

The database you configured is used for data retrieval unless you change it again using this same procedure.

77.1.2 Viewing the Inventory Summary of an Inventoried Workstation

The Inventory Summary window displays the information from the last inventory scan for the inventoried workstation.

To view the inventory information of an inventoried workstation:

- 1 Configure the Inventory database.

For more information, see [Section 77.1.1, “Configuring the Inventory Database,” on page 1096](#).
- 2 Right-click an inventoried workstation object, then click *Actions*, then click *Inventory*.










or











In the Query Results window, double-click an inventoried workstation.



















ZENworks® 7 Desktop Management provides the following inventory information collected from the inventoried workstations:




Table 77-1 Inventory information as displayed in Inventory Summary












Scan Data Group	Scan Data Item	Description
 Inventory Information	General Dictionary Version	Version number of the General Dictionary NOTE: The General Dictionary version is not same as the ZENworks product version.
	Inventory Server	Name of the Inventory server to which the scans are sent
	Last Scan Date	List of all inventoried workstations that were scanned on or before the specified date and time
	Private Dictionary Version	Version number of the Private Dictionary
	Scan Mode	Mode used by the Inventory scanner to scan the inventoried workstation
	Version	Version number of the Inventory scanner
 Hardware/Software Inventory > General > System Information	Asset Tag	Asset tag number that the ROM-based setup program creates
	Computer Model	Identifying information of the computer such as Compaq or Dell
	Computer Type	Type of computer, such as IBM PC
	Machine Name	DNS name of the inventoried workstation
	Management Technology	Technology available on the inventoried workstation such as DMI, WMI, and others
	Model Number	Model number of the inventoried workstation
	Serial Number	Serial number of the inventoried workstation assigned by manufacturer
	Tag	Unique identifier of system information
 Hardware/Software Inventory > General > System Identification	Primary Owner Name	The name of the primary user or owner of this system
	Primary Owner Contact	The phone number of the primary user of this system
	Name	Name of the inventoried workstation as represented in eDirectory, such as the fully qualified DN of the inventoried workstation
 Hardware/Software Inventory > General > eDirectory Login Details	Current login user	User logged into the Primary eDirectory tree when the inventoried workstation was scanned







Scan Data Group	Scan Data Item	Description
	Last login user	User most recently logged into the Primary eDirectory tree through Novell Client when the inventoried workstation was scanned
 Hardware/Software Inventory >  General >  Login Details >  Windows Domain	Name	Domain name of the inventoried workstation
 Hardware/Software Inventory >  Software >  Application Vendors > <i>Vendor_name</i> >  <i>software_group_name</i> >  <i>software</i>	Name	Vendor-defined name of the product represented as a vendor trademark or registered trademark
	Version	<p>User-friendly version of a product</p> <p>For example, the version for Windows 2000 is 2000 or Major.Minor Version of the Product</p>
	Category	<p>Product category to which the product belongs</p> <p>For example, Office is a part of the Productivity tools category and Solitaire is a game</p>
	Description	Description of the product
	Help Link	Support Web site URL for the product that is available in ARP and MSI
	Package GUID	Vendor-defined GUID for a product that is available in MSI
	Product Identifier	<p>A unique, 16-character identifier for an installed product. This identifier is available from MSI on Windows</p> <p>The format is ABCD-1234-WXYZ-PQRS</p>
	Internal Version	<p>Internal version of a product</p> <p>The format is:</p> <p><i>major version.minor version.build.sub build number</i></p> <p>or</p> <p><i>major version.minor version.build</i></p>
	Language	User-friendly name for the language of this copy of the product
	Uninstall String	The command to invoke for uninstalling this product instance. Currently, this is available in Add/Remove Programs (ARP) and MSI on Windows

















Scan Data Group	Scan Data Item	Description
	Install Source	Identifies the file system path where the installation files were stored when installing this product instance. Currently, this is available in ARP and MSI on Windows
	Last Execution Time	Date and time stamp when the product was last executed
	Frequency of Usage	Number of times the product has been used
	Friendly Name	Display name of the software
	Installation Repository	Source of scan, which can be, Add/Remove Programs, MSI, Software Dictionary, or PRODUCTS.DAT
	Support Pack	Installed support pack number of the product
	Product Edition	Product edition defined by the vendor. For example, Professional
	Path	Directory path where the product is installed on the inventoried workstation
	AntiVirus Definition Date	The date of the virus definition file installed on the computer. Some anti-virus products combine date and version into a single string
	NOTE: This is applicable only for antivirus products.	
	AntiVirus Definition Version	The vendor-defined version of the virus definition file that has been installed on a computer
	NOTE: This is applicable only for antivirus products.	
 Hardware/Software Inventory >  Software >  Application Vendors > <i>Vendor_name</i> >  <i>software_group_name</i> >  <i>software</i> > Patches	Name	Vendor-defined name for the patch
 Hardware/Software Inventory >  Software >  Application Vendors > <i>Vendor_name</i> >  <i>software_group_name</i> >  <i>software</i> > Representative File Information	File Name	Name of the file representing the software
	File Version	Version of the file representing the software
	File Size	Size of the file representing the software



















Scan Data Group	Scan Data Item	Description
	Last Modified	Last modified date of the file representing the software
	Internal Name	Internal name
	Product Version	The version of the product represented by this file
	Company	Vendor name
	Product Name	The product that this file represents
	Language	User-friendly name for the language of this copy of the file
	File Path	Location of the file on the inventoried workstation
 Hardware/Software Inventory >  Software >  Disk Usage	Software Dictionary ID	ID of the file as represented in the General software dictionary
	File Extension Name	The file extension for which the disk usage is scanned for
 Hardware/Software Inventory >  Software >  Device Drivers >  Pointing Device Drivers > <i>Pointing Device driver name</i>	Total Disk Usage	Total disk usage for all the files of the specified extension.
	Name	Name of the mouse driver
 Hardware/Software Inventory >  Software >  Device Drivers >  Display Drivers	Version	Version number of the mouse driver
	Install Date	Install date of the display driver
	Manufacturer	Name of the display driver manufacturer
	Is Shadowed (True or False)	If True, the display driver is currently being shadowed
 Hardware/Software Inventory >  Software >  Device Drivers >  Network Drivers	Version	Version number of the display driver
	Description	Description of the network driver
 Hardware/Software Inventory >  Software >  Operating System	Name	Network driver name
	Version	Version number of the network driver
	Code Page	Language code page of the operating system
	OS Type	Operating system of the inventoried workstation
	Install Date	Install date of the operating system















Scan Data Group	Scan Data Item	Description
 Hardware/Software Inventory >  Hardware >  Monitor	Caption	Operating system name, for example, Windows 95/Windows 2000
	Other Description	Additional description of the operating system if available
	Role	Type of the operating system such as server or workstation
	Total Virtual Memory Size	Total number of bytes in the virtual address space of the calling process
	Total Memory Size	Total memory of the operating system
	Version	Version number of the operating system
	Device ID	Unique ID of a desktop monitor that is attached to an inventoried workstation For example, DesktopMonitor1
	Description	Description of the monitor.
	Nominal Size	A number representing the diagonal width of the monitor (the distance from one corner of the screen to the opposite corner of the screen) For example, 17" You can customize the scan of the nominal size of the monitor by configuring the HWRules .ini file using the Workstation Inventory policy
	Viewable Size	A number representing the diagonal width of the screen image excluding the black borders around the image's edge For example, 15.8"
	Manufacturer	Name of the monitor's manufacturer For example, DELL Computer Corp
	Serial Number	Manufacturer's number used to identify a monitor For example, 23DDC24N9067
	Model	Product name of the monitor given by the manufacturer For example, DELL E771a
	Manufacture Date	Year in which the monitor was manufactured For example, 2003


Scan Data Group	Scan Data Item	Description
 Hardware/Software Inventory >  Hardware >  Chassis	Model ID	Unique ID of a model of the monitor; it is a combination of the Manufacturer ID and Product ID For example, DELA001
	Asset Tag	Asset tag number of the system chassis. For example, S11127.
	Number of Power Cords	Total number of power cords attached to a system chassis
	Chassis Type	Represents whether the system chassis is a laptop, desktop, notebook, docking station and so on
	Manufacturer	Name of the system chassis manufacturer For example, Compaq
	Serial Number	Manufacturer's number used to identify a system chassis For example, 53R661S
	Version	Version number of the system chassis
	Tag	Unique ID of the system chassis attached to a particular inventoried workstation For example, System Enclosure 0
	IRQ Number	Interrupt assigned to this device
	Name	Identifying information of the mouse
 Hardware/Software Inventory >  Hardware >  Pointing Device >  <i>Pointing device name</i>	Number of Buttons	Number of buttons on the mouse
	Delay	Delay before the repeat of a key
	Description	Description of the keyboard, such as IBM Enhanced 101 or 102 keys
	Layout	Layout of the keyboard
	Number of Function Keys	Total number of function keys
	Subtype	Type of the keyboard
	Typematic Rate	Rate of processing the keys
	Chip Set	Chip set used by the controller to compare system capabilities
 Hardware/Software Inventory >  Hardware >  Display Adapter >  <i>Display adapter name</i>		










Scan Data Group	Scan Data Item	Description
	Current Bits/Pixel	Number of adjacent color bits for each pixel
	Current Horizontal Resolution	Number of horizontal pixels shown by the display
	Current Vertical Resolution	Number of vertical pixels shown by the display
	DAC Type	Digital-to-Analog converter type
	Description	Description of the display adapter
	Maximum Memory Supported	Maximum memory that the display adapter supports for VIDEO RAM
	Maximum Refresh Rate	Maximum refresh rate of the monitor for redrawing the display, measured in Hertz
	Minimum Refresh Rate	Minimum refresh rate of the monitor for redrawing the display, measured in Hertz
	Number of Color Planes	Number of color planes supported by the video system
	Provider	Vendor name
	Video Architecture	The architecture of the video subsystem in this system, for example, CGA/VGA/SVGA/8514A
 Hardware/Software Inventory >  Hardware >  BIOS	Video Memory Type	The type of video memory for this adapter, for example, VRAM/SRAM/DRAM/EDO RAM
	BIOS Identification Bytes	Byte in the BIOS that indicates the computer model
	Install Date	The manufacturing date of the BIOS
	Manufacturer	BIOS vendor name
	Caption	BIOS label
	Primary BIOS	True state indicates Primary BIOS
	Serial Number	Serial number of the computer, assigned during manufacture
	Size	Size of the BIOS
	Version	Version or revision level of the BIOS
	Current Clock Speed (in MHz)	Current clock speed of the processor
	Device ID	Special hexadecimal string identifying the processor type
 Hardware/Software Inventory >  Hardware >  Processor	Maximum Clock Speed (in MHz)	Maximum clock speed of the processor




Scan Data Group	Scan Data Item	Description
	Other Family Description	Additional description about the Processor Family, such as Pentium Processor with MMX technology
	Processor Family	Identification of the processor family such as Pentium II or Pentium III
	Processor Stepping	Single-byte code characteristic provided by microprocessor vendors to identify the processor model
	Role	Type of processor such as central processor, math coprocessor, and others
	Upgrade Method	The method by which this processor can be upgraded, if upgrades are supported
 Hardware/Software Inventory >  Hardware >  Modem	Description	Additional information about the modem
	Name	Identifying information of the modem
	Device ID	Special hexadecimal string identifying the modem type
	Provider	Name of the vendor
 Hardware/Software Inventory >  Hardware >  Battery	Chemistry	The battery chemistry, for example, lithium-ion or nickel metal hydride
	Design Capacity	The design capacity of the battery in mWatt-hours
	Design Voltage	The design voltage of the battery in mVolts
	Install Date	The battery manufacture date
	Manufacturer	The name of the company that manufactured the battery
	Name	Device name for this battery, for example, Duracell* DR-36
	Serial Number	The serial number for this battery
	Smart Battery Version	The Smart Battery Data Specification version number supported by this battery
 Hardware/Software Inventory >  Hardware >  Power Supply	Description	Expanded description of the input voltage capability for this power supply
	Total Output Power (in milliwatts)	Attribute value that represents the total output power of the power supply
 Hardware/Software Inventory >  Hardware >  Memory	Total Memory	Total memory of the inventoried workstation
 Hardware/Software Inventory >  Hardware >  Disk Drives >  Floppy	Capacity	Floppy drive capacity

Scan Data Group	Scan Data Item	Description
	Description	Floppy drive description
	Drive Letter	Letter name of the drive
	Manufacturer	Vendor name
	Physical Cylinders	Floppy drive cylinders
	Physical Heads	Floppy drive R/W heads
	Sectors/Track	Floppy drive sectors per track
 Hardware/Software Inventory >  Hardware >  Disk Drives >  Physical Disk >  Fixed Disk	Description	Description
	Manufacturer	Vendor name
	Physical Cylinders	Number of cylinders
	Physical Heads	Number of heads
	Sectors/Track	Fixed disk drive sectors per track
	Size	Size of the fixed disk
 Hardware/Software Inventory >  Hardware >  Disk Drives >  Physical Disk >  Removable Disk	Description	Description
	Manufacturer	Vendor name
	Physical Cylinders	Number of cylinders
	Physical Heads	Number of heads
	Sectors/Track	Removable disk drive sectors per track
	Size	Size of the removable disk
 Hardware/Software Inventory >  Hardware >  Disk Drives >  Logical Disk > <i>Logical disk name</i>	Drive Letter	Letter name of the drive
	File System Type	Type of file system, such as File Allocation Table (FAT)
	Free Size	Drive's actual size in MB
	Volume Label	Name of the hard disk volume
	Size	Drive's available space in MB
	Volume Serial Number	Hard disk volume serial number
	Name	Name of the CD drive attached to the inventoried workstation
	Description	Description of the CD
 Hardware/Software Inventory >  Hardware >  Disk Drives >  CDROM	Name	Name of the CD drive attached to the inventoried workstation
	Description	Description of the CD

Scan Data Group	Scan Data Item	Description
 Hardware/Software Inventory >  Hardware >  Ports >  Serial Port	Drive Letter	Mapped drive name of the CD
	Manufacturer	Vendor name
	Caption	Caption of the CD
	Address	Base input/output address for this serial port
	IRQ Number	IRQ number of the serial port
	Name	The logical name of the I/O device on this serial port, under this operating environment
 Hardware/Software Inventory >  Hardware >  Ports >  Parallel Port	Address	Base I/O address for this parallel port
	DMA Support (True or False)	If True, DMA is supported
	Name	The logical name of the input-output device on this parallel port, under this operating environment
	IRQ Number	IRQ number of the parallel port
 Hardware/Software Inventory >  Hardware >  Bus	Bus Type	Bus type indicates PCI, ISA, and others
	Description	Bus description
	Name	Bus name
	Version	Version of the bus supported by the motherboard
	Adapter Type	Type of network adapter, such as FDDI or token ring
 Hardware/Software Inventory >  Hardware >  Network Adapter	Auto Sense	A Boolean value indicating whether the network adapter is capable of automatically determining the speed or other communication characteristics of the attached network media
	Card Manufacturer	Name of the card manufacturer
	Description	Adapter description
	Install Date	Install date of the network adapter
	Maximum Speed	Rate at which the data is transferred over the LAN
	Name	Network adapter name

Scan Data Group	Scan Data Item	Description
	Permanent Address	Node address stored permanently in the adapter
	Provider	Name of the provider
 Hardware/Software Inventory >  Hardware >  Sound Adapter	Description	Description of the multimedia component for the workstation
	Name	Label of the multimedia card
	Provider	Name of the provider
 Hardware/Software Inventory >  Network >  DNS	DNS Name	The DNS name of the inventoried workstation
 Hardware/Software Inventory >  Network >  Network (<i>instance_number</i>) >  IP	IP Address	The unique address assigned to a computer on an IP Internet
	Subnet Mask	The subnet mask of the inventoried workstation paired with an IP address specifies to an IP router which octets or bits in the IP address are the network ID and which octets or bits are the node ID
 Hardware/Software Inventory >  Network >  Network (<i>instance_number</i>) >  IPX	IPX Address	The IPX™ address of the inventoried workstation
 Hardware/Software Inventory >  Network >  Network (<i>instance_number</i>) >  MAC	MAC Address	Unique node address permanently coded in the network adapter that identifies a specific computer on a network
 Hardware/Software Inventory >  Network > IP	IP Address	The unique address assigned to a computer on an IP Internet
	Subnet Mask	The subnet mask of the inventoried workstation paired with an IP address specifies to an IP router which octets or bits in the IP address are the network ID and which octets or bits are the node ID
Hardware/Software Inventory > Network > IPX	IPX Address	The IPX address of the inventoried workstation
Hardware/Software Inventory > Network > MAC	MAC Address	Unique node address permanently coded in the network adapter that identifies a specific computer on a network
 Hardware/Software Inventory >  System >  System IRQ	Availability	Availability of the specific IRQ channel
	IRQ Number	Number of the Interrupt Request Line (IRQ), from 0 to 15
	IRQ Trigger Type	IRQ Trigger type
	Shareable	If True, the system IRQ can be shared across devices

Scan Data Group	Scan Data Item	Description
 Hardware/Software Inventory >  System >  System Cache	Associativity	Defines the system cache associativity (direct-mapped, 2-way, 4-way)
	Cache Type	Defines the system cache type, for example, Instruction, Data, Unified
	Capacity	Size of the data store where the cache information is kept
	Error Methodology	Error correction scheme supported by this cache component, for example, Parity/ Single Bit ECC/MultiBit ECC
	Level	Indicates the cache level; internal cache that is built in to the microprocessors; external cache that is between the CPU and DRAM
	Line Size	Size in bytes of a single cache bucket or line
	Read Policy	Indicates whether the data cache is for read operations
	Replacement Policy	Algorithm that the cache uses to determine which cache lines or buckets should be reused
	Speed	Speed of this System Cache module in nanoseconds
	Write Policy	Indicates the two different ways (Write-Back and Write-Through Cache) that the cache can handle to write to the memory
 Hardware/Software Inventory >  System >  System DMA	Availability	Indicates whether Virtual Direct Memory Access (DMA) is supported
	Description	Name of the logical device that is currently using this DMA channel
	DMA Burst Mode	A data transmission mode in which data is sent faster than normal
	DMA Channel Number	Number of the Direct Memory Access (DMA) channel that a computer uses for transferring data to and from devices quicker than from computers without a DMA channel
 Hardware/Software Inventory >  System >  System Slot	Description	Card currently occupying this slot
	Maximum Data Width	Maximum bus width of cards accepted in the slot
	Thermal Rating	Maximum thermal dissipation of the slot in milliwatts

Scan Data Group	Scan Data Item	Description
 Hardware/Software Inventory >  System >  Motherboard	Manufacturer	Name of the motherboard manufacturer
	Number of Slots	The number of expansion slots in the motherboard for adding more memory, graphic capabilities, and support for special devices
	Version	Version of the motherboard
	Description	General description of the motherboard

NOTE: For an enumerated attribute, the value is displayed in the format *enumerated_value* [*enumerated_ID*]. For example, Processor.Processor Family = Pentium (R) III [17].

The Status bar displays the following information:

- **Tree Name:** Displays the eDirectory tree name where the inventoried workstation resides.
- **Recent Information:** Set to Yes if the Inventory database has been updated with the latest inventory information of the selected inventoried workstation.

77.1.3 Viewing Inventory Information by Querying the Database

Using ConsoleOne, you can query the Inventory database to display the hardware and software components of inventoried workstations that you want to view. The Inventory Query window displays the information satisfying the criteria you specify.

The Inventory database stores inventory information (general, hardware, software, network, and system information) for each inventoried workstation. Querying the Inventory database helps to create groups of similar devices and to focus your reports on specific types of machines. For example, you can query the database to find machines that have an i486D processor and a VGA card.

To query the Inventory database for inventory information:

- 1 In ConsoleOne, select a container.
- 2 Invoke the query.
 - To invoke the Inventory query from a database object, right-click the database object, click *ZENworks Inventory*, then click *Inventory Query*.
 - To invoke the Inventory query from the ConsoleOne *Tools* menu, you must first configure the Inventory database, then click *Tools*, click *ZENworks Inventory*, then click *Inventory Query*. For more information on how to configure the Inventory database, see [Section 77.1.1, “Configuring the Inventory Database,” on page 1096](#).
- 3 Specify the criteria for the query:

Query the Inventory database for: By default, the *Workstations* option is enabled. The query locates all inventoried workstations satisfying the query expression. If ZENworks 7 Server Management and ZENworks 7 Desktop Management are installed in the same environment, then the *Workstations*, the *Servers*, and *Both* options are available. When you select

Workstations, the query locates all inventoried workstations satisfying the query expression. Choose *Both* to include all inventoried workstations and inventoried servers satisfying the query expression.

Find Type: Select *Simple* or *Advanced*. Click *Simple* to specify a simple query. When you choose a *Simple* query, you specify one attribute, relational operators, and the value of the attribute. Choose *Advanced* query to specify many attributes. You can combine multiple query groups so each group defines a set of query criteria. For example, use the Advanced query to run a query to discover all devices in the database with 486 processors and use query connectors, and add another query to discover which of these inventoried workstations have a VGA color video adapter.

Display Machine(s) Not Satisfying the Query: Select the check box to retrieve machines that do not satisfy the query.

Attribute: Select the component or component attributes. Attributes that you can specify to query on the inventoried workstations are grouped into the following categories: General, Software, Hardware, Network, and System.

The custom attribute is prefixed by an asterisk (*).

For example, to find the machines that do not have a pointing device installed, select Pointing Device as the component. To specify the version of BIOS as a component in the query, select BIOS as the component and VERSION as the component attribute.

Operator or Relational Operator: Select to determine the relationship between the components and the value. The relational operators are grouped on the basis on the data type of the attribute selected in the Select Attribute window as shown in the following table:

Data Type of the Attribute	Relational Operators
String	Equal To (=), Not Equal To (!=), Matches ([]), Does Not Match (![]) and Is NULL (null)
Numeric	Equal (=), Not Equal (!=), Less Than (<), Less Than or Equal To (<=), Greater Than (>), Greater Than or Equal To (>=), and Is NULL (null)
Date	After (>), On or After (>=), Before (<), On or Before (<=), and Is NULL (null)
Enum	Equal To (=), Not Equal To (!=), and Is NULL (null)
Custom	Includes all the relational operators that are grouped under the String, Numeric, and Date data types

For more information on using the relational operators, see [“Using Relational Operators” on page 1111](#).

NOTE: If the query does not display the result when the data type of the attribute is Custom and the relational operator is Numeric or Date, use the Equal To operator to find the values for the custom attributes that are stored in the Inventory database.

If you select only the component in the Select Attribute window, the Relational Operator is set to NULL by default and other relational operators are not available.

Value: Description values are the possible values of an inventory component. For example, 6.0 is a possible value for the DOS-Version attribute. Description values are not case sensitive.

NOTE: For an enumerated attribute, the value is displayed in the format, *enumerated_value* [*enumerated_ID*]. For example, Processor.Processor Family = Pentium (R) III [17].

If you choose Matches ([]) or Does Not Match (![]) as the relational operator, you can use wildcards to substitute characters in the Value field. The following table lists the wildcards that can be used according to the SQL documentation:

Example	Specifies to Include
?	Any one character
_ (underscore)	Any one character
%	Any string of zero or more characters
[]	Any one character in the specified range or set
[^]	Any one character not in the specified range or set

NOTE: To define a query using special characters such as ? or [, specify the query in the following formats: [?] or [[]].

The list of description values displayed for an Inventory component is taken from the Inventory database corresponding to the component.

Logical Operator: This option is available only for the Advanced query. Logical Operator forms query groups that is combined with the previous query group by using the relational operator specified between the query groups.

Save: This option is available only for the Advanced query. It saves the query expression as a file in the location that you specify. The query file does not have a default extension; however, we recommend the .qry extension for easy reference.

Load: This option is available only for the Advanced query. It loads the query file that you specify. You must provide the full filename with its extension.

4 Click *Find*.

This will query based on the query criteria you specify and display the inventoried workstations that match the query in the Query Results window.

In the Query Results window, double-click the inventoried workstation or click *File*, then click *Advanced Inventory* to view the inventory information of the inventoried workstation.

Using Relational Operators

- **Match:** Use the Match operator to find the inventoried workstations that satisfy the query condition.

For example, use the Match operator to find all the inventoried workstations with IP address 164.99.151.%,

- **NULL:** Use the NULL operator to query for those inventoried workstations whose particular attribute is not scanned but the component has been scanned and some attributes are populated.

For example, to find a list of inventoried workstations for which BIOS.Manufacturer is not scanned, form a BIOS.Manufacturer is NULL query. This query displays the inventoried workstations for which the BIOS has been scanned.

- **NOT SATISFYING:** Use the NOT SATISFYING query (or the NOT SATISFYING filter condition) to find filter conditions for the inventoried workstations that negate the given query. For example, two workstations W1 and W2 contain serial ports COM1 and COM2. The query (SerialPort='COM1') returns W1 and the query (SerialPort!='COM1') also returns the W1 because W1 contains the serial port COM2. To query the inventoried workstations that do not contain the serial port COM1 you must use <NOT SATISFYING>(SerialPort='COM1'). To use the NOT SATISFYING option, click the Display Machines Not Satisfying the Query check box in the query window.

77.1.4 Viewing the Minimal Inventory Information from an eDirectory Object

The Scanners store minimal inventory information as an eDirectory Workstation object. You can view this minimal information from ConsoleOne. The Minimal Information page lists the inventory information of the scanned inventoried workstations.

For more information about the listed items in this page, see [“Mapping Between Minimal Information Attributes and Attributes in the Inventory Database” on page 1112](#).

To view the inventory information stored in eDirectory:

- 1 Right-click an inventoried workstation that has been successfully scanned, click *Properties*, click the *ZENworks Inventory* tab, then click *Minimal Information*.

If you click the More Workstation Information button in this page, the [Workstation Inventory window](#) is displayed.

Mapping Between Minimal Information Attributes and Attributes in the Inventory Database

The following table shows the mapping between minimal information attributes and attributes in the Inventory database:

Table 77-2 Mapping between Minimal information attributes and attributes in the Inventory database

Minimal Information	Inventory Database
Asset Tag	Scanned Inventory - Asset Tag
BIOS Type	Hardware - BIOS - Type
Computer Model	Scanned Inventory.Computer Model
Computer Type	Scanned Inventory.Computer Type
Disk Information	Hardware - Disk - Hard Disk - Drive Letter
IP Address	Network - IP Address
IPX Address	Network - IPX Address
Last Scan Date	Date and time when the inventoried workstation was scanned
MAC Address	Network - MAC Address

Minimal Information	Inventory Database
Memory Size	Hardware - Memory - Total Extended Memory
Model Number	Scanned Inventory.Model Number
NIC Type	Hardware - Network Adapter Driver - Description
Novell Client	Novell Client version
OS Type	Software - Operating Systems - OS - Name
OS.Version	Software - Operating Systems - OS - Version
Processor	Hardware - Processor
Serial Number	Workstation Serial Number
Subnet Mask	Network - Subnet Mask
Video Type	Hardware - Display - Type

77.1.5 Running Inventory Reports

You can run reports to gather inventory information from the Inventory database. The Inventory reports are designed using Crystal Reports*.

You can select from a predefined set of report forms to generate a report.

You can print or export the report as desired. Remember that any reports you generate would be empty if you have not configured ZENworks 7 Desktop Management to start populating the Inventory database with the information you want.

This section covers the information on the following topics:

- [“Prerequisites for Generating Inventory Reports” on page 1113](#)
- [“Types of Inventory Reports” on page 1113](#)
- [“Generating Inventory Reports” on page 1122](#)
- [“Understanding the Proxy Database” on page 1124](#)
- [“Printing an Inventory Report” on page 1125](#)
- [“Exporting an Inventory Report to a File” on page 1125](#)
- [“Understanding User-Defined Reports” on page 1126](#)

Prerequisites for Generating Inventory Reports

Before running the inventory reports, make sure that you have installed the appropriate ODBC client. For more information, see the *Novell ZENworks 7 Desktop Management Installation Guide*.

Types of Inventory Reports

You can generate the types of reports described below, assuming you have already configured ZENworks 7 Desktop Management to start populating the Inventory database with the information you want. The following table lists the Simple Inventory lists that provide information on individual aspects of Workstation Inventory, such as operating systems and their selection criteria. The table

also lists the Comprehensive Inventory Reports that combine several aspects of Workstation Inventory into each report, such as memory, hard disk, and processor.

The following table lists the Inventory reports, and also provide information on individual aspects of each report such as the selection criteria and the information displayed in the report.

Table 77-3 *List of Inventory reports and information displayed by each report*

Inventory Report Group	Report Name	Selection Criteria	Information Displayed in the Inventory Report
Hardware Inventory	Asset Management Report	Scope, Machine Name, IP Address, and DNS Name You can also select to display the following options in the report: Memory, Processor, Display Adapter, Keyboard, Pointing Device, Fixed and Removable Disk, Floppy, CDROM, Network Adapter, and Monitor	Memory, processor, display details, keyboard, pointing device, fixed and removable disk, floppy, CD drive, network adapter, and monitor details for inventoried workstations.
	BIOS Listing	Scope, Machine Name, IP Address, DNS Name, BIOS Install Date, and Manufacturer	List of all the inventoried workstations with BIOS manufacturer, BIOS release date, and the total number of such machines.
	Battery Listing	Scope, Machine Name, IP Address, DNS Name, and Name	List of all inventoried workstations that match the specified battery name.
	Bus Listing	Scope, Machine Name, IP Address, DNS Name, and Bus Type	List of all inventoried workstations with the selected bus type.
	CDROM Listing	Scope, Machine Name, IP Address, DNS Name, Caption, Description, and Manufacturer	List of all inventoried workstations that match the specified CD caption, description, and manufacturer's name.
	Display Adapter Listing	Scope, Machine Name, IP Address, DNS Name, Video Architecture, and Description	List of all inventoried workstations that match the specified display adapter's video architecture and description.
	Floppy Listing	Scope, Machine Name, IP Address, DNS Name, Manufacturer, and Description	List of all inventoried workstations that match the specified floppy description and manufacturer's name.

Inventory Report Group	Report Name	Selection Criteria	Information Displayed in the Inventory Report
	Hardware Summary Report	Scope, Machine Name, IP Address, DNS Name, Operating System Type, Operating System Version, Processor Family, Curr. Clock Speed (Lower Bound in MHz), Curr. Clock Speed (Upper Bound in MHz), Total Memory (Lower Bound in MB), Total Memory (Upper Bound in MB), Hard Disk Size (Lower Bound in GB), and Hard Disk Size (Upper Bound in GB)	Operating system name, operating system version, processor family, processor current clock speed, memory, and hard disk size for each inventoried workstation.
	Keyboard Listing	Scope, Machine Name, IP Address, DNS Name, Description, and Layout	List of all inventoried workstations that match the specified keyboard description and layout.
	Modem Listing	Scope, Machine Name, IP Address, DNS Name, and Name	List of all inventoried workstations that match the specified modem name.
	Monitor Listing	Scope, Machine Name, IP Address, DNS Name, Manufacturer, Manufacture Date, Nominal Size (Lower Bound in inches), and Nominal Size (Upper Bound in inches)	List of all inventoried workstations that match the specified monitor manufacturer's name, manufacture date, and the specified range of monitor's nominal size.
	Network Adapter Listing	Scope, Machine Name, IP Address, DNS Name, and Name	List of all inventoried workstations that match the specified network adapter's name.
	Physical Disk Listing	Show Chart, Scope, Machine Name, IP Address, DNS Name, Removable, Manufacturer, Description, Total Size (Lower Bound in GB), and Total Size (Upper Bound in GB)	<p>List of all inventoried workstations that match the specified physical disk manufacturer's name, description, the specified range of total size and disks that are fixed, removable, or both.</p> <p>You can also select the Show Chart box to display the Physical Disk Listing report in a pie chart.</p>
	Pointing Device Listing	Scope, Machine Name, IP Address, DNS Name, Pointing Device Type, and Pointing Device Name	List of all inventoried workstations that match the specified pointing device type and name.
	Power Supply Listing	Scope, Machine Name, IP Address, DNS Name, and Description	List of all inventoried workstations that match the specified power supply description.

Inventory Report Group	Report Name	Selection Criteria	Information Displayed in the Inventory Report
	Processor Listing	Show Chart, Scope, Machine Name, IP Address, DNS Name, Processor Family, Maximum Speed (Lower Bound in MHz), Maximum Speed (Upper Bound in MHz), Current Speed (Lower Bound in MHz), and Current Speed (Upper Bound in MHz)	<p>List of all the inventoried workstations with a processor family (such as Pentium Pro), processor maximum clock speed, and the processor current clock speed of the machines.</p> <p>You can also select the Show Chart box to display the Processor Listing report in a pie chart.</p>
	Sound Adapter Listing	Scope, Machine Name, IP Address, DNS Name, and Name	List of all inventoried workstations that match the specified sound adapter name.
	Storage Devices Inventory Report	Scope, Machine Name, IP Address, and DNS Name You can also select to display the following options in the report: Fixed and Removable Disk, Logical Disk, Floppy, and CDROM.	Fixed disk, removable disk, logical disk, floppy, and CD drive details for each inventoried workstation.
	System Chassis Listing	Scope, Machine Name, IP Address, DNS Name, Chassis Type, and Manufacturer	List of all inventoried workstations that match the specified system chassis type and manufacturer's name.
System Configuration Inventory	Inventory Scan Listing	Show Chart, Scope, Machine Name, IP Address, DNS Name, Last Scan Date (On or Before), Inventory Server Name, and Recent Information	<p>Date and time of the last inventory scan, Inventory server name, and recent information on each inventoried workstation.</p> <p>You can also select the Show Chart box to display the System Configuration Inventory report in a pie chart.</p>
	Memory Listing	Show Chart, Scope, Machine Name, IP Address, DNS Name, Total Memory (Lower Bound in MB), and Total Memory (Upper Bound in MB)	<p>List of all the inventoried workstations within a range of memory size (such as 200-400 MB) and the total number of such machines.</p> <p>You can also select the Show Chart box to display the Memory Listing report in a pie chart.</p>
	Operating System Listing	Show Chart, Scope, Machine Name, IP Address, DNS Name, Operating System Type, and Operating System Version	<p>List of all inventoried workstations that match the specified operating system type and version.</p> <p>You can also select the Show Chart box to display the Operating System Listing in a pie chart.</p>

Inventory Report Group	Report Name	Selection Criteria	Information Displayed in the Inventory Report
Software Inventory	Networking Information Report	Scope, Machine Name, IP Address, and DNS Name	Network adapter type, DNS, IP address, MAC address, IPX address, and Windows Domain name for each inventoried workstation.
	System Information Listing	Scope, Machine Name, IP Address, DNS Name, and Computer Manufacturer	List of all inventoried workstations that match the specified computer manufacturer's name.
	System Internal Hardware Inventory Report	Scope, Machine Name, IP Address, and DNS Name You can also select to display the following options in the report: System IRQ, System Cache, System DMA, System Slot, and Motherboard.	IRQ, cache, DMA, slot, and motherboard for each inventoried workstation.
	Add-Remove Programs by Application	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, and Software Name	List of all software that are listed in the Add/Remove Programs list for each inventoried workstation.
	Add-Remove Programs by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, and Software Name	List of all software that are listed in the Add/Remove Programs list for each inventoried workstation.
	Anti-Virus Signature Files by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, Software Name, Min Virus Definition Date and Max Virus Definition Date	List of all antivirus signature files grouped by antivirus product installed on each inventoried workstation.
	Anti-Virus Signature Machine Count	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, Software Name, Min Virus Definition Date and Max Virus Definition Date	List showing the count of inventoried workstations that have any antivirus product installed.
	Disk Usage by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, and File Extension	List of all inventoried workstations and the disk usage that match the specified file extension.
	Exception List by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, File Name, Vendor Name, and Product Name	List of all inventoried workstations and the file information that match the specified filename, vendor name, and product name.
	Installed NetWare Software by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, and Software Name	List of all inventoried NetWare machines and the products.dat details that match the given software name.

Inventory Report Group	Report Name	Selection Criteria	Information Displayed in the Inventory Report
	Internet Explorer Installation Count	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, Internet Explorer Version, and Service Pack	List showing the count of inventoried workstations with Internet Explorer installed.
	Internet Explorer Patches by Machine	Scope, Machine Name, IP Address, DNS Name, Internet Explorer Version, and Service Pack	List of all installed patches for the Internet Explorer version that matches the specified value and patch name.
	Internet Explorer by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, Internet Explorer Version, and Service Pack	List of all Internet Explorer installations that match the specified version.
	MSI Products by Application	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, Software Name, and Vendor Name	List of all products installed on each inventoried workstation and that are listed in the MSI (Microsoft Installer) database.
	MSI Products by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, Software Name, and Vendor Name	List of all products installed on each inventoried workstation and that are listed in the MSI (Microsoft Installer) database.
	Microsoft Office Components by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, Microsoft Office Version, and Service Pack	List of all products that match the specified product name and vendor name, and have been installed from the specified source.
	Microsoft Office Installation Count	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, Microsoft Office Version, and Service Pack	List showing the count of inventoried workstations with Microsoft Office installed.
	Microsoft Office by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, Microsoft Office Version, and Service Pack	List of all Microsoft Office installations that match the specified version.
	Novell Client Components by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, Novell Client Version, and Service Pack	List of all Novell Client components that match the specified version.

Inventory Report Group	Report Name	Selection Criteria	Information Displayed in the Inventory Report
	Novell Client Installation Count	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, Novell Client Version, and Service Pack	List showing the count of inventoried workstations with Novell Client installed.
	Novell Client by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, Novell Client Version, and Service Pack	List of all Novell Client installations that match the specified version.
	Outlook Express Installation Count	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, and Outlook Express Version	List showing the count of inventoried workstations with Outlook Express installed.
	Outlook Express by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, and Patch Name	List of all Outlook Express installations that match the specified version.
	Software Dictionary Application Files by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, Vendor Name, Software Name, and Software Version	List of all inventoried workstations and their software dictionary application files that match the specified vendor, software, and software version.
	Software Dictionary Applications by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, Vendor Name, Software Name, and Software Category	List of all inventoried workstations and their software dictionary applications that match the specified vendor, software, and software version.
	Software Dictionary Versions Machine Count	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, General Dictionary Version, and Private Dictionary Version	List showing the count of all inventoried workstations with specified General Dictionary and Private Dictionary versions.
	Software Dictionary Versions by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, General Dictionary Version, and Private Dictionary Version	List of all inventoried workstations with specified General Dictionary and Private Dictionary versions.
	Software Installation Count	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, Vendor Name, Software Name, and Software Version	List showing the count of inventoried workstations with specified vendor name, software, and version.

Inventory Report Group	Report Name	Selection Criteria	Information Displayed in the Inventory Report
	Software Installations	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, Vendor Name, Software Name, and Software Version	List of all inventoried workstations with specified vendor name, software, and version.
	Software by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, Vendor Name, Software Name, and Software Version	List of all inventoried workstations and software information that match the specified vendor name, software, and version.
	System Software Inventory Report	Scope, Machine Name, IP Address, and DNS Name. You can also select to display the following options in the report: Display Driver, Pointing Device Driver, Network Adapter Driver, and NetWare Client.	Drivers (such as pointing device drivers, network adapter drivers, and display drivers) and Novell NetWare Client for each inventoried workstation.
	Windows Components by Machine	Scope, Machine Name, IP Address, DNS Name, Windows Version, and Service Pack	List of all Windows components that match the specified version.
	Windows Installation Count	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, Windows Version, and Service Pack	List showing the count of inventoried workstations that have Windows operating system installed.
	Windows Media Player Count	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, and Windows Media Player Version	List showing the count of inventoried workstations with Windows Media Player installed.
	Windows Media Player Patches by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, and Windows Media Player Version	List of all patches for Windows Media Player installations that match the specified version and patch name.
	Windows Media Player by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, and Windows Media Player Version	List of all Windows Media Player installations that match the specified version.
	Windows Operating System by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, Windows Version, and Service Pack	List of all Windows operating systems that match the specified version and serial number.

Inventory Report Group	Report Name	Selection Criteria	Information Displayed in the Inventory Report
	Windows Security Patches by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, Windows Version, and Service Pack	List of all patches for Windows operating systems that match the specified version and patch name.
	Windows Security Patches by Patch	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, Max Last Scan Time, Windows Version, and Service Pack	List of all patches for Windows operating systems that match the specified version and patch name.
	Novell ZENworks Desktop Management Installed Agent Components by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, and Max Last Scan Time	List of all machines that were successfully last scanned within the specified time range and the agent components of ZENworks 7 Desktop Management installed on these machines.
	Novell ZENworks Desktop Management Installed Server Components by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, and Max Last Scan Time	List of all machines that were successfully last scanned within the specified time range and the server components of ZENworks 7 Desktop Management installed on these machines.
	Novell ZENworks Handheld Management Installed Components by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, and Max Last Scan Time	List of all machines that were successfully last scanned within the specified time range and the ZENworks 7 Handheld Management components installed on these machines.
	Novell ZENworks Installed Components by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, and Max Last Scan Time	List of all machines that were successfully last scanned within the specified time range and the ZENworks 7 components installed on these machines.
	Novell ZENworks Installed Suites by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, and Max Last Scan Time	List of all machines that were successfully last scanned within the specified time range and the ZENworks 7 suites installed on these machines.

Inventory Report Group	Report Name	Selection Criteria	Information Displayed in the Inventory Report
	Novell ZENworks Server Management Installed Agent Components by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, and Max Last Scan Time	List of all machines that were successfully last scanned within the specified time range and the agent components of ZENworks 7 Server Management installed on these machines.
	Novell ZENworks Server Management Installed Server Components by Machine	Scope, Machine Name, IP Address, DNS Name, Min Last Scan Time, and Max Last Scan Time	List of all machines that were successfully last scanned within the specified time range and the server components of ZENworks 7 Server Management installed on these machines.
Others	User Defined Reports For more information on how to create user-defined reports, see the “Understanding User-Defined Reports” on page 1126.	Based on the options specified by the user in the <code>consoleone\consoleone_version\bin\userreports.ini</code> file	Displays the user-defined report.

NOTE: The Show Chart selection criteria display a graphical representation of the Inventory report.

Generating Inventory Reports

- 1 Invoke the Inventory report using any of the following methods:
 - To invoke the Inventory report from a database object, right-click the database object, then click *Reporting*.
 - To invoke the Inventory report from the ConsoleOne *Tools* menu, you must first configure the database, click *Tools*, then click *ZENworks Reports*. For more information on how to configure the Inventory database, see [Section 77.1.1, “Configuring the Inventory Database,”](#) on page 1096.
- 2 Click the report you want to generate.
The description for the report is displayed on the right side of the screen.
See the table with listing of simple Inventory lists and listing of the comprehensive inventory reports.
- 3 Specify the selection criteria.

The *Scope* selection criteria is enabled only if both ZENworks 7 Desktop Management and ZENworks 7 Server Management are installed on the same machine.

For example, if you want to view the inventory information of all inventoried workstations, select Workstation as the scope selection criteria. The report displays the inventory information of all inventoried workstations within the configured Inventory database.

Based on the type of report you want, you can filter the information. For example, to view all inventoried workstations that have the Windows 2000 operating system, you would select Operating System Listing, specify the selection criteria scope as Both, and the operating system type as Windows 2000.

Depending on the type of report you want, you can filter the information.

Follow these guidelines as you work with the Reporting dialog:

- The selection criteria in the Inventory report is case-sensitive.
- If the Reporting dialog box allows wildcards, you can use an asterisk (*) or question mark (?) with all selection criteria. The wildcard characters can be used for text fields only.

You can use * to retrieve the remaining entire text of a string where as ? can be used to retrieve only one character of a string.

Example 1: Lets assume that a machine name is "workstation1". If you query using work*, then workstation1 is found. If you query using work?, then the machine is not found. To find workstation1 using the ?, you must query using work??????, where each ? represents a character.

Example 2: Lets assume that the machine name is "CN=MACHINE1.OU=ENG.O=NOVELL.T=TREE". To find the machine, you can query by using "CN=MA*.OU=ENG.O=NOVELL.T=TREE" or CN=MA*. The machine name can be queried partly also. If you want to query by "O=novell.T=TREE", use * as "*O=novell.T=TREE".

The following table lists examples of wildcards.

Example	Specifies to Include
*	All items
164.99.*	All items starting with 164.99.
164.9?.215.23	All items starting with 164.9, followed by any character, and ending with ".215.23"
164.96.215.23	The single named item, in this case the inventoried workstation with the specified IP address

4 Click *Run Selected Report*.

A status box appears, displaying the progress of the report generation. When the report is generated, it appears in the viewer. Use the buttons on the toolbar to page through, print, or export the report.

NOTE: ZENworks Inventory report supports only the following double-byte character languages: German, English, Spanish, French, Portugese, and Japanese. Other double-byte characters might not be displayed properly in the Inventory reports.

Understanding the Proxy Database

When you run the reports from a non-English management console on a Sybase Inventory database running on NetWare, the Sybase database starts on the console on invoking the selected report. This is called the ZENworks 7 Desktop Management proxy database.

A *Sybase ASA* icon is displayed in the system tray of the management console as soon as you run the selected report. The proxy database automatically connects to the remote database on which the reports are being invoked and retrieves the required information. Because the data in the remote database (Sybase running on NetWare) is stored in UTF-8 format and Crystal Reports cannot display the characters encoded in UTF-8 format, the proxy database converts all UTF-8 data into the local Windows language character set.

The following sections provide information on:

- “Invoking the Proxy Database” on page 1124
- “Shutting Down the Proxy Database” on page 1124
- “Configuring the Proxy Databases to Run on Ports Other Than the Default Ports” on page 1125

Invoking the Proxy Database

The proxy database is invoked in the following scenarios:

- If reports are invoked from a non-English management console on the ZENworks 7 Desktop Management or ZENworks for Desktops 4.x Sybase Inventory database running on NetWare.
- If reports are invoked from a non-English management console on the ZENworks for Desktops 4.x Sybase Inventory database running on Windows.

The proxy database is not invoked in the following scenarios:

- If reports are invoked from an English management console.
- If reports are invoked from a non-English management console on the ZENworks 7 Desktop Management or ZENworks for Desktops 4.x Inventory database mounted on Oracle or MSSQL 2000 database.
- If reports are invoked from a non-English management console on the ZENworks 7 Desktop Management Sybase Inventory database running on Windows.
- If any inventory components other than reports are invoked.

Two proxy databases can be mounted simultaneously; one for the ZENworks 7 Desktop Management database and, the other for the ZENworks for Desktops 4.x database.

Shutting Down the Proxy Database

If you close the Reporting dialog box or if you close ConsoleOne, you must manually shut down the proxy database.

To manually shut down the proxy database:

- 1 In the management console, right-click the proxy database icon located in the system tray, then click *Exit*.

Configuring the Proxy Databases to Run on Ports Other Than the Default Ports

If the default ports that are used by Sybase are also used by other applications, there might be potential port conflicts. To avoid this, you can configure the proxy database to run on ports other than the default ports.

- 1 Bring up Proxy DB on Port 2639/2640 depending on the database port with the database messages redirected to a file.

If 2639/2640 are already blocked by some other application, then Sybase mounts the proxy database on a free port that it finds and puts this information in the output file. On trying to connect, “Unable to connect...” error message is displayed.

- 2 Exit Proxy Sybase, get the port number from the output file, and enter the port number into the Proxy Ports configuration file
(`Consoleone\1.2\bin\zen\sybaseproxy\proxyproperties.properties`)
- 3 Invoke the reports again, so Sybase reads the proxy ports configuration file, get the port, and start Sybase in the specified port.

The Reporting snap-in modifies ODBC DSN with the new port information.

- 4 Restart ConsoleOne for the changes to take effect.

Printing an Inventory Report

- 1 **Generate and view the report.**
- 2 To change the default settings of the Printer, click the *Printer Setup* icon and modify the settings.
- 3 Click the *Printer* icon.

Exporting an Inventory Report to a File

- 1 **Generate and view the report.**
- 2 On the toolbar, click the *Export Report* icon.
- 3 In the Export dialog box, specify the location and file format.

If you choose to export the Inventory report to a text file, in the Export to Text dialog box, select the *User Defined* option and set the value to 16 because the data exported is truncated if the value is less than 16.

If you want to export the Inventory report to an HTML file, you can select *HTML 3.2* or *HTML 4.0 (DHTML)* file format. We recommend that you export to HTML 4.0 (DHTML) because the data exported to HTML 3.2 is not formatted properly.

If you want to export the Inventory report to a comma-separated value (.csv) file, do the following:

- 3a Export the report to Microsoft Excel.

NOTE: If you choose to export to .csv at this point, the report is not properly exported.

- 3b Open the .xls file.

- 3c Click *File*, then click *Save As*.

- 3d In the *Save as type* field, choose *CSV (Comma delimited) (*.csv)*.

- 3e Click *Save*.

- 4 Click *OK*.
- 5 Browse for and select the directory where you want to save the exported file.
- 6 Click *OK*.

Understanding User-Defined Reports

You can use the Crystal Report Designer to generate reports displaying information in the Inventory database.

Before generating the reports, you must make sure that the report file (.rpt) is created using Crystal Report Designer 8.0/8.5. For more information on how to create a .rpt file, see the Crystal Report documentation.

IMPORTANT: Except for the Software Inventory reports, you can use any Inventory report as a template to create a report.

To generate the User-defined Inventory report:

- 1 On the machine where you are designing the report, set the ODBC DSN name to ZenInventory.
 - 1a Click *Start*, click *Settings*, then click *Control Panel*.
 - 1b Double-click *ODBC Data Sources (32 Bit)*, then click *Add*.
 - 1c Select the ODBC driver for the database you want to connect to.
 - 1d Click *Finish*.
 - 1e Specify the Data Source name as ZenInventory and specify the details.

NOTE: If you want to specify a data source name other than ZenInventory, you must configure the ODBC name on each of the machines where you invoke user-defined reports through ConsoleOne.

- 2 After you have designed the report, place the report in the
 \consoleone\version\reporting\canned\novellreporting\
 zeninventory\locale directory.

Where *locale* can be EN for English language reports, FR for French language reports, PT_BR for Portuguese-Brazilian language reports, DE for German language reports, and ES for Spanish language reports. The non-English reports are displayed based on the respective locale of the machine.

- 3 Set the values in the `userreports.ini` file in the `\consoleone\version\bin` directory. The `userreports.ini` file must contain the following values:

```
#[ReportName] <actual name of the rpt file without the .rpt
extension>

#DisplayName=User Defined Report's display name
#Param1=Constant,Display name,<if combo then {val-1|val-2|val-3}>
#<where Param1 is the internal name of the parameter as stored in
the .rpt file>

#<Constants are 1, 2 and 3 for Combo selection, text field and
numeric field respectively>
```

For example, you can set the value as given below:

```
[ListSystemInformation]DisplayName=System Information
```

```
Role=1,Role,{2|3|5}
```

```
IPAddress=2,IP Address
```

```
DNName=2,Distinguished Name
```

```
DNTree=2,Distinguished Tree
```

```
DNSName=2,DNS Name
```

```
[ListMemory]
```

```
DisplayName=Memory
```

```
Role=1,Role,{2|3|5}
```

```
IPAddress=2,IP Address
```

```
DNName=2,Distinguished Name
```

```
DNTree=2,Distinguished Tree
```

```
DNSName=2,DNS Name
```

```
MemoryLowerLimit=3,Memory Lower Bound
```

After you set the values in the `userreports.ini` file, the user defined report is displayed in the inventory reports tree. You can specify multiple reports in the `userreports.ini` file.

NOTE: If the `userreports.ini` file is empty, the user cannot view the user-defined reports in the inventory reports tree.

4 Click *Run Selected Report*.

77.1.6 Quickly and Easily Viewing the Inventory Data Using Quick Reports

In ZENworks 7, Workstation Inventory provides a new tool called Quick Reports to easily retrieve and view the data from the ZENworks Inventory database. Each Quick Report contains a list of inventory attributes and a query that you define using the Quick Report wizard.

The following sections provide more information about working with Quick Report:

- “Invoking the Quick Report Wizard” on page 1127
- “Creating a Quick Report” on page 1128
- “Modifying an Existing Quick Report” on page 1131
- “Viewing the Data Retrieved by the Quick Report” on page 1132
- “Deleting a Quick Report” on page 1134
- “Configuring the Inventory Database” on page 1135
- “Working with the Query Results Window” on page 1136

Invoking the Quick Report Wizard

Invoke the Quick Report Wizard using any of the following methods:

- To invoke the Quick Report from a database object, right-click the database object, click *ZENworks Inventory*, then click *Quick Report*.

- To invoke the Quick Report from the ConsoleOne *Tools* menu, click *ZENworks Inventory*, then click *Quick Report*.

If you have already configured the Inventory database, the Quick Report wizard uses that database.

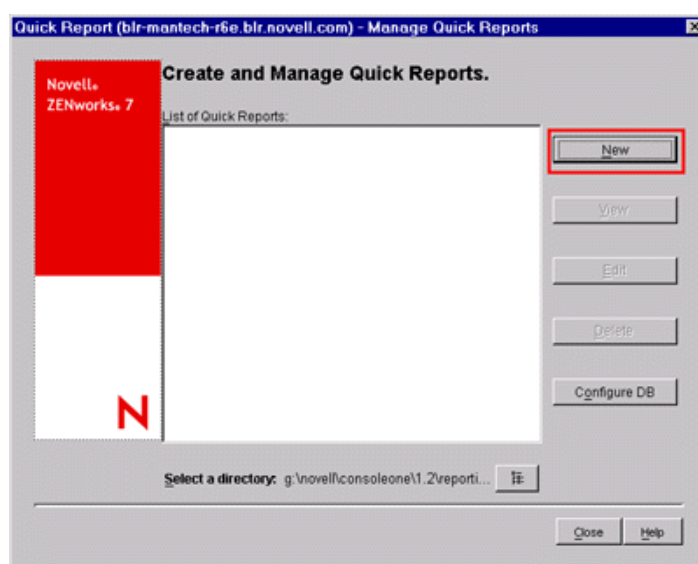
If you have not yet configured the Inventory database, the Quick Report wizard is displayed, and you can configure the database using the wizard. For more information, see “[Configuring the Inventory Database](#)” on page 1135.

Creating a Quick Report

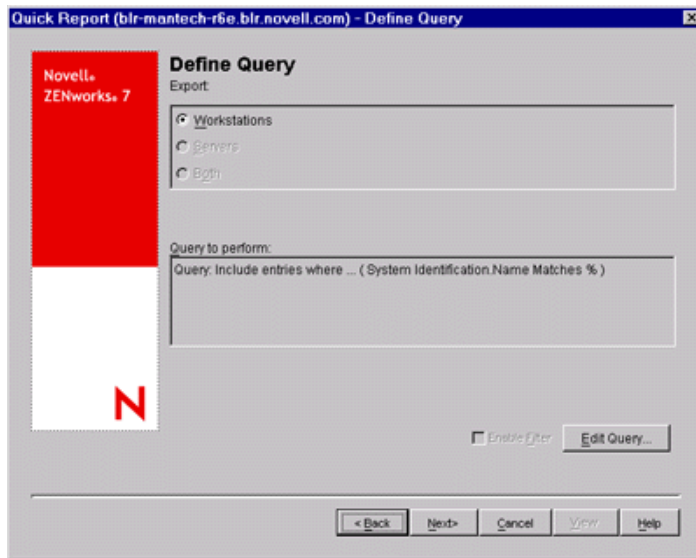
- 1 Invoke the Quick Report wizard.

The Create and Manage Quick Reports page is displayed.

- 2 Click *New*.



- 3 In the Define Query page, define the query criteria and specify the scope for viewing the data from the Inventory database.



You can use either the default query or define a new query.

Using the Default Query:

To use the default query, click Next. The Quick Report is created with the default query: System Identification.Name Matches %.

Defining a New Query:

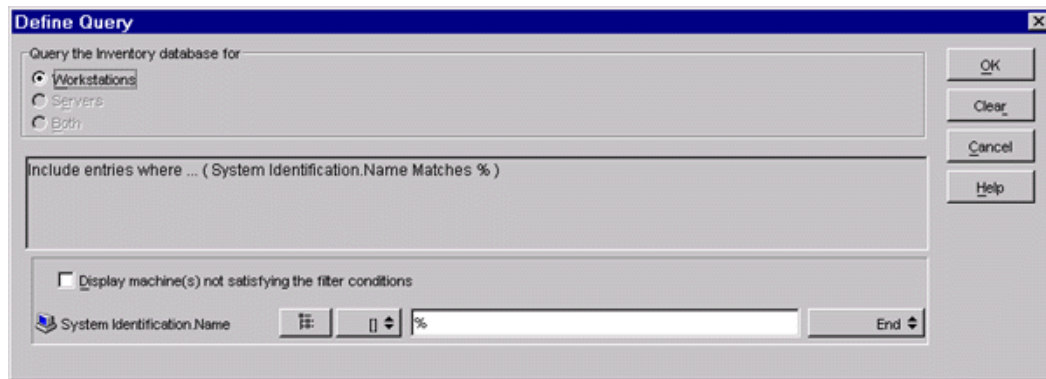
3a Select one of the following options.

- **Workstations:** Select this option to view the data satisfying the specified filter conditions for inventoried workstations. If you have only Desktop Management installed, this option is enabled by default and the other two options are unavailable.
- **Servers:** Select this option to view the data satisfying the specified filter conditions for inventoried servers. If you have only Server Management installed, this option is enabled by default and the other two options are unavailable.
- **Both:** Select this option to view the data satisfying the specified filter conditions for both inventoried servers and inventoried workstations. If you want to view data for inventoried workstations only, or for inventoried servers only, use one of the other query options. This option is available only if you have both ZENworks 7 Desktop Management and ZENworks 7 Server Management installed.

3b (Optional) If you want to apply the filter condition defined in the Define Query window, select the *Enable Filter* option.

This option is available only if you define the query using the following software classes and its attributes in the Define Query window: Software Group, Software Group File Information, Software Group Patch Information, Software, File Information, Patch Information, Exclude File Information, and Disk Usage.

3c Click *Edit Query* to change the query.

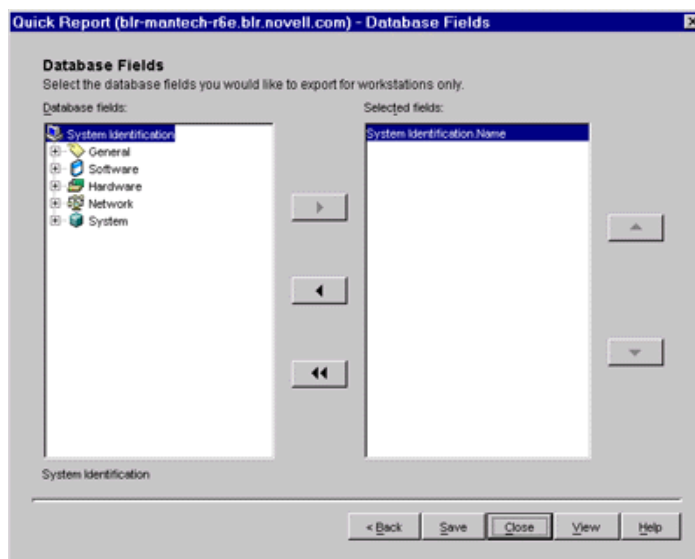


For detailed information on how to change the query, see [Section 77.1.3, “Viewing Inventory Information by Querying the Database,”](#) on page 1109.

3d Review the query and make changes as necessary. The Query to Perform pane displays the query you define.

3e Click *Next*.

4 In the Database Fields page, do the following:





4a From the *Database Fields* list, select the inventory attribute that you want to report.

By default, System Identification.Name is selected. You cannot deselect or change the order of this attribute.

4b Click  to add the selected inventory attribute to the Selected Fields list.

If you select a group attribute, all attributes of the group are added. For example, if you select the *Software* attribute, the *Software* attributes such as vendor name, product name, and version are included in the *Selected Fields* list.

4c To add an additional inventory attribute, repeat [Step 4a](#) and [Step 4b](#).

NOTE: You can change the order of the attributes using  and .

4d To view the report, click *View*.

The data is displayed in the Query Results window. For more information about the Query Results window, see “[Working with the Query Results Window](#)” on page 1136.

4e To save the report, click *Save*, specify the filename, and then click *OK*.

IMPORTANT: Only the saved Quick Reports are listed on the Create and Manage Quick Reports page.

4f Click *Close*.

Modifying an Existing Quick Report

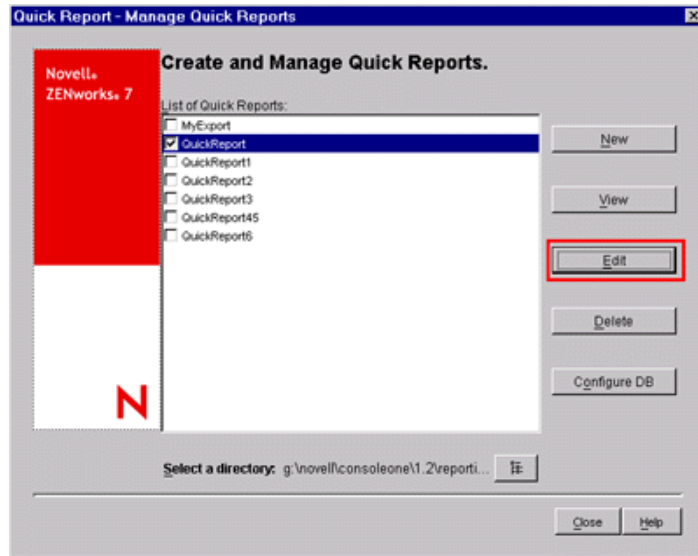
- 1** In the Create and Manage Quick Reports page, select the Quick Report that you want to modify from the list of Quick Reports.

You can modify only one Quick Report at a time.

By default, the list displays all the Quick Reports saved in the `ConsoleOne_installation_directory\consoleone\1.2\reporting\export` directory. To modify a Quick Report residing in another directory, click the *Browse* icon to browse and select the directory.

IMPORTANT: Only the saved Quick Reports are listed on the Create and Manage Quick Reports page.

- 2** Click *Edit*.



- 3** (Optional) In the Define Query page, change the existing query criteria and specify the scope for viewing the data from the Inventory database.

To define a new query:

3a Select one of the following options.

- **Workstations:** Select this option to view the data satisfying the specified filter conditions for inventoried workstations.

- **Servers:** Select this option to view the data satisfying the specified filter conditions for inventoried servers.
- **Both:** Select this option to view the data satisfying the specified filter conditions for both inventoried servers and inventoried workstations.

3b (Optional) If you want to apply the filter condition, select the *Enable Filter* option.

This option is available only if you define the query using the following software classes and its attributes in the Define Query window: Software Group, Software Group File Information, Software Group Patch Information, Software, File Information, Patch Information, Exclude File Information, and Disk Usage.

3c Click *Edit Query* to change the query.

For detailed information on how to change the query, see [Section 77.1.3, “Viewing Inventory Information by Querying the Database,” on page 1109](#).

3d Review the query and make changes as necessary. The Query to Perform pane displays the query you define.

3e Click *Next*.

4 (Optional) In the Database Fields page, do the following:



4a From the *Database Fields* list, select the inventory attribute that you want to report.

By default, *System Identification.Name* is selected. You cannot deselect or change the order of this attribute.

4b Click  to add the selected inventory attribute to the Selected Fields list.

If you select a group attribute, all attributes of the group are added. For example, if you select the *Software* attribute, the *Software* attributes such as vendor name, product name, and version are included in the *Selected Fields* list.

4c To add an additional inventory attribute, repeat [Step 4a](#) and [Step 4b](#).

NOTE: You can change the order of the attributes using  and .

4d To view the report, click *View*.

The report is displayed in the Query Results window. For more information about the Query Results window, see [“Working with the Query Results Window” on page 1136](#).

4e To save the report, click *Save*, specify the filename, and then click *OK*.

IMPORTANT: Only the saved Quick Reports are listed on the Create and Manage Quick Reports page.

4f Click *Close*.

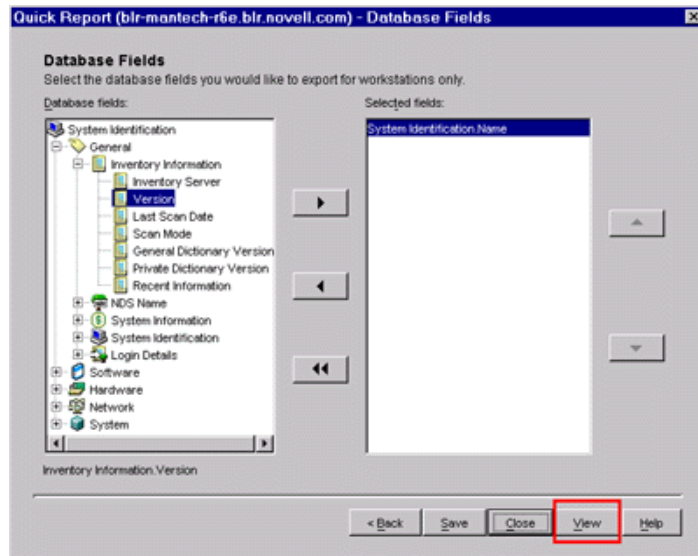
Viewing the Data Retrieved by the Quick Report

You can view the data retrieved by the Quick Report using any of the following methods:

- [“Viewing the Data While Creating or Modifying a Quick Report” on page 1133](#)
- [“Viewing the Data of a Saved Quick Report” on page 1133](#)

Viewing the Data While Creating or Modifying a Quick Report

- 1 In the Database Fields page, click *View*.



Viewing the Data of a Saved Quick Report

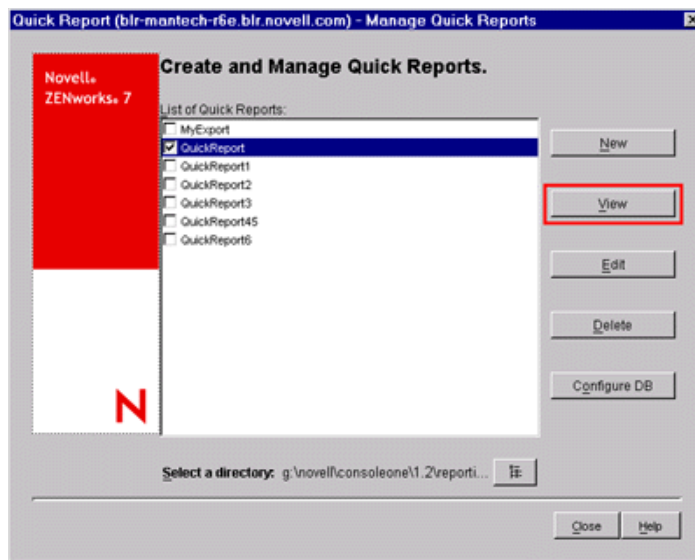
- 1 In the Create and Manage Quick Reports page, select the Quick Report that you want to view from the list of Quick Reports.

You can view only one Quick Report at a time.

By default, the list displays all the Quick Reports saved in the `ConsoleOne_installation_directory\consoleone\1.2\reporting\export` directory. To view a Quick Report residing in another directory, click the *Browse* icon to browse and select the directory.

IMPORTANT: Only the saved Quick Reports are listed on the Create and Manage Quick Reports page.

2 Click *View*.



The data is displayed in the Query Results window. For more information about the Query Results window, see [“Working with the Query Results Window” on page 1136](#).

Deleting a Quick Report

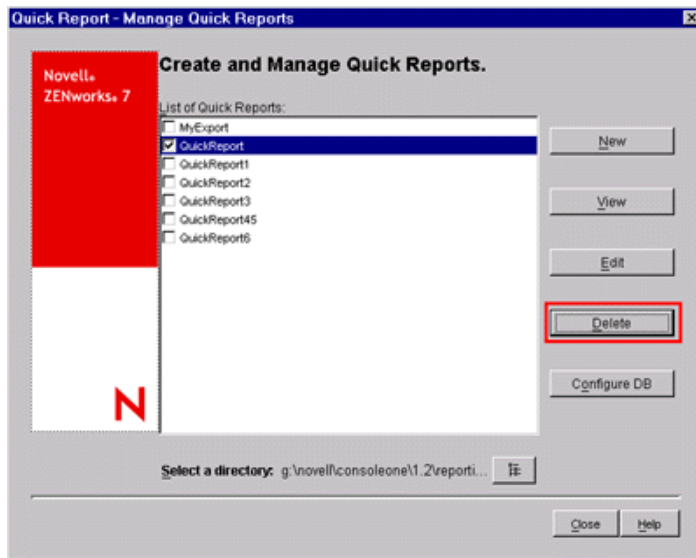
- 1 In the Create and Manage Quick Reports page, select the Quick Report that you want to delete from the list of Quick Reports.

You can select and delete multiple reports at a time.

By default, the list displays all the Quick Reports saved in the *ConsoleOne_installation_directory\consoleone\1.2\reporting\export* directory. To delete a Quick Report residing in another directory, click the *Browse* icon to browse and select the directory.

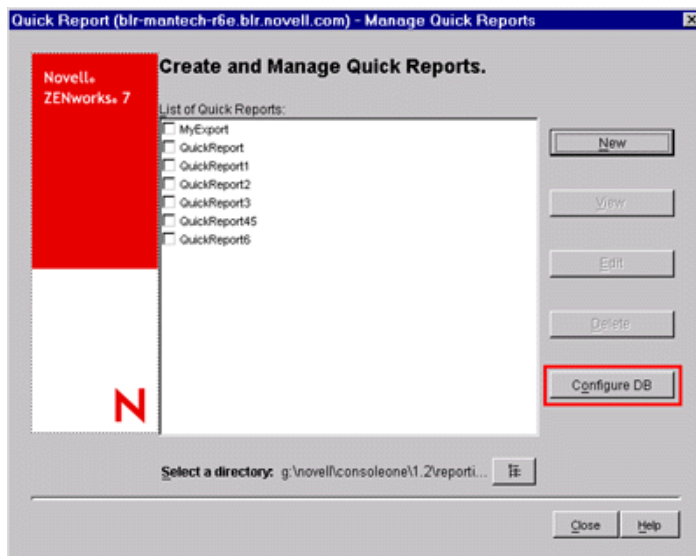
IMPORTANT: Only the saved Quick Reports are listed on the Create and Manage Quick Reports page.

- 2 Click *Delete*.



Configuring the Inventory Database

- 1 In Create and Manage Quick Reports page, click *Configure DB*.

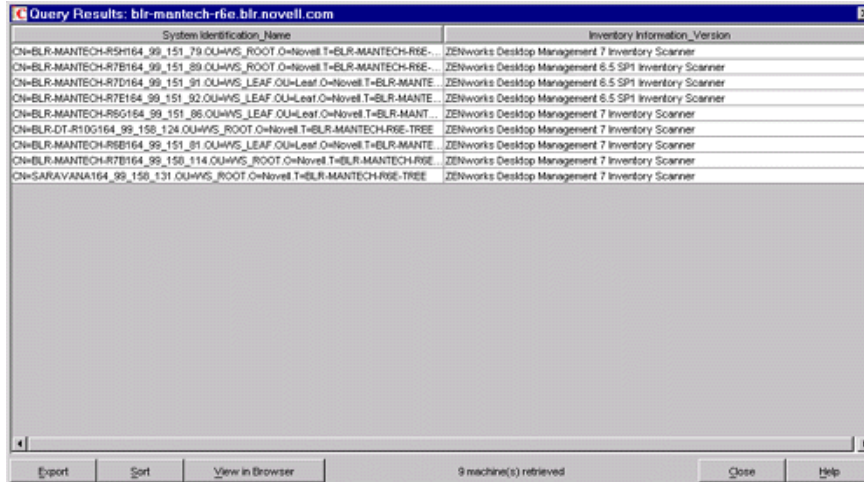


The Configure ZENworks Database window is displayed.

- 2 Click *Browse* to select an existing ZENworks database object from the list.
This database object contains the database settings such as the protocol, port in use by the database, and so forth.
- 3 Click *OK*.

Working with the Query Results Window

The Query Results window displays the data stored in the ZENworks Inventory database on querying the selected quick report. The Query Results window displays data for a maximum of 500 inventoried machines.



The screenshot shows a window titled "Query Results: blr-mantech-r6e.blr.novell.com". It contains a table with two columns: "System Identification_Name" and "Inventory Information_Version". The table lists several system entries, each with a unique identifier and the version of the ZENworks Desktop Management 7 Inventory Scanner. At the bottom of the window, there are buttons for "Export", "Sort", "View in Browser", and "Close", along with a status bar indicating "9 machine(s) retrieved".

System Identification_Name	Inventory Information_Version
CH-BLR-MANTECH-R5H164_99_151_79.OUWYS_ROOT.O=Novell.T=BLR-MANTECH-R5E...	ZENworks Desktop Management 7 Inventory Scanner
CH-BLR-MANTECH-R7B164_99_151_89.OUWYS_ROOT.O=Novell.T=BLR-MANTECH-R5E...	ZENworks Desktop Management 6.5 SP1 Inventory Scanner
CH-BLR-MANTECH-R7D164_99_151_91.OUWYS_LEAF.OU=Leat.O=Novell.T=BLR-MANTE...	ZENworks Desktop Management 6.5 SP1 Inventory Scanner
CH-BLR-MANTECH-R7E164_99_151_92.OUWYS_LEAF.OU=Leat.O=Novell.T=BLR-MANTE...	ZENworks Desktop Management 6.5 SP1 Inventory Scanner
CH-BLR-MANTECH-R5G164_99_151_86.OUWYS_LEAF.OU=Leat.O=Novell.T=BLR-MANTE...	ZENworks Desktop Management 7 Inventory Scanner
CH-BLR-DT-R1G164_99_158_124.OUWYS_ROOT.O=Novell.T=BLR-MANTECH-R5E-TREE	ZENworks Desktop Management 7 Inventory Scanner
CH-BLR-MANTECH-R5B164_99_151_91.OUWYS_LEAF.OU=Leat.O=Novell.T=BLR-MANTE...	ZENworks Desktop Management 7 Inventory Scanner
CH-BLR-MANTECH-R7B164_99_158_114.OUWYS_ROOT.O=Novell.T=BLR-MANTECH-R5E...	ZENworks Desktop Management 7 Inventory Scanner
CH-SARAVANA164_99_158_131.OUWYS_ROOT.O=Novell.T=BLR-MANTECH-R5E-TREE	ZENworks Desktop Management 7 Inventory Scanner

You can perform the following operations in this window:

- **Export entries to an xml or a csv file.**
- **Sort the display of entries.**
- View the data in a browser.

IMPORTANT: When you click *View in Browser*, the inventory data is exported in the XML format for rendering in the browser. Make sure that the browser, such as Microsoft Internet Explorer or Mozilla* Firefox, is the default application associated with the XML format.

If Internet Explorer is the default application associated with the XML format and it is already opened, and when you click *View in Browser*, you want the data to displayed in a new Internet Explorer window, do the following:

1. Invoke Windows Explorer on the machine running Quick Report.
 2. Click the *Tools* menu, then click *Folder Options*.
 3. In the Folder Options window, click the *File Types* tab.
 4. From the list of registered file types, select *XML*.
 5. In the *Details for 'XML' extension* pane, click *Advanced*.
 6. In the Edit File Type window, click *New*.
 7. Specify an action name, and in the *Application Used to Perform Action* field, type `Internet_Explorer_installation_directory\iexplore.exe" -new %1`.
 8. Click *OK*.
 9. In Edit File Type window, select the newly created action from the Actions pane, and click *Set Default*.
 10. Click *OK*, then click *Close*.
- Stop the data retrieval process.

The Quick Report retrieves the data from the ZENworks Inventory database. You can stop the retrieval process by clicking *Stop* in the status bar of the Query Results dialog box.

The status bar displays the count of machines whose data has been retrieved. If you stop the process while the data for a single machine has not yet been completely retrieved, the Query Results dialog box displays the data retrieved until that time, but the status bar does not contain any message. And, if you stop the process while the data is being retrieved for multiple machines, the status bar displays the count of machines for which the data has been completely retrieved.

- Re-order the columns by dragging and dropping them.
- Re-size the columns.
- Select the entries by using the mouse or pressing Ctrl+A.
- Copy and paste the entries to the Clipboard by pressing Ctrl+C and Ctrl+V.

Exporting the Entries to an XML or a CSV File

- 1 Click *Export*.
- 2 In the Export Results dialog box, specify the XML or the CSV filename, and select the corresponding file type.

By default, the file is saved as `quick_report_name.xml` in the `ConsoleOne_installation_directory\consoleone\1.2\reporting\export` directory.

NOTE: If you specify a filename within double quotes, and without an extension or with an extension other than `.xml` or `.csv`, the file is stored in the comma-separated value (CSV) format irrespective of the file type you select.

Sorting the Display in Ascending or Descending Order

- 1 Click *Sort*.
- 2 In the *Sort Items By* list, select the column by which you want to sort the entries.
- 3 Select either *Ascending* or *Descending*.
- 4 Configure the *Then By* drop-down lists.
- 5 Click *OK*.

For example, the Query Results window has the following entries:

Product Name	Vendor Name
Microsoft Word	Microsoft
Microsoft Excel	Microsoft
ZENworks	Novell
iPrint	Novell
GroupWise	Novell
Adobe Acrobat	Adobe

If you want to sort the entries first by the vendor name in the ascending order and then sort all the Novell products in the ascending order, do the following:

- 1 Click the *Sort* button.
- 2 In the *Sort By* drop-down list, select *Vendor Name*.
- 3 Select the *Ascending* option.
- 4 In the *Then By* drop-down list, select *Product Name*.
- 5 Select the *Ascending* option.
- 6 Click *OK*.

The entries are displayed as shown below:

Product Name	Vendor Name
Adobe Acrobat	Adobe
Microsoft Excel	Microsoft
Microsoft Word	Microsoft
GroupWise	Novell
iPrint	Novell
ZENworks	Novell

77.2 Exporting the Inventory Information

You can customize the inventory information you want to export from the Inventory database into a comma-separated value (.csv) or an XML file.

You select the inventory components that should be exported, such as the Operating System Name and Version. You can further filter the inventoried workstations whose attributes are exported depending upon the export scope. For example, you can export only those inventoried workstations with a particular processor speed. The Data Export tool exports all inventoried workstations satisfying these query conditions into a .csv or .xml file.

If you want to reuse the same data export settings for export, you can save the data export configurations.

The following sections help you use the Data Export tool:

- [Section 77.2.1, “Procedure to Export the Inventory Information,” on page 1138](#)
- [Section 77.2.2, “Loading an Existing Configuration File,” on page 1141](#)
- [Section 77.2.3, “Running the Data Export Program From the Inventory Server,” on page 1142](#)

77.2.1 Procedure to Export the Inventory Information

- 1 In ConsoleOne, select a container.
- 2 Invoke the Data Export tool.
 - To invoke the Data Export tool from a database object, right-click the database object, click *ZENworks Inventory*, then click *Data Export*.

- To invoke the Data Export tool from the ConsoleOne *Tools* menu, you must first configure the Inventory database and then click *Tools*, click *ZENworks Inventory*, then click *Data Export*. For more information on how to configure the Inventory database, see [Section 77.1.1, “Configuring the Inventory Database,” on page 1096](#).

3 Select *Create a New Database Query*.

This option lets you add a new query that defines the inventory components such as hardware, software, network, and others that you want to export. You can also specify the criteria to limit the inventoried workstations and the database sites to be included in the query. Based on the inventory components and criteria you specify, the inventory information from the database is exported to a `.csv` or `.xml` file.

NOTE: If you want to load existing configuration settings for data export, select *Open a Saved Database Query*. This option lets you modify the settings for data export and then export the data to a `.csv` or `.xml` file. For more information, see [Section 77.2.2, “Loading an Existing Configuration File,” on page 1141](#).

4 Click *Next*.

5 Specify the filter conditions for the inventoried workstations.

5a Click *Edit Query*. For more information on how to define a query, see [Section 77.1.3, “Viewing Inventory Information by Querying the Database,” on page 1109](#).

5b (Optional) The *Enable Filter* option is available for selection only if you define the query using the software classes and its attributes of a supported category. Following are supported categories:

Category 1: Software Group, Software Group File Information, Software Group Patch Information, Software, File Information, and Patch Information

Category 2: Exclude File Information

Category 3: Disk Usage

The *Enable Filter* option is not available for selection if the query contains attributes belonging to different categories. For example, a query containing `software.name=word`, `softwaregroup.name=office`, and `diskusage.name=exe`.

If you want the results stored in `.csv` or `.xml` file to be filtered on the basis of the above query, select the *Enable Filter* check box.

5c Set the scope for exporting the information from the Inventory database.

If the ConsoleOne snap-ins and the Data Export tool have been installed for both ZENworks 7 Server Management and ZENworks 7 Desktop Management, the Data Export tool allows you to change the scope of exporting the inventory information.

By default, the *Workstations* option is enabled. The query locates all inventoried workstations satisfying the query expression. If ZENworks 7 Server Management and ZENworks 7 Desktop Management are installed in the same environment, the *Workstations*, the *Servers* and the *Both* options are available.

When you select *Workstations*, the query locates all inventoried workstations satisfying the query expression. Choose *Both* to include all inventoried workstations and inventoried servers satisfying the query expression.

5d Review the query that you define.

5e Click *Next*.

6 Select the database fields from the list of database fields, then click *Add*.

If you select a group component, all subcomponents of the group are added. For example, if you select the Software component group, the subcomponents of Software such as vendor name, product name, and version are added.

7 Click *Next*.

8 View the data export settings.

8a Click *Save Configuration* to save the configurations settings to an `.exp` file. Specify the filename for the `.exp` file and then click *Save*.

The configuration file (`.exp`) contains the settings such as the inventory components you selected, and also the query formed for filtering the inventoried workstation data export.

You create an `.exp` file so that you can reload the configuration settings and generate the `.csv` or `.xml` files any time you need to.

8b Click *Next*.

9 Select the machine from where you intend to perform the query.

9a Perform the Query from This Computer: Select this option to run the data export processing from the workstation computer. This option accesses the Inventory database on the specified database server and export the data in to a `.csv` or `.xml` file.

Perform the Query on a Remote Server: Select this option to run the data export program from any server that has Workstation Inventory components installed.

Running the Data Export program from a server is recommended if you are exporting data from a large database with more than 10,000 inventoried workstations or if you have specified complex queries with more than 20 database fields selected for exporting.

9b If you want to apply default encoding of the machine to the `.csv` or `.xml` file, select *Default Encoding*. The *Default Encoding* check box is selected by default. To apply Unicode encoding to the `.csv` or `.xml` file, select *Unicode Encoding*.

NOTE: If you create an `.exp` file to perform the data export from the local machine but use the same `.exp` to perform data export from a remote server and you want Unicode encoding, you must manually edit the `.exp` file and set the value of `DEExportEncode` to `UNICODE`.

9c Click *Next*.

10 Select an export option.

10a Select one the following options:

Export to CSV: Saves the inventory information in a `.csv` file.

Export to XML: Saves the inventory information in a `.xml` file.

10b Specify the path and the filename where you want to create the `.csv` or `.xml` file.

10c Click *Finish*.

If the configuration settings are not saved, you are prompted to save the changes.

This generates the `.csv` or `.xml` file in the specified directory.

Open the `.csv` file in Microsoft Excel or any other CSV-supported viewer to view the exported data.

Open the `.xml` file in a XML viewer such as XML Spy. For more information, see [Section 77.2.4, “An Overview of XML and the Contents of an XML File,” on page 1143](#).

77.2.2 Loading an Existing Configuration File

You can load an existing configuration file (.exp). An .exp file contains the settings such as the inventory components you selected, and also the query formed for filtering the inventoried workstation data export.

After you load the .exp file, you can modify the settings for data export and then export the data to a .csv or .xml file.

To load existing configuration settings for data export:

- 1 Make sure that you have generated the data configuration files.

Complete the procedure outlined in [Section 77.2.1, “Procedure to Export the Inventory Information,” on page 1138](#). This procedure generates the .csv or .xml file and the data configuration files.

- 2 In ConsoleOne, select a container and invoke the Data Export tool using any of the following methods:

- To invoke the Data Export tool from a database object, right-click the database object, click *ZENworks Inventory*, then click *Data Export*.
- To invoke the Data Export tool from the ConsoleOne *Tools* menu, you must first configure the Inventory database and then click *Tools*, click *ZENworks Inventory*, then click *Data Export*. For more information on how to configure the Inventory database, see [Section 77.1.1, “Configuring the Inventory Database,” on page 1096](#).

- 3 Select *Open a Saved Database Query*, then click *Next*.

The default directory for .exp files is `consoleone\consoleone_version\reporting\export`. Click *Browse* to open an existing .exp file.

If the .exp and .cfg files are invalid or are an older version, the data export will not proceed. The data export displays the number of servers and servers that satisfy the query and filter conditions for export.

- 4 Select a saved database query from the list of saved queries.

- 4a Select a saved database query from the list of saved queries. The list box displays the .exp files that are saved in `consoleone\consoleone_version\reporting\export`.

or

Click *Browse* to open an existing .exp file in any other location.

- 4b (Optional) If the .exp and .cfg files are invalid or are an older version, the data export will not proceed. The data export displays the number of servers and servers that satisfy the query and filter conditions for export.

If you want to modify the existing query, click *Edit* and modify the query and select the new database fields. For more information on how to define a query, see [Section 77.1.3, “Viewing Inventory Information by Querying the Database,” on page 1109](#).

- 4c Click *Next*.

- 5 View the data export settings.

- 5a Click *Save Configuration* to save the configurations settings to an .exp file. Specify the filename for the .exp file and then click *Save*.

The configuration file (.exp) contains the settings such as the inventory components you selected, and also the query formed for filtering the inventoried workstation data export. You create an .exp file so that you can reload the configuration settings and generate the .csv or .xml files any time you need to.

5b Click *Next*.

6 Select the machine from where you intend to perform the query.

6a Perform the Query from This Computer: Select this option to run the data export processing from the workstation computer. This option accesses the Inventory database on the specified database server and export the data in to a .csv or .xml file.

Perform the Query on a Remote Server: Select this option to run the data export program from any server that has Workstation Inventory components installed.

Running the Data Export program from a server is recommended if you are exporting data from a large database with more than 10,000 inventoried workstations or if you have specified complex queries with more than 20 database fields selected for exporting.

6b If you want to apply default encoding of the machine to the .csv or .xml file, select *Default Encoding*. The *Default Encoding* check box is selected by default. To apply Unicode encoding to the .csv or .xml file, select *Unicode Encoding*.

6c Click *Next*.

7 Select an export option.

7a Select one the following options:

Export to CSV: Saves the inventory information in a .csv file.

Export to XML: Saves the inventory information in a .xml file.

7b Specify the path and the filename where you want to create the .csv or .xml file.

7c Click *Finish*.

77.2.3 Running the Data Export Program From the Inventory Server

Running the Data Export program from a server is recommended if you are exporting information from a large database with more than 10,000 inventoried workstations or if you have specified complex queries with more than 20 database fields selected for exporting.

To run the data export program from the server:

1 Make sure that you have generated the data configuration files.

Follow the Step 1 to Step 5 as outlined in [Section 77.2.1, “Procedure to Export the Inventory Information,” on page 1138](#) and make sure that you save the settings in the .exp file.

When you save an .exp file, a corresponding data configuration file is created in the same directory with the same filename as the .exp file and with the .cfg file extension.

2 Click *Perform the Query on a Remote Server* to run the data export program from any server that has Workstation Inventory components installed, then click *Finish*.

3 Copy the .exp file and .cfg file to the server.

These two files should exist in the same directory on the Inventory server.

From the server console, run `dbexport.ncf` on NetWare servers, `dbexport.bat` on Windows servers, `/opt/novell/bin/DBExport` on Linux servers. To do so, enter

```
DBEXPORT "configuration_filename.exp" "csv_filename.csv"
```

where *configuration_filename.exp* is an existing file that contains the data export settings. You must enter the *configuration_filename.exp* and the *csv_filename.csv* filenames within double quotes. The data exported from the database is stored in *csv_filename.csv*.

The corresponding `.cfg` file for the `.exp` file should be in the same folder as the `.exp` file. The `.cfg` file contains the list of the database attributes to be exported.

If the `.exp` and `.cfg` files are invalid or are older versions, the data export will not proceed. The data export displays the number of inventoried workstations that satisfy the query and filter conditions for export.

77.2.4 An Overview of XML and the Contents of an XML File

Workstation Inventory allows you to export the inventory information from the Inventory database into an Extensible Markup Language (`.xml`) file by using the Data Export tool.

XML is a markup language that provides a format for describing structured data. An XML document is a text-based format. The XML source is made up of XML elements. The XML tags are not predefined and you must define your own tags.

For more information about XML, see the [World Wide Web Consortium \(W3C\) XML Activity and Information web site \(http://www.w3.org/XML\)](http://www.w3.org/XML).

A sample `.xml` file is as follows:

```
<?xml version="1.0" encoding='UTF-8'?>

<!DOCTYPE InventoryInformation [
```

```

        name CDATA #REQUIRED
    >
<!--ELEMENT value (#PCDATA)-->]
>
<InventoryInformation>
  <Machine name="blr-stl-zen1.blr.novell.com">
    <Class name="Processor" instance="1">
      <Attribute name="Current Clock Speed" type="regular" units="MHz">
        <value>2800</value>
      </Attribute>
      <Attribute name="Processor Family" type="regular">
        <value>"Intel (R) Xeon (TM) "</value>
      </Attribute>
    </Class>
    <Class name="IP" instance="1">
      <Attribute name="IP Address" type="regular">
        <value>164.99.163.9</value>
      </Attribute>
      <Attribute name="Subnet Mask" type="regular">
        <value>255.255.252.0</value>
      </Attribute>
    </Class>
  </Machine>
</InventoryInformation>

```

XML uses a Document Type Definition (DTD) to describe the data. The DTD is embedded within the XML document.

A DTD lists the elements, attributes, and entities contained in a document and also, defines the relationship between the elements and attributes.

Following is the DTD embedded in the preceding sample xml file:

```

<?xml version="1.0" encoding='UTF-8' ?>
<!--DOCTYPE InventoryInformation [!ELEMENT Attribute (value)-->
<!--ATTLIST Attribute

```

```

        name CDATA #REQUIRED

        type (custom | regular) #REQUIRED

        units CDATA #IMPLIED
    >

<!--ELEMENT Class (Attribute*)-->
<!--ATTLIST Class
        name CDATA #REQUIRED
        instance CDATA #REQUIRED
-->

<!--ELEMENT InventoryInformation (Machine+)-->
<!--ELEMENT Machine (Class+)-->
<!--ATTLIST Machine
        name CDATA #REQUIRED
-->

<!--ELEMENT value (#PCDATA)-->
-->

```

The following table explains the elements used in the sample XML file:

Elements Used in the Sample XML File	Description
Class	Device name
Type	Custom or Regular attribute
Units	Unit information
Instance	Device instance count

77.3 Viewing Inventory Information Without Using ConsoleOne

The `desktop4.exe` application that ships with ZENworks 7 Desktop Management allows you to view the Workstation Inventory and query the Inventory database without using ConsoleOne.

You can install `desktop4.exe` using either of the following methods:

- Install the ZENworks 7 Desktop Management Workstation Inventory ConsoleOne snap-ins. This automatically installs `desktop4.exe`. `Desktop4.exe` is located in the `Consoleone_installation_directory\consoleone_version\bin` directory.
- From the desktop directory in the *ZENworks 7 Companion 2* CD, extract `desktop.zip` to a temporary directory on your machine. Copy the contents of the `temporary_directory\desktop` directory to `Consoleone_installation_directory`.

Before you run `desktop4.exe`, you must perform the following tasks:

1 Identify your Inventory database.

Depending upon the Inventory database that you have configured for, you must edit the following `.ini` files: `sybase.ini`, `oracle.ini`, or `mssql.ini`. These files are located in the `consoleone_installation_directory\bin` directory.

2 Specify the following details in the `.ini` file:

IP Address: IP address of the server on which the Inventory database is running.

User Name: Database user ID having Read permissions on the database.

Password: Database password for the above user.

Scope: The scope for querying the Inventory database. If you have installed ZENworks 7 Desktop Management, specify `ZFD`. If you have installed ZENworks 7 Server Management, specify `ZFS`. If you have installed ZENworks 7 Desktop Management and ZENworks 7 Server Management in the same setup, specify `BOTH`.

Database Administrator Username: Specify the database administrator username in the `DBAUSERNAME` parameter.

Database Administrator Password: Specify the database administrator password in the `DBAPASSWORD` parameter.

A sample `sybase.ini` file is as follows:

```
# Novell Inc.
IPADDRESS=164.99.149.247
USERNAME=MW_READER
PASSWORD=novell
# ZFD / ZFS / BOTH
SCOPE=Both
DBAUSERNAME=MW_DBA
DBAPASSWORD=novell
```

A sample `oracle.ini` file is as follows:

```
# Novell Inc.
IPADDRESS=164.99.149.247
USERNAME=MWO_READER
PASSWORD=novell
# ZFD / ZFS / BOTH
SCOPE=ZFD
ORACLE_SID=orcl
DBAUSERNAME=MW_DBA
DBAPASSWORD=novell
```

A sample `mssql.ini` file is as follows:

```
# Novell Inc.
IPADDRESS=164.99.149.247
USERNAME=MW_READER
```

```

PASSWORD=novell
# ZFD / ZFS / BOTH
SCOPE=ZFS
ORACLE_SID=orcl
DBAUSERNAME=MW_DBA
DBAPASSWORD=novell

```

You can run `desktop4.exe` from the MS-DOS prompt or by using a `.bat` file. You must specify valid values for the following parameters:

- **-w:** Typeful and fully qualified distinguished name (DN) of the inventoried workstation
- **-n:** eDirectory tree name to which the inventoried workstation is registered.
- **-c:** Inventory operation to be performed on the inventoried workstation. To perform a query, enter `-c"Query"`. To perform an inventory summary, enter `-c"Inventory"`.
- **-d:** Type of the Inventory database server: Sybase, Oracle, or MSSQL.

For example, to perform a query using `desktop4.exe`, use either of the following methods:

- At the MS-DOS prompt, enter the following command:

```

Desktop4 -w"CN=WINXP-R1B164_99_151_48.OU=WsProm.O=novell"
-n"MANTECHR5C-TREE" -c"Query" -D"Sybase"

```

where `Desktop4` is the name of the application; `"CN=WINXP-R1B164_99_151_48.OU=WsProm.O=novell"` is the DN of the inventoried workstation; `"MANTECHR5C-TREE"` is the eDirectory tree name; `"Query"` is the Inventory operation to be performed on the inventoried workstation; and `"Sybase"` is the Inventory database.

- Use a `.bat` file:

- 1 Create a `.bat` file with the following contents in the same directory as `desktop4.exe`:

```

Desktop4 -w"CN=WINXP-R1B164_99_151_48.OU=WsProm.O=novell"
-n"MANTECHR5C-TREE" -c"Query" -D"Sybase"

```

where `Desktop4` is the name of the application; `"CN=WINXP-R1B164_99_151_48.OU=WsProm.O=novell"` is the DN of the inventoried workstation; `"MANTECHR5C-TREE"` is the eDirectory tree name; `"Query"` is the Inventory operation to be performed on the inventoried workstation; and `"Sybase"` is the Inventory database.

- 2 Run the `.bat` file.

You can perform an inventory summary using either of the following methods:

- At the MS-DOS prompt, enter the following command:

```

Desktop4 -w"CN=WINXP-R1B164_99_151_48.OU=WsProm.O=novell" -
n"INDYPROM-TREE" -c"Inventory" -D"Oracle"

```

where `Desktop4` is the name of the application; `"CN=WINXP-R1B164_99_151_48.OU=WsProm.O=novell"` is the DN of the inventoried workstation; `"INDYPROM-TREE"` is the eDirectory tree name; `"Inventory"` is the Inventory operation to be performed on the inventoried workstation; and `"Oracle"` is the Inventory database.

- Use a .bat file:

1 Create a .bat file with the following contents in the same directory as desktop4.exe:

```
Desktop4 -w"CN=WINXP-R1B164_99_151_48.OU=WsProm.O=novell" -
n"INDYPROM-TREE" -c"Inventory" -D"Oracle"
```

where Desktop4 is the name of the application; "CN=WINXP-R1B164_99_151_48.OU=WsProm.O=novell" is the DN of the inventoried workstation; "INDYPROM-TREE" is the tree name; "Inventory" is the Inventory operation to be performed on the inventoried workstation; and "Oracle" is the Inventory database.

2 Run the .bat file.

For more information on how to query an Inventory database, see [Section 77.1.3, "Viewing Inventory Information by Querying the Database," on page 1109](#). For more information on inventory information displayed by the Workstation Inventory, see [Section 77.1.2, "Viewing the Inventory Summary of an Inventoried Workstation," on page 1096](#).

Desktop4.exe is a back-end utility that can be leveraged by developing user-friendly interface to launch desktop4.exe.

Using desktop4.exe, you can also initiate Remote Management operations. For more information, see [Section 69.8, "Starting Remote Management Operations Without Using ConsoleOne," on page 827](#).

77.4 Retrieving Inventory information from the Inventory Database Without Using the CIM Schema

ZENworks 7 Desktop Management SP1 provides easy-to-use Inventory database views that allow you to retrieve inventory information from the Inventory database without using the CIM schema.

The Inventory views are predefined views that are automatically created in the Inventory database after you install the Workstation Inventory component of ZENworks 7 Desktop Management SP1.

The nomenclature for the Inventory views is database_schema_name.zen_devicename. For example, mw_dba.zen_processor.

Inventory views that are associated with enums have localized views. For example, mw_dba.zen_processor_ja is the Japanese view for the Processor.

77.4.1 List of Inventory Views

Table 77-4 ZENworks Inventory Views and their functionality

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
mw_dba.zen_asset	Retrieves the Asset information	SystemName	DNS name of the inventoried workstation	Yes

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
mw_dba.zen_battery	Retrieves the Battery information	Manufacturer	Name of the manufacturer	Yes
		Model	Model of the computer system	
		SerialNumber	Serial number of the computer system assigned by the manufacturer	
		Tag	Unique identifier of system information	
		ManagementTechnology	Technology available on the inventoried workstation such as DMI, WMI, and others	
		AssetTag	Asset tag number that the ROM-based setup program creates	
		ModelNumber	Model number of the computer system	
		Name	Device name for the battery, for example, Duracell* DR-36	
		Chemistry	The battery chemistry, for example, lithium-ion or nickel metal hydride	
		DesignCapacity	The design capacity of the battery in mWatt-hours	
		DesignVoltage	The design voltage of the battery in mVolts	
		SmartBatteryVersion	The Smart Battery Data Specification version number supported by this battery	
		InstallDate	The battery manufacture date	
		Manufacturer	The name of the company that manufactured the battery	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
mw_dba.zen_bios	Retrieves the BIOS information	SerialNumber	The serial number for the battery	Yes
		Caption	BIOS label	
		InstallDate	The manufacturing date of the BIOS	
		SerialNumber	Serial number of the computer, assigned during the manufacture	
		Version	Version or revision level of the BIOS	
		Manufacturer	BIOS vendor name	
		PrimaryBIOS	True state indicates Primary BIOS	
		BIOSIDBytes	Byte in the BIOS that indicates the computer model	
mw_dba.zen_bus	Retrieves the Bus information	Size	Size of the BIOS	Yes
		BusType	Bus type indicates PCI, ISA, and others	
		BusName	Bus name	
		BusDescription	Bus description	
		BusVersion	Version of the bus supported by the motherboard	
mw_dba.zen_cachememory	Retrieves the Cache memory information	DeviceID	The unique hexadecimal ID for the specific bus	Yes
		ErrorMethodology	Error correction scheme supported by this cache component, for example, Parity/ Single Bit ECC/ MultiBit ECC	
		Level	Indicates the cache level; internal cache that is built in to the microprocessors; external cache that is between the CPU and DRAM	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
		WritePolicy	Indicates the two different ways (Write-Back and Write-Through Cache) that the cache can handle to write to the memory	
		CacheType	Defines the system cache type, for example, Instruction, Data, Unified	
		LineSize	Size in bytes of a single cache bucket or line	
		ReplacementPolicy	Algorithm that the cache uses to determine which cache lines or buckets should be reused	
		ReadPolicy	Indicates whether the data cache is for read operations	
		Associativity	Defines the system cache associativity (directmapped, 2-way, 4-way)	
		Speed	Speed of this System Cache module in nanoseconds	
		Capacity	Size of the data store where the cache information is kept	
mw_dba.zen_cdrom	Retrieves the CDROM information	DeviceID	Drive letter allocated for the CD on the inventoried workstation	No
		Manufacturer	Vendor name of the CD	
		Description	Description of the CD	
		Caption	Caption of the CD	
mw_dba.zen_chassis	Retrieves the Chassis information	AssetTag	Asset tag number of the system chassis. For example, S11127	Yes

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
		NumberOfPowerCords	Total number of power cords attached to a system chassis	
		ChassisType	Represents whether the system chassis is a laptop, desktop, notebook, docking station and so on	
		Manufacturer	Name of the system chassis manufacturer. For example, Compaq	
		SerialNumber	Manufacturer's number used to identify a system chassis. For example, 53R661S	
		Tag	Unique ID of the system chassis attached to a particular inventoried workstation. For example, System Enclosure 0	
mw_dba.zen_computerinformation	Retrieves the computer information	Version	Version number of the system chassis	No
		ComputerName	Name of the inventoried workstation as represented in eDirectory, such as the fully qualified DN of the inventoried workstation	
		PrimaryOwner	The name of the primary user or owner of this system	
mw_dba.zen_currentlogin	Retrieves the current login information	PrimaryOwnerContact	The phone number of the primary user of this system	No
		CurrentUser	User logged into the primary eDirectory tree when the inventoried workstation was scanned	
mw_dba.zen_disk	Retrieves the disk information	RemovableDisk	Removable disk	Yes

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
mw_dba.zen_diskusage	Retrieves the disk usage information	Manufacturer	Vendor name of the disk	No
		Description	Description of the disk	
		PhysicalCylinders	Number of cylinders	
		PhysicalHeads	Number of heads	
		SectorsPerTrack	Removable disk drive sectors per track	
		Capacity	Capacity of the removable disk	
mw_dba.zen_displayadapter	Retrieves the display adapter information	FileExtension	The file extension for which the disk usage is scanned for.	Yes
		TotalDiskUsage	Total disk usage for all the files of the specified extension	
		Description	Description of the display adapter	
		VideoMemoryType	The type of video memory for this adapter, for example, VRAM/SRAM/DRAM/EDO RAM	
		MaxMemorySupported	Maximum memory that the display adapter supports for VIDEO RAM	
		CurrentBitsPerPixel	Number of adjacent color bits for each pixel	
		CurrentHorizontalResolution	Number of horizontal pixels shown by the display	
		CurrentVerticalResolution	Number of vertical pixels shown by the display	
		MaxRefreshRate	Maximum refresh rate of the monitor for redrawing the display, measured in Hertz	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
mw_dba.zen_displaydriver	Retrieves the display driver information	MinRefreshRate	Minimum refresh rate of the monitor for redrawing the display, measured in Hertz	Yes
		VideoArchitecture	The architecture of the video subsystem in this system, for example, CGA/VGA/SVGA/8514A	
		NumberOfColorPlanes	Number of color planes supported by the video system	
		ChipSet	Chip set used by the controller to compare system capabilities	
		DACType	Digital-to-Analog converter type	
		ProviderName	Vendor name	
		Manufacturer	Name of the display driver manufacturer	
		Version	Version number of the display driver	
mw_dba.zen_distinguishedname	Retrieves the distinguished name	InstallDate	Install date of the display driver	No
		IsShadowed	If True, the display driver is currently being shadowed	
		DistinguishedName	Distinguished name	
mw_dba.zen_dma	Retrieves the DMA information	Tree	eDirectory tree name	Yes
		Description	Name of the logical device that is currently using this DMA channel	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
		DMAChannel	Number of the Direct Memory Access (DMA) channel that a computer uses for transferring data to and from devices quicker than from computers without a DMA channel	
		Availability	Indicates whether Virtual Direct Memory Access (DMA) is supported	
		BurstMode	A data transmission mode in which data is sent faster than normal	
mw_dba.zen_dnsname	Retrieves the DNS name	HostName	DNS name of the inventoried workstation	No
mw_dba.zen_floppy	Retrieves the floppy information	DeviceID	The floppy name representing the floppy	No
		Manufacturer	Vendor name	
		Description	Floppy drive description	
		PhysicalCylinders	Total number of cylinders or tracks on the floppy	
		PhysicalHeads	Floppy drive R/W heads	
		SectorsPerTrack	Floppy drive sectors per track	
mw_dba.zen_inventoryscanner	Retrieves the inventory scanner information	Capacity	Floppy drive capacity	Yes
		LastScanDate	The date when the Scanner was last scanned. Stored as milliseconds so it can be read and displayed in any appropriate date format.	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
		InventoryServer	Name of the Inventory server to which the scans are sent. It is not the complete DN of the server name.	
		Version	Version of the Scanner running on the inventoried workstation	
		ScanMode	The management technology used by the Scanner, such as WMI or DMI, for scanning the computer system	
		RecentInformation	Latest inventory information	
		generaldictionaryversion	Version of the General dictionary	
		privatedictionaryversion	Version of the Private dictionary	
mw_dba.zen_ipaddress	Retrieves the IP address	Address	The unique address assigned to a computer on an IP Internet	No
		SubnetMask	The subnet mask of the inventoried workstation paired with an IP address specifies to an IP router which octets or bits in the IP address are the network ID and which octets or bits are the node ID	
mw_dba.zen_ipxaddress	Retrieves the IPX address	Address	The IPX address of the inventoried workstation	No
mw_dba.zen_irq	Retrieves the IRQ information	IRQNumber	Number of the Interrupt Request Line (IRQ), from 0 to 15	Yes
		Availability	Availability of the specific IRQ channel	
		TriggerType	IRQ Trigger type	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
mw_dba.zen_keyboard	Retrieves the keyboard information	Shareable	If True, the system IRQ can be shared across devices	No
		KeyboardLayout	Layout of the keyboard	
		KeyboardSubtype	Type of the keyboard	
		KeyboardDescription	Description of the keyboard, such as IBM Enhanced 101 or 102 keys	
		NumberOfFunctionKeys	Total number of function keys	
		KeyboardDelay	Delay before the repeat of a key	
		TypematicRate	Rate of processing the keys	
mw_dba.zen_lastlogindetails	Retrieves the last login details	LastUser	User most recently logged into the primary eDirectory tree through Novell Client when the inventoried workstation was scanned	No
mw_dba.zen_macaddresses	Retrieves the MAC address	MACAddress	Unique node address permanently coded in the network adapter that identifies a specific computer on a network	No
mw_dba.zen_memory	Retrieves the memory information	TotalMemory	Total memory of the inventoried workstation	No
mw_dba.zen_microsoftdomainname	Retrieves the Microsoft domain name	DomainName	Domain name of the inventoried workstation	No
mw_dba.zen_internalmodem	Retrieves the internal modem information	Name	Identifying information of the modem	No
		Description	Additional information about the modem	
		ProviderName	Name of the vendor	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
mw_dba.zen_monitor	Retrieves the monitor information	DeviceID	Special hexadecimal string identifying the modem type	No
		DeviceID	Unique ID of a desktop monitor that is attached to an inventoried workstation For example, DesktopMonitor1	
		ModelID	Unique ID of a model of the monitor. It is a combination of the Manufacturer ID and Product ID For example, DELA001	
		MonitorDescription	Description of the monitor	
		NominalSize	A number representing the diagonal width of the monitor (the distance from one corner of the screen to the opposite corner of the screen) For example, 17" You can customize the scan of the nominal size of the monitor by configuring the HWRules ini file using the Workstation Inventory policy.	
		ViewableSize	A number representing the diagonal width of the screen image excluding the black borders around the image's edge For example, 15.8"	
		ManufacturedDate	Year in which the monitor was manufactured	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
		MonitorSerialNumber	Manufacturer's number used to identify a monitor For example, 23DDC24N9067	
		Manufacturer	Name of the monitor's manufacturer For example, DELL Computer Corp	
		Model	Product name of the monitor given by the manufacturer For example, DELL E771a	
mw_dba.zen_motherboard	Retrieves the motherboard information	Description	General description of the motherboard	No
		Manufacturer	Name of the motherboard manufacturer	
		Version	Version of the motherboard	
		NumberOfSlots	The number of expansion slots in the motherboard for adding more memory, graphic capabilities, and support for special devices	
mw_dba.zen_mouse	Retrieves the mouse information	MouseType	Mouse type	Yes
		MouseName	Identifying information of the mouse	
		NumberOfButtons	Number of buttons on the mouse	
		IRQNumber	Interrupt assigned to this device	
mw_dba.zen_mousedriver	Retrieves the mouse driver information	DriverName	Name of the mouse driver	No

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
mw_dba.zen_NetworkAdapter	Retrieves the network adapter information	DriverVersion	Version number of the mouse driver	Yes
		Caption	Network adapter caption	
		Description	Network adapter description	
		InstallDate	Install date of the network adapter	
		Name	Network adapter name	
		PermanentAddress	Node address stored permanently in the adapter	
		MACAddress	The MAC address stored in the network adapter	
		MaxSpeed	Rate at which the data is transferred over the LAN	
		AdapterType	Type of network adapter, such as FDDI or token ring	
		ProviderName	Name of the provider	
mw_dba.zen_NetworkAdapterDriver	Retrieves the network adapter driver information	Description	Description of the network adapter driver installed on the inventoried workstation	No
			For example, IBM 10/100 Ethernet adapter, EN-2420Px Ethernet adapter	
		Name	Name of the network adapter driver	
mw_dba.zen_parallelport	Retrieves the parallel port information	Version	Version of the network adapter	Yes
		PortName	The logical name of the input-output device on this parallel port, under this operating environment	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
mw_dba.zen_powersupply	Retrieves the power supply information	HasDMASupport	If True, DMA is supported	No
		PortAddress	Base I/O address for this parallel port	
		IRQNumber	IRQ number of the parallel port	
		Description	Expanded description of the input voltage capability for this power supply	
mw_dba.zen_processor	Retrieves the processor information	TotalOutputPower	Attribute value that represents the total output power of the power supply	Yes
		DeviceID	Special hexadecimal string identifying the processor type	
		Description	Additional information about the processor	
		Role	Type of processor such as central processor, math coprocessor, and others	
		Family	Identification of the processor family such as Pentium II, Pentium III, and others	
		OtherFamilyDescription	Additional description about the Processor Family, such as Pentium Processor with MMX technology	
		UpgradeMethod	The method by which this processor can be upgraded, if upgrades are supported	
		MaxClockSpeed	Maximum clock speed of the processor	
		CurrentClockSpeed	Current clock speed of the processor	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
mw_dba.zen_serialport	Retrieves the serial port information	Stepping	Single-byte code characteristic provided by microprocessor vendors to identify the processor model	No
		PortName	The logical name of the I/O device on this serial port, under this operating environment	
		PortAddress	Base input-output address for this serial port	
mw_dba.zen_soundadapter	Retrieves the sound adapter information	IRQNumber	IRQ number of the serial port	No
		Name	Label of the multimedia card	
		Description	Description of the multimedia component for the workstation	
mw_dba.zen_systemslot	Retrieves the system slot information	ProviderName	Name of the provider	No
		SlotDescription	Card currently occupying this slot	
		MaxDataWidth	Maximum bus width of cards accepted in the slot	
mw_dba.zen_unixOS	Retrieves the UNIX operating system information	ThermalRating	Maximum thermal dissipation of the slot in milliwatts	Yes
		Type	Operating system of the inventoried workstation	
		Caption	Operating system name	
		CodePage	Language code page of the operating system	
		Version	Version number of the operating system	
		InstallDate	Install date of the operating system	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
mw_dba.zen_windowsOS	Retrieves the Windows operating system information	VirtualMemorySize	Total number of bytes in the virtual address space of the calling process	Yes
		VisibleMemorySize	Total memory as reported by the operating system	
		ProviderName	Name of the provider	
		KernelVersion	Version number of the operating system	
		SwapSpaceSize	Total swap space size	
		Type	Operating system of the inventoried workstation	
		OtherTypeDescription	Additional description of the operating system if available	
		Caption	Operating system name	
		CodePage	Language code page of the operating system	
		Version	Version number of the operating system	
mw_dba.zen_NetWareOS	Retrieves the NetWare operating system information	InstallDate	Install date of the operating system	Yes
		VirtualMemorySize	Total number of bytes in the virtual address space of the calling process	
		VisibleMemorySize	Total memory as reported by the operating system	
		ProviderName	Name of the provider	
		Type	Operating system of the inventoried workstation	
		Caption	Operating system name	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
		CodePage	Language code page of the operating system	
		Version	Version number of the operating system	
		InstallDate	Install date of the operating system	
		VirtualMemorySize	Total number of bytes in the virtual address space of the calling process	
		VisibleMemorySize	Total memory as reported by the operating system	
		SizeStoredInPagingFiles	NetWare server specific attributes	
		ProviderName	Name of the provider	
		AccountingVersion	NetWare server specific attributes	
		InternetBridgeSupport	NetWare server specific attributes	
		MaxNumberOfConnections	NetWare server specific attributes	
		MaxNumberOfVolumes	NetWare server specific attributes	
		PeakConnectionsUsed	NetWare server specific attributes	
		PrintServerVersion	NetWare server specific attributes	
		QueuingVersion	NetWare server specific attributes	
		RevisionLevel	NetWare server specific attributes	
		SecurityRestrictionLevel	NetWare server specific attributes	
		SFTLevel	NetWare server specific attributes	
		TTSlevel	NetWare server specific attributes	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
mw_dba.zen_software	Retrieves the software information	VAPVersion	NetWare server specific attributes	Yes
		VirtualConsoleVersion	NetWare server specific attributes	
		InternalNetworkNumber	NetWare server specific attributes	
		Name	Vendor-defined name of the product represented as a vendor trademark or registered trademark	
		Vendor	Vendor name of the software	
		Version	User-friendly version of a product For example, the version for Windows 2000 is 2000 or Major.Minor Version of the Product	
		ProductID	A unique, 16-character identifier for an installed product. This identifier is available from MSI on Windows The format is ABCD-1234-WXYZ-PQRS	
		InternalVersion	Internal version of a product The format is: <i>major version.minor version.build.sub build number</i> or <i>major version.minor version.build</i>	
		Language	User-friendly name for the language of this copy of the product	
		FriendlyName	Display name of the software	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
		Uninstallstring	The command to invoke for uninstalling this product instance. Currently, this is available in Add/Remove Programs (ARP) and MSI on Windows	
		Supportpack	Installed support pack number of the product	
		SoftwareEdition	Product edition defined by the vendor. For example, Professional	
		LastExecutionTime	Date and time stamp when the product was last executed	
		Frequencyofusage	Number of times the product is used	
		Description	Description of the product.	
		InstallationSource	Identifies the file system path where the installation files were stored when installing this product instance. Currently, this is available in ARP and MSI on Windows.	
		InformationRepository	Source of scan, which can be, Add/Remove Programs, MSI, Software Dictionary, or PRODUCTS.DAT	
		Category	Product category to which the product belongs For example, Office is a part of the Productivity tools category and Solitaire is a game	
		Helpink	Support Web site URL for the product that is available in ARP and MSI	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
mw_dba.zen_softwaregroup	Retrieves the software group information	PackageGUID	Vendor-defined GUID for a product that is available in MSI	Yes
		Path	Directory path where the product is installed on the inventoried workstation	
		Name	Vendor-defined name of the software group represented as a vendor trademark or registered trademark	
		Vendor	Vendor name for the software group	
		Version	User-friendly version of a software group	
		ProductID	A unique, 16-character identifier for an installed product. This identifier is available from MSI on Windows. The format is ABCD-1234-WXYZ-PQRS	
		InternalVersion	Internal version of a product The format is: <i>major version.minor version.build.sub build number</i> or <i>major version.minor version.build</i>	
		Language	User-friendly name for the language of this copy of the product	
		FriendlyName	Display name of the software	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
		Uninstallstring	The command to invoke for uninstalling this product instance. Currently, this is available in Add/Remove Programs (ARP) and MSI on Windows.	
		Supportpack	Installed support pack number of the product	
		SoftwareEdition	Product edition defined by the vendor. For example, Professional	
		LastExecutionTime	Date and time stamp when the product was last executed	
		Frequencyofusage	Number of times the product group is used	
		Description	Description of the product group	
		InstallationSource	Identifies the file system path where the installation files were stored when installing this product instance. Currently, this is available in ARP and MSI on Windows.	
		InformationRepository	Source of scan, which can be, Add/Remove Programs, MSI, Software Dictionary, or PRODUCTS.DAT	
		Category	Product category to which the product belongs For example, Office is a part of the Productivity tools category and Solitaire is a game	
		Helpink	Support Web site URL for the product that is available in ARP and MSI	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
mw_dba.zen_softwarepatch	Retrieves the software patch information	PackageGUID	Vendor-defined GUID for a product that is available in MSI	No
		Path	Directory path where the product is installed on the inventoried workstation	
		productid	Software ID of the software patch	
mw_dba.zen_antivirus	Retrieves the antivirus product information	PatchName	Vendor-defined name for the patch	Yes
		Name	Vendor-defined name of the antivirus product represented as a vendor trademark or registered trademark	
		Vendor	Vendor name for the antivirus product	
		Version	User-friendly version of the antivirus product	
		ProductID	A unique, 16-character identifier for an installed antivirus product. This identifier is available from MSI on Windows. The format is ABCD-1234-WXYZ-PQRS	
		InternalVersion	Internal version of the antivirus product The format is: <i>major version.minor version.build.sub build number</i> or <i>major version.minor version.build</i>	
		Language	User-friendly name for the language of this copy of antivirus product	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
		FriendlyName	Display name of the antivirus product	
		Uninstallstring	The command to invoke for uninstalling this product instance. Currently, this is available in Add/Remove Programs (ARP) and MSI on Windows.	
		Supportpack	Installed support pack number of the antivirus product	
		SoftwareEdition	Antivirus Product edition defined by the vendor	
		LastExecutionTime	Date and time stamp when the antivirus product was last executed	
		Frequencyofusage	Number of times the antivirus product is used	
		Description	Description of the antivirus product	
		InstallationSource	Identifies the file system path where the installation files were stored when installing this antivirus product instance. Currently, this is available in ARP and MSI on Windows.	
		InformationRepository	Source of scan, which can be, Add/Remove Programs, MSI, Software Dictionary, or PRODUCTS.DAT	
		DefinitionDate	The date of the virus definition file installed on the computer. Some anti-virus products combine date and version into a single string.	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
mw_dba.zen_dictionaryfile	Retrieves the ZENworks software dictionary file information	DefinitionVersion	The vendor-defined version of the virus definition file that has been installed on a computer	Yes
		Category	Product category to which the antivirus product belongs	
		Helplink	Support web site URL for the antivirus product that is available in ARP and MSI	
		PackageGUID	Vendor-defined GUID for the antivirus product that is available in MSI	
		Path	Directory path where the antivirus product is installed on the inventoried workstation	
		fileid	Dictionary File ID	
		directoryid	Directory ID	
		FileName	Filename of the dictionary file	
		Directory	Directory name in which the dictionary file is stored	
		FileVersion	Dictionary file version	
		FileSize	Dictionary file size	
		LastModified	Last modified date of the dictionary file	
		InternalName	Internal name	
		ProductVersion	The version of the product represented by this file	
		Company	Vendor name	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
mw_dba.zen_excludedfile	Retrieves the excluded file information	ProductName	The product which this file represents	Yes
		Language	User-friendly name for the language of this copy of the file	
		SoftwareDictionaryID	ID of the file as represented in the General software dictionary	
		fileid	Excluded file ID	
		directoryid	Directory ID	
		FileName	Filename of the excluded file	
		Directory	Directory name in which the excluded file is stored	
		FileVersion	Excluded file version	
		FileSize	Excluded file size	
		LastModified	Last modified date of the excluded file	
		InternalName	Internal name	
		ProductVersion	The version of the product represented by this file	
		Company	Vendor name	
		ProductName	The product which this file represent	
		Language	User-friendly name for the language of this copy of the file	
mw_dba.zen_locktable	Retrieves the lock table information	ComputerName	Computer name	Yes
		LastScanTime	The date when the Scanner was last scanned. Stored as milliseconds so it can be read and displayed in any appropriate date format.	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
mw_dba.zen_removabledisk	Retrieves the removable disk information	RecentInformation	Latest information	No
		Manufacturer	Vendor name for the removable disk	
		Description	Description of the removable disk	
		PhysicalCylinders	Total number of cylinders or tracks on the disk	
		PhysicalHeads	Number of heads	
		SectorsPerTrack	Number of sectors per track	
mw_dba.zen_fixeddisk	Retrieves the fixed disk information	Capacity	Total size	No
		Manufacturer	Vendor name of the fixed disk	
		Description	Description of the fixed disk	
		PhysicalCylinders	Total number of cylinders or tracks on the disk	
		PhysicalHeads	Number of heads	
		SectorsPerTrack	Number of sectors per track	
mw_dba.zen_WindowsLocalFileSystem	Retrieves the Windows local file system information	Capacity	Total size	No
		Name	Windows local file system name	
		FileSystemSize	Windows local file system size	
		AvailableSpace	Windows local file system space	
		FileSystemType	Windows local file system type	
		Caption	Windows local file system caption	
		DeviceID	Device ID	

Inventory View Name	Functionality	Attributes	Description	Is the view Localized?
mw_dba.zen_NetWareLocalFileSystem	Retrieves the NetWare local file system information	VolumeSerialNumber	Windows local file system volume number	No
		Name	NetWare local file system name	
		FileSystemSize	NetWare local file system size	
		AvailableSpace	NetWare local file system space	
		FileSystemType	NetWare local file system type	
		Caption	NetWare local file system caption	
		DeviceID	Device ID	
mw_dba.zen_LinuxLocalFileSystem	Retrieves the Linux local file system information	VolumeSerialNumber	NetWare local file volume serial number	No
		Name	Linux local file system name	
		FileSystemSize	Linux local file system size	
		AvailableSpace	Linux local file system available space	
		FileSystemType	Linux local file system type	
		Caption	Linux local file system caption	
		DeviceID	Device ID	
		VolumeSerialNumber	Linux local file system volume serial number	

77.4.2 How to Use the Inventory Views

You can use the Inventory views in SQL statements, and execute the SQL statements from the Inventory database prompt or in any third-party application.

Examples:

- To retrieve all the processor information:

```
select * from mw_dba.zen_processor
```

- To retrieve specific processor information:

```
select DeviceID, Description, Role, Family,  
OtherFamilyDescription, UpgradeMethod, MaxClockSpeed,  
CurrentClockSpeed from mw_dba.zen_processor
```

- To retrieve all software information:

```
select * from mw_dba.zen_software
```

- To retrieve software information along with its suite details:

```
select soft.name, softsuite.name from mw_dba.zen_software soft,  
mw_dba.zen_softwaregroup softsuite where soft.name = 'ZENworks  
Desktop Management Inventory Server' and  
soft.parentinstanceid=softsuite.pinstanceid;
```

- To retrieve software patch information:

```
select suite.name, patchname from mw_dba.zen_softwaregroup suite,  
mw_dba.zen_softwarepatch patch where  
suite.pinstanceid=patch.pinstanceid
```

- To retrieve software suite patch information:

```
select soft.name, patchname from mw_dba.zen_software soft,  
mw_dba.zen_softwarepatch patch where  
soft.pinstanceid=patch.pinstanceid;
```

- To retrieve anti-virus software information:

```
select * from mw_dba.zen_antivirus
```


Monitoring Workstation Inventory Using Status Logs

78

Novell® ZENworks® 7 Workstation Inventory lets you track whether the scan or the roll-up of information is successful by viewing the log files and scan history.

The inventory components report the status of the inventory scanning and roll-up of scan information in Novell eDirectory™.

For example, when you view the scan logs, you can determine whether the scan was successful or if there were any errors while scanning the inventoried workstation or at the time of roll-up.

You can view the following status information:

- [Section 78.1, “Viewing the Scan History of an Inventoried Workstation,” on page 1177](#)
- [Section 78.2, “Viewing the Scan Status of an Inventoried Workstation,” on page 1178](#)
- [Section 78.3, “Viewing the Roll-Up History of the Server,” on page 1179](#)
- [Section 78.4, “Viewing the Status of Inventory Components on a Server,” on page 1179](#)
- [Section 78.5, “Viewing the Status of the Last Scan in the Workstation Scan Log,” on page 1180](#)
- [Section 78.6, “Viewing the Roll-Up Log for Servers,” on page 1181](#)
- [Section 78.7, “Status Logs and Scan Logs Overview,” on page 1182](#)
- [Section 78.8, “Viewing the Status Log in XML Format,” on page 1182](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

78.1 Viewing the Scan History of an Inventoried Workstation

The Scan Status reports the history of the scans done at the inventoried workstation. For example, you view the Scan Status window to determine whether the scan was successful for the inventoried workstation, or whether the Storer has stored the .str files of the inventoried workstation in the database. The inventory components (Scanner and Storer) write the scan information in the Status log.

To invoke the Scan Status window:

- 1 In ConsoleOne®, right-click the inventoried workstation, click *Properties*, click the *ZENworks Inventory* tab, then click *Scan Status*.

If the scan is disabled in the Inventory policy, the Scanner does not log any status messages in the Status Report log.

The following table lists the details of the log:

Table 78-1 Details available in the Status Report log

Status Information	Details
Time of Scan	Displays the date and time of the scan.
Message	Displays the message reported by the inventory components while scanning the inventoried workstation and storing the inventory information in the database.

You can export the log file as a .csv or tab-delimited file.

The Scan Status displays the history of the latest ten scans of the selected inventoried workstation.

78.2 Viewing the Scan Status of an Inventoried Workstation

The Workstation Scan Status reports the scan status of the inventoried workstation in the eDirectory and the Inventory database from the specified time. For example, you can view the scan status of an inventoried workstation in the eDirectory and Inventory database during the specified time and date.

To view the scan status of an inventoried workstation:

- 1 In ConsoleOne, select a container object, click *Tools*, click *ZENworks Inventory*, then click *Workstation Scan Status*.
- 2 Specify the date and time.
- 3 To include all subcontainers within the selected container, select the *Search Subcontainers* option.

All the inventoried workstations in the selected container with their scan status in eDirectory and Inventory database during the specified time and date are displayed in the Results of Scan Status Lookup dialog box.

The following table lists the details of the scan status lookup:

Table 78-2 Details available in the Scan Status Lookup

Parameter	Details
Workstation DN	Displays the DN of all inventoried workstations satisfying the filter condition.
Status in Novell eDirectory	Displays whether the inventoried workstation is scanned in eDirectory.
Status in Database	Displays whether the scanned information of the inventoried workstation is stored in the database.
Last Scan Time	Displays the time when the inventoried workstation was last scanned according to eDirectory.

78.3 Viewing the Roll-Up History of the Server

The Roll-Up Status reports the status of the roll-up information from the server that initiated the roll-up of information. For example, if your inventory setup consists of a Leaf Server that initiates the roll-up of information to the next-level Root Server, the Roll-Up log displays the roll-up history of the Leaf Server.

If the roll-up of information is across trees, the Roll-Up log might fail to display the roll-up history of the next-level servers. To view the Roll-Up log, you must explicitly log into all trees from the inventoried workstation where you are running ConsoleOne and view the Roll-Up log.

The inventory components of the server (Sender, Receiver, and Storer) write the roll-up information in the Roll-Up Status. For example, you view the Roll-Up log to determine whether there were any errors during roll-up of inventory information from the server. This log also displays the most recent storage time of the inventory information that was stored in the database on the topmost level server (Root Server). This log displays the history of the ten previous roll-up sessions done from the current server and the roll-up history from the next-level servers.

The following table lists the details of the log:

Table 78-3 Details available in the Roll-Up log

Status Information	Details
Roll-Up Start Time	Displays the date and time of the roll-up.
Message	Displays the message reported by the inventory component while moving the inventory information across the servers.

You can export the file as a .csv or tab-delimited file.

To invoke the Roll-Up Status window:

- 1 In ConsoleOne, right-click the Inventory Service object (Inventory Service_server_name), from which the roll-up is done, click *Properties*, click the *Status Report* tab, then click *Roll-Up Status*.

78.4 Viewing the Status of Inventory Components on a Server

The Server Status window reports the status of the Inventory server components on the selected server. You can view the Server Status log for any Inventory Service object. For example, you can determine whether the Sender sent the files to the Receiver or whether the Storer was able to establish the connection with the database successfully. The Server Status window displays the details of the ten latest status messages logged by the Inventory server components.

If the Inventory server components (Sender, Receiver, Selector, Storer, Service Manager, Roll-Up Scheduler, Inventory Sync Service) encounter an error while starting or running on the server, the status of the server displays the information.

Table 78-4 *Inventory Details displayed in the Server Status window*

Status Information	Details
Time of Log	Displays the date and time when the message was reported by the inventory components.
Source	Displays the inventory component that has logged the status message.
Message Type	Displays the severity of the message.
Message	Displays the message reported by the inventory components.

You can export the log file as a `.csv` or tab-delimited file.

To view the Server Status window:

- 1 In ConsoleOne, right-click the Inventory Service object (Inventory Service_*server_name*), click *Properties*, click *Status Report*, then click *Server Status*.

78.5 Viewing the Status of the Last Scan in the Workstation Scan Log

The Workstation Scan log reports the status of the latest scan done at the inventoried workstations associated with the selected Container. For example, you view the Workstation Scan log to determine whether the latest scans were successful for the inventoried workstations or whether the Storer has stored the inventoried workstation `.str` files in the database. The inventory components (Scanner and Storer) write the scan information in the Status log.

You can also choose whether to display error, warning, and informational status messages of the inventoried workstations.

The following table lists the details of the log:

Table 78-5 *Details available in the Workstation Scan log*

Status Information	Details
Scanned Workstation Name	Displays the DN of the inventoried workstation.
Time of Scan	Displays the date and time the status was logged.
Message Type	Displays the severity of the message.
Message	Displays the message reported by the inventory components while scanning the inventoried workstation or storing the inventory information in the database.

You can export the file as a `.csv` or tab-delimited file.

If the scan is disabled in the Inventory policy, the Scanner does not log any status messages in the Status Report log.

To view the Workstation Scan log window:

- 1 In ConsoleOne, click the container, click *Tools*, click *ZENworks Inventory*, then click *Workstation Scan Log*.
- 2 Click the message severity type, then click *OK*.
- 3 To export the Workstation scan log to files, click *Export*.
- 4 Choose the file type, then specify the filename.
- 5 Click *OK*.

When the Scanner creates a `.str` file of an inventoried workstation and the Selector processes this file, the inventory components also log the status of the scanning in the Workstation Status log. It is possible that at the same time, the Storer is processing the `.str` files of another inventoried workstation. Meanwhile, the Scanner continues scanning and updates the Workstation Status log for the next scan.

78.6 Viewing the Roll-Up Log for Servers

The Roll-Up log reports the status of the latest roll-up from the Inventory Service objects in the Container. For example, you view the Roll-Up log to determine whether the latest roll-up of information from the Roll-Up server for the Inventory Service object was successful. The inventory components (Sender, Receiver, and Storer) write the roll-up information in the Roll-Up log. You can also choose to display error, warning, and informational status messages of the Intermediate servers.

The following table lists the details of the log:

Table 78-6 Details available in the Roll-Up log

Status Information	Details
Roll-Up Initiated From	Displays the DN of the Intermediate server that initiated the roll-up.
Roll-Up Start Time	Displays the date and time the roll-up of information was initiated.
Source	Displays the inventory component that logs the status.
Message Type	Displays the severity of the message.
Message	Displays the message reported by the inventory components while scanning the inventoried workstation.

You can export the log as a `.csv` or tab-delimited file.

To invoke the Roll-Up Log window:

- 1 In ConsoleOne, click the container that contains the Inventory Service object (Inventory Service_ *server_name*), click *Tools*, click *ZENworks Inventory*, then click *Roll-Up Log*.
- 2 Click the severity type of the messages you want to view, then click *OK*.
- 3 To export the Roll-Up log to files, click *Export*.
- 4 Choose the file type, then specify the filename.
- 5 Click *OK*.

78.7 Status Logs and Scan Logs Overview

Table 78-7 *List of the Inventory status logs and scan logs*

Status/Scan Log	Inventory Components that Log the Status	Details of the Log	How to View the Log File in ConsoleOne
Workstation Scan Log	Scan program, Storer	Scanned inventoried workstation name, time of scan, inventory component, message type, and status message	Click the container, click <i>Tools</i> , click <i>ZENworks Inventory</i> , then click <i>Workstation Scan Log</i>
Roll-Up Log	Sender, Receiver, Storer	Roll-up initiated from, roll-up start time, inventory component, message type, status message	Click the container for the Inventory Service object, click <i>Tools</i> , click <i>ZENworks Inventory</i> , then click <i>Roll-Up Log</i>
Workstation Scan Status	Scan program, Storer	Time of scan and status message	In ConsoleOne, right-click the inventoried workstation, click <i>Properties</i> , click the <i>ZENworks Inventory</i> tab, then click <i>Scan Status</i>
Status of Inventory Components on Server	Sender, Receiver, Selector, Storer, Service Manager, Roll-Up Scheduler	Time of log, source, message type, message	In ConsoleOne, right-click the Inventory Service object, click <i>Properties</i> , click <i>Status Report</i> , then click <i>Server Status</i>
Roll-Up Status	Sender, Receiver, Storer	Roll up start time, message	In ConsoleOne, right-click the Inventory Service object, click <i>Properties</i> , click <i>Status Report</i> , then click <i>Roll-Up Status</i>

78.8 Viewing the Status Log in XML Format

All inventory components log the status messages in a log file maintained in XML (Extensible Markup Language) format. Unlike the status logs that contain a history of the ten latest status messages, the status XML log stores all status messages.

The log file contains the following information:

- Inventory module name
- Date and time of status logging
- Severity of the message
- Message text and status message number
- DN name, if the inventory module is associated with a particular DN object in eDirectory
- Product specific details of the module

The format of the log file is as follows:

```
?xml version="1.0" encoding="UTF-8"?>
```

```
?xml stylesheet type="text/xml" href="inventorylog.xml"?
<message_log>
  <message_entry>
    <module_name>Scanner</module_name>
    <severity>Critical</severity>
    <date_time>8/3/00 12:49 PM</date_time>
    <message_tag>unable to create scan data files</ message_tag>
    <dn_name>Inv_server</dn_name>
  </message_entry>
  <module_name>Storer</module_name>
  <severity>Critical</severity>
  <date_time>8/3/00 12:49 PM</date_time>
  <message_tag>unable to update the database</message_tag>
  <dn_name>Inv_server</dn_name>
</message_entry>
..
</message_log>
```

A sample style sheet and Document Type Declaration (DTD) file are located in *inventory_installation_directory\inv\server\xmlog* on the server.

The *inventorylog.xml* log file is located in the *inventory_installation_directory\inv\server\xmlog* directory on NetWare® and Windows* servers.

By default, the maximum size of the log file is 120 KB. To modify the maximum size of the log file, edit the *inventorylog.ini* file. On NetWare and Windows servers, this file is in the *inventory_installation_directory\inv\server\xmlog* directory.

The contents of *inventorylog.ini* are as follows:

```
max_file_size=100 KB
```

Modify the *MAX_FILE_SIZE* parameter, if required.

If the file size exceeds the value specified in the *MAX_FILE_SIZE* parameter, the file is archived as *filename_old.xml*. The latest messages are in the current log file.

To view the log data file, use a third-party XML browser.

Performance Tips

M

This section provides information on the system and database parameters that you need to tune to obtain improved performance for Novell® ZENworks® 7 Desktop Management Workstation Inventory. Specific tuning tips are provided for working with Inventory Reports, Database Export, and Query.

In addition to reviewing this information, we recommend that you refer to vendor documentation or other related articles regarding performance tuning and database tuning available on the Internet.

This chapter contains the following sections:

- [Section M.1, “Database Parameter Tuning Tips,” on page 1185](#)
- [Section M.2, “Improving the Throughput of the Inventory Storer,” on page 1191](#)
- [Section M.3, “Performance Tips for the Inventory Server \(Support Pack 1\),” on page 1194](#)
- [Section M.4, “Performance Tips for the Inventory ConsoleOne Utilities,” on page 1196](#)
- [Section M.5, “References,” on page 1198](#)

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

M.1 Database Parameter Tuning Tips

- [“Sybase in the NetWare, Windows, or Linux Environment” on page 1185](#)
- [“Oracle in the NetWare, Windows, or Linux Environment” on page 1188](#)
- [“MS SQL in the Windows Environment” on page 1190](#)

M.1.1 Sybase in the NetWare, Windows, or Linux Environment

- We recommend you to set the database cache size as follows by configuring the -c parameter in the Sybase startup:

Table M-1 Recommended total system memory and Sybase cache memory

Inventoried Workstations in the Database (in thousands)	Total Memory of the System	Sybase Cache Memory
less than 1	384 MB	128 MB
1 - 5	512 MB	128 MB
5 - 10	512 MB - 768 MB	128 MB - 256 MB
10 - 25	768 MB - 1 GB	256 MB - 400 MB
greater than 25	1 - 2 GB	30 - 40% of RAM

- If you have more than 5,000 workstations, we recommend that you use multiprocessors for servers hosting the database and span the data files.
- If you have more than 10,000 workstations, we recommend that you use a dedicated server for the database.
- The following table lists the free hard disk space recommendations:

Table M-2 *Recommended free hard disk space*

Inventoried Workstations in the Database (thousands)	Free Hard Disk Space (GB)
Up to 5	1
Up to 10	2
Up to 15	3
Up to 20	5
Up to 25	6
Up to 30	7
Up to 35	8
Up to 40	9
Up to 45	11

IMPORTANT: Make sure that the drives in which the database files are located have sufficient additional free disk space for storing the temporary files generated during the operations of Inventory ConsoleOne utilities.

- If the Storer is taking significant time to store the inventory information in the following scenarios, you can run the Sybindex utility to improve the Storer performance:
 - Many Inventory agents are simultaneously upgraded to ZENworks 7 and subsequently, all these agents send the full scans for the time to the Inventory server.
 - The administrator manually triggers full scan from the Inventory Service object resulting in all Inventory agents send the full scan to the Inventory server.
 - The Inventory database is either re-installed or changed and then the administrator manually triggers full scan from the Inventory Service object resulting in all Inventory agents sending the full scan to the Inventory server.

Before running the Sybindex utility, make sure that the Sybase Inventory database is up and running, and then stop the Storer.

If you have ZENworks 7 Desktop Management installed, do the following to run the Sybindex utility. If you have ZENworks 7 Desktop Management with Support Pack 1 installed, see [Section M.3, “Performance Tips for the Inventory Server \(Support Pack 1\),” on page 1194](#) to run the Sybindex utility.

On a NetWare server: At the server console prompt, enter sybindex.

On a Windows server: At the server command prompt, go to `inventory_server_installation_path\zenworks\inv\server\wminv\bin` and enter sybindex.

On a Linux server: At the server command prompt, go to `/opt/novell/bin` and enter `sybindex`.

NOTE: If the Sybase Inventory database is either not hosted on the current Inventory server or is running on a port other than 2638, edit the `sybindex.ncf` (on NetWare), `sybindex.bat` (on Windows), or `sybindex` (on Linux) to change the host and port before running `sybindex`.

Changing the Database Cache Size on a NetWare Database Server

- 1 Stop the Inventory service. For more information, see [Section 73.1.5, “Starting and Stopping the Inventory Service,” on page 915](#).
- 2 Close all connections to the Inventory database.
- 3 Quit the Sybase server.
- 4 Open the `mgmt dbs.ncf` file in the `sys:\system` directory.
- 5 Modify the `-c` parameter.
For example, `-c 64M` sets the cache size to 64 MB.
- 6 Save the file.
- 7 On the server console, load the Inventory database. Enter `MGMTDBS`.
- 8 Start the Inventory service. For more information, see [Section 73.1.5, “Starting and Stopping the Inventory Service,” on page 915](#).

Changing the Database Cache Size on a Windows Database Server

- 1 Stop the Inventory service. For more information, see [Section 73.1.5, “Starting and Stopping the Inventory Service,” on page 915](#).
- 2 Stop the Sybase service.
On Windows 2000/2003, in the Control Panel, double-click *Administrative Tools*, double-click *Services*, select *Novell Database - Sybase*, then click *Stop*.
- 3 On the database server, run the `ntdbconfig.exe` file from the `inventory_database_installation_path\zenworks\database\dbengine` directory.
`Ntdbconfig.exe` is a ZENworks database configuration utility for the ZENworks database using Sybase on Windows servers. This utility enables you to reconfigure the Sybase service. For the list of parameters recommended by Sybase, see [“Understanding the Sybase Database Startup Parameters” on page 933](#).
- 4 Modify the `-c` parameter.
- 5 Click *OK*.
- 6 Restart the Sybase service.
On Windows 2000/2003, in the Control Panel, double-click *Administrative Tools*, double-click *Services*, select *Novell Database - Sybase*, then click *Start*.

- 7 Stop the Inventory service. For more information, see [Section 73.1.5, “Starting and Stopping the Inventory Service,” on page 915.](#)

Changing the Database Cache Size on a Linux Database Server

- 1 Stop the Inventory service. For more information, see [Section 73.1.5, “Starting and Stopping the Inventory Service,” on page 915.](#)
- 2 Close all connections to the Inventory database.
- 3 Quit the Sybase server.
- 4 Open the `mgmt dbs .sh` file in the `/opt/novell/zenworks/bin/` directory.
- 5 Modify the `-c` parameter.
For example, `-c 64M` sets the cache size to 64 MB.
- 6 Save the file.
- 7 On the server console, load the Inventory database. Enter `MGMTDBS .`
- 8 Start the Inventory service. For more information, see [Section 73.1.5, “Starting and Stopping the Inventory Service,” on page 915.](#)

For more information on Performance tips, see [Section M.1, “Database Parameter Tuning Tips,” on page 1185.](#)

M.1.2 Oracle in the NetWare, Windows, or Linux Environment

- Use the following memory recommendations:

Table M-3 *Recommended total system memory and Oracle SGA memory*

Inventoried Workstations in the Database (in thousands)	Total Memory of the System	Oracle SGA Memory
less than 1	512 MB	128 MB
1 - 5	768 MB	256 MB
5 - 10	1 GB	400 MB
10 - 100	1 GB - 2 GB	40% of the total memory

- Use the following disk space recommendations:

Table M-4 *Recommended free hard disk space*

Inventoried Workstations in the Database (thousands)	Free Hard Disk Space (GB)
Up to 5	3
Up to 10	6
Up to 15	9
Up to 20	11

Inventoried Workstations in the Database (thousands)	Free Hard Disk Space (GB)
Up to 25	12
Up to 30	13
Up to 35	15
Up to 40	20
Up to 45	25

IMPORTANT: Make sure that the drives in which the database files are located have sufficient additional free disk space for storing the temporary files generated during the operations of Inventory ConsoleOne utilities.

- Stop unnecessary services and applications running on the server to enable a background service such as Oracle server to run.
- We recommend that you use a dedicated server to host the Oracle database.
- Span the data files across multiple physical disks if you have more than 10,000 workstations.
- Set the virtual memory value between 2 - 4 times the RAM.
- We recommend that you use multiprocessors for servers hosting the database.
- Refer to the Oracle performance tuning documentation and other general recommendations that are listed in the [Section M.5, “References,” on page 1198](#) section.
 - Reduce the priority of the foreground application.
 - Reduce the file cache value and maximize data for network applications.
- Modify the `init.ora` file for specific organizational requirements.

For example, to obtain about 260 MB of Oracle SGA with `db_block_size=4096`, modify the `init.ora` file with the following values:

```
db_block_buffers = 50000
shared_pool_size = 32768000
sort_area_size = 10000000
```

- Invoke and append lines to the `_start.sql` file. The `_start.sql` file is invoked by the `mgmtdbo.ncf` or the `mgmtdbo.bat` file when you start the Inventory database instance. Append the following lines to the existing `_start.sql` file:


```
connect mw_dba;alter table cim.t$product cache;
```
- If you run the Inventory database on Oracle9i, you can set `db_cache_size` instead of `db_block_buffers * db_block_size`.
- Refer to the Oracle Administration guide or Performance guide for more information.

M.1.3 Optimizing the Performance of the Oracle Database

If you have an Inventory database on Oracle, you can improve the performance of the database when you generate the inventory reports or query the database.

You use the database buffer cache to store the most recently used data blocks. The database cache is determined as `db_block_buffers * db_block_size`. These parameters are specified in the `zenworks\database\init.ora` file on the database server.

`DB_BLOCK_BUFFERS` specifies the number of database buffers. `DB_BLOCK_SIZE` specifies the size of each database buffer in bytes.

The size of each buffer in the buffer cache is equal to the size of the data block.

If there is additional memory, you configure the database cache size by increasing the `DB_BLOCK_BUFFERS` parameter in the `init.ora` file. If you run Inventory database on Oracle9i, you can set `db_cache_size` instead of `db_block_buffers * db_block_size`

For more information for Performing tips, see [Section M.1, “Database Parameter Tuning Tips,” on page 1185](#).

M.1.4 MS SQL in the Windows Environment

- We recommend that you use a dedicated server for MS SQL.
- On the MS SQL server, make sure that the tempdb system database is located on the drive having sufficient disk space.
- Boost the MS SQL server priority.
- Enable optimization for background services.
- Use the configuration in the following table:

Table M-5 *Recommended total system memory, processor speed and MS SQL cache memory*

Inventoried Workstations in the Database (thousands)	Total Memory of the System	MS SQL Cache Memory	Processor Speed
less than 10	512 MB	256 MB	Pentium III: 450 M Hz
10 - 20	512 MB - 1 GB	256 MB - 384 MB	Pentium 4: 1.8 G Hz
20 - 50	1 GB - 1.5 GB	512 MB - 768 MB	Pentium 4: 1.8 G Hz

- Use the following disk space recommendations:

Table M-6 *Recommended free hard disk space*

Inventoried Workstations in the Database (thousands)	Free Hard Disk Space (GB)
Up to 5	5
Up to 10	10
Up to 15	15
Up to 20	20
Up to 25	26

Inventoried Workstations in the Database (thousands)	Free Hard Disk Space (GB)
Up to 30	31
Up to 35	36
Up to 40	41
Up to 45	46

- Span the data files across the multiple physical disks if you have more than 5,000 workstations.
- We recommend that you use multiprocessors for servers hosting the database.
- For additional tips on MS SQL, refer to the [MS SQL Server documentation \(http://www.sql-server-performance.com/default.asp\)](http://www.sql-server-performance.com/default.asp).

M.2 Improving the Throughput of the Inventory Storer

You can now improve the throughput of the Inventory Storer by deploying multiple Root Servers to directly store the inventory data to the Oracle 9.2.0.6 Inventory database.

The following sections provide more information:

- [Section M.2.1, “Factors to be Considered Before Deployment,” on page 1191](#)
- [Section M.2.2, “Procedure to Improve the Throughput,” on page 1191](#)
- [Section M.2.3, “Recommendations for Administering the ZENworks Inventory Server,” on page 1193](#)
- [Section M.2.4, “Recommendations for Administering the Inventory Database,” on page 1194](#)

M.2.1 Factors to be Considered Before Deployment

- **Network Topology:** The Root Servers and the Database server must be located in the same LAN.
- **Frequency of Scans Received by the Inventory Server:** Large number of scans to be processed within a short duration. For example, scanning 25000 workstations every day.
- **Scan Type:** An initial FULL scan storage would take more time compared to subsequent DELTA scan times.
- **Total number of Root Servers:** If the size of the scan files is smaller, you can achieve a better throughput by deploying a maximum of 6 to 8 Root Servers. But if you deploy more than 8 servers, the throughput might degrade. All servers that you plan to deploy must be receive approximately equivalent number of scans.

M.2.2 Procedure to Improve the Throughput

- 1 Make sure that the Inventory database has been successfully migrated.
- 2 Stop the Inventory service and the Inventory database.
- 3 Configure a minimum of two Root Servers but a maximum of eight Root Servers to store the inventory data to an Oracle 9.2.0.6 Inventory database.

4 Make sure that the Database server has the following requirements:

- Three physical disks
- Each disk has a drive with at least 30 GB free disk space
- Two Pentium IV processors with 2.4 GHz and 2 GB RAM

For example, on Windows let's assume that the C drive is on disk1, the E drive on disk2, and the F drive on disk3. And the F drive contains the database files.

5 Create the following directory structure for database files on all the three drives:

`drive_name\zenworks\inventory\oracle\database`

For example:

```
c:\zenworks\inventory\oracle\database\  
f:\zenworks\inventory\oracle\database\  
e:\zenworks\inventory\oracle\database\
```

Let's assume that all the inventory database files are present in
`f:\zenworks\inventory\oracle\database`.

6 Move the following database files from

`f:\zenworks\inventory\oracle\database` as explained below:

- Move `log1.ora`, `cim8.ora`, `cim81.ora`, `cim82.ora`, and `index1.ora` to
`c:\zenworks\inventory\oracle\database`.
- Move the following files to `e:\zenworks\inventory\oracle\database`:

```
rbs1.ora  
tmp1.ora  
cim1.ora  
cim2.ora  
cim21.ora  
cim3.ora  
cim4.ora  
cim5.ora  
cim51.ora  
cim7.ora  
cim71.ora  
cim72.ora  
index2.ora
```

7 Edit the `f:\zenworks\inventory\oracle\database\init.ora` file to set values for the following parameters as mentioned:

```
db_cache_size=700000000 or above  
shared_pool_size = 300000000 or above  
pga_aggregate_target=300000000 or above  
sort_area_size=10000000 or above  
log_buffer = 1024000 or above  
compatible=8.1.6.0.0 or above  
open_cursors=2048
```

```
session_cached_cursors=2048
```

```
processes=200
```

- 8** Extract the platform-specific `atlasperf_alterctrl.sql` from `ZENworks_installation_directory\zenworks\inv\server\wminv\properties\sql.zip`.

If Oracle is running on Windows, extract `atlasperf_alterctrl.sql` from the `oracle\winntspecific` directory within `sql.zip`.

If Oracle is running on Unix, extract `atlasperf_alterctrl.sql` from the `oracle\unixspecific` directory within `sql.zip`.

- 9** Modify the file paths in `atlasperf_alterctrl.sql`, if required, and execute `atlasperf_alterctrl.sql` at the SQLPLUS prompt.

- 10** Start the Inventory database.

- 11** Extract the `\oracle\common\atlasperf_alterfreelist.sql` file from `ZENworks_installation_directory\zenworks\inv\server\wminv\properties\sql.zip`, and execute `atlasperf_alterfreelist.sql` at the SQLPLUS prompt.

- 12** Open the Oracle Enterprise Manager console, and make sure that all the indices and primary key constraints of the following tables are set to Degree of the Parallel option - Default, NOLOGGING and Free Lists is 10:

```
zenworks.t$installedproduct
cim.t$product
mw_dba.installedsoftwarepatch
mw_dba.patch
mw_dba."file"
mw_dba.installedfile
```

- 13** On all Inventory servers, edit `ZENworks_installation_directory\zenworks\inv\server\wminv\properties\storerdebug.properties` to set the value of the following parameters as mentioned:

```
filebatchupdate=true
cursorclosedelay=500
```

- 14** Start the Inventory services on all the Inventory servers that are connected to this database.

M.2.3 Recommendations for Administering the ZENworks Inventory Server

- Avoid or minimize the frequency of importing or removing workstations because it would result in many FULL scans.
- Avoid NDS time out of sync situation because it may trigger FULL scans.
- Trigger FULL scan on the Inventory service object only if required because it would trigger FULL scans on all inventoried machines connected to the Inventory server.
- Balance the load of inventory scan and zip files on each server.
- Stagger the inventory scan and the roll-up schedule.

- Avoid scheduling too many frequent scans and roll-ups such as daily scans and daily roll-ups.
- Minimize the scanning of unknown application files and tune the software dictionary. For detailed information, see [Section 76.3.30, “Base-Lining the Software Dictionary Deployment,” on page 1078](#).

M.2.4 Recommendations for Administering the Inventory Database

- Resize the Oracle SGA parameters appropriately to handle the concurrent updates.
- Configure appropriate database server hardware requirements such as adding memory, disks.
- If required, rebuild the indices in the database and scatter them to different tablespaces. Do not have more than one index of the same table on a tablespace.
- Scatter the data files on multiple physical disks.
- Apply the standard recommendations as suggested in the Oracle administration or Performance guides.
- Use a dedicated network between the Inventory server and the Inventory database. For example, 100 MBPS.
- Add enough rollback segments and properly size them to avoid the ORA-01555 error.
- If a large number of workstations are processed for FULL scan, delete old database and use a new database.

M.3 Performance Tips for the Inventory Server (Support Pack 1)

IMPORTANT: Review this section only if you installed ZENworks 7 Desktop Management with Support Pack 1

- The Server Inventory service might demand high (up to 100%) processor utilization in the following scenarios:
 - Many Inventory agents are simultaneously upgraded to ZENworks 7 and subsequently, all these agents send the full scans for the time to the Inventory server.
 - The administrator manually triggers full scan from the Inventory Service object resulting in all Inventory agents send the full scan to the Inventory server.
 - The Inventory database is either re-installed or changed and then the administrator manually triggers full scan from the Inventory Service object resulting in all Inventory agents sending the full scan to the Inventory server.
 - The Server Inventory process or other applications are running on the ZENworks server.
 - The indexes of the Inventory database might have to be recreated.
- 1** If the utilization rate is unacceptable, or if the Inventory Storer takes a considerable amount of time to store the inventory data, perform the following tasks to improve the Inventory server performance:
- 1** Stop the Inventory Service. For more information, see [Section 73.1.5, “Starting and Stopping the Inventory Service,” on page 915](#).

- 2 Close all instances of ConsoleOne that are connected to this database.
- 3 If your Inventory database is running on Sybase, modify the database indexes using the sybindex utility.
 - To run the sybindex utility on a NetWare server:
 1. On the Inventory server, extract *Inventory_server_installation_path\zenworks\inv\server\wminv\properties\sql.zip* to a temporary directory retaining the directory structure. For example, extract *sql.zip* to *sys:\sql*. The temporary directory contains the Sybase directory.
 2. If the Sybase Inventory database is either not hosted on the Inventory server or is running on a port other than 2638, edit *Inventory_server_installation_path\zenworks\inv\server\wminv\properties\sqlupdater.properties* to specify the host and port on which the Sybase Inventory database is running.
 3. At the Inventory server system console prompt, enter:


```
sybindex -path
complete_path_of_sql.zip_extracted_directory\sybase.
```

 For example, *sybindex -path sys:\sql\sybase* where *sql* is the directory to which *sql.zip* is extracted in Step 1.
 - To run the sybindex utility on a Windows server:
 1. On the Inventory server, extract *Inventory_server_installation_path\zenworks\inv\server\wminv\properties\sql.zip* to a temporary directory retaining the directory structure. For example, extract *sql.zip* to *c:\sql*. The temporary directory contains the Sybase directory.
 2. If the Sybase Inventory database is either not hosted on the Inventory server or is running on a port other than 2638, edit *Inventory_server_installation_path\zenworks\inv\server\wminv\properties\sqlupdater.properties* to specify the host and port on which the Sybase Inventory database is running.
 3. At the Inventory server command prompt, navigate to *Inventory_server_installation_path\zenworks\inv\server\wminv\bin*, and enter


```
sybindex -path
complete_path_of_sql.zip_extracted_directory/sybase.
```

 For example, *sybindex -path c:\sql\sybase* where *sql* is the directory to which *sql.zip* is extracted in Step 1.
 - To run the Sybindex utility on a Linux server:
 1. On the Inventory server, extract */etc/opt/novell/zenworks/inv/sql.zip* to a temporary directory retaining the directory structure. For example, extract *sql.zip* to */home/user*. The temporary directory contains the Sybase directory.
 2. If the Sybase Inventory database is either not hosted on the Inventory server or is running on a port other than 2638, edit */etc/opt/novell/zenworks/inv/SQLUpdater.properties* to specify the host and port on which the Sybase Inventory database is running.

3. At the Inventory server command prompt, navigate to `/opt/novell/bin`, and enter
`sybindex -path
complete_path_of_sql.zip_extracted_directory/sybase.`
For example, `sybindex -path home/user/sql/sybase`

NOTE: This execution might take significant amount of time to complete depending on the database size.

- 4 If your Inventory database is running MSSQL database, execute the following scripts available in the MSSQL directory of
`Inventory_server_installation_path\zenworks\inv\server\wminv\properties\sql.zip` with appropriate user logins as explained below from the MS SQL Query Analyzer:

- Log in as CIM and execute `mssql_perf_cim.sql`.
- Log in as ZENworks and execute `mssql_perf_zenworks`.
- Log in as ManageWise and execute `mssql_perf_managewise`.
- Log in as MW_DBA and execute `mssql_perf_mw_dba`.

Ignore any warnings related to DROP statements during the script execution.

- 5 Restart the Inventory Service. For more information, see [Section 73.1.5, “Starting and Stopping the Inventory Service,” on page 915](#).
- 6 Restart the ConsoleOne.
- 7 To improve the throughput of the Storer, you can tune the parameters of the service.
 - 7a Stop the Inventory service. For more information, see [Section 73.1.5, “Starting and Stopping the Inventory Service,” on page 915](#).
 - 7b Run a text editor and navigate to the
`Inventory_server_installation_path\zenworks\inv\server\wminv\properties` directory.
 - 7c Open the `storerdebug.properties` file, make the following value change to the uncommented parameter:
`filebatchupdate=true`
 - 7d Save the changes and close the file.
 - 7e Restart the Inventory service. For more information, see [Section 73.1.5, “Starting and Stopping the Inventory Service,” on page 915](#).

M.4 Performance Tips for the Inventory ConsoleOne Utilities

This section discusses the performance tips for the following Inventory ConsoleOne utilities:

- [“Inventory Reports Performance Tips” on page 1197](#)
- [“Inventory Data Export Performance Tips” on page 1197](#)
- [“Inventory Query Performance Tips” on page 1197](#)

NOTE: If the Inventory ConsoleOne utilities are retrieving data from a large database, you must stop the Storer service before running the utilities. This improves the performance of the ConsoleOne utilities.

If your database is huge, make sure that the machine running the Inventory ConsoleOne utilities has at least 5 GB free hard disk space.

M.4.1 Inventory Reports Performance Tips

- If you have more than 1000 workstations in your database, listing all of the subreports consumes time. We recommend that you specify the list of subreports. By doing so, the general performance of the reports is improved.
- If your Inventory database is running on MS SQL, execute the following script at the Inventory server console prompt before generating Inventory reports:

```
CREATE INDEX i$FkPinstanceId ON  
ZENworks.t$InstalledProduct(fk_pinstanceid) ON CIM9
```

The script helps in generating the reports in optimal time.

M.4.2 Inventory Data Export Performance Tips

- To maximize the performance of Inventory Data Export, you need to enable the filter condition in Database Export. Based on the query you specify, the Database Export exports only selected software.
- During export, deselect the attributes that you do not want to use. To do this, use the *Database Export* and the *Required Attributes Only* option.
- Perform the software export separately. This greatly improves the performance of the Non-Software Export function.

M.4.3 Inventory Query Performance Tips

- Specify queries using the AND condition in multiple groups to increase performance.
- Split a complex query with several logical operators into multiple groups separated by a logical operator.
- If you want to use a complex query, increase the database cache size. For more information on tuning databases, see [Section M.1, “Database Parameter Tuning Tips,” on page 1185](#).
- Save fast, narrowed-down queries for future use.
- Do not invoke the Inventory Query by connecting to a database over a slow link.
- If a complex query takes more than 10 minutes to execute over a fast link, you probably do not have any workstations that match the query you specified. The following message is displayed:

```
No Computer system matched the query
```

Close the Result window, narrow your input query and retry. Repeat the process of narrowing your query until you locate your workstations.

- For optimal performance, we recommend that you do not use more than four groups and not more than three logical operators separating the four groups in your query.

- If you know the exact logical string, avoid using the MATCHES operator. The MATCHES operator searches the database for a result based on the pattern you specify. This results in performance degradation.
- If you want to check for a particular inventory component not stored in the Inventory database, use the (ISNULL) operator instead of a query with a regular attribute.

M.5 References

For additional information on performance tuning tips, refer to the following documentation for specific components:

- [MS SQL performance information \(http://www.sql-server-performance.com\)](http://www.sql-server-performance.com)
- Oracle9i Database and Performance guide and reference
- Oracle9i Database Administrator's guide

Hardware Information Collected by the Inventory Scanners

N

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

Table N-1 Hardware information collected on the NetWare inventoried servers

Scan Data	DMI Class and Attribute	WMI Class and Attribute
System.Manufacturer	DMTF Component 1	Win32_ComputerSystemProduct.Vendor
System.MachineName	Not applicable	Win32_ComputerSystem.Caption
System.AssetTag	DMTF System Enclosure 001.2	Not applicable
System.Model	DMTF Component 2	Win32_ComputerSystemProduct.Name
System.ModelNumber	Not applicable	Not applicable
System.SystemIdentifier(GUID)	Not applicable	Not applicable
System.SerialNumber	DMTF Component 3	Win32_ComputerSystemProduct.IdentifyingNumber
System.Tag	Not applicable	Not applicable
System.ManagementTechnology	Not applicable	Not applicable
eDirectory.DNName	Not applicable	Not applicable
eDirectory.TreeName	Not applicable	Not applicable
NetworkAdapter.MACAddress	Not applicable	Win32_NetworkAdapterConfiguration.MACAddress (Only on Windows 2000/XP; get it through association with Win32_NetworkAdapterSetting)
IP.Address	Not applicable	Win32_NetworkAdapterConfiguration.IPAddress (Only on Windows 2000/XP; get it through association with Win32_NetworkAdapterSetting)

Scan Data	DMI Class and Attribute	WMI Class and Attribute
IP.Subnet (Subnet Mask)	Not applicable	Win32_NetworkAdapterConfiguration.IPSubnet (Only on Windows 2000/XP; get it through association with Win32_NetworkAdapterSetting)
NetworkAdapter.MACAddress	Not applicable	Win32_NetworkAdapterConfiguration.MACAddress (Only on Windows 2000/XP; get it through association with Win32_NetworkAdapterSetting)
IPX.Address	Not applicable	Win32_NetworkAdapterConfiguration.IPXAddress (Only on Windows 2000/XP; get it through association with Win32_NetworkAdapterSetting)
NetworkAdapter.MACAddress	Not applicable	Win32_NetworkAdapterConfiguration.MACAddress (Only on Windows 2000/XP; get it through association with Win32_NetworkAdapterSetting)
DNS.HostName	Not applicable	Win32_NetworkAdapterConfiguration.DNSHostName + DNSDomain (Only on Windows 2000/XP; get it through association with Win32_NetworkAdapterSetting)
Modem.Description	Not applicable	Win32_POTSModem.Description
Modem.Name	Not applicable	Win32_POTSModem.Name
Modem.Vendor	Not applicable	Not applicable
Modem.DeviceID	Not applicable	Win32_POTSModem.DeviceID
NetworkAdapter.DriverVersion	DMTF Network Adapter Driver 001.Driver Software Version	Not applicable
Login.CurrentLoggedInUser	Not applicable	Not applicable
Login.LastLoggedIn User	Not applicable	Not applicable
Login.DomainName	Not applicable	Win32_ComputerSystem.Domain
NWClient.Version	Not applicable	Not applicable
Processor.stepping	Not applicable	CIM_Processor.Stepping
Processor.DeviceID	Not applicable	CIM_Processor.DeviceID
Processor.Family	DMTF Processor 004.3	CIM_Processor.Family
Processor.OtherFamily	Not applicable	CIM_Processor.OtherFamilyDescription

Scan Data	DMI Class and Attribute	WMI Class and Attribute
Processor.MaxClockSpeed	DMTF Processor 004.5	CIM_Processor.MaxClockSpeed
Processor.CurrentClockSpeed	DMTF Processor 004.6	CIM_Processor.CurrentClockSpeed
Processor.Role	DMTF Processor 004.2	CIM_Processor.ProcessorType
Processor.Upgrade	DMTF Processor 004.7	CIM_Processor.UpgradeMethod
Processor.Description	DMTF Processor 004.4	CIM_Processor.Description
Processor.Name	Enum equivalent of DMTF Processor 004.3	CIM_Processor.Name
BIOS.Manufacturer	DMTF SystemBIOS 001.2	Win32_BIOS.Manufacturer
BIOS.BIOSDate	Not applicable	Win32_BIOS.InstallDate
BIOS.BIOSIDBytes	Not applicable	Not applicable
BIOS.Copyright	Not applicable	Win32_BIOS.Caption
BIOS.SerialNumber	Not applicable	Win32_BIOS.SerialNumber
BIOS.BIOSType	DMTF SystemBIOS 001.3	Win32_BIOS.SMBIOSBIOSVersion
BIOS.PrimaryBIOS	DMTF SystemBIOS 001.9	Win32_BIOS.PrimaryBIOS
BIOS.Size	DMTF SystemBIOS 001.4	Not applicable
Bus.Type	Not applicable	Win32_Bus.BusType
Bus.Name	Not applicable	Win32_Bus.Name
Bus.Description	Not applicable	Win32_Bus.Descriptipon
Bus.Version	Not applicable	Not applicable
Bus.DeviceID	Not applicable	Win32_Bus.DeviceID
IRQ.Number	DMTF IRQ 002.IRQNumbe r	CIM_IRQ.IRQNumber
IRQ.Availability	DMTF IRQ 002.Availability	CIM_IRQ.Availability
IRQ.TriggerType	DMTF IRQ 002.TriggerTyp e	CIM_IRQ.TriggerType
IRQ.Shareable	DMTF IRQ 002.Shareable	CIM_IRQ.Shareable
Keyboard.Layout	DMTF Keyboard 003.Layou t	CIM_Keyboard.Layout
Keyboard.Subtype	Not applicable	Not applicable
Keyboard.Type	DMTF Keyboard 003.Keyb oard.Type	CIM_Keyboard.Description
Keyboard.Fkeys	Not applicable	CIM_Keyboard.NumberOfFunctionKeys
Keyboard.Delay	Not applicable	Not applicable
Keyboard.TypeomaticRate	Not applicable	Not applicable

Scan Data	DMI Class and Attribute	WMI Class and Attribute
VideoAdapter.NumberOfColorPlanes (NEW)	Not applicable	Win32_VideoController.NumberOfColorPlanes
VideoAdapter.HorizontalResolution	DMTF Video 004.Current Horizontal Resolution	Win32_VideoController.CurrentHorizontalResolution
VideoAdapter.VerticalResolution	DMTF Video 004.Current Vertical Resolution	Win32_VideoController.CurrentVerticalResolution
VideoAdapter.DisplayType	DMTF Video 004.Video Type	Win32_VideoController.VideoArchitecture
VideoAdapter.MemoryType	DMTF Video 004.Video Memory Type	Win32_VideoController.VideoMemoryType
VideoAdapter.MaxMemorySupported	DMTF Video 004.Video RAM Memory Size	Win32_VideoController.AdapterRAM
VideoAdapter.Bitsperpixel	DMTF Video 004.Current Number of Bits per Pixel	Win32_VideoController.CurrentBitsPerPixel
VideoAdapter.ControllerDescription	DMTF Video 004.Video Controller Description	Win32_VideoController.Description
VideoAdapter.MaxRefreshrate	DMTF Video 004.Maximum Refresh Rate	Win32_VideoController.MaxRefreshRate
VideoAdapter.MinRefreshrate	DMTF Video 004.Minimum Refresh Rate	Win32_VideoController.MinRefreshRate
VideoAdapter.DACType	Not applicable	Win32_VideoController.AdapterDACType
VideoAdapter.ChipSet	Not applicable	Win32_VideoController.VideoProcessor
VideoAdapter.ProviderName	Not applicable	Win32_VideoController.VideoAdapterCompatibility
VideoBIOS.VideoBIOSManufacturer	DMTF Video BIOS 001.BIOS Manufacturer	CIM_VideoBIOSElement.Manufacturer
VideoBIOS.VideoBIOSVersion	DMTF Video BIOS 001.Video.BIOS Version	CIM_VideoBIOSElement.Version
VideoBIOS.VideoBIOSReleaseDate	DMTF Video BIOS 001.Video.BIOS Release Date	CIM_VideoBIOSElement.InstallDate
VideoBIOS.VideoBIOS.IsShadowed	DMTF Video BIOS 001.Video.Shadowing State	CIM_VideoBIOSElement.IsShadowed
ParallelPort.Name	DMTF Parallel Ports 003.Parallel Port Index	CIM_ParallelController.Name
ParallelPort.DMASupport	DMTF Parallel Ports 003.DMA Support	CIM_ParallelController.DMASupport

Scan Data	DMI Class and Attribute	WMI Class and Attribute
ParallelPort.Address	DMTF Parallel Ports 003.Parallel Base I/O Address	Not applicable
ParallelPort.IRQ	DMTF Parallel Ports 003.IRQ Used	Not applicable
SerialPort.Name	DMTF Serial Ports 004.Serial Port Index	CIM_SerialController.Name
SerialPort.Address	DMTF Serial Ports 004.Serial Base I/O Address	Not applicable
SerialPort.IRQ	DMTF Serial Ports 004.IRQ Used	Not applicable
FloppyDrive.DeviceID	DMTF Logical Drives 001.Logical Drive Name (when DMTF Logical Drives 001.Logical Drive Type=Floppy Drive(7))	Win32_LogicalDisk.DeviceID (where Win32_LogicalDisk.DriveType = 2 (Removable Disk) and Win32_LogicalDisk.MediaType = [1,10])
FloppyDrive.Manufacture	Not applicable	Not applicable
FloppyDrive.Description	Hard Code: Floppy Drive (when DMTF Disks 003.Storage Type=Floppy Disk(4))	Win32_LogicalDisk.Description (where Win32_LogicalDisk.DriveType = 2 (Removable Disk) and Win32_LogicalDisk.MediaType = [1,10])
FloppyDrive.MaxNumberOfCylinders	Not applicable	Not applicable
FloppyDrive.NumberOfHeads	Not applicable	Not applicable
FloppyDrive.SectorsPerTrack	Not applicable	Not applicable
FloppyDrive.Size	DMTF Logical Drives 001.Logical Drive Size (when DMTF Logical Drives 001.Logical Drive Type = Floppy Drive(7))	Win32_LogicalDisk.Size (where Win32_LogicalDisk.DriveType = 2 (Removable Disk) and Win32_LogicalDisk.MediaType = [1,10])
CDROMDrive.DeviceID	DMTF Logical Drives 001.Logical Drive Name (When DMTF Logical Drives 001.Logical Drive Type = 6)	Win32_CDROMDrive.Drive
CDROMDrive.Manufacture	Not applicable	Win32_CDROMDrive.Manufacturer
CDROMDrive.Description	Not applicable	Win32_CDROMDrive.Description

Scan Data	DMI Class and Attribute	WMI Class and Attribute
CDROMDrive.Caption	Hard code: CDROM Device (when DMTF Disks 001.Logical Drive Type = 6)	Win32_CDROMDrive.Caption
HardDrive.Media Type	DMTF Disks 003.Removable Media	Win32_DiskDrive.MediaType
HardDrive.Vendor	Not applicable	Win32_DiskDrive.Manufacturer
HardDisk.Description	DMTF Disks 003.Interface Description (when DMTF Disks 003.Storage Type=Hard Disk(3))	Win32_DiskDrive.Description
HardDisk.Cylinders	DMTF Disks 003.Number of Physical Cylinders	Win32_DiskDrive.TotalCylinders
HardDisk.Heads	DMTF Disks 003.Number of Physical Heads	Win32_DiskDrive.TotalHeads
HardDisk.Sectors	DMTF Disks 003.Number of Physical Sectors per Track	Win32_DiskDrive.SectorsPerTrack
HardDisk.Capacity	DMTF Disks 003.Total Physical Size	Win32_DiskDrive.Size
LogicalDrive.Name	Not applicable	Win32_LogicalDiskDeviceID (when Win32_LogicalDisk.DriveType = 3 (Local Disk))
LogicalDrive.VolumeSerialNumber	Not applicable	Win32_LogicalDisk.VolumeSerialNumber (when Win32_LogicalDisk.DriveType = 3 (Local Disk))
LogicalDrive.Volume (Volume Label)	Not applicable	Win32_LogicalDisk.VolumeName (when Win32_LogicalDisk.DriveType = 3 (Local Disk))
Operating System.OSType	Not applicable	Win32_OperatingSystem.OSType
OperatingSystem.Version	Not applicable	Not applicable
OperatingSystem.Codepage	Not applicable	Win32_OperatingSystem.CodeSet
OperatingSystem.InstallDate	Not applicable	Win32_OperatingSystem.InstallDate
OperatingSystem.TotalSwapSpaceSize	DMTF System Memory Settings 001.Total Size of Paging Files	Win32_OperatingSystem.SizeStoredInPagingFiles
OperatingSystem.Description	DMTF Operating System 001.Operating System Description	Win32_OperatingSystem.Caption

Scan Data	DMI Class and Attribute	WMI Class and Attribute
OperatingSystem.OtherTypeDescription	Not applicable	Win32_OperatingSystem.OtherTypeDescription
OperatingSystem.VirtualMemorySize	DMTF System Memory Settings 001.Total Virtual Memory	Win32_OperatingSystem.TotalVirtualMemory
OperatingSystem.VisibleMemorySize	Not applicable	Win32_OperatingSystem.TotalVisibleMemorySize
OperatingSystem.Role	Not applicable	Not applicable
InventoryScanner.Version	Not applicable	Not applicable
InventoryScanner.LastScanDate	Not applicable	Not applicable
InventoryScanner.InventoryServer	Not applicable	Not applicable
InventoryScanner.ScanMode	Not applicable	Not applicable
InventoryScanner.GeneralDictionaryVersion	Not applicable	Not applicable
InventoryScanner.PrivateDictionaryVersion	Not applicable	Not applicable
SoundCard.Description	Not applicable	Win32_SoundDevice.Description
SoundCard.Name	Not applicable	Win32_SoundDevice.Name
SoundCard.Manufacturer	Not applicable	Win32_SoundDevice.Manufacturer
Cache.Level	DMTF System Cache 003.System Cache Level	Win32_CacheMemory.Level
Cache.WritePolicy	DMTF System Cache 003.System Cache Write Policy	Win32_CacheMemory.WritePolicy
Cache.ErrorCorrection	DMTF System Cache 003.System Cache Error Correction	Win32_CacheMemory.ErrorCorrectType
Cache.Type	DMTF System Cache 003.System Cache Type	Win32_CacheMemory.CacheType
Cache.LineSize	DMTF System Cache 003.Line Size	Win32_CacheMemory.LineSize
Cache.ReplacementPolicy	DMTF System Cache 003.Replacement Policy	Win32_CacheMemory.ReplacementPolicy
Cache.ReadPolicy	DMTF System Cache 003.Read Policy	Win32_CacheMemory.ReadPolicy

Scan Data	DMI Class and Attribute	WMI Class and Attribute
Cache.Associativity	DMTF System Cache 003.Associativity	Win32_CacheMemory.Associativity
Cache.Speed	DMTF System Cache 003.System Cache Speed	Win32_CacheMemory.CacheSpeed
Cache.Size	DMTF System Cache 003.System Cache Size	Win32_CacheMemory.MaxCacheSize
MotherBoard.Version	Not applicable	Win32_BaseBoard.Version
MotherBoard.Description	Not applicable	Win32_BaseBoard.Description
MotherBoard.Slots	DMTF Motherboard 001.Nu mber of Expansion slots	Not applicable
MotherBoard.Manufacture	Not applicable	Win32_BaseBoard.Manufacture
Battery.Name	DMTF Portable Battery 002.Portable Battery Device Name	Win32_Battery.Name
Battery.Chemistry	DMTF Portable Battery 002.Portable Battery Device Chemistry	Win32_Battery.Chemistry
Battery.Capacity	DMTF Portable Battery 002.Portable Battery Design Capacity	Win32_Battery.DesignCapacity
Battery.Voltage	DMTF Portable Battery 002.Portable Battery Design Voltage	Win32_Battery.DesignVoltage
Battery.Version	DMTF Portable Battery 002.Portable Battery Smart Battery Version	Win32_Battery.SmartBatteryVersion
Battery.Manufacturer	DMTF Portable Battery 002.Portable Battery Manufacturer	Win32_PortableBattery.Manufacturer
Battery.ManufactureDate	DMTF Portable Battery 002.Portable Battery Manufacturer Date	Win32_Battery.InstallDate
Battery.SerialNumber	DMTF Portable Battery 002.Portable Battery Serial Number	Not applicable
PowerSupply.InputVoltageDes cription	DMTF Power Supply 002.Power Supply Input Voltage Capability Description	CIM_UninterruptiblePowerSupply.Descrip tion

Scan Data	DMI Class and Attribute	WMI Class and Attribute
PowerSupply.Power	DMTF Power Supply 002.Total Output Power	CIM_UninterruptiblePowerSupply.TotalOutputPower
DMA.Number	DMTF DMA 001.DMA Number	CIM_DMA.DMAChannel
DMA.Description	DMTF DMA 001.DMA Description	CIM_DMA.Description
DMA.Availability	DMTF DMA 001.DMA Channel Availability	CIM_DMA.Availability
DMA_BurstMode	DMTF DMA 001.DMA BurstMode	CIM_DMA.BurstMode
UCS.DNName	Not applicable	Not applicable
UCS.PrimaryOwnerContact	DMTF General Information 001.3	CIM_UnitaryComputerSystem.PrimaryOwnerContact
UCS.PrimaryOwnerName	DMTF General Information 001.4	CIM_UnitaryComputerSystem.PrimaryOwnerName
PointingDevice.DeviceType	DMTF Pointing Device Pointing Device Type(1)	CIM_PointingDevice.PointingType
PointingDevice.Type	DMTF Pointing Device Pointing Device Interface (2)	CIM_PointingDevice.Name
PointingDevice.NumberOfButtons	DMTF Pointing Device Pointing Device Buttons (4)	CIM_PointingDevice.NumberOfButtons
PointingDevice.DriverName	DMTF Pointing Device Pointing Device Driver Name (6)	Not applicable
PointingDevice.DriverVersion	DMTF Pointing Device Pointing Device Driver Version (7)	CIM_PointingDevice.Name
PointingDevice.IRQ	DMTF Pointing Device Pointing Device IRQ (3)	Not applicable
Slot.Description	DMTF System Slots 003.Description	Win32_SystemSlot. SlotDesignation
Slot.MaxDataWidth	DMTF System Slots 003.MaxDataWidth	Win32_SystemSlot. MaxDataWidth
Slot.ThermalRating	DMTF System Slots 003.Slot Thermal Rating	Win32_SystemSlot. ThermalRating

Scan Data	DMI Class and Attribute	WMI Class and Attribute
FileSystem.Drive	Not applicable	Win32_LogicalDisk.DeviceID (when Win32_LogicalDisk.DriveType = 3 (Local Disk))
FileSystem.FileSystemSize	Not applicable	Win32_LogicalDisk.Size (when Win32_LogicalDisk.DriveType = 3 (Local Disk))
FileSystem.AvailableSpace	Not applicable	Win32_LogicalDisk.FreeSpace (when Win32_LogicalDisk.DriveType = 3 (Local Disk))
FileSystem.FileSystem	Not applicable	Win32_LogicalDisk.FileSystem (when Win32_LogicalDisk.DriveType = 3 (Local Disk))
Monitor.Device ID	Not applicable	Not applicable
Monitor.Description	Not applicable	Not applicable
Monitor.Manufacturer Date	Not applicable	Not applicable
Monitor.Model ID	Not applicable	Not applicable
Monitor.ViewableSize (inches)	Not applicable	Not applicable
Monitor.NominalSize (inches)	Not applicable	Not applicable
Monitor.Serial Number	Not applicable	Not applicable
Monitor.Manufacturer	Not applicable	Not applicable
Monitor.Model	Not applicable	Not applicable
Chassis.Type (enum)	DMTF Physical Container Global Table 1	Win32_SystemEnclosure. ChassisTypes
Chassis.Manufacturer	DMTF FRU 4	Win32_SystemEnclosure. Manufacturer
Chassis.SerialNumber	DMTF FRU 7	Win32_SystemEnclosure. SerialNumber
Chassis.AssetTag	DMTF Physical Container Global Table 2	Win32_SystemEnclosure. SMBIOSAssetTag
Chassis.Version	Not applicable	Win32_SystemEnclosure. Version
Chassis.NumberOfPowerCords	Not applicable	Win32_SystemEnclosure. NumberOfPowerCords
Chassis.Tag	Not applicable	Win32_SystemEnclosure. Tag

NOTE: PCMCIA modems are connected to the computer through the PCMCIA slots on the inventoried workstations. The Scanner detects PCMCIA modems that are active on the computer. If you want to know which modem is installed on the computer, use the Windows System Device Manager on the Windows workstation.

Non-PCMCIA modems are connected to the computer through the external ports. For example, some non-PCMCIA modems are connected through the serial ports. The Scanner detects non-PCMCIA modems that are installed on the computer.

Non-PCMCIA modems might not be active at the time of scanning. Also, these modems might not be connected, although they are configured on the computer. In this case, the Scanner detects the modem and reports the scan information of the modem.

The Inventory scanner reports inventory information for the monitors that are manufactured only after 1997.

ZENworks 7 Desktop Management Inventory Attributes



The following table lists the Workstation Inventory attributes that ZENworks® 7 Desktop Management uses.

Each row in the table has:

- The name of the attribute as displayed in the Inventory Database Export Wizard in ConsoleOne
- The name of the attribute in the exported .csv file (first row in the .csv file)
- The inventory database attribute name
- The type of the attribute in the Inventory database
- The length of the attribute in the Inventory database
- A brief description of the attribute

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

Table O-1 Workstation Inventory attributes used in ZENworks Desktop Management

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
General-NDSName-Label	NDSName_LABEL	ManageWise.NDSName.Label	String	254	The DN name of the inventoried workstation registered in Novell® eDirectory™.
SystemInfo.Description	Asset_Description	Zenworks.SystemInfo.Description	String	254	Description of the system asset information.
SystemInfo.Caption	Asset_Caption	Zenworks.SystemInfo.Caption	String	64	Identifying information of the computer.
SystemInfo.Tag	Asset_Asset Tag	Zenworks.SystemInfo.Tag	String	254	Asset tag number that the ROM-based setup program creates. This is unique to every inventoried workstation.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
SystemInfo.ModelNumber	Asset_Model Number	Zenworks.SystemInfo.Model	String	64	Model number value for the computer, assigned during manufacture.
SystemInfo.SerialNumber	Asset_Serial Number	Zenworks.SystemInfo.SerialNumber	String	64	Model serial number value for the computer, assigned during manufacture.
SystemInfo.ManagementTechnology	Asset_Management Technology	Zenworks.SystemInfo.ManagementTechnology	Integer		The management technology available on the computer system.
CurrentLoginUser.Name	Current Login User.Name	ManageWise."User".Name	String	254	User logged into the primary eDirectory tree when the inventoried workstation was scanned.
LastLoginUser.Name	Last Login User.Name	ManageWise."User".Name	String	254	User most recently logged in to the primary eDirectory tree through Novell Client when the inventoried workstation was scanned.
Product.Name	Applications_Name	CIM.Product.Name	String	254	Name of the software application.
Product.Vendor	Applications_Vendor	CIM.Product.Vendor	String	254	Name of the software application manufacturer.
Product.Version	Applications_Version	CIM.Product.Version	String	64	Version of the software application.
Product.Location	Applications_Path	CIM.Directory.Location	String	254	The product installation path.
Product.IdentifyingNumber	Applications_Identifying Number	CIM.Product.IdentifyingNumber	String	64	Microsoft product ID

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
WinOperatingSystem.OSType	Windows_Name	ZENworks.WINOperatingSystem.OSType	Unsigned Small Integer (enum)		Operating system name. For example, Windows 2000. See Section P.3, "Enumeration Values for Software-Operating Systems-Windows - Name," on page 1238.
WinOperatingSystem.Version	Windows_Version	ZENworks.WINOperatingSystem.Version	String	254	Version of the operating system.
WinOperatingSystem.Caption	Windows_Caption	ZENworks.WINOperatingSystem.Caption	String	64	Short name of the operating system. For example, Windows 2000.
WinOperatingSystem.Role	Windows_Role	ZENworks.WINOperatingSystem.Role	Integer (enum)		The role of the computer system. For example, server or workstation.
WinOperatingSystem.OtherTypeDescription	Windows_OtherDescription	ZENworks.WINOperatingSystem.Description	String	254	More description about the operating system.
WinOperatingSystem.InstallDate	Windows_InstallDate	ZENworks.ZENOperatingSystem.InstallDate	String	25	Installation date of the operating system.
WinOperatingSystem.CodePage	Windows_CodePage	ZENworks.WINOperatingSystem.CodePage	String	254	Current language code page being used.
WinOperatingSystem.TotalVisibleMemorySize	Windows_TotalMemory (MB)	ZENworks.WINOperatingSystem.TotalVisibleMemorySize	Integer		Total memory as reported by the Windows operating system.
WinOperatingSystem.TotalVirtualMemorySize	Windows_TotalVirtualMemory (MB)	ZENworks.WINOperatingSystem.TotalVirtualMemorySize	Integer		Total virtual memory as reported by the Windows operating system.
InventoryScanner.Version	Scanner Information_Version	ZENworks.InventoryScanner.Version	String	64	Version of the Scanner running on the inventoried workstation.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
InventoryScanner.LastScanDate	Scanner Information_Last Scan Date	ZENworks.InventoryScanner.LastScanDate	Unsigned Integer		The date when the Scanner was last scanned. Stored as milliseconds time value so it can be read and displayed in any appropriate date format.
InventoryScanner.Inventory Server	Scanner Information_Inventory Server	ZENworks.InventoryScanner.InventoryServer	String	254	Name of the Inventory server to which the scans are sent. It is not the complete DN of the server name.
InventoryScanner.ScanMode	Scanner Information_Scan Mode	ZENworks.InventoryScanner.ScanMode	Integer (enum)		The management technology used by the Scanner, such as WMI or DMI, for scanning the computer system.
NetWareClient.Version	Netware Client_Version	ZENworks.NetWareClient.Version	String	64	Version of the NetWare® client software installed on the inventoried workstation.
NetworkAdapterDriver.Description	Network Adapter Driver_Description	ZENworks.NetworkAdapterDriver.Description	String	254	Description of the network adapter driver installed on the inventoried workstation. For example, IBM 10/100 Ethernet adapter, EN-2420Px Ethernet adapter.
NetworkAdapterDriver.Name	Network Adapter Driver_Name	ZENworks.NetworkAdapterDriver.Name	String	254	Name of the network adapter driver software installed that corresponds to the adapter. For example, ne2000.sys, pppmac.vxd, and others.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
NetworkAdapterDriver.Version	Network Adapter Driver_Version	ZENworks.NetworkAdapterDriver.Version	String	64	Network adapter driver version.
PointingDeviceDeviceDriver.Name	Pointing Device Driver_Name	ZENworks.PointingDeviceDeviceDriver.Name	String	254	Name of the mouse driver installed on the inventoried workstation.
PointingDeviceDeviceDriver.Version	Pointing Device Driver_Version	ZENworks.PointingDeviceDeviceDriver.Version	String	64	Mouse driver version.
PointingDevice.Name	Pointing Device_Name	CIM.PointingDevice.Name	String	254	<p>The name of the pointing device, such as Mouse. The string stored in this field is MOUSE.</p> <p>The CIM.PointingDevice.PointingType field determines the type of the pointing device.</p> <p>The different types of pointing devices are as listed in Section P.7, "Enumeration Values for Hardware-Pointing Device-Name," on page 1239.</p>
PointingDevice.NumberOfButtons	Pointing Device_Number of Buttons	CIM.PointingDevice.NumberOfButtons	Unsigned Tiny Integer		The number of buttons used by the pointing device.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
PointingDevice.IRQNumber	Pointing Device_IRQ Number	CIM.IRQ.IRQNumber	Unsigned Integer		The IRQ channel on the system to which the Mouse pointing device is attached. This information is stored in an IRQ class and not in the PointingDevice class in the database. For more information on how they are associated, see “Understanding the Inventory Database Schema” on page 987.
PointingDevice.PointingType	Pointing Device_Type	CIM.PointingDevice.PointingType	Integer (enum)		The pointing device type.
ZENKeyboard.NumberOfFunctionKeys	Keyboard_Number of Function Keys	ZENworks.ZENKeyboard.NumberOfFunctionKeys	Unsigned Small Integer		Number of function keys on keyboard.
ZENKeyboard.Layout	Keyboard_Layout	ZENworks.ZENKeyboard.layout	String	254	Layout information. For example, US English.
ZENKeyboard.SubType	Keyboard_Subtype	ZENworks.ZENKeyboard.SubType	Unsigned Integer		A number indicating the subtype of the keyboard.
ZENKeyboard.Delay	Keyboard_Delay (mSecs)	ZENworks.ZENKeyboard.Delay	Unsigned Integer		Delay before the repeat of a key.
ZENKeyboard.TypeomaticRate	Keyboard_Typeomatic Rate (mSecs)	ZENworks.ZENKeyboard.TypeomaticRate	Unsigned Integer		Rate of processing the keys.
ZENKeyboard.Description	Keyboard_Description	ZENworks.ZENKeyboard.Description	String	254	Keyboard description indicating the type of keyboard. For example, IBM enhanced (101/102 key) keyboard.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
VideoBIOSElement.Manufacturer	Display Driver_Manufacturer	CIM.VideoBIOSElement.Manufacturer	String	254	Manufacturer of the video BIOS driver installed on the system.
VideoBIOSElement.Version	Display Driver_Version	CIM.VideoBIOSElement.Version	String	254	Version of the Video BIOS driver.
VideoBIOSElement.Install Date	Display Driver_Install Date	CIM.VideoBIOSElement.InstallDate	String	25	Video BIOS release date.
VideoBIOSElement.Is Shadowed	Display Driver_Is Shadowed	CIM.VideoBIOSElement.ISShadowed	BIT (Used for Boolean conditions)		A Boolean condition indicating if the video BIOS supports shadow memory. 0 represents False and 1 is True.
VideoAdapter.NumberOfcolorpanes	Display Adapter_Number of Color Planes	ZENworks.VideoAdapter.NumberOfColorPlanes	Unsigned Integer		Number of color planes supported by the video system.
VideoAdapter.CurrentVerticalResolution	Display Adapter_Current Vertical Resolution	ZENworks.VideoAdapter.CurrentVerticalResolution	Unsigned Integer		Vertical resolution of the display.
VideoAdapter.CurrentHorizontalResolution	Display Adapter_Current Horizontal Resolution	ZENworks.VideoAdapter.CurrentHorizontalResolution	Unsigned Integer		Horizontal resolution of the display.
VideoAdapter.Description	Display Adapter_Description	ZENworks.VideoAdapter.Description	String	254	Video adapter description.
VideoAdapter.MinRefreshRate	Display Adapter_Minimum Refresh Rate	ZENworks.VideoAdapter.MinRefreshRate	Unsigned Integer		Minimum refresh rate of the monitor for redrawing the display, measured in Hertz.
VideoAdapter.MaxRefreshRate	Display Adapter_Maximum Refresh Rate	ZENworks.VideoAdapter.MaxRefreshRate	Unsigned Integer		Maximum refresh rate of the monitor for redrawing the display, measured in Hertz.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
VideoAdapter.VideoArchitecture	Display Adapter_Video Architecture	ZENworks.VideoAdapter.VideoArchitecture	Unsigned Integer (enum)		The architecture of the video subsystem in this system. For example, CGA/VGA/SVGA/8514A. See Section P.5, "Enumeration Values for Hardware-Display Adapter-Video Architecture," on page 1239.
VideoAdapter.VideoMemoryType	Display Adapter_Video Memory Type	ZENworks.VideoAdapter.VideoMemoryType	Unsigned Small Integer (Enum)		The type of memory for this adapter. For example, VRAM/ SRAM/DRAM/ EDO RAM. See Enumeration Values for Hardware-Display Adapter-Video Memory Type.
VideoAdapter.MaximumMemorySupported	Display Adapter_Maximum Memory Supported(KB)	ZENworks.VideoAdapter.MaximumMemorySupported	Unsigned Integer		Maximum memory that the display adapter supports for VIDEO RAM.
VideoAdapter.CurrentBitsPerPixel	Display Adapter_Current Bits/Pixel	ZENworks.VideoAdapter.CurrentBitsPerPixel	Unsigned Integer		Number of adjacent color bits for each pixel.
VideoAdapter.ChipSet	Display Adapter_Chip Set	ZENworks.VideoAdapter.ChipSet	String	254	The chip set used in the video adapter.
VideoAdapter.DACType	Display Adapter_DAC Type	ZENworks.VideoAdapter.DAC Type	String	254	The digital to analog converter type used in the video adapter.
VideoAdapter.ProviderName	Display Adapter_Provider	ZENworks.VideoAdapter.Provider	String	254	The manufacturer or the provider name.
ZENPOTSModem.Caption	Modem_Caption	ZENworks.ZENPOTSModem.Caption	String	64	The short name of the modem.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
ZENPOTSModem.Description	Modem_Description	ZENworks.ZENPOTSModem.Description	String	254	The complete description of the modem. For example, Standard 2400 bps modem, IBM PCMCIA HPC modem.
ZENPOTSModem.Name	Modem_Name	ZENworks.ZENPOTSModem.Name	String	254	The name of the modem dictating its type and usage. For example, Standard Windows Modem means that this is used in standard Windows architecture.
ZENPOTSModem.ProviderName	Modem_Provider	ZENworks.ZENPOTSModem.Provider	String	254	The manufacturer or the provider name.
ZENPOTSModem.DeviceID	Modem_Device ID	ZENworks.ZENPOTSModem.DeviceID	String	64	The unique ID assigned to the device.
BIOS.BIOSIDBytes	BIOS_BIOS Identification Bytes	ZENworks.BIOS.BIOSIDBytes	String	254	Byte in the BIOS that indicates the computer model.
BIOS.SerialNumber	BIOS_Serial Number	ZENworks.BIOS.SerialNumber	String	64	Serial number of BIOS assigned by the manufacturer.
BIOS.PrimaryBIOS	BIOS_Primary Bios	ZENworks.BIOS.PrimaryBIOS	BIT (Used for Boolean conditions here)		True when set to 1, indicating that this BIOS is the primary BIOS. Used in systems with additional BIOS chips.
BIOS.InstallDate	BIOS_Install Date	ZENworks.BIOS.InstallDate	String	25	The release date of the BIOS given by the manufacturer.
BIOS.Version	BIOS_Version	ZENworks.BIOS.Version	String	254	Version or revision level of the BIOS.
BIOS.Manufacturer	BIOS_Manufacturer	ZENworks.BIOS.Manufacturer	String	254	The manufacturer name of BIOS.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
BIOS.Caption	BIOS_Caption	ZENworks. BIOS.Caption	String	64	The name of the BIOS as given by the BIOS manufacturer.
BIOS."size"	BIOS_Size(KB)	ZENworks. BIOS.size	Unsigned Integer		Size of the BIOS in bytes.
Processor.CurrentClockSpeed	Processor_Current Clock Speed(MHz)	CIM. Processor. CurrentClockSpeed	Unsigned Integer		Current clock speed of the processor in MHz.
Processor.Maxclockspeed	Processor_Maximum Clock Speed(MHz)	CIM. Processor. MaxClockSpeed	Unsigned Integer		Maximum clock speed of the processor in MHz.
Processor.Role	Processor_Role	CIM. Processor. Role	String	254	Type of processor such as central processor, math coprocessor, and others
Processor.Family	Processor_Processor Family	CIM. Processor. Family	Unsigned Small Integer (enum)		Family the processor belongs to. See Section P.9, "Enumeration Values for Hardware-Processor-Processor Family," on page 1240.
Processor.Otherfamily description	Processor_Other Family Description	CIM. Processor. OtherFamily Description	String	64	Additional description about the processor family, such as the Pentium processor with MMX technology when the processor cannot be designated using Family.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
Processor.UpgradeMethod	Processor_Upgrade Method	CIM.Processor.Upgrade Method	Unsigned Small Integer (Enum)		The method by which this processor can be upgraded, if upgrades are supported. See Section P.10, "Enumeration Values for Hardware-Processor-Upgrade Method," on page 1240.
Processor.Stepping	Processor_Processor Stepping	CIM.Processor.Stepping	String	254	Single-byte code characteristic provided by microprocessor vendors to identify the processor stepping model.
Processor.Device ID	Processor_DeviceID	CIM.Processor.DeviceID	String	64	Special hexadecimal string identifying the processor type.
CacheMemory.Speed	Cache Memory_Speed(nsec)	CIM.PhysicalMemory.Speed	Unsigned Integer		Speed of this System Cache module in nanoseconds. This is stored in CIM.PhysicalMemory class and is associated to CIM.CacheMemory. For more information on how they are associated, see "Understanding the Inventory Database Schema" on page 987.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
CacheMemory.Capacity	Cache Memory_Capacity(MB)	CIM.PhysicalMemory.Capacity	Unsigned Integer		Capacity of this System Cache module in nanoseconds. This is stored in CIM.PhysicalMemory class and is associated to CIM.CacheMemory. For more information on how they are associated, see "Understanding the Inventory Database Schema" on page 987 .
CacheMemory.Level	Cache Memory_Level	CIM.CacheMemory."Level"	Unsigned Small Integer (enum)		Indicates the cache level: internal cache that is built in to the microprocessors, or external cache that is between the CPU and DRAM.
CacheMemory.WritePolicy	Cache Memory_Write Policy	CIM.CacheMemory.WritePolicy	Unsigned Small Integer (enum)		Indicates the two different ways (Write-Back and Write-Through Cache) that the cache can handle to write to the memory.
CacheMemory.ErrorMethodology	Cache Memory_Error Methodology	CIM.CacheMemory.Error Methodology	String	254	Error correction scheme supported by this cache component, for example, Parity/Single Bit ECC/MultiBit ECC.
CacheMemory.CacheType	Cache Memory_Cache Type	CIM.CacheType	Unsigned Small Integer (enum)		Defines the system cache type. For example, Instruction, Data, Unified.
CacheMemory.LineSize	Cache Memory_Line Size (Bytes)	CIM.CacheMemory.LineSize	Unsigned Integer		Size in bytes of a single cache bucket or line.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
CacheMemory.ReplacementPolicy	Cache Memory_Replacement Policy	CIM.Cache Memory.ReplacementPolicy	Unsigned Integer (enum)		Algorithm that the cache uses to determine which cache lines or buckets should be reused.
CacheMemory.ReadPolicy	Cache Memory_Read Policy	CIM.Cache Memory.ReadPolicy	Unsigned Small Integer (enum)		Indicates whether the data cache is for read operation.
CacheMemory.Associativity	Cache Memory_Associativity	CIM.Cache Memory.Associativity	Unsigned Integer (enum)		Defines the system cache associativity (direct-mapped, 2-way, 4-way).
Diskette Drive.Manufacturer	Diskette Drive_Manufacturer	ZENworks.Physical Diskette.Manufacturer	String	254	Vendor name.
Diskette Drive.Description	Diskette Drive_Description	ZENworks.Physical Diskette.Description	String	254	Floppy diskette description.
Diskette Drive.PhysicalCylinders	Diskette Drive_Physical Cylinders	ZENworks.Physical Diskette.Physical Cylinders	Unsigned Integer		Total number of cylinders or tracks on the floppy.
Diskette Drive.PhysicalHeads	Diskette Drive_Physical Heads	ZENworks.Physical Diskette.Physical Heads	Unsigned Small Integer		Number of heads.
Diskette Drive.Capacity	Diskette Drive_Capacity (MB)	ZENworks.Physical Diskette.Capacity	Unsigned Integer		Total size.
Diskette Drive.SectorsPerTrack	Diskette Drive_Sectors/Track	ZENworks.Physical Diskette.SectorsPerTrack	Unsigned Integer		Number of sectors per track.
Diskette Drive.DeviceID	Diskette Drive_DeviceID	CIM.Diskette Drive	String	64	The drive name representing the floppy drive.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
ZENDiskDrive.Manufacturer	Physical Disk Drive_Manufacturer	ZENworks.PhysicalDisk.Manufacturer	String	254	Vendor name.
ZENDiskDrive.Description	Physical Disk Drive_Description	ZENworks.PhysicalDisk.Description	String	254	Hard disk vendor description.
ZENDiskDrive.PhysicalCylinders	Physical Disk Drive_Physical Cylinders	ZENworks.PhysicalDisk.Physical Cylinders	Unsigned Integer		Total number of cylinders.
ZENDiskDrive.PhysicalHeads	Physical Disk Drive_Physical Heads	ZENworks.PhysicalDisk.Physical Heads	Unsigned Small Integer		Number of heads.
ZENDiskDrive.SectorsPerTrack	Physical Disk Drive_Sectors/Track	ZENworks.PhysicalDisk.SectorsPerTrack	Unsigned Integer		Number of sectors per track.
ZENDiskDrive.Capacity	Physical Disk Drive_Capacity(MB)	ZENworks.PhysicalDisk.Capacity	Unsigned Integer		Total size of the hard disk.
ZENDiskDrive.Removable	Physical Disk Drive_Removable	ZENworks.LogicalDiskDrive.Removable	BIT		0 indicates that it is a fixed disk and 1 indicates that it is a removable disk.
LocalFileSystem.DeviceID	Logical Disk Drive_Device ID	ZENworks.LogicalDiskDrive.DeviceID	String	64	The drive letter, such as C: or A:.
LocalFileSystem.FileSystemSize	Logical Disk Drive_Size(MB)	CIM.LocalFileSystem.FileSystemSize	Integer		The total size of the file system or the logical disk.
LocalFileSystem.AvailableSpace	Logical Disk Drive_Free Size(MB)	CIM.LocalFileSystem.AvailableSpace	Integer		The available size of the file system or the logical disk.
LocalFileSystem.VolumeSerial Number	Logical Disk Drive_Volume Serial Number	CIM.LocalFileSystem.VolumeSerialNumber	String	254	The volume serial number of the specified drive.
LocalFileSystem.Caption	Logical Disk Drive_Caption	CIM.LocalFileSystem.Caption	String	64	The volume label of the specified drive.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
LocalFileSystem.FileSystemType	Logical Disk Drive_ File System Type	CIM.LocalFileSyst em.FileSystemType	String	254	The file system on the drive, such as FAT or NTFS.
CDROMDrive.Manufacturer	CDROM_Manufacturer	ZENworks. Physical CDROM. Manufacturer	String	254	The manufacturer of the CD-ROM drive.
CDROMDrive.Caption	CDROM_Caption	ZENworks. Physical CDROM. Caption	String	64	CD-ROM label.
CDROMDrive.Description	CDROM_ Description	ZENworks. Physical CDROM. Description	String	254	Description of the CD drive, as given by the manufacturer. For example, ATAPI CDROM, CREATIVE CD1620E SL970520.
CDROMDrive.DeviceID	CDROM_ Device ID	ZENworks. Logical CDROM. DeviceID	String	64	Drive letter allocated for the CD on the inventoried workstation.
SerialPort.Name	Serial Port_Name	ZENworks. SerialPort. Name	String	254	The name of the serial port. For example, COM1, COM2, and others.
SerialPort.Address	Serial Port_ Address	ZENworks. SerialPort. Address	Unsigned Integer		The address mapped in memory for the serial port.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
SerialPort.IRQNumber	Serial Port_IRQ Number	CIM.IRQ.IRQNumber	Unsigned Integer		<p>The IRQ channel on the system to which the serial port is attached. In the database, this information is stored in an IRQ class and not in a Serial Port class.</p> <p>For more information on how they are associated, see Chapter 75, "Understanding the Inventory Database Schema," on page 987.</p>
ParallelPort.Name	Parallel Port_Name	ZENworks.ParallelPort.Name	String	254	The name of the parallel port. For example, LPT1 and others.
ParallelPort.Address	Parallel Port_Address	ZENworks.ParallelPort.Address	Unsigned Integer		The name of the parallel port. For example, LPT1 and others.
ParallelPort.DMASupport	Parallel Port_DMA Support	ZENworks.ParallelPort.DMASupport	BIT (used for Boolean conditions here)		If True or 1, then it means that DMA is the channel that is allocated for bulk data transfer for use with devices connected to the parallel ports.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
ParallelPort.IRQNumber	Parallel Port_IRQ Number	CIM.IRQ.IRQNumber	Unsigned Integer		<p>The IRQ channel on the system to which the parallel port is attached. This information is stored in an IRQ class and not in a parallel port class in the database.</p> <p>For more information on how they are associated, see Chapter 75, "Understanding the Inventory Database Schema," on page 987.</p>
Bus.Version	Bus_Version	ZENworks.Bus.Bus Version	String	254	Version of the bus supported by the inventoried workstation.
Bus.Description	Bus_Description	ZENworks.Bus.Description	String	254	Description of the bus.
Bus.BusType	Bus_Bus Type	ZENworks.Bus.BusType	Integer (enum)		The bus type of the system.
Bus.Name	Bus_Name	ZENworks.Bus.Name	String	254	Name of the internal system bus.
Bus.DeviceID	Bus_Device ID	ZENworks.Bus.DeviceID	String	64	The unique ID for the specific bus.
ZENNetworkAdapter.Name	Network Adapter_Name	CIM.ZENworks.ZENNetworkAdapter.Name	String	254	Network adapters installed on the system.
ZENNetworkAdapter.MaxSpeed	Network Adapter_Max_Speed (Mbps)	CIM.ZENworks.ZENNetworkAdapter.MaxSpeed	Unsigned Integer		Rate at which the adapter can transfer data.
ZENNetworkAdapter.PermanentAddress	Network Adapter_Permanent Address	CIM.ZENworks.ZENNetworkAdapter.PermanentAddresses	String	64	Machine address stored permanently in the adapter (MAC address).
ZENNetworkAdapter.MACAddress	Network Adapter_Address	CIM.ZENworks.ZENNetworkAdapter.MACAddress	String	64	The MAC address stored in the network adapter.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
ZENNetworkAdapter.ProviderName	Network Adapter_Provider	CIM.ZENworks.ZENAdapter.Provider	String	254	The manufacturer or the provider.
ZENNetworkAdapter.AdapterType	Network Adapter_Adapter Type	CIM.ZENworks.ZENAdapter.AdapterType	String	254	Type of the adapter, such as Ethernet or FDDI adapter.
SoundAdapter.Description	Multimedia Card_Description	ZENworks.SoundAdapter.Description	String	254	Description of the multimedia component for the inventoried workstation.
SoundAdapter.Name	Multimedia Card_Name	ZENworks.SoundAdapter.Name	String	254	Name of the sound card installed on the system.
SoundAdapter.Manufacturer	Multimedia Card_Manufacturer	ZENworks.SoundAdapter.Manufacturer	String	254	Vendor name.
SoundAdapter.ProviderName	Multimedia Card_Provider	ZENworks.SoundAdapter.Provider	String	254	The provider or the manufacturer of the multimedia card.
Battery.Name	Battery_Name	CIM.Battery.Name	String	254	Name of the battery installed on the system.
Battery.Chemistry	Battery_Chemistry	CIM.Battery.Chemistry	Unsigned Small Integer		Indicates the battery's chemistry, such as lead acid, nickel cadmium and others. See Section P.8, "Enumeration Values for Hardware-Battery-Chemistry," on page 1239.
Battery.DesignCapacity	Battery_Design Capacity(mWatt-hours)	CIM.Battery.Design Capacity	Unsigned Integer		The design capacity of the battery in mWatt-hours.
Battery.DesignVoltage	Battery_Design Voltage(MilliVolts)	CIM.Battery.DesignVoltage	Unsigned Integer		The design voltage of the battery in mVolts.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
Battery.SmartBatteryVersion	Battery_Smart Battery Version	CIM.Battery.SmartBatteryVersion	String	64	The Smart Battery Data Specification version number supported by this battery.
Battery.Manufacturer	Battery_Manufacturer	CIM.PhysicalComponent.Manufacturer	String	254	Vendor name of the battery.
Battery.InstallDate	Battery_Install Date	CIM.PhysicalComponent.InstallDate	String	25	Date of manufacturing the battery.
Battery.SerialNumber	Battery_Serial Number	CIM.PhysicalComponent.SerialNumber	String	64	Battery serial number.
PowerSupply.Description	Power Supply_Description	CIM.PowerSupply.Description	String	254	Name and description of the power supply on the system.
PowerSupply.TotalOutputPower	Power Supply_Total Output Power (MilliWatts)	CIM.PowerSupply.TotalOutputPower	Unsigned Integer		Total output power of the power supply.
IPProtocolEndPoint.Address	IP Address_Address	CIM.IPProtocolEndpoint.Address	String	254	IP address of the inventoried workstation.
IPProtocolEndPoint.Subnet Mask	IP Address_Subnet Mask	CIM.IPProtocolEndpoint.SubnetMask	String	254	The subnet mask of the inventoried workstation.
DNSName.LABEL	DNS_LABEL	ManageWise.DNS Name.Label	String	254	DNS name of the inventoried workstation.
IPXProtocolEndPoint.Address	IPX Address_Address	CIM.IPXProtocolEndpoint.Address	String	254	IPX address of the inventoried workstation.
LANEndPoint.MACAddress	MAC Address_Address	CIM.LANEndpoint.MACAddress	String	12	MAC address of the inventoried workstation.
MotherBoard.Version	MotherBoard_Version	ZENworks.Motherboard.Version	String	64	Motherboard version.
MotherBoard.Description	MotherBoard_Description	ZENworks.Motherboard.Description	String	254	The description of the motherboard.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
MotherBoard.Manufacturer	MotherBoard_Manufacturer	ZENworks.Motherboard.Manufacturer	String	254	The manufacturer of the motherboard.
MotherBoard.NumberOfSlots	MotherBoard_NumberOfSlots	ZENworks.Motherboard.Numberofslots	Integer		The number of expansion slots on the motherboard.
IRQ.Number	IRQ_IRQ Number	CIM.IRQ.IRQNumber	Unsigned Integer		The system interrupt number.
IRQ.Availability	IRQ_Availability	CIM.IRQ.Availability	Unsigned Small Integer (Enum)		Indicates whether the IRQ channel is used or available. Enumeration values are as follows: 1 = "Other" 2 = "Unknown" 3 = "Available" 4 = "In Use/Not Available" 5 = "In Use and Available/Shareable"
IRQ.TriggerType	IRQ_IRQ Trigger Type	CIM.IRQ.TriggerType	Unsigned Small Integer		IRQ trigger type indicating whether edge (value=4) or level triggered (value=3) interrupts occur. Enumeration values are as follows: 1 = "Other" 2 = "Unknown" 3 = "Level" 4 = "Edge"
IRQ.Shareable	IRQ_IRQ Shareable	CIM.IRQ.Shareable	Unsigned Small Integer		Boolean indicating whether the IRQ can be shared.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
SLOT.MaxDataWidth	Slot_Maximum Data Width	CIM.Slot.MaxData Width	Unsigned Small Integer		Maximum bus width of adapter cards that can be inserted into this slot in bits. If the value is Unknown, enter 0. If the value is other than 8, 16, 32, 64 or 128, enter 1. It is expressed in bits.
SLOT.ThermalRating	Slot_Thermal Rating (MilliWatts)	CIM.Slot.Thermal Rating	Unsigned Integer		Maximum thermal dissipation of the slot in milliwatts.
SLOT.Description	Slot_Description	CIM.SlotDescription	String	254	The description of the adapter mounted on the slot.
DMA.DMAChannel	DMA_DMA Channel Number	CIM.DMA.DMAChannel	Unsigned Integer		The DMA channel number.
DMA.Description	DMA_Description	CIM.DMA.Description	String	254	The name of the device using the DMA channel.
DMA.Availability	DMA_Availability	CIM.DMA.Availability	Unsigned Small Integer		Indicates whether the DMA channel is available. Enumeration values are as follows: 1 = "Other" 2 = "Unknown" 3 = "Available" 4 = "In Use/Not Available" 5 = "In Use and Available/Shareable"
DMA.BurstMode	DMA_DMA Burst Mode	CIM.DMA.BurstMode	BIT (used for Boolean condition here)		Indication that the DMA channel supports the burst mode.
NetWareOperatingSystem.Version	NetWare.Version	ZENworks.NetWareOperating.Version	String	254	Version of the NetWare operating system.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
Memory.TotalMemory	Memory_TotalMemory(MB)	ZENOperatingSystem.TotalVisibleMemorySize	Integer		Total memory of the Windows operating system.
MSDomainName.Label	WindowsDomain_Name	ManageWise.MSDomainName	String	254	The Windows domain to which the workstation is attached.
Monitor.DeviceID	Monitor_DeviceID	ZENworks.ZENDesktopMonitor.DeviceID	Integer		Unique ID of a desktop monitor that is attached to a computer system.
Monitor.Description	Monitor_Description	ZENworks.ZENDesktopMonitor.Description	varchar	254	Description of the monitor.
Monitor.ModelID	Monitor_ModelID	ZENworks.ZENDesktopMonitor.ModelID	varchar		Unique ID of a model of the monitor. It is a combination of the Manufacturer ID and Product ID.
Monitor.ManufactureDate	Monitor_ManufactureDate	ZENworks.ZENDesktopMonitor.ManufacturerDate	char	25	Year in which the monitor was manufactured.
Monitor.ViewableSize	Monitor_ViewableSize	ZENworks.ZENDesktopMonitor.ViewableSize	integer		A number representing the diagonal width of the screen image excluding the black borders around the image's edge.
Monitor.NominalSize	Monitor_NominalSize	ZENworks.ZENDesktopMonitor.NominalSize	integer		A number representing the diagonal width of the monitor (the distance from one corner of the screen to the opposite corner of the screen).
Monitor.Serial Number	Monitor_Serial Number	ZENworks.ZENDesktopMonitor.Serial Number	varchar	128	Manufacturer's number used to identify a monitor.
Monitor.Manufacturer	Monitor_Manufacturer	ZENworks.ZENDesktopMonitor.Manufacturer	varchar	254	Name of the monitor's manufacturer.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
Monitor.Model	Monitor_Model	ZENworks.ZENDesktopMonitor.Model	varchar	254	Product name of the monitor given by the manufacturer.
Chassis.AssetTag	Chassis_AssetTag	ZENworks_ZENC_hassis	varchar	254	Asset tag number of the system chassis.
Chassis.ChassisType	Chassis_ChassisType	ZENworks_ZENC_hassis	unsigned small int		Represents whether the system chassis is a laptop, desktop, notebook, docking station and so on.
Chassis.NumberOfPowerCords	Chassis_NumberOfPowerCords	ZENworks_ZENC_hassis	varchar	128	Total number of power cords attached to a system chassis.
Chassis.Manufacturer	Chassis_Manufacturer	ZENworks_ZENC_hassis	varchar	254	Name of the system chassis manufacturer.
Chassis.SerialNumber	Chassis_SerialNumber	ZENworks_ZENC_hassis	varchar	128	Manufacturer's number used to identify a system chassis.
Chassis.Version	Chassis_Version	ZENworks_ZENC_hassis	varchar	64	Version number of the system chassis.
Chassis.Tag	Chassis_Tag	ZENworks_ZENC_hassis	varchar	64	Unique ID of the system chassis attached to a particular computer system.
Software.ProductIdentifier	Software_productIdentifier	MW_DBA.InstalledSoftware.productIdentifier	varchar	254	A unique, 16-character identifier for an installed product. This identifier is available from MSI on Windows.
Software.InternalVersion	Software_InternalVersion	MW_DBA.InstalledSoftware.InternalVersion	varchar	64	Internal version of a product

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
Software.Language	Software_Language	MW_DBA.InstalledSoftware.Language	smallint		User-friendly name for the language of this copy of the product.
Software.UninstallString	Software_UninstallString	MW_DBA.InstalledSoftware.UninstallString	varchar	254	The command to invoke for uninstalling this product instance. Currently, this is available in Add/Remove Programs (ARP) and MSI on Windows.
Software.InstallationSource	Software_InstallationSource	MW_DBA.InstalledSoftware.InstallationSource	varchar	254	Identifies the file system path where the installation files were stored when installing this product instance. Currently, this is available in ARP and MSI on Windows.
Software.FriendlyName	Software_FriendlyName	MW_DBA.InstalledSoftware.FriendlyName	varchar	254	Display name of the software.
Software.LastExecutionTime	Software_LastExecutionTime	MW_DBA.InstalledSoftware.LastExecutionTime	bigint		Date and time stamp when the product was last executed.
Software.FrequencyOfUsage	Software_FrequencyOfUsage	MW_DBA.InstalledSoftware.FrequencyOfUsage	smallint		Number of times the product is used.
Software.Description	Software_Description	MW_DBA.InstalledSoftware.Description	varchar	254	Description of the product.
Software.DefinitionDate	Software_DefinitionDate	MW_DBA.InstalledVirusScanner.DefinitionDate	bigint		The date of the virus definition file installed on the computer. Some anti-virus products combine date and version into a single string.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
Software.DefinitionVersion	Software_DefinitionVersion	MW_DBA.InstalledVirusScanner.DefinitionVersion	varchar	64	The vendor-defined version of the virus definition file that has been installed on a computer
Software.Edition	Software_Edition	MW_DBA.ProductEdition.Name	varchar	128	Product edition defined by the vendor. For example, Professional.
Software.SupportPack	Software_SupportPack	MW_DBA.SupportPack.Name	varchar	128	Support pack name.
Software.Path	Software_Path	MW_DBA.Directory.Path	varchar	254	Directory path where the product is installed on the computer system.
Software.Name	Software_Name	MW_DBA.Software.Name	varchar	254	Vendor-defined name of the product represented as a vendor trademark or registered trademark.
Software.Vendor	Software_Vendor	MW_DBA.Software.Vendor	varchar	254	Name of the software manufacturer
Software.Version	Software_Version	MW_DBA.Software.Version	varchar	64	User-friendly version of a product.
Software.Category	Software_Category	MW_DBA.Software.Category	varchar	64	Product category to which the product belongs.
Software.HelpLink	Software_HelpLink	MW_DBA.Software.HelpLink	varchar	254	Support web site URL for the product that is available in ARP and MSI.
Software.PackageGUID	Software_PackageGUID	MW_DBA.Software.PackageGUID	varchar	64	Vendor-defined GUID for a product that is available in MSI.
Software.PatchName	Software_PatchName	MW_DBA.Patch.Name	varchar	254	Vendor-defined name for the patch.

Export Wizard Attribute Name	Export Attribute Name (Column Heading in the .csv file)	Database Schema Attribute Name	Data Type	Length	Description of the Attribute
File.Name	File_Name	MW_DBA.File.Name	varchar	254	Name of the file representing the software.
File.FileVersion	File_FileVersion	MW_DBA.File.FileVersion	varchar	64	Version of the file representing the software.
File.InternalName	File_InternalName	MW_DBA.File.InternalName	varchar	254	Internal name.
File.ProductVersion	File_ProductVersion	MW_DBA.File.ProductVersion	varchar	64	The version of the product represented by this file.
File.Size	File_size	MW_DBA.File.size	bigint		Size of the file representing the software.
File.LastModified	File_LastModified	MW_DBA.File.LastModified	bigint		Last modified date of the file representing the software.
File.Company	File_Company	MW_DBA.File.Company	varchar	254	Vendor name.
File.ProductName	File_ProductName	MW_DBA.File.ProductName	varchar	254	The product which this file represents.
File.Language	File_Language	MW_DBA.File.Language	smallint		User-friendly name for the language of this copy of the file
File.SoftwareDictionaryID	File_SoftwareDictionaryID	MW_DBA.File.SoftwareDictionaryID	varchar	64	ID of the file as represented in the General software dictionary.
DiskUsage.TotalDiskUsage	DiskUsage.TotalDiskUsage	MW_DBA.DiskUsage.TotalDiskUsage	bigint		Total disk usage for all the files of the specified extension.
DiskUsage.Name	DiskUsage.Name	MW_DBA.DiskUsage.Name	varchar	32	The file extension for which the disk usage is scanned for.

Enumeration Values

P

This section provides information on the following topics:

- Section P.1, “Enumeration Values for General-System Information-Management Technology,” on page 1237
- Section P.2, “Enumeration Values for General-Inventory Information-Scan Mode,” on page 1238
- Section P.3, “Enumeration Values for Software-Operating Systems-Windows - Name,” on page 1238
- Section P.4, “Enumeration Values for Installation Repository,” on page 1238
- Section P.5, “Enumeration Values for Hardware-Display Adapter-Video Architecture,” on page 1239
- Section P.6, “Enumeration Values for Hardware-Display Adapter-Video Memory Type,” on page 1239
- Section P.7, “Enumeration Values for Hardware-Pointing Device-Name,” on page 1239
- Section P.8, “Enumeration Values for Hardware-Battery-Chemistry,” on page 1239
- Section P.9, “Enumeration Values for Hardware-Processor-Processor Family,” on page 1240
- Section P.10, “Enumeration Values for Hardware-Processor-Upgrade Method,” on page 1240
- Section P.11, “Enumeration Values for Hardware-Chassis-Chassis Type,” on page 1240
- Section P.12, “Enumeration Values for Hardware-Bus-Protocol Supported,” on page 1241
- Section P.13, “Enumeration Values for Hardware-Processor-Role,” on page 1241
- Section P.14, “Enumeration Values for System-System Cache-Level,” on page 1241
- Section P.15, “Enumeration Values for System-System Cache-Cache Type,” on page 1241
- Section P.16, “Enumeration Values for System-System Cache-Replacement Policy,” on page 1241
- Section P.17, “Enumeration Values for System-System Cache-Read Policy,” on page 1242
- Section P.18, “Enumeration Values for System-System Cache-Write Policy,” on page 1242
- Section P.19, “Enumeration Values for System-System Cache-Associativity,” on page 1242
- Section P.20, “Enumeration Values for System-System IRQ-Availability,” on page 1242
- Section P.21, “Enumeration Values for System-System IRQ-IRQ Trigger Type,” on page 1242
- Section P.22, “Enumeration Values for System-System DMA-Availability,” on page 1243
- Section P.23, “Enumeration Values for Language,” on page 1243

P.1 Enumeration Values for General-System Information-Management Technology

1 = Unknown

3= DMI Enabled

5= SNMP Enabled

2 = Other	4 = WMI Enabled	6 = DMI and WMI Enabled
-----------	-----------------	-------------------------

P.2 Enumeration Values for General-Inventory Information-Scan Mode

1 = Unknown	3= DMI	5= SNMP
2 = Other	4 = WMI	6 = DMI and WMI

P.3 Enumeration Values for Software-Operating Systems-Windows - Name

0 = Unknown	18 = WINNT	59 = Dedicated
1 = Other	21 = NetWare	63 = Windows (R) Me
16 = WIN95	36 = Linux	67 = Windows XP
17 = WIN98	58 = Windows	

P.4 Enumeration Values for Installation Repository

The following Installation Repository enum values are displayed in the Software > Software Group Components > Software Group and Software > Software Components > Software classes.

0 = Others	7 = MSI, Add Remove Programs, Software Dictionary	20 = Software Dictionary, Probe
1 = MSI	8 = NetWare Products.dat	21= MSI, Software Dictionary, Probes
2 = Add/Remove Programs	12 = Software Dictionary, NetWare Products.dat	22 = Add Remove programs, Software Dictionary, Probe
3 = MSI, Add Remove Programs	16 = Probe	23 = MSI, Add Remove programs, Software Dictionary, Probe
4 = Software Dictionary	17 = MSI, Probe	24 = NetWare Products.dat, Probe
5 = MSI, Software Dictionary	18 = Add Remove Programs, Probe	28 = Software Dictionary, NetWare Products.dat, Probe
6 = Add Remove Programs, Software Dictionary	19 = MSI, Add Remove Programs, Probe	

P.5 Enumeration Values for Hardware-Display Adapter-Video Architecture

1 = Other	6 = SVGA	11 = XGA
2 = Unknown	7 = MDA	12 = Linear Frame Buffer
3 = CGA	8 = HGC	160 = PC-98
4 = EGA	9 = MCGA	
5 = VGA	10 = 8514A	

P.6 Enumeration Values for Hardware-Display Adapter-Video Memory Type

1 = Other	6 = WRAM	11 = 3DRAM
2 = Unknown	7 = EDO RAM	12 = SDRAM
3 = VRAM	8 = Burst Synchronous DRAM	13 = SGRAM
4 = DRAM	9 = Pipelined Burst SRAM	
5 = SRAM	10 = CDRAM	

P.7 Enumeration Values for Hardware-Pointing Device-Name

1 = Other	4 = Track Ball	7 = Touch Pad
2 = Unknown	5 = Track Point	8 = Touch Screen
3 = Mouse	6 = Glide Point	9 = Mouse - Optical Sensor

P.8 Enumeration Values for Hardware-Battery-Chemistry

1 = Other	5 = Nickel Metal Hydride
2 = Unknown	6 = Lithium-ion
3 = Lead Acid	7 = Zinc air
4 = Nickel Cadmium	8 = Lithium Polymer

P.9 Enumeration Values for Hardware-Processor-Processor Family

1 = Other	24 = AMD Duron(TM) Processor Family	130 = Itanium(TM) Processor
2 = Unknown	25 = K5 Family	176 = Pentium(R) III Xeon(TM)
11 = Pentium(R) Brand	26 = K6 Family	177= Pentium(R) III Processor with Intel(R) SpeedStep(TM) Technology
12 = Pentium(R) Pro	27 = K6 -2	178 = Pentium(R) 4 Processor
13 = Pentium(R) II	28 = K6 -3	181 = Inter(R) Xeon (TM) Processor MP
14 = Pentium(R) Processor with MMX(TM) Technology	29 = AMD Athlon (TM) Processor Family	182 = AMD Athlon XP (TM) Processor Family
15 = Celeron(TM)	30 = AMD29000 Family	183 = AMD Athlon MP(TM) Processor Family
16 = Pentium(R) II Xeon(TM)	31 = K6-2+	300 = 6 x 86
17 = Pentium(R) II		

P.10 Enumeration Values for Hardware-Processor-Upgrade Method

1= Other	5 = Replacement/Piggy Back	9 = Slot 2
2 = Unknown	6 = None	10 = 370 Pin Socket
3 = Daughter Board	7 = LIF Socket	11 = Slot A
4 = ZIF Socket	8 = Slot 1	12 = Slot M

P.11 Enumeration Values for Hardware-Chassis-Chassis Type

1 = Other	10 = Notebook	19 = SubChassis
2 = Unknown	11 = Hand Held	20 = Bus Expansion Chassis
3 = Desktop	12 = Docking Station	21 = Peripheral Chassis
4 = Low Profile Desktop	13 = All in One	22 = Storage Chassis
5 = Pizza Box	14 = Sub Notebook	23 = Rack Mount Chassis
6 = Mini Tower	15 = Space-Saving	24 = Sealed-Case PC
7= Tower	16 = Lunch Box	25 = Multi-system Chassis

8 = Portable	17 = Main System Chassis
9 = LapTop	18 = Expansion Chassis

P.12 Enumeration Values for Hardware-Bus-Protocol Supported

0 = Internal	6 = VME Bus	12 = Internal Processor
1 = ISA	7 = NuBus	13 = Internal Power Bus
2 = EISA	8 = PCMCIA Bus	14 = PNP ISA Bus
3 = MicroChannel	9 = C Bus	15 = PNP Bus
4= TurboChannel	10 = MPI Bus	16= Maximum Interface Type
5 = PCI Bus	11 = MPSA Bus	

P.13 Enumeration Values for Hardware-Processor-Role

1 = Other	3= Central Processor	5= DSP Processor
2 = Unknown	4 = Math Processor	6 = Video Processor

P.14 Enumeration Values for System-System Cache-Level

1 = Other	3 = Write Back	5 = Varies with Address
2 = Unknown	4 = Write Through	6 = Determination Per I/O

P.15 Enumeration Values for System-System Cache-Cache Type

1 = Other	3 = Instruction	5 = Unified
2 = Unknown	4 = Data	

P.16 Enumeration Values for System-System Cache-Replacement Policy

1 = Other	4 = First In First Out (FIFO)	7 = Most Frequently Used (MFU)
-----------	-------------------------------	--------------------------------

2 = Unknown	5 = Last In First Out (LIFO)	8 = Data Dependent Multiple Algorithms
3 = Least Recently Used (LRU)	6 = Least Frequently Used (LFU)	

P.17 Enumeration Values for System-System Cache-Read Policy

1 = Other	3 = Read	5 = Read and Read-ahead
2 = Unknown	4 = Read-ahead	6 = Determination Per I/O

P.18 Enumeration Values for System-System Cache-Write Policy

1 = Other	3 = Write Back	5 = Varies with Address
2 = Unknown	4 = Write Through	6 = Determination Per I/O

P.19 Enumeration Values for System-System Cache-Associativity

1 = Other	4 = 2-way Set-Associative	7 = 8-way Set-Associative
2 = Unknown	5 = 4-way Set-Associative	8 = 16-way Set-Associative
3 = Direct Mapped	6 = Fully Associative	

P.20 Enumeration Values for System-System IRQ-Availability

1 = Other	3 = Available	5 = In Use and Available/Shareable
2 = Unknown	4 = In Use/Not Available	

P.21 Enumeration Values for System-System IRQ-IRQ Trigger Type

1 = Other	3 = Level
2 = Unknown	4 = Edge

P.22 Enumeration Values for System-System DMA-Availability

1 = Other	3 = Available	5 = In Use and Available/ Shareable
2 = Unknown	4 = In Use/Not Available	

P.23 Enumeration Values for Language

The following Language enum values are displayed in the following classes: Software Group, Software Group File Information, Software, File Information, and Exclude Information.

0=Neutral	97=Not supported	1095=Windows XP: Gujarati. This is Unicode only.
1=Arabic	101=Divehi	1037=Hebrew
2=Bulgarian	127=Invariant Locale	1081=Windows 2000/XP: Hindi. This is Unicode only.
3=Catalan	1024=Process or User Default Language	1038=Hungarian
4=Chinese	2048=System Default Language	1039=Icelandic
5=Czech	1078=Afrikaans	1057=Indonesian
6=Danish	1052=Albanian	1040=Italian (Standard)
7=German	1025=Arabic (Saudi Arabia)	2064=Italian (Switzerland)
8=Greek	2049=Arabic (Iraq)	1041=Japanese
9=English	3073=Arabic (Egypt)	1099=Windows XP: Kannada. This is Unicode only.
10=Spanish	4097=Arabic (Libya)	1111=Windows 2000/XP: Konkani. This is Unicode only.
11=Finnish	5121=Arabic (Algeria)	1042=Korean
12=French	6145=Arabic (Morocco)	2066=Windows 95
13=Hebrew	7169=Arabic (Tunisia)	1088=Windows XP: Kyrgyz.
14=Hungarian	8193=Arabic (Oman)	1062=Latvian
15=Icelandic	9217=Arabic (Yemen)	1063=Lithuanian
16=Italian	10241=Arabic (Syria)	2087=Windows 98 only: Lithuanian (Classic)
17=Japanese	11265=Arabic (Jordan)	1071=FYRO Macedonian
18=Korean	12289=Arabic (Lebanon)	1086=Malay (Malaysian)
19=Dutch	13313=Arabic (Kuwait)	2110=Malay (Brunei Darussalam)

20=Norwegian	14337=Arabic (U.A.E.)	1102=Windows 2000/XP: Marathi. This is Unicode only.
21=Polish	15361=Arabic (Bahrain)	1104=Windows XP: Mongolian
22=Portuguese	16385=Arabic (Qatar)	1044=Norwegian (Bokmal)
24=Romanian	1067=Windows 2000/XP: Armenian. This is Unicode only.	2068=Norwegian (Nynorsk)
25=Russian	1068=Azeri (Latin)	1045=Polish
26=Croatian	2092=Azeri (Cyrillic)	1046=Portuguese (Brazil)
27=Slovak	1069=Basque	2070=Portuguese (Portugal)
28=Albanian	1059=Belarusian	1094=Windows XP: Punjabi. This is Unicode only.
29=Swedish	1026=Bulgarian	1048=Romanian
30=Thai	1109=Burmese	1049=Russian
31=Turkish	1027=Catalan	1103=Windows 2000/XP: Sanskrit. This is Unicode only.
32=Urdu	1028=Chinese (Taiwan)	3098=Serbian (Cyrillic)
33=Indonesian	2052=Chinese (PRC)	2074=Serbian (Latin)
34=Ukrainian	3076=Chinese (Hong Kong SAR, PRC)	1051=Slovak
35=Belarusian	4100=Chinese (Singapore)	1060=Slovenian
36=Slovenian	5124=Windows 98/Me, Windows 2000/XP: Chinese (Macau SAR)	1034=Spanish (Spain, Traditional Sort)
37=Estonian	1050=Croatian	2058=Spanish (Mexican)
38=Latvian	1029=Czech	3082=Spanish (Spain, Modern Sort)
39=Lithuanian	1030=Danish	4106=Spanish (Guatemala)
41=Farsi	1125=Windows XP: Divehi. This is Unicode only.	5130=Spanish (Costa Rica)
42=Vietnamese	1043=Dutch (Netherlands)	6154=Spanish (Panama)
43=Armenian	2067=Dutch (Belgium)	7178=Spanish (Dominican Republic)
44=Azeri	1033=English (United States)	8202=Spanish (Venezuela)
45=Basque	2057=English (United Kingdom)	9226=Spanish (Colombia)
47=FYRO Macedonian	3081=English (Australian)	10250=Spanish (Peru)
54=Afrikaans	4105=English (Canadian)	11274=Spanish (Argentina)
55=Georgian	5129=English (New Zealand)	12298=Spanish (Ecuador)
56=Faeroese	6153=English (Ireland)	13322=Spanish (Chile)

57=Hindi	7177=English (South Africa)	14346=Spanish (Uruguay)
62=Malay	8201=English (Jamaica)	15370=Spanish (Paraguay)
63=Kazak	9225=English (Caribbean)	16394=Spanish (Bolivia)
64=Kyrgyz	10249=English (Belize)	17418=Spanish (El Salvador)
65=Swahili	11273=English (Trinidad)	18442=Spanish (Honduras)
67=Uzbek	12297=Windows 98/Me, Windows 2000/XP: English (Zimbabwe)	19466=Spanish (Nicaragua)
68=Tatar	13321=Windows 98/Me, Windows 2000/XP: English (Philippines)	20490=Spanish (Puerto Rico)
69=Not supported	1061=Estonian	1072=Sutu
70=Punjabi	1080=Faeroese	1089=Swahili (Kenya)
71=Gujarati	1065=Farsi	1053=Swedish
72=Not supported	1035=Finnish	2077=Swedish (Finland)
73=Tamil	1036=French (Standard)	1114=Windows XP: Syriac. This is Unicode only.
74=Telugu	2060=French (Belgian)	1097=Windows 2000/XP: Tamil. This is Unicode only.
75=Kannada	3084=French (Canadian)	1092=Tatar (Tatarstan)
76=Not supported	4108=French (Switzerland)	1098=Windows XP: Telugu. This is Unicode only.
77=Not supported	5132=French (Luxembourg)	1054=Thai
78=Marathi	6156=Windows 98/Me, Windows 2000/XP: French (Monaco)	1055=Turkish
79=Sanskrit	1110=Windows XP: Galician	1058=Ukrainian
80=Mongolian	1079=Windows 2000/XP: Georgian. This is Unicode only.	1056=Windows 98/Me, Windows 2000/XP: Urdu (Pakistan)
86=Galician	1031=German (Standard)	2080=Urdu (India)
87=Konkani	2055=German (Switzerland)	1091=Uzbek (Latin)
88=Not supported	3079=German (Austria)	2115=Uzbek (Cyrillic)
89=Not supported	4103=German (Luxembourg)	1066=Windows 98/Me, Windows NT 4.0 and later: Vietnamese
90=Syriac	5127=German (Liechtenstein)	
96=Not supported	1032=Greek	

Documentation Updates

Q

This section contains information on documentation content changes that have been made in the *Administration* guide for Workstation Inventory since the initial release of Novell® ZENworks® 7 Desktop Management. The information will help you to keep current on updates to the documentation.

All changes that are noted in this section were also made in the documentation. The documentation is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the documentation changes listed in this section.

The documentation update information is grouped according to the date the changes were published. Within a dated section, the changes are alphabetically listed by the names of the main table of contents sections for Workstation Inventory.

If you need to know whether a copy of the PDF documentation you are using is the most recent, the PDF document contains the date it was published on the front title page.

The documentation was updated on the following date:

- [Section Q.1, “July 14, 2006 \(Support Pack 1\),” on page 1247](#)
- [Section Q.2, “December 23, 2005,” on page 1249](#)
- [Section Q.3, “December 9, 2005,” on page 1250](#)
- [Section Q.4, “September 30, 2005,” on page 1251](#)

Q.1 July 14, 2006 (Support Pack 1)

For Support Pack 1, each section in the guide was modified with the following note:

NOTE: The information in this section also applies to ZENworks 7 Desktop Management with Support Pack 1.

Other updates were made to the following sections. The changes are explained below.

Q.1.1 Appendix L: Performance Tips

The following updates were made in this section:

Location	Change
Section M.1.1, “Sybase in the NetWare, Windows, or Linux Environment,” on page 1185	Added a paragraph to reference the new section in the appendix.
Section M.3, “Performance Tips for the Inventory Server (Support Pack 1),” on page 1194	Added this section for Support Pack 1.

Q.1.2 Managing Your Inventory System

The following updates were made in this section:

Location	Change
Section 76.7, "Removing Redundant Inventoried Workstations from the Inventory Database," on page 1084	Added new paragraph to Step 2 on page 1085 . Added new paragraph to Step 3 on page 1085 . Added new paragraph to Step 4 on page 1085 .
Section 76.7.1, "Understanding the NDS Lookup for DB Utility," on page 1086	Added new paragraph to Step 1 on page 1086 . Added new paragraph to Step 3 on page 1086 .

Q.1.3 Setting Up Workstation Inventory

The following updates were made in this section:

Location	Change
"Creating the Oracle10g Inventory Database on a Windows Server" on page 939	Changed the content of this section.
Section 73.2.3, "Setting Up the MS SQL Server 2000 or MS SQL Server 2005 Inventory Database," on page 945	Added "MS SQL Server 20005" to the title of the section.
"Configuring the MS SQL Server 2005 Inventory Database" on page 948	Added this section for Support Pack 1.
"Manually Creating the Inventory Database Object for MS SQL 2000 or MS SQL 2005" on page 951	Added "MS SQL 2005" to the section title and changed the content accordingly.
"Connecting the Inventory Server and ConsoleOne to the MS SQL 2000 or MS SQL 2005 Inventory Database" on page 953	Added "MS SQL 2005" to the section title and changed the content accordingly.

Q.1.4 Viewing Inventory Information

The following updates were made in this section:

Location	Change
"Generating Inventory Reports" on page 1122	Deleted an example from the first bullet in Step 3 on page 1122 .

Q.2 December 23, 2005

Updates were made to the following sections. The changes are explained below.

- [Section Q.2.1, “Appendix L: Performance Tips,” on page 1249](#)
- [Section Q.2.2, “Deploying Workstation Inventory,” on page 1249](#)
- [Section Q.2.3, “Managing Your Inventory System,” on page 1249](#)
- [Section Q.2.4, “Viewing Inventory Information,” on page 1249](#)

Q.2.1 Appendix L: Performance Tips

The following updates were made in this section:

Change	Location
“Oracle in the NetWare, Windows, or Linux Environment” on page 1188.	Added the reference to Linux in the entire section.
“Sybase in the NetWare, Windows, or Linux Environment” on page 1185.	Added the reference to Linux in the entire section.

Q.2.2 Deploying Workstation Inventory

The following updates were made in this section:

Location	Change
“Configuring the MS SQL Server 2000 Inventory Database” on page 945	Added the following information to Step 11e on page 947 : “During the execution of the drop trigger sqls, the following error message might be displayed on the console, “Cannot drop the trigger ‘ <i>trigger_name</i> ’, because it does not exist in the system catalog”. Ignore the error message.”

Q.2.3 Managing Your Inventory System

The following updates were made in this section:

Change	Location
“Removing Duplicate Workstation Objects from the Inventory Database” on page 1086.	Added the reference to Linux in the entire section.

Q.2.4 Viewing Inventory Information

The following updates were made in this section:

Change	Location
“Generating Inventory Reports” on page 1122.	Added the following information as a note in Step 4 on page 1123 : “ZENworks Inventory report supports only the following double-byte character languages: German, English, Spanish, French, Portugese, and Japanese. Other double-byte characters might not be displayed properly in the Inventory reports.”

Q.3 December 9, 2005

The page design of the entire guide was reformatted to comply with revised Novell documentation standards.

Other upates were made to the following sections. The changes are explained below.

- [Section Q.3.1, “Setting Up Workstation Inventory,” on page 1250](#)
- [Section Q.3.2, “Understanding Workstation Inventory Components,” on page 1250](#)
- [Section Q.3.3, “Viewing Inventory Information,” on page 1250](#)

Q.3.1 Setting Up Workstation Inventory

The following updates were made in this section:

Location	Change
Section 73.3, “Configuring the Inventory Service Object,” on page 955.	Newly added Step 3 on page 956 .

Q.3.2 Understanding Workstation Inventory Components

The following updates were made in this section:

Change	Location
Section 74.3.3, “Scanning for the Hardware Inventory Information,” on page 970.	Following products have been added to the list of antivirus products scanned by. the Inventory scanner: Symantec AntiVirus Corporate Edition 9.0 Symantec AntiVirus Corporate Edition 10.0

Q.3.3 Viewing Inventory Information

The following updates were made in this section:

Change	Location
“Generating Inventory Reports” on page 1122 > Step 3 on page 1122.	Updated the guidelines to be followed as you work with the Reporting dialog.

Q.4 September 30, 2005

Updates were made to the following sections. The changes are explained below.

- [Section Q.4.1, “Setting Up Workstation Inventory,” on page 1251](#)

Q.4.1 Setting Up Workstation Inventory

The following updates were made in this section:

Location	Change
“Backing Up the Sybase Inventory Database” on page 933	This section has been reorganized. There is no change in the content of the section.

