

Policy Management Reference

Novell® ZENworks® Configuration Management

10.1

February 18, 2009

www.novell.com



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. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://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 © 2007 - 2009 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 on the [Novell Legal Patents Web page \(http://www.novell.com/company/legal/patents/\)](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 latest online documentation for this and other Novell products, see the [Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](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	7
1 Overview	9
1.1 What Is a Policy?	9
1.2 What Is a Policy Group?	9
1.3 Understanding the Policy Types	10
1.4 Understanding the Features of a Policy	10
2 Creating Policies	13
2.1 Browser Bookmarks Policy	13
2.2 Dynamic Local User Policy	14
2.3 Local File Rights Policy	17
2.4 Printer Policy	19
2.5 Remote Management Policy	23
2.6 Roaming Profile Policy	23
2.7 SNMP Policy	24
2.8 Windows Group Policy	26
2.9 ZENworks Explorer Configuration Policy	27
2.10 Creating Policies by Using the zman Command Line Utility	29
2.10.1 Creating a Policy without Content	30
2.10.2 Creating a Policy with Content	32
2.10.3 Understanding the zman Policy XML File Format	33
3 Managing Policies	37
3.1 Policy Groups	37
3.2 Editing Policies	38
3.3 Deleting Policies	39
3.4 Adding Policies to Existing Groups	39
3.5 Assigning a Policy to Devices	40
3.6 Assigning a Policy to Users	41
3.7 Assigning the Local File Rights Policy to Devices Running Different Languages	42
3.8 Adding System Requirements for a Policy	42
3.8.1 Filter Conditions	43
3.8.2 Filter Logic	46
3.9 Disabling Policies	47
3.10 Enabling the Disabled Policies	47
3.11 Copying a Policy to a Content Server	47
3.12 Incrementing the Policy Version	49
3.13 Reviewing the Status of the Policies at the Managed Device	50
3.14 Predefined Policy Reports	50
4 Managing Policy Groups	51
4.1 Creating Policy Groups	51
4.2 Renaming or Moving Policy Groups	52

4.3	Copying a Policy Group's System Requirements	52
4.4	Deleting a Policy Group	53
4.5	Assigning a Policy Group to Devices	53
4.6	Assigning a Policy Group to Users	53
4.7	Adding a Policy to a Group	54
5	Managing Folders	55
5.1	Creating Folders	55
5.2	Renaming or Moving Folders	55
5.3	Copying a Folder's System Requirements	56
5.4	Deleting a Folder	56
A	Troubleshooting Policy Management	57
A.1	Browser Bookmarks Policy Error Messages	57
A.2	Dynamic Local User Policy Error Messages	58
A.3	General Policy Troubleshooting Scenarios	59
A.4	Local File Rights Policy Error Messages	60
A.5	Printer Policy Error Messages	61
A.6	Printer Policy Troubleshooting Strategies	64
A.7	Roaming Profile Policy Errors	65
A.8	SNMP Policy Errors	65
A.9	Windows Group Policy Errors	66
A.10	ZENworks Explorer Configuration Policy Errors	69
A.11	Dynamic Local User Policy Troubleshooting Strategies	71
A.12	Windows Group Policy Troubleshooting Strategies	72
B	Best Practices	77
B.1	Local File Rights Policy	77
B.2	Dynamic Local User Policy	77
B.3	Roaming Profile Policy	77
B.4	SNMP Policy	77
B.5	Windows Group Policy	77
C	Documentation Updates	79
C.1	February 18, 2009: 10.1.3	79
	C.1.1 Creating Policies	79
	C.1.2 Best Practices	79
	C.1.3 Troubleshooting Policy Management	79
C.2	October 3, 2008: 10.1.1	80
	C.2.1 Adding System Requirements for a Policy	80
C.3	August 6, 2008: SP1 (10.1)	80
	C.3.1 Managing Policies	80
	C.3.2 Troubleshooting Policy Management	80
	C.3.3 Best Practices	81

About This Guide

This *Novell ZENworks 10 Configuration Management Policy Management Reference* includes information about Policy Management features and procedures to help you configure and maintain your Novell® ZENworks® 10 Configuration Management with SP1 (10.1) system. The information in this guide is organized as follows:

- ♦ Chapter 1, “Overview,” on page 9
- ♦ Chapter 2, “Creating Policies,” on page 13
- ♦ Chapter 3, “Managing Policies,” on page 37
- ♦ Chapter 4, “Managing Policy Groups,” on page 51
- ♦ Chapter 5, “Managing Folders,” on page 55
- ♦ Appendix A, “Troubleshooting Policy Management,” on page 57
- ♦ Appendix B, “Best Practices,” on page 77
- ♦ Appendix C, “Documentation Updates,” on page 79

Audience

This guide is intended for Novell ZENworks administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to the [Novell Documentation Feedback site \(http://www.novell.com/documentation/feedback.html\)](http://www.novell.com/documentation/feedback.html) and enter your comments there.

Additional Documentation

ZENworks Configuration Management is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the [ZENworks 10 Configuration Management with SP1 \(10.1\) documentation \(http://www.novell.com/documentation/zcm10/index.html\)](http://www.novell.com/documentation/zcm10/index.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*, should use forward slashes as required by your software.

Novell® ZENworks® 10 Configuration Management provides policies to configure operating system settings and select application settings. By applying a policy to multiple devices, you can ensure that all of the devices have the same configuration.

The following sections contain additional information:

- ♦ [Section 1.1, “What Is a Policy?,” on page 9](#)
- ♦ [Section 1.2, “What Is a Policy Group?,” on page 9](#)
- ♦ [Section 1.3, “Understanding the Policy Types,” on page 10](#)
- ♦ [Section 1.4, “Understanding the Features of a Policy,” on page 10](#)

1.1 What Is a Policy?

A policy is a rule that controls a range of hardware and software configuration settings on the managed devices. For example, an administrator can create policies to control browser bookmarks available in the browser, printers to access, and security and system configuration settings on the managed devices.

You can use the policies to create a set of configurations that can be assigned to any number of managed devices. It helps you to provide the devices with a uniform configuration, and it eliminates the need to configure each device separately.

You can assign a policy directly to a device or a user. You can also assign the policy to a folder or group where the user or device is a member. Assigning a policy to device groups rather than device folders is the preferred way, because a device can be a member of multiple device groups, but it can be a member of only one device folder.

On managed devices, each policy type is enforced by a Policy Handler or Enforcer, which makes all the configuration changes necessary to enforce or unenforce the settings in a given policy.

1.2 What Is a Policy Group?

A policy group is a collection of one or more policies. Creating policy groups eases the administration efforts in managing policies. You can create policy groups and assign them to managed devices the same way you would assign individual policies.

Because the policy inherits the group’s assignments, managing a policy group is easier than managing individual policy. For example, if multiple policies are included in a policy group and the policy group is assigned to a device or a device group, then all the policies included in the policy group are automatically assigned to the device or device group at the same time. You need not individually assign each policy to a device or a device group.

1.3 Understanding the Policy Types

ZENworks Configuration Management 10 lets you create the following policy types:

- ♦ **Browser Bookmarks Policy:** Lets you configure Internet Explorer* favorites for Windows* devices and users.
- ♦ **Dynamic Local User Policy:** Lets you create new users and manage existing users created on Windows 2000, Windows XP, and Windows Vista* workstations; and Windows 2000 and Windows 2003 Terminal Server sessions after the users have successfully authenticated to the user source.
- ♦ **Local File Rights Policy:** Lets you configure rights for files or folders that exist on the NTFS file systems.

The policy can be used to configure basic and advanced permissions for both local and domain users and groups. It provides the ability for an administrator to create custom groups on managed devices.

- ♦ **Printer Policy:** Lets you configure Local, SMB, HTTP, and iPrint printers on a Windows machine.
- ♦ **Remote Management Policy:** Lets you configure the behavior or execution of Remote Management sessions on the managed device. The policy includes properties such as Remote Management operations and security.
- ♦ **Roaming Profile Policy:** Lets you to create a user profile that is stored in a network path.

A user profile contains information about a user's desktop settings and personal preferences, which are retained from session to session.

Any user profile that is stored in a network path is known as a roaming profile. Every time the user logs on to a machine, his profile is loaded from the network path. This helps the user to move from machine to machine and still retain consistent personal settings.
- ♦ **SNMP Policy:** Lets you configure SNMP services on the managed devices.
- ♦ **Windows Group Policy:** Lets you configure a group policy for Windows devices.
- ♦ **ZENworks Explorer Configuration Policy:** Lets you to administer and centrally manage the behavior and features of the ZENworks Explorer.

1.4 Understanding the Features of a Policy

- ♦ A policy is applied to a device or a user only if the policy is directly or indirectly associated to that device or user.

The Browser Bookmarks policy, Dynamic Local User policy, Printer policy, Remote Management policy, Windows Group policy, and ZENworks Explorer Configuration policy can be applied to a device or a user:

The Local File Rights and SNMP policies can be applied only to a device.

The: Roaming Profile policy can be applied only to a user.

- ♦ A policy can be associated to groups and containers.

In ZENworks Control Center, devices and users can be organized by using containers and groups. A device or user can be a member of multiple groups. The containers can be nested within other containers. If a policy is associated to a group of users, it applies to all users in that group. If a policy is associated to a user container, it applies to all users in the entire subtree rooted at that container. The same behavior applies to device groups and containers.

- ♦ A policy can be associated to query groups.

In ZENworks Control Center, the devices can also be members of query groups. Query groups are similar to ordinary groups except that the membership is determined by a query defined by the administrator. All devices that satisfy the query become members of that device group. The query is evaluated periodically and the membership is updated with the results. An administrator can configure the periodicity of the evaluation. An administrator can also force an immediate refresh of a query group. Query groups act just like other groups where policies are concerned.

- ♦ Policies are chronologically ordered by default.

When multiple policies are associated to a device, user, group, or container, the associations are chronologically ordered by default. The administrator can change the ordering.

If a device or user belongs to multiple groups, the groups are ordered. Consequently, the policies associated to those groups are also ordered. The administrator can change the ordering of groups for a device or user at any time.

In addition, the policies in a policy group are ordered.

- ♦ Policies have a precedence configured to determine the policy that is effective for a device or a user.

Many policies of the same type can be applied to a user or a device through direct association and inheritance. For example, if a Browser Bookmark policy is associated to a user and another Browser Bookmark policy is associated to a container containing that user, the policy directly associated to that user overrides the policy associated to the container.

- ♦ Policies support management by exception.

You can define a global policy for your enterprise and associate it to the top-level container containing all your user objects. You can then override configuration items in the global policy by defining a new policy and associating it to specific users or user groups. These users receive their configuration from the new policy. All other users receive their configuration from the global policy.

- ♦ Policies support system requirements.

You can specify the system requirements of a device or user in a policy. The policy is applied to a device or user only if the device or user meets the system requirements.

For example, the SNMP policy is applied by default on all devices having the SNMP service installed.

- ♦ ZENworks Configuration Management supports singular and plural policies.

Singular Policy: If multiple policies of the same policy type are assigned to a device or a user and the policy type is a Singular policy, then only the nearest associated policy meeting the system requirements is applied. If the policy type is associated to both user and device, then two different policies can be assigned to user and device.

The SNMP policy, Dynamic Local User policy, Remote Management policy, Roaming Profile policy, and ZENworks Explorer Configuration policy are singular policies.

Plural Policy: If multiple policies of the same policy type are assigned to a device or a user and the policy type is a Plural type, then all policies meeting the associated system requirement are applied.

The Browser Bookmarks policy, Local File Rights policy, Windows Group policy, and Printer policy are plural policies.

- ♦ Policies can be disabled.

When you create a policy in ZENworks Configuration Management, the policy is enabled by default. You can disable it if you do not want to apply it on a user or a device.

- ♦ ZENworks Configuration Management allows you to resolve policy conflicts.

The set of effective policies is a subset of the set of assigned policies. The set of effective policies for a device or user is calculated by applying precedence rules, multiplicity rules, and system requirements filters on the set of assigned policies. Effective policies are calculated separately for devices and users. The Policy Conflict Resolution setting determines how user and device policies interact for a specific user and device combination.

Effective policies are calculated separately for devices and users. When a user logs in to a device, policies associated to both the user and the device must be applied. Policy Conflict Resolution settings are used only when policies of the same type are associated to both the device and the user. This setting determines the precedence order among the policies associated to the user and those associated to the device. The Policy Conflict Resolution settings are applied after the effective policies are calculated.

Policy Conflict Resolution settings are defined when associating a policy to a device. The settings cannot be defined for associations to users. For each policy type, the Policy Conflict Resolution setting defined in the closest effective policy of that type is applied for all policies of that type.

A Policy Resolution Conflict setting can have one of the following values:

- ♦ **User Last:** Applies the policies associated to the device first, then the policies associated to the user. This is the default value.
- ♦ **Device Last:** Applies the policies associated to the user first, then the policies associated to the device.
- ♦ **User Only:** Applies only the policies associated to the user and ignores the policies associated to the device.
- ♦ **Device Only:** Applies only the policies associated to the device and ignore the policies associated to the user.

NOTE: The Policy Conflict Resolution setting is taken from the device-associated policy with the highest precedence.

Creating Policies

2

Novell® ZENworks® 10 Configuration Management lets you create policies by using ZENworks Control Center or by using the zman command line utility.

The following sections contain step-by-step instructions about creating policies by using ZENworks Control Center:

- ♦ [Section 2.1, “Browser Bookmarks Policy,” on page 13](#)
- ♦ [Section 2.2, “Dynamic Local User Policy,” on page 14](#)
- ♦ [Section 2.3, “Local File Rights Policy,” on page 17](#)
- ♦ [Section 2.4, “Printer Policy,” on page 19](#)
- ♦ [Section 2.5, “Remote Management Policy,” on page 23](#)
- ♦ [Section 2.6, “Roaming Profile Policy,” on page 23](#)
- ♦ [Section 2.7, “SNMP Policy,” on page 24](#)
- ♦ [Section 2.8, “Windows Group Policy,” on page 26](#)
- ♦ [Section 2.9, “ZENworks Explorer Configuration Policy,” on page 27](#)

The following section explains how to create policies by using the zman command line utility:

- ♦ [Section 2.10, “Creating Policies by Using the zman Command Line Utility,” on page 29](#)

2.1 Browser Bookmarks Policy

The Browser Bookmarks policy lets you configure Internet Explorer favorites for Windows devices and users.

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 In the *Policies* list, click *New*, then click *Policy* to display the Select Policy Type page.
- 3 Select *Browser Bookmarks Policy*, click *Next* to display the Define Details page, then fill in the fields:
 - Policy Name:** Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in ZENworks Control Center.
 - Folder:** Type the name or browse to and select the ZENworks Control Center folder where you want the policy to reside. The default is /policies, but you can create additional folders to organize your policies.
 - Description:** Provide a short description of the policy’s content. This description displays in ZENworks Control Center.
- 4 Click *Next* to display the Bookmarks Tree Data Source page.
- 5 Create a browser bookmarks tree by exporting the bookmarks to a file in UTF-8 format or by manually entering the data source.

The following list contains browser-specific information to create the exported file:

- ♦ **Internet Explorer 6.x:** In the browser window, click *File > Import and Export*. Follow the instructions given in the Import/Export Wizard to create the `bookmark.htm` file.
- ♦ **Internet Explorer 7:** In the browser window, click *Add to Favorites > Import and Export*. Follow the instructions given in the Import/Export Wizard to create the `bookmark.htm` file.
- ♦ **Mozilla Firefox:** In the browser window, click *Bookmarks > Organize Bookmarks*, then click *File > Export* to create the `bookmarks.html` file.

NOTE: Use a text editor to manually convert the bookmark file into UTF-8 format.

- 6** Click *Next* to display the Bookmarks Tree Configuration page, then use the options to configure the bookmarks tree.

The following table lists the tasks you can perform with the *New*, *Edit*, and *Delete* options.

Field	Details
<i>New</i>	<ul style="list-style-type: none">♦ Click <i>New > Folder</i> to display the Add Folder to Bookmarks dialog box, through which you can add a new folder to the bookmarks tree.♦ Click <i>New > Bookmark</i> to display the Add Bookmark to Bookmarks dialog box, through which you can add a new bookmark to the bookmarks tree by specifying the bookmark name and a URL. Click the button next to the URL field to verify that the URL entered by you is correct and functional.
<i>Edit</i>	<ul style="list-style-type: none">♦ Select the bookmark name you want to change, click <i>Edit > Rename</i>, then specify a new name.♦ Click <i>Edit > Sort</i> to organize the bookmarks in ascending or descending order.♦ Click <i>Edit > Move Up</i>, <i>Move Down</i>, or <i>Move To</i> to relocate a bookmark.♦ Click <i>Edit > Select All Children</i> to select all the subdirectories and bookmarks of the selected parent directory.♦ Click <i>Edit > Deselect All Children</i> to deselect all the subdirectories and bookmarks of the selected parent directory.♦ Click <i>Edit > Clear Selection</i> to clear the selections.
<i>Delete</i>	<ul style="list-style-type: none">♦ Click <i>Delete</i> to delete a bookmark from the bookmarks tree.

- 7** Click *Next* to display the Summary page.
- 8** Click *Finish* to create the policy now, or select *Define Additional Properties* to specify additional information, such as policy assignment, **system requirements**, enforcement, status, and which group the policy is a member of.

2.2 Dynamic Local User Policy

The Dynamic Local User policy lets you create new users and manage existing users on Windows 2000, Windows XP, and Windows Vista workstations; and Windows 2000 and Windows 2003 Terminal Server sessions after they have successfully authenticated to user source.

NOTE: Ensure that the latest version of the Novell client is installed on the managed device before the Dynamic Local User policy is enforced. To obtain the latest version of Novell Client™, see the [Novell Download Web site \(http://download.novell.com/index.jsp\)](http://download.novell.com/index.jsp).

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 In the *Policies* list, click *New*, then click *Policy* to display the Select Policy Type page.
- 3 Select *Dynamic Local User Policy*, click *Next* to display the Define Details page, then fill in the fields:

Policy Name: Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in ZENworks Control Center.

Folder: Type the name or browse to the ZENworks Control Center folder where you want the policy to reside. The default is */policies*, but you can create additional folders to organize your policies.

Description: Provide a short description of the policy's content. This description displays in ZENworks Control Center.

- 4 Click *Next* to display the User Configurations page, then use the options on the page to configure the user account.

The following table contains information about configuring dynamic local user accounts and managing them on managed devices:

Field	Details
<i>Use User Source Credentials</i>	Enables logging in through the user's authoritative source credentials instead of Windows 2000, Windows XP, or Windows Vista credentials.
<i>Volatile User (Remove User After Logout)</i>	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.
<i>Use the Credentials Specified Below (Always volatile)</i>	Allows you to specify the following user credentials for a volatile user: <ul style="list-style-type: none">♦ User Name: Specify the user's name.♦ Full Name: Specify the user's complete name.♦ Description: Provide any additional information that helps the administrator to further identify this user account.
<i>Manage Existing User Account (if any)</i>	Helps you to manage a user object that already exists. If you select both the <i>Volatile User (Remove User After Logout)</i> and <i>Manage Existing User Account (If Any)</i> check boxes, and the user has a permanent local account that uses the same credentials specified in the user source, the permanent account is changed to a volatile (temporary) account and is removed when the user logs out.
Enable Volatile User Cache	Enables the caching of the volatile user account on the device for a specified period of time.
Cache Volatile User for Time Period (Days)	Allows you to specify the number of days to cache the volatile user account on the device. The default value is 5. You can specify a value from 1 to 999 days.

Field	Details
<i>Not a Member Of</i>	Displays the available group to which a user can be assigned as a member.
<i>Member Of</i>	Displays groups a user is member of.

- 5 Click *Next* to display the Login Restrictions page, then use the options on the page to configure user access.

The following table contains information about providing and managing dynamic local user access:

Field	Details
<i>Included / Excluded Workstations</i>	Lists the workstations and containers that you want to include or exclude DLU access to.
<i>Included / Excluded Users</i>	Lists the users and containers that you want to include or exclude DLU access to.

- 6 Click *Next* to display the File Rights page.

The following table contains information about managing Dynamic Local User file system access on Windows 2000, Windows XP, and Windows Vista workstations, and Windows 2000 and Windows 2003 Terminal Server sessions:

Field	Details
<i>Add</i>	<p>Allows you to select and assign appropriate file rights.</p> <p>To add a file/folder:</p> <ol style="list-style-type: none"> 1. Click <i>Add</i>, then specify a file or folder. 2. Select the file rights you want to assign to the specified file or folder. 3. If you want to restrict the inheritance of the rights to only the immediate child file or folder, select <i>Restrict inheritance to immediate child files/folders only</i>. 4. Click <i>OK</i>.
<i>Edit</i>	<p><i>Copy</i>: Allows you to copy and add a file rights setting to the list.</p> <ol style="list-style-type: none"> 1. Select a file or folder, then click <i>Edit</i>. 2. Click <i>Copy</i>. 3. Specify a new name. 4. Click <i>OK</i>. <p><i>Rename</i>: Allows you to edit only the filename.</p> <ol style="list-style-type: none"> 1. Select a file or folder, then click <i>Edit</i>. 2. Click <i>Rename</i>. 3. Specify a new filename. 4. Click <i>OK</i>.

Field	Details
<i>Move Up</i> or <i>Move Down</i>	Allows you to reorder the files or folders. <ol style="list-style-type: none"> 1. Select the check box next to the file or folder you want to move. 2. Click <i>Move Up</i> and <i>Move Down</i> to relocate it.
<i>Remove</i>	Allows you to delete a file or a folder. <ol style="list-style-type: none"> 1. Select the check box next to the file or folder. 2. Click <i>Remove</i>.

- 7 Click *Next* to display the Summary page.
- 8 Click *Finish* to create the policy now, or select *Define Additional Properties* to specify additional information, such as policy assignment, **system requirements**, enforcement, status, and which group the policy is a member of.

2.3 Local File Rights Policy

The Local File Rights policy allows you to configure rights for files or folders that exist on the NTFS file systems.

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 In the *Policies* list, click *New*, then click *Policy* to display the Select Policy Type page.
- 3 Select *Local File Rights Policy*, click *Next* to display the Define Details page, then fill in the fields:

Policy Name: Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in ZENworks Control Center.

Folder: Type the name or browse to and select the ZENworks Control Center folder where you want the policy to reside. The default is `/policies`, but you can create additional folders to organize your policies.

Description: Provide a short description of the policy's content. This description displays in ZENworks Control Center.

- 4 Click *Next* to display the Configure Basic Properties page, then use the options on the page to configure the attributes.

The following table contains information about configuring a file or folder and the attributes associated with it:

Field	Details
<i>File / Folder Path</i>	Allows you to specify the complete path of a file or folder on the managed device. You can use the ZENworks system variables or environment variables to specify the path. <p>To configure system variables in ZENworks Control Center, click the <i>Configuration</i> tab > the <i>Content</i> setting in the Management Zone Settings panel > <i>System Variables</i>. Click the <i>Help</i> button for details about configuring system variables.</p>

Field	Details
<i>Attributes</i>	Allows you to specify the attributes of a file or folder, such as <i>Read only</i> and <i>Hidden</i> .

This page allows you to configure permissions for only one file or folder. If you want to assign permissions to multiple files or folders, then configure them in the Details page after creating the policy.

- 5 Click *Next* to display the Configure Permissions page, then use the options on the page to configure permissions for selected users or groups.

The following table contains information about configuring permissions:

Field	Details
<i>Permission for Users or Groups</i>	<p>Allows you to configure permissions for users or groups.</p> <ol style="list-style-type: none"> 1. Click <i>Add</i>, then Click <i>User</i> or <i>Group</i> to select a user or a group from the appropriate drop-down list. 2. Select the type of permission you want to configure as <i>Simple NTFS Permissions</i> or <i>All NTFS Permissions</i>. Depending on the type of permission you select, a list of permissions are displayed. Configure the permissions as applicable to the selected user or group. 3. By default, when a permission is set on a folder, all the subfolders and the files also inherit the permissions. If you want to restrict the inheritance of the rights to only the immediate child file or folder, select <i>Restrict inheritance to immediate child files/folders only</i>. 4. Click <i>OK</i>.
<i>Create Groups on the Managed Device if they Do not Exist</i>	Creates a group for which permissions are configured; however the group does not exist on the managed device. With this option, you can create only local groups.
<i>Remove Access Control Rules not Configured by ZENworks</i>	Removes all access control entries for users or groups not configured by the ZENworks Local File Rights policy. Also, updates the existing access control entries for users and groups configured in the policy. After the policy is applied, any manual changes made to the permissions for a user or group configured by the policy are lost when the policy is re-applied.
<i>Inherit Applicable Access Rights Configured on Parent Folders</i>	Select <i>Yes</i> if you want a file or folder to inherit applicable access control rules from its parent object. If you select <i>No</i> , inherited rules are removed. If you do not want to make any changes, select <i>not configured</i> on the managed device. At least one attribute, permission, or inheritance setting must be configured to create a policy. Without configuring any settings, you cannot create a policy.

- 6 Click *Next* to display the Summary page.
- 7 Click *Finish* to create the policy now, or select *Define Additional Properties* to specify additional information, such as policy assignment, **system requirements**, enforcement, status, and which group the policy is a member of.

2.4 Printer Policy

The Printer policy allows you to configure Local, SMB, HTTP, and iPrint printers on a Windows device.

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 In the *Policies* list, click *New*, then click *Policy* to display the Select Policy Type page.
- 3 Select *Printer Policy*, click *Next* to display the Define Details page, then fill in the fields:
 - Policy Name:** Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in ZENworks Control Center.
 - Folder:** Type the name or browse to and select the ZENworks Control Center folder where you want the policy to reside. The default is `/policies`, but you can create additional folders to organize your policies.
 - Description:** Provide a short description of the policy's content. This description displays in ZENworks Control Center.
- 4 Click *Next* to display the Printer Identification page, then select the type of printer to be installed on the managed device.
- 5 Click *Next*, then skip to the appropriate step, depending on which printer type you chose in **Step 4**:
 - ♦ **Local Printer:** Continue with **Step 6**.
 - ♦ **Network Printer:** Skip to **Step 7**.
 - ♦ **iPrint Printer:** Skip to **Step 8**.
- 6 (Conditional) If you are configuring a local printer, refer to the following table for more information:

Field	Details
<i>Name</i>	Specify the name of the local printer that you want to configure on the target device.
<i>Port</i>	Select the physical port to which the printer is added, such as LPT1 or COM1.
<i>Driver</i>	Browse to and select a suitable driver for the printer. If the driver is not contained in the browser list, type in the correct model name. The driver must either be installed on the target device or specified in the installed policies.

Field	Details
<i>Install a Driver</i>	<p>Select this option to install a driver on the target device. The driver installation must be non-interactive and silent. The supported driver installation type is <code>.inf</code> and the <code>.inf</code> driver files can be bundled in <code>.zip</code> or <code>.tar</code> formats. The <code>.inf</code> file can be specified directly if it is already available on the target device.</p> <hr/> <p>NOTE: To add a new printer driver to the existing driver list:</p> <p>Edit the <code>zenworks_installdir\novell\zenworks\share\tomcat\webapps\zenworks\WEB-INF\conf\printerDriverDetails.conf</code> file to add the following line:</p> <pre>Printer_Manufacturername = Printer_Model</pre> <p>For example, if you want to add an HP* Color LaserJet* 4550 PCL printer, then add the following line:</p> <pre>HP = HP Color LaserJet 4550 PCL</pre> <hr/>
<i>Model Name</i>	Browse to select the model name of the driver. The <code>.inf</code> file should support installation of the driver with a similar name.
<i>Driver File Path</i>	Specify the driver files either from a particular device where the browser is running or from a path in the managed device, such as <code>C:\temp\nipp.zip</code> .
<i>Supported Platforms</i>	Specify a platform for the driver. The platform information helps to select a suitable driver from the available drivers list, which is based on the installation platform.
<i>Language of Installation</i>	Select the installation language. Your choices are English (United States), French, German, Portuguese, Spanish, Italian, Chinese (Traditional), Chinese (Simplified), or Japanese.
<i>Install Forcefully Even if the Driver is Already Installed</i>	Select this option to force installation of the driver, even though it is already installed on the target device.

- 7** (Conditional) If you are configuring a Network printer, refer to the following table for more information:

Field	Details
<i>Name / Location</i>	<p>Specify the UNC path or URL name of the HTTP or an SMB printer.</p> <p>For example, it is <code>\\server-name\printer-name</code> for an SMB printer, and <code>http://server/printers/.myprinter/.printer</code> for a HTTP printer.</p>
<i>Driver</i>	Browse to add and select a suitable driver for the Windows HTTP printer. You can ignore this for SMB printers.

Field	Details
<i>Install a Driver</i>	<p>Use this option to install a driver on the target device. The driver installation is non-interactive and silent. The supported driver installation types are <code>.inf</code> and <code>.exe</code>. For the <code>.inf</code> type, the driver files can be bundled in <code>.zip</code> or <code>.tar</code> formats. The <code>.inf</code> file can be specified directly if it is already available on the target device.</p> <hr/> <p>NOTE: To add a new printer driver to the existing driver list:</p> <p>Edit the <code>zenworks_installdir\novell\zenworks\share\tomcat\webapps\zenworks\WEB-INF\conf\printerDriverDetails.conf</code> file to add the following line:</p> <pre>Printer_Manufacturername = Printer_Model</pre> <p>For example, if you want to add an HP Color LaserJet 4550 PCL printer, then add the following line:</p> <pre>HP = HP Color LaserJet 4550 PCL</pre> <hr/>
<i>Model Name</i>	Browse to select the model name of the driver. The <code>.inf</code> file should support installation of the driver with a similar name.
<i>Driver File Path</i>	Specify the driver files either from a particular device where the browser is running or from a path in the managed device, such as <code>c:\temp\nip.zip</code> .
<i>Supported Platforms</i>	Specify a platform for the driver. The platform information helps to select a suitable driver from the available drivers list, which is based on the installation platform.
<i>Language of Installation</i>	Select the installation language. Your choices are English (United States), French, German, Portugese, Spanish, Italian, Chinese (Traditional), Chinese (Simplified), or Japanese.
<i>Install Forcefully Even if the Driver is Already Installed</i>	Select this option to force installation of the driver, even though it is already installed on the target device.

- 8** (Conditional) If you are configuring an iPrint printer, refer to the following table for more information:

On Windows Vista devices, you need to install the Novell iPrint client 5.04 or later.

Field	Details
<i>Name / Location</i>	Specify the URI name of the iPrint printer. For example, <code>ipp://acme.com/ipp/servername</code> .
<i>Update iPrint Printer while Installing the Driver</i>	Select this option to update the printer driver and to reinstall the printer driver from the iPrint server while installing the iPrint printer.
<i>Install iPrint Client</i>	<p>Select this option to install the iPrint client on a target machine.</p> <p>The installation file can be either <code>nipp.zip</code> or <code>nipp-s.exe</code>, both of which are capable of carrying out non-interactive silent installation. These files can be uploaded from the machine where the browser is running.</p>

Field	Details
<i>iPrint Client Installer File Path</i>	<p>Allows to specify the path to the iPrint Client Installer (which installs the iPrint client on the managed device).</p> <ul style="list-style-type: none"> ♦ On the Managed Device: Select this option to specify the path to the iPrint client installer on the managed device. ♦ Select from this Device: Select this option to add the iPrint client installer as content with the policy. You can also distribute the iPrint client installer along with the policy.
<i>Install Forcefully Even if the Driver is Already Installed</i>	Select this option to force installation of the driver, even though it is already installed on the target device.
<i>Configure iPrint Client</i>	<p>Select this option to configure the iPrint proxy server.</p> <p>If the workstations are located outside the physical firewall, you can use this option to specify the proxy address followed by a (:) and the port number.</p>
<i>Proxy Server</i>	Specify the iPrint proxy server name. For example, <code>http://proxy.companyx.com:8080</code>

- 9 Click *Next* to display the Printing Preferences page, then use the options to specify the preferences. Refer to the following table for more information:

Field	Details
<i>Orientation</i>	Select this option to specify the paper layout for the printer, such as landscape or portrait.
<i>Duplex Printing</i>	Specify whether or not to print on both sides of the paper, if the printer has that capability.
<i>Collate</i>	Specify whether or not the printer should organize multiple copies of a document, if the printer has that capability.
<i>Print Quality</i>	Select the print quality. Select <i>High</i> quality, for the best possible resolution, or select <i>Low</i> quality for lower resolution and lower quality.
<i>Paper Source</i>	<p>Specify the paper source for the printer. A source that is not listed in the standard available list can also be specified, but it must be supported by the printer. Information on supported paper sources is available in the printer documentation or in the registry key</p> <p><code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\printer-name\DsDriver\printBinNames</code> on a Windows machine.</p>
<i>Paper Size</i>	<p>Specify the paper size for the printer. You can specify any paper size supported by the printer, in addition to the options listed in the menu. Information on supported sizes is available in the printer documentation or in the registry key</p> <p><code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\printer-name\DsDriver\printMediaSupported</code> for a Windows machine, where a printer is locally installed.</p>

- 10 Click *Next* to display the Additional Printer Policy settings, then use the options to specify the settings. Refer to the following table for more information:

Field	Details
<i>Set as Default Printer</i>	Select this option to specify a printer as the default printer to which the print requests are sent if no other printer is specified by the user.
<i>Remove all Printers not Specified by ZENworks Printer Policies</i>	Select this option to remove all printers that are not specified through the ZENworks Printer policy.

- 11 Click *Next* to display the Summary page.

This wizard allows you to configure only one printer. If you want to configure additional printers, then configure them in the Details page after creating the policy.
- 12 Click *Finish* to create the policy now, or select *Define Additional Properties* to specify additional information, such as policy assignment, **system requirements**, enforcement, status, and which group the policy is a member of.

Only the preferences that are supported by the printer are configured on that printer.

2.5 Remote Management Policy

The Remote Management policy lets you configure the behavior or execution of a Remote Management session on the managed device. The policy includes properties such as Remote Management operations and security.

By default, a secure Remote Management policy is created on the managed device when the ZENworks Adaptive Agent is deployed with the Remote Management component on the device. You can use the default policy to remotely manage a device. To override the default policy, you can explicitly create a Remote Management policy for the device.

For information on creating the Remote Management policy, see “**Creating the Remote Management Policy**” in the *ZENworks 10 Configuration Management Remote Management Reference*.

2.6 Roaming Profile Policy

The Roaming Profile policy allows you to create a user profile that is stored in a network path. An administrator can either use the roaming profile stored in the user’s home directory or the profile stored in the network directory location.

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 In the *Policies* list, click *New*, then click *Policy* to display the Select Policy Type page.
- 3 Select *Roaming Profile Policy*, click *Next* to display the Define Details page, then fill in the fields:

Policy Name: Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in ZENworks Control Center.

Folder: Type the name or browse to and select the ZENworks Control Center folder where you want the policy to reside. The default is /policies, but you can create additional folders to organize your policies.

Description: Provide a short description of the policy's content. This description displays in ZENworks Control Center.

- 4 Click *Next* to display the Roaming Profile Policy page, then use the options to specify the settings. Refer to the following table for more information:

Field	Details
<i>Store User Profile in User's Home Directory</i>	Select this option to load and save a user's profile from the user's home directory as specified in eDirectory. This option is applicable only if the user object is in eDirectory.
<i>User Profile Path</i>	Select a UNC path to a user's roaming profile. If you want to administer the policy on more than one user object, use %USERNAME% as the environment variable. In this case, the environment variable is resolved with the logged-on username and the user profile is loaded from the specified path.
<i>Override Terminal Server Profile</i>	If a user is accessing a terminal server that has its own profile, enable this option to override the terminal server's profile.

- 5 Click *Next* to display the Summary page.
- 6 Click *Finish* to create the policy now, or select *Define Additional Properties* to specify additional information, such as policy assignment, **system requirements**, enforcement, status, and which group the policy is a member of.

2.7 SNMP Policy

The SNMP policy allows you to configure SNMP parameters on the managed devices.

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 In the *Policies* list, click *New*, then click *Policy* to display the Select Policy Type page.
- 3 Select *SNMP Policy*, click *Next* to display the Define Details page, then fill in the fields:

Policy Name: Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in ZENworks Control Center.

Folder: Type the name or browse to the ZENworks Control Center folder where you want the policy to reside. The default is /policies, but you can create additional folders to organize your policies.

Description: Provide a short description of the policy's content. This description displays in ZENworks Control Center.
- 4 Click *Next* to display the SNMP Community Strings page. Refer to the following table for more information:

Field	Details
<i>Add a Community String</i>	Allows you to add a community string.

Field	Details
<i>Community String</i>	Specify the name of the SNMP community string to be added.
<i>Community Rights</i>	Allows you to administer rights for a selected community, such as Read Only, Read & Write, Read & Create, and Notify.
<i>Remove All SNMP Community Strings not specified by ZENworks SNMP Policies</i>	Select this option to remove all the community strings that are not specified through ZENworks SNMP policy.
<i>Send SNMP Authentication Trap</i>	Select this option if you want to send authentication trap information.

This page allows you to add only one community string to the policy. If you want to add multiple community strings, then configure them in the Details page after creating the policy.

- 5 Click *Next* to display the SNMP Default Access Control List page, then use the options to specify the settings. Refer to the following table for more information:

Field	Details
<i>Allow SNMP Communication</i>	Select this option to specify whether SNMP communication is allowed from any host or a list of predefined hosts.
<i>Remove All SNMP Allowed Hosts not Specified by ZENworks SNMP Policies</i>	Select this option to remove all the SNMP allowed hosts that are not specified through the ZENworks SNMP policy.

- 6 Click *Next* to display the SNMP Trap Targets page, then use the options to specify the settings. Refer to the following table for more information:

Field	Details
<i>Add a Trap Target</i>	Allows you to add a trap target for the SNMP service.
<i>IP Address / Host Name</i>	Specify an IP address or host name of the target device.
<i>Community String</i>	Specify a community string for the trap target defined in <i>IP address/ Host name</i> .
<i>Remove All SNMP Trap Targets Not Specified by ZENworks SNMP Policies</i>	Select this option to remove all the trap targets that are not specified through the ZENworks SNMP policy.

This page allows you to add only one trap target to the policy. If you want to add multiple trap targets, then configure them in the Details page after creating the policy.

- 7 Click *Next* to display the Default System Requirements for SNMP Policy page, then use the options to specify the settings. Refer to the following table for more information:

Field	Details
<i>Apply Policy Only if SNMP Service Exists On the Target Device</i>	Select this option apply the SNMP policy only if the SNMP service exists on the target device. If the target device does not contain the SNMP service, the SNMP policy cannot be fully applied or effective on the target device.

- 8 Click *Next* to display the Summary page.
- 9 Click *Finish* to create the policy now, or select *Define Additional Properties* to specify additional information, such as policy assignment, **system requirements**, enforcement, status, and which group the policy is a member of.

2.8 Windows Group Policy

The Windows Group policy allows you to configure Group policy for Windows devices.

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 In the *Policies* list, click *New*, then click *Policy* to display the Select Policy Type page.
- 3 Select *Windows Group Policy*, click *Next* to display the Define Details page, then fill in the fields:

Policy Name: Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in ZENworks Control Center.

Folder: Type the name or browse to and select the ZENworks Control Center folder where you want the policy to reside. The default is `/policies`, but you can create additional folders to organize your policies.

Description: Provide a short description of the policy's content. This description displays in ZENworks Control Center.
- 4 Click *Next* to display the Windows Group Policy Settings page, then use the options to specify the settings. Refer to the following table for more information:

Field	Details
<i>Select the Type of Group Policy to Manage</i>	<p>With the Windows Group policy, you can manage either a Local group or an Active Directory group policy.</p> <p>Before you can configure the Group policy, you need to install a helper application. Click <i>Install the Group Policy Helper</i> to install the <code>novell-zenworks-grouppolicyhelper-10.1.x.x.msi</code>, which is a Windows installer package. This installation needs to be done only once. After the helper is installed, clicking <i>Configure</i> launches the helper, which you then use to configure or import a policy.</p> <ul style="list-style-type: none"> ♦ Local Group Policy: Select this option to configure a Local Group policy. To launch the group policy helper, click <i>Configure</i>. Configure or edit the settings in the Local Group policy, then upload the configured policy to the ZENworks Server. ♦ Active Directory Group Policy: Select this option to use an Active Directory Group policy. To launch the group policy helper, click <i>Configure</i>. Import an Active Directory Group policy, then upload the ZENworks Server. (You cannot edit an Active Directory policy through ZENworks Control Center.)
<i>Select the Configuration Settings to Be Applied On the Managed Device</i>	<p>After you have adjusted the policy settings as you prefer, you can select how to apply the settings to the managed device.</p> <hr/> <p>NOTE: The Computer Configuration settings from a user associated group policy are not applied when the user logs into a Windows 2000 or Windows 2003 Terminal Server.</p>

- 5 Click *Next* to display the Summary page.
- 6 Click *Finish* to create the policy now, or select *Define Additional Properties* to specify additional information, such as policy assignment, **system requirements**, enforcement, status, and which group the policy is a member of.

If the login/logoff scripts are configured in a user-associated group policy and the *Apply Immediate* option is selected, then a relogin is forced and the login scripts run when the user logs into the managed device again. The startup scripts from a device-associated policy run only when the device reboots the next time.

IMPORTANT: If you want to apply the Windows Group policy on Windows XP SP1 or SP2 managed devices, ensure that the devices have Windows Hotfix KB897327 installed. For more information about how to install the Hotfix, see the [Microsoft Support Web site \(http://support.microsoft.com/KB/897327\)](http://support.microsoft.com/KB/897327).

2.9 ZENworks Explorer Configuration Policy

The ZENworks Explorer Configuration Policy allows you to administer and centrally manage the behavior and features of ZENworks Explorer.

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 In the *Policies* list, click *New*, then click *Policy* to display the Select Policy Type page.

- 3 Select *ZENworks Explorer Configuration Policy*, click *Next* to display the Define Details page, then fill in the fields:

Policy Name: Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in ZENworks Control Center.

Folder: Type the name or browse to and select the ZENworks Control Center folder where you want the policy to reside. The default is */policies*, but you can create additional folders to organize your policies.

Description: Provide a short description of the policy's content. This description displays in ZENworks Control Center.

- 4 Click *Next* to display the ZENworks Explorer Configuration Settings page, then use the options to specify the settings. Refer to the following table for more information:

Field	Details
<i>Enable Folder View</i>	Use this option to display a folder list in the application window. The values are <i>Yes</i> , <i>No</i> , and <i>Unconfigured</i> . The default value is <i>Unconfigured</i> and the existing settings of the managed device are retained.
<i>Expand the Entire Folder Tree</i>	Use this option to expand the entire folder tree when the application window is opened. The values are <i>Yes</i> , <i>No</i> , and <i>Unconfigured</i> . The default value is <i>Unconfigured</i> and the existing settings of the managed device are retained.
<i>Display Applications in Windows Explorer</i>	Use this option to display only the application list in Windows Explorer. The values are <i>Yes</i> , <i>No</i> , and <i>Unconfigured</i> . The default value is <i>Unconfigured</i> and the existing settings of the managed device are retained.
<i>Name of Root Folder</i>	Use this option to change the name of the root folder.
Hide the Zicon in the taskbar	Use this option to hide the ZENworks icon in the taskbar. The values are <i>Yes</i> , <i>No</i> , and <i>Unconfigured</i> . The default value is <i>Unconfigured</i> and the existing settings of the managed device are retained.
<i>Enable Manual Refresh</i>	Use this option to specify whether manual refresh of applications is enabled after starting ZENworks Explorer. The values are <i>Yes</i> , <i>No</i> , and <i>Unconfigured</i> . The default value is <i>Unconfigured</i> and the existing settings of the managed device are retained.
<i>Allow Logout / Login as a New User</i>	Use this option to enable the user to log out and log in as a new user. The values are <i>Yes</i> , <i>No</i> , and <i>Unconfigured</i> . The default value is <i>Unconfigured</i> and the existing settings of the managed device are retained.

Field	Details
<i>Show Progress</i>	<p>Use this option to specify whether the progress of the bundle operations should be displayed.</p> <p>The values are <i>Yes</i>, <i>No</i>, and <i>Unconfigured</i>. The default value is <i>Unconfigured</i> and the existing settings of the managed device are retained.</p>
<i>Show Default Notification</i>	<p>Use this option to specify whether the default notification should be displayed.</p> <p>The values are <i>Yes</i>, <i>No</i>, and <i>Unconfigured</i>. The default value is <i>Unconfigured</i> and the existing settings of the managed device are retained.</p>
<i>Start the ZENworks Explorer with the {All} Folder Displayed</i>	<p>Use this option to specify whether the [All] folder should be displayed when ZENworks Explorer starts.</p> <p>The values are <i>Yes</i>, <i>No</i>, and <i>Unconfigured</i>. The default value is <i>Unconfigured</i> and the existing settings of the managed device are retained.</p>

- 5 Click *Next* to display the Summary page.
- 6 Click *Finish* to create the policy now, or select *Define Additional Properties* to specify additional information, such as policy assignment, **system requirements**, enforcement, status, and which group the policy is a member of.

2.10 Creating Policies by Using the zman Command Line Utility

ZENworks Configuration Management allows you to create different types of policies, such as Browser Bookmarks policy, Dynamic Local User policy, Local File Rights policy, and Printer policy. Each policy has its own set of data and configuration settings. Because it is complex to pass the data as arguments in the command line, the zman utility takes XML files as an input to create policies. You can use the exported XML file as a template to create policies. To use the zman command line utility to create a policy, you must have a policy of the same type already created through ZENworks Control Center and export it to an XML file. For more information on creating policies by using ZENworks Control Center, see [Chapter 2, “Creating Policies,” on page 13](#).

For example, you can export a Browser Bookmarks Policy already created through ZENworks Control Center into an XML file, then use it to create another Browser Bookmarks Policy by using zman.

A policy can have file content associated with it. For example, the printer driver to be installed is a file associated with the Printer policy.

Review the following sections to create a policy by using the zman command line utility:

- ♦ [Section 2.10.1, “Creating a Policy without Content,” on page 30](#)
- ♦ [Section 2.10.2, “Creating a Policy with Content,” on page 32](#)
- ♦ [Section 2.10.3, “Understanding the zman Policy XML File Format,” on page 33](#)

2.10.1 Creating a Policy without Content

- 1 Create a policy in ZENworks Control Center.

For example, use ZENworks Control Center to create a Browser Bookmarks Policy called google containing a bookmark to <http://www.google.co.in>.

- 2 Export the policy to an XML file by using the following command:

```
zman policy-export-to-file policy_name policy_filename.xml
```

For example, export the google policy to `google.xml` by using the

```
zman policy-export-to-file google google.xml
```

 command.

If you want to create a new policy with new data, continue with **Step 3**. If you want to create a new policy with the same data as the google policy, skip to **Step 4**.

- 3 Modify the XML file according to your requirements.

For example, in `google.xml`, change the value of `<URL>` from `http://www.google.co.in` to `http://www.yahoo.com` in the browserbookmarkspolicy action of the Enforcement action set and `<PolicyData>` element in both `<Actions>` and `<PolicyData>` elements as shown below.

```
<ns2:ActionSets>

  <Id>879de60b7591b6f6aefae09fcd83db54</Id>

  <Type>Enforcement</Type>

  <Version>1</Version>

  <Modified>>false</Modified>

  <Actions>

    <Id>0ab9a1785370bcd38bc862bd2817abac</Id>

    <Name>browserbookmarkspolicy</Name>

    <Type>browserbookmarkspolicy</Type>

    <Data>

      <PolicyData xmlns="http://novell.com/zenworks/datamodel/objects/policies">

        <BookmarksPolicyHandlerData xmlns="">

          <EnforcePolicy>

            <Bookmarks>

              <Bookmark Type="url_string">

                <Name>Google</Name>

                <Url>http://www.yahoo.com</Url>
```

```

        <Folder>/</Folder>

    </Bookmark>

</Bookmarks>

</EnforcePolicy>

</BookmarksPolicyHandlerData>

</PolicyData>

</Data>

<ContinueOnFailure>true</ContinueOnFailure>

<Enabled>true</Enabled>

<Properties>StandaloneName=browserbookmarksenf;Impersonation=SYSTEM;</
Properties>

</Actions>

</ns2:ActionSets>

<ns2:ActionSets xmlns:ns2="http://novell.com/zenworks/datamodel/objects/
actions" xmlns="http://novell.com/zenworks/datamodel/objects/actions">

    <Id>4efa37c827cf0e8a8ac20b23a3022227</Id>

    <Type>Distribution</Type>

    <Version>1</Version>

    <Modified>>false</Modified>

    <Actions>

        <Id>27c4a42544210b3ac3b067ff6aff2d5c</Id>

        <Name>Distribute Action</Name>

        <Type>Distribute Action</Type>

        <ContinueOnFailure>true</ContinueOnFailure>

        <Enabled>true</Enabled>

        <Properties />

    </Actions>
</ns2:ActionSets>

<ApplyImmediate>>false</ApplyImmediate>

<PolicyData>

    <BookmarksPolicyHandlerData>

```

```

<EnforcePolicy>

  <Bookmarks>

    <Bookmark Type="url_string">

      <Name>Google</Name>

      <Url>http://www.yahoo.com</Url>

      <Folder></Folder>

    </Bookmark>

  </Bookmarks>

</EnforcePolicy>

</BookmarksPolicyHandlerData>

</PolicyData>

```

- 4 Create a new policy by using the following command:

```
zman policy-create new_policy_name policy_xml_filename.xml
```

For example, to create the yahoo policy, use the `zman policy-create yahoo google.xml` command.

2.10.2 Creating a Policy with Content

- 1 Create a policy in ZENworks Control Center.

For example, use ZENworks Control Center to create a Printer policy of type iPrint called iPrintPolicy that automatically installs an iPrint driver from the `driver.zip` file provided as the policy content, and configures an iPrint printer on the device.

- 2 Export the policy to an XML file by using the following command:

```
zman policy-export-to-file policy_name policy_filename.xml
```

This creates `policy_filename.xml` and `policy_filename_ActionContentInfo.xml` files.

For example, export iPrintPolicy to `iPrintPolicy.xml` by using the `zman policy-export-to-file iPrintPolicy iPrintPolicy.xml` command. The `iPrintPolicy.xml` and `iPrintPolicy_ActionContentInfo.xml` files are created. For more information about `ActionContentInfo.xml`, see [Section 2.10.3, “Understanding the zman Policy XML File Format,”](#) on page 33.

If you want to create a new policy with new data, continue with [Step 3](#). If you want to create a new policy with the same data as iPrintPolicy, skip to [Step 4](#).

- 3 Modify the `iPrintPolicy.xml` and `iPrintPolicy_actioncontentinfo.xml` files according to your requirements.

For example, to create a new policy to configure and install another iPrint in the network with a newer version of the driver, do the following:

- ♦ Change all references of `driver.zip` to `newDriver.zip` in the `<ActionSet>` and the `<PolicyData>` section of `iPrintPolicy.xml`, and in the `<ActionSet>` section of `iPrintPolicy_actioncontentinfo.xml`.
- ♦ Replace the name of the printer in the `iPrintPolicy.xml` file with the new name of the printer.

A sample `iPrintPolicy_actioncontentinfo.xml` is shown below.

```
<ActionInformation>

<ActionSet type="Enforcement">

  <Action name="printer policy" index="1">

    <Content>

      <ContentFilePath>driver.zip</ContentFilePath>

    </Content>

  </Action>

</ActionSet>

</ActionInformation>
```

4 Create a new policy by using the following command:

```
zman policy-create new_policy_name policy_xml_filename.xml --
actioninfo policy_name_actioncontentinfo.xml
```

For example, use the following command to create a policy called `New_iPrintPolicy`:

```
zman policy-create New_iPrintPolicy iPrintPolicy.xml --
actioninfo iPrintPolicy_ActionContentInfo.xml
```

2.10.3 Understanding the zman Policy XML File Format

The `policy-export-to-file` command serializes the policy information, which is stored in the database, into an XML file. Each policy contains actions that are grouped into Action Sets, Enforcement, and Distribution. An exported policy XML file contains information for the policy, such as UID, Name, Path, PrimaryType, SubType, PolicyData, System Requirements, and information on all Action Sets and their actions. The file does not include information about assignment of the policy to devices or users.

A sample XML format template, `WindowsGroupPolicy.xml`, is available at `/opt/novell/zenworks/share/zman/samples/policies` on a Linux server and in `ZENworks_Installation_directory:\Novell\Zenworks\share\zman\samples\policies` on a Windows server.

NOTE: If the exported XML file contains extended ASCII characters, you must open it in an editor by using UTF-8 encoding instead of ANSI coding, because ANSI coding displays the extended ASCII characters as garbled.

When you create a policy from the XML file, zman uses the information specified in the `<Description>`, `<SubType>`, `<Category>`, `<ActionSets>`, `<PolicyData>`, and `<SysReqs>` tags of the file. The values for the Name and Parent folder are taken from the command line. For the remaining elements, the default value is used.

Follow the guidelines listed below to work with the XML file:

- ♦ If you want to create a policy without file content, you need only the policy XML file to create the policy.

For example, Local File Rights Policy does not have file content associated with it.

- ♦ If you want to create a policy with content, you must provide an additional XML file, which contains the path of the content file, as an argument to the `--actioninfo` option of the `policy-create` command.

For example, Printer policy can have the printer drivers to be installed as associated file content.

A sample XML format template, `ActionInfo.xml`, is available at `/opt/novell/zenworks/share/zman/samples/policies` on a Linux server and in `ZENworks_Installation_directory:\Novell\Zenworks\share\zman\samples\policies` on a Windows server.

- ♦ If you want to modify the `<Data>` element of actions in the exported XML file, ensure that the new data is correct and that it conforms to the schema. The zman utility does a minimal validation of the data and does not check for the errors. Hence, the policy might be successfully created, but with invalid data. Such a policy fails when deployed on a managed device.
- ♦ File content is associated with a particular action in an Action Set. The Action Content Information XML file should contain the path of the file to which the file content is to be associated and the index of the action in the Action Set.

For example, the Printer driver selected to be installed when creating a Printer policy is associated to the `printerpolicy` action in the Enforcement action set of the created Printer policy.

- ♦ The Action Set is specified by the `type` attribute in `<ActionSet>` element. It should be the same as the Action Set type of the policy XML file.
- ♦ The `<Action>` element has a `name` attribute, which is optional, for user readability.
- ♦ The `index` attribute is mandatory. It specifies the action to which the content should be associated to. The index value of the first action in the Action Set is 1.
- ♦ Each action can have multiple `<Content>` elements, each containing a `<ContentFilePath>` element. The `<ContentFilePath>` element contains the path of the file content to be associated with the Action. Ensure that the filename is the same as the filename specified in the policy XML file in `<Data>` for that action.
- ♦ Ensure that the order of the `<Content>` elements is in accordance with the order in the policy XML file. For example, a Printer Policy can have multiple drivers configured. The path to the driver files should be specified in the `<Content>` elements in the order the files are specified in the data for the action as show below.

```
<ActionInformaion>

  <ActionSet type="Enforcement">

    <Action name="printer policy" index="1">
```

```
<Content>

  <ContentFilePath>driver1.zip</ContentFilePath>

</Content>

<Content>

  <ContentFilePath>driver2.zip</ContentFilePath>

</Content>

</Action>

</ActionSet>

</ActionInformation>
```


Managing Policies

3

Novell® ZENworks® 10 Configuration Management lets you use effectively manage software and content in your ZENworks system. In addition to editing and deleting existing objects, you can create new objects and perform various tasks on the objects.

You can use ZENworks Control Center or the zman command line utility to manage policies. This section explains how to perform this task by using the ZENworks Control Center. If you prefer the zman command line utility, see “[Policy Commands](#)” in the *ZENworks 10 Configuration Management Command Line Utilities Reference*.

- ♦ [Section 3.1, “Policy Groups,” on page 37](#)
- ♦ [Section 3.2, “Editing Policies,” on page 38](#)
- ♦ [Section 3.3, “Deleting Policies,” on page 39](#)
- ♦ [Section 3.4, “Adding Policies to Existing Groups,” on page 39](#)
- ♦ [Section 3.5, “Assigning a Policy to Devices,” on page 40](#)
- ♦ [Section 3.6, “Assigning a Policy to Users,” on page 41](#)
- ♦ [Section 3.7, “Assigning the Local File Rights Policy to Devices Running Different Languages,” on page 42](#)
- ♦ [Section 3.8, “Adding System Requirements for a Policy,” on page 42](#)
- ♦ [Section 3.9, “Disabling Policies,” on page 47](#)
- ♦ [Section 3.10, “Enabling the Disabled Policies,” on page 47](#)
- ♦ [Section 3.11, “Copying a Policy to a Content Server,” on page 47](#)
- ♦ [Section 3.12, “Incrementing the Policy Version,” on page 49](#)
- ♦ [Section 3.13, “Reviewing the Status of the Policies at the Managed Device,” on page 50](#)
- ♦ [Section 3.14, “Predefined Policy Reports,” on page 50](#)

3.1 Policy Groups

A policy group is two or more policies. Creating policy groups eases administration efforts by letting you assign the group, rather than each individual policy, to devices and users.


- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 In the *Policies* list, click *New*, click *Policy Group* to display the Basic Information page, then fill in the fields:
 - Group Name:** Provide a unique name for your policy group. The name you provide displays in the ZENworks Control Center interface.
 - Folder:** Type the name or browse to and select the folder the contains this policy group
 - Description:** Provide a short description of the policy group’s content. This description displays in ZENworks Control Center.
- 3 Click *Next* to display the Add Group Members page. You can add any number of policies to the group. You cannot add other policy groups to the group.

To add a policy:

3a Click *Add* to display the Select Members dialog box.

Because you are adding policies to the group, the Select Members dialog box opens with the *Policies* folder displayed.

3b Browse for and select the policies you want to add to the group. To do so:

3b1 Click  next to a folder to navigate the folders until you find the policy you want to select.

If you know the name of the policy you are looking for, you can also use the *Item name* box to search for the policy.

3b2 Click the underlined link in the *Name* column to select the policy and display its name in the *Selected* list.

3b3 (Optional) Repeat **Step 3b1** and **Step 3b2** to add additional policies to the *Selected* list.

3b4 Click *OK* to add the selected policies to the group.

4 Click *Next* to display the Summary page.

5 Click *Finish* to create the policy group now, or select *Define Additional Properties* to specify additional information, such as user assignment, device assignment, and which members the policy group is a member of.

3.2 Editing Policies

The following table lists the tasks you can perform for a policy:

Task	Steps	Additional Details
Edit the content of a policy	<ol style="list-style-type: none">1. Click the policy whose content you want to edit.2. Click the <i>Details</i> tab, then edit the settings according to your requirements.3. Click <i>Apply</i>.4. Click the <i>Summary</i> page.5. Increment the version of the policy to enforce the changes made to the policy on the managed device.	
Rename a policy	<ol style="list-style-type: none">1. Select the check box next to the policy.2. Click <i>Edit > Rename</i>, then specify the new name.	If more than one check box is selected, the <i>Rename</i> option is not available in the <i>Edit</i> menu.
Create a copy of the policy	<ol style="list-style-type: none">1. Select the check box next to the policy.2. Click <i>Edit > Copy</i>, then specify a new name.	<p>If more than one check box is selected, the <i>Copy</i> option is not available in the <i>Edit</i> menu.</p> <p>The copy option is useful to create a new policy that is similar to an existing policy. You can copy a policy and then edit the new policy's settings.</p>

Task	Steps	Additional Details
Move a policy to a different folder	<ol style="list-style-type: none"> 1. Select the check box next to the policy (or policies). 2. Click <i>Edit > Move</i>, then select the target folder. 	
Copy the system requirements of one policy to another policy	<ol style="list-style-type: none"> 1. Select the check box next to the policy. 2. Click <i>Edit > Copy System Requirements</i>. 3. Select <i>Policies</i>, then click <i>Add</i> to select the policies to which you want to copy the selected policy's system requirements. 	If more than one check box is selected, the <i>Copy System Requirements</i> option is not available in the <i>Edit</i> menu.

3.3 Deleting Policies

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 Select the check box next to the policy (or policies) that you want to delete.
- 3 Click *Delete*.

3.4 Adding Policies to Existing Groups


- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 Select the check box next to the policy (or policies) that you want to add to the group.
- 3 Click *Action > Add to Group* to display the Existing Group or a New Group page.
- 4 You can add the selected objects (users, devices, bundles, policies) to an existing group or a new group.
 - ♦ If the group to which you want to add the objects already exists, select *Add selected items to an existing group*, then click *Next* to continue with **Step 5**.
 - ♦ If you need to create a new group for the selected objects, select *Create a new group to contain the selected items*, then click *Next* to skip to **Step 6**.
- 5 (Conditional) If you are adding selected items to an existing group, the Targets page is displayed. Select the groups to which you want to add the objects (users, devices, bundles, policies).

You can add any number of policies to the group. You cannot add other policy groups to the group.

- 5a Click *Add* to display the Select Groups dialog box.

Because you are adding policies to the group, the Select Members dialog box opens with the *Policies* folder displayed.


- 5b Browse for and select the policies you want to add to the group. To do so:

- 5b1 Click  next to a folder to navigate the folders until you find the policy you want to select.

If you know the name of the policy you are looking for, you can also use the *Item name* box to search for the bundle.

- 5b2** Click the underlined link in the *Name* column to select the policy and display its name in the *Selected* list.
- 5b3** (Optional) Repeat **Step 5a** and **Step 5b** to add additional policies to the *Selected* list.
- 5b4** Click *OK* to add the selected policies to the group.
- 5c** Click *Next* to skip to **Step 7**.
- 6** (Conditional) If you are creating a new group to contain the selected items, the Basic Information page is displayed. Fill in the following fields, then click *Next* to continue with **Step 7**.
 - Group Name:** Provide a unique name for your policy group. The name you provide displays in the ZENworks Control Center interface.
 - Folder:** Type the name or browse to and select the folder that contains this policy group
 - Description:** Provide a short description of the policy group's content. This description displays in ZENworks Control Center.
- 7** On the Finish page, review the information and, if necessary, use the *Back* button to make changes to the information.
- 8** Click *Finish*.

3.5 Assigning a Policy to Devices

- 1** In ZENworks Control Center, click the *Policies* tab.
- 2** In the *Policies* list, select the check box next to the policy (or policies).
- 3** Click *Action > Assign to Device*.
- 4** Browse for and select the devices, device groups, and device folders to which you want to assign the group. To do so:
 - 4a** Click  next to a folder (for example, the *Workstations* folder or *Servers* folder) to navigate through the folders until you find the device, group, or folder you want to select.
If you are looking for a specific item, such as a Workstation or a Workstation Group, you can use the *Items of type* list to limit the types of items that are displayed. If you know the name of the item you are looking for, you can use the *Item name* box to search for the item.
 - 4b** Click the underlined link in the *Name* column to select the device, group, or folder and display its name in the *Selected* list box.
 - 4c** Click *OK* to add the selected devices, folders, and groups to the *Devices* list.
- 5** Click *Next* to display the Policy Conflict Resolution page.
- 6** Set the priority between device-associated policies and user-associated policies for resolving conflicts that arise when policies of the same type are associated to both devices and users.
 - ♦ **User Last:** Select this option to apply policies that are associated to devices first and then the users.
 - ♦ **Device Last:** Select this option to apply policies that are associated to users first and then the devices.
 - ♦ **Device Only:** Select this option to apply policies that are associated only to devices.
 - ♦ **User Only:** Select this option to apply policies that are associated only to users.

- 7 Click *Next* to display the Finish page, review the information and, if necessary, use the *Back* button to make changes to the information.

If you want the policies to be immediately enforced on all the assigned devices, select *Enforce Policies Immediately on all Assigned Devices*.

- 8 Click *Finish*.


NOTE: If you are assigning a Local File Rights policy to a network made up of devices running different languages, see [Section 3.7, “Assigning the Local File Rights Policy to Devices Running Different Languages,”](#) on page 42.

3.6 Assigning a Policy to Users

There are two types of users: users in the corporate directory and local users on managed devices. Policies can be associated to users in the corporate directory. ZENworks assumes that a mapping exists between users in the corporate directory and users on a device. When a user logs in to the corporate directory, ZENworks obtains the policies for the corporate user and caches them on the device.

If a mapping exists between a corporate user and a local user, ZENworks also associates the cached policies with the local user. When a user logs in to the device, the previously cached policies are enforced for the local user. When the user also logs in to the corporate directory, the policies for the corporate user are refreshed, then enforced.

The set of policies, both directly assigned and inherited, is called as a set of assigned policies for a device or a user. When calculating the set of assigned policies, filters such as multiplicity or system requirements are not applied. Groups and containers also have assigned policies. Policies that are disabled are not included in the set of assigned policies.

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 In the *Policies* list, select the check box next to the policy group (or policy groups).
- 3 Click *Action > Assign to User*.
- 4 Browse for and select the user, user groups, and user folders to which you want to assign the group. To do so:
 - 4a Click  next to a folder to navigate through the folders until you find the user, group, or folder you want to select.

If you are looking for a specific item, such as a User or a User Group, you can use the *Items of type* list to limit the types of items that are displayed. If you know the name of the item you are looking for, you can use the *Item name* box to search for the item.
 - 4b Click the underlined link in the *Name* column to select the user, group, or folder and display its name in the *Selected* list box.
 - 4c Click *OK* to add the selected devices, folders, and groups to the *Users* list.
- 5 Click *Next* to display the Finish page, review the information and, if necessary, use the *Back* button to make changes to the information.
- 6 Click *Finish*.

NOTE: If you are assigning a Local File Rights policy to a network made up of devices running different languages, see [Section 3.7, “Assigning the Local File Rights Policy to Devices Running Different Languages,”](#) on page 42.

If a Printer policy that is assigned to a user is unenforced, then the printer permissions of that particular user are removed.

3.7 Assigning the Local File Rights Policy to Devices Running Different Languages

- 1 Create separate Local File Rights policy for each language. For more information on creating the policy, see [Section 2.3, “Local File Rights Policy,” on page 17](#).
- 2 Add filter for each policy:
 - 2a Click the policy, then click *Requirements*.
 - 2b Click *Add Filter*, select the *Registry Key Value* condition, then specify the following:

Key:
`\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\WOW\boot.description`

Value: `language.dll`

Comparator: = (String Type)

Value Data: *language*

For example, on a device with the English language, *language* is *English (American)*. You can use the registry editor to determine the value data of the language.
 - 2c Click *Apply*.
- 3 Assign the policy to the device. For more information on assigning a policy to a device, see [Section 3.5, “Assigning a Policy to Devices,” on page 40](#).
or
Assign the policy to the user. For more information on assigning a policy to a user, see [Section 3.6, “Assigning a Policy to Users,” on page 41](#).

3.8 Adding System Requirements for a Policy

The System Requirements panel lets you define specific requirements that a device must meet for the policy to be assigned to it.

You define requirements through the use of filters. A filter is a condition that must be met by a device in order for the policy to be applied. For example, you can add a filter to specify that the device must have exactly 512 MB of RAM in order for the policy to be applied, and you can add another filter to specify that the hard drive be at least 20 GB in size.

To create system requirements for a policy:

- 1 In ZENworks Control Center, click the *Policies* tab.
 - 2 Click the underlined link for the desired policy to display the policy’s Summary page.
 - 3 Click the *Requirements* tab.
 - 4 Click *Add Filter*, select a filter condition from the drop-down list, then fill in the fields.
- As you construct filters, you need to know the conditions you can use and how to organize the filters to achieve the desired results. For more information, see [Section 3.8.1, “Filter Conditions,” on page 43](#) and [Section 3.8.2, “Filter Logic,” on page 46](#).

5 (Conditional) Add additional filters and filter sets.

6 Click *Apply* to save the settings.

3.8.1 Filter Conditions

You can choose from any of the following conditions when creating a filter:

Bundle Installed: Determines if a specific policy is installed. After specifying the bundle, the two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the specified bundle must already be installed to meet the requirement. If you select *No*, the bundle must not be installed.

Connected: Determines if the device is connected to the network. The two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the device must be connected to the network to meet the requirement. If you select *No*, it must not be connected.

Connection Speed: Determines the speed of the device's connection to the network. The condition you use to set the requirement includes an operator and a value. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible values are bits per second (*bps*), kilobits per second (*Kbps*), megabits per second (*Mbps*), and gigabits per second (*Gbps*). For example, if you set the condition to >= 100 Mbps, the connection speed must be greater than or equal to 100 megabits per second to meet the requirement.

Disk Space Free: Determines the amount of free disk space on the device. The condition you use to set the requirement includes a disk designation, an operator, and a value. The disk designation can be a local drive map (for example, c: or d:). The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible values are bytes (*Bytes*), kilobytes (*KB*), megabytes (*MB*), and gigabytes (*GB*). For example, if you set the condition to c: >= 80 MB, the free disk space must be greater than or equal to 80 megabytes to meet the requirement.

Disk Space Total: Determines the amount of total disk space on the device. The condition you use to set the requirement includes a disk designation, an operator, and a value. The disk designation can be a local drive map (for example, c: or d:). The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible values are bytes (*Bytes*), kilobytes (*KB*), megabytes (*MB*), and gigabytes (*GB*). For example, if you set the condition to c: >= 40 GB, the total disk space must be greater than or equal to 40 gigabytes to meet the requirement.

Disk Space Used: Determines the amount of used disk space on the device. The condition you use to set the requirement includes a disk designation, an operator, and a value. The disk designation can be a local drive map (for example, c: or d:). The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible values are bytes (*Bytes*), kilobytes (*KB*), megabytes (*MB*), and gigabytes (*GB*). For example, if you set the condition to c: <= 10 GB, the used disk space must be less than or equal to 10 gigabytes to meet the requirement.

Environment Variable Exists: Determines if a specific environment variable exists on the device. After specifying the environment variable, the two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the environment variable must exist on the device to meet the requirement. If you select *No*, it must not exist.

Environment Variable Value: Determines if an environment variable value exists on the device. The condition you use to set the requirement includes the environment variable, an operator, and a variable value. The environment variable can be any operating system supported environment variable. The possible operators are *equal to*, *not equal to*, *contains*, and *does not contain*. The possible variable values are determined by the environment variable. For example, if you set the condition to `Path contains c:\windows\system32`, the Path environment variable must contain the `c:\windows\system32` path to meet the requirement.

File Date: Determines the date of a file. The condition you use to set the requirement includes the filename, an operator, and a date. The filename can be any filename supported by the operating system. The possible operators are *on*, *after*, *on or after*, *before*, and *on or before*. The possible dates are any valid dates. For example, if you set the condition to `app1.msi on or after 6/15/07`, the `app1.msi` file must be dated 6/15/2007 or later to meet the requirement.

File Exists: Determines if a file exists. After specifying the filename, the two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the specified file must exist to meet the requirement. If you select *No*, the file must not exist.

File Size: Determines the size of a file. The condition you use to set the requirement includes the filename, an operator, and a size. The filename can be any file name supported by the operating system. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible sizes are designated in bytes (*Bytes*), kilobytes (*KB*), megabytes (*MB*), and gigabytes (*GB*). For example, if you set the condition to `doc1.pdf <= 3 MB`, the `doc1.pdf` file must be less than or equal to 3 megabytes to meet the requirement.

IP Segment: Determines the device's IP address. After specifying the IP segment name, the two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the device's IP address must match the IP segment. If you select *No*, the IP address must not match the IP segment.

Memory: Determines the amount of memory on the device. The condition you use to set the requirement includes an operator and a memory amount. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The memory amounts are designated in megabytes (*MB*) and gigabytes (*GB*). For example, if you set the condition to `>= 2 GB`, the device must have at least 2 gigabytes of memory to meet the requirement.

Novell Client 32 Connection Used: Determines if the device is using the Novell Client™ for its network connection. The two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the device must be using the Novell Client to meet the requirement. If you select *No*, it must not be using the Novell Client.

Operating System - Windows: Determines the architecture, service pack level, type, and version of Windows running on the device. The condition you use to set the requirement includes a property, an operator, and a property value. The possible properties are *architecture*, *service pack*, *type*, and *version*. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The property values vary depending on the property. For example, if you set the condition to `architecture = 32`, the device's Windows* operating system must be 32-bit to meet the requirement.

NOTE: Be aware that operating system version numbers contain four components: Major, Minor, Revision, and Build. For example, the Windows 2000 SP4 release's number might be 5.0.2159.262144. Each component is treated independently. For this reason, the system requirements that you set might not provide your expected results.

For example, if you specify *Operating System - Windows* in the first field, *Version* in the second field, *>* in the third field, and *5.0 - Windows 2000 Versions* in the last field, you are specifying only the first two components of the version number: Major (Windows) and Minor (5.0). As a result, for the requirement evaluated to true, the OS will have to be at least 5.1 (Windows XP). Windows 2003 is version 5.2, so specifying *> 5.2* will also evaluate to true.

However, because each component is independent, if you specify the version *> 5.0*, Windows 2000 SP4 evaluates to false because the actual version number might be 5.0.2159.262144. You can type *5.0.0* to make the requirement evaluate as true because the actual revision component is greater than 0.

When you select the OS version from the drop-down, the Major and Minor components are populated. The Revision and Build components must be typed in manually.

Primary User Is Logged In: Determines if the device's primary user is logged in. The two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the primary user must be logged in to meet the requirement. If you select *No*, the user must not be logged in.

Processor Family: Determines the device's processor type. The condition you use to set the requirement includes an operator and a processor family. The possible operators are equals (=) and does not equal (<>). The possible processor families are *Pentium*, *Pentium Pro*, *Pentium II*, *Pentium III*, *Pentium 4*, *Pentium M*, *WinChip*, *Duron*, *BrandID*, *Celeron*, and *Celeron M*. For example, if you set the condition to *<> Celeron*, the device's processor can be any processor family other than Celeron* to meet the requirement.

Processor Speed: Determines the device's processor speed. The condition you use to set the requirement includes an operator and a processor speed. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible processor speeds are hertz (*Hz*), kilohertz (*KHz*), megahertz (*MHz*), and gigahertz (*GHz*). For example, if you set the condition to *>= 2 GHz*, the device's speed must be at least 2 gigahertz meet the requirement.

Registry Key Exists: Determines if a registry key exists. After specifying the key name, the two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the specified key must exist to meet the requirement. If you select *No*, the key must not exist.

Registry Key Value: Determines if a registry key value exists on the device. The condition you use to set the requirement includes the key name, the value name, an operator, a value type, and a value data. The key and value names must identify the key value you want to check. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible value types are *INT_TYPE* and *STR_TYPE*. The possible value data is determined by the key, value name, and value type.

Registry Key and Value Exists: Determines if a registry key and value exists. After specifying the key name and value, the two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the specified key and value must exist to meet the requirement. If you select *No*, the key and value must not exist.

Service Exists: Determines if a service exists. After specifying the service name, the two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the service must exist to meet the requirement. If you select *No*, the service must not exist.

Specified Devices: Determines if the device is one of the specified devices. After specifying the devices, the two conditions you can use to set the requirement are *Yes* and *No*. If you select *Yes*, the device must be included in the specified devices list to meet the requirement (an inclusion list). If you select *No*, the device must not be included in the list (an exclusion list).

3.8.2 Filter Logic

You can use one or more filters to determine whether the policy should be applied to a device. A device must match the entire filter list (as determined by the logical operators that are explained below) for the policy to be applied to the device.

There is no technical limit to the number of filters you can use, but there are practical limits, such as:

- ♦ Designing a filter structure that is easy to understand
- ♦ Organizing the filters so that you do not create conflicting filters

Filters, Filter Sets, and Logical Operators

You can add filters individually or in sets. Logical operators, either *AND* or *OR*, are used to combine each filter and filter set. By default, filters are combined using *OR* (as determined by the *Combine Filters Using* field) and filter sets are combined using *AND*. You can change the default and use *AND* to combined filters, in which case filter sets are automatically combined using *OR*. In other words, the logical operator that is to combine individual filters (within in a set) must be the opposite of the operator that is used between filter sets.

You can easily view how these logical operators work. Click both the *Add Filter* and *Add Filter Set* options a few times each to create a few filter sets, then switch between *AND* and *OR* in the *Combine Filters Using* field and observe how the operators change.

As you construct filters and filter sets, you can think in terms of algebraic notation parentheticals, where filters are contained within parentheses, and sets are separated into a series of parenthetical groups. Logical operators (*AND* and *OR*) separate the filters within the parentheses, and the operators are used to separate the parentheticals.

For example, “(u AND v AND w) OR (x AND y AND z)” means “match either uvw or xyz.” In the filter list, this looks like:

```
u AND
v AND
w
OR
x AND
y AND
z
```

Nested Filters and Filter Sets

Filters and filter sets cannot be nested. You can only enter them in series, and the first filter or filter set to match the device is used. Therefore, the order in which they are listed does not matter. You are simply looking for a match to cause the policy to be applied to the device.

3.9 Disabling Policies

When you create a policy in ZENworks Configuration Management, the policy is enabled by default. Policies can be disabled by an administrator. If a policy is disabled, it is not considered for enforcement on any of the devices and users that it applies to.

To disable a policy:

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 Select the check box next to the policy (or policies) that you want to disable.
- 3 Click *Action > Disable Policies*.

In the Policies list, the status of *Enabled* for the policy (or policies) is changed to *No*.

When you disable a policy that has already been enforced for some managed devices and users, the policy is removed from those devices and it is not enforced for new devices and users.

3.10 Enabling the Disabled Policies

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 Select the check box next to the policy (or policies) that you want to enable.
- 3 Click *Action > Enable Policies*.

In the Policies list, the status of the *Enabled* column for the policy (or policies) is changed to *Yes*.

3.11 Copying a Policy to a Content Server

By default, a policy is copied to each content server. If you specify certain content servers as hosts, the policy is hosted on only those content servers; it is not copied to all content servers. You can also specify whether the selected policy is replicated to new content servers (ZENworks Servers and satellite servers) that are added to the Management Zone.

To specify a content server:

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 In the *Bundles* list, select the check box next to the policy (or policies).
- 3 Click *Action > Specify Content Server* to display the New Content Replication Rules page.

Wizard
Step 1: New Server Content Replication Rules

Choose whether you would like new servers added to the system, to replicate the content selected by this wizard.

WARNING: Any content replication relationships previously set between the content and servers selected by this wizard will be LOST.

For the selected content, please choose the default replication behavior for new servers added to the system:

New *Primary* Servers will:

☒ Include this content
☐ Exclude this content

New *Satellite* Servers will:

☒ Include this content
☐ Exclude this content

<< Back Next >> Cancel

- 4 Specify the default replication behavior for new servers added to the system:
 - ♦ **New Primary Servers Will:** Specify the default replication behavior for new ZENworks Primary Servers added to the system:
 - ♦ **Include This Content:** Replicates the content to any servers created in the future.
 - ♦ **Exclude This Content:** Excludes the content from being replicated to any servers created in the future.
 - ♦ **New Satellite Servers Will:** Specify the default replication behavior for new ZENworks satellite servers added to the system:
 - ♦ **Include This Content:** Replicates the content to any servers created in the future.
 - ♦ **Exclude This Content:** Excludes the content from being replicated to any servers created in the future.

Be aware that any content replication relationships previously set between the content and servers are lost upon completion of this wizard.

- 5 Click *Next* to display the Include or Exclude Primary Servers/Satellite Servers page:

Wizard
Step 2: Include or Exclude Primary Servers/Satellite Servers

Choose from the available Content Servers, all servers that should replicate the content selected by this wizard. Please note that the specified content will be removed from all servers not marked as included.

WARNING: Any content replication relationships previously set between the content and servers selected by this wizard will be LOST.

Excluded Primary Servers		Included Primary Servers
/Devices/Servers/krobinson2	>	
/Devices/Servers/Primary Server 1	<	
/Devices/Servers/Primary Server 2		

Excluded Satellite Servers		Included Satellite Servers
/Devices/Servers/Satellite Server 1	>	
/Devices/Servers/Satellite Server 2	<	
/Devices/Servers/DP 1		
/Devices/Servers/DP 2		

This page lets you specify on which content servers (ZENworks Servers and satellite servers) the content is hosted.

The relationships between content and content servers that you create using this wizard override any existing relationships. For example, if Policy A is currently hosted on Server 1 and Server 2 and you use this wizard to host it on Server 1 only, Policy A is excluded from Server 2 and is removed during the next scheduled replication.

5a In the *Excluded Primary Servers* or *Excluded Satellite Servers* list, select the desired content server.

You can use Shift+click and Ctrl+click to select multiple content servers.

You cannot include content on a satellite server without including it on the satellite server's parent ZENworks Server. You must select both the satellite server and its parent.

5b Click the Included Primary Servers or *Included Satellite Servers* list.

6 Click *Next* to display the *Finish* page, then review the information and, if necessary, use the *Back* button to make changes to the information.

7 Click *Finish* to create the relationships between the content and the content servers. Depending on the relationships created, the content is replicated to or removed from content servers during the next scheduled replication.

3.12 Incrementing the Policy Version

1 In ZENworks Control Center, click the *Policies* tab.

2 Select the check box next to the policy (or policies) for which you want to increment the version.

3 Click *Action > Increment Version*.


In the Policies list, the version number in the *Version* column for the policy (or policies) is incremented.

You should increment the version number whenever the policy is updated. This ensures that the latest policy is enforced on the managed device.

3.13 Reviewing the Status of the Policies at the Managed Device


The ZENworks Adaptive Agent applies policies that your administrator defines. Policies are rules that control a range of hardware and software configuration settings. For example, your administrator can create policies that control the Adaptive Agent features you can use, the bookmarks available in your browser, the printers you can access, and the security and system configuration settings for your.

You cannot change the policies applied by your administrator. Policies might be assigned to you or they might be assigned to your device. Policies assigned to you are referred to as user-assigned policies, and bundles assigned to your device are referred to as device-assigned policies

The ZENworks Adaptive Agent enforces your user-assigned policies only when you are logged in to your user directory (Microsoft* Active Directory* or Novell eDirectory™). If you are not logged in, you can log in through the ZENworks Configuration Management login screen. To do so, right-click the ZENworks icon  in the notification area, then click *Login*.

The Adaptive Agent always enforces the device-assigned policies regardless of whether or not you are logged in. Therefore, device-assigned policies are enforced for all users of the device.

To view the policies assigned to you and your device:

- 1 Double-click the ZENworks icon  in the notification area.
- 2 In the left navigation pane, click *Policies*.

3.14 Predefined Policy Reports

The Predefined Reports folder contains policy reports that are bundled with the product. This folder and its contents is accessible by all the administrators on the server. The administrators can schedule, view, and manage the historical instances of these reports only if they are assigned the Execute/Publish Report right. However, the administrators cannot modify, create or delete these reports.

For more information on the reports, see the “**Bundles and Policies Reports**” in the *ZENworks 10 Configuration Management System Reporting Reference*.

Managing Policy Groups

4

A policy group lets you group policies to ease administration and to provide easier assigning and scheduling of the policies in the policy group.

You can use ZENworks® Control Center or the zman command line utility to create policy groups. This section explains how to perform this task using the ZENworks Control Center. If you prefer the zman command line utility, see “[Policy Commands](#)” in the *ZENworks 10 Configuration Management Command Line Utilities Reference*.

- ♦ [Section 4.1, “Creating Policy Groups,” on page 51](#)
- ♦ [Section 4.2, “Renaming or Moving Policy Groups,” on page 52](#)
- ♦ [Section 4.3, “Copying a Policy Group’s System Requirements,” on page 52](#)
- ♦ [Section 4.4, “Deleting a Policy Group,” on page 53](#)
- ♦ [Section 4.5, “Assigning a Policy Group to Devices,” on page 53](#)
- ♦ [Section 4.6, “Assigning a Policy Group to Users,” on page 53](#)
- ♦ [Section 4.7, “Adding a Policy to a Group,” on page 54](#)

4.1 Creating Policy Groups

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 Click *New > Policy Group*.
- 3 Fill in the fields:

Group Name: Provide a name for the policy group. The name must be different than the name of any other item (policy, group, folder, and so forth) that resides in the same folder. The name you provide displays in ZENworks Control Center.

For more information, see “[Naming Conventions in ZENworks Control Center](#)” in *ZENworks 10 Configuration Management System Administration Reference*

Folder: Type the name or browse to and select the ZENworks Control Center folder where you want the policy to reside. The default is /policies, but you can create additional folders to organize your policies.

If you want to create the group in another folder, browse to and select the folder. By default, the group is created in the current folder.


Description: Provide a short description of the policy group's contents. This description displays in ZENworks Control Center.

- 4 Click *Next* to display the Add Group Members page, then specify policies to be members for the group.

You can add any number of policies to the group. You cannot add other policy groups to the group.

- 4a Click *Add* to display the Select Members dialog box.

Because you are adding policies to the group, the Select Members dialog box opens with the *Policies* folder displayed.

- 4b** Browse for and select the policies you want to add to the group. To do so:
 - 4b1** Click  next to a folder to navigate the folders until you find the policy you want to select.

If you know the name of the policy you are looking for, you can also use the *Item name* box to search for the bundle.
 - 4b2** Click the underlined link in the *Name* column to select the policy and display its name in the *Selected* list.
 - 4b3** (Optional) Repeat **Step 4a** and **Step 4b** to add additional policies to the *Selected* list.
 - 4b4** Click *OK* to add the selected policies to the group.
- 5** Click *Next* to display the Summary page, review the information and, if necessary, use the *Back* button to make changes to the information.
- 6** (Optional) Select the *Define Additional Properties* option to display the group's properties page after the group is created. You can then configure additional policy properties.
- 7** Click *Finish* to create the group.

Before the bundle group's contents are distributed to devices or users, you must continue with [Section 3.5, "Assigning a Policy to Devices," on page 40](#) or [Section 3.6, "Assigning a Policy to Users," on page 41](#).

4.2 Renaming or Moving Policy Groups

Use the *Edit* drop-down list on the Policies page to edit an existing object. To access the *Edit* drop-down list, you must select an object by clicking the check box next to the object's name in the list.

Depending on the type of object you select, you can rename, copy, or move the selected object. For example, if you select a policy object, you can rename, copy, and move the policy. If you select a Policy Group object, you can rename or move the policy group object, but not copy it. If the option is dimmed, that option is not available for the selected object type.

Some actions cannot be performed on multiple objects. For example, if more than one check box is selected, the *Rename* option is not available from the *Edit* menu.

- 1** In ZENworks Control Center, click the *Policies* tab.
- 2** In the *Policies* list, select the box next to the policy group's name, click *Edit*, then click an option:
 - Rename:** Click *Rename*, provide a new name for the policy group, then click *OK*.
 - Move:** Click *Move*, select a destination folder for the selected objects, then click *OK*.

4.3 Copying a Policy Group's System Requirements

- 1** In ZENworks Control Center, click the *Policies* tab.
- 2** In the *Policies* list, select the check box next to the policy group.
- 3** Click *Edit > Copy System Requirements*.

If more than one check box is selected, the *Copy System Requirements* option is not available on the *Edit* menu.


- 4 Select *Bundles* or *Policies*, then click *Add* to select the policies or bundles to which you want to copy the selected policy group's system requirements.

4.4 Deleting a Policy Group

Deleting a policy group does not delete its policies. It also does not uninstall the policies from devices where they have already been installed. To uninstall the policies from devices, you should use the *Uninstall* option for each policy before deleting the policy group.


- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 In the *Policies* list, select the check box next to the policy group (or policy groups).
- 3 Click *Delete*.

4.5 Assigning a Policy Group to Devices

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 In the *Policies* list, select the check box next to the policy group (or policy groups).
- 3 Click *Action > Assign to Device*.
- 4 Browse for and select the devices, device groups, and device folders to which you want to assign the group. To do so:
 - 4a Click  next to a folder (for example, the *Workstations* folder or *Servers* folder) to navigate through the folders until you find the device, group, or folder you want to select.

If you are looking for a specific item, such as a *Workstation* or a *Workstation Group*, you can use the *Items of type* list to limit the types of items that are displayed. If you know the name of the item you are looking for, you can use the *Item name* box to search for the item.
 - 4b Click the underlined link in the *Name* column to select the device, group, or folder and display its name in the *Selected* list box.
 - 4c Click *OK* to add the selected devices, folders, and groups to the *Devices* list.
- 5 Click *Next* to display the *Finish* page, review the information and, if necessary, use the *Back* button to make changes to the information.
- 6 Click *Finish*.

4.6 Assigning a Policy Group to Users

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 In the *Policies* list, select the check box next to the policy group (or policy groups).
- 3 Click *Action > Assign to User*.
- 4 Browse for and select the user, user groups, and user folders to which you want to assign the group. To do so:
 - 4a Click  next to a folder to navigate through the folders until you find the user, group, or folder you want to select.

If you are looking for a specific item, such as a User or a User Group, you can use the *Items of type* list to limit the types of items that are displayed. If you know the name of the item you are looking for, you can use the *Item name* box to search for the item.

- 4b** Click the underlined link in the *Name* column to select the user, group, or folder and display its name in the *Selected* list box.
- 4c** Click *OK* to add the selected devices, folders, and groups to the *Users* list.
- 5** Click *Next* to display the Finish page, review the information and, if necessary, use the *Back* button to make changes to the information.
- 6** Click *Finish*.

4.7 Adding a Policy to a Group

For more information, see [Section 3.4, “Adding Policies to Existing Groups,” on page 39](#).

Managing Folders

5

A folder is an organizational object. You can use folders to structure your policies and policy groups into a manageable hierarchy for your ZENworks® system. For example, you might want a folder for each type of policy (Browser Bookmarks policy, Dynamic Local User policy, and so forth), or, if applications are department-specific, you might want a folder for each department (Accounting Department folder, Payroll Department folder, and so forth).

The following sections contain additional information:

- ♦ [Section 5.1, “Creating Folders,” on page 55](#)
- ♦ [Section 5.2, “Renaming or Moving Folders,” on page 55](#)
- ♦ [Section 5.3, “Copying a Folder’s System Requirements,” on page 56](#)
- ♦ [Section 5.4, “Deleting a Folder,” on page 56](#)

5.1 Creating Folders

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 Click *New > Folder*.
- 3 Provide a unique name for your folder. This is a required field.

When you name an object in ZENworks Control Center (folders, policies, policy groups, and so forth), ensure that the name adheres to the naming conventions; not all characters are supported. For more information on naming conventions, see [“Naming Conventions in ZENworks Control Center”](#) in *ZENworks 10 Configuration Management System Administration Reference*.

- 4 Type the name or browse to and select the folder that contains this folder in the ZENworks Control Center interface. This is a required field.
- 5 Provide a short description of the folder's contents.
- 6 Click *OK*.

5.2 Renaming or Moving Folders

Use the *Edit* drop-down list on the Policies page to edit an existing object. To access the *Edit* drop-down list, you must select an object by clicking the check box next to the object's name in the list.

Depending on the type of object you select, you can rename, copy, or move the selected object. For example, if you select a Policy object, you can rename, copy, and move the policy. If you select a Folder object, you can rename or move the Folder object, but not copy it. If the option is dimmed, that option is not available for the selected object type.

Some actions cannot be performed on multiple objects. For example, if more than one check box is selected, the *Rename* option is not available from the *Edit* menu.

- 1 In ZENworks Control Center, click the *Policies* tab.

- 2 In the *Policies* list, select the box next to the folder's name, then click *Edit*.
- 3 Select an option:
 - ♦ **Rename:** Click *Rename*, provide a new name for the folder, then click *OK*.
 - ♦ **Move:** Click *Move*, choose a destination folder for the selected objects, then click *OK*.

5.3 Copying a Folder's System Requirements

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 In the *Policies* list, select the check box next to the folder.
- 3 Click *Edit > Copy System Requirements*.

If more than one check box is selected, the *Copy System Requirements* option is not available on the *Edit* menu.
- 4 Select *Policies*, then click *Add* to select the policies to which you want to copy the selected policy's system requirements.

5.4 Deleting a Folder

Deleting a folder also deletes all of its contents (policies, policy groups, and subfolders).

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 In the *Policies* list, select the check box next to the folder (or folders).
- 3 Click *Delete*.

Troubleshooting Policy Management

A

The following sections contain detailed explanations of the error messages or problems you might encounter when using the Novell® ZENworks® 10 Configuration Management policies.

- ♦ Section A.1, “Browser Bookmarks Policy Error Messages,” on page 57
- ♦ Section A.2, “Dynamic Local User Policy Error Messages,” on page 58
- ♦ Section A.3, “General Policy Troubleshooting Scenarios,” on page 59
- ♦ Section A.4, “Local File Rights Policy Error Messages,” on page 60
- ♦ Section A.5, “Printer Policy Error Messages,” on page 61
- ♦ Section A.6, “Printer Policy Troubleshooting Strategies,” on page 64
- ♦ Section A.7, “Roaming Profile Policy Errors,” on page 65
- ♦ Section A.8, “SNMP Policy Errors,” on page 65
- ♦ Section A.9, “Windows Group Policy Errors,” on page 66
- ♦ Section A.10, “ZENworks Explorer Configuration Policy Errors,” on page 69
- ♦ Section A.11, “Dynamic Local User Policy Troubleshooting Strategies,” on page 71
- ♦ Section A.12, “Windows Group Policy Troubleshooting Strategies,” on page 72

A.1 Browser Bookmarks Policy Error Messages

- ♦ “The folder cannot be created to add bookmark as Internet Explorer does not allow such folder” on page 57
- ♦ “The bookmark cannot be created as the bookmark name is not proper. Internet Explorer does not allow such bookmarks” on page 58
- ♦ “Unable to apply the Browser Bookmark Policy. For more information, see the ZENworks error message online documentation at <http://www.novell.com/documentation>” on page 58
- ♦ “On a managed device, empty folders cannot be created in a user’s favorites folder” on page 58
- ♦ “The Browser Bookmarks policy fails on a Windows Vista managed device” on page 58

The folder cannot be created to add bookmark as Internet Explorer does not allow such folder

Source: ZENworks 10 Configuration Management; Policy Management; Browser Bookmarks Policy.

Possible Cause: On Windows managed devices, Internet Explorer does not allow a bookmark folder name with special characters such as ! , * , / , or \\.

Action: When creating the policy, ensure that special characters such as ! , * , / , or \\. are not used in the bookmark folder name.

The bookmark cannot be created as the bookmark name is not proper. Internet Explorer does not allow such bookmarks

Source: ZENworks 10 Configuration Management; Policy Management; Browser Bookmarks Policy.

Possible Cause: On Windows managed devices, the Internet Explorer does not allow a bookmark name with special characters such as ! , * , / , or \.

Action: When creating the policy, ensure that special characters such as ! , * , / , or \ are not used in the bookmark name.

Unable to apply the Browser Bookmark Policy. For more information, see the ZENworks error message online documentation at <http://www.novell.com/documentation>

Source: ZENworks 10 Configuration Management; Policy Management; Browser Bookmarks Policy.

Action: Ensure that the Browser Bookmark policy has been correctly created. For more information, see [Section 2.1, “Browser Bookmarks Policy,” on page 13](#).

Action: If the problem persists, contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

On a managed device, empty folders cannot be created in a user’s favorites folder

Source: ZENworks 10 Configuration Management; Policy Management; Browser Bookmarks Policy.

Action: None.

The Browser Bookmarks policy fails on a Windows Vista managed device

Source: ZENworks 10 Configuration Management; Policy Management; Browser Bookmarks Policy.

Explanation: If you assign a Browser Bookmarks policy to a Windows Vista managed device, the following error is displayed:

The Favorites folder for the user was not found to operate on.

Action: Refresh the managed device.

A.2 Dynamic Local User Policy Error Messages

- ♦ “The policy *policy_name* was failed in include/exclude list calculation” on page 58
- ♦ “There was an error while applying settings for the group *group_name*” on page 59
- ♦ “There was an error while applying settings for the file *filename*” on page 59
- ♦ “Unable to enforce the *policy_name* policy because the policy data is empty” on page 59

The policy *policy_name* was failed in include/exclude list calculation

Source: ZENworks 10 Configuration Management; Policy Management; Dynamic Local User Policy.

- Explanation: This error occurs if the Include/Excluded workstation or the user list is configured, and the workstation or user did not qualify.
- Action: Remove the user or device from the Excluded list configured in the policy and increment the version of the policy to enforce the policy updates to the managed device.

There was an error while applying settings for the group *group_name*

- Source: ZENworks 10 Configuration Management; Policy Management; Dynamic Local User Policy.
- Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the *ZENworks 10 Configuration Management Message Logging Reference*.
- Action: If the problem persists, contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

There was an error while applying settings for the file *filename*

- Source: ZENworks 10 Configuration Management; Policy Management; Dynamic Local User Policy.
- Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the *ZENworks 10 Configuration Management Message Logging Reference*.
- Action: If the problem persists, contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

Unable to enforce the *policy_name* policy because the policy data is empty

- Source: ZENworks 10 Configuration Management; Policy Management; Dynamic Local User Policy.
- Possible Cause: The ZENworks Adaptive Agent did not receive any data to be configured on the managed device.
- Action: Review the policy content in ZENworks Control Center. For more information about the Dynamic Local User Policy, see *Section 2.2, “Dynamic Local User Policy,”* on page 14.

A.3 General Policy Troubleshooting Scenarios

- ♦ “The user is prompted to log in again immediately after logging in to ZENworks by using ZENworks icon” on page 60
- ♦ “Unable to view the newly added user source in all the other concurrent sessions of ZENworks Control Center” on page 60
- ♦ “The Wake-on-LAN policy is not available in ZENworks Configuration Management” on page 60

The user is prompted to log in again immediately after logging in to ZENworks by using ZENworks icon

Source: ZENworks 10 Configuration Management; Policy Management.

Explanation: If the following conditions are met, a ZENworks user is prompted to log in again immediately after logging in to the device, in spite of providing the right credentials:

- ♦ The user has logged in to a device where another ZENworks user has logged in and logged out within 5 to 10 mins of the desktop login.
- ♦ The Dynamic Local User policy or the Windows Group policy that is assigned to the user has the *After enforcement, force a re-login on the managed device, if necessary* option selected.

Action: Edit the policy to deselect *After enforcement, force a re-login on the managed device, if necessary*.

Unable to view the newly added user source in all the other concurrent sessions of ZENworks Control Center

Source: ZENworks 10 Configuration Management; Policy Management.

Explanation: If ZENworks Control Center is opened by more than one user at the same time and a new user source is added to the management zone by one of the users, the newly added user source is not reflected in the other open sessions of ZENworks Control Center. Consequently, the policies might not be assigned to the new user source.

Action: To assign policies to the new user source, log in to ZENworks Control Center again.

The Wake-on-LAN policy is not available in ZENworks Configuration Management

Source: ZENworks 10 Configuration Management; Policy Management.

Action: Perform the following steps to create the functionality of the Wake-on-LAN policy:

1. In ZENworks Control Center, create an empty bundle without any actions.
2. Select the bundle and click *Action > Assign Bundle to Device*, then click *Next*.
3. Select the *Distribution Schedule* option, then click *Next*.
4. Select the *Wake-on-LAN* option, then click *Next*.
5. Click *Finish*.

A.4 Local File Rights Policy Error Messages

- ♦ “The file/folder filename or folder_name was not found while enforcing policy policy_name” on page 61
- ♦ “There was an error while unenforcing the policy” on page 61
- ♦ “There was an error while applying the policy policy_name” on page 61

The file/folder *filename* or *folder_name* was not found while enforcing policy *policy_name*

Source: ZENworks 10 Configuration Management; Policy Management; Local File Rights Policy.

Possible Cause: This occurs when a file or folder configured in the policy is not found on the managed device.

Action: Do the following:

- 1 Verify whether the file or folder exists on the managed device and the name and path are correct.
- 2 Ensure that Windows Explorer is configured to display extensions for a file of a known type. In Windows Explorer, click *Tools > Folder Options* to display the Folder Options dialog box. Click the *View* tab, then ensure that the *Hide Extension for known file types* option is not selected.

There was an error while unenforcing the policy

Source: ZENworks 10 Configuration Management; Policy Management; Local File Rights Policy.

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the *ZENworks 10 Configuration Management Message Logging Reference*.

Action: If the problem persists, contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

There was an error while applying the policy *policy_name*

Source: ZENworks 10 Configuration Management; Policy Management; Local File Rights Policy.

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the *ZENworks 10 Configuration Management Message Logging Reference*.

Action: If the problem persists, contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

A.5 Printer Policy Error Messages

- ♦ “Printer driver installation failed for *printer_name*. The provided driver install file type is not supported” on page 62
- ♦ “Printer driver installation failed for *printer_name*. File extraction failed for *filename*” on page 62
- ♦ “Printer driver installation failed for *printer_name*. Check if provided drivers inf file is in proper format” on page 62
- ♦ “Unable to get iprint install file from the specified location in managed device, please check if file is there in specified location” on page 62

- ♦ “Unable to extract iprint client installer from the content” on page 63
- ♦ “Bad iprint install file. Unable to extract setupipp.exe file. Expectation is for a zip file which extracts setupipp.exe on the root. check the file mentioned for install” on page 63
- ♦ “iPrint client install failed. Check if the provided iprint client supports silent install” on page 63
- ♦ “Failed to add smb printer printer_name” on page 63
- ♦ “Failed to add iprint printer printer_name” on page 63

Printer driver installation failed for *printer_name*. The provided driver install file type is not supported

Source: ZENworks 10 Configuration Management; Policy Management; Printer Policy.

Possible Cause: The Printer policy supports only `.inf` drivers.

Action: A `.inf` type driver along with all the dependent files can be zipped or tarred and uploaded using the policy. If you have a self-extracting `exe`, extract it to a temporary location, compress it into a `.zip` file, then distribute it through the policy.

Printer driver installation failed for *printer_name*. File extraction failed for *filename*

Source: ZENworks 10 Configuration Management; Policy Management; Printer Policy.

Possible Cause: The policy cannot extract the zipped or tarred files for the driver because the file might be corrupted.

Action: Ensure that the files are not corrupted by manually extracting the `.tar` or `.zip` file, then include the `.tar` or `.zip` file in the policy.

Printer driver installation failed for *printer_name*. Check if provided drivers inf file is in proper format

Source: ZENworks 10 Configuration Management; Policy Management; Printer Policy.

Possible Cause: This error message can occur if the driver `.inf` file is not in proper format, or the `.inf` file does not contain installation instructions for the driver’s model name.

Action: Extract the driver files and verify whether the driver’s model name provided in the Printer policy is contained in the `.inf` file. The model name must exactly match the name contained in the file.

Unable to get iprint install file from the specified location in managed device, please check if file is there in specified location

Source: ZENworks 10 Configuration Management; Policy Management; Printer Policy.

Possible Cause: The iPrint installer is not found on the managed device. This error message can occur if the location of the file is not correctly specified in the Printer policy, or the file resides in a shared network location and is not available to the Printer policy handler module.

Action: Ensure that the file exists on the managed device or it is directly associated to the Printer policy.

Unable to extract iprint client installer from the content

Source: ZENworks 10 Configuration Management; Policy Management; Printer Policy.

Possible Cause: The iPrint client attached with the Printer policy is not available on the managed device. This error message can occur if the policy is enforced immediately after it's created.

Action: After creating the policy, wait for five to ten minutes before enforcing the policy, then try to log into the managed device.

Bad iprint install file. Unable to extract setupipp.exe file. Expectation is for a zip file which extracts setupipp.exe on the root. check the file mentioned for install

Source: ZENworks 10 Configuration Management; Policy Management; Printer Policy.

Possible Cause: The Printer policy supports iPrint installation only in silent mode and does not require user intervention. Hence, `nipp-s.exe` or `nipp.zip` can be used, but not `nipp.exe`.

Action: If `nipp.zip` is used for installation, extract it to verify whether the installation file is correct and the extracted files contain `setupipp.exe`.

iPrint client install failed. Check if the provided iprint client supports silent install

Source: ZENworks 10 Configuration Management; Policy Management; Printer Policy.

Possible Cause: The Printer policy supports iPrint installation only in silent mode and does not require a user intervention. Hence, `nipp-s.exe` or `nipp.zip` can be used, but not `nipp.exe`.

Action: If `nipp.zip` is used for installation, extract it to verify whether the installation file is correct and the extracted files contain `setupipp.exe`.

Failed to add smb printer *printer_name*

Source: ZENworks 10 Configuration Management; Policy Management; Printer Policy.

Possible Cause: The SMB printer connection is not valid.

Action: Ensure that there is no problem in the network by using the UNC path to add the printer through the Windows Add Wizard.

Failed to add iprint printer *printer_name*

Source: ZENworks 10 Configuration Management; Policy Management; Printer Policy.

Action: Verify whether the iPrint URL is correct. The iPrint URL must be specified in the format `ipp://server-address/ipp/printer name`.

Also, check if the iPrint client is installed on the target device. If the client is not installed, attach it through the Printer policy.

A.6 Printer Policy Troubleshooting Strategies

- ♦ “Unable to install a printer driver on Windows managed devices through the Printer Policy” on page 64
- ♦ “Unable to install the printer driver on a Windows Vista SP1 device” on page 64
- ♦ “Changing the iPrint printer driver on a server does not update the driver on the managed device” on page 64
- ♦ “Unable to install or update the printer drivers on re-enforcing the policy” on page 65

Unable to install a printer driver on Windows managed devices through the Printer Policy

Source: ZENworks 10 Configuration Management; Policy Management; Printer Policy.

Possible Cause: A printer model name is represented in different ways on Windows managed devices. For example, the HP LaserJet 8100 Series PCL6 printer model is represented as HP LaserJet 8100 Series PCL 6 on Windows 2000. (Note that there is a space between PCL and 6).

While creating a Printer policy, you can manually specify the printer model or select it from a predefined list. If you select it from a predefined list, the printer is installed based on the model name defined in the list, which might not be the printer model name on the Windows managed device. For example, if you select HP LaserJet 8100 Series PCL6, the printer driver is installed only on the managed devices having the HP LaserJet 8100 Series PCL6 printer model. Consequently, the driver is not installed on the Windows 2000 managed device.

Action: While creating the Printer policy, ensure that the correct printer model name is specified.

Unable to install the printer driver on a Windows Vista SP1 device

Source: ZENworks 10 Configuration Management; Policy Management; Printer Policy.

Explanation: If the printer driver contains more than one `.inf` file, the installation of the driver fails because the policy handler does not know which `.inf` file to use.

Action: While installing the printer driver, ensure that only the valid `.inf` file is available in the ZIP file. For example, if you download the HP 4700 Color LaserJet print drivers for Vista, the ZIP file contains more than one `.inf` file. Remove all the `.inf` files other than `hpc4700c.inf` because this is the only `.inf` file required to install the HP 4700 Color LaserJet print driver.

Changing the iPrint printer driver on a server does not update the driver on the managed device

Source: ZENworks 10 Configuration Management; Policy Management; Printer Policy.

Explanation: If you update the iPrint printer driver on a server through a console such as iManager, the driver is not updated on the managed device.

Action: After updating the iPrint driver in iManager, perform the following steps to update the driver on the device:

- 1 In ZENworks Control Center, click *Policies*.
- 2 Select the policy, then click *Action > Disable Policies* to disable the policy.
- 3 Click *Quick Tasks > Refresh All Devices*.
- 4 Click *Action > Enable Policies* to enable the policy.
- 5 Click *Quick Tasks > Refresh All Devices*.

Unable to install or update the printer drivers on re-enforcing the policy

Source: ZENworks 10 Configuration Management; Policy Management; Printer Policy.

Explanation: The Printer policy installs the printer driver during the first enforcement of the policy. If the driver is changed after the first enforcement of the policy, the new drivers are not installed or updated on the subsequent enforcement of the policy.

Action: Create a new printer policy with the new driver and assign it to the same device or user.

A.7 Roaming Profile Policy Errors

- ♦ “The policy *policy_name* could not be successfully enforced as policy data was empty” on page 65

The policy *policy_name* could not be successfully enforced as policy data was empty

Source: ZENworks 10 Configuration Management; Policy Management; Roaming Profile Policy.

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the *ZENworks 10 Configuration Management Message Logging Reference*.

Action: If the problem persists, contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

A.8 SNMP Policy Errors

- ♦ “The policy *policy_name* could not be successfully enforced due to an error” on page 66
- ♦ “The policy *policy_name* could not be successfully enforced as policy data was empty” on page 66

The policy *policy_name* could not be successfully enforced due to an error

Source: ZENworks 10 Configuration Management; Policy Management; SNMP Policy.

Possible Cause: An internal error was occurred while configuring the policy.

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the *ZENworks 10 Configuration Management Message Logging Reference*.

Action: If the problem persists, contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

The policy *policy_name* could not be successfully enforced as policy data was empty

Source: ZENworks 10 Configuration Management; Policy Management; SNMP Policy.

Possible Cause: The agent did not receive the data to be configured on the managed device.

Action: Review the policy content in ZENworks Control Center.

A.9 Windows Group Policy Errors

- ♦ “There was an error while enforcing the policy *policy_name*. Please refer the managed device log for details” on page 66
- ♦ “The policy *policy_name* was not applied” on page 67
- ♦ “The security settings in policy *policyname* were not applied” on page 67
- ♦ “The Windows Hotfix “KB897327” required for exporting and applying Group policy security settings on Windows XP was not found. Computer configuration security settings could not be exported/applied” on page 67
- ♦ “There was an error while unenforcing Group policy settings” on page 67
- ♦ “There was an error while cleaning up Group policy settings at logout for user *username*” on page 68
- ♦ “There was an error while accessing content for policy *policy_name*.” on page 68
- ♦ “Some security settings could not be configured” on page 68
- ♦ “To operate on security settings, Windows XP Hotfix KB897327 is required” on page 68
- ♦ “Failure importing group policy settings” on page 68

There was an error while enforcing the policy *policy_name*. Please refer the managed device log for details

Source: ZENworks 10 Configuration Management; Policy Management; Windows Group Policy.

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the *ZENworks 10 Configuration Management Message Logging Reference*.

Action: If the problem persists, contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

The policy *policy_name* was not applied

Source: ZENworks 10 Configuration Management; Policy Management; Windows Group Policy.

Action: Ensure that the managed device meets the ZENworks Configuration Management requirements. For more information about the managed device system requirements, see the *ZENworks 10 Configuration Management Installation Guide*.

The security settings in policy *policyname* were not applied

Source: ZENworks 10 Configuration Management; Policy Management; Windows Group Policy.

Possible Cause: The security settings are not applied if a local group policy is created on a higher version of Windows but applied to a managed device that is running a lower version of Windows.

Action: Ensure that the ZENworks server and the managed device meet the ZENworks Configuration Management requirements. For more information about the managed device system requirements, see the *ZENworks 10 Configuration Management Installation Guide*.

The Windows Hotfix "KB897327" required for exporting and applying Group policy security settings on Windows XP was not found. Computer configuration security settings could not be exported/applied

Source: ZENworks 10 Configuration Management; Policy Management; Windows Group Policy.

Possible Cause: This message is logged if the Hotfix KB897327 is not applied on Windows XP devices before the policy is applied. The Hotfix is required for security settings to be configured on the managed device.

Action: Install Windows Hotfix KB897327 on the Windows XP managed device from the [Microsoft Support Web site \(http://support.microsoft.com/KB/897327\)](http://support.microsoft.com/KB/897327).

There was an error while unenforcing Group policy settings

Source: ZENworks 10 Configuration Management; Policy Management; Windows Group Policy.

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the *ZENworks 10 Configuration Management Message Logging Reference*.

Action: If the problem persists, contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

There was an error while cleaning up Group policy settings at logout for user *username*

- Source: ZENworks 10 Configuration Management; Policy Management; Windows Group Policy.
- Action: Turn on debug logging on the managed device and refer the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see *ZENworks 10 Configuration Management Message Logging Reference*.
- Action: If the problem persists, contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

There was an error while accessing content for policy *policy_name*.

- Source: ZENworks 10 Configuration Management; Policy Management; Windows Group Policy.
- Possible Cause: The error occurs if the managed device is immediately refreshed after the policy was created and assigned. Hence, the content for the policy might have not been completely processed at the server.
- Action: Wait for five minutes and refresh the managed device.

Some security settings could not be configured

- Source: ZENworks 10 Configuration Management; Policy Management; Windows Group Policy.
- Possible Cause: This message is logged if some of the security settings of a policy are not applied on the managed device.
- Action: Contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

To operate on security settings, Windows XP Hotfix KB897327 is required

- Source: ZENworks 10 Configuration Management; Policy Management; Windows Group Policy.
- Explanation: The error message might occur while creating or editing group policies for Windows XP managed devices.
- Possible Cause: The Windows Hotfix KB897327 is not installed on the Windows XP managed device.
- Action: Ignore the error message if you are not configuring security settings in the Windows Group Policy.
- Action: Install Windows Hotfix KB897327 on the Windows XP managed device from the [Microsoft Support Web site \(http://support.microsoft.com/KB/897327\)](http://support.microsoft.com/KB/897327).

Failure importing group policy settings

- Source: ZENworks 10 Configuration Management; Policy Management; Windows Group Policy.
- Explanation: When `gpedit.msc` is closed, the GPHelper displays the error message with the ID `POLICYHANDLERS.WinGPPolicy.ExportFailure`.

Possible Cause: The Windows Hotfix KB897327 is not installed on the Windows XP managed device.

Action: Ignore the error message if you are not configuring security settings in the Windows Group policy.

Action: Install Windows Hotfix KB897327 on the Windows XP managed device from the [Microsoft Support Web site \(http://support.microsoft.com/KB/897327\)](http://support.microsoft.com/KB/897327).

A.10 ZENworks Explorer Configuration Policy Errors

- ♦ “There was an error while unenforcing the policy” on page 69
- ♦ “There was an error while enforcing the policy *policy_name*. Please refer the managed device log for details” on page 69
- ♦ “There was an error while setting the desktop icon name” on page 70
- ♦ “The policy *policy_name* could not be successfully enforced as policy data was empty” on page 70
- ♦ “There was an error while configuring the setting “Enable manual refresh”” on page 70
- ♦ “There was an error while configuring the setting “Enable folder view”” on page 70
- ♦ “There was an error while configuring the setting “Expand the entire folder tree”” on page 71
- ♦ “There was an error while configuring the setting “Display applications in windows explorer”” on page 71
- ♦ “There was an error while configuring the setting “Allow logout/login as new user”” on page 71

There was an error while unenforcing the policy

Source: ZENworks 10 Configuration Management; Policy Management; ZENworks Explorer Configuration Policy.

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the *ZENworks 10 Configuration Management Message Logging Reference*.

Action: If the problem persists, contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

There was an error while enforcing the policy *policy_name*. Please refer the managed device log for details

Source: ZENworks 10 Configuration Management; Policy Management; ZENworks Explorer Configuration Policy.

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the *ZENworks 10 Configuration Management Message Logging Reference*.

Action: If the problem persists, contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

There was an error while setting the desktop icon name

Source: ZENworks 10 Configuration Management; Policy Management; ZENworks Explorer Configuration Policy.

Possible Cause: This message is logged if an error occurred while configuring the Desktop icon of ZENworks Application Launcher.

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the *ZENworks 10 Configuration Management Message Logging Reference*.

Action: If the problem persists, contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

The policy `policy_name` could not be successfully enforced as policy data was empty

Source: ZENworks 10 Configuration Management; Policy Management; ZENworks Explorer Configuration Policy.

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the *ZENworks 10 Configuration Management Message Logging Reference*.

Action: If the problem persists, contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

There was an error while configuring the setting "Enable manual refresh"

Source: ZENworks 10 Configuration Management; Policy Management; ZENworks Explorer Configuration Policy.

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the *ZENworks 10 Configuration Management Message Logging Reference*.

Action: If the problem persists, contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

There was an error while configuring the setting "Enable folder view"

Source: ZENworks 10 Configuration Management; Policy Management; ZENworks Explorer Configuration Policy.

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the *ZENworks 10 Configuration Management Message Logging Reference*.

Action: If the problem persists, contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

There was an error while configuring the setting "Expand the entire folder tree"

Source: ZENworks 10 Configuration Management; Policy Management; ZENworks Explorer Configuration Policy.

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the *ZENworks 10 Configuration Management Message Logging Reference*.

Action: If the problem persists, contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

There was an error while configuring the setting "Display applications in windows explorer"

Source: ZENworks 10 Configuration Management; Policy Management; ZENworks Explorer Configuration Policy.

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the *ZENworks 10 Configuration Management Message Logging Reference*.

Action: If the problem persists, contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

There was an error while configuring the setting "Allow logout/login as new user"

Source: ZENworks 10 Configuration Management; Policy Management; ZENworks Explorer Configuration Policy.

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the *ZENworks 10 Configuration Management Message Logging Reference*.

Action: If the problem persists, contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

A.11 Dynamic Local User Policy Troubleshooting Strategies

- ♦ "Unable to update the group membership of the user on the managed device" on page 71
- ♦ "Dynamic Local User is unable to log on to the managed device" on page 72

Unable to update the group membership of the user on the managed device

Source: ZENworks 10 Configuration Management; Policy Management; Dynamic Local User Policy.

Explanation: On the managed device, the group membership of the user is not updated according to the User Configurations settings of the Dynamic Local User policy.

Possible Cause: The *DontUpdateGroupMemberships* registry key is set to 1

Action: On the managed device, set the registry key
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\NWGINA\Dynamic
Local User\DontUpdateGroupMemberships to 0.

Dynamic Local User is unable to log on to the managed device

Source: ZENworks 10 Configuration Management; Policy Management; Dynamic Local User Policy.

Explanation: If the password of the Dynamic Local User in the user source does not meet the password complexity requirements, the user fails to log on to the managed device.

Possible Cause: *Password must meet complexity requirements* is enabled in the password policy setting of the Group policy of the device (*Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy*).

Action: Do one of the following:

- ♦ Ensure that the password specified for the user in the user source meets the password complexity requirements. For information on the password complexity requirements, double-click *Password must meet complexity requirements* in the password policy setting of the Group policy (*Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy*).
- ♦ Disable the *Password must meet complexity requirements* setting on the managed device.

A.12 Windows Group Policy Troubleshooting Strategies

- ♦ “The Group Policy Helper tool is not backward compatible with the earlier versions of ZENworks Configuration Management releases” on page 73
- ♦ “Favorites configured by using the Group policy are not cleared when the group policy is unenforced” on page 73
- ♦ “Internet Explorer Settings configured in the Group policy are not applied on Internet Explorer 7 or later” on page 73
- ♦ “Security settings of the Windows Group policy are not effective on the device” on page 73
- ♦ “The Security settings configured in the Windows Group policy are not applied on a Windows XP managed device” on page 74
- ♦ “Unable to install the Group policy Helper tool on a 64-bit Windows device by using the Internet Explorer browser.” on page 74
- ♦ “Unable to launch the Group Policy Helper tool on a Windows Vista device” on page 74

- ♦ “Policy Enforcement status is not properly displayed” on page 74
- ♦ “Unable to export Group Policy content” on page 75
- ♦ “Unable to view the 64 bit snap-ins in the Group Policy Helper tool” on page 75

The Group Policy Helper tool is not backward compatible with the earlier versions of ZENworks Configuration Management releases

Source: ZENworks 10 Configuration Management; Policy Management; Windows Group Policy.

Action: Install the version of the Group Policy Helper tool available with the corresponding ZENworks Configuration Management release.

Favorites configured by using the Group policy are not cleared when the group policy is unenforced

Source: ZENworks 10 Configuration Management; Policy Management; Windows Group Policy.

Explanation: If you use the *Internet Explorer Maintenance* settings of the Group policy to configure favorites, the favorites are not cleared when the Group policy is unenforced.

Action: Use the Browser Bookmark policy to configure the favorites.

Internet Explorer Settings configured in the Group policy are not applied on Internet Explorer 7 or later

Source: ZENworks 10 Configuration Management; Policy Management; Windows Group Policy.

Explanation: On launching the Internet Explorer browser, the [runonce \(http://runonce.msn.com/runonce2.aspx\)](http://runonce.msn.com/runonce2.aspx) page is displayed instead of the home page configured in the Group policy.

Action: On the [runonce \(http://runonce.msn.com/runonce2.aspx\)](http://runonce.msn.com/runonce2.aspx) page, follow the on-screen prompts to configure the settings.

Security settings of the Windows Group policy are not effective on the device

Source: ZENworks 10 Configuration Management; Policy Management; Windows Group Policy.

Explanation: If the security settings are not configured in the Windows Group policy, the policy uses the default security settings of the device on which it was created. When more than one Windows Group policy is applied to a device, the security settings of the last applied policy are effective on the device.

Action: If you assign multiple policies to a device, ensure that the policy whose security settings you want to be effective on the device is applied last on the device.

The Security settings configured in the Windows Group policy are not applied on a Windows XP managed device

Source: ZENworks 10 Configuration Management; Policy Management; Windows Group Policy.

Action: On the Windows XP managed device, install Windows Hotfix KB897327 from the [Microsoft Support Web site \(http://support.microsoft.com/KB/897327\)](http://support.microsoft.com/KB/897327).

Unable to install the Group policy Helper tool on a 64-bit Windows device by using the Internet Explorer browser.

Source: ZENworks 10 Configuration Management; Policy Management; Windows Group Policy.

Explanation: If you use the Internet Explorer browser on a 64-bit Windows device, the Group policy Helper tool cannot be installed by clicking the *Install Group Policy Helper* link.

Action: Save the `novell-zenworks-grouppolicyhelper-10.1.x.x.msi` package to your local device, then double-click the MSI to install the package.

Unable to launch the Group Policy Helper tool on a Windows Vista device

Source: ZENworks 10 Configuration Management; Policy Management; Windows Group Policy.

Explanation: The Group Policy Helper tool does not launch on a Windows Vista device if the User Account Control (*Start > Settings > Control Panel > User Accounts*) is enabled and Mozilla Firefox 2.0.0.8 or later is installed.

Action: Configure Firefox to run with administrator credentials.

- ♦ To configure Firefox for a session, right-click the Firefox shortcut icon on the desktop, then select *Run as administrator*.
- ♦ To configure Firefox permanently:
 1. On the desktop, right-click the Firefox shortcut icon and select *Properties*. Click the *Shortcut* tab, then click the *Advanced* button. In the Advanced Properties dialog box, select *Run as administrator*.
or
In Windows Explorer, navigate to the Firefox executable file, right-click the file, then select *Properties*. Click the *Compatibility* tab, then select *Run this program as an administrator*.
 2. Restart the browser

Policy Enforcement status is not properly displayed

Source: ZENworks 10 Configuration Management; Policy Management; Windows Group Policy.

Explanation: If you assign more than one policy to a user or a device, the policy enforcement status is not properly displayed. The consolidated status of a Group policy is displayed in the ZENworks icon only for the last enforced

policy. That is, if any of the Group policies fail, the last effective policy is displayed in the ZENworks icon as *Failed* and rest of the policies are displayed as *Success*.

Possible Cause: The consolidated settings are applied only for the last policy.

Action: None.

Unable to export Group Policy content

Source: ZENworks 10 Configuration Management; Policy Management; Windows Group Policy.

Explanation: If you use the `zman` command to export a policy with content, the content (.zip file) is not exported.

Action: Perform the following steps:

1. In ZENworks Control Center, edit the policy you want to export.
2. Click *Upload* to upload the policy settings to the content server.
3. The Upload Confirm dialog box displays the name of the .zip file that stores the policy settings. Copy the .zip file to the required location, such as `c:\`.
4. Run the `zman petf` command to export the policy to an XML file, such as `export.xml`.
For example, `zman petf \policies c:\export.xml`.
5. Edit the `export_actioncontentinfo.xml` file to update the path of the .zip file.

Unable to view the 64 bit snap-ins in the Group Policy Helper tool

Source: ZENworks 10 Configuration Management; Policy Management; Windows Group Policy.

Explanation: While creating or editing the Group policy in ZENworks Control Center, you cannot view the 64-bit snap-ins in the Group Policy Helper tool because the 32-bit version of the Group Policy Helper tool is launched by default.

Action: None.

Best Practices

B

The following sections contain information on the best practices to follow when using the Novell® ZENworks® 10 Configuration Management policies:

- ♦ [Section B.1, “Local File Rights Policy,” on page 77](#)
- ♦ [Section B.2, “Dynamic Local User Policy,” on page 77](#)
- ♦ [Section B.3, “Roaming Profile Policy,” on page 77](#)
- ♦ [Section B.4, “SNMP Policy,” on page 77](#)
- ♦ [Section B.5, “Windows Group Policy,” on page 77](#)

B.1 Local File Rights Policy

- ♦ For information on managing access control to files and folders, see [Microsoft’s Access Control Best Practices Web site \(http://technet2.microsoft.com/windowsserver/en/library/5a6d7830-6c5e-4c93-b8e7-fb446954d91b1033.mspx?mfr=true\)](http://technet2.microsoft.com/windowsserver/en/library/5a6d7830-6c5e-4c93-b8e7-fb446954d91b1033.mspx?mfr=true).

B.2 Dynamic Local User Policy

- ♦ Ensure that the latest version of the Novell Client™ is installed on the managed device before the Dynamic Local User policy is enforced. To obtain the latest version of Novell Client, see the [Novell Download Web site \(http://download.novell.com/index.jsp\)](http://download.novell.com/index.jsp).

B.3 Roaming Profile Policy

- ♦ The local user account must have the same username and password on both the managed device and the shared server because Windows authenticates the user before loading or saving the profile across the devices.
- ♦ Provide the necessary permission on the shared location to users whose profile is configured for roaming.
- ♦ You cannot load the Windows Vista profile on other Windows operating systems.

B.4 SNMP Policy

- ♦ Ensure that the SNMP service is running before applying the SNMP policy.

B.5 Windows Group Policy

- ♦ Do not apply the Windows Group policy on Windows 2000 or Windows 2003 domain controllers.
- ♦ Do not apply the Windows Group policy to a Windows managed device that is a part of the Microsoft domain and has a group policy from the Windows domain controller applied. The ZENworks Windows Group policy must be applied only if the group policy from the Windows domain controller is not applied.

- ♦ If you want the Windows Group policy settings to be applied to all users of a device, the settings must be configured as a part of a device-assigned policy. The user-assigned policies must contain only the configuration settings specific to the user to whom the policy is assigned.
- ♦ The group policy cache is created on a device when a group policy is enforced on the device. By default, the group policy cache is deleted when the last available group policy is unenforced from the device. A fresh group policy cache is created at the next enforcement of the group policy and this introduces some delay in the policy enforcement cycle.

To prevent the deletion of the group policy cache from the device and thereby speed up the policy enforcement cycle:

1. Open the Registry Editor.
2. Go to HKLM\Software\Novell\ZENworks\GroupPolicy.
3. Create a string called `keepOriginalCache`, and set the value to `true`.

The group policy cache is automatically deleted when ZENworks 10 Configuration Management is uninstalled from the device.

Documentation Updates

C

This section contains information on documentation content changes that were made in this *ZENworks Policy Management Reference* after the initial release of Novell® ZENworks® 10 Configuration Management. The changes are listed according to the date they were published.

The documentation for this product is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the changes listed in this section.

If you need to know whether a copy of the PDF documentation that you are using is the most recent, the PDF document includes a publication date on the title page.

The documentation was updated on the following dates:

- [Section C.1, “February 18, 2009: 10.1.3,” on page 79](#)
- [Section C.2, “October 3, 2008: 10.1.1,” on page 80](#)
- [Section C.3, “August 6, 2008: SP1 \(10.1\),” on page 80](#)

C.1 February 18, 2009: 10.1.3

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

- [Section C.1.1, “Creating Policies,” on page 79](#)
- [Section C.1.2, “Best Practices,” on page 79](#)
- [Section C.1.3, “Troubleshooting Policy Management,” on page 79](#)

C.1.1 Creating Policies

The following changes were made in this section:

Location	Change
Step 4 on page 28	Updated the section.

C.1.2 Best Practices

The following changes were made in this section:

Location	Change
Section B.5, “Windows Group Policy,” on page 77	Updated the section.

C.1.3 Troubleshooting Policy Management

The following changes were made in this section:

Location	Change
"Dynamic Local User is unable to log on to the managed device" on page 72	Added the scenario.

C.2 October 3, 2008: 10.1.1

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

- ♦ [Section C.2.1, "Adding System Requirements for a Policy," on page 80](#)

C.2.1 Adding System Requirements for a Policy

The following changes were made in this section:

Location	Change
Section 3.8, "Adding System Requirements for a Policy," on page 42	Added the entire section. Previously, this information was in online Help only.

C.3 August 6, 2008: SP1 (10.1)

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

- ♦ [Section C.3.1, "Managing Policies," on page 80](#)
- ♦ [Section C.3.2, "Troubleshooting Policy Management," on page 80](#)
- ♦ [Section C.3.3, "Best Practices," on page 81](#)

C.3.1 Managing Policies

The following changes were made in this section:

Location	Change
Section 3.7, "Assigning the Local File Rights Policy to Devices Running Different Languages," on page 42	Added the section.
Section 3.14, "Predefined Policy Reports," on page 50	Added the section.

C.3.2 Troubleshooting Policy Management

The following changes were made in this section:

Location	Change
Appendix A, "Troubleshooting Policy Management," on page 57	Updated the section.

C.3.3 Best Practices

The following changes were made in this section:

Location	Change
Section B.2, "Dynamic Local User Policy," on page 77	Updated the section.