

## Administration Guide

# Novell® ZENworks® Handheld Management

7

July 14, 2006

[www.novell.com](http://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. Please refer to [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 © 2006 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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

Novell, Inc.  
404 Wyman Street, Suite 500  
Waltham, MA 02451  
U.S.A.  
[www.novell.com](http://www.novell.com)

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

## **Novell Trademarks**

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

## **Third-Party Materials**

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



# Contents

<b>About This Guide</b>	<b>9</b>
<b>1 Setting Up Handheld Import</b>	<b>11</b>
1.1 Creating the Handheld Service Package	11
1.2 Configuring the Handheld Import Policy	12
1.3 Associating the Handheld Service Package	16
<b>2 Using ZENworks Handheld Management Policies</b>	<b>17</b>
2.1 Understanding ZENworks Handheld Management Policies	17
2.2 Creating Policy Packages	22
2.3 Setting Up Container Package Policies	22
2.3.1 Search Policy Overview	22
2.3.2 Search Policy	24
2.3.3 Handheld Application Search Policy	26
2.3.4 Associating the Container Package	29
2.4 Setting Up Handheld Package and Handheld User Policies	29
2.4.1 BlackBerry Configuration Policy	30
2.4.2 BlackBerry Inventory Policy	32
2.4.3 BlackBerry Security Policy	34
2.4.4 Palm Client Configuration Policy	36
2.4.5 Palm Configuration Policy	39
2.4.6 Palm Access Point Configuration Policy	43
2.4.7 Palm File Retrieval Policy	45
2.4.8 Palm Security Policy	48
2.4.9 WinCE Client Configuration Policy	53
2.4.10 WinCE Configuration Policy	55
2.4.11 WinCE Access Point Configuration Policy	59
2.4.12 WinCE File Retrieval Policy	62
2.4.13 WinCE Remote Management Policy	66
2.4.14 WinCE Security Policy	68
2.4.15 Associating the Handheld Package or the Handheld User Package	73
2.4.16 Associating a User Object to a BlackBerry Device	74
2.4.17 Scheduling Packages and Policies	74
2.5 Setting Up Handheld Service Package Policies	76
2.6 Viewing Policy Status Information	76
2.6.1 Viewing Status for a Specific Policy	76
2.6.2 Viewing Policy Status for a Specific Handheld Device	78
<b>3 Using Queries and Groups</b>	<b>81</b>
3.1 Using Queries	81
3.1.1 Creating a Query	81
3.1.2 Using Logical Operators	84
3.2 Using Groups	84
3.2.1 Creating Groups	85
3.2.2 Viewing the Properties of a Group	89
3.2.3 Changing Group Membership	91
3.2.4 Changing the Update Schedule of Query-Based Groups	91
3.2.5 Deleting a Group	92

3.2.6	Viewing Handheld Application Objects Assigned to a Group .....	93
3.2.7	Changing a Group's Type .....	94
<b>4</b>	<b>Distributing Software to Handheld Devices</b>	<b>95</b>
4.1	Understanding Handheld Application Objects .....	95
4.1.1	Specifying Source Files .....	95
4.1.2	Understanding Automatic Application Updates .....	96
4.1.3	Installing Software at a Predefined Time Even When the Device is Not Connected to the Network .....	97
4.2	Distributing Applications to Handheld Devices .....	97
4.2.1	Creating a Handheld Application Object .....	97
4.2.2	Configuring a Handheld Application Object .....	98
4.2.3	Scheduling the Distribution of a Handheld Application Object .....	102
4.3	Displaying Handheld Application Object Status .....	104
4.4	Modifying a Handheld Application Object .....	105
4.4.1	Modifying the Contents of a Handheld Application Object .....	105
4.4.2	Scanning for Updated Components .....	105
4.4.3	Deleting a Handheld Application Object .....	106
4.4.4	Deleting a Handheld Application Object's Associations .....	106
<b>5</b>	<b>Using Inventory and Reports</b>	<b>107</b>
5.1	Viewing Software Inventory .....	108
5.1.1	Viewing Software Inventory for a Specific Handheld Device .....	109
5.1.2	Viewing Software Inventory Across All Palm OS, BlackBerry, or Windows CE Devices in Your System .....	109
5.1.3	Identifying Files for Windows CE Devices .....	111
5.1.4	Ignoring or Identifying Windows CE Files and Applications .....	113
5.2	Viewing Hardware Inventory .....	118
5.3	Viewing Network Information .....	120
5.4	Using Inventory Reports .....	120
5.4.1	Running Reports .....	121
5.4.2	Exporting Reports .....	122
5.4.3	Creating Custom Reports .....	122
5.5	Printing Data from the ZENworks Handheld Management Inventory Viewer .....	123
<b>6</b>	<b>Remotely Viewing or Controlling the IP-Enabled Windows CE Devices</b>	<b>125</b>
6.1	Configuring WinCE Remote Management Policy .....	125
6.2	Setting a VNC Password on the Handheld Device .....	125
6.3	Initiating a Remote View or a Remote Control Session .....	126
6.3.1	Initiating a Remote View or a Remote Control Session from a Device Object .....	126
6.3.2	Initiating a Remote View or a Remote Control Session from a User Object .....	127
<b>7</b>	<b>Making System Configuration Changes</b>	<b>129</b>
7.1	Configuring User Authentication .....	129
7.2	Configuring the Proxy Service .....	131
7.2.1	Configuring Network Settings .....	131
7.2.2	Configuring Network Usage Restrictions .....	132
7.2.3	Configuring Dial-Up Communications .....	134
7.2.4	Enabling or Disabling Message Transfers .....	135
7.2.5	Configuring Handheld Communications .....	135
7.2.6	Configuring IP Communication for the ZENworks Handheld Management Access Point .....	136

7.2.7	Connecting to the ZENworks Handheld Management Server . . . . .	136
7.3	Converting to Microsoft SQL Server . . . . .	136
7.4	Compacting and Repairing the Database . . . . .	138
7.4.1	Compacting the Server Database . . . . .	138
7.4.2	Compacting the Proxy Service Database . . . . .	139
7.4.3	Compacting and Repairing the Database . . . . .	139
7.5	Configuring the ZENworks Handheld Management Access Point and the Desktop Synchronization Integration . . . . .	140
7.5.1	Configuring Bandwidth Usage . . . . .	140
7.5.2	Configuring Client Retries and Power Down (or Suspend) . . . . .	140
7.6	Configuring the ZENworks Handheld Management IP Clients . . . . .	141
7.6.1	Configuring the ZENworks Handheld Management Palm OS IP Client . . . . .	141
7.6.2	Configuring the ZENworks Handheld Management Windows CE IP Client . . . . .	143
<b>A Troubleshooting</b>		<b>145</b>
A.1	Error Logs . . . . .	145
A.2	ConsoleOne Status Pages . . . . .	145
A.3	Error Messages . . . . .	146
A.4	Troubleshooting Strategies . . . . .	147
A.5	Contacting Technical Support . . . . .	152
<b>B Configuring SSL and HTTP Settings</b>		<b>153</b>
B.1	Configuring the SSL and HTTP Communication between the ZENworks Handheld Management Server and the ZENworks Handheld Management Access Point . . . . .	154
B.2	Configuring SSL and HTTP Communication between the ZENworks Handheld Management Access Point and the Handheld Devices . . . . .	156
B.3	Changing the Default Ports on the ZENworks Handheld Management Server and ZENworks Handheld Management Access Point Communication . . . . .	159
B.4	Changing the Default Ports for the ZENworks Handheld Management Access Point and the Handheld Devices Communication . . . . .	159
<b>C Security Considerations</b>		<b>161</b>
<b>D Documentation Updates</b>		<b>163</b>
D.1	July 14, 2006 . . . . .	163
D.1.1	Appendix C: Security Considerations . . . . .	163
D.2	December 9, 2005 . . . . .	163
D.3	October 7, 2005 . . . . .	164
D.3.1	Using Inventory and Reports . . . . .	164
D.3.2	Using ZENworks Handheld Management Policies . . . . .	164



# About This Guide

This *Administration Guide* consists of comprehensive, conceptual information to help you understand and use Novell® ZENworks® 7 Handheld Management.

The sections include:

- ◆ Chapter 1, “Setting Up Handheld Import,” on page 11
- ◆ Chapter 2, “Using ZENworks Handheld Management Policies,” on page 17
- ◆ Chapter 3, “Using Queries and Groups,” on page 81
- ◆ Chapter 4, “Distributing Software to Handheld Devices,” on page 95
- ◆ Chapter 5, “Using Inventory and Reports,” on page 107
- ◆ Chapter 6, “Remotely Viewing or Controlling the IP-Enabled Windows CE Devices,” on page 125
- ◆ Chapter 7, “Making System Configuration Changes,” on page 129
- ◆ Appendix A, “Troubleshooting,” on page 145
- ◆ Appendix B, “Configuring SSL and HTTP Settings,” on page 153
- ◆ Appendix C, “Security Considerations,” on page 161
- ◆ Appendix D, “Documentation Updates,” on page 163

## Audience

This guide is intended for system administrators installing ZENworks 7 Handheld Management software. These users should be familiar with their own network and the hardware configuration of the management zone where they intend to install this product. A working knowledge of Novell eDirectory™ and Novell ConsoleOne® is required.

## Feedback

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

## Documentation Updates

For the most recent version of the *ZENworks 7 Handheld Management Administration Guide*, visit the [Novell ZENworks 7 Web site \(http://www.novell.com/documentation/zenworks7\)](http://www.novell.com/documentation/zenworks7).

## Additional Documentation

For information about installing ZENworks Handheld Management, see the *Novell ZENworks 7 Handheld Management Installation Guide*.

## Documentation Conventions

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

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

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

# Setting Up Handheld Import

# 1

Novell® ZENworks® 7 Handheld Management provides simplified, hands-off management of enterprise handheld devices.

For more information about installing ZENworks Handheld Management, see the *Novell ZENworks 7 Handheld Management Installation Guide*.

In order to manage the handheld devices, you must do the following:

- ◆ Import handheld devices into Novell eDirectory™.

The following sections provide information you need for setting up an Import policy:

- ◆ [Section 1.1, “Creating the Handheld Service Package,” on page 11](#)
- ◆ [Section 1.2, “Configuring the Handheld Import Policy,” on page 12](#)
- ◆ [Section 1.3, “Associating the Handheld Service Package,” on page 16](#)
- ◆ Ensure that the users synchronize their handheld devices using their normal synchronization process (Microsoft\* ActiveSync, Palm\* HotSync, and so forth).

After the handheld objects are imported into the directory, you can begin using policy-based management, distributing software applications to individual handheld devices or to groups of handheld devices, collecting hardware and software inventory for all enterprise handheld devices, and more.

- ◆ Set up the policies that can be associated with handheld objects. For more information, see [Chapter 2, “Using ZENworks Handheld Management Policies,” on page 17](#).

## 1.1 Creating the Handheld Service Package

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

In ZENworks Handheld Management, the Handheld Service Package contains only the Handheld Import policy.

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

- ◆ Partitions in your tree
- ◆ The 256-character limit in eDirectory for the full distinguished name
- ◆ The Search policy that is used to locate the policy package

To minimize tree walking, it is best to create this policy package OU at the root of the partition that contains the objects with which the policy package is associated. It also maximizes the number of characters that are available for naming the policy.

To create the Handheld Service Package:

- 1 In Novell ConsoleOne<sup>®</sup>, right-click the container where you want the container for the policy packages placed, click *New*, then click *Organizational Unit*.

The New Organizational Unit window is displayed.



- 2 Give the container a short name, then click *OK*.
- 3 Right-click the newly created container that holds your policy packages, click *New*, then click *Policy Package*.
- 4 Select *Handheld Service Package*, then click *Next*.

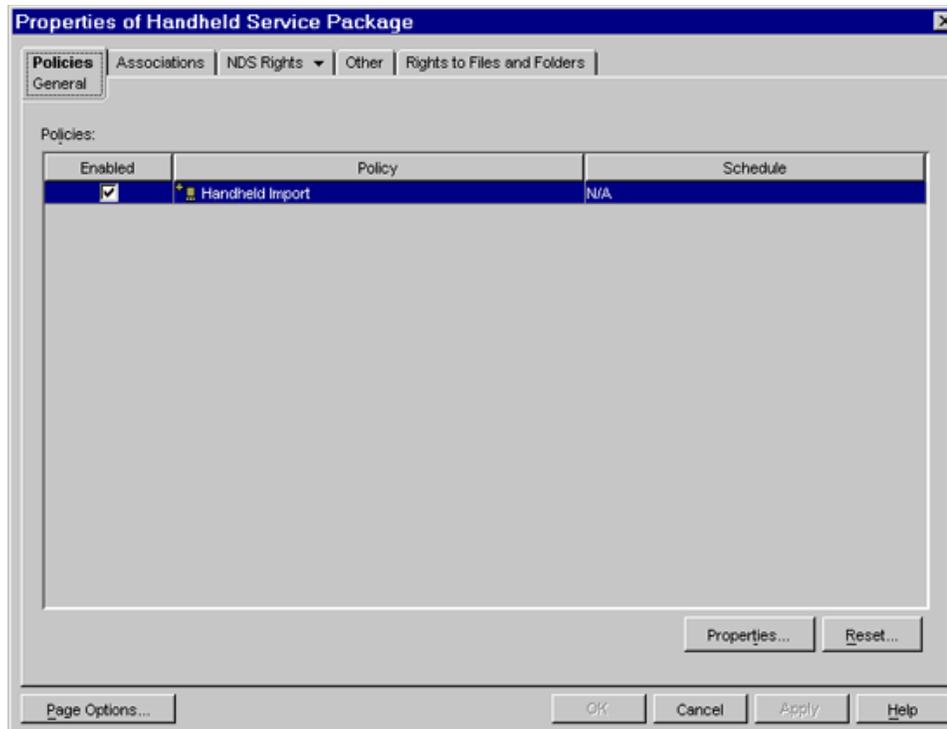


- 5 Give the policy package a short name, then click *Next*.
- 6 Review the information in the Summary page, then click *Finish*.

## 1.2 Configuring the Handheld Import Policy

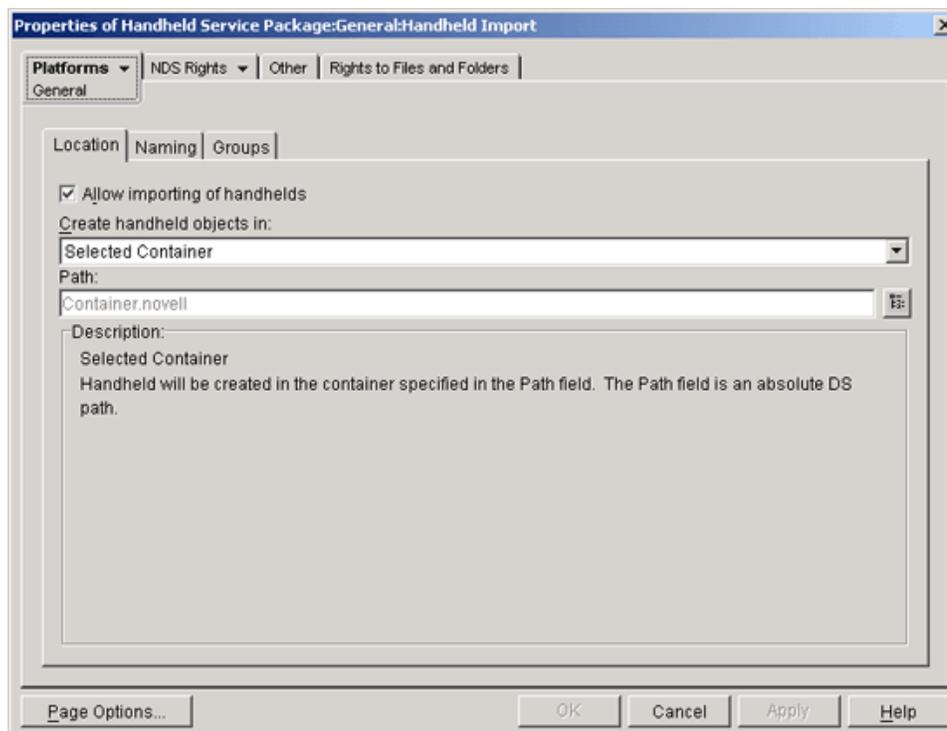
- 1 In ConsoleOne, right-click the Handheld Service Package object that is created during [Section 1.1, “Creating the Handheld Service Package,” on page 11](#), then click *Properties*.
- 2 Select the check box under the *Enabled* column for the Handheld Import policy.

This both selects and enables the policy.



3 Click *Properties*.

The *Location* tab of the *General* page is displayed.



You can configure the Handheld Import policy on this page to enable importing of BlackBerry\*, Palm OS\*, and Windows\* CE devices.

In addition to the *General* page, ZENworks Handheld Management provides three platform-specific pages: *BlackBerry*, *Palm*, and *Windows CE*. If you want to specify different settings for each type of device, you can use the appropriate platform page. For example, you could specify different containers to hold the different types of handheld devices.

4 Click the down-arrow on the *Platforms* tab, then select the desired platform.

5 Fill in the fields:

**Enable Platform Settings to Override General Settings:** This option displays only on the BlackBerry, Palm, and WinCE platform pages. Select this option if you want the settings specified on the BlackBerry, Palm, or WinCE page to override those settings specified on the General page.

**Allow Importing of Handhelds:** Enable this option to allow registered handheld devices to be imported into the directory.

**Create Handheld Objects In:** Select an option from the drop-down list.

- ♦ **Selected Container:** The handheld device objects are created in the container specified in the Path field. This is an absolute DS path.
- ♦ **Server Container:** The handheld device objects are created in the same container where the handheld service object is created. You can specify a relative DS path from the server container.
- ♦ **Associated Object Container:** The handheld device objects are created in the container that is associated with the Handheld Import policy. You can specify a relative DS path from the associated container.

Relative Path = handheld. means to go up one level from the container to create the handheld device object.

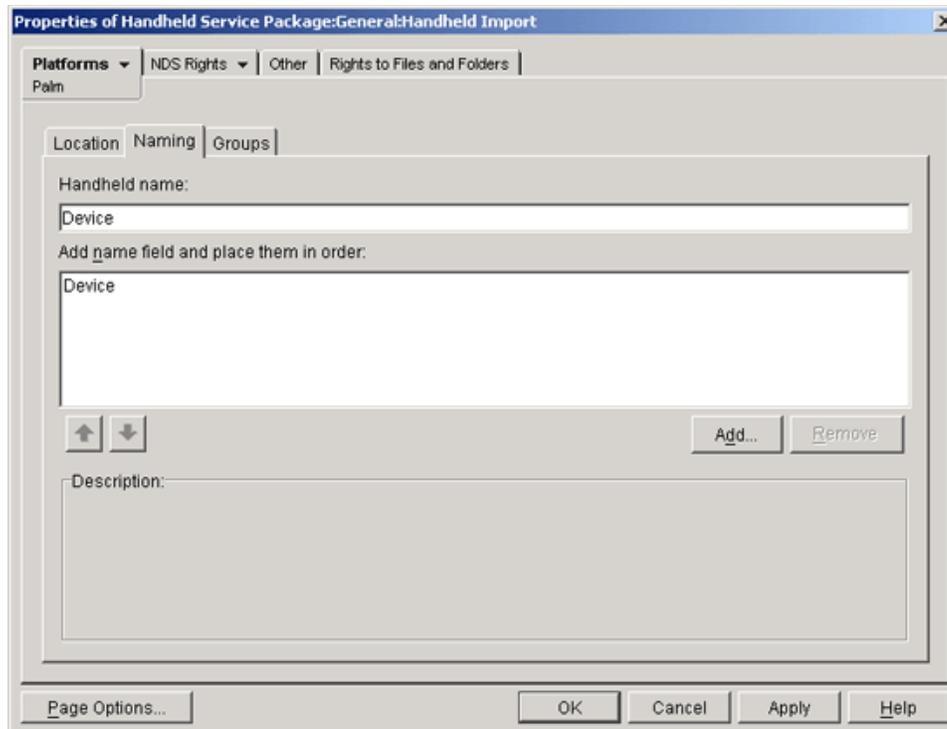
**Path:** If you are using a relative path, enter a string. The number of periods you end the path with determines the number of relative levels. If you are using an absolute path, select the container.

---

**NOTE:** The *Description* box describes where the handheld device objects are created, based on the settings you selected on the Location page. Review the description and make any necessary changes.

---

6 Click the *Naming* tab.



**7** Fill in the fields:

**Handheld Name:** Displays the handheld naming convention currently defined in the *Add Name Fields and Place Them in Order* list.

Whenever there is a potential name conflict (such as two handheld device objects in the same container with the same name), the system appends a number on the end of the name that you enter here.

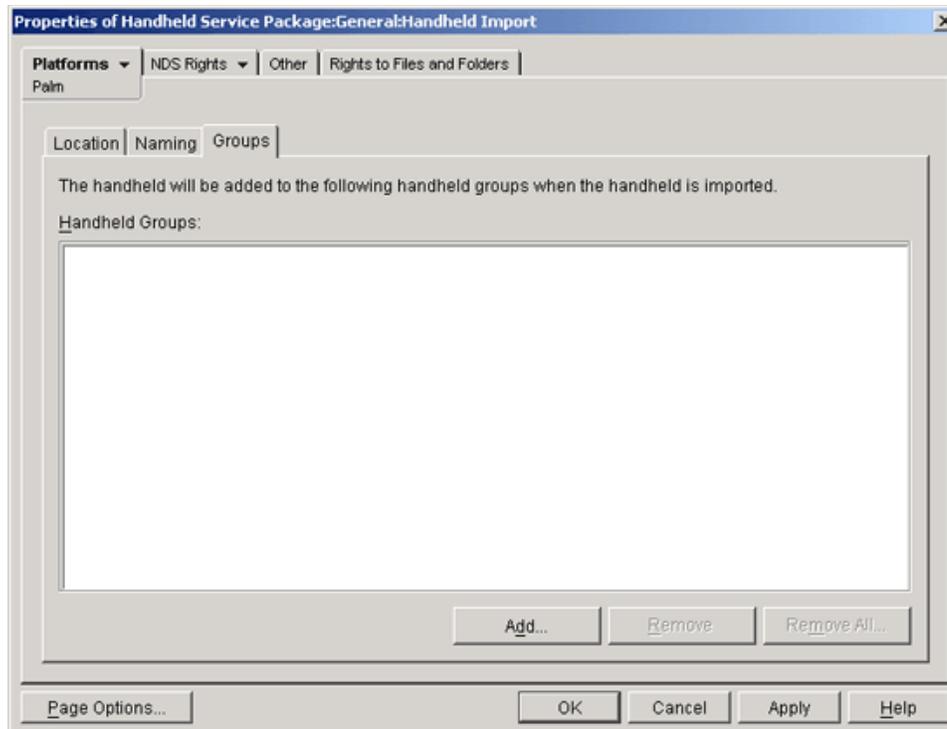
**Add Name Field and Place Them in Order:** You must have at least one option in this list.

You can add or remove options, or click the arrows to move an option up or down the list. The handheld device objects are named in the order these options display in the list.

The name options are:

- ◆ **<User Defined>:** You can any text here such as the separator between the Device and User value. For example, Device\_UserName. In this example, the underscore ( \_ ) is the user defined value.
- ◆ **Device:** The device's name.
- ◆ **User:** The device's owner name or the name provided by Palm HotSync or Microsoft ActiveSync.
- ◆ **Computer:** The name of the Access Point to which the device is connected.

**8** Click the *Groups* tab.



- 9 Click *Add*, then browse for the Handheld Group objects you want this handheld device object to belong to when it is imported.

For more information about Handheld Group objects, see [Section 3.2, “Using Groups,”](#) on page 84.

- 10 Click *OK* to save the policy.
- 11 Continue with [Section 1.3, “Associating the Handheld Service Package,”](#) on page 16.

## 1.3 Associating the Handheld Service Package

The Handheld Import policy you configured and enabled is not in effect until you associate its policy package with the ZENworks Handheld Management Service object directly or with a container object.

To associate the Handheld Service Package:

- 1 In ConsoleOne, right-click the *Handheld Service Package*, then click *Properties*.
- 2 Click the *Associations* tab, then click *Add*.
- 3 To associate the package, browse for the ZENworks Handheld Management Service object, the container containing the Service object, or the container object created during the installation of ZENworks Handheld Management server components.
- 4 Click *OK*.

# Using ZENworks Handheld Management Policies

# 2

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

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

ZENworks Handheld Management has four policy packages: Container Package, Handheld Package, Handheld Service Package, and Handheld User Package.

The following sections contain additional information:

- ♦ [Section 2.1, “Understanding ZENworks Handheld Management Policies,” on page 17](#)
- ♦ [Section 2.2, “Creating Policy Packages,” on page 22](#)
- ♦ [Section 2.3, “Setting Up Container Package Policies,” on page 22](#)
- ♦ [Section 2.4, “Setting Up Handheld Package and Handheld User Policies,” on page 29](#)
- ♦ [Section 2.5, “Setting Up Handheld Service Package Policies,” on page 76](#)
- ♦ [Section 2.6, “Viewing Policy Status Information,” on page 76](#)

## 2.1 Understanding ZENworks Handheld Management Policies

The following table lists each ZENworks Handheld Management policy, indicates the package that contains the policy, and provides a brief description of the policy.

**Table 2-1** List of ZENworks Handheld Management Policies

Policy	Container	Description
Handheld Import Policy	Handheld Service Package	Lets you enable handheld import and configure settings, such as how handheld device objects are named, where they are stored in eDirectory, and which Handheld Group objects you want certain handheld device objects associated with.  For more information, see <a href="#">Chapter 1, “Setting Up Handheld Import,” on page 11.</a>

Policy	Container	Description
Search Policy	Container Package	<p>Lets you specify how far up the tree ZENworks Handheld Management searches for effective policies.</p> <p>For more information, see <a href="#">“Search Policy” on page 24.</a></p>
Handheld Application Search Policy	Container Package	<p>Lets you specify how far up the tree ZENworks Handheld Management searches for Handheld Application objects.</p> <p>For more information, see <a href="#">“Handheld Application Search Policy” on page 26.</a></p>
BlackBerry Configuration Policy	Handheld Package and Handheld User Package	<p>Lets you set configuration information for associated BlackBerry* devices, including the owner name for the device and any additional information you want to include.</p> <p>For more information, see <a href="#">“BlackBerry Configuration Policy” on page 30.</a></p>
BlackBerry Inventory Policy	Handheld Package and Handheld User Package	<p>Lets you enable the collection of hardware and software inventory from associated BlackBerry devices.</p> <p>For more information, see <a href="#">“BlackBerry Inventory Policy” on page 32.</a></p>
BlackBerry Security Policy	Handheld Package and Handheld User Package	<p>Lets you ensure that a password is set on associated BlackBerry devices.</p> <p>For more information, see <a href="#">“BlackBerry Security Policy” on page 34.</a></p>
Palm Client Configuration Policy	Handheld Package	<p>Lets you enable user authentication on associated Palm OS* devices.</p> <p>For more information, see <a href="#">Section 2.4.4, “Palm Client Configuration Policy,” on page 36.</a></p>

Policy	Container	Description
Palm Access Point Configuration Policy	Handheld Package and Handheld User Package	<p>Lets you assign multiple ZENworks Handheld Management Access Points to a device and also define the order of the ZENworks Handheld Management Access Points to which the Palm OS device must connect.</p> <p>For more information, see <a href="#">Section 2.4.6, “Palm Access Point Configuration Policy,” on page 43.</a></p>
Palm Configuration Policy	Handheld Package and Handheld User Package	<p>Lets you set general preferences, such as auto-off, system sound, and beam retrieve settings; associate different software programs with the buttons on the Palm OS device; assign a feature users can access when they drag the pen from the writing area to the top of the screen on the Palm OS device; and specify which software programs are allowed or not allowed on Palm OS devices.</p> <p>Also lets you configure the files that must be automatically deleted from the Windows CE device.</p> <p>For more information, see <a href="#">“Palm Configuration Policy” on page 39.</a></p>
Palm File Retrieval Policy	Handheld Package and Handheld User Package	<p>Lets you specify files to retrieve from the associated Palm OS device to copy to a specified location.</p> <p>For more information, see <a href="#">“Palm File Retrieval Policy” on page 45.</a></p>

Policy	Container	Description
Palm Security Policy	Handheld Package and Handheld User Package	<p>Lets you ensure that a password is set on the associated Palm OS device and lets you configure Auto Lock Configuration and enhanced password protection.</p> <p>Lets you set a user's network password as the device password for the Palm OS device.</p> <p>Also lets you specify self-destruct settings to disable a Palm device after a specified number of failed password attempts or after a specified number of days since the device was last synchronized.</p> <p>For more information, see <a href="#">"Palm Security Policy" on page 48.</a></p>
WinCE Access Point Configuration Policy	Handheld Package and Handheld User Package	<p>Lets you assign multiple ZENworks Handheld Management Access Points to a device and also define the order of the ZENworks Handheld Management Access Points to which the Windows* CE device must connect.</p> <p>For more information, see <a href="#">Section 2.4.11, "WinCE Access Point Configuration Policy," on page 59.</a></p>
WinCE Client Configuration Policy	Handheld Package	<p>Lets you enable user authentication on associated Windows CE devices.</p> <p>Also lets you configure the software or files that must be automatically uninstalled or deleted from the Windows CE device.</p> <p>For more information, see <a href="#">Section 2.4.9, "WinCE Client Configuration Policy," on page 53.</a></p>

Policy	Container	Description
WinCE Configuration Policy	Handheld Package and Handheld User Package	<p>Lets you associate different software programs or functions with the buttons on the associated Windows CE device; specify which programs you want to include on the Start menu (on a Pocket PC) or on the desktop (on a handheld PC); and specify power settings for Windows CE devices.</p> <p>Also, lets you configure the software to be uninstalled from Windows CE device.</p> <p>For more information, see <a href="#">“WinCE Configuration Policy” on page 55.</a></p>
WinCE File Retrieval Policy	Handheld Package and Handheld User Package	<p>Lets you specify files to retrieve from the associated Windows CE device to copy to a specified location.</p> <p>For more information, see <a href="#">“WinCE File Retrieval Policy” on page 62.</a></p>
WinCE Remote Management Policy	Handheld Package and Handheld User Package	<p>Lets the administrator or remote users perform Remote View or Remote Control operations on the IP-enabled Windows CE devices.</p> <p>For more information, see <a href="#">Section 2.4.13, “WinCE Remote Management Policy,” on page 66.</a></p>
WinCE Security Policy	Handheld Package and Handheld User Package	<p>Lets you ensure that a password is set on the Windows CE device and configure enhanced security options for Pocket PCs.</p> <p>Lets set a user’s network password as the device password for the Windows CE device.</p> <p>Also lets you specify self-destruct settings to disable a Windows CE device after a specified number of failed password attempts or after a specified number of days since the device was last synchronized.</p> <p>For more information, see <a href="#">“WinCE Security Policy” on page 68.</a></p>

## 2.2 Creating Policy Packages

A policy package is an eDirectory object containing one or more individual policies. Before you can configure, enable, and associate the policies contained in a policy package, you must create the policy package.

- 1 In Novell ConsoleOne<sup>®</sup>, right-click the container that holds your policy packages, then click *New*, then click *Policy Package*.
- 2 Select *Container Package*.  
or  
Select *Handheld Package*.  
or  
Select *Handheld Service Package*.  
or  
Select *Handheld User Package*.

---

**TIP:** To list the policies that are contained in each policy package, click the name of each policy in the Policy Packages list on the left side of the Policy Package Wizard page. The available policies are displayed in the Policies list on the right side of the Policy Package Wizard page.

---

- 3 Click *Next*.
- 4 Give the policy package a short name, then click *Next*.
- 5 Review the information in the Summary page, then click *Finish*.

## 2.3 Setting Up Container Package Policies

In ZENworks Handheld Management, the Container package contains two policies: Search and Handheld Application Search.

The following sections contain additional information:

- ♦ [“Search Policy Overview” on page 22](#)
- ♦ [“Search Policy” on page 24](#)
- ♦ [“Handheld Application Search Policy” on page 26](#)
- ♦ [“Associating the Container Package” on page 29](#)

### 2.3.1 Search Policy Overview

ZENworks Handheld Management policies are associated to a handheld device object in any of the following ways:

- ♦ To the handheld device object itself
- ♦ To a User object
- ♦ To a Handheld Group where the handheld device is a member
- ♦ To a User Group where the user is a member
- ♦ To a parent container of the handheld device or User object

The search order that ZENworks Handheld Management uses is consistent with standard eDirectory behavior and any search policies that are in the tree. By default, ZENworks Handheld Management starts at the handheld device or user object, followed by any Handheld groups or User groups that the device is a member of, and then starts walking up the tree looking for policies to enforce. All handheld policies are merged and the culmination is applied to the handheld device. If any conflicts occur, such as two Palm Configuration policies (one associated directly to the handheld device object and the other associated to a parent container of the handheld device object), the first policy found is enforced. In this case, the Palm Configuration policy directly associated to the handheld device object is enforced.

If a policy contained in a Handheld User Package and another policy in the Handheld Package conflict, the settings in the Handheld User Package are enforced. For example, if you configure and enable the Palm Configuration policy in the Handheld User Package, but you also have an enabled Palm Configuration policy in the Handheld Package, the policy in the Handheld User Package takes precedence.

The File Retrieval policies (Palm File Retrieval and WinCE File Retrieval) present exceptions to rule that the first policy found is enforced. These policies are both plural (meaning they can be added many times to a policy package) and cumulative (meaning that many different File Retrieval policies with different settings can be effective for a single handheld device object, handheld group object, or container object). Because the File Retrieval policies are plural and cumulative, no conflicts occur when ZENworks Handheld Management encounters multiple File Retrieval policies: every effective File Retrieval policy is enforced.

The Search policy is used to limit how far up the tree ZENworks Handheld Management searches for the effective policies. In addition to limiting how far up the tree ZENworks Handheld Management searches for policies, both policies let you determine the searching order (object, group, container) that ZENworks Handheld Management uses as it searches for policies. The search order is significant because the first policy found is enforced (except for the File Retrieval policies, as explained previously).

The Handheld Application Search policy is used to limit how far up the tree ZENworks Handheld Management searches for handheld application objects.

If your directory contains many objects, ZENworks Handheld Management performs significant tree-walking if no search policies are enabled. For this reason, you should make use of both the Search policy and the Handheld Application Search policy.

The Search policy and the Handheld Application Search policy provide the following benefits

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

The Search policy specifies how ZENworks Handheld Management determines which policies are associated with handheld device objects. The Handheld Application Search policy specifies how ZENworks Handheld Management determines which handheld application objects are associated with handheld device objects. To make either search policy effective, you associate it with a container. Both search policies apply to handheld device or user objects within or beneath a given container.

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

**Table 2-2** Search Levels

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

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

The default search policy recognizes the policy package associated with the handheld device object before it looks in any group or container where such an object resides.

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

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

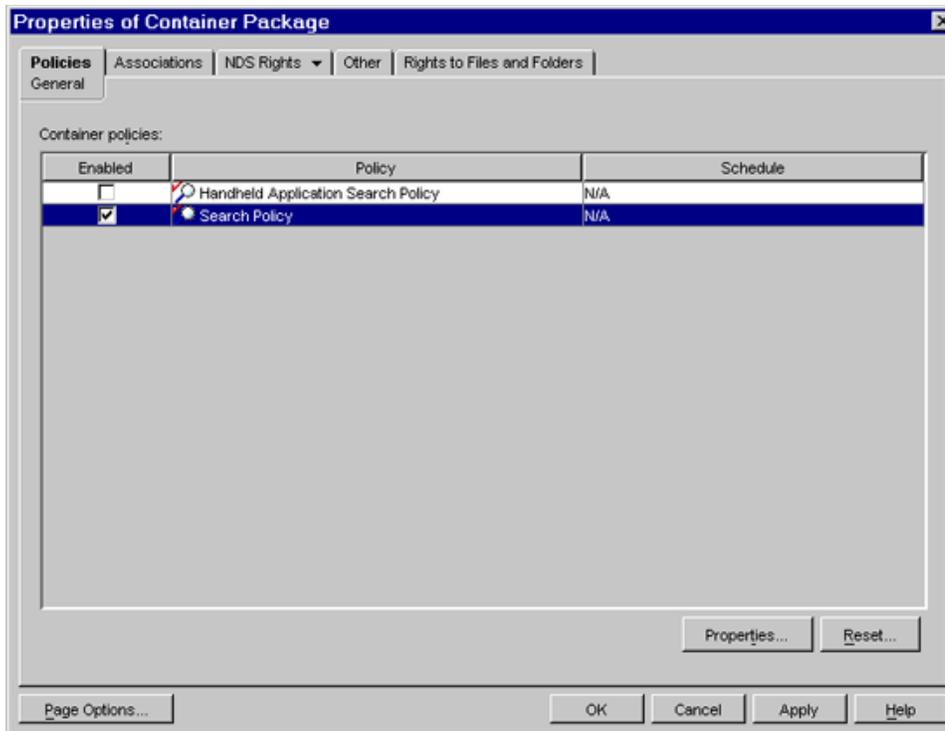
The Search policy is required for finding other policies. You set up Search policies at a container level. Set up as many Search policies as you need to help minimize network traffic.

### 2.3.2 Search Policy

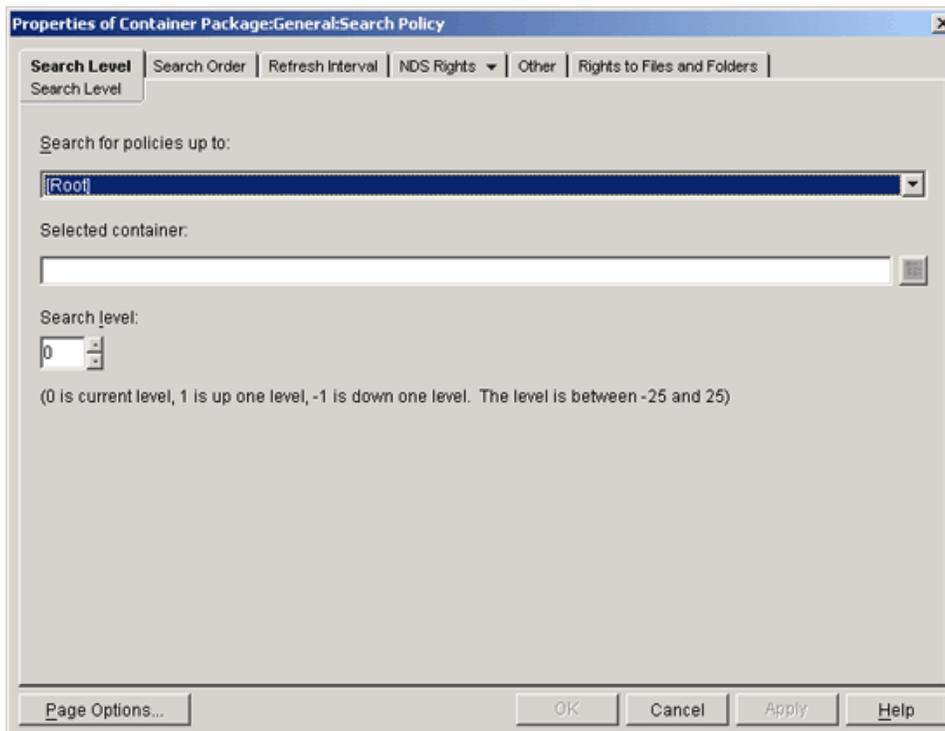
The Search policy is used to limit how far up the tree ZENworks Handheld Management searches for the effective policies.

To set up a Search policy:

- 1 In ConsoleOne, right-click the newly created Container Package, then click *Properties*.  
For information on creating the Container Package, see [Section 2.2, "Creating Policy Packages," on page 22](#).
- 2 Select the check box under the *Enabled* column for the Search policy.  
This both selects and enables the policy.



3 Click Properties to display the *Search Level* page.



4 Select the level to search to from the drop-down list:

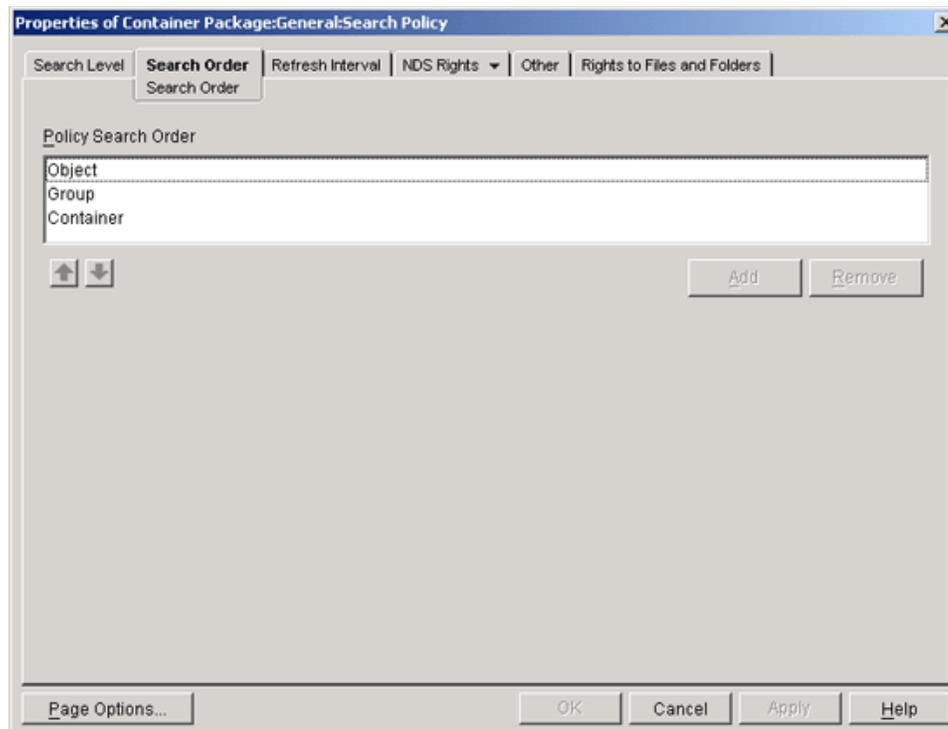
**[Root]**: Search from the handheld device object to the root of the tree.

**Object Container:** Search from the handheld device object to the parent container of the object.

**Partition:** Search from the object to the partition.

**Selected Container:** Search from the handheld device object to the selected container.

- 5 If you chose *Selected Container*, browse to select the container.
- 6 To determine the searching limits in either direction, specify a number between -25 and 25.
- 7 Click the *Search Order* tab.



- 8 Specify the policy searching order, using the arrow keys, the *Add* button, and the *Remove* button as necessary.

---

**NOTE:** Depending on which other ZENworks products (ZENworks Desktop Management and ZENworks Server Management) are present, ConsoleOne might display a *Refresh Interval* page; however, ZENworks Handheld Management does not use the settings on the *Refresh Interval* page.

---

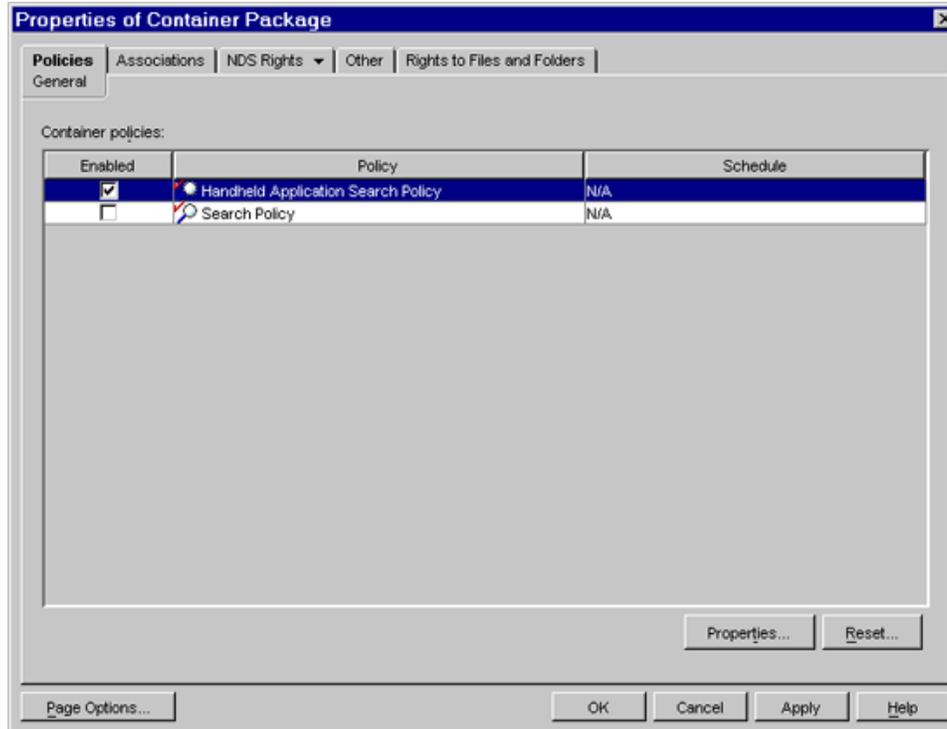
- 9 Click *OK*.
- 10 When you have finished configuring all of the policies for this package, continue with the steps under "[Associating the Container Package](#)" on page 29 to associate the policy package.

### 2.3.3 Handheld Application Search Policy

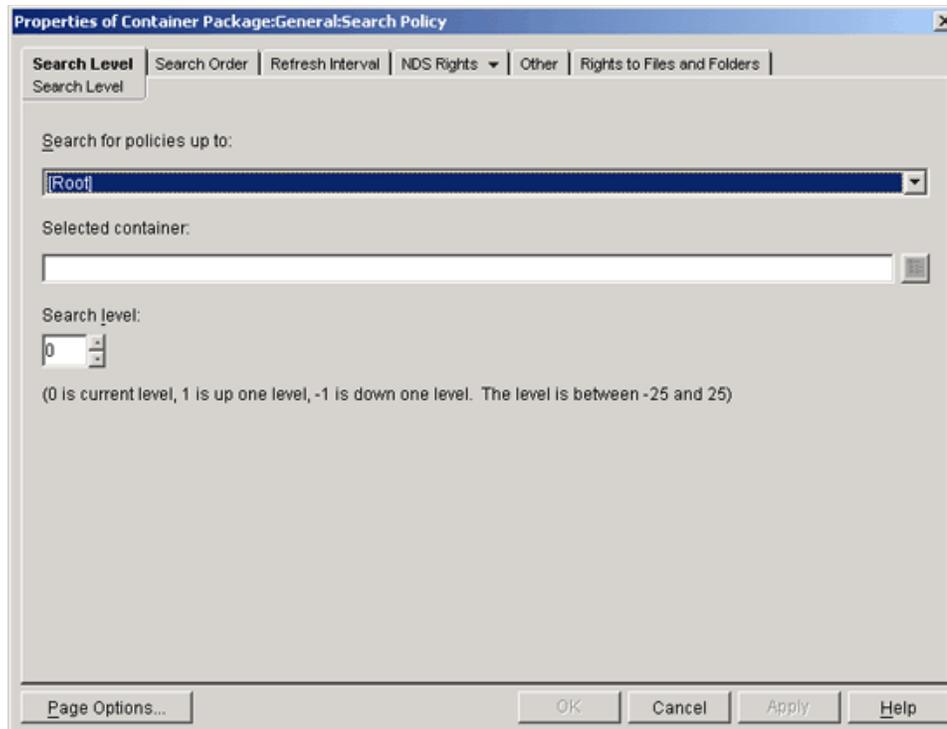
The Handheld Application Search policy is used to limit how far up the tree ZENworks Handheld Management searches for Handheld Application objects.

To set up the Handheld Application Search policy:

- 1 In ConsoleOne, right-click the *Container Package*, then click *Properties*.
- 2 Select the check box under the *Enabled* column for the Handheld Application Search policy.  
This both selects and enables the policy.



- 3 Click *Properties* to display the *Search Level* page.



4 Select the level to search to:

**[Root]:** Search from the handheld device object to the root of the tree.

**Object Container:** Search from the handheld device object to the parent container of the object.

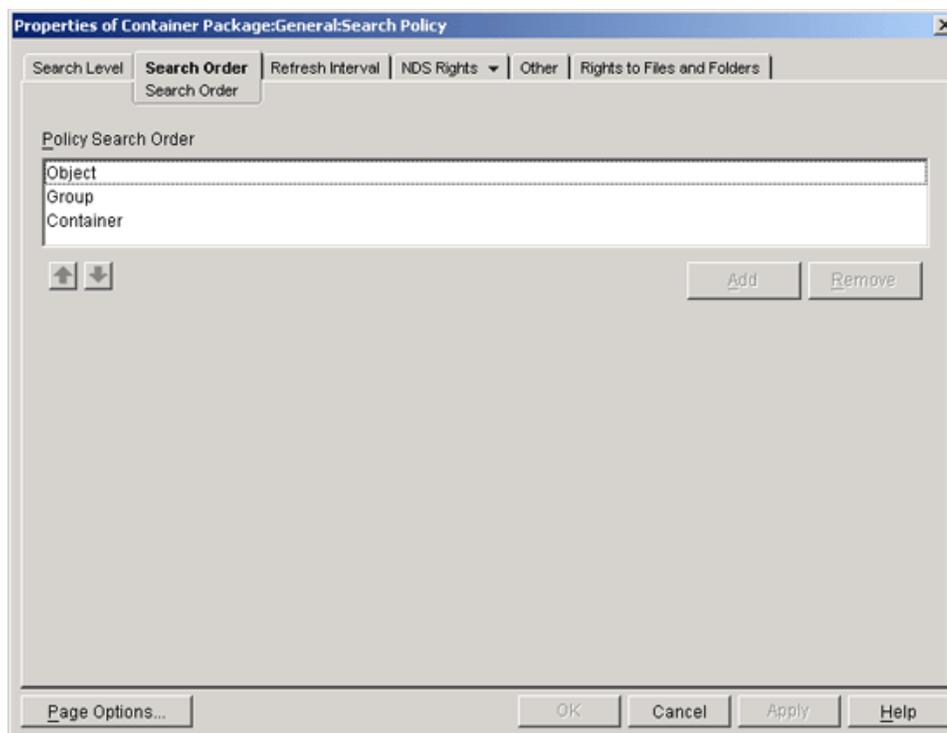
**Partition:** Search from the object to the partition.

**Selected Container:** Search from the handheld device object to the selected container.

5 If you chose *Selected Container*, browse to select the container.

6 To determine the searching limits in either direction, specify a number between -25 and 25.

7 Click the *Search Order* tab.



- 8 Specify the policy searching order.  
Use the arrow keys, the *Add* button, and the *Remove* button as necessary to create your search order.
- 9 Click *OK*.
- 10 When you have finished configuring all of the policies for this package, continue with the steps under [“Associating the Container Package” on page 29](#) to associate the policy package.

### 2.3.4 Associating the Container Package

The policies you configured and enabled are not in effect until you associate their policy package with a container object.

- 1 In ConsoleOne, right-click the *Container Package*, then click *Properties*.
- 2 Click the *Associations* tab, then click *Add*.
- 3 Browse for the container for associating the package, then click *OK*.

## 2.4 Setting Up Handheld Package and Handheld User Policies

ZENworks Handheld Management provides Handheld Package and Handheld User Package policies for the Palm OS, Windows CE, and BlackBerry platforms.

Each platform has its own page where you can view and configure available policies. To display a desired platform page: In ConsoleOne, right-click the *Handheld Package* or the *Handheld User Package*, click *Properties*, click the down-arrow on the *Policies* tab, then click the appropriate platform: *Palm*, *WinCE*, or *BlackBerry*.

Review the following sections for more information to help you set up the Handheld Package and Handheld User Package policies:

- ◆ [Section 2.4.1, “BlackBerry Configuration Policy,” on page 30](#)
- ◆ [Section 2.4.2, “BlackBerry Inventory Policy,” on page 32](#)
- ◆ [Section 2.4.3, “BlackBerry Security Policy,” on page 34](#)
- ◆ [Section 2.4.4, “Palm Client Configuration Policy,” on page 36](#)
- ◆ [Section 2.4.5, “Palm Configuration Policy,” on page 39](#)
- ◆ [Section 2.4.6, “Palm Access Point Configuration Policy,” on page 43](#)
- ◆ [Section 2.4.7, “Palm File Retrieval Policy,” on page 45](#)
- ◆ [Section 2.4.8, “Palm Security Policy,” on page 48](#)
- ◆ [Section 2.4.9, “WinCE Client Configuration Policy,” on page 53](#)
- ◆ [Section 2.4.10, “WinCE Configuration Policy,” on page 55](#)
- ◆ [Section 2.4.11, “WinCE Access Point Configuration Policy,” on page 59](#)
- ◆ [Section 2.4.12, “WinCE File Retrieval Policy,” on page 62](#)
- ◆ [Section 2.4.13, “WinCE Remote Management Policy,” on page 66](#)
- ◆ [Section 2.4.14, “WinCE Security Policy,” on page 68](#)
- ◆ [Section 2.4.15, “Associating the Handheld Package or the Handheld User Package,” on page 73](#)
- ◆ [Section 2.4.16, “Associating a User Object to a BlackBerry Device,” on page 74](#)
- ◆ [Section 2.4.17, “Scheduling Packages and Policies,” on page 74](#)

## 2.4.1 BlackBerry Configuration Policy

The BlackBerry Configuration policy lets you specify a standard owner name and additional information that is set on the associated BlackBerry devices. For example, you could specify that your company name, address, and telephone number be set on all associated BlackBerry devices to help recover lost devices.

---

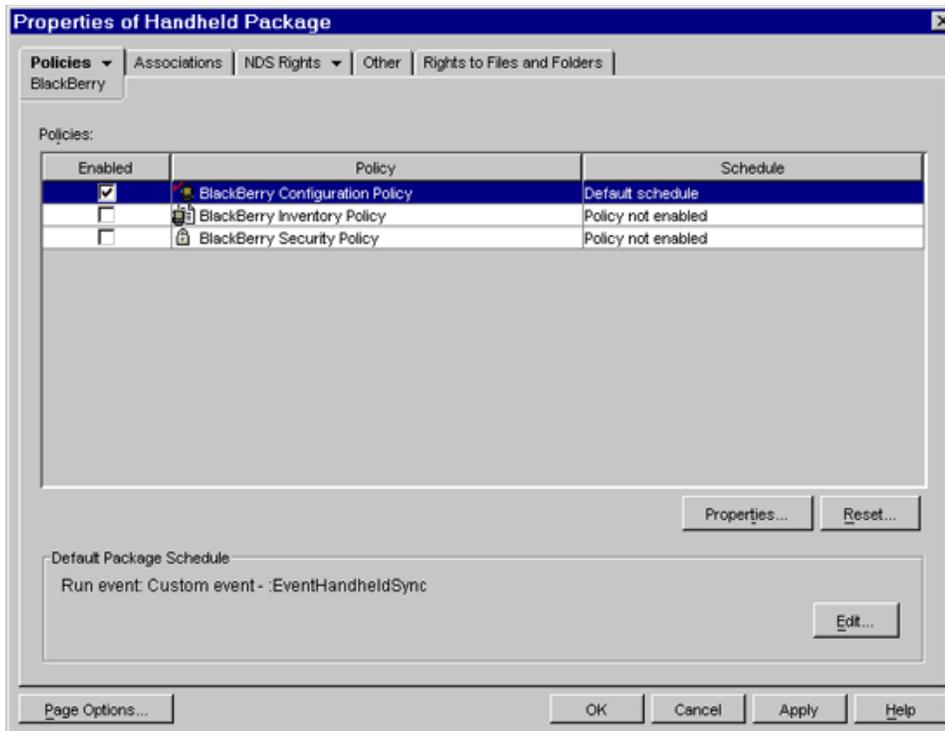
**NOTE:** This policy is not supported for Java-based BlackBerry devices.

---

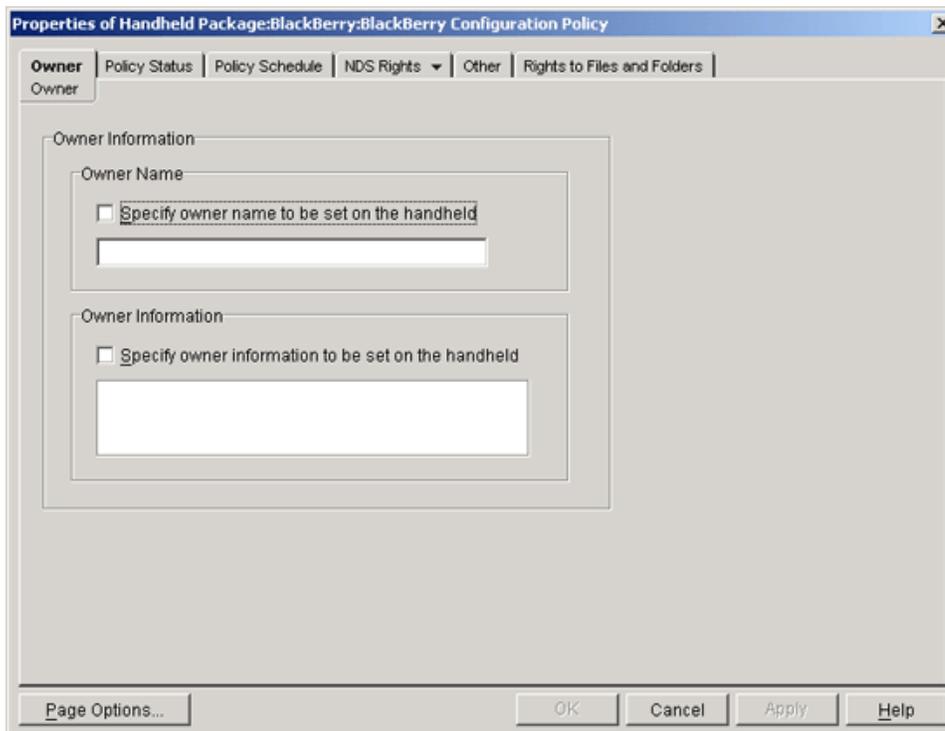
The owner name and information that you specify using this policy does not affect the naming of the device objects in eDirectory; the owner name and information you specify in this policy displays only on the actual device.

To set up the BlackBerry Configuration policy:

- 1** In ConsoleOne, right-click the *Handheld Package* or *Handheld User Package* object, then click *Properties*.
- 2** On the *Policies* tab, click the down-arrow, then click *BlackBerry*.
- 3** Select the check box under the *Enabled* column for the BlackBerry Configuration policy.  
This both selects and enables the policy.



4 Click *Properties* to display the *Owner* page.



5 Fill in the fields:

**Owner Name:** Select the *Specify Owner Name To Be Set on the Handheld* check box, then type the owner name that you want to be set on associated BlackBerry devices.

**Owner Information:** Select the *Specify Owner Information To Be Set on the Handheld* check box, then type any additional information that you want to be set on associated BlackBerry devices.

The owner name and information that you specify using this policy does not affect the naming of the device objects in Novell eDirectory; the owner name and information you specify in this policy displays only on the actual device.

- 6 Click *OK* to save the policy.
- 7 When you have finished configuring all of the policies for this package, continue with the steps under [“Associating the Handheld Package or the Handheld User Package” on page 73](#) to associate the policy package.
- 8 If desired, schedule the policy. For more information, see [“Scheduling Packages and Policies” on page 74](#).

---

**NOTE:** For BlackBerry devices, a policy schedule of Custom Event:EventHandheldSync gets translated on the device to Daily.

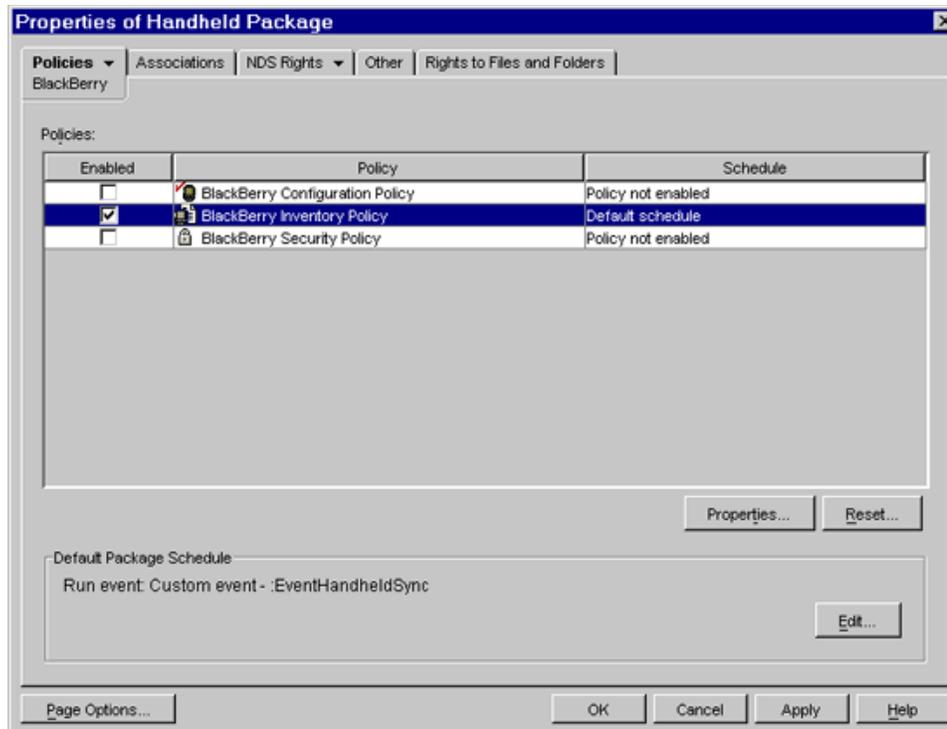
---

## 2.4.2 BlackBerry Inventory Policy

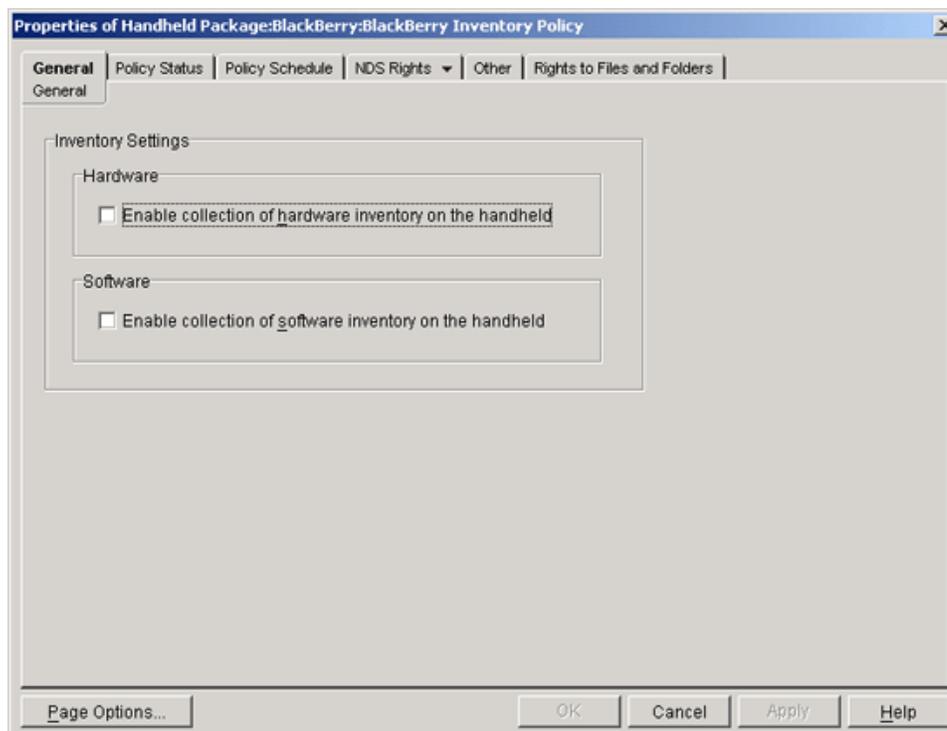
The BlackBerry Inventory policy lets you enable the collection of hardware and software inventory from associated BlackBerry devices.

To set up the BlackBerry Inventory policy:

- 1 In ConsoleOne, right-click the *Handheld Package* or the *Handheld User Package* object, then click *Properties*.
- 2 On the *Policies* tab, click the down-arrow, then click *BlackBerry*.
- 3 Select the check box under the *Enabled* column for the BlackBerry Inventory policy.  
This both selects and enables the policy.



4 Click *Properties* to display the *General* page.



5 Fill in the fields:

**Hardware:** To collect hardware information for associated BlackBerry devices, select the *Enable Collection of Hardware Inventory on the Handheld* check box.

Collected data about hardware is stored on a per-device basis and is found on the ZENworks Inventory page in ConsoleOne or on the Clients: Hardware Inventory page in the ZENworks Handheld Management Inventory Viewer. To view the ZENworks Inventory page in ConsoleOne, right-click a handheld device object, click *Properties*, then click the *ZENworks Inventory* tab. To open the ZENworks Handheld Management Inventory Viewer, right-click a handheld device object, click *Actions*, then click *Inventory*. For more information, see [Section 5.2, “Viewing Hardware Inventory,” on page 118](#).

**Software:** To collect software information for associated BlackBerry devices, select the *Enable Collection of Software Inventory on the Handheld* check box.

Collected data about software is found in the ZENworks Handheld Management Inventory Viewer. To open the ZENworks Handheld Management Inventory Viewer, right-click a handheld device object, click *Actions*, then click *Inventory*. You can view software inventory information for a specific device or across all BlackBerry devices in your system. For more information, see [Section 5.1, “Viewing Software Inventory,” on page 108](#).

- 6 Click *OK* to save the policy.
- 7 When you have finished configuring all of the policies for this package, continue with the steps under [“Associating the Handheld Package or the Handheld User Package” on page 73](#) to associate the policy package.
- 8 If desired, schedule the policy. For more information, see [“Scheduling Packages and Policies” on page 74](#).

---

**NOTE:** You must schedule inventory for BlackBerry devices because they are always connected to the ZENworks Handheld Management Server. For Palm and Windows CE devices, you do not need to schedule inventory; software inventory is collected once a day.

For BlackBerry devices, a policy schedule of Custom Event:EventHandheldSync gets translated on the device to Daily.

---

### 2.4.3 BlackBerry Security Policy

The BlackBerry Security policy lets you ensure that a password is set on associated BlackBerry devices. You can also use the BlackBerry Device Lockout feature to lock a device that you suspect has been lost or stolen. For more information, see [“BlackBerry Device Lockout” on page 36](#).

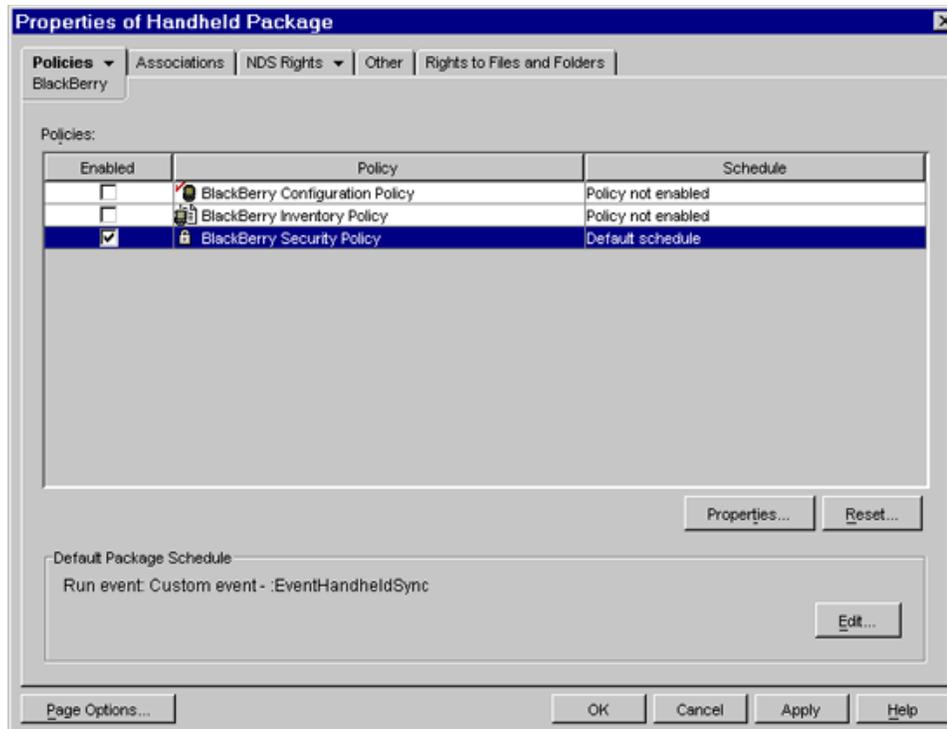
---

**NOTE:** This policy is not supported for Java-based BlackBerry devices.

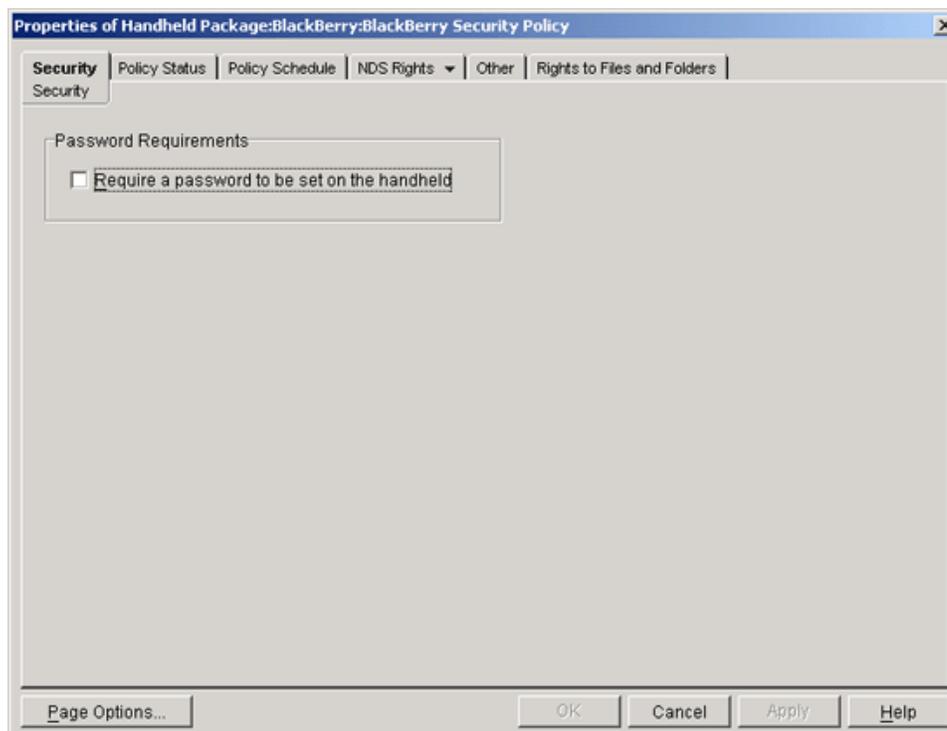
---

To set up the BlackBerry Security policy:

- 1 In ConsoleOne, right-click the *Handheld Package* or *Handheld User Package* object, then click *Properties*.
- 2 On the *Policies* tab, click the down-arrow, then click *BlackBerry*.
- 3 Select the check box under the *Enabled* column for the BlackBerry Security policy.  
This both selects and enables the policy.



4 Click *Properties* to display the *Security* page.



5 Select the *Require a Password To Be Set On the Handheld* check box.

If your organization has a rule stating that all handheld devices must have a password, you should enable this policy.

When the BlackBerry Security policy is enforced, if the user does not have a password set, he or she is prompted to create one. If the user ignores the prompt, he or she is prompted every 15 minutes to create a password for the device.

- 6 Click *OK* to save the policy.
- 7 When you have finished configuring all of the policies for this package, continue with the steps under [“Associating the Handheld Package or the Handheld User Package” on page 73](#) to associate the policy package.
- 8 If desired, schedule the policy. For more information, see [“Scheduling Packages and Policies” on page 74](#).

---

**NOTE:** For BlackBerry devices, a policy schedule of Custom Event:EventHandheldSync gets translated on the device to Daily.

---

## BlackBerry Device Lockout

The BlackBerry Device Lockout feature lets you disable a BlackBerry device if you suspect that it has been lost or stolen. After the device is locked, no applications can run on the device other than ZENworks Handheld Management, which can be used to unlock the device.

To lock or unlock a BlackBerry device:

- 1 In ConsoleOne, right-click the desired BlackBerry handheld device object, click *Actions*, then click *Lock/Unlock Device*.
- 2 Click *Unlock the Device*.  
or  
Click *Lock the Device*, then type the text you want displayed on the device when in is locked.
- 3 Click *OK*.

## 2.4.4 Palm Client Configuration Policy

The Palm Client Configuration policy lets you override the user authentication settings of the ZENworks Handheld Management Service object for associated Palm OS devices.

You can set up user authentication on a global basis for all handheld devices in your ZENworks Handheld Management system during installation or you can edit the properties of the ZENworks Handheld Management Service object.

If you do not want to enable user authentication for all handheld devices in your system, you can choose to not enable global user authentication during installation or by editing the properties of the ZENworks Handheld Management Service object. You can then configure and enable the Palm Client Configuration policy by following the procedure in this section to target only specific handheld devices or groups of handheld devices.

For more information about setting up user authentication on a global basis during installation, see [“Installing the ZENworks Handheld Management Server”](#) in the *Novell ZENworks 7 Handheld Management Installation Guide*. For more information about editing the properties of the ZENworks Handheld Management Service object to enable global user authentication, see [Section 7.1, “Configuring User Authentication,” on page 129](#).

If user authentication is enabled, the user is prompted for his or her credentials (username and password) the first time the device connects/synchronizes. ZENworks Handheld Management then authenticates the user using LDAP to log in to the directory. After the user is authenticated, you can target policies and applications to the user of the handheld device.

The user must enter the credentials only once; ZENworks Handheld Management does not prompt the user for the credentials again. If a user that has been authenticated gives the device to another person, you should reconfigure the user on the device itself. For more information, see the documentation that came with your handheld device.

If the device uses the Palm IP client to connect, the user-authentication dialog box displays on the handheld device. If the device uses Palm HotSync, the user-authentication dialog box displays on the desktop computer during synchronization. When the user is prompted for authentication, if he or she clicks Cancel, the handheld device can be managed by device policies, but user-based management does not function because the user is not authenticated. If the user mis-types the username or password, he or she is immediately prompted for the credentials again.

---

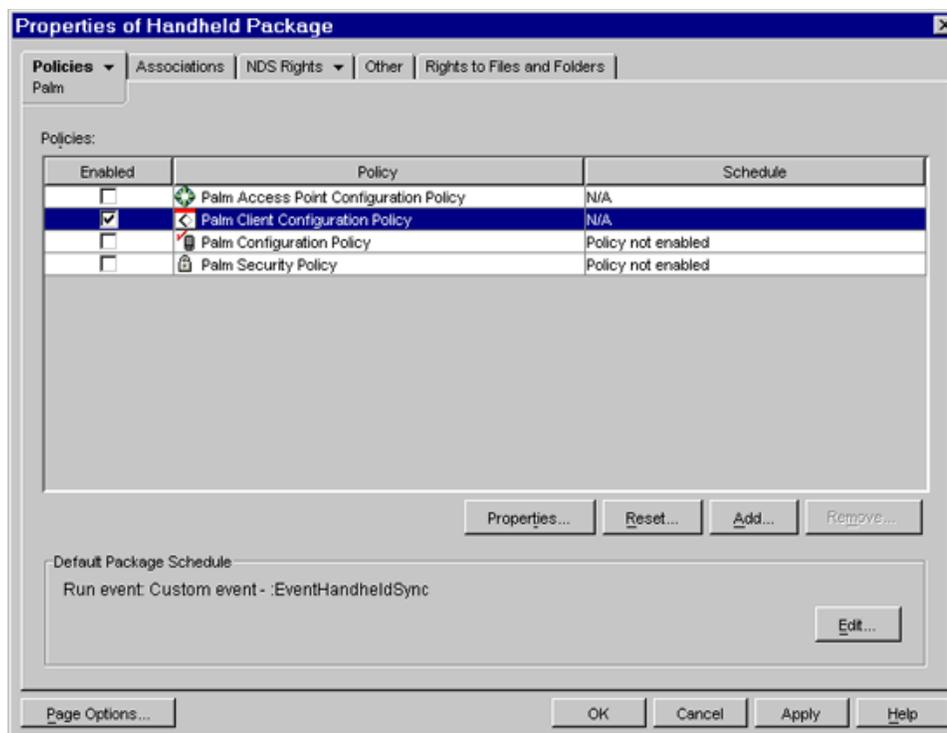
**NOTE:** There are two places in ZENworks Handheld Management where users can be required to enter a password: to authenticate to the directory as part of the Palm Client Configuration policy and to power on a handheld device as part of the Palm Security policy. These two passwords are independent of each other. For more information about the password users must enter to power on a device, see [“Palm Security Policy” on page 48](#).

---

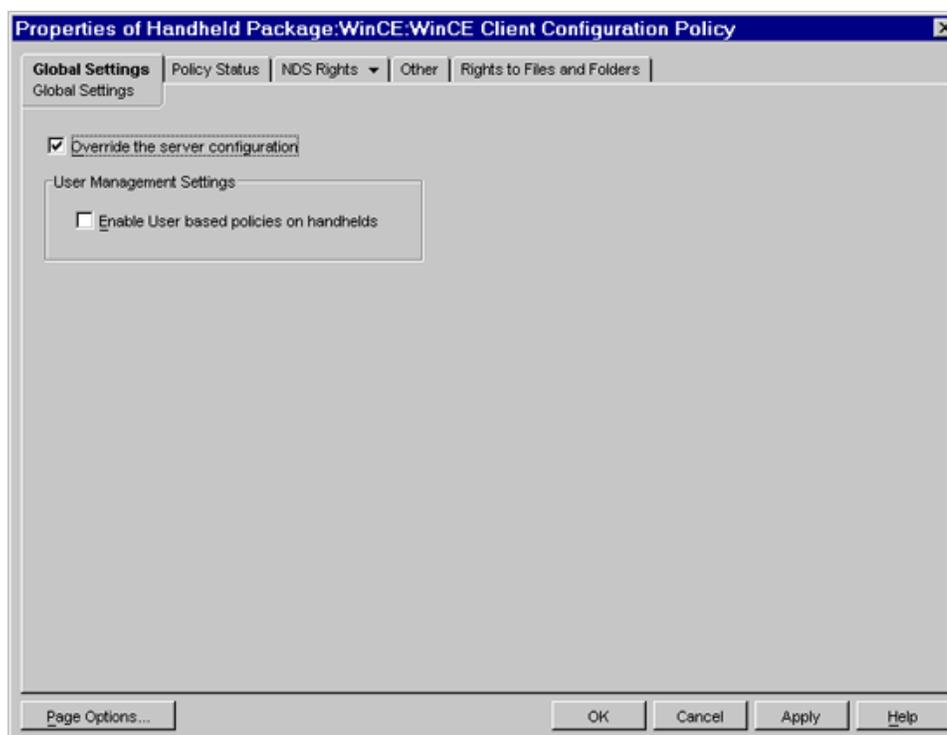
To set up the Palm Client Configuration policy:

- 1 In ConsoleOne, right-click the Handheld Package object, then click *Properties*.
- 2 On the Policies tab, click the down-arrow, then click *Palm*.
- 3 Select the check box under the *Enabled* column for the Palm Client Configuration policy.

This both selects and enables the policy.



- 4 Click *Properties* to display the *Global Settings* page.
- 5 To override the user authentication settings of the ZENworks Handheld Management Service object, Select the *Override the Server Configuration* option.



- 6 Select the *Enable User Based Policies on Handhelds* option.
- 7 Click *OK* to save the policy.
- 8 When you have finished configuring all of the policies for this package, continue with the steps under “[Associating the Handheld Package or the Handheld User Package](#)” on page 73 to associate the policy package.

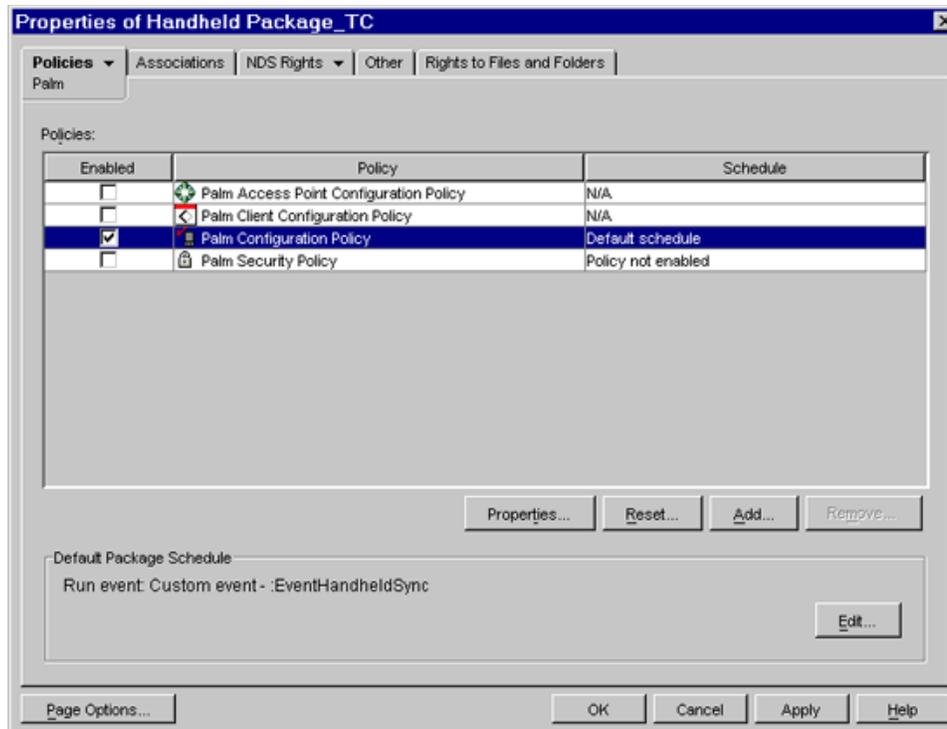
## 2.4.5 Palm Configuration Policy

The Palm Configuration policy lets you configure the following:

- ♦ **General Preferences:** Lets you set preferences for associated Palm OS devices, for example how long before an idle device turns itself off, whether or not a device stays on when cradled, and more.
- ♦ **Buttons:** Lets you associate different software programs with the buttons on associated Palm OS devices. Also lets you assign a feature users can access when they drag the pen from the writing area to the top of the screen on the Palm OS device. For example, you can select *Turn Off & Lock* to make it easier for users to turn off and lock their Palm OS devices.
- ♦ **Programs:** Lets you specify which software programs are allowed or not allowed on associated Palm OS devices. Programs that are not allowed can be automatically removed from the devices.
- ♦ **Files:** Lets you specify the files to be automatically deleted from the Palm devices.

To set up the Palm Configuration policy:

- 1 In ConsoleOne, right-click the Handheld Package or Handheld User Package object, then click *Properties*.
- 2 On the *Policies* tab, click the down-arrow, then click *Palm*.
- 3 Select the check box under the *Enabled* column for the Palm Configuration policy.  
This both selects and enables the policy.



- 4 Click *Properties*.
- 5 On the *General* page, make the desired configuration changes, then click *Apply*.

You can change the settings for the following preferences:

- ◆ *Auto-Off After*
- ◆ *Stay On in Cradle*
- ◆ *System Sound*
- ◆ *Alarm Sound*
- ◆ *Alarm Vibrate*
- ◆ *Alarm LED*
- ◆ *Game Sound*
- ◆ *Beam Receive*

Each preference in the list contains a *Don't Change* setting. If you choose this setting, ZENworks Handheld Management does not change that preference on associated devices; the corresponding setting on each device determines its behavior. For example, if you choose the *Don't Change* setting for *Auto-Off After*, each associated device uses its own preference settings to determine how long an idle Palm OS device waits until it turns itself off. If you want to ensure consistency across all associated Palm OS devices, choose the appropriate setting.

- 6 On the *Buttons: Configuration* page, make the desired configuration changes, then click *Apply*.  
The Button Column lists the available buttons on the Palm OS device. To change a button's association, select a button from the *Button* list, click *Edit*, click *Set to Application*, browse to an application, then click *OK*.

---

**NOTE:** Depending on your particular Palm OS device, the available buttons in the *Button* list are named differently than those in the preceding illustration.

---

The *Pen Function* drop-down list lets you assign a feature users can access when they drag the pen from the writing area to the top of the screen on the Palm OS device. For example, you can select *Turn Off & Lock* to make it easier for users to turn off and lock their Palm OS devices. To assign a feature, choose an option from the drop-down list.

The following options are available:

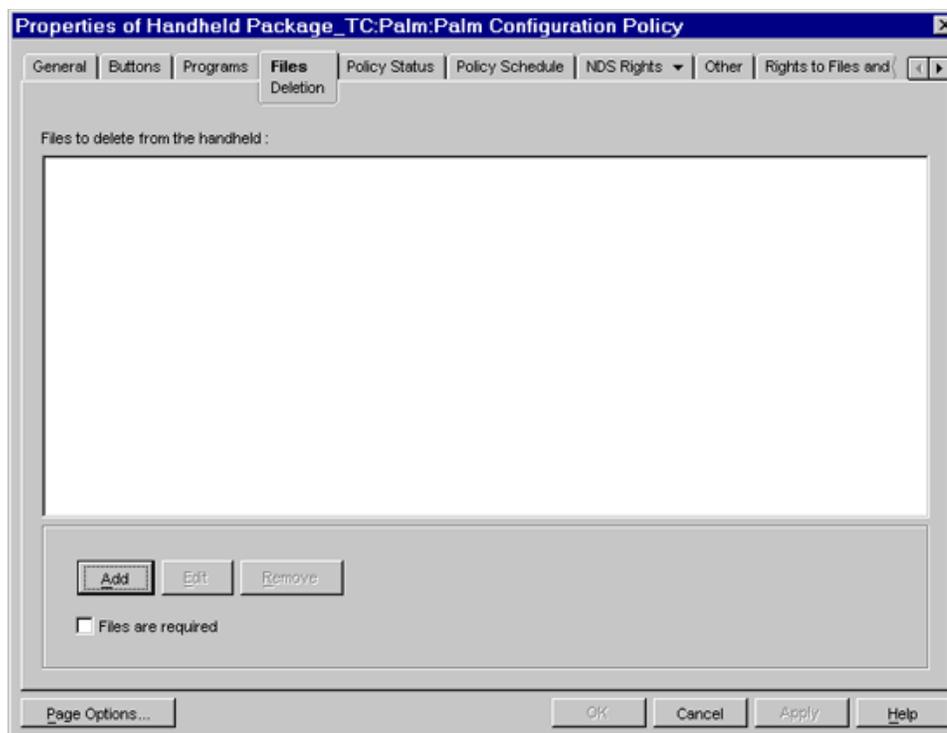
- ◆ *Not Specified*
- ◆ *Backlight*
- ◆ *Keyboard*
- ◆ *Graffiti Help*
- ◆ *Turn Off & Lock*
- ◆ *Beam Data*

**7** On the *Programs* page, make the desired configuration changes, then click *Apply*.

The *Application* column lists the applications that you want to allow on the device or remove from the device.

- ◆ To add an application to the list, click *Add*, specify or browse to the application, select one of the following rules to apply to the application, then click *OK*.
  - ◆ *Allow the Application on the Handheld*
  - ◆ *Remove the Application from the Handheld*
- ◆ Rather than selecting certain applications to be removed from the device, you might find it easier to specify a list of allowed applications and select the *Remove All Other Applications from the Handheld* check box. When the policy is enforced or when the user synchronizes the device, all applications not listed in the *Applications* list with the Allow rule set are removed from the device.
- ◆ If the application listed in the *Application* column list is to be added or removed from storage card, select the *Search for Application on Storage Cards* check box.

**8** On the *Files* page, do the following:



- 8a** Click *Add*.
- 8b** In the Add Files to Delete from Handheld dialog box, specify the name of the file to be deleted.

The filename is added to the *Files to Delete from the Handheld* list.

Ensure that the name of the application matches the file properties name because the name displayed in the Application Launcher screen might not be the actual filename. To determine the actual filename, you need to use a third-party application such as FileZ, a shareware application.
- 8c** Click *OK*.
- 8d** (Optional) Select the *Files are Required* option if you want Handheld Management to report a failed status if the specified files do not exist on the handheld device or if the specified wildcard characters do not provide a match for files on the device.
- 8e** Click *Apply*, then click *Close*.
- 9** Click *OK* to save the policy.
- 10** When you have finished configuring all of the policies for this package, continue with the steps under [“Associating the Handheld Package or the Handheld User Package” on page 73](#) to associate the policy package.
- 11** If desired, schedule the policy. For more information, see [“Scheduling Packages and Policies” on page 74](#).
- 12** (Optional) To ensure that the Handheld Management Server immediately receives the new policy changes, right-click the Handheld service object, then click *Scan Now*.

## 2.4.6 Palm Access Point Configuration Policy

The Palm Access Point Configuration Policy lets you assign multiple ZENworks Handheld Management Access Points to a device and also define the order of the ZENworks Handheld Management Access Points to which the Palm OS device must connect. If the device is unable to connect to the ZENworks Handheld Management Access Point configured first, then it automatically tries to connect to the ZENworks Handheld Management Access Point configured next in the sequence.

---

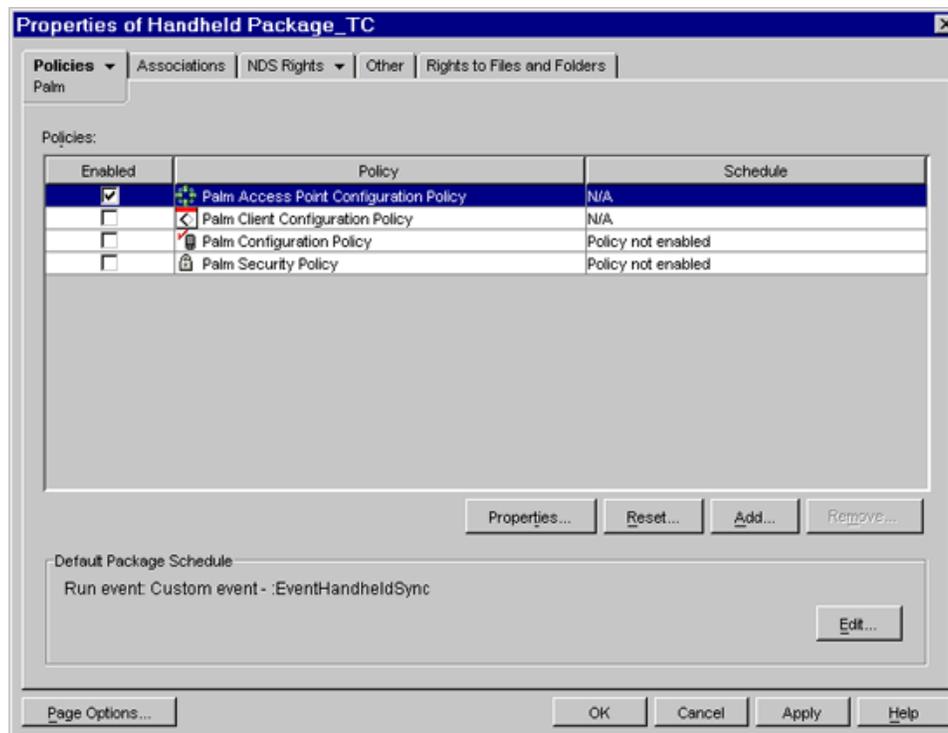
**NOTE:** The Palm Access Point Configuration policy is not supported on cradled Palm devices.

---

To configure the Palm Access Point Configuration Policy:

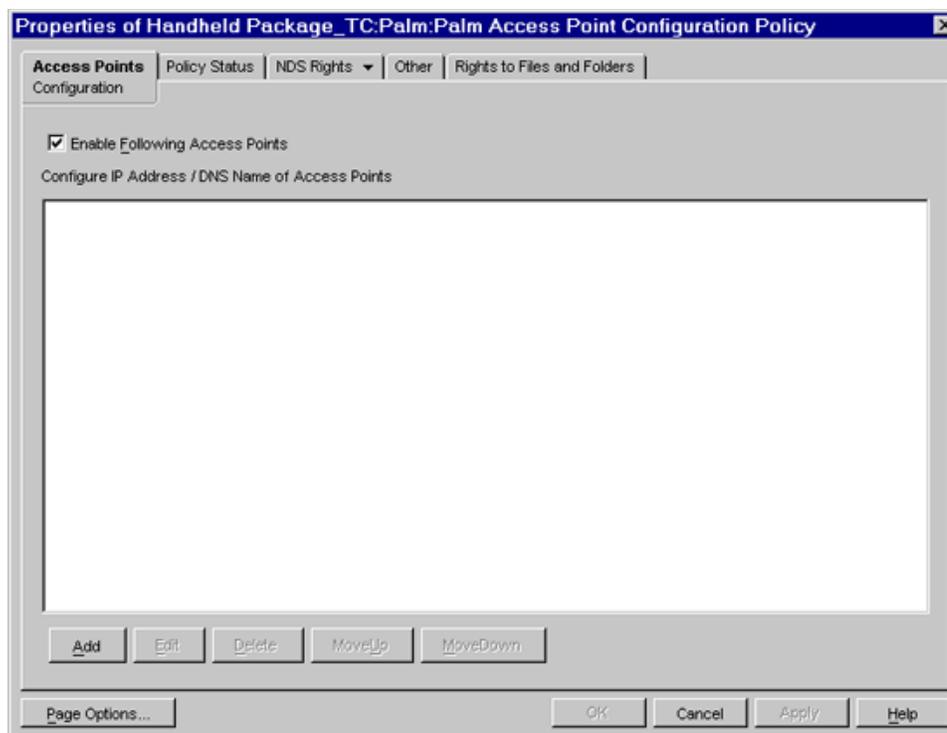
- 1 In ConsoleOne, right-click the Handheld Package or Handheld User Package object, then click *Properties*.
- 2 On the *Policies* tab, click the down-arrow, then click *Palm*.
- 3 Select the check box under the *Enabled* column for the Palm Access Point Configuration policy.

This both selects and enables the policy.



- 4 Click *Properties*.

This displays the *Access Points - Configuration* page.



- 5 In the *Access Points - Configuration* page, do the following:
  - 5a If you want to add the ZENworks Handheld Management Access Points to the *Configure IP Address /DNS Name of Access Points* list, and define the order of the ZENworks Handheld Management Access Points to which the handheld device must connect to, select the *Enable Following Access Points* option.  
If you do not select this check box, the ZENworks Handheld Management Access Points list is not available on the handheld device.
  - 5b Click *Add*.
  - 5c In the Add Access Points dialog box, specify the IP address or the full DNS name of the ZENworks Handheld Management Access Point, or click *Select*. If you specify the IP address or the full DNS of the ZENworks Handheld Management Access Point, skip to **Step 5h**.
  - 5d By default, the service object of the Handheld Management server is displayed. To select another service object, click the *Browse* icon, select the service object, then click *OK*.
  - 5e Click *Display*.  
The IP address of the ZENworks Handheld Management Access Points associated with service object is displayed
  - 5f From the *Access Points* list, select the IP address of the ZENworks Handheld Management Access Point to which you want to connect the device.
  - 5g Click *OK*.  
The ZENworks Handheld Management Access Points IP address followed by a semicolon (;) is displayed in the Access Points option.
  - 5h (Optional) To add another ZENworks Handheld Management Access Point, repeat **Step 5c** through **Step 5g**.

You can add a maximum of eight ZENworks Handheld Management Access Points IP addresses, but ensure that the IP addresses or the DNS names of the ZENworks Handheld Management Access Points are separated with semicolons (;).

- 5i** Click *Apply*.
- 6** (Optional) To change the order of the ZENworks Handheld Management Access Points in the *Configure IP Address /DNS Name of Access Points* list:
  - 6a** Select the IP address or the full DNS name of the ZENworks Handheld Management Access Point.
  - 6b** Click *Move Up* or *Move Down*.
- 7** (Optional) To modify the value of an ZENworks Handheld Management Access Point displayed in the *Configure IP Address /DNS Name of Access Points* list:
  - 7a** Select the IP address or the full DNS name of the ZENworks Handheld Management Access Point whose value you want to modify.
  - 7b** Click *Edit*.
  - 7c** In the Edit Access Points dialog box, change the value of the ZENworks Handheld Management Access Point.
  - 7d** Click *OK*.
- 8** Click *Apply*, then click *Close* to save the policy.
- 9** Associate the policy package.

For more information on how to associate the policy package, see the [“Associating the Handheld Package or the Handheld User Package” on page 73](#).
- 10** If desired, schedule the policy.

For more information on how to schedule a policy, see the [“Scheduling Packages and Policies” on page 74](#).
- 11** (Optional) To ensure that the Handheld Management Server immediately receives the new policy changes, right-click the Handheld service object, then click *Scan Now*.

---

**IMPORTANT:** If you push `zfhpcclient.pdb` after enforcing the Palm Access Point Configuration policy on the device, the Palm Access Point Configuration policy settings are removed. You must reconfigure the policy.

---

## 2.4.7 Palm File Retrieval Policy

The Palm File Retrieval policy lets you specify source files you want to retrieve from a Palm OS device and copy to a specified destination location.

The File Retrieval policy is a plural policy, meaning it can be added many times to a policy package. You can set up as many File Retrieval policies as required to adequately retrieve important files from the handheld devices in your organization. When you name these plural policies, be sure to give them descriptive names.

The File Retrieval policy is also cumulative, meaning that many different Palm File Retrieval policies can be effective for a single handheld device object, handheld group object, or container object.

---

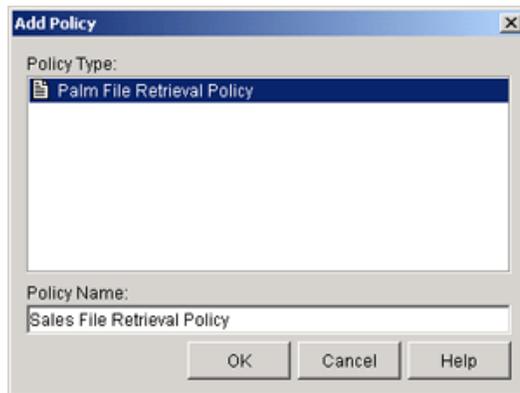
**NOTE:** If you want to retrieve files from handheld devices and store them on a Novell NetWare<sup>®</sup> volume, you must install the Novell Client<sup>™</sup> on the ZENworks Handheld Management Server.

---

To set up the Palm File Retrieval policy:

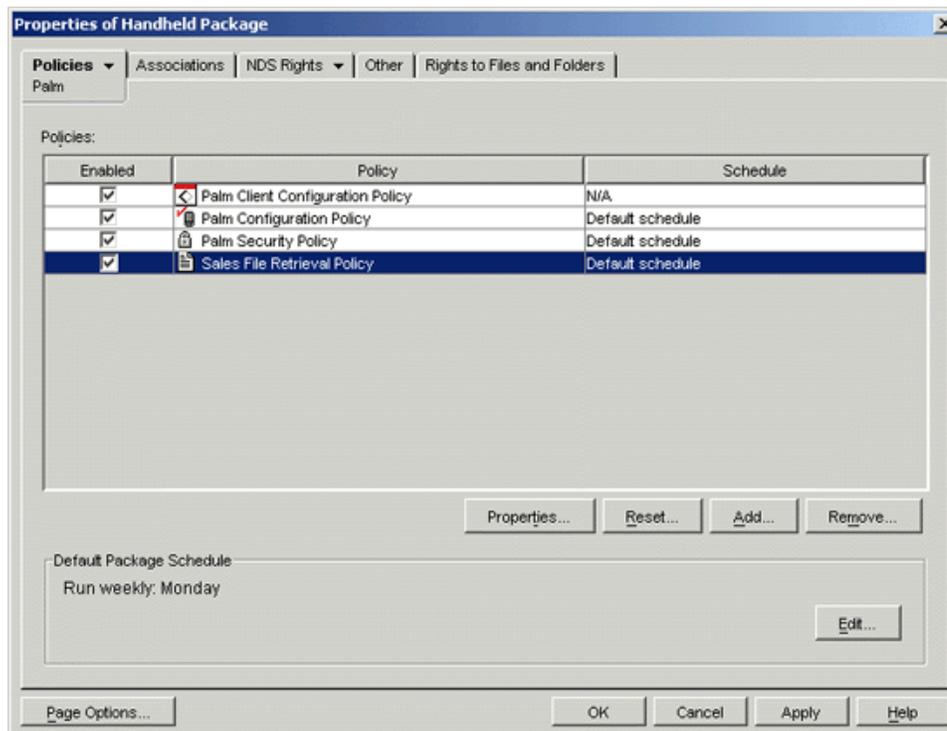
- 1 In ConsoleOne, right-click the Handheld Package object or the Handheld User Package object, then click *Properties*.
- 2 On the *Policies* tab, click the down-arrow, then click *Palm*.
- 3 Click *Add*.

The Add Policy window is displayed.

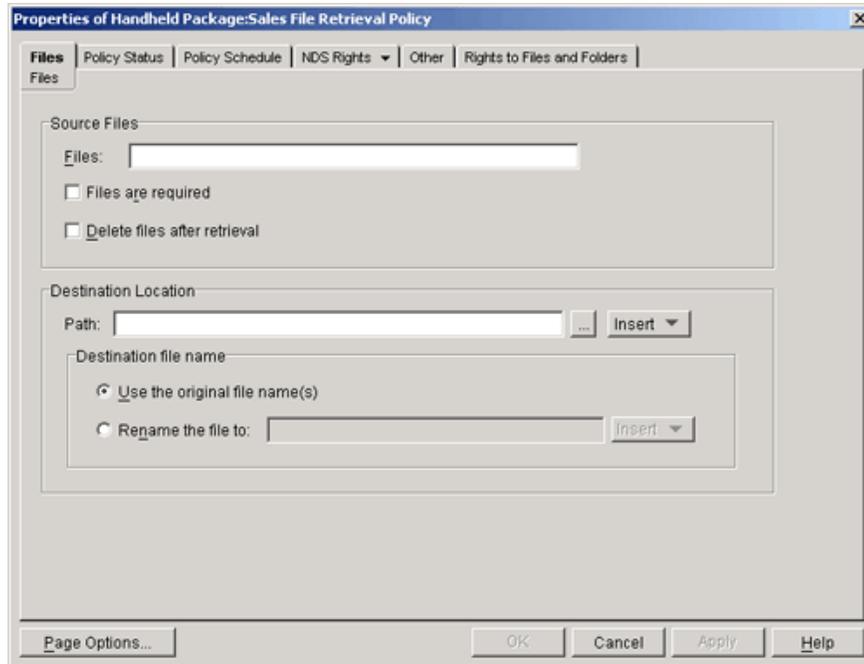


- 4 Type a descriptive name in the *Policy Name* field, then click *OK*.

The newly created File Retrieval policy is displayed in the Handheld Policies list.



- 5 Select the check box under the *Enabled* column for the newly created Palm File Retrieval policy.  
This both selects and enables the policy.
- 6 Click *Properties* to display the *Files* page.



- 7 In the *Files* field, specify the source files to be retrieved from the handheld device.

---

**NOTE:** You must specify the Palm database or resource filename in the Files field. A third-party file utility tool (such as FileZ, a shareware program) might be necessary to determine the actual filename.

---

When you specify source files, be aware that filenames are case sensitive. You can use wildcard characters to specify source files.

When the policy is enforced, all specified source files are retrieved from the device; the files are retrieved even if the same files were previously retrieved at another time.

- 8 Select the *Files Are Required* check box if you want ZENworks Handheld Management to report a failed status if the specified files do not exist on the handheld device or if the specified wildcard characters do not provide a match for files on the device.

For more information about policy status, see [Section 2.6, “Viewing Policy Status Information,” on page 76](#).

- 9 Select the *Delete Files After Retrieval* check box if you want the specified source files to be deleted from the handheld device after they have been retrieved from the handheld device.

If you do not enable this option, the source files are copied to the specified location but a copy also remains on the handheld device.

- 10 In the *Path* field, browse to or specify the destination location where you want the specified files copied to.

The renamed file can include variables. To include variables, click the *Insert* button, then click the desired variable.

The following variables are available for use:

Variable	Description
<i>device</i>	The CN of the device. For example, in Dan m130.Handhelds.NovellBangalore, the string would be Dan m130.
<i>devicedn</i>	The full DN of the device. For example, In Dan m130.Handhelds.NovellWheaton, the string would be Dan m130.Handhelds.NovellWheaton.
<i>user</i>	The username of the device. This is the value stored in the UserName attribute for the object in the directory. When this value is not configured on the handheld device, it is set to <Undefined>.
<i>date</i>	The date the file was retrieved from the handheld device. This value is the date only; the time that the file was retrieved is not included. For example, if the file was retrieved on September 15, 2002 at 3:15 p.m., the string would be 2002-09-15. The string is always in the format of yyyy-mm-dd.
<i>time</i>	The time the file was retrieved from the handheld device. This value is for the time only; the date that the file was retrieved is not included. For example, if a file was retrieved on September 15, 2002 at 3:20 p.m., the string would be 15-20. The string is always in the format of hh-mm, with hh representing the hour in 24-hour format.
<i>guid</i>	The GUID for the handheld device.
<i>server</i>	The name of the Windows NT server that received the data.

To use a variable, place an @ sign on either side of the variable in the string. For example, you could use the following syntax:

@user@\_filename

- 11 Select *Use the Original File Name(s)* to use the original source filenames for the destination files.  
or  
Select *Rename the Files To* and specify new filenames for the destination files.
- 12 Click *OK* to save the policy.
- 13 When you have finished configuring all of the policies for this package, continue with the steps under [“Associating the Handheld Package or the Handheld User Package” on page 73](#) to associate the policy package.
- 14 If desired, schedule the policy. For more information, see [“Scheduling Packages and Policies” on page 74](#).

## 2.4.8 Palm Security Policy

The Palm Security policy lets you configure the following:

- ♦ **Password Requirements:** Lets you ensure that a password is set on the associated Palm devices, and also lets you set a user’s password as the device password, configure enhanced security options, such as the number of days to allow before a password expires, the number of grace logins permitted before the user must change the password, the minimum number of

characters to allow for the password, and whether the password must contain a mix of letters and numbers. For devices running Palm OS 4.x or newer, you can also configure auto-lock options.

---

**IMPORTANT:** Before configuring the policy, you must configure the containers to be searched to authenticate the handheld user credentials. You can do it either during the ZENworks 7 Handheld Management server installation or after the installation.

To configure user authentication during the installation, you must select the Enable User Authentication option, and specify the containers to search for user objects.

To configure user authentication after the installation, see [Section 7.1, “Configuring User Authentication,”](#) on page 129.

---

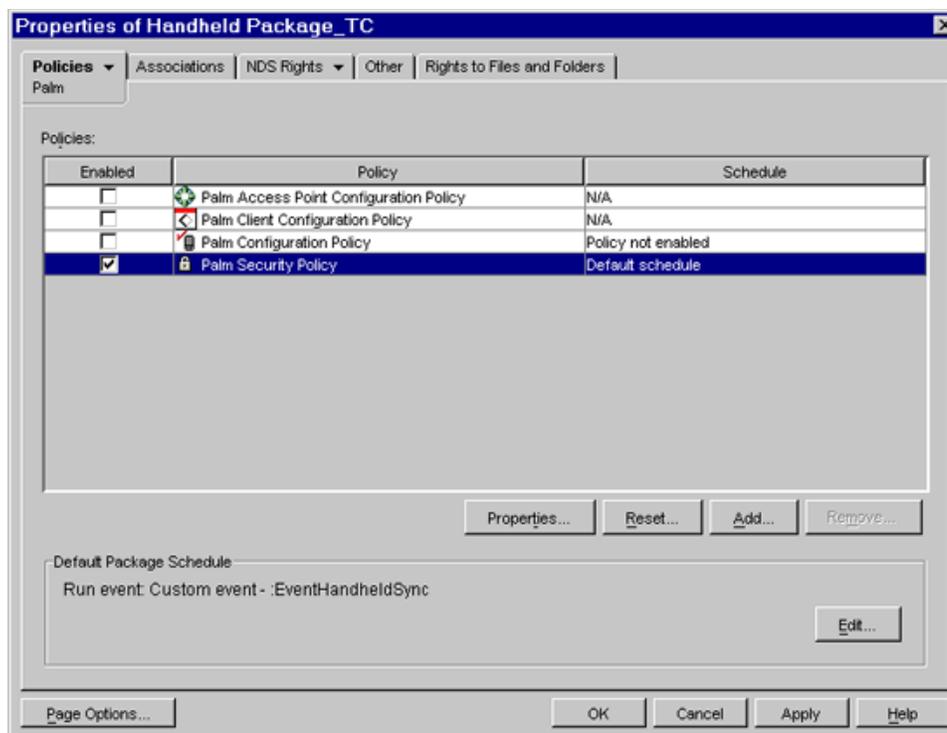
There are two places in ZENworks Handheld Management where users can be required to enter a password: to authenticate to the directory as part of the Palm Client Configuration policy and to power on a handheld device as part of the Palm Security policy. These two passwords are independent of each other. For more information about the password users must enter to authenticate to the directory, see [Section 2.4.4, “Palm Client Configuration Policy,”](#) on page 36.

- ♦ **Self-Destruct Settings:** Lets you specify self-destruct settings to disable a Palm device after a specified number of failed password attempts or after a specified number of days since the device was last connected or synchronized.

To set up the Palm Security policy:

- 1 In ConsoleOne, right-click the Handheld Package or Handheld User Package object, then click *Properties*.
- 2 On the *Policies* tab, click the down-arrow, then click *Palm*.
- 3 Select the check box under the *Enabled* column for the Palm Security policy.

This both selects and enables the policy.



4 Click *Properties* to display the *Security* page.

5 In the *Security* page, do the following:

**5a** To set a password on the Palm OS device, select the *Require a Password to Be Set on the Handheld* option.

This option lets you specify that a password must be set on the Palm OS device. If your organization has a rule that states that all handheld devices must have a password, you should enable this policy. If a user does not have a password set, he or she is prompted to create one.

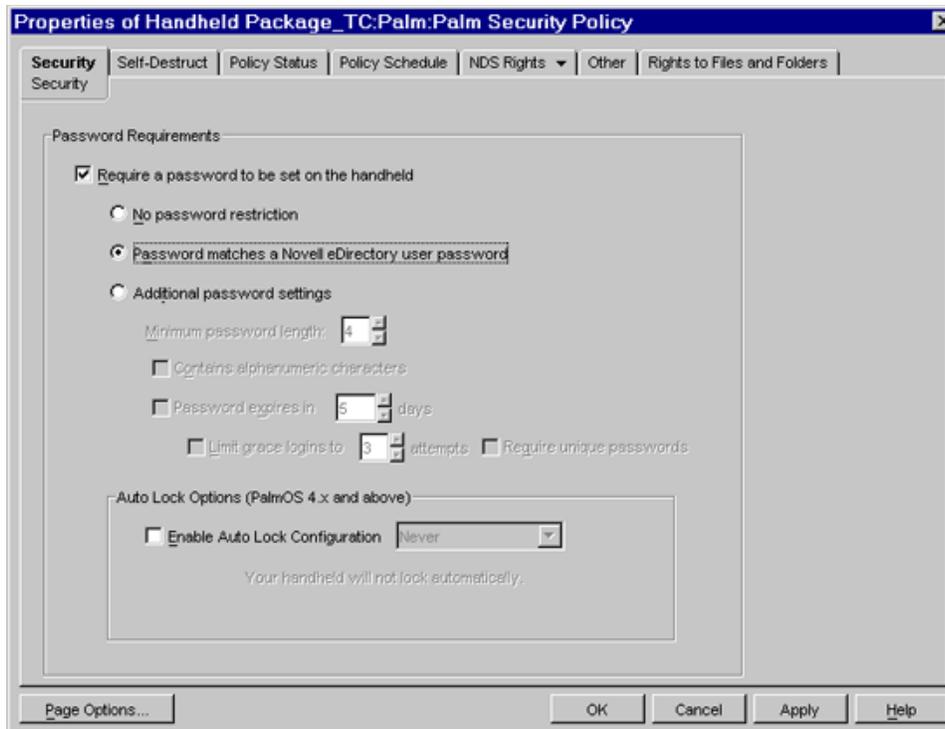
For Palm OS devices, ZENworks Handheld Management replaces the Palm password applet if you select *Require a Password to Be Set on the Handheld*; users see ZENworks Handheld Management password dialog boxes rather than the default Palm OS dialog boxes.

**5b** (Conditional) To set a user's network password as the device password, select the *Password Matches a Novell eDirectory User Password* option.

---

**WARNING:** If you forget your network password, you cannot access the Handheld device. You can access the device only by Hard Reset but this erases all data on the device.

---



- 5c** (Conditional) To configure enhanced security options, select Additional Password Settings, and configure the following options:
- ◆ **Minimum Password Length:** Specify the minimum number of characters to allow for the password on the device. You should choose a number great enough to ensure adequate security, but small enough not to excessively burden the user.
  - ◆ **Contains Alphanumeric Characters:** Select this check box to require that the user use both letters and numbers in the password. To improve the security of a password, it should contain both letters (uppercase and lowercase) and numbers.
  - ◆ **Password Expires In \_ Days:** Select this check box and specify the number of days that you want the password to expire in. When the specified number of days has expired, the user is prompted to change the password for the device.
  - ◆ **Limit Grace Logins to \_ Attempts:** Select this check box and specify the number of grace logon attempts you want to allow the user before he or she must change the password for the device. After the number of days in Password Expires in \_ Days, the user is prompted to change the password. The user can choose to ignore this prompt and keep the same password for the number of logon attempts you specify.
  - ◆ **Require Unique Passwords:** Select this check box to require that the user enter a new password; he or she cannot reuse the previous eight passwords.
- 5d** If you want the Palm OS device to be automatically locked when a specified event occurs, select the *Enable Auto Lock Configuration* option, then select any of the following events from the drop-down list:
- ◆ *Never*
  - ◆ *On Power Off*

- ◆ *At Present Time*
- ◆ *After a Preset Delay*

---

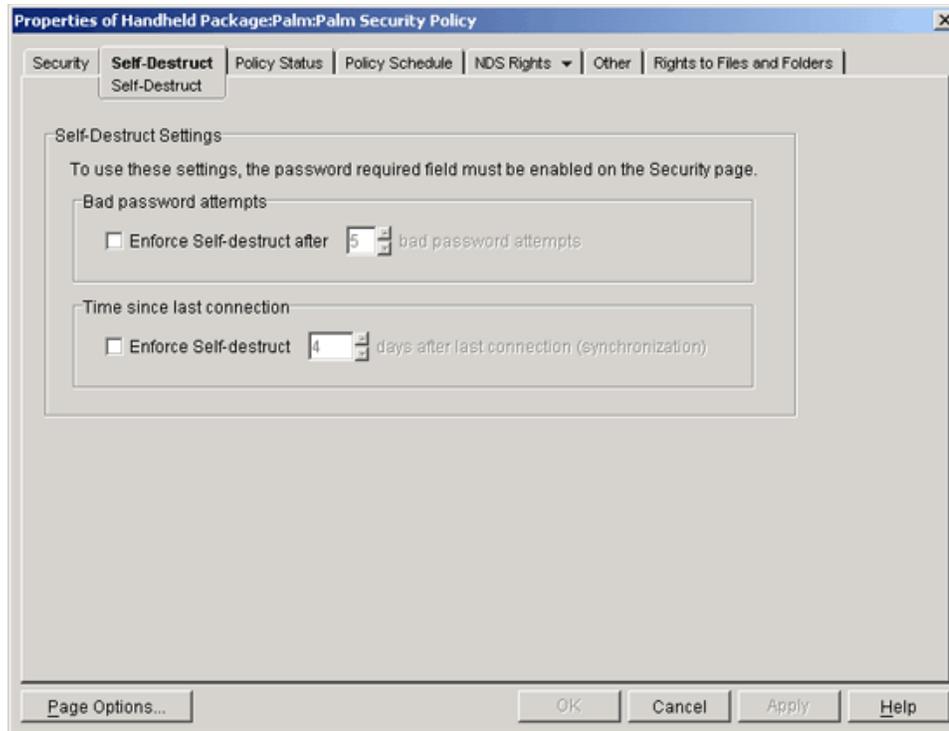
**IMPORTANT:** To use this setting, the handheld device must be running Palm OS 4.x or later.

---

Using this policy improves the security of the data on your Palm OS devices.

**5e** Click *Apply*.

**6** Click the *Self-Destruct* tab.



The *Self-destruct* page lets you configure self-destruct settings for Palm OS devices so that data is not accessible from handheld devices that are lost or stolen. When the self-destruct feature is activated, the data on the device is made unusable and the device must be manually reset, which restores the device to its out-of-the-box state.

To use the self-destruct options for Palm OS devices, you must select the *Require a Password to Be Set on the Handheld* check box on the *Security* page.

---

**IMPORTANT:** Use caution when you use the self-destruct feature. Be sure to allow an adequate number of password attempts and an adequate number of days since the last connection or synchronization to prevent data loss to users who incorrectly enter the password or do not connect or synchronize the device during a short vacation.

For Palm devices using HotSync, if the user synchronizes the device using the same desktop or laptop machine as usual, the data can be restored by HotSync.

---

7 Configure the following Self-Destruct settings:

- ♦ **Bad Password Attempts:** Select the *Enforce Self-destruct* check box and specify the number of bad password attempts to allow before activating the self-destruct feature.
- ♦ **Time Since Last Connection:** Select the *Enforce Self-Destruct* check box and specify the number of days after the last connection before activating the self-destruct feature. The *Time Since Last Connection* option refers to the last time the handheld device connected to the ZENworks Handheld Management Access Point.

Each day is made up of 24 hours. If you connect (synchronize) the device on Monday at 2 p.m. and specify three days after the last connection before activating the self-destruct feature, the self-destruct feature activates Thursday at 2 p.m (72 hours after the last connection/synchronization) unless the device is connected/synchronized during that period.

8 Click *OK* to save the policy.

9 When you have finished configuring all of the policies for this package, continue with the steps under [“Associating the Handheld Package or the Handheld User Package” on page 73](#) to associate the policy package.

10 If desired, schedule the policy. For more information, see [“Scheduling Packages and Policies” on page 74](#).

11 (Optional) To ensure that the Handheld Management Server immediately receives the new policy changes, right-click the Handheld service object, then click *Scan Now*.

## 2.4.9 WinCE Client Configuration Policy

The WinCE Client Configuration policy lets you override the user authentication settings of the ZENworks Handheld Management Service object for associated WinCE devices.

You can set up user authentication on a global basis for all handheld devices in your ZENworks Handheld Management system during installation or you can edit the properties of the ZENworks Handheld Management Service object.

If you do not want to enable user authentication for all handheld devices in your system, you can choose to not enable global user authentication during installation or by editing the properties of the ZENworks Handheld Management Service object. You can then configure and enable the WinCE Client Configuration policy by following the procedure in this section to target only specific handheld devices or groups of handheld devices.

For more information about setting up user authentication on a global basis during installation, see [“Installing the ZENworks Handheld Management Server”](#) in the *Novell ZENworks 7 Handheld Management Installation Guide*. For more information about editing the properties of the ZENworks Handheld Management Service object to enable global user authentication, see [Section 7.1, “Configuring User Authentication,” on page 129](#).

If user authentication is enabled, the user is prompted for his or her credentials (username and password). ZENworks Handheld Management then authenticates the user using LDAP to log in to the directory. After the user is authenticated, you can target policies and applications to the user of the handheld device.

If the device uses the Windows IP client to connect, the user-authentication dialog box displays on the handheld device.

When the user is prompted for authentication, if he or she clicks *Cancel*, the handheld device can be managed by device, but user-based management does not function because the user is not authenticated. If the user mis-types the username or password, he or she is immediately prompted for the credentials again.

---

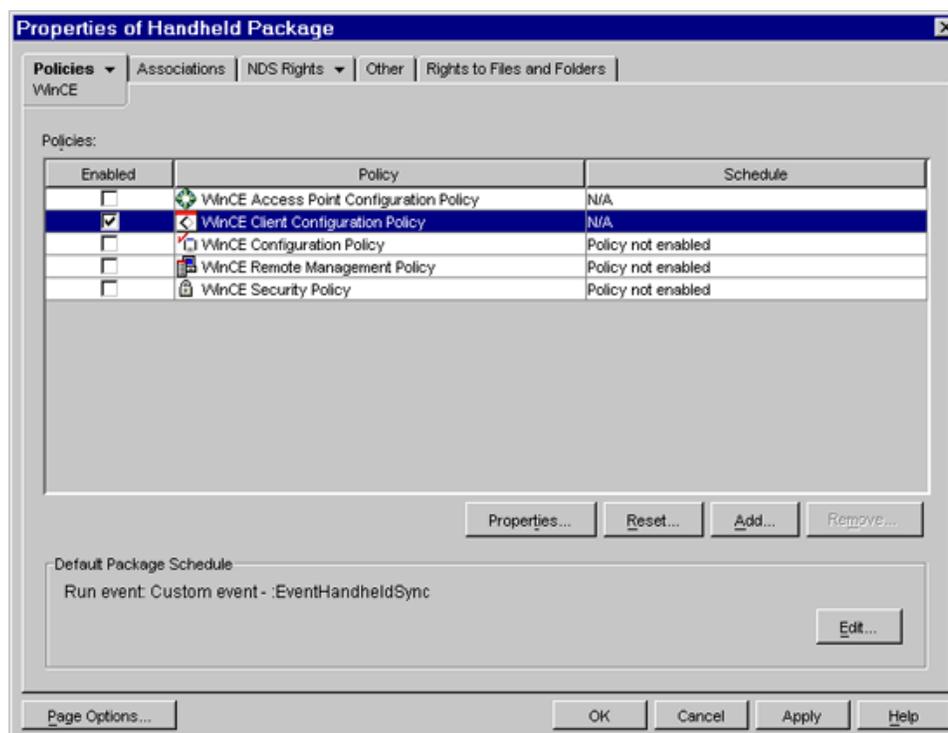
**NOTE:** There are two places in ZENworks Handheld Management where users can be required to enter a password: to authenticate to the directory as part of the WinCE Client Configuration policy and to power on a handheld device as part of the WinCE Security policy. These two passwords are independent of each other. For more information about the password users must enter to power on a device, see “[WinCE Security Policy](#)” on page 68.

---

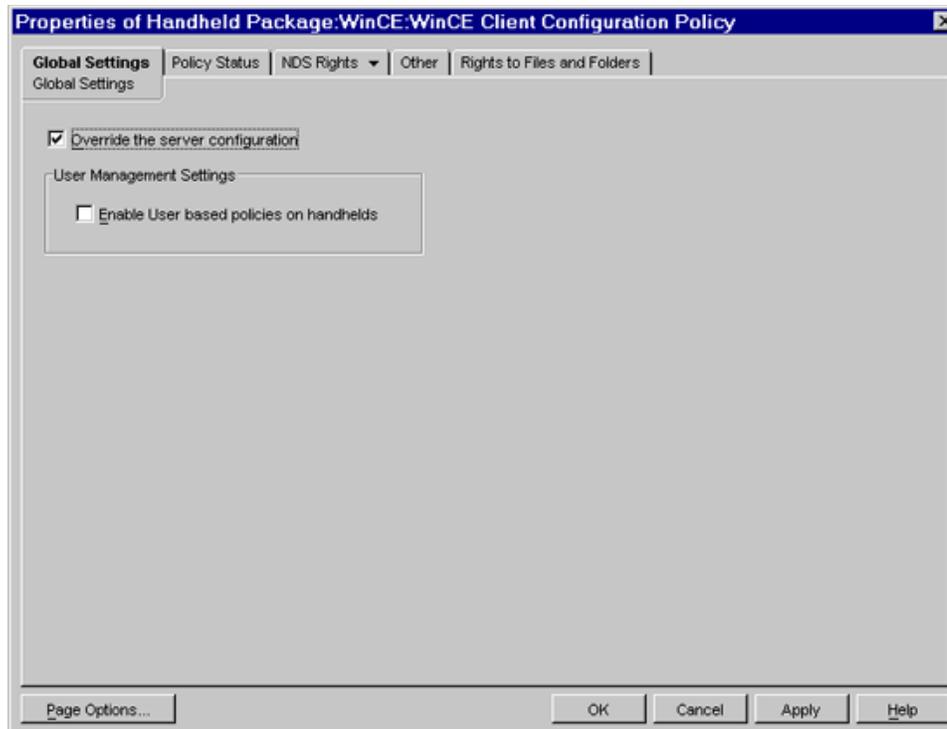
To set up the WinCE Client Configuration policy:

- 1 In ConsoleOne, right-click the Handheld Package or Handheld User object, then click *Properties*.
- 2 On the *Policies* tab, click the down-arrow, then click *WinCE*.
- 3 Select the check box under the *Enabled* column for the WinCE Client Configuration policy.

This both selects and enables the policy.



- 4 Click *Properties* to display the *Global Settings* page.
- 5 To override the user authentication settings of the ZENworks Handheld Management Service object, select the *Override the Server Configuration* option.



- 6 Select the *Enable User Based Policies on Handhelds* option.
- 7 Click *OK* to save the policy.
- 8 When you have finished configuring all of the policies for this package, continue with the steps under [“Associating the Handheld Package or the Handheld User Package”](#) on page 73 to associate the policy package.

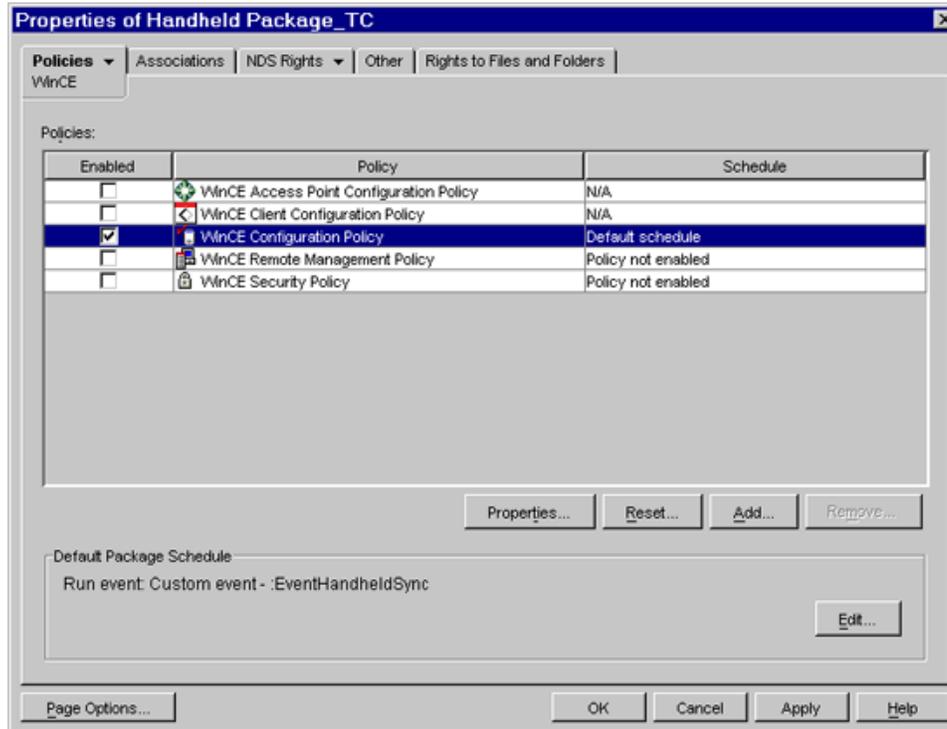
## 2.4.10 WinCE Configuration Policy

The WinCE Configuration policy lets you configure the following:

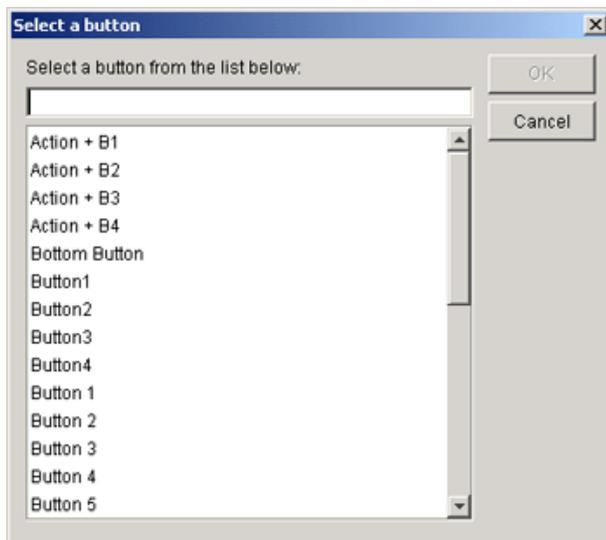
- ♦ **Buttons:** Lets you associate different software programs with the buttons on the Windows CE device. Also lets you assign another function to a button. For example, you can assign the *Start* menu to a button on the Windows CE device, making it easier for users to access the *Start* menu.
- ♦ **Programs:** Lets you specify which programs you want to include on the *Start* menu (on a Pocket PC) or on the desktop (on a Handheld PC). Programs that are not allowed can be automatically removed from the *Start* menu/desktop of the device.
- ♦ **Applications:** Lets you specify which applications or software you want to uninstall from Windows CE device.
- ♦ **Power:** Lets you specify power settings for associated Windows CE devices. You can specify power settings that apply to Windows CE devices running on internal batteries or on external power.
- ♦ **Files:** Lets you specify the files to be deleted from the Windows CE devices.

To set up the WinCE Configuration policy:

- 1 In ConsoleOne, right-click the Handheld Package or Handheld User object, then click *Properties*.
- 2 On the *Policies* tab, click the down-arrow, then click *WinCE*.
- 3 Select the check box under the *Enabled* column for the WinCE Configuration policy.  
This both selects and enables the policy.



- 4 Click *Properties*.
- 5 On the *Buttons: Configuration* page, do the following:
  - 5a Click *Add* to change a button's assignment.



To view the button naming conventions for your particular handheld device: on the handheld device, click *Start > Settings > Buttons*. For example, on a Compaq\* iPAQ Pocket PC, the buttons are named Button 1, Button 2, and so forth. On a HP\* Jornada Pocket PC, the buttons are named Hot key 1, Hot key 2, and so forth.

- 5b** Select a button or type the name of a button, click *OK*, then select an option:
- ♦ **Reset to Default:** Resets the selected button's association to the factory default association.
  - ♦ **Set to Application:** Lets you specify the application to assign to the selected button. If you specify an application that is not in the *Start* menu path (or subpath), the button applet might not show the correct settings. To apply the changes, you are prompted to restart the handheld device.
  - ♦ **Set to Other Function:** Lets you specify a function from the drop-down list to assign a function to the selected button.

**5c** Click *Apply*.

**6** On the *Programs: Start Menu/Desktop* page, do the following:

**6a** Click *Add* to specify a program to be added to the *Short Cut* list.

**6b** In the Edit Program dialog box, fill in the *Shortcut Name* option (this is the name that displays in the *Start* menu or on the desktop), fill in the *Target* path (the full path to an application's executable file), then click *OK*.

**6c** To remove certain programs from the device's *Start* menu/desktop, you might find it easier to specify a list of allowed applications and select the *Move All Other Start Menu/Desktop Items to the Programs Folder* check box. When the policy is enforced, all programs not listed in the *Icon Name* list are moved to the *Programs* folder.

**6d** To hide the names and icons of all listed programs in the *Programs* folder, select *Hide All Items* in the *Programs* Folder. Using this option lets the user run applications only from the *Start* menu (on Pocket PC devices) or on the desktop (on handheld PC devices).

**6e** Click *Apply*.

**7** On the *Applications* page, do the following:

**7a** Click *Add*.

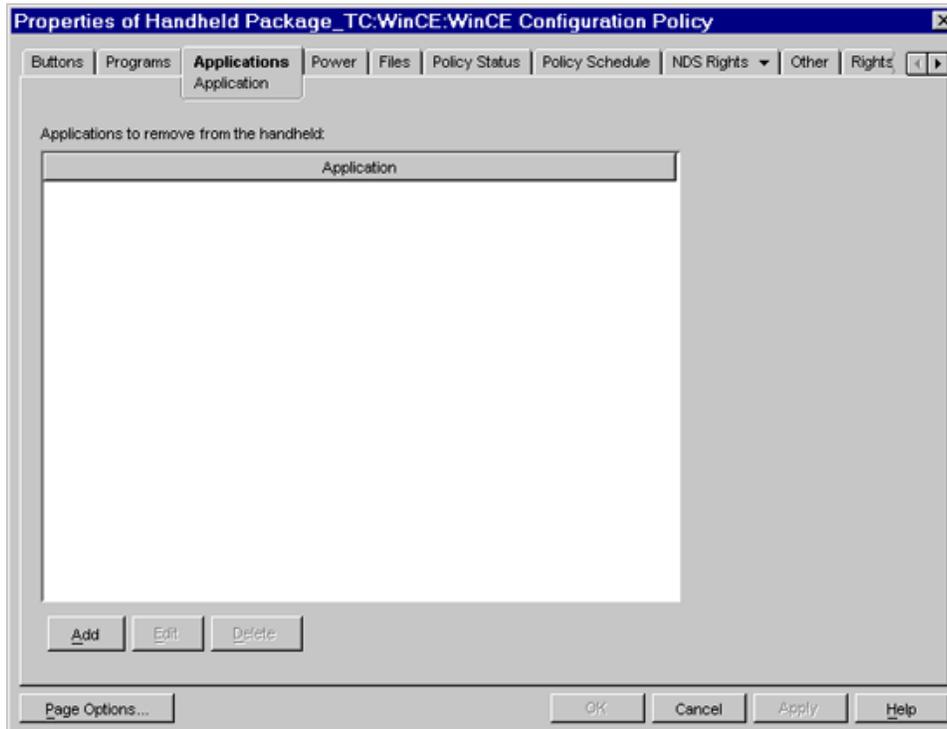
- 7b** In the *Add Application* dialog box, type or browse to the software that you want to uninstall.

---

**IMPORTANT:** If you manually type the software name, make sure to type the name exactly as it appears in the Remove Programs settings of the Windows CE device.

---

- 7c** Click *OK*.
- 7d** Click *Apply*.



- 8** On the *Power* page, make the desired configuration changes, then click *Apply*.

---

**NOTE:** The *Power* settings do not apply to HP Jornada devices running Microsoft Pocket PC 2002 software.

The *External Power* settings do not apply to Handheld PC.

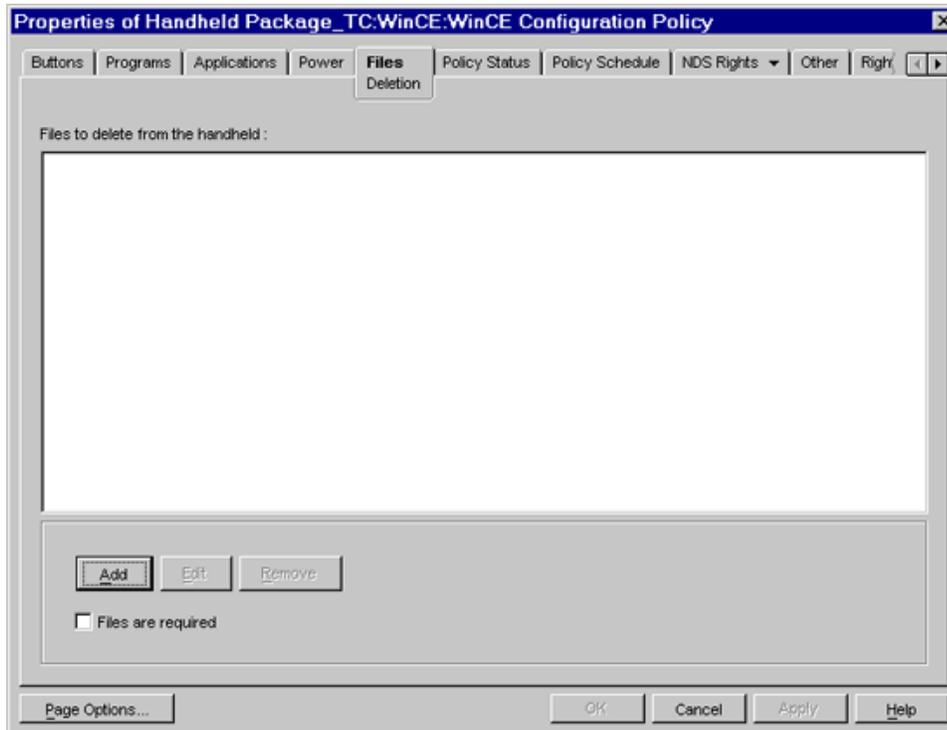
---

If you select the *Don't Change* setting, ZENworks Handheld Management does not change that setting on associated devices; the corresponding setting on each device determines its behavior. For example, if you select the *Don't Change* setting, each associated device uses its own preference settings to determine how long an idle Windows CE device waits until it turns itself off. If you want to ensure consistency across all associated Windows CE devices, select the appropriate setting.

If you select the *Disable* setting, ZENworks Handheld Management disables that setting on all associated Windows CE devices; the power of Windows CE devices is turned off.

- 9** On the *Files* page, do the following:
- 9a** Click *Add*.
  - 9b** In the Add Files to Delete from Handheld dialog box, specify the complete path of the file and the filename.

- 9c Click *OK*.
- 9d (Optional) Select the *Files are Required* option if you want Handheld Management to report a failed status if the specified files do not exist on the handheld device or if the specified wildcard characters do not provide a match for files on the device.
- 9e Click *Apply*, then click *Close*.



- 10 When you have finished configuring all of the policies for this package, continue with the steps under [“Associating the Handheld Package or the Handheld User Package” on page 73](#) to associate the policy package.
- 11 If desired, schedule the policy. For more information, see [“Scheduling Packages and Policies” on page 74](#).
- 12 (Optional) To ensure that the Handheld Management Server immediately receives the new policy changes, right-click the Handheld service object, then click *Scan Now*.

### 2.4.11 WinCE Access Point Configuration Policy

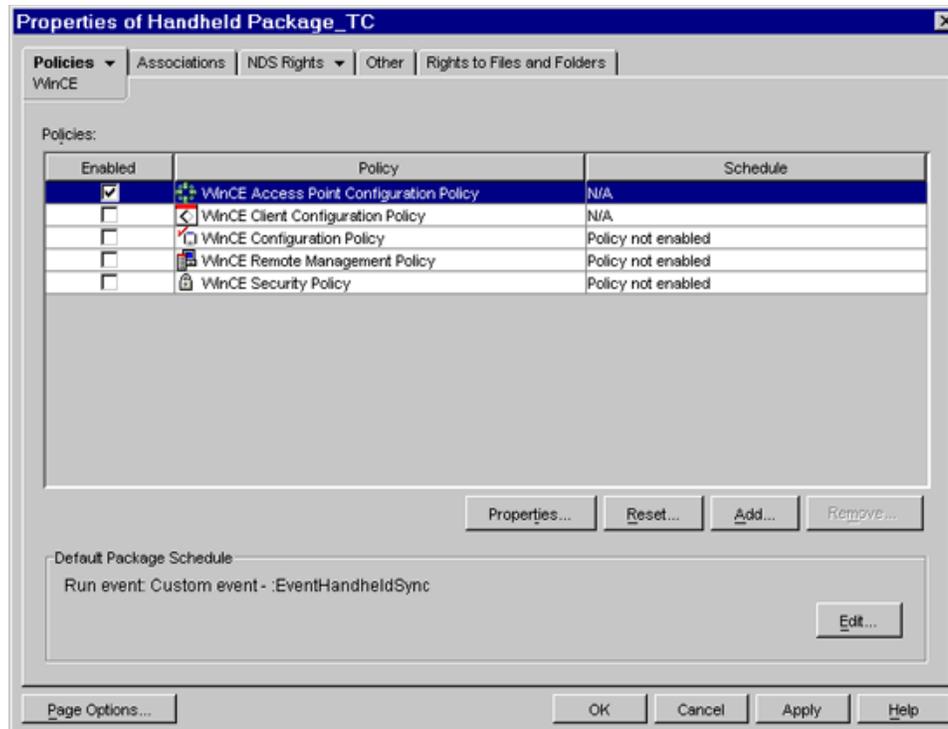
The WinCE Access Point Configuration Policy lets you assign multiple ZENworks Handheld Management Access Points to a device and also define the order of the ZENworks Handheld Management Access Points to which the Windows CE device must connect. If the device is unable to connect to the ZENworks Handheld Management Access Point configured first, then it automatically tries to connect to the ZENworks Handheld Management Access Point configured next in the sequence.

To configure the WinCE Access Point Configuration Policy:

- 1 In ConsoleOne, right-click the Handheld Package or Handheld User Package object, then click *Properties*.

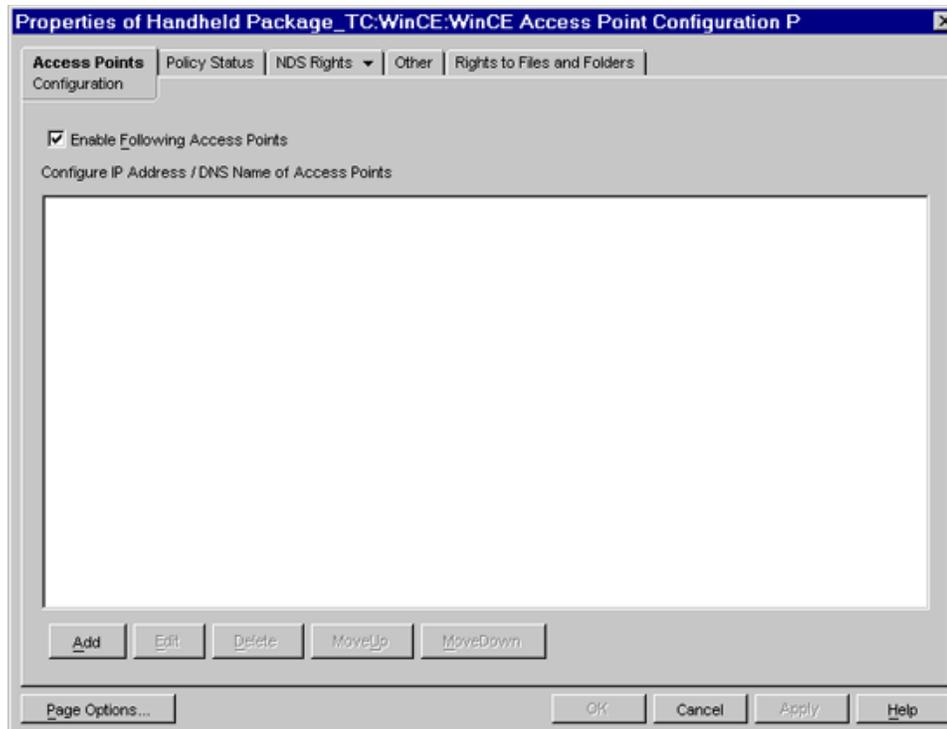
- 2 On the *Policies* tab, click the down-arrow, then click *WinCE*.
- 3 Select the check box under the *Enabled* column for the WinCE Access Point Configuration policy.

This both selects and enables the policy.



- 4 Click *Properties*.

This displays the *Access Points - Configuration* page.



**5** In the *Access Points* page, do the following:

**5a** If you want to add the ZENworks Handheld Management Access Points to the *Configure IP Address /DNS Name of Access Points* list, and define the order of the ZENworks Handheld Management Access Points to which the handheld device must connect to, select the *Enable Following Access Points* option.

If you do not select this check box, the ZENworks Handheld Management Access Points list is not available on the handheld device.

**5b** Click *Add*.

**5c** In the Add Access Points dialog box, specify the IP address or the full DNS name of the ZENworks Handheld Management Access Point, or click *Select*. If you specify the IP address or the full DNS of the ZENworks Handheld Management Access Point, skip to **Step 5h**.

**5d** By default, the service object of the Handheld Management server is displayed. To select another service object, click the *Browse* icon, select the service object, then click *OK*.

**5e** Click *Display*.

The IP address of the ZENworks Handheld Management Access Points associated with service object is displayed

**5f** From the *ZENworks Handheld Management Access Points* list, select the IP address of the ZENworks Handheld Management Access Point to which you want to connect the device.

**5g** Click *OK*.

The ZENworks Handheld Management Access Points IP address followed by a semicolon (;) is displayed in the *Access Points* option.

**5h** (Optional) To add another ZENworks Handheld Management Access Point, repeat **Step 5c** through **Step 5g**.

You can add a maximum of eight ZENworks Handheld Management Access Points IP addresses but ensure that the IP addresses or the DNS names of the ZENworks Handheld Management Access Points are separated with semicolons (;)

- 5i** Click *Apply*.
- 6** (Optional) To change the order of the ZENworks Handheld Management Access Points in the *Configure IP Address /DNS Name of Access Points* list:
  - 6a** Select the IP address or the full DNS name of the ZENworks Handheld Management Access Point.
  - 6b** Click *Move Up* or *Move Down*.
- 7** (Optional) To modify the value of a ZENworks Handheld Management Access Point displayed in the *Configure IP Address /DNS Name of Access Points* list:
  - 7a** Select the IP address or the full DNS name of the ZENworks Handheld Management Access Point whose value you want to modify.
  - 7b** Click *Edit*.
  - 7c** In the Edit Access Points dialog box, change the value of the ZENworks Handheld Management Access Point.
  - 7d** Click *OK*.
- 8** Click *Apply*, then click *Close* to save the policy.
- 9** Associate the policy package.

For more information on how to associate the policy package, see the [“Associating the Handheld Package or the Handheld User Package”](#) on page 73.
- 10** If desired, schedule the policy.

For more information on how to schedule a policy, see the [Section 2.5, “Setting Up Handheld Service Package Policies,”](#) on page 76.
- 11** (Optional) To ensure that the Handheld Management Server immediately receives the new policy changes, right-click the Handheld service object, then click *Scan Now*.

## 2.4.12 WinCE File Retrieval Policy

The WinCE File Retrieval policy lets you specify source files you want to retrieve from a Windows CE device and copy to a specified destination location.

The WinCE File Retrieval policy is a plural policy, meaning it can be added many times to a policy package. You can set up as many File Retrieval policies as required to adequately retrieve important files from the handheld devices in your organization. When you name these plural policies, be sure to give them descriptive names.

The WinCE File Retrieval policy is also cumulative, meaning that many different WinCE File Retrieval policies can be effective for a single handheld device object, handheld group object, or container object.

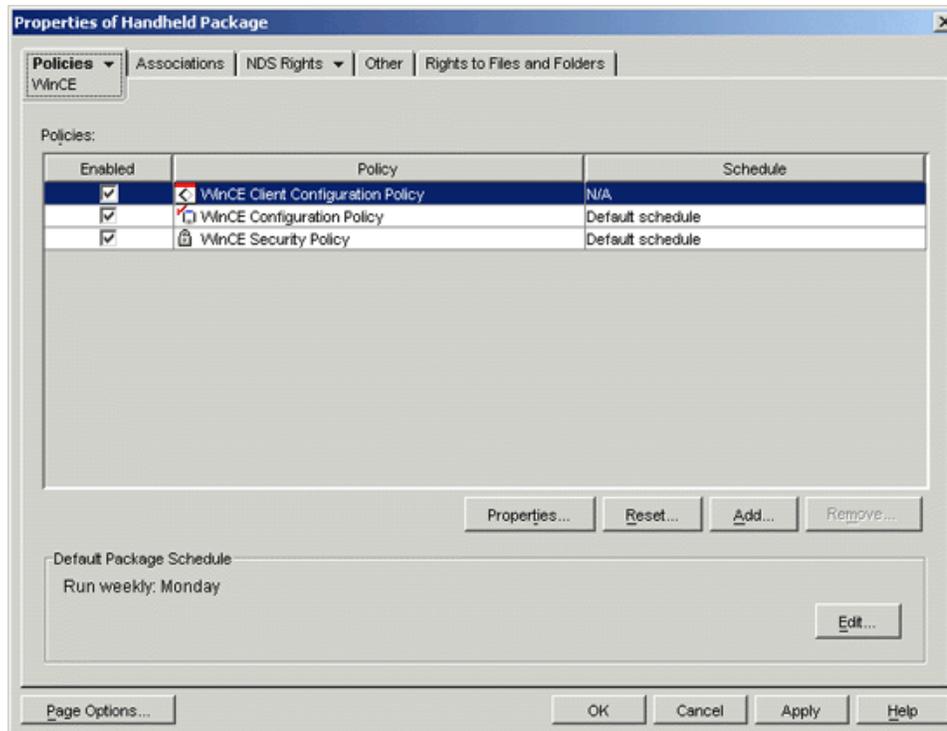
---

**NOTE:** If you want to retrieve files from handheld devices and store them on a NetWare volume, you must install the Novell Client on the ZENworks Handheld Management Server.

---

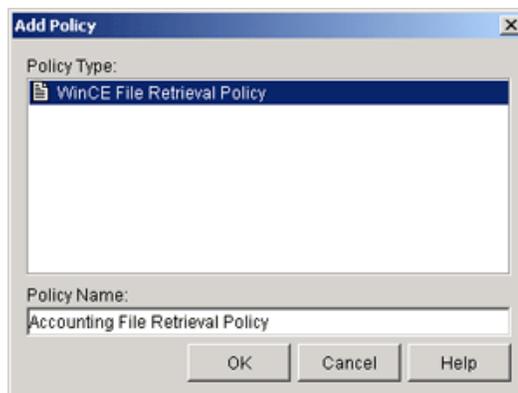
To set up the WinCE File Retrieval policy:

- 1 In ConsoleOne, right-click the Handheld Package or Handheld User Package, then click *Properties*.
- 2 On the *Policies* tab, click the down-arrow, then click *WinCE*.



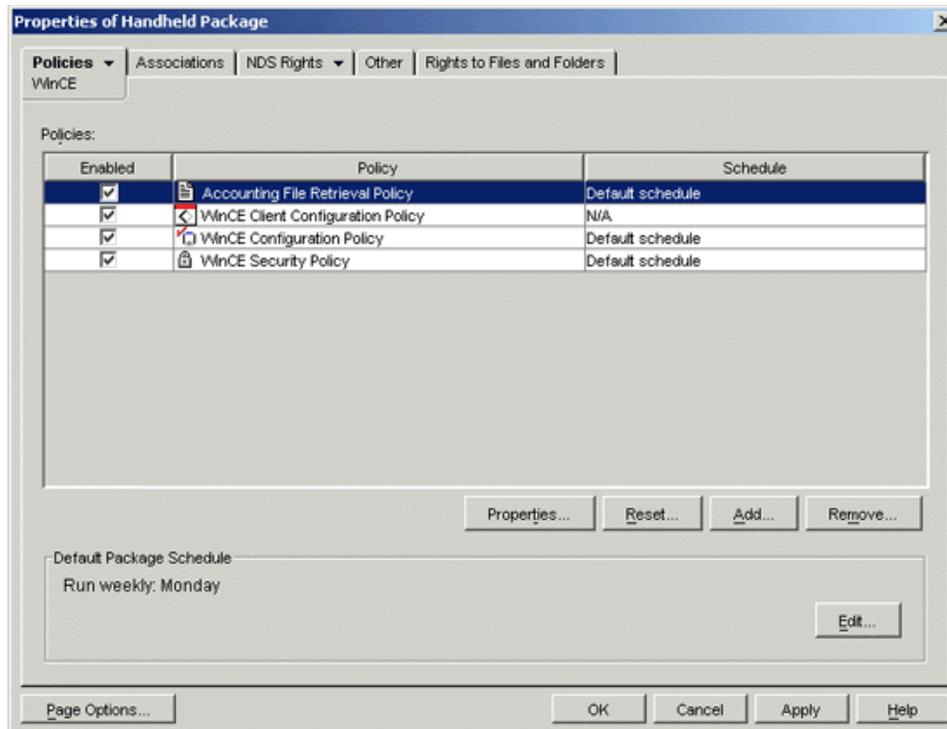
- 3 Click *Add*.

The Add Policy window is displayed.



- 4 Type a descriptive name in the *Policy Name* field, then click *OK*.

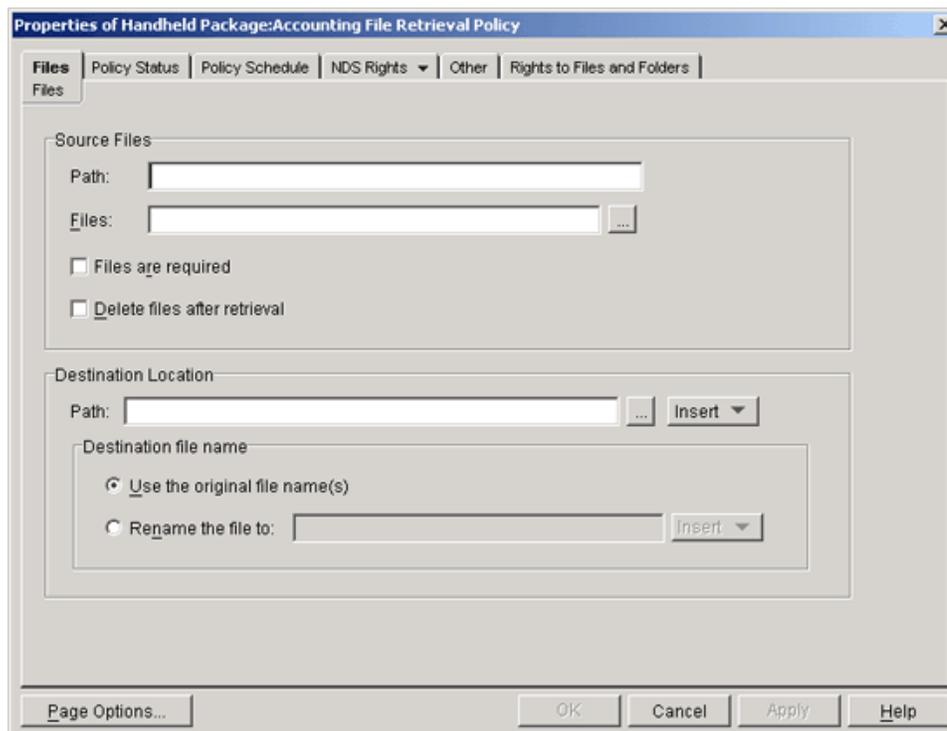
The newly created File Retrieval policy is displayed in the Handheld Policies list.



5 Select the check box under the *Enabled* column for the newly created WinCE File Retrieval policy.

This both selects and enables the policy.

6 Click *Properties* to display the *Files* page.



- 7 In the *Path* field in the *Source Files* box, specify the path to the source files.
- 8 In the *Files* field, browse to or specify the source files to be retrieved from the Windows CE device.

You can use wildcard characters to specify source files.

When the policy is enforced, all specified source files are retrieved from the device; the files are retrieved even if the same files were previously retrieved at another time.

- 9 Select the *Files Are Required* check box if you want ZENworks Handheld Management to report a failed status if the specified files do not exist on the Windows CE device or if the specified wildcard characters do not provide a match for files on the device.

---

**NOTE:** For more information about policy status, see [Section 2.6, “Viewing Policy Status Information,”](#) on page 76.

---

- 10 Select the *Delete Files After Retrieval* check box if you want the specified source files to be deleted from the Windows CE device after they have been retrieved from the handheld device.

If you do not enable this option, the source files are copied to the specified location but also remain on the Windows CE device.

- 11 In the *Path* field in the *Destination Location* box, browse to or specify the destination location where you want the specified files copied to.

The renamed file can include variables. To include variables, click the *Insert* button, then click the desired variable.

The following variables are available for use:

---

Variable	Description
<i>device</i>	The CN of the device. For example, in Dan m130.Handhelds.NovellBangalore, the string would be Dan m130.
<i>devicedn</i>	The full DN of the device. For example, In Dan m130.Handhelds.NovellWheaton, the string would be Dan m130.Handhelds.NovellWheaton.
<i>user</i>	The username of the device. This is the value stored in the <i>zfhUserName</i> attribute for the object in the directory. When this value is not configured on the handheld device, it is set to <Undefined>.
<i>date</i>	The date the file was retrieved from the handheld device. This value is the date only; the time that the file was retrieved is not included. For example, if the file was retrieved on September 15, 2002 at 3:15 p.m., the string would be 2002-09-15. The string is always in the format of yyyy-mm-dd.
<i>time</i>	The time the file was retrieved from the handheld device. This value is for the time only; the date that the file was retrieved is not included. For example, if a file was retrieved on September 15, 2002 at 3:20 p.m., the string would be 15-20. The string is always in the format of hh-mm, with hh representing the hour in 24-hour format.
<i>guid</i>	The GUID for the handheld device.
<i>server</i>	The name of the server that received the data. This is the Windows NT name of the server.

---

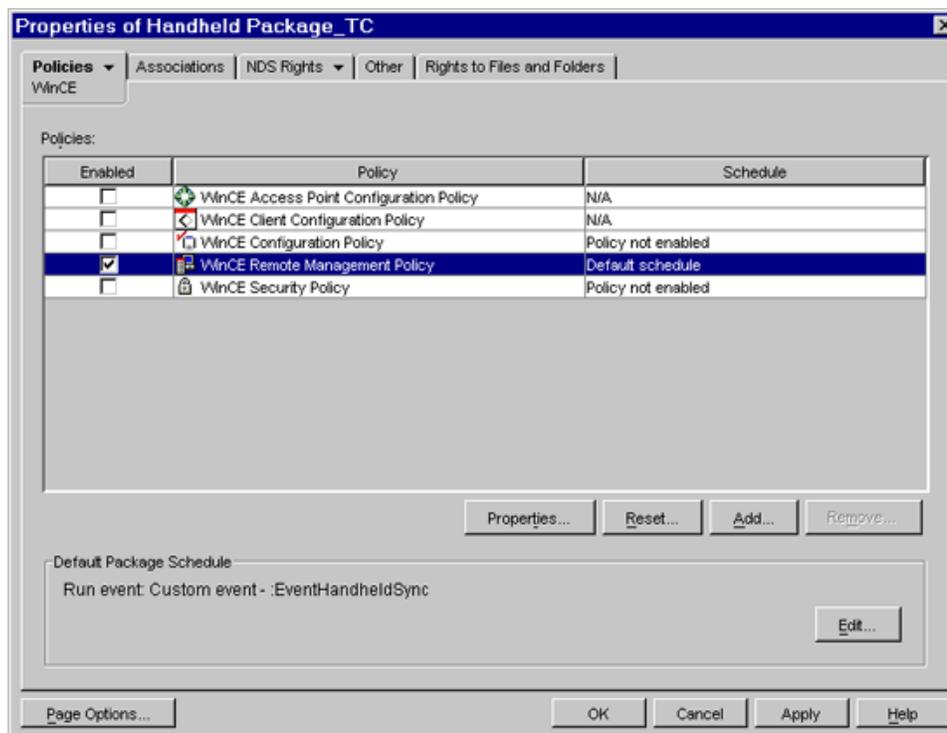
To use a variable, place an @ sign on either side of the variable in the string. For example, you could use the following syntax:

@user@\_filename

- 12 Select *Use the Original File Name(s)* to use the original source filenames for the destination files.  
or  
Select *Rename the Files To* and specify new filenames for the destination files.
- 13 Click *OK* to save the policy.
- 14 When you have finished configuring all of the policies for this package, continue with the steps under “[Associating the Handheld Package or the Handheld User Package](#)” on page 73 to associate the policy package.
- 15 If desired, schedule the policy. For more information, see “[Scheduling Packages and Policies](#)” on page 74.

### 2.4.13 WinCE Remote Management Policy

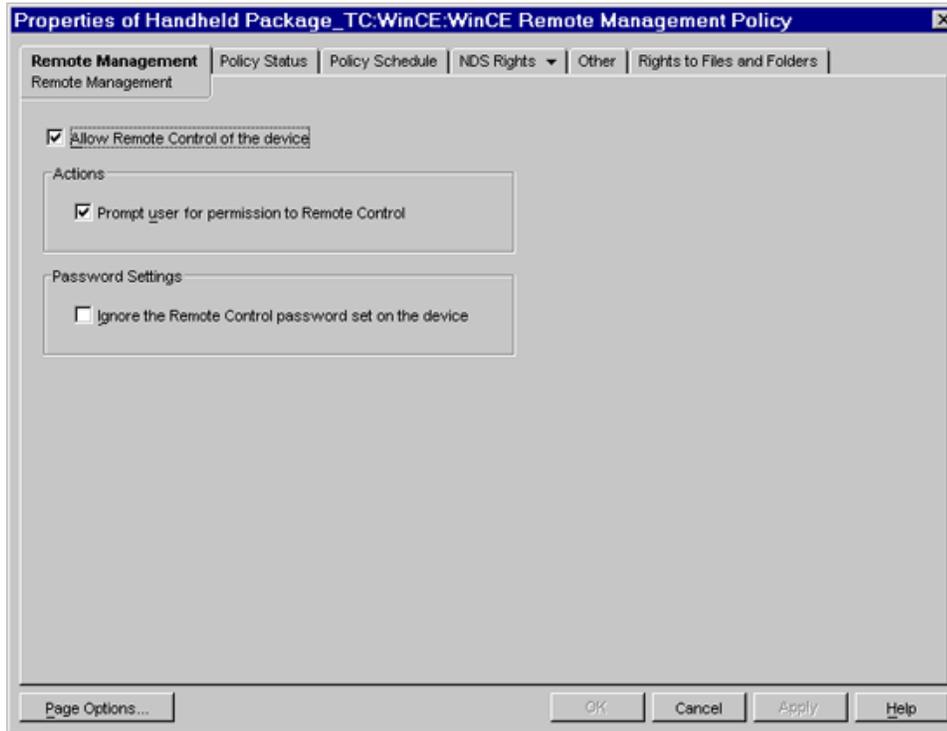
- 1 In ConsoleOne, right-click the Handheld Package or Handheld User Package object, then click *Properties*.
- 2 On the *Policies* tab, click the down-arrow, then click *WinCE*.
- 3 Select the check box under the *Enabled* column for the WinCE Remote Management policy.  
This both selects and enables the policy.



- 4 Click *Properties* to display the *Remote Management* page.

- 5** In the *Remote Management* page, do the following:
- 5a** Select the *Allow Remote Control of the Device* option.
  - 5b** If you want to enable the Windows CE device user to either accept or reject the Remote Management session initiated by the administrator or remote user, select the *Prompt User for Permission to Remote Control* option.

By default, this option is selected.



- 5c** If you want to enable the administrator or the remote user to initiate a Remote Management session on the Windows CE devices without being prompted to enter the password set by the device user, select the *Ignore the Remote Control Password Set on the Device* option.
  - 5d** Click *Apply*, then click *Close*.
- 6** Associate the policy package.  
For more information on how to associate the policy package, see the [“Associating the Handheld Package or the Handheld User Package”](#) on page 73.
- 7** If desired, schedule the policy.  
For more information on how to schedule a policy, see the [“Scheduling Packages and Policies”](#) on page 74.
- 8** (Optional) To ensure that the Handheld Management Server immediately receives the new policy changes, right-click the Handheld service object, then click *Scan Now*.

## 2.4.14 WinCE Security Policy

The WinCE Security policy lets you configure the following:

- ♦ **Password Requirements:** Lets you ensure that a password is set on associated Windows CE devices and also lets you set a user's network password as the device password, configure enhanced security options for Pocket PCs, such as the number of days to allow before a password expires, the number of grace logins permitted before the user must change the password, the minimum number of characters to allow for the password, and whether the password must contain a combination of letters and numbers.

---

**IMPORTANT:** Before configuring the policy, you must configure the containers to be searched to authenticate the handheld user credentials. You can do it either during the ZENworks 7 Handheld Management server installation or after the installation.

To configure user authentication during the installation, you must select the Enable User Authentication option, and specify the containers to search for user objects.

To configure user authentication after the installation, see [Section 7.1, "Configuring User Authentication,"](#) on page 129.

---

There are two places in ZENworks Handheld Management where users can be required to enter a password: to authenticate to the directory as part of the WinCE Client Configuration policy and to power on a handheld device as part of the WinCE Security policy. These two passwords are independent of each other. For more information about the password users must enter to authenticate to the directory, see [Section 2.4.9, "WinCE Client Configuration Policy,"](#) on page 53.

- ♦ **Self-Destruct Settings:** Lets you specify self-destruct settings to disable a Windows CE device after a specified number of failed password attempts or after a specified number of days since the device was last connected or synchronized.

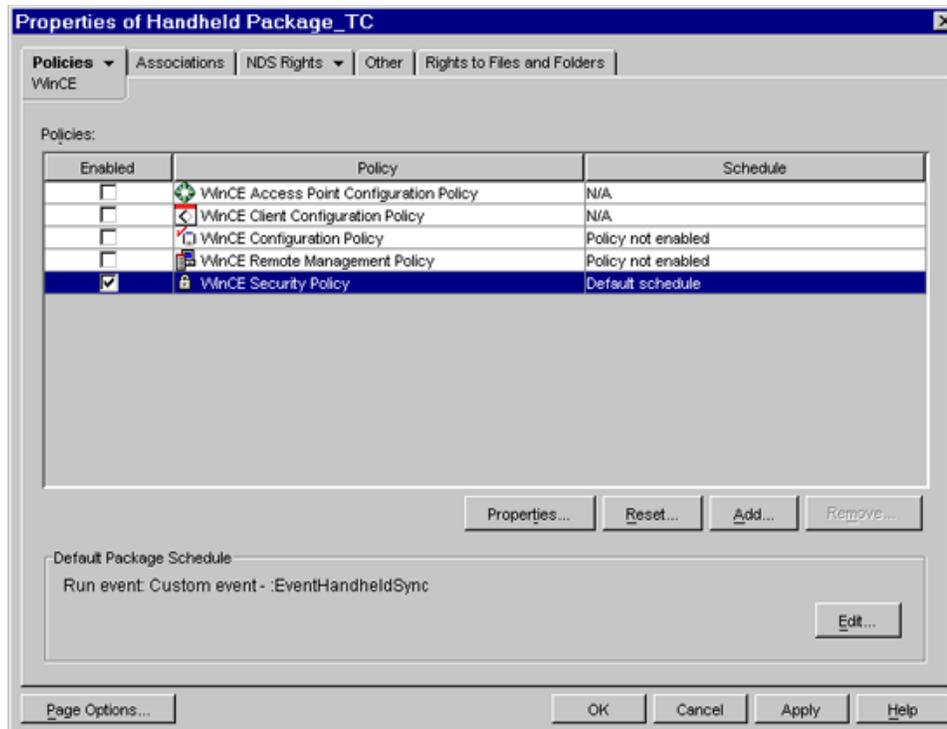
---

**IMPORTANT:** The WinCE Security policy does not function on the Denso devices (BHT-200), Symbol PPT 8800 or the Jornada Pocket PCs running Microsoft Windows for Pocket PC 2000 software. However, the Jornada Pocket PCs running Microsoft Pocket PC 2002 software can use the WinCE Security policy.

---

To set up the WinCE Security policy:

- 1 In ConsoleOne, right-click the Handheld Package object, then click *Properties*.
- 2 On the *Policies* tab, click the down-arrow, then click *WinCE*.
- 3 Select the check box under the *Enabled* column for the WinCE Security policy.  
This both selects and enables the policy.

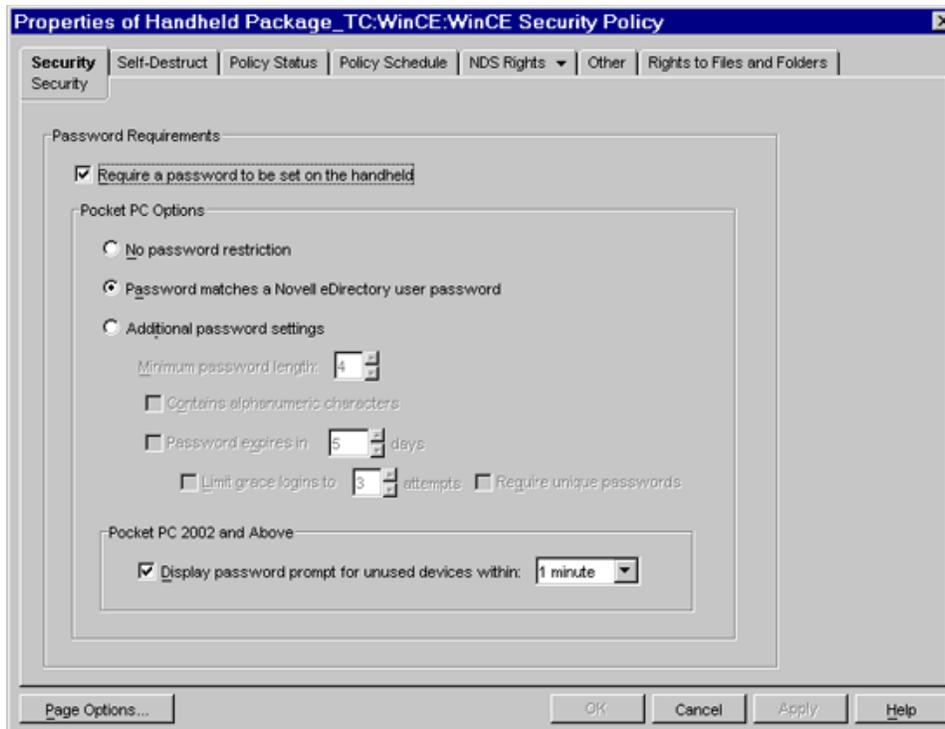


4 Click *Properties* to display the *Security* page.

5 In the *Security* page, do the following:

**5a** To set a password on the Windows CE device, select the *Require a Password to Be Set on the Handheld* option.

If your organization has a rule that states that all handheld devices must have a password, you should enable this policy. If a user does not have a password set, he or she is prompted to create one.




---

**NOTE:** The password set on a Symbol device is not case sensitive.

---

**5b** Configure the following *Pocket PC Options*, which lets you specify enhanced security options for Pocket PCs. The options in this group box are disabled unless you check Require a Password to Be Set on the Handheld.

- ◆ **Password Matches a Novell eDirectory User Password:** Select this option to set a user's network (eDirectory) password as the device password.

---

**WARNING:** If you forget your network password, you cannot access the Handheld device. You can access the device only by Hard Reset but this erases all data on the device.

---

- ◆ **Additional Password Settings:** Select this option to specify enhanced password support settings for Pocket PCs.

For Pocket PCs, where enhanced security like biometric is not supported by the device, if you select *Enable Enhanced Password Support*, ZENworks Handheld Management displays its own password dialog box instead of default Windows CE dialog box.

---

**IMPORTANT:** For Pocket PCs, where the device supports enhanced security, if you select *Enable Enhanced Password Support*, ZENworks Handheld Management displays a dialog box saying that a password must be set on the device. In that case, the default Windows CE dialog box is shown.

---

The *Enable Enhanced Password Support* option does not function on handheld PCs. If, in the future, you want to remove the ZENworks Handheld Management password applet and restore the original Windows CE password applet, you need to reconfigure the WinCE Security policy and disable the *Enable Enhanced Password Support*

option and then resynchronize the device so that the policy is enforced. Uninstalling the ZENworks Handheld Management handheld client on the device or disassociating the device from the WinCE Security policy does not remove the ZENworks Handheld Management password applet.

---

**NOTE:** You can replace the bitmap image that displays in the ZENworks Handheld Management password dialog boxes with a bitmap image of your choosing. For more information, see [“Replacing the ZENworks Handheld Management Password Dialog Box Bitmap Image”](#) on page 73.

---

Configure the following additional password settings:

**Minimum Password Length:** Specify the minimum number of characters to allow for the password on the device. You should choose a number great enough to ensure adequate security, but small enough not to excessively burden the user.

**Contains Alphanumeric Characters:** Select this check box to require that the user use both letters and numbers in the password. To improve the security of a password, it should contain both letters (uppercase and lowercase) and numbers.

**Password Expires in \_ Days:** Select this check box and specify the number of days that you want the password to expire in. When the specified number of days has expired, the user is prompted to change the password for the Pocket PC.

**Limit Grace Logins to \_ Attempts:** Select this check box and specify the number of grace logon attempts you want to allow the user before he or she must change the password for the device. After you enter the number of days in *Password Expires in \_ Days*, the user is prompted to change the password. The user can choose to ignore this prompt and keep the same password for the number of logon attempts you specify.

**Require Unique Passwords:** Select this check box to require that the user enter a new password; he or she cannot reuse the previous eight passwords.

**5c** Configure the *Pocket PC 2002 and Above* option.

The Pocket PC 2002 options lets you specify a time limit that the Pocket PC can remain idle for before a password prompt is displayed. For Pocket PC 2003, this option lets you specify a time limit that the Pocket PC can be turned off for before a password prompt is displayed when the device is turned back on.

For example, if you set this option to 5 minutes, if the user turns the device off and then back on within 5 minutes, no password is required to use the device. However, if more than 5 minutes passes, the user must enter a password to use the device.

**Display Password Prompt for Unused Devices Within:** Select this check box and choose a time limit from the drop-down list. When the time limit expires, a password prompt is displayed on the device.

For example, if you set this option to 5 minutes and the user turns the device off and then back on within 5 minutes, no password is required to use the device. However, if more than 5 minutes passes, the user must enter a password to use the device.

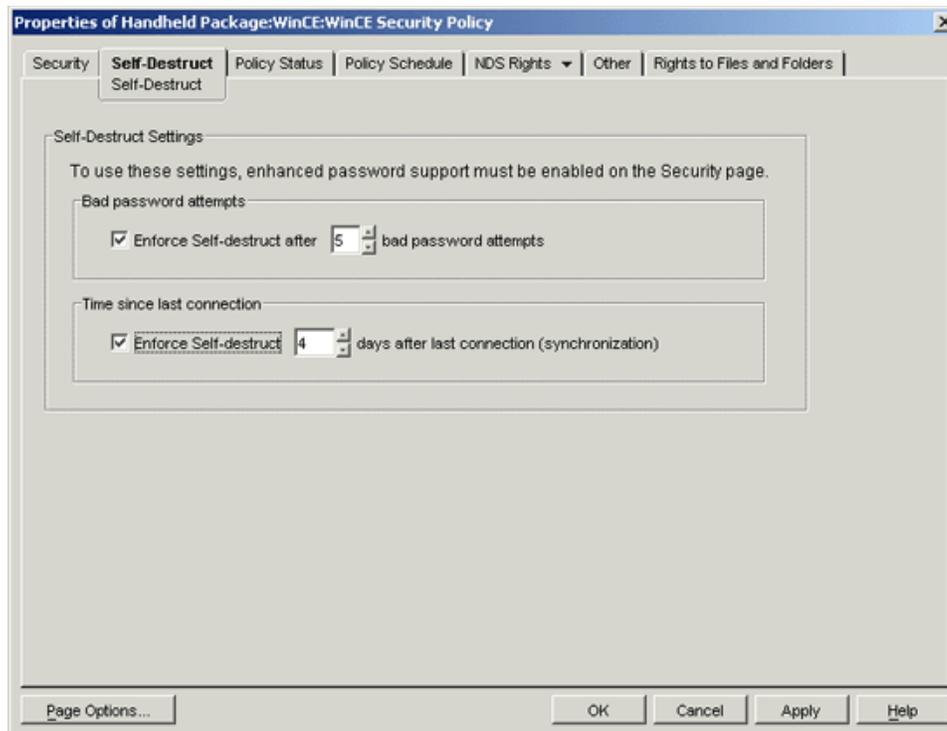
The Windows CE device user can change the corresponding setting on the actual handheld device; however, the value you enter in the Display Password Prompt for Unused Devices Within field is the maximum amount of time the user can set; he or she cannot increase the time limit beyond this value.

---

**IMPORTANT:** To use this setting, the handheld device must be running Pocket PC 2002 or later.

---

- 5d Click *Apply*.
- 6 Click the *Self-Destruct* tab.



The *Self-Destruct* page lets you configure self-destruct settings for Windows CE devices so that data is not accessible from handheld devices that are lost or stolen. When the self-destruct feature is activated, the data on the device is made unusable and the device must be manually reset, which restores the device to its out-of-the-box state.

To use the self-destruct options for Windows CE devices, you must select the *Enable Enhanced Password Support* check box on the *Security* page. You cannot use the self-destruct options on handheld PCs because the *Enable Enhanced Password Support* option does not function on them.

---

**IMPORTANT:** Use caution when you use the self-destruct feature. Be sure to allow an adequate number of password attempts and an adequate number of days since the last connection or synchronization to prevent data loss to users who incorrectly enter the password or do not connect or synchronize the device during a short vacation.

For Windows CE devices, ActiveSync does not automatically back up data. If the user has manually backed up the data, he or she can then manually restore the data to the device.

---

- 7 Configure the following Self-Destruct settings:

**Bad Password Attempts:** Select the *Enforce Self-Destruct* check box and specify the number of bad password attempts to allow before activating the self-destruct feature.

**Time Since Last Connection:** Select the *Enforce Self-destruct* check box and specify the number of days after the last connection before activating the self-destruct feature. The *Time Since Last Connection* option refers to the last time the handheld device connected to the ZENworks Handheld Management Access Point.

Each day is made up of 24 hours. If you connect (synchronize) the device on Monday at 2 p.m. and specify three days after the last connection before activating the self-destruct feature, the self-destruct feature activates Thursday at 2 p.m (72 hours after the last connection/synchronization) unless the device is connected/synchronized during that period.

- 8 Click *OK* to save the policy.
- 9 When you have finished configuring all of the policies for this package, continue with the steps under “**Associating the Handheld Package or the Handheld User Package**” on page 73 to associate the policy package.
- 10 If desired, schedule the policy. For more information, see “**Scheduling Packages and Policies**” on page 74.
- 11 (Optional) To ensure that the Handheld Management Server immediately receives the new policy changes, right-click the Handheld service object, then click *Scan Now*.

### Replacing the ZENworks Handheld Management Password Dialog Box Bitmap Image

You can replace the ZENworks Handheld Management bitmap image that displays in the following ZENworks Handheld Management password dialog boxes with a bitmap image of your choosing:

- ♦ The login dialog box if you selected *Enable Enhanced Password Support* in **Step 5 on page 69**.
- ♦ The dialog boxes that display when the WinCE Security policy is enforced and you selected *Require a Password to Be Set on the Handheld* in **Step 5 on page 69**.

To replace the bitmap image in these dialog boxes, create a bitmap file called `logo.bmp` and place it in the ZENworks Handheld Management installation directory on the handheld device. The size of this bitmap image should be 240 pixels wide by 35 pixels high.

### 2.4.15 Associating the Handheld Package or the Handheld User Package

The policies you configured and enabled are not in effect until you associate their policy package with a handheld device object, a User object, a handheld group object, a user group, or a container object.

- 1 In ConsoleOne, right-click the Handheld Package or Handheld User Package object, then click *Properties*.
- 2 Click the *Associations* tab, then click *Add*.
- 3 Browse for the object for associating the package, then click *OK*.

The Handhelds Package can be associated with a handheld device object, a handheld group object, or a container object containing these objects.

The Handhelds User Package can be associated with a User object, a user group object, or a container object containing these objects.

## 2.4.16 Associating a User Object to a BlackBerry Device

- 1 In ConsoleOne, right-click the BlackBerry device, then click *Properties*.  
The *General* page is displayed by default.
- 2 Click the *Browse* icon next to the *Associated User* option to browse for and select the user object.
- 3 Click *OK*.

## 2.4.17 Scheduling Packages and Policies

Some policies can be scheduled to run at a certain time. During creation, all policy packages are given a default run schedule (EventHandheldSync, by default). This means that all applicable policies in this package are enforced every time the handheld device synchronizes/connects to the ZENworks Handheld Management Access Point. However, you can change the entire policy package schedule, or you can set a policy within the package to run at a different time from the rest of the package.

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

If you have configured and enabled policies, but they have not been enforced on individual handheld devices, consider the following:

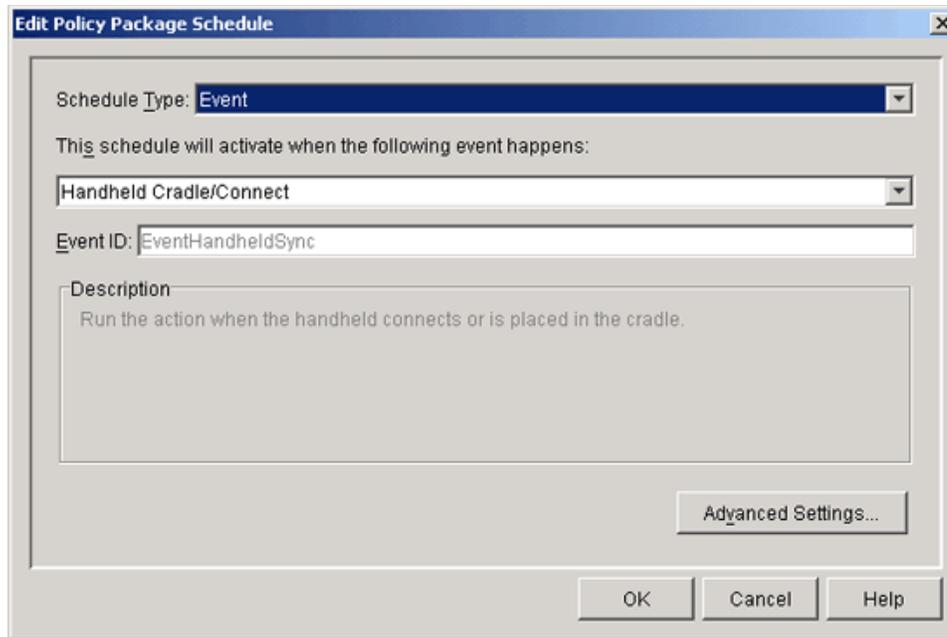
1. When you configure and enable policies, ConsoleOne records the new information in the directory.
2. The ZENworks Handheld Management Server scans for new information hourly, by default. You must wait for up to one hour to ensure that the Handheld Management Server has received the policy changes, depending on when the last scan was performed.  
  
You can force an immediate directory scan to ensure that the Handheld Management Server receives the new policy changes by right-clicking the ZENworks Handheld Management Service object, clicking *Actions*, then clicking *Scan Now*.
3. For Palm OS and Windows CE devices, the default Policy Package Schedule is EventHandheldSync (whenever the handheld device connects/synchronizes); for BlackBerry devices, the default Policy Package Schedule is once per day. If you have changed the default Policy Package Schedule, it might take longer to enforce the policy changes on the associated handheld devices. In addition, if the handheld devices were unable to connect to the ZENworks Handheld Management system (because of connectivity problems, for example), you might need to reconnect/resynchronize the devices.

The following sections contain additional information:

- ♦ [“Changing the Handheld Package or Handheld User Package Schedule” on page 74](#)
- ♦ [“Changing an Individual Policy’s Schedule” on page 75](#)

### Changing the Handheld Package or Handheld User Package Schedule

- 1 In ConsoleOne, right-click the Handheld Package or Handheld User Package object, click *Properties*, then click the desired platform page.
- 2 Click the *Edit* button in the *Default Package Schedule* group box. The Edit Policy Package Schedule page is displayed.



**3** Make the desired changes to the schedule.

Be aware that changing the policy package's schedule to run too frequently affects performance, depending on your environment. The default schedule should be adequate for most situations.

---

**NOTE:** Click the *Help* button for detailed information about the options in the Edit Policy Package Schedule dialog box.

---

**4** Click *OK*.

### Changing an Individual Policy's Schedule

**1** In ConsoleOne, right-click the Handheld Package or Handheld User Package object, click *Properties*, then click the desired platform page.

**2** Select the check box under the *Enabled* column for the desired policy.

This both selects and enables the policy.

**3** Click *Properties*.

**4** Click the *Policy Schedule* tab, then make the desired changes to the schedule.

Be aware that changing the an individual policy's schedule to run too frequently affects performance, depending on your environment. The default schedule should be adequate for most situations.

---

**NOTE:** Click the *Help* button for detailed information about the options in the *Policy Schedule* page.

---

**5** Click *OK*.

## 2.5 Setting Up Handheld Service Package Policies

The Handheld Service Package currently contains one policy: Handheld Import. Creating the Handheld Service Package and configuring and associating the Handheld Import policy are covered in [“Setting Up Handheld Import” on page 11](#).

## 2.6 Viewing Policy Status Information

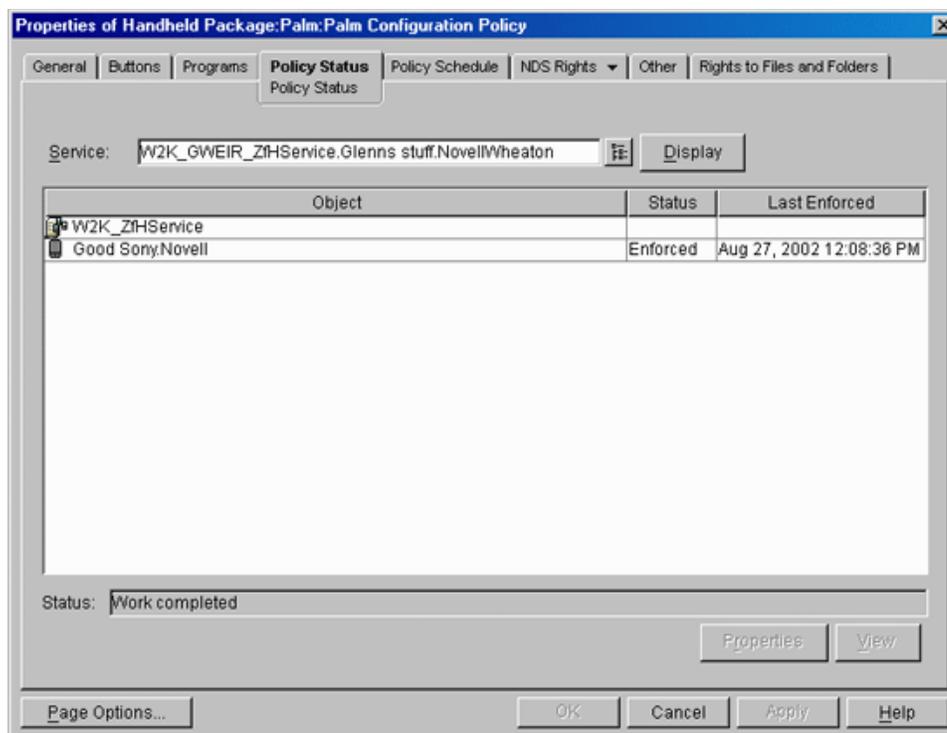
ZENworks Handheld Management lets you view policy status information for each enabled policy, including a list of all handheld devices and User objects that a policy is associated with, the status of each policy, and the date and time that the policy was last enforced. You can also view status information about all policies associated with a specific handheld device.

The following sections contain more information:

- ♦ [“Viewing Status for a Specific Policy” on page 76](#)
- ♦ [“Viewing Policy Status for a Specific Handheld Device” on page 78](#)

### 2.6.1 Viewing Status for a Specific Policy

- 1 In ConsoleOne, right-click the Handheld Package or Handheld User Package object, then click *Properties*.
- 2 Select the check box under the *Enabled* column for the desired policy.  
This both selects and enables the policy.
- 3 Click *Properties*.
- 4 Click the *Policy Status* tab.




---

**NOTE:** Click *Display* to refresh the information in the *Object*, *Status*, and *Last Enforced* columns.

---

**Object:** Lists the individual handheld device objects that the policy is associated with. You can select a handheld device in the list, then click *Properties* to view that device's properties.

**Status:** Lists the status of the policy on each handheld device:

---

Status	Description
<i>Successful</i>	The policy was successfully enforced on the corresponding handheld device.
<i>Pending</i>	The policy has reached its scheduled run time but has not yet reported results. For example, the policy has been enforced on the handheld device, but the ZENworks Handheld Management Access Point has not yet connected to the ZENworks Handheld Management Server to relay the information.
<i>Failed</i>	The policy was not successfully enforced on the handheld device. For troubleshooting information, see <a href="#">"Why are policies that I have configured and enabled not being enforced on individual handheld devices?" on page 148.</a>
<i>Disabled</i>	The policy has been disabled in ConsoleOne. To re-enable a policy, right-click the Handheld Package or Handheld User Package object, click <i>Properties</i> , then select the check box in the <i>Enabled</i> column for the desired policy.
<i>Inactive</i>	The policy is inactive. For example, the policy has been disassociated with the handheld device; however, policy status information still exists in ZENworks Handheld Management.

---

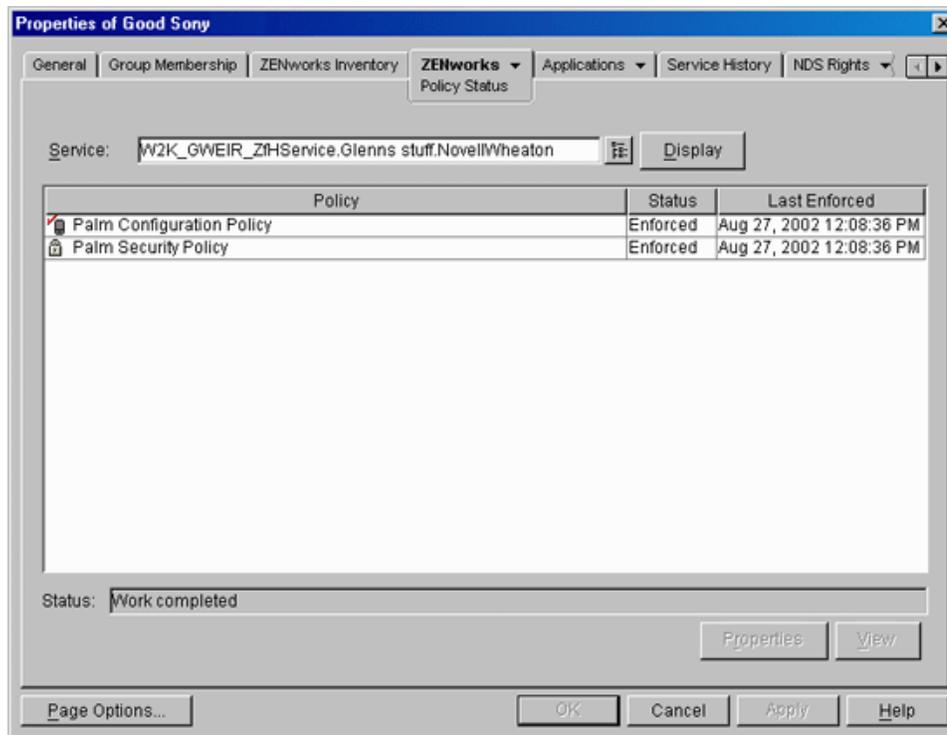
**Last Enforced:** Lists the date and time that the policy was last enforced.

For most policies, the date and time in the *Last Enforced* column is based on the handheld device's date and time. For File Retrieval policies, the date and time in the *Last Enforced* column is based on the ZENworks Handheld Management Access Point date and time.

The *Status* field at the bottom of the page displays *Work Completed* if all information has been gathered for the policy and for the associated handheld devices. The *Status* field displays *Connecting to Server* if you click *Display*. When all information has been gathered, the status returns to *Work Completed*.

## 2.6.2 Viewing Policy Status for a Specific Handheld Device

- 1 In ConsoleOne, right-click the desired Handheld Device object, then click *Properties*.
- 2 Click the down-arrow on the *ZENworks* tab, then click *Policy Status*.



**NOTE:** Click *Display* to refresh the information in the *Object*, *Status*, and *Last Enforced* columns.

**Policy:** Lists the individual policies that are associated with the selected Handheld Device object. Select a policy in the list, then click *Properties* to view that policy's properties.

**Status:** Lists the status of the policy on each handheld device:

Status	Description
<i>Successful</i>	The policy was successfully enforced on the corresponding handheld device.

Status	Description
<i>Pending</i>	The policy has reached its scheduled run time but has not yet reported results. For example, the policy has been enforced on the handheld device, but the ZENworks Handheld Management Access Point has not yet connected to the ZENworks Handheld Management Server to relay the information.
<i>Failed</i>	The policy was not successfully enforced on the handheld device. For troubleshooting information, see <a href="#">"Why are policies that I have configured and enabled not being enforced on individual handheld devices?"</a> on <a href="#">page 148</a> .
<i>Disabled</i>	The policy has been disabled in ConsoleOne. To re-enable a policy, right-click the Handheld Package or Handheld User Package object, click <i>Properties</i> , then select the check box in the <i>Enabled</i> column for the desired policy.
<i>Inactive</i>	The policy is inactive. For example, the policy has been disassociated with the handheld device; however, policy status information still exists in ZENworks Handheld Management.

**Last Enforced:** Lists the date and time that the policy was last enforced.

For most policies, the date and time in the *Last Enforced* column is based on the handheld device's date and time. For File Retrieval policies, the date and time in the *Last Enforced* column is based on the ZENworks Handheld Management Access Point date and time.

The *Status* field at the bottom of the page displays `Work Completed` if all information has been gathered for the policy and for the associated handheld devices. The *Status* field displays `Connecting to Server` if you click *Display*. When all information has been gathered, the status returns to `Work Completed`.



# Using Queries and Groups

# 3

After handheld devices have registered with Novell® ZENworks® 7 Handheld Management, you can use queries to quickly find handheld devices that match criteria specified in the query and create custom groups to make managing handheld devices easier.

The following sections contain additional information:

- ♦ [Section 3.1, “Using Queries,” on page 81](#)
- ♦ [Section 3.2, “Using Groups,” on page 84](#)

## 3.1 Using Queries

Queries let you quickly find handheld devices that match criteria specified in the query.

Using queries, administrators can save time by automatically creating handheld groups populated with handheld devices that have the same attributes.

For example, you can create a group from a query that contains all devices that have:

- ♦ A specific processor type (for example, Intel\* StrongARM)
- ♦ RAM greater than 8 MB but less than 64 MB
- ♦ A specific version of an application installed

You can define separate queries for BlackBerry, Palm OS, and Windows CE devices, but you cannot create a single query that returns all types of devices.

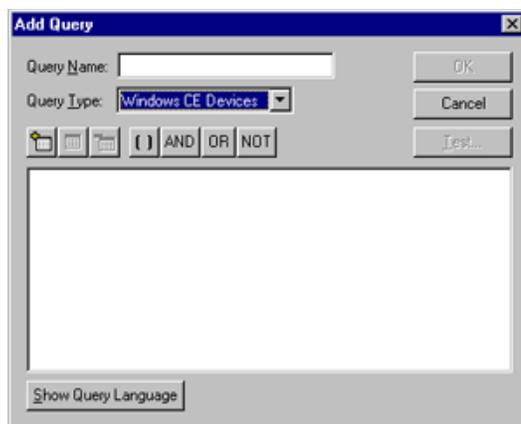
The following sections contain additional information about creating queries:

- ♦ [Section 3.1.1, “Creating a Query,” on page 81](#)
- ♦ [Section 3.1.2, “Using Logical Operators,” on page 84](#)

### 3.1.1 Creating a Query

You create queries in the ZENworks Handheld Management Inventory Viewer.

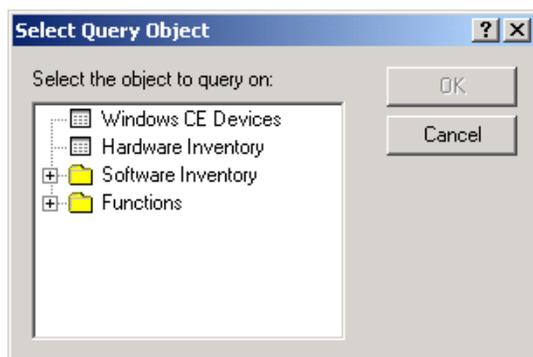
- 1 In Novell ConsoleOne®, right-click a handheld device object, click *Actions*, then click *Inventory*.
- 2 Click *Queries*, then click *Add Query* to display the Add Query window.



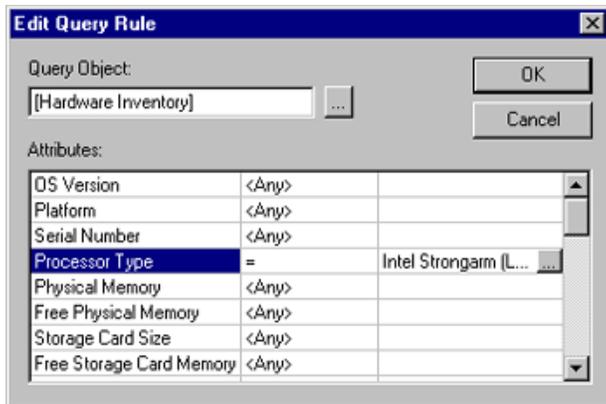
- 3 Type a name for the query.
- 4 Click *Palm OS Handhelds* in the *Query Type* drop-down list to create a query for Palm OS devices.  
or  
Click *Windows CE Devices* in the *Query Type* drop-down list to create a query for Windows CE devices.  
or  
Click *BlackBerry Devices* in the *Query Type* drop-down list to create a query for BlackBerry devices.

- 5 Click the *Add Item* button .

The following dialog box appears if you are querying on Windows CE devices.

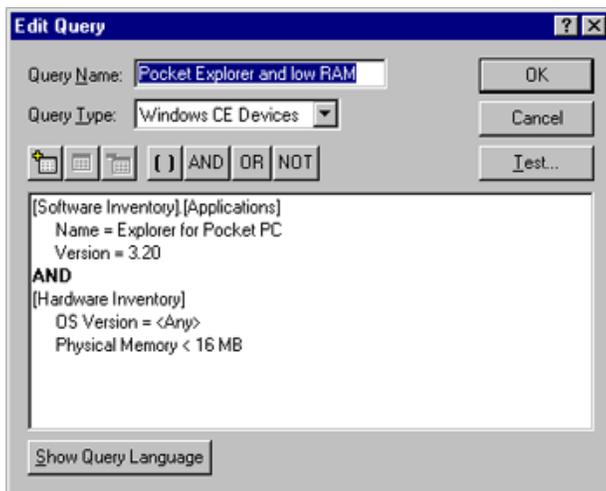


- 6 Select the first object you want to make part of the query, then click *OK*.



The first column lists the attributes you can make part of the query. Click the second column to display a down-arrow, click the down-arrow, then select the operator that you want to use. When you click the third column, a browse button displays. Click the browse button, then select a value for the query.

- 7 Select the attributes, operator, and values of the object that you want ZENworks Handheld Management to query on, then click *OK*.



If you want to the query to contain multiple objects, click the *Add Item* button again to add a new object.

---

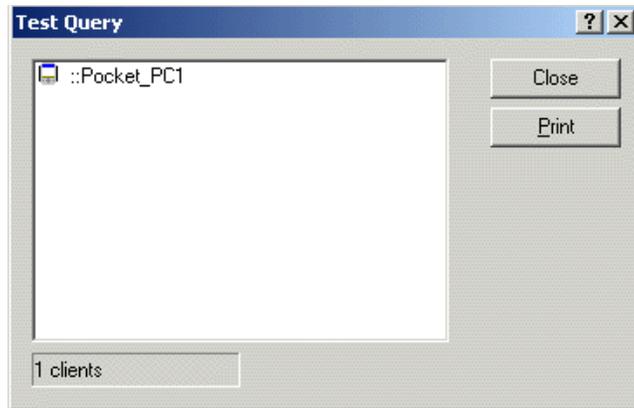
**NOTE:** Select the statements and click the parenthesis button  if you want to group statements using parentheses.

---

When you select multiple attributes to query on, be aware that they are filtered by the first object you pick.

For example, if the first attribute you select is OS Version = 3.5 and the second object you select is Free RAM, when you choose a specific value for Free RAM, the only values in the list are handheld devices running OS version 3.5.

If you want to review the results of the query that you have defined, click *Test*. The result is displayed in the Test Query dialog box.



8 Click *OK* to save the query.

### 3.1.2 Using Logical Operators

Logical operators in a query allow you to refine or expand the scope of the query. ZENworks Handheld Management provides the following logical operators:

**Table 3-1** Logical Operators provided by ZENworks Handheld Management

Operator	Description	Example
AND	Find devices that match the object criteria joined by the AND.	All Pocket PC devices AND less than 10 MB of free RAM.
OR	Find devices that match at least one of the criteria joined by the OR.	All Pocket PC devices OR all devices with more than 8 MB of RAM.
NOT	Find devices that match one criteria but not another.	All Palm OS devices and NOT with the application FileZ installed.

If you insert multiple objects for querying, ZENworks Handheld Management automatically adds an AND operator between the two object statements.

#### Understanding the Order of Operations

When evaluating a query, the following order of operations is used:

1. Expressions in parentheses
2. Expressions negated by NOT
3. Expressions joined by AND
4. Expressions joined by OR

## 3.2 Using Groups

Placing devices in groups can save you time when scheduling distributions, defining filters, and checking system status. With groups, you can use a single entity to manage multiple devices.

The following sections contain information to help you create and use groups:

- ◆ [Section 3.2.1, “Creating Groups,” on page 85](#)
- ◆ [Section 3.2.2, “Viewing the Properties of a Group,” on page 89](#)
- ◆ [Section 3.2.3, “Changing Group Membership,” on page 91](#)
- ◆ [Section 3.2.4, “Changing the Update Schedule of Query-Based Groups,” on page 91](#)
- ◆ [Section 3.2.5, “Deleting a Group,” on page 92](#)
- ◆ [Section 3.2.7, “Changing a Group’s Type,” on page 94](#)

## 3.2.1 Creating Groups

You can create custom groups based on the way you manage the handheld devices in your organization. For example:

- ◆ **Functional groups:** Sales, Marketing, Development, Admin, and so forth.
- ◆ **Geographical location:** Central, East, West, Europe, and so forth.

Think about the way you want to manage your handheld devices before you create groups. Keeping a clean and uncluttered group structure helps minimize confusion when scheduling distributions or defining filters for multiple groups.

ZENworks Handheld Management provides two types of user-created groups:

- ◆ **Static Groups:** Handheld devices are assigned to the group manually by the administrator or according to the settings specified in the Handheld Import policy.
- ◆ **Query-Based Groups:** Handheld devices are automatically placed in a group by ZENworks Handheld Management because they meet criteria specified in the query (for example, operating system version, manufacturer, and so forth).

Handheld devices can belong to multiple groups; they do not need to be limited to one group.

The following sections contain additional information about creating and viewing groups:

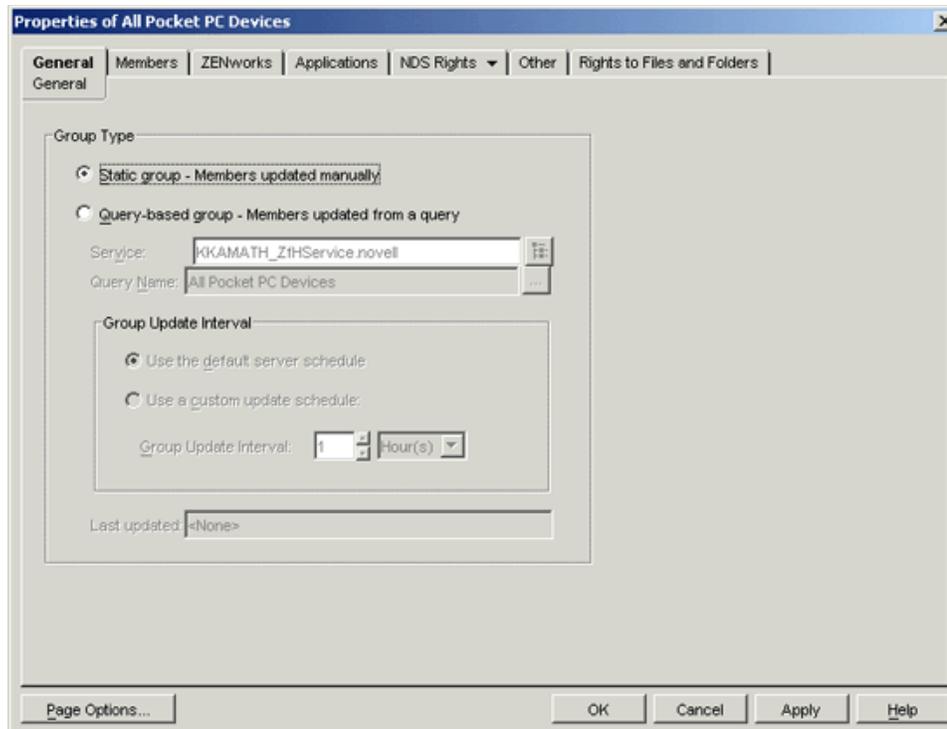
- ◆ [“Creating Static Groups” on page 85](#)
- ◆ [“Creating Query-Based Groups” on page 87](#)

### Creating Static Groups

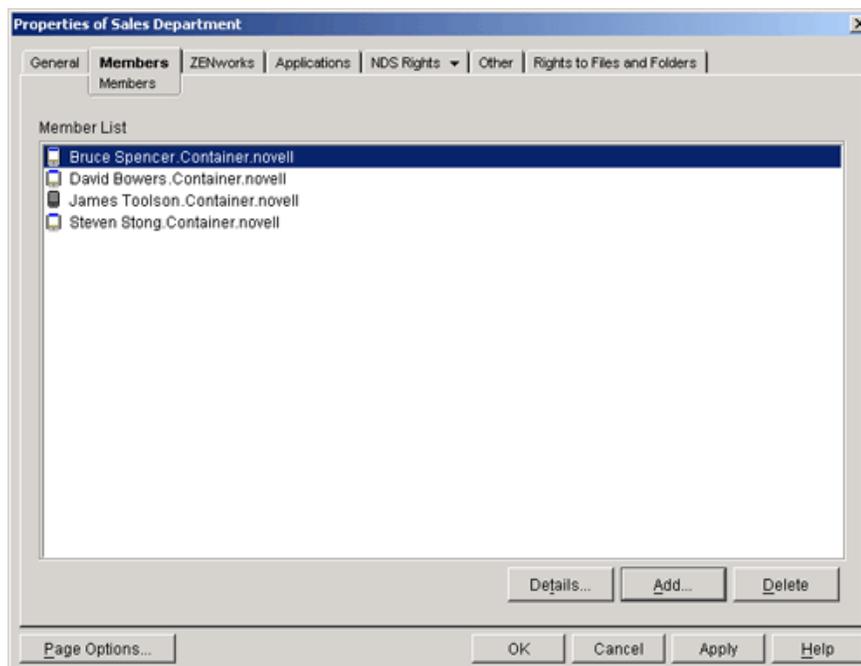
Handheld devices are manually assigned to a static group by the administrator.

To create a static group and assign members to it:

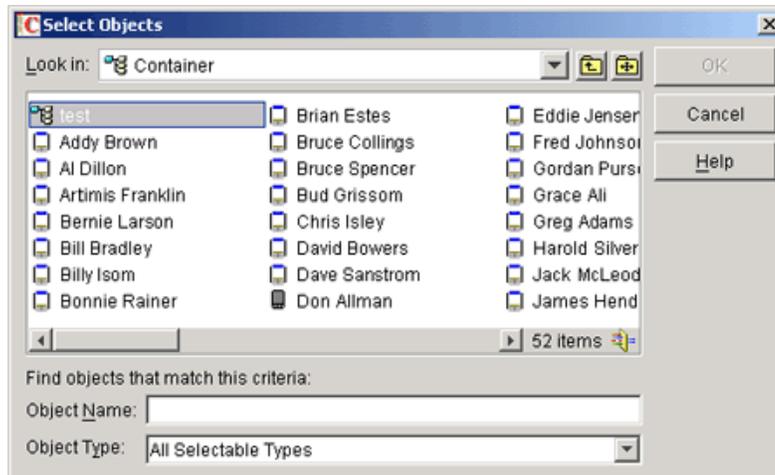
- 1 In ConsoleOne, click the container where you want to create the static group.
- 2 Click *File*, click *New*, then click *Object*.
- 3 Click *Handheld Group*, then click *OK*.
- 4 Specify a descriptive name for the group, select the *Define Additional Properties* check box, then click *OK*.
- 5 Select *Static Group - Members Updated Manually*.



6 Click the *Members* tab.



7 Click *Add Select Objects* to display the Select Objects dialog box.



8 Select the handheld device objects that you want to be members of this static group.

You can use Shift+click or Ctrl+click to select multiple handheld device objects.

9 Click *OK*.

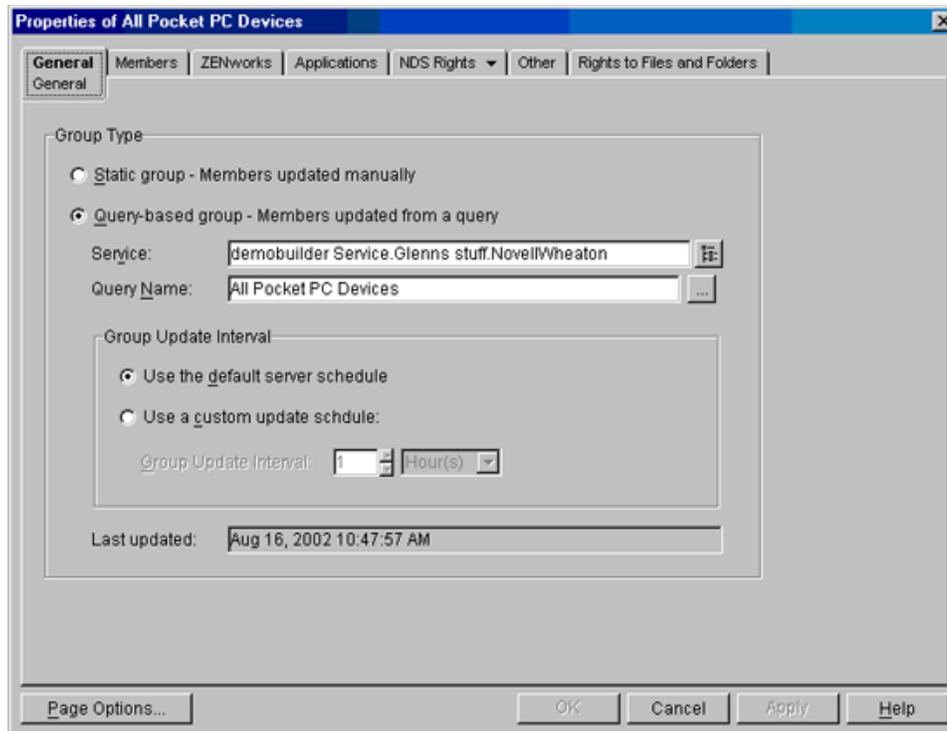
Static groups are indicated by  (yellow folder icon) in the ZENworks Handheld Management Inventory Viewer.

### Creating Query-Based Groups

Handheld devices are automatically placed in a query-based group by ZENworks Handheld Management because they meet criteria specified in the query (for example, operating system version, manufacturer, and so forth).

To create a query-based group:

- 1 In ConsoleOne, click the container where you want to create the query-based group.
- 2 Click *File*, click *New*, then click *Object*.
- 3 Click *Handheld Group*, then click *OK*.
- 4 Specify a descriptive name for the group, select the *Define Additional Properties* check box, then click *OK*.
- 5 Select *Query-Based Group - Members Are Updated From a Query*.



- 6 In the *Service* field, browse to the ZENworks Handheld Management Service object.
- 7 In the *Query Name* field, browse to the query on which you want to base the group, then click *OK*.

You need to create a query before it is displayed in the list. For more information, see [Section 3.1, “Using Queries,” on page 81](#).

---

**NOTE:** If you define and base a query-based group on a specific query and you later change the name of the query in the ZENworks Handheld Management Inventory Viewer, you must re-assign the new query to the group (it is not updated automatically). You cannot change the name of a query in ConsoleOne.

---

- 8 Select a Group Update Interval:

**Use the Default Server Schedule:** Select this option if you want the group to be updated with new members according to the default server schedule.

The group is populated with handheld device objects during the server’s next maintenance scan, which is hourly, by default. You can force an immediate update of a specific query-based group.

To do this:

- 8a** In ConsoleOne, right-click the *ZENworks Handheld Management Service* object, click *Actions*, then click *Scan Now*.

This performs the directory scan.

- 8b** Again in the ConsoleOne, right-click the desired *Handheld Group* object, click *Actions*, then click *Update*.

This updates the list of handhelds that belong to this group.

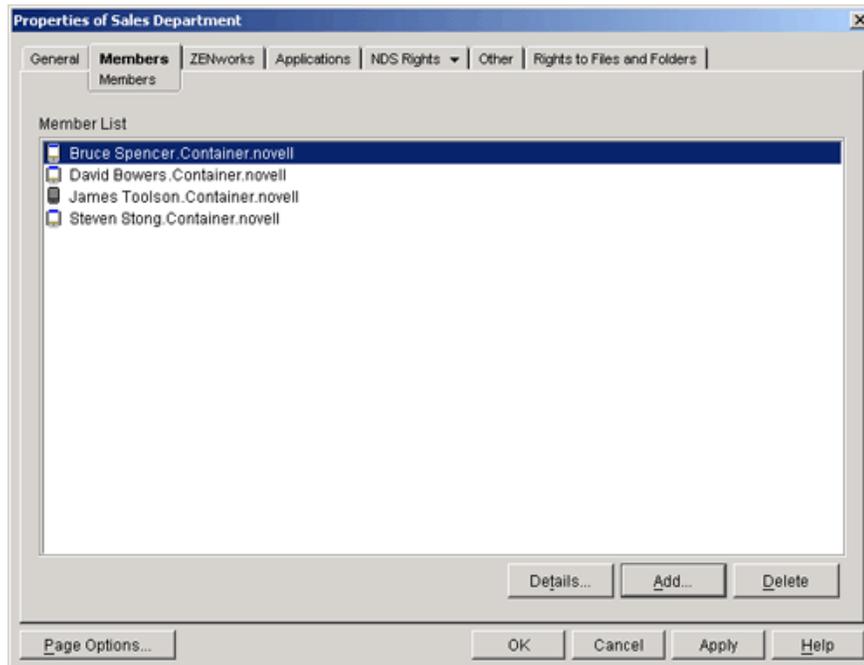
**Use a Custom Update Schedule:** Select this option if you want to specify a custom update schedule, then specify the group update interval.

9 Click *OK*.

The query-based group (indicated by  in the ZENworks Handheld Management Inventory Viewer) is created and populated with the handheld devices that currently match the criteria specified in the query.

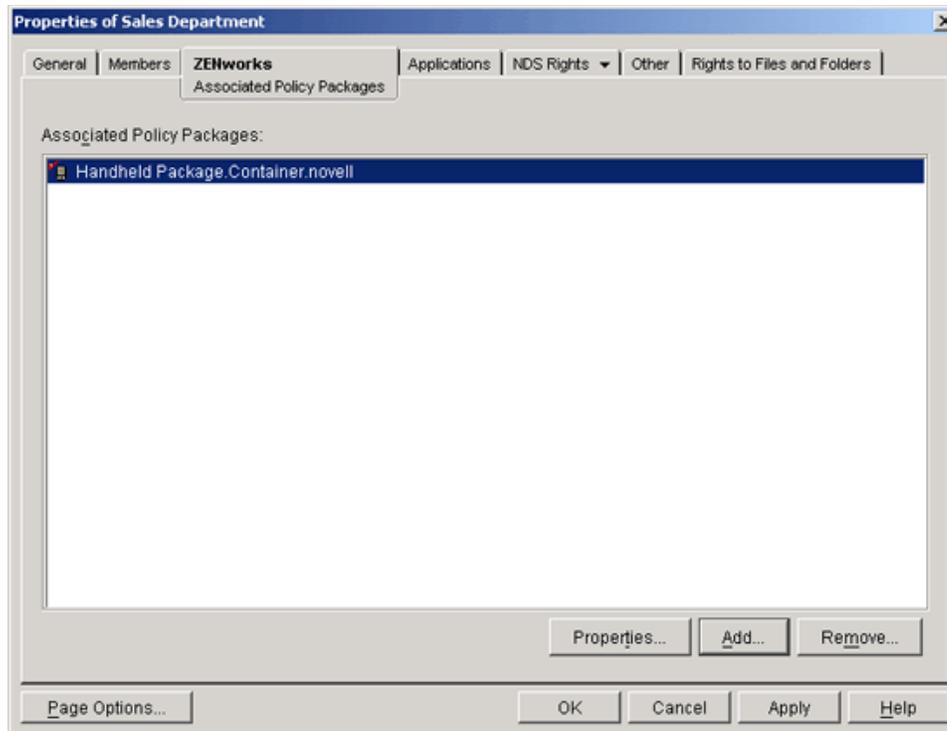
### 3.2.2 Viewing the Properties of a Group

- 1 In ConsoleOne, right-click the desired Handheld Group object, then click *Properties*.
- 2 Click the *Members* tab.



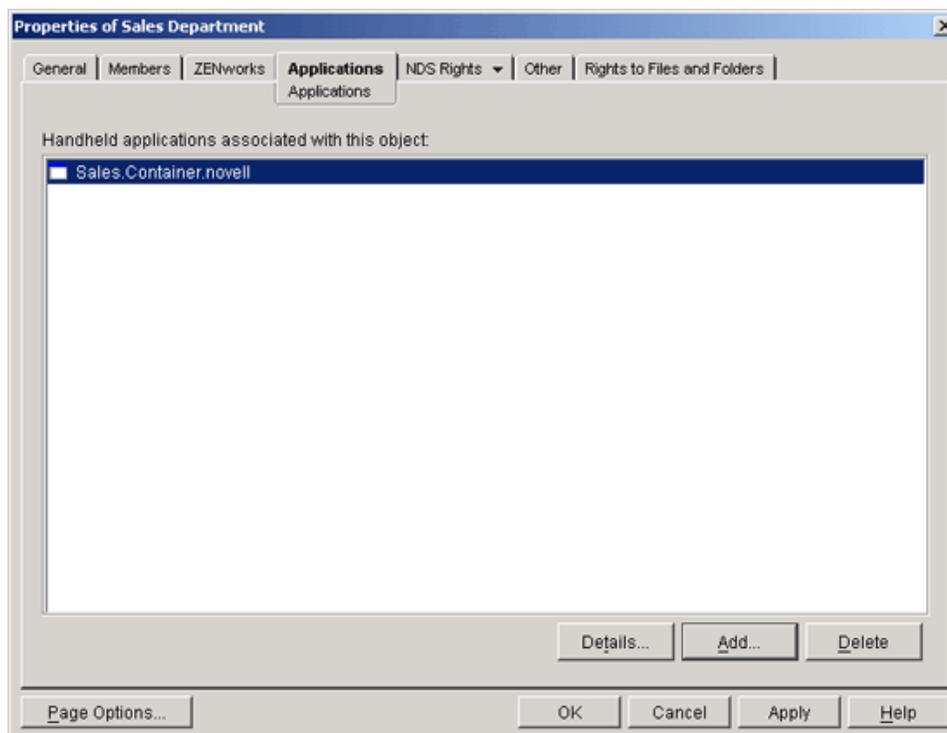
From the Members page, you can view which handheld objects are members of the selected group.

- 3 Click the *ZENworks* tab.



From the *Associated Policy Packages* page, you can view which policy packages are associated to the selected Handheld Group object.

- 4 Click the *Applications* tab.



From the *Applications* tab, you can view which Handheld Application objects are associated to the selected Handheld Group object.

### 3.2.3 Changing Group Membership

From time to time you need to modify static group membership by adding or deleting handheld device objects.

Query-based groups are updated according to the query parameters; membership cannot be changed manually without changing the criteria specified in the query.

For example, if you have divided your client groups by functions, and you have a user who transfers from Sales to Systems Engineering, you might need to delete the user from one group and add the user to another group.

Whenever you add a handheld device to a group, it automatically inherits any distributions assigned to that group.

The following sections contain additional information about changing group membership:

- ♦ “Adding a Device to a Static Group” on page 91
- ♦ “Removing a Device from a Static Group” on page 91

#### Adding a Device to a Static Group

- 1 In ConsoleOne, right-click the desired Handheld Group object, then click *Properties*.
- 2 Click the *Members* tab, then click *Add*.
- 3 Select the device you want to include in the group.  
You can use Shift+click or Ctrl+click to select multiple handheld device objects.
- 4 Click *OK*.

#### Removing a Device from a Static Group

- 1 In ConsoleOne, right-click the desired Handheld Group object, then click *Properties*.
- 2 Click the *Members* tab.
- 3 Select the device you want to remove from this group.  
You can use Shift+click or Ctrl+click to select multiple handheld device objects.
- 4 Click *Delete*.

### 3.2.4 Changing the Update Schedule of Query-Based Groups

When you create a query-based group, you can choose how often the group should be updated. Updating runs the query against existing handheld devices to check which devices match the criteria. Any handheld devices that match the criteria of the query are automatically placed in the appropriate query-based group; any handheld devices that no longer match the criteria of the query are automatically removed from the query-based group.

By default, query-based groups are updated once an hour. You can configure updating system wide so that all groups are updated on the same schedule or on a per-group basis. You can also turn off group updating (essentially making the query-based group a static group).

The following sections contain additional information:

- ♦ [“Changing the Update Schedule of a Specific Query-Based Group” on page 92](#)
- ♦ [“Changing the Update Schedule of All Query-Based Groups” on page 92](#)

### Changing the Update Schedule of a Specific Query-Based Group

- 1 In ConsoleOne, right-click the desired Handheld Group object, then click *Properties*.
- 2 On the *General* page, select *Use a Custom Update Schedule*, then specify the *Group Update Interval*.
- 3 Click *OK*.

If you modify the update schedule, the next maintenance scan (hourly, by default) detects the change and reschedule the update accordingly.

---

**NOTE:** You can force an immediate update of a specific query-based group. In ConsoleOne, right-click the *ZENworks Handheld Management Service* object, click *Actions*, then click *Scan Now* to perform a directory scan. Next, right-click the desired Handheld Group object, click *Actions*, then click *Update*.

---

### Changing the Update Schedule of All Query-Based Groups

- 1 In ConsoleOne, right-click the *ZENworks Handheld Management Service* object, then click *Properties*.
- 2 Select the desired Group Update Interval.
- 3 Click *OK*.

---

**NOTE:** You can force an immediate update of a specific query-based group. In ConsoleOne, right-click the *ZENworks Handheld Management Service* object, click *Actions*, then click *Scan Now* to perform a directory scan. Next, right-click the desired Handheld Group object, click *Actions*, then click *Update*.

---

## 3.2.5 Deleting a Group

As your installation changes over time, you might want to remove groups based on changes in your organization or in the types of equipment you are using, or you might just want to change the grouping scheme you've implemented.

To delete a group:

- 1 In ConsoleOne, right-click the desired Handheld Group object, then click *Delete NDS object*.
- 2 Click *Yes* to confirm the deletion.

The Handheld Group object is removed from the directory and its update schedule is removed from ZENworks Handheld Management.

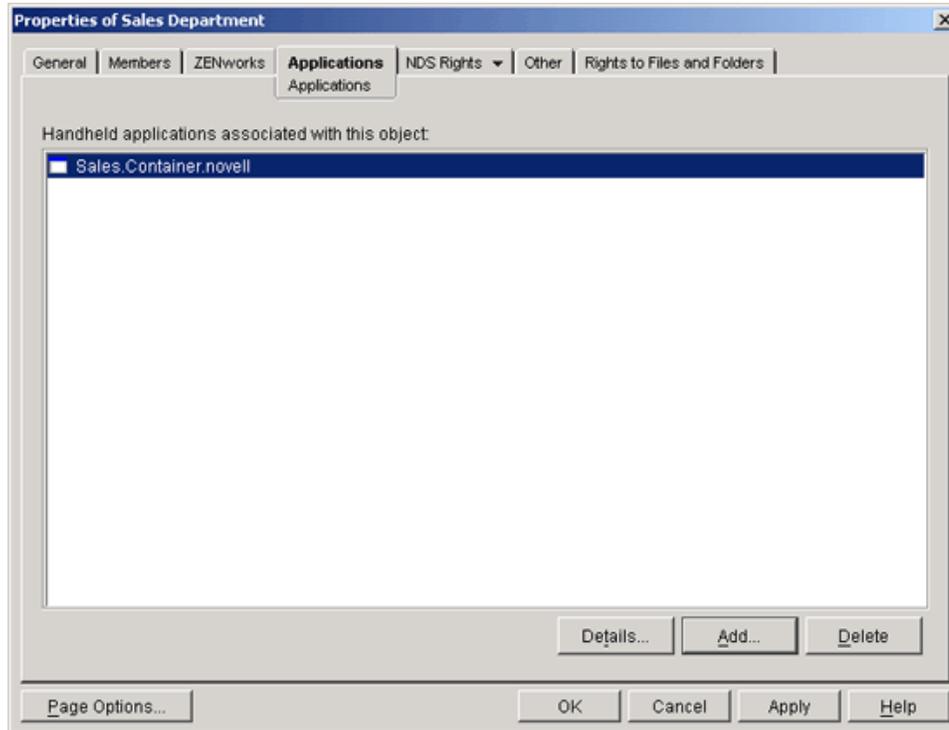
---

**NOTE:** When you delete a Handheld Group object, the object is deleted but the handheld device objects are not deleted from the directory; they simply lose their association with the deleted object and all distributions the device inherited that were targeted for the group.

---

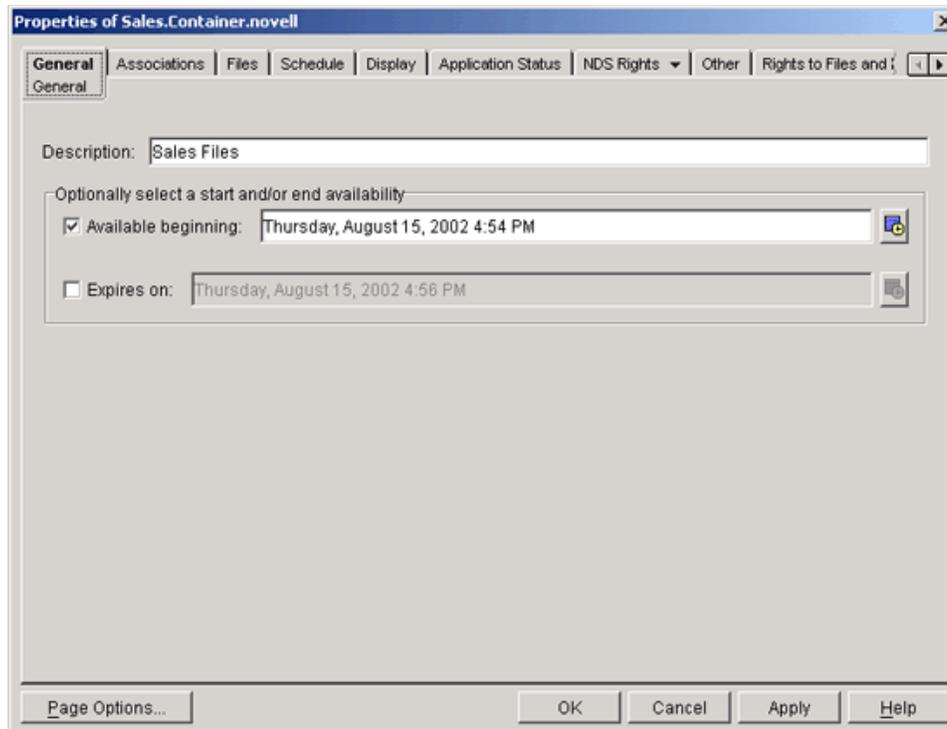
### 3.2.6 Viewing Handheld Application Objects Assigned to a Group

- 1 In ConsoleOne, right-click the desired Handheld Group object, then click *Properties*.
- 2 Click the *Applications* tab.



The Applications list displays the Handheld Application objects that are associated to the selected Handheld Group object.

- 3 To view an application object's details, click a Handheld Application object, then click *Details*. The *General* page displays the application object's properties, including its description, when it becomes available for distribution, and when it is no longer be available for distribution.



---

**NOTE:** When you are viewing the Handheld Application objects that are associated with a Handheld Group object, you only see Handheld Application objects that are associated to that specific group; you do not see all Handheld Application objects that are associated with all individual devices in that group.

---

### 3.2.7 Changing a Group's Type

To change a static group to a query-based group or a query-based group to a static group:

- 1 In ConsoleOne, right-click the desired Handheld Group object, then click *Properties*.
- 2 On the *General* page, click *Static Group* or *Query-Based Group*.  
If you choose Query-Based, select the query on which you want to base the group.
- 3 Click *OK*.

Because you cannot schedule the update of a static group, if you change a query-based group to a static group, the group's update schedule is removed from ZENworks Handheld Management.

# Distributing Software to Handheld Devices

# 4

This section describes how to create and distribute Handheld Application objects to handheld devices using Novell® ZENworks® 7 Handheld Management.

The following sections contain detailed information:

- ♦ [Section 4.1, “Understanding Handheld Application Objects,” on page 95](#)
- ♦ [Section 4.2, “Distributing Applications to Handheld Devices,” on page 97](#)
- ♦ [Section 4.3, “Displaying Handheld Application Object Status,” on page 104](#)
- ♦ [Section 4.4, “Modifying a Handheld Application Object,” on page 105](#)

## 4.1 Understanding Handheld Application Objects

ZENworks Handheld Management software distribution allows you to distribute Handheld Application objects to handheld devices as part of software distributions. Handheld Application objects contain collections of files that you want copied to your handheld devices.

Handheld Application objects usually consist of applications to install on handheld devices, for example, `.prc` files (for Palm OS devices); `.cab` files (for Windows CE devices); and `.alx`, `.ali`, `.cod`, and `.dll` files for BlackBerry devices.

The following sections contain additional information:

- ♦ [Section 4.1.1, “Specifying Source Files,” on page 95](#)
- ♦ [Section 4.1.2, “Understanding Automatic Application Updates,” on page 96](#)
- ♦ [Section 4.1.3, “Installing Software at a Predefined Time Even When the Device is Not Connected to the Network,” on page 97](#)

### 4.1.1 Specifying Source Files

When creating Handheld Application objects, you can select files, directories (and subdirectories), or both as the components of your object. You can also specify wildcard characters as a source file specification.

The following sections contain additional information:

- ♦ [“Files for Palm OS Devices” on page 96](#)
- ♦ [“Files for Windows CE Devices” on page 96](#)
- ♦ [“Files for BlackBerry Devices” on page 96](#)

## Files for Palm OS Devices

Only standard Palm OS file types should be selected when creating handheld application objects targeted for Palm OS devices. Supported file types include:

- ♦ Application files (\*.prc)
- ♦ Database files (\*.pdb)
- ♦ Query application files (\*.pqa)
- ♦ Configuration files (\*.pnc and \*.scp)

## Files for Windows CE Devices

- ♦ Because Windows CE devices support different processor types, ZENworks Handheld Management ensures that only CAB files compatible with the processor are copied to the Windows CE device when it synchronizes.

If CAB files are included in the handheld application object, they are automatically extracted and installed.

- ♦ Other files such as .txt, .html, or any other format supported by the handheld device.

## Files for BlackBerry Devices

Only standard RIM BlackBerry file types should be selected when creating handheld application objects targeted for BlackBerry devices. Supported file types include:

- ♦ Configuration files (\*.alx and \*.ali) along with Dynamic link library files (\*.dll)
- ♦ Configuration files (\*.alx) along with Java Applications (\*.cod)

ZENworks Handheld Management lets you distribute software to BlackBerry devices that are synchronized with a cradle; ZENworks Handheld Management does not support software distribution to BlackBerry devices using wireless synchronization.

## 4.1.2 Understanding Automatic Application Updates

For recurring software distributions (distributions that are scheduled to run more than once, for example, weekly), ZENworks Handheld Management automatically scans the application's source directories at the scheduled time and includes new or changed files with the software distribution.

This allows an administrator to copy new or updated files to the source directory for distribution to handheld devices without needing to create a new Handheld Application object.

For example, you distribute sales data weekly to your sales staff. Each Monday, before sending out the distributions, ZENworks Handheld Management scans the application's source directory. If there are any new or changed files added during the previous week, they are included in that Monday's application distribution. The handheld device receives only the files that have changed.

If the source directory has no changes during the week, the application is not sent (unless new handheld devices have been added to the list of recipients).

### 4.1.3 Installing Software at a Predefined Time Even When the Device is Not Connected to the Network

You can now specify the date and time when you want to install the Handheld Application object files on the device by configuring the date and time in the Handheld Application object's properties. This feature helps you in synchronizing the software updates across the Palm or Windows CE devices.

## 4.2 Distributing Applications to Handheld Devices

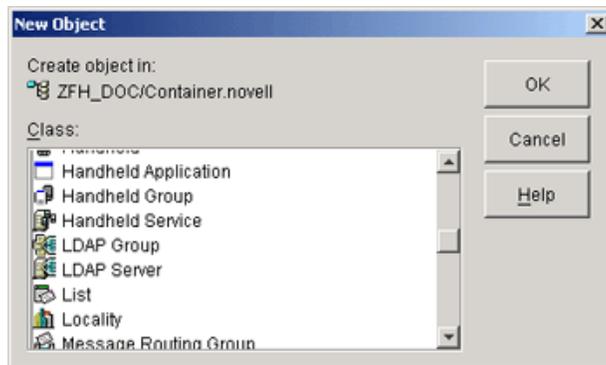
ZENworks Handheld Management lets you create and distribute Application objects to individual handheld devices or to groups of handheld devices.

The following sections contain additional information:

- ♦ [Section 4.2.1, "Creating a Handheld Application Object," on page 97](#)
- ♦ [Section 4.2.2, "Configuring a Handheld Application Object," on page 98](#)
- ♦ [Section 4.2.3, "Scheduling the Distribution of a Handheld Application Object," on page 102](#)

### 4.2.1 Creating a Handheld Application Object

- 1 In Novell ConsoleOne<sup>®</sup>, right-click the container where you want to create the Handheld Application object, click *New*, then click *Object* to display the New Object window.



- 2 Click *Handheld Application*, then click *OK* to display the New Application window.



- 3 In the *Name* field, type a name for the Handheld Application object, then click *OK*.

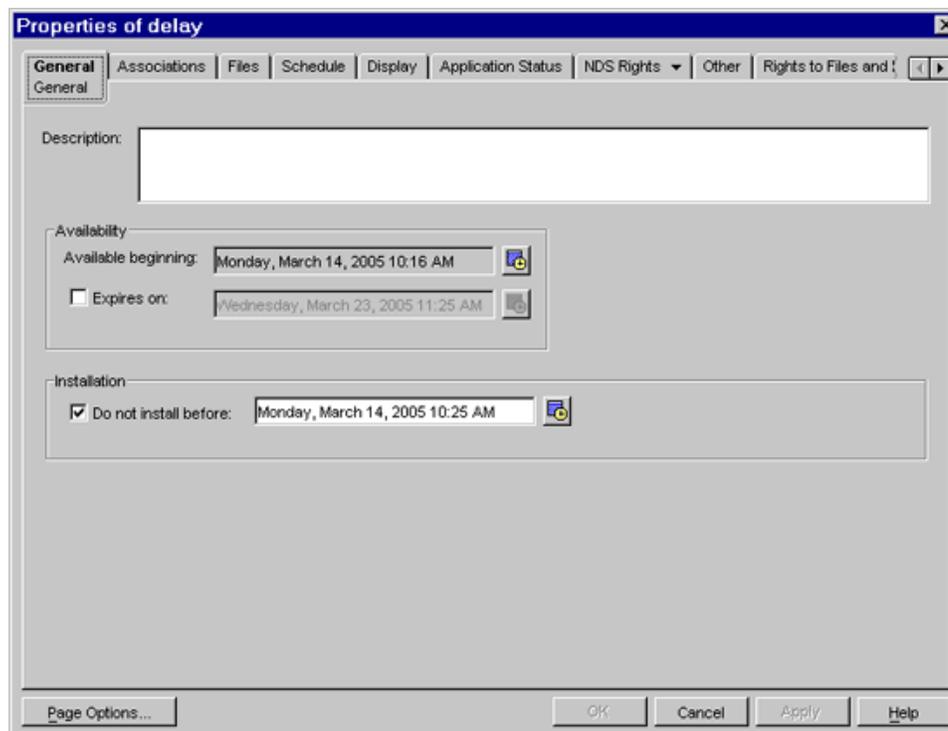
The object's name must conform to the following rules:

- ♦ The name must be unique in the container.
- ♦ Special characters are allowed. However, plus (+), equals (=), and period (.) must be preceded by a backslash (\) if used.
- ♦ Uppercase and lowercase letters, as well as underscores and spaces, are displayed as you first entered them, but they aren't distinguished. For example, ZENworks\_Handheld\_Management and ZENWORKS\_HANDHELD\_MANAGEMENT are considered identical.

4 Click *OK*.

## 4.2.2 Configuring a Handheld Application Object

1 In ConsoleOne, right-click the newly created Handheld Application object, then click *Properties* to display the *General* page.



2 Type a description of the Handheld Application object, if desired.

This description is available by viewing the properties of the object in ConsoleOne; users do not see this description during distribution.

3 Click the *Calendar/Clock* icon to specify a date and time that the application object is available for distribution.

If you do not change this setting, the object is distributed the next time the device connects to the ZENworks Handheld Management Access Point.

4 Select the *Expires On* option, then specify a date and time that the application object is no longer be available for distribution.

- 5 To specify the date and time when you want to install the Handheld Application object files (configured in the Files tab) on the device, select the *Do Not Install Before* option, and click the *Calendar/Clock* icon.

By default, the date and time is the date and time specified in the Available Beginning option.

If you specify a date or time later than the current date and time, the application object files are immediately deployed on the device after synchronization but installed at the specified date and time. If the device has older versions of the application object files installed, these files can be in use until the newer files are installed.

---

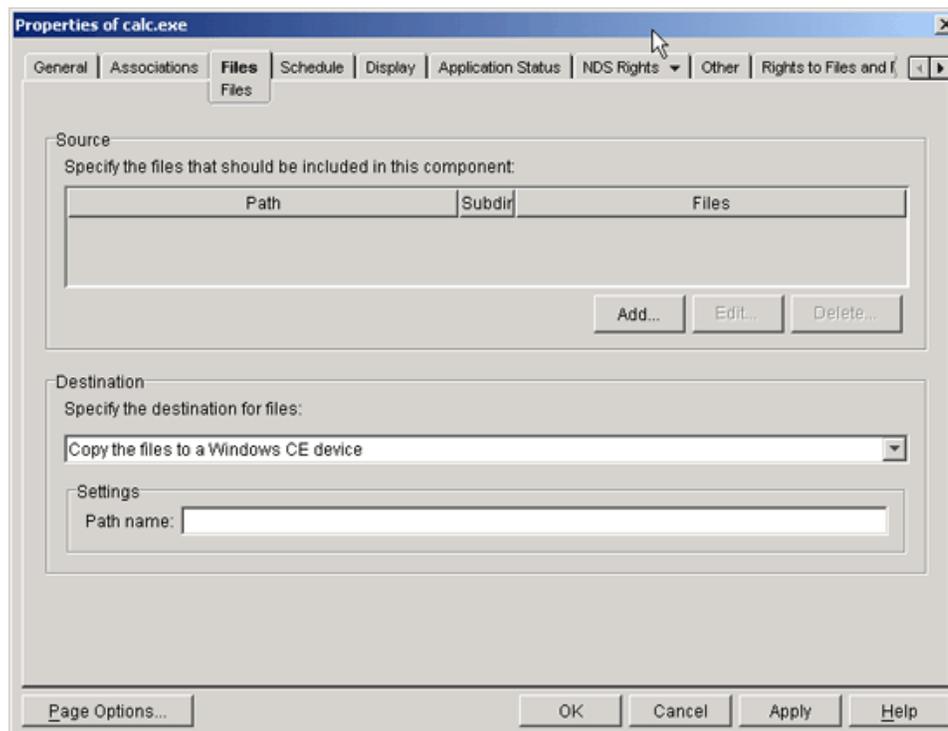
**IMPORTANT:** For Palm devices with a feature set version less than 4.0, the application is installed on the device as soon as you sync the device with the ZENworks Handheld Management server and not at the time configured in the handheld application object.

This feature is not supported for storage cards.

---

If you do not configure this option, the files are installed when they are sent to the device.

- 6 Click *Apply*.
- 7 Click the *Files* tab.



- 8 Click *Add*, then fill in the fields:

**Path:** Browse to or type the UNC path to the location of the application's executable file.

**Files:** Browse to or type the files that you want to include in the Handheld Application object.

---

**TIP:** You can use wildcard characters to specify the source files.

---

**Include Subdirectories of This Path:** Enable this option if you want to include subdirectories of the path.

---

**IMPORTANT:** If you want to access application data on a Novell NetWare<sup>®</sup> volume, you must install the Novell Client<sup>™</sup> on the ZENworks Handheld Management Server. You might be able to browse to and select application data on the NetWare volume without the Novell Client installed, but the handheld application object is not built unless the Novell Client is installed on the ZENworks Handheld Management Server.

---

9 Click *OK*.

10 In the *Destination* field, select a destination for the files from the drop-down list:

- ♦ **Copy the files to a Windows CE device:** Copies the files that are in the Handheld Application object to an individual Windows CE device or to a group of Windows CE devices.

---

**NOTE:** If the files being copied already exist on Windows CE, ZENworks Handheld Management overwrites the files with the files that are in the Handheld Application object.

---

- ♦ **Copy the files to a Palm device:** Copies the files that are in the Handheld Application object to an individual Palm OS device or to a group of Palm OS devices.

---

**NOTE:** If the files in the Handheld Application object are newer than the files on the Palm OS device, ZENworks Handheld Management overwrites the old files with the new ones.

---

- ♦ **Copy the files to a RIM BlackBerry device:** Copies the Application object files to the sync machine and queues the files in the appropriate directory for installation by the Application Loader.

---

**NOTE:** ZENworks Handheld Management overwrites the files on the device with the Handheld Application object files only if the files being installed are newer than then files on the device.

---

- ♦ **Copy the files to a temporary location on the sync machine:** Copies the files to a temporary location on the machine that the handheld device synchronizes with.

Some applications require that users run Windows desktop routines before installing files on Palm OS or Windows CE devices. If this is the case, select *Copy the files to a temporary location on the sync machine* so that users can run those routines before installing them on the handheld device. The iPAQ ROM update is an example of an application that you would use this option for.

---

**NOTE:** The distribution fails when the files contained in a Handheld Application object are copied to a handheld device or sync machine where the same files are already in use. If you enable automatic updates for the Handheld Application object, the device receives the distribution at its next scheduled time, if the files on the machine are not in use at that time. If the Handheld Application object is scheduled to run only one time, you must resend it when the files are not in use.

---

11 **Windows CE Devices:** If you select *Copy the Files to a Windows CE Device*, you can specify the path on the Windows CE device where you want the files copied to.

or

**Palm OS Devices:** If you select *Copy the Files to a Palm Device* and you have a storage card installed, select *Install Files on Storage Card*, if desired.

ZENworks Handheld Management supports expansion cards in Palm OS devices running Palm OS 4.x and later. Expansion cards are usually referred to as secure digital (SD) cards or memory sticks.

---

**IMPORTANT:** If you select the *Install Files on Storage Card* option, ZENworks Handheld Management installs the files only to a storage card. If the storage card is not available, the installation fails; ZENworks Handheld Management does not install the files in the Palm OS device's main memory.

---

or

**Sync Machines:** If you chose *Copy the Files to a Temporary Location* on the Sync Machine, specify the command to run, then select *Fail Installation if Command Reports Failure*, if desired. These machines must be running the ZENworks Handheld Management Desktop Synchronization Integration or ZENworks Handheld Management Access Point.

You can specify whether or not dialog boxes display when files contained in this Handheld Application object are installed on machines that associated handheld devices synchronize with. Click the *Display* tab to configure these settings. Click *Help* for more information on each option.

or

**RIM BlackBerry Devices:** If you chose *Copy the Files to a RIM BlackBerry Device*, you can specify whether or not dialog boxes display when files contained in this Handheld Application object are installed on desktop computer that associated BlackBerry devices synchronize with. For example, you could display a message on the desktop computer to inform users that files have been queued and they should run the BlackBerry Application Loader. Click the *Display* tab to configure these settings. Click *Help* for more information on each option.

**11a** (Optional) To assign a desktop computer to the selected BlackBerry device, right-click a BlackBerry device object, click *Properties*, then click *Assign Desktop* on the *General* page, select the desired desktop computer from the list, then click *OK*.

Because ZENworks Handheld Management lets you distribute software to BlackBerry devices that are synchronized with a cradle (ZENworks Handheld Management does not support software distribution to BlackBerry devices using wireless synchronization), this association tells the ZENworks Handheld Management Server where to send handheld application objects during a distribution.

---

**IMPORTANT:** The Handheld Application object you configured cannot be distributed to handheld devices until you associate the object with individual handheld devices or to a group of handheld devices.

---

**12** Click the *Associations* tab, then click *Add*.

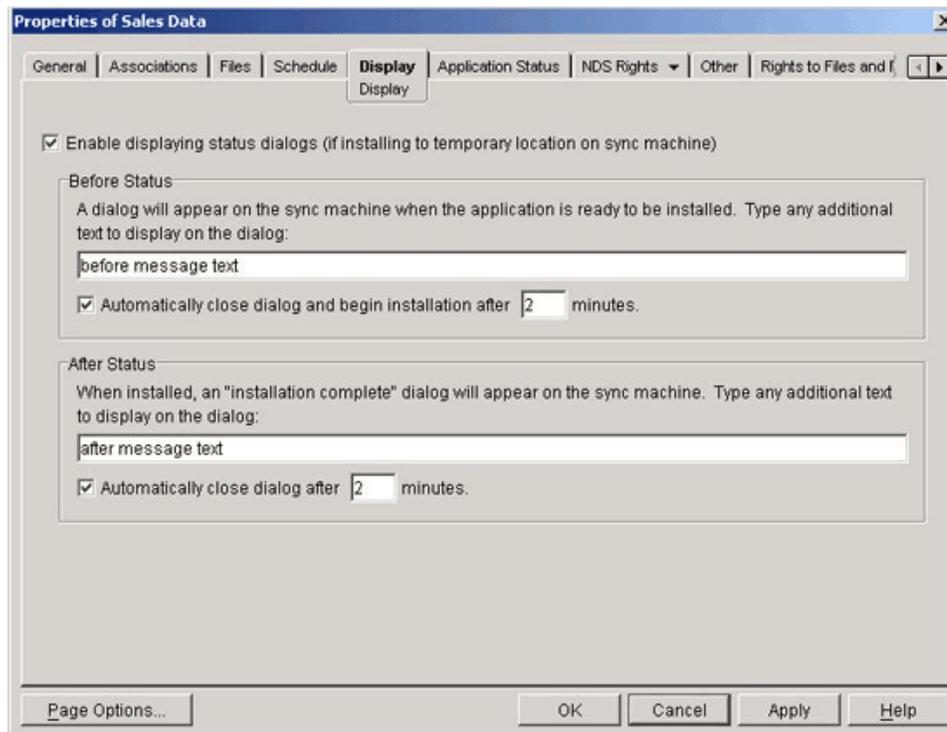
**13** Select the handheld devices, User objects, or groups of handheld devices you want to distribute the Handheld Application object to, then click *OK*.

The Handheld Application object is distributed to each handheld device the next time it connects or according to the application object's schedule.

If you are distributing an application, you probably do not want the distribution to recur. If you are distributing files, such as marketing information, you can schedule the distribution to recur using the *Schedule* page.

**14** Click *OK* to save your settings.

- 15 If you chose *Copy the Files to a Temporary Location on the Sync Machine* or *Copy the Files to a RIM BlackBerry Device* in [Step 10 on page 100](#), click the *Display* tab.



- 16 Fill in the fields:

**Show Status Dialogs on Desktop Sync Machine:** Select this option if you want informational dialog boxes to display on desktop computers when application files are installed.

**Before Dialog:** Any information that you type in this text box displays on the dialog box that displays on the desktop computer. You can use this text box to provide any additional information or instructions that you want users to see when the files are installed.

**Automatically Close Dialog and Begin Installation After \_ Minutes:** Select this option, then specify the number of minutes that you want to wait before installing the files. Using this option enables installation of the files even if the user is away from his or her desk when the files are ready to be installed.

**After Dialog:** Type any additional text to display on the dialog box after the files are installed.

**Automatically Close Dialog After \_ Minutes:** Select this option, then specify the number of minutes that you want to wait before closing the Installation Complete dialog box.

- 17 Click *OK* to save your settings.

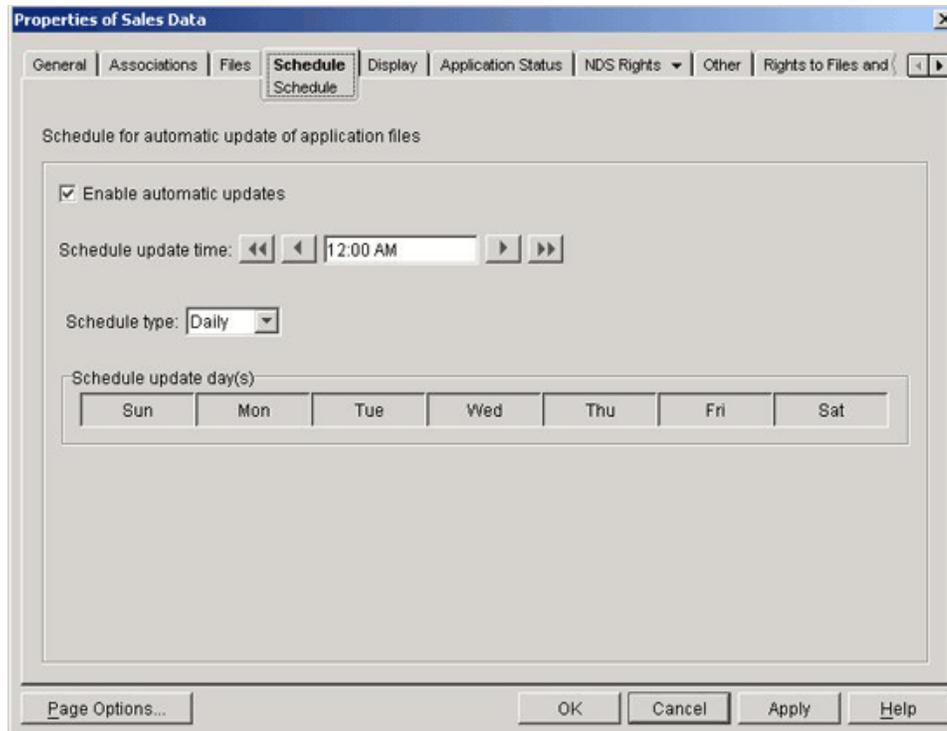
### 4.2.3 Scheduling the Distribution of a Handheld Application Object

If your handheld application object contains files that you want to redistribute periodically, use the *Schedule* page to schedule its distribution.

If you want the handheld application object to be distributed only once, you do not need to schedule it; the object is distributed the next time the associated handheld devices synchronize.

To schedule the distribution of a Handheld Application object:

- 1 In ConsoleOne, right-click the Handheld Application object, then click *Properties* to display the *General* page.
- 2 Click the *Schedule* tab.



- 3 Click *Enable Automatic Updates*.

If you select this option, ZENworks Handheld Management scans the source directory at the scheduled time for any additions or changes to the source files. If something has changed, the application is pushed out at that time.

- 4 Specify an update time in the *Schedule Update Time* field.
- 5 Select a schedule from the *Schedule Type* drop-down list:
  - ♦ Daily
  - ♦ Weekly
  - ♦ Monthly
  - ♦ Yearly

---

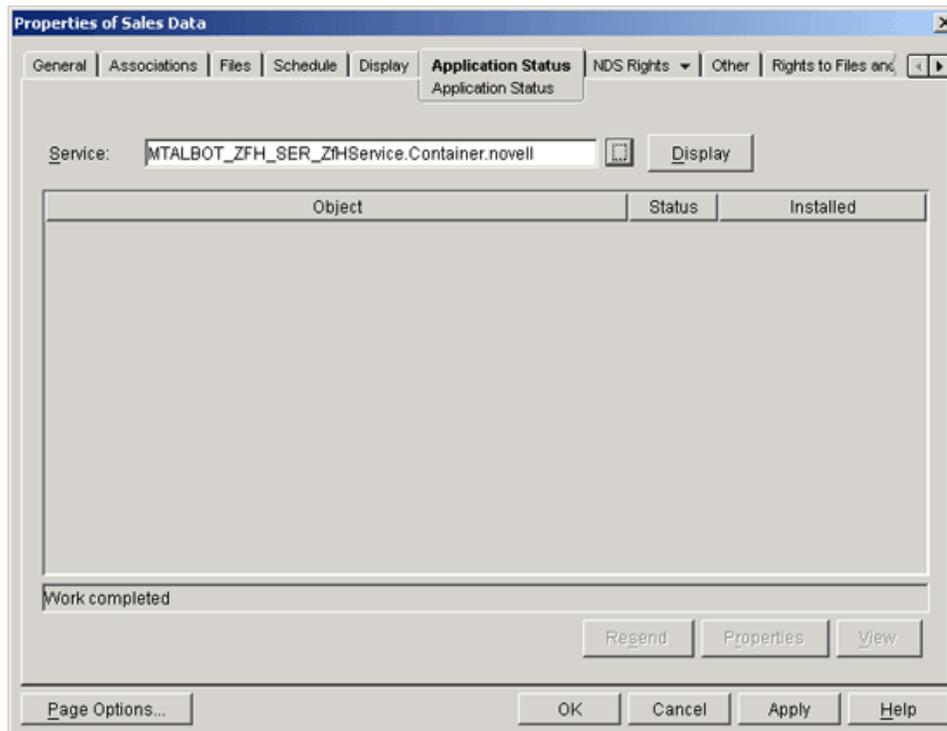
**NOTE:** Click the *Help* button for detailed instructions about each schedule.

---

- 6 Specify the hours and days that you want the schedule to activate.
- 7 Click *OK*.

## 4.3 Displaying Handheld Application Object Status

- 1 In ConsoleOne, right-click the Handheld Application object, then click *Properties* to display the *General* page.
- 2 To view the status of a Handheld Application object, click the *Application Status* tab.



The results lists the Handheld Application objects distributed by the ZENworks Handheld Management service listed in the *Service* field, the status of each object, and the version number of each Handheld Application object.

The status of the application can be any of the following:

- ♦ **Canceled:** The distribution of the application was cancelled because the distribution it is associated with was deleted.
- ♦ **Failed:** The application could not be installed by the device.
- ♦ **Installed:** The application was installed without a problem.
- ♦ **Pending:** The application has not been distributed yet or results have not yet been made available.
- ♦ **Skipped:** The device contained the current version of the application or the application has not changed.

---

**TIP:** You can force an application to be installed on an associated handheld device, even if it has already been installed on the device, by using the *Resend* button on the *Application Status* page of the application object. You cannot force ZENworks Handheld Management to resend an application by deleting the application from the handheld device; you must use the *Resend* button.

---

## 4.4 Modifying a Handheld Application Object

You can add or delete components and distribute the changes without creating a new Handheld Application object.

The following sections contain additional information about modifying Handheld Application objects:

- ♦ [Section 4.4.1, “Modifying the Contents of a Handheld Application Object,” on page 105](#)
- ♦ [Section 4.4.2, “Scanning for Updated Components,” on page 105](#)
- ♦ [Section 4.4.3, “Deleting a Handheld Application Object,” on page 106](#)
- ♦ [Section 4.4.4, “Deleting a Handheld Application Object’s Associations,” on page 106](#)

### 4.4.1 Modifying the Contents of a Handheld Application Object

If you change components of a Handheld Application object (for example, the files that are included in the object) or you want to change the object’s associations, you can modify the object using ConsoleOne; you do not need to create a new Handheld Application object.

To modify the contents a Handheld Application object, follow the steps in [Section 4.2.2, “Configuring a Handheld Application Object,” on page 98](#), modifying the settings as appropriate.

### 4.4.2 Scanning for Updated Components

For recurring distributions of Handheld Application objects, ZENworks Handheld Management scans component directories at the scheduled time to see if their contents have changed before sending out the distribution. Therefore, recurring distributions send out the most recent versions of files that make up the application.

For example, if you add or replace files in the source directory for the application, those files are included the next time the Handheld Application object is scheduled to be distributed. You do not need to create a new Handheld Application object to include the files. See [Section 4.1.2, “Understanding Automatic Application Updates,” on page 96](#) for an example of how ZENworks Handheld Management automatic updates work.

You can also force a source directory to be scanned.

---

**IMPORTANT:** Because the ZENworks Handheld Management Server scans component directories for recurring distributions, the ZENworks Handheld Management Server service account must have proper rights to access the component directories.

---

To force a source directory scan immediately and distribute the Handheld Application object if the directory has changed:

- 1 In ConsoleOne, right-click the desired Handheld Application object, then click *Actions*.
- 2 Click *Update Now*.

### 4.4.3 Deleting a Handheld Application Object

If you decide that you do not want to distribute a specific Handheld Application object again, you can delete its object from the directory using ConsoleOne.

- 1 In ConsoleOne, right-click the desired Handheld Application object, then click *Delete NDS Object*.
- 2 Click *Yes* to confirm the deletion.

### 4.4.4 Deleting a Handheld Application Object's Associations

If you decide that you do not want to distribute a specific Handheld Application object to a handheld device, User object, or to a group of handheld devices, but you want to keep the object in the directory for future use, you can delete the object's associations.

- 1 In ConsoleOne, right-click the appropriate Handheld Application object, then click *Properties*.
- 2 Click the *Associations* tab, select the handheld devices or groups you want to remove the association from, then click *Delete*.

Removing an association from a handheld device does not remove that application from the handheld device.

- 3 Click *OK*.

# Using Inventory and Reports

# 5

After you install the Novell® ZENworks® 7 Handheld Management software, **set up Handheld Import**, and users have synchronized their handheld devices, you are ready to collect software and hardware inventory for all managed handheld devices in your ZENworks Handheld Management system.

Managing software and hardware assets is a critical function for most companies. ZENworks Handheld Management inventory capabilities capture asset information to support analysis, troubleshooting, and planning.

ZENworks Handheld Management lets you collect and view software and hardware inventory information for Palm\* OS\*, Windows\* CE (including Pocket PCs), and BlackBerry\* handheld devices.

During the ZENworks Handheld Management Server installation, if you selected the “Internal ODBC-Compatible Database” option, then you must set the path for database files in the ZENworks Handheld Management service object.

To set the path for database files in the ZENworks Handheld Management service object:

- 1 In Novell ConsoleOne®, right-click the ZENworks Handheld Management service object, then click *Properties*.
- 2 Click the *General* tab.
- 3 In the *Remote Path* section, add the complete path to the ZENworks Handheld Management server installation folder share. For example, `\\myZfHServer\ZfH`.  
Make sure that this share has the Read-Write permission for the user who has launched ConsoleOne.

Using ZENworks Handheld Management, you can do the following:

- ♦ View software inventory information across all your handheld devices or on a per-device basis to ensure software licensing compliance
- ♦ Plan for software and hardware upgrades with a complete view of application versions and hardware configurations
- ♦ Troubleshoot problems with a thorough knowledge of each handheld device’s hardware and software

The following sections contain additional information:

- ♦ [Section 5.1, “Viewing Software Inventory,” on page 108](#)
- ♦ [Section 5.2, “Viewing Hardware Inventory,” on page 118](#)
- ♦ [Section 5.3, “Viewing Network Information,” on page 120](#)
- ♦ [Section 5.4, “Using Inventory Reports,” on page 120](#)
- ♦ [Section 5.5, “Printing Data from the ZENworks Handheld Management Inventory Viewer,” on page 123](#)

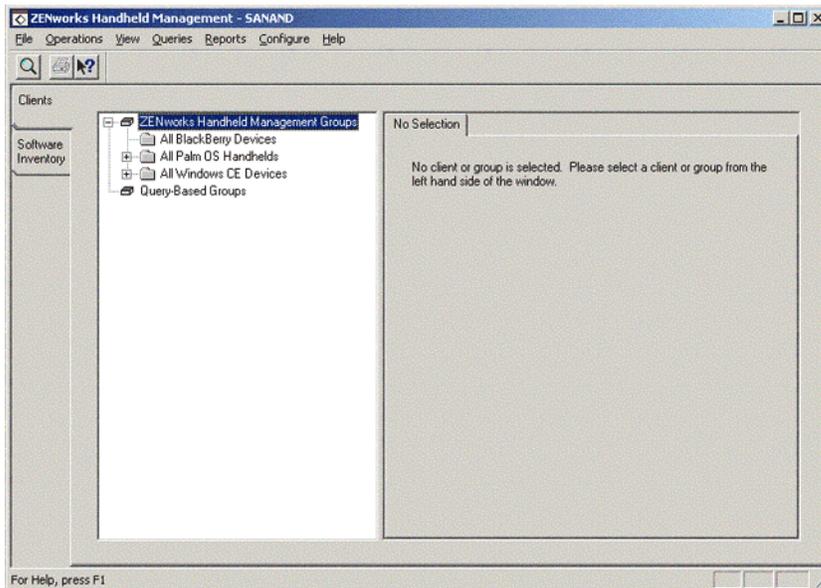
## 5.1 Viewing Software Inventory

Software inventory is collected once a day from the handheld device. Software inventory data is displayed in the ZENworks Handheld Management Inventory Viewer.

ZENworks Handheld Management lets you collect and view software inventory information for Palm OS, Windows CE (including Pocket PCs), and BlackBerry devices.

To view software inventory:

- 1 In ConsoleOne, right-click a handheld device object, click *Actions*, then click *Inventory*.
- 2 Click the *Software Inventory* tab.



The Software Inventory list in the left frame contains directories named Palm Applications, BlackBerry Applications, and Windows CE Applications. You can expand these directories to display a list of all the applications found on all handheld devices in your system.

If ZENworks Handheld Management cannot identify an application on a Windows CE device, the application is listed in the Unidentified Windows CE Files tree in the Software Inventory list in the left frame.

The right frame contains a *Name* column that lists each application in alphabetical order by company name and a *Version* column that lists each application's version number.

---

**NOTE:** For BlackBerry devices, ZENworks Handheld Management collects software inventory only for applications that display on the device's *Options > Status* screen.

---

The following sections contain additional information:

- ♦ [Section 5.1.1, “Viewing Software Inventory for a Specific Handheld Device,” on page 109](#)
- ♦ [Section 5.1.2, “Viewing Software Inventory Across All Palm OS, BlackBerry, or Windows CE Devices in Your System,” on page 109](#)

- ♦ [Section 5.1.3, “Identifying Files for Windows CE Devices,” on page 111](#)
- ♦ [Section 5.1.4, “Ignoring or Identifying Windows CE Files and Applications,” on page 113](#)

## 5.1.1 Viewing Software Inventory for a Specific Handheld Device

ZENworks Handheld Management lets you view the applications installed on a specific Palm OS, BlackBerry, or Windows CE handheld device. You can also view application details about a specific application on any handheld device in your system.

To view software inventory for a specific device:

- 1 In ConsoleOne, right-click any handheld device object, click *Actions*, then click *Inventory* to open the ZENworks Handheld Management Inventory Viewer.
- 2 Click the *Clients* tab, then expand the ZENworks Handheld Management Groups directory.
- 3 Expand the desired platform directory in the tree: *All BlackBerry Devices*, *All Palm OS Handhelds*, or *All Windows CE Devices*.
- 4 Click the handheld device whose software applications you want to view.
- 5 Click the *SW Inventory* tab in the right pane.

Depending on which platform you chose in [Step 3](#), the information displayed in the SW Inventory page varies.

**Palm OS Devices:** Lists the application name, version, creator ID, and whether the application is installed in ROM, RAM, or on a storage card.

**BlackBerry Devices:** Lists the application name and version.

**Windows CE Devices:** Lists the name of the company that created the application, the application name, and the version.

---

**NOTE:** You can determine when the last inventory scan was performed by looking at the Last Software Inventory information at the bottom of the dialog box.

---

- 6 To view details about a specific application, double-click the application.

The View Application Details dialog box displays the application’s size, creation date, backup date, and more.

## 5.1.2 Viewing Software Inventory Across All Palm OS, BlackBerry, or Windows CE Devices in Your System

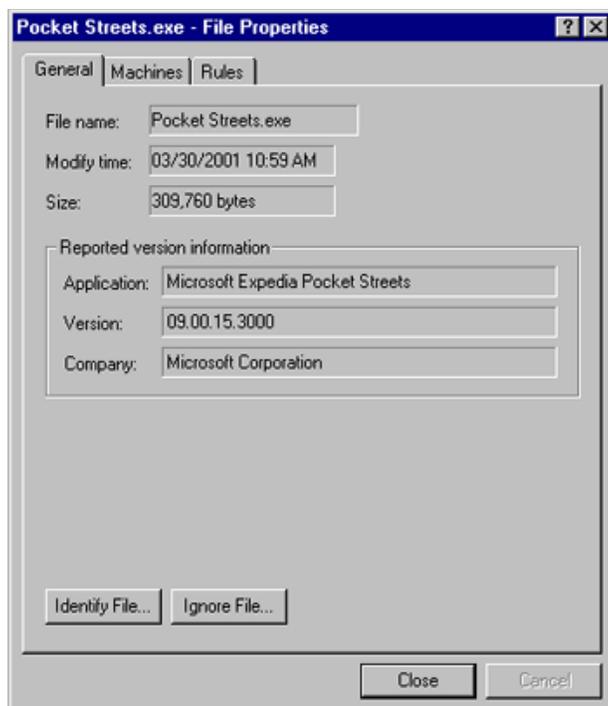
ZENworks Handheld Management lets you view software inventory information across all of the Palm OS, BlackBerry, or Windows CE devices in your system. Suppose, for example, that you want to ensure licensing compliance for a certain application. ZENworks Handheld Management helps you determine how many copies of that application users have installed on individual devices in your organization. You can also display a list containing the name of each device that has the application installed.

To view software inventory information for all Palm OS, BlackBerry, or Windows CE devices in your system:

- 1 In ConsoleOne, right-click any handheld device object, click *Actions*, then click *Inventory* to open the ZENworks Handheld Management Inventory Viewer.
- 2 Click the *Software Inventory* tab on the left side of the dialog box, then expand the desired platform folder in the tree: *Palm Applications*, *BlackBerry Applications*, or *Windows CE Applications*.  
If you expand the *Windows CE Applications* folder, you also need to expand the company folder.
- 3 Click the application whose details you want to view.
- 4 Click the *General* tab to view the application's details, which vary depending on the platform.  
**Palm OS Applications:** Lists the application's name, the version, the Creator ID, the icon name, and how many installations of the application exist on the Palm OS devices in your system.  
**BlackBerry Applications:** Lists the application's name and its version, and the total number of copies installed.  
**Windows CE Applications:** Lists the application's name, version, company name, the files that make up the application, and the total number of copies installed.
- 5 Click the *Clients* tab in the right frame to view all the handheld devices in your system that have the selected application installed and to list additional details, depending on the platform.  
**Palm OS Devices:** Lists information about the individual devices that the selected application is installed on, including the name of the device, where the application is installed (RAM, ROM, or on a Storage Card), the application's size, create date, modify date, and record count.  
**BlackBerry Devices:** Lists information about the individual devices that the selected application is installed on, including the name of the device, the application's size, and more.  
**Windows CE Devices:** Lists information about the individual devices that the selected application is installed on, including the name of the device, the last time the application was scanned, and the installation path on those devices.

For Windows CE applications, you can also view file details if you want to know details about a specific file that is part of an application (for example, to determine the version of a specific executable file you are running).

- 1 Click the *Software Inventory* tab in the left frame.
- 2 Click the *General* tab in the right frame.
- 3 Double-click the application file in the *Application Files* list box.



The File Properties dialog box provides a quick snapshot of information about the file.

Click the following tabs to view information about the selected file:

- ♦ **General:** Lists all application version information, including filename, modify time, and file size.
- ♦ **Clients:** Lists the Windows CE devices that the file is installed on.
- ♦ **Rules:** Lists the Identification and Ignore rules created for the file. For more information, see [“Viewing Windows CE Identified and Ignored File Rules”](#) on page 117.

### 5.1.3 Identifying Files for Windows CE Devices

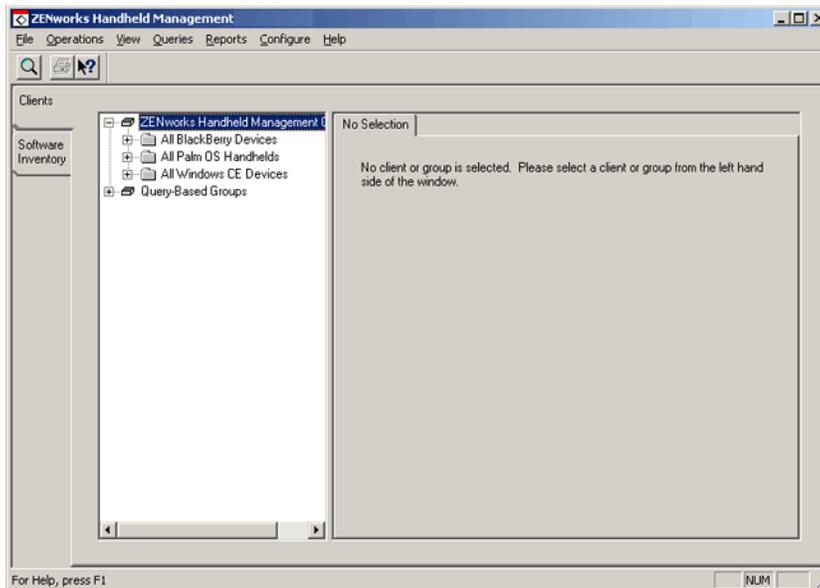
If a Windows CE application file does not have any product information associated with it, ZENworks Handheld Management considers it “unidentified” and stores it in the Unidentified Windows CE Files folder.

There may be some unidentified files that you want ZENworks Handheld Management to recognize as valid applications whenever ZENworks Handheld Management finds the files on a device. For these files, ZENworks Handheld Management allows you to specify the product, company, and version information so that the files are identified as applications.

When you identify files, an identification rule is created for the files. After they are identified, the files appear in the Windows CE Applications folder (with a list of the devices it is found on). The files are then removed from the list of unidentified files.

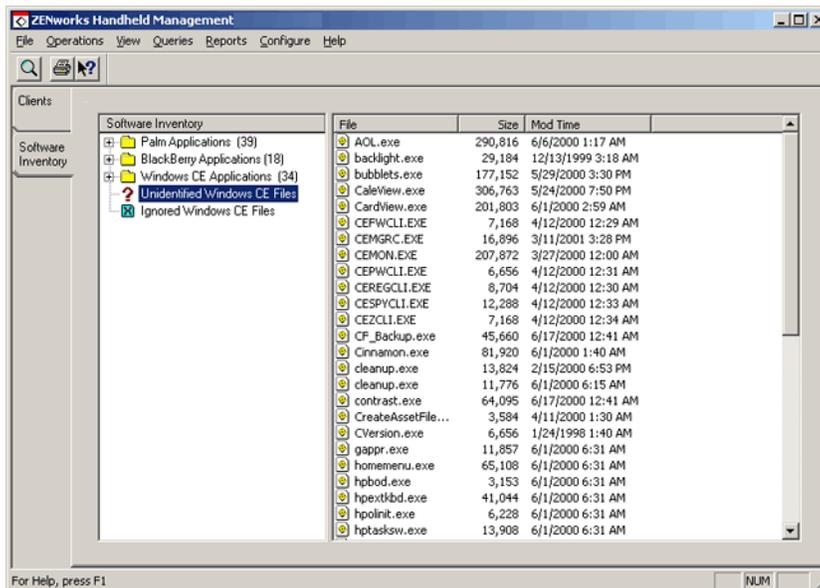
To make an unidentified file a known application:

- 1 In ConsoleOne, right-click a handheld device object, click *Actions*, then click *Inventory*.

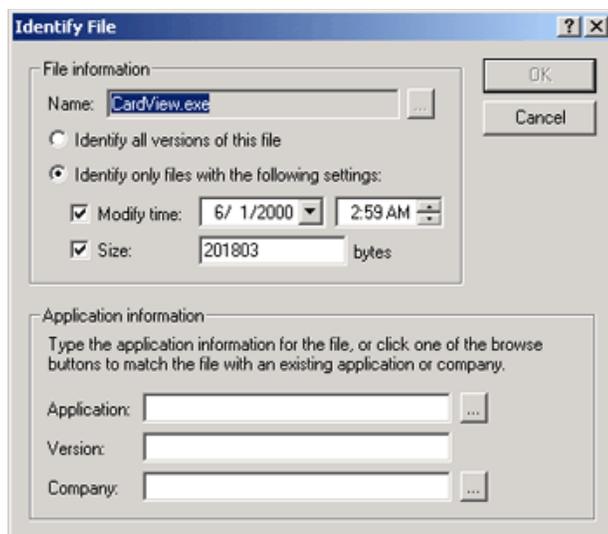


2 Click the *Software Inventory* tab, then click the *Unidentified Windows CE Files* icon (the question mark).

A list of unidentified files displays in the right pane.



3 Double-click the file you want to identify, then click *Identify File*.



- 4 Specify the name of the application you want this file to identify with, the version, and the company name.

If desired, change the modify time and size for the identification rule.

If you specify a different size and/or date, only files matching those exact specifications are identified as a known application. Versions of the file not matching the criteria still appears as unidentified.

- 5 Click *OK*.

The file now appears as an application in the Windows CE Applications folder in the tree.

## 5.1.4 Ignoring or Identifying Windows CE Files and Applications

ZENworks Handheld Management by default ignores some Windows CE application files so the application view remains manageable. Ignored files appear in the Ignored Windows CE Files folder in the Software Inventory page and in the *Ignored Files* tab in the Clients page.

The following sections contain additional information:

- ♦ [“Ignoring Windows CE Files” on page 113](#)
- ♦ [“Ignoring Windows CE Applications” on page 115](#)
- ♦ [“Identifying Ignored Windows CE Files” on page 116](#)
- ♦ [“Viewing Windows CE Identified and Ignored File Rules” on page 117](#)

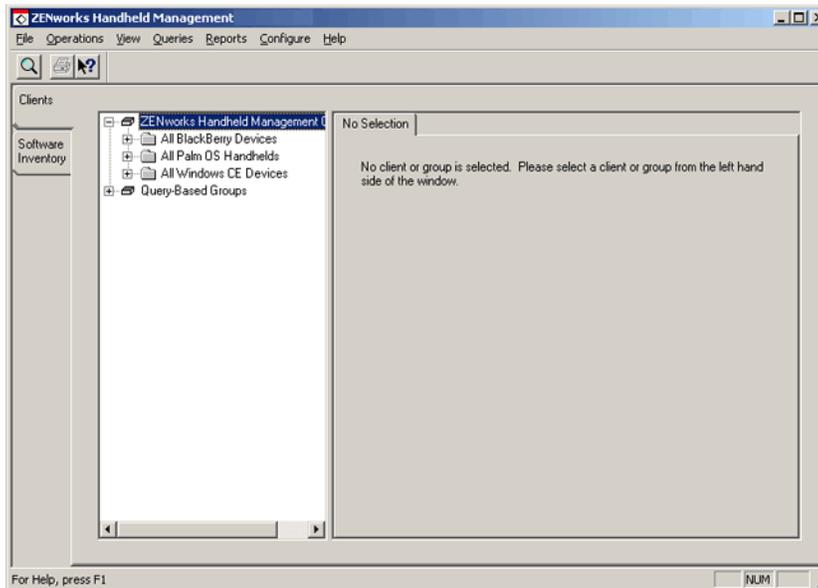
### Ignoring Windows CE Files

To keep your list of unidentified files more manageable, you can ignore unidentified files that you are not going to identify as applications.

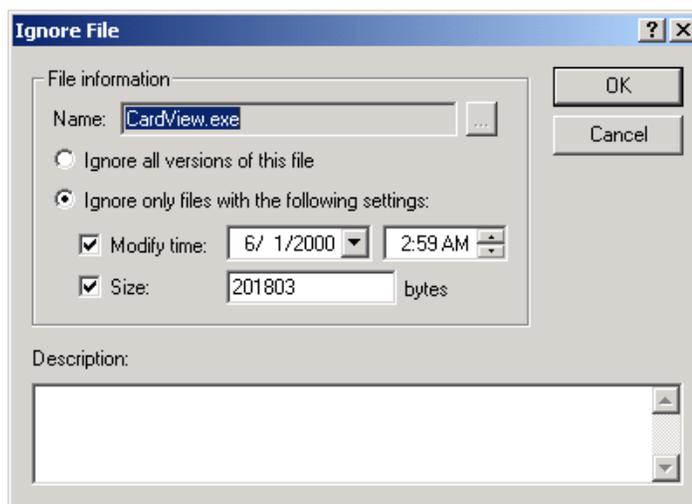
Ignoring these files keeps your unidentified files list smaller, which might help you to recognize when ZENworks Handheld Management encounters new unidentified files during software inventory.

To ignore unidentified files:

- 1 In ConsoleOne, right-click a handheld device object, click *Actions*, then click *Inventory*.



- 2 Click the *Software Inventory* tab, then click the *Unidentified Windows CE Files* icon (the question mark).
- 3 Double-click the file in the right pane.
- 4 Click *Ignore File*.



- 5 Select *Ignore All Versions of this File*.  
or  
Select *Ignore Only Files with the Following Settings*, then specify the modify time and size settings as appropriate.
- 6 If desired, type a description of why you are ignoring the file.
- 7 Click *OK*.

The file appears in the Ignored Windows CE Files tree view.

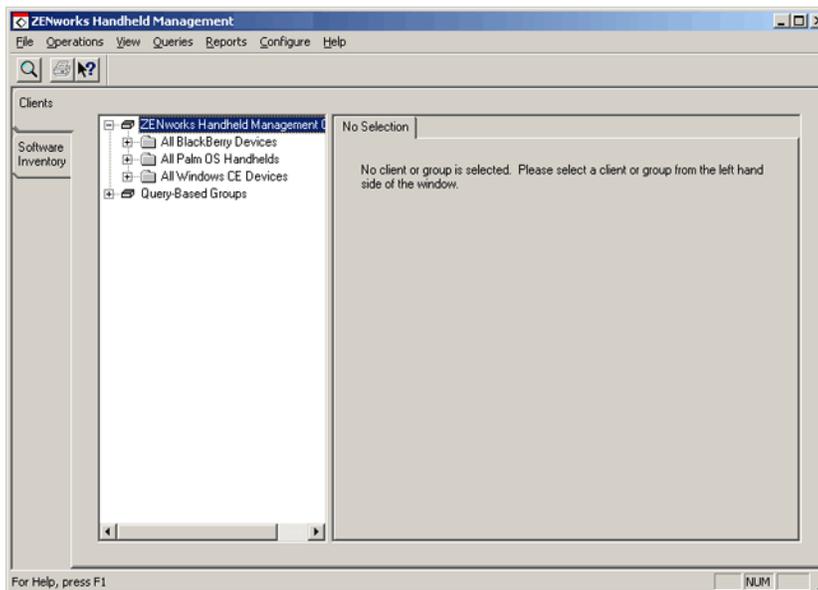
## Ignoring Windows CE Applications

To keep your Applications folder manageable, you can ignore applications. This allows you to view only the applications that you think are important to display.

For example, you might want to ignore any applications that are by default included with the operating systems (for example, Microsoft Clock).

To ignore an application:

- 1 In ConsoleOne, right-click a handheld device object, click *Actions*, then click *Inventory*.



- 2 Click the *Software Inventory* tab, then click the application you want to ignore.

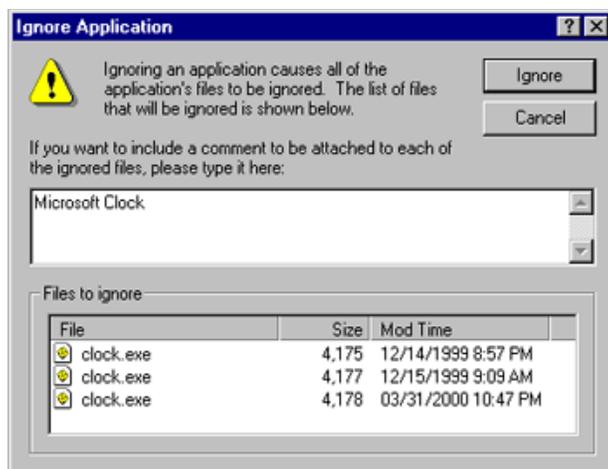
---

**NOTE:** You can ignore Windows CE applications only; you cannot ignore Palm OS and BlackBerry applications.

---

- 3 Click *Operations*, then click *Ignore Application*.

The Ignore Application dialog box lists files that are ignored.



- 4 If desired, type a description of why you are ignoring the files.

The description is stored with the file and can be viewed with the rule created for the file. For more information, see [“Viewing Windows CE Identified and Ignored File Rules” on page 117](#).

- 5 Click *Ignore*.

The application files are stored as Ignored files. Any files that future software inventory collections find that match the criteria you specified are also stored as Ignored files.

---

**NOTE:** Ignoring applications ignores files that are currently known that identify themselves with the ignored application. If new files appear that identify themselves as this application, the application reappears in the Applications view.

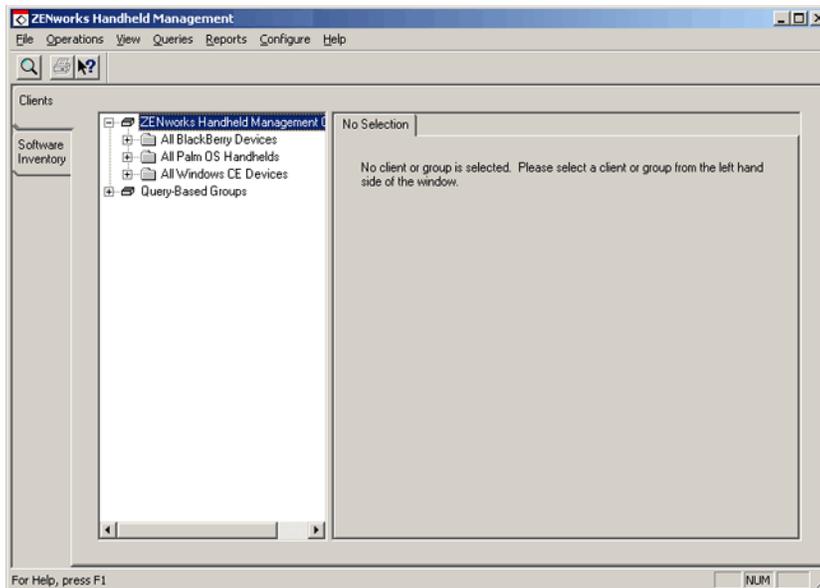
---

### Identifying Ignored Windows CE Files

You can identify ignored application files that you want to be recognized as applications.

To identify ignored files:

- 1 In ConsoleOne, right-click a handheld device object, click *Actions*, then click *Inventory*.



- 2 Click the *Software Inventory* tab, then click the *Ignored Windows CE Files* icon.
- 3 Double-click the file you want to identify, then click *Identify File*.
- 4 Specify the name of the application you want this file to identify with, the version, and the company name.
- 5 If desired, change the modify time and size for the identification rule.  
If you specify a different size and/or date, only files matching those exact specifications are identified as a known application. Versions of the file not matching the criteria still appear as unidentified.
- 6 Click *OK*.

## Viewing Windows CE Identified and Ignored File Rules

When you identify or ignore a Windows CE file or application, a rule is created for the file.

You can view all the rules you have created by clicking *Configure > Software Inventory Rules* in the ZENworks Handheld Management Inventory Viewer.

A rule applies to a file name, not to versions, so you might see rules even if you did not create the rule for a specific version of a file you are viewing. Another rule could have been created for a file that had a different time stamp or size but the same name.

When you identify or ignore all versions of a file, the size and modify time fields display Any. When you identify or ignore a specific version of a file, the size and modify time fields match the file you have created the rule for.

If you attempt to create a rule for a file that matches an existing rule, you are warned before overwriting the existing rule. The same thing happens if you try to create an ignore rule for a file that already has an identification rule.

To view all rules an administrator has created in ZENworks Handheld Management:

- 1 In ConsoleOne, right-click a handheld device object, click *Actions*, then click *Inventory*.
- 2 Click *Configure*, then click *Software Inventory Rules*.



The Software Inventory Rules dialog box lists any files you have identified or ignored.

You can change any rule by selecting the rule, then clicking *Edit*. You can also identify or ignore a file by clicking *Add*, then creating the rule. You can even create a rule for files that have not been installed on your devices yet.

To view rules for a specific file:

- 1 In ConsoleOne, right-click a handheld device object, click *Actions*, then click *Inventory*.
- 2 Double-click an unidentified or ignored file.
- 3 Click the *Rules* tab.

All user-defined ignore and identification rules that match the name of the file appear.

## 5.2 Viewing Hardware Inventory

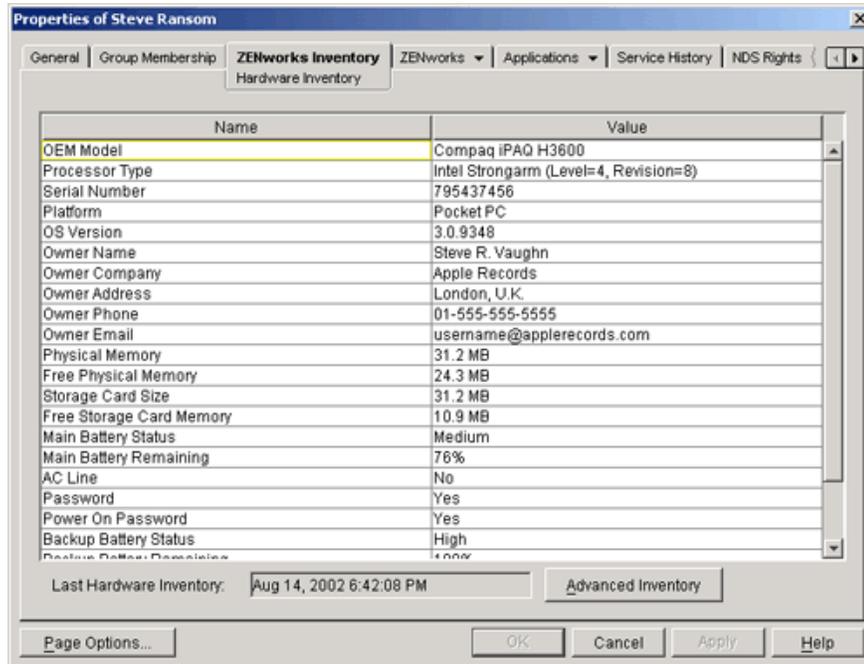
ZENworks Handheld Management collects hardware information from each handheld device in your system, including the model, OS version, processor type, free RAM, RAM used, battery type and remaining charge on the battery.

Collected data about hardware is stored on a per-device basis and is found on the ZENworks Inventory page in ConsoleOne or on the Clients: Hardware Inventory page in the Inventory Viewer.

Hardware inventory data is collected every time the handheld device connects to the ZENworks Handheld Management Access Point.

To view hardware inventory using ConsoleOne:

- 1 In ConsoleOne, right-click a handheld device object, then click *Properties*.
- 2 Click the *ZENworks Inventory: Hardware Inventory* tab.



The device's hardware inventory information is displayed.

---

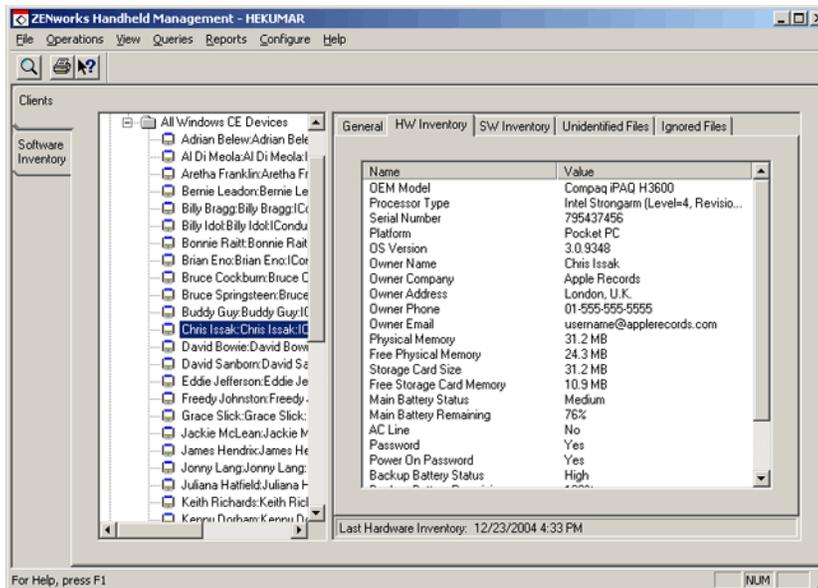
**NOTE:** For Java-based BlackBerry devices, the *Password Enabled* field value is not scanned for and the value is always displayed as *No*. The value of *Power Save Mode* is always *Off*. The serial number is same as the PIN value of the device.

---

The Last Hardware Inventory box displays the date and time that hardware inventory was last collected for the device.

To view hardware inventory using the ZENworks Handheld Management Inventory Viewer:

- 1 In ConsoleOne, right-click a handheld device object, click *Actions*, then click *Inventory*.
- 2 Click the *Clients* tab, select a handheld device object, then click the *HW Inventory* tab in the right pane.



## 5.3 Viewing Network Information

You can view a list of network adapters that were found on handheld devices in your ZENworks Handheld Management installation.

---

**NOTE:** For Pocket PCs, network information is not available for devices running Pocket PC 2000; network information is available for devices running Pocket PC 2002 and later. For handheld PCs, network information is not available for devices running Windows CE 2.11 or 3.0. For Palm OS devices, network information is not available for devices running Bluetooth\*.

---

To view network information from ConsoleOne:

- 1 In ConsoleOne, right-click a handheld device object, then click *Properties*.
- 2 Click the *ZENworks Inventory: Network Information* tab.

To view network information using the ZENworks Handheld Management Inventory Viewer:

- 1 In ConsoleOne, right-click a handheld device object, click *Actions*, then click *Inventory*.
- 2 Click the *Clients* tab, select a handheld device object, then click the *Network* tab in the right pane (this tab only displays if there is network information available the selected handheld device).

## 5.4 Using Inventory Reports

You can generate reports about the hardware and software on your handheld devices to make it easy to see the applications you have installed, which devices need upgrades, which hardware components are installed, and more.

ZENworks Handheld Management provides predefined reports for information stored in the ZENworks Handheld Management database, including:

- ◆ Handheld Application objects (status, run time, and so forth)

- ◆ Devices (groups belonged to, distributions run, hardware/software inventory)
- ◆ Groups
- ◆ Software inventory (list of all software applications and where they are installed, unidentified files, and so forth)
- ◆ Hardware inventory

After they are generated, reports can be viewed online, sent to a printer, or saved to a file in a variety of formats.

---

**TIP:** ZENworks Handheld Management is compatible with the Seagate\* Software Crystal Reports\* reporting engine. Using Crystal Reports, you can create your own custom reports. See your Crystal Reports documentation for further details.

---

The following sections contain more information about using reports:

- ◆ [Section 5.4.1, “Running Reports,” on page 121](#)
- ◆ [Section 5.4.2, “Exporting Reports,” on page 122](#)
- ◆ [Section 5.4.3, “Creating Custom Reports,” on page 122](#)

## 5.4.1 Running Reports

You generate and view ZENworks Handheld Management reports in the ZENworks Handheld Management Inventory Viewer.

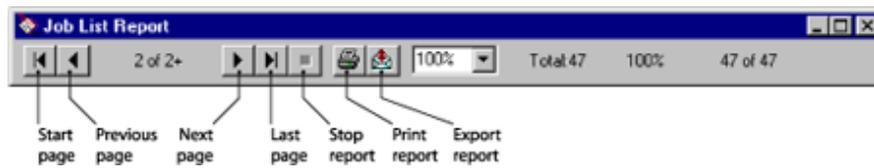
- 1 In ConsoleOne, right-click a handheld device object, click *Actions*, then click *Inventory*.
- 2 Click *Reports*, then select the type of report to generate.

After choosing a report, you might be prompted to pick a device or group before generating the data. After the report is generated, a screen similar to the following displays.

The screenshot shows a window titled "Windows CE Device Summary" with a navigation bar at the top. The report content is as follows:

ZENworks Handheld Management						
Windows CE Summary (For a Group)						
Group: All Windows CE Devices						
Device Name (User)	OS Version	RAM	Free RAM	Last Sync	Main Battery	
Adrian Belew:Adrian Belew:Conduit Nashville Server (Adrian Belew)	3.0 Build 126	31.2 MB	24.3 MB	12/23/2004	5:16PM	Medium (78%)
Al Di Meola:Al Di Meola:Conduit Nashville Server (Al Di Meola)	3.0 Build 126	31.2 MB	24.3 MB	12/23/2004	7:50PM	Medium (78%)
Aretha Franklin:Aretha Franklin:Conduit Seattle Server (Aretha Franklin)	3.0.9348	31.2 MB	24.3 MB	12/23/2004	7:40PM	Medium (76%)
Bernie Leadon:Bernie Leadon:Conduit Seattle Server (Bernie Leadon)	3.0.9348	31.2 MB	24.3 MB	12/23/2004	10:22PM	Medium (76%)
Billy Bragg: Billy Bragg:Conduit Nashville Server (Billy Bragg)	3.0 Build 126	31.2 MB	24.3 MB	12/23/2004	7:17PM	Medium (78%)
Billy Idol: Billy Idol:Conduit Nashville Server (Billy Idol)	3.0 Build 126	31.2 MB	24.3 MB	12/23/2004	9:06PM	Medium (78%)
Bonnie Raitt:Bonnie Raitt:Conduit Nashville Server (Bonnie Raitt)	3.0 Build 126	31.2 MB	24.3 MB	12/23/2004	8:35PM	Medium (78%)

After the report is generated, you can scroll through the report, print it, or export it to many different formats including Excel, HTML, RTF, and so forth. The following illustration shows the toolbar buttons you can use to view and print the report.



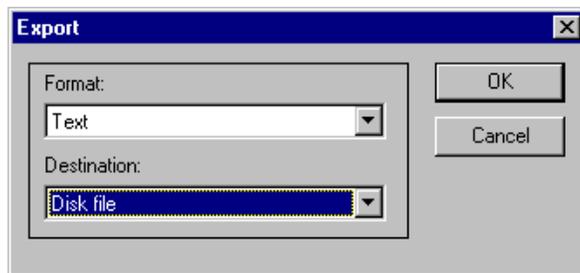
## 5.4.2 Exporting Reports

After you generate a report you can export the report to a file or import the data into a database or spreadsheet.

Reports can be exported to formats such as HTML, tab/comma-delimited text files, Microsoft Excel, and so forth. After choosing the export format, you can choose the destination, such as a file, a Lotus Notes\* database, or an e-mail system.

To export a report:

- 1 Click  on the toolbar.



- 2 Choose the format in which to export the report.
- 3 Select the destination for the report.
- 4 Click *OK*.

You are prompted for additional information based on the format and destination.

## 5.4.3 Creating Custom Reports

Users who have Crystal Reports can create their own custom reports from the ZENworks Handheld Management server database.

The ZENworks Handheld Management server database can be either Microsoft Access\* or MS SQL, depending on the database type you selected during the installation of the ZENworks Handheld Management server components. If you selected the *Internal ODBC-Compatible Database* option during the installation, the Handheld Management server database is the Microsoft Access database (`serverdata.mdb`) located in the Handheld Management server installation directory (by default, `c:\program files\novell\zfh`). If you selected the *Microsoft SQL Server* option, the MS SQL Handheld Management server database is located in the path specified during the installation. For more information, see "[Installing the ZENworks Handheld Management Server](#)" in the *Novell ZENworks 7 Handheld Management Installation Guide*.

---

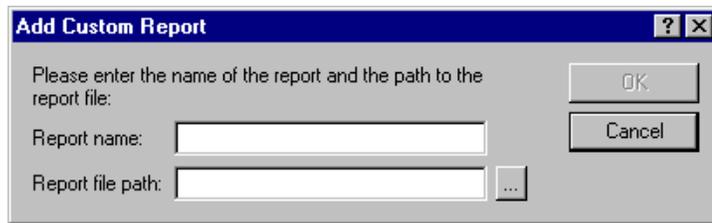
**IMPORTANT:** If you create custom reports, the reports must be stored in a shared path if you want them to be accessed by a remote ConsoleOne installation. When saving a custom report, specify a UNC path to the share (do not use local drive letters).

---

To create a custom report:

- 1 In ConsoleOne, right-click a handheld device object, click *Actions*, then click *Inventory*.
- 2 Click *Reports*, then click *Custom Report*.
- 3 Click *Add*.

The Add Custom Report dialog box is displayed.



- 4 Type a name for the report.
- 5 Specify a location for the report you created, then click *OK*.
- 6 Click *Run* to generate the report.

The report displays similar to any standard report.

## 5.5 Printing Data from the ZENworks Handheld Management Inventory Viewer

You can print data from most views in the ZENworks Handheld Management Inventory Viewer.

- 1 In ConsoleOne, right-click a handheld device object, click *Actions*, then click *Inventory*.
- 2 Click the tab from which you want to print data.
- 3 Click *File*, then click *Print*.



# Remotely Viewing or Controlling the IP-Enabled Windows CE Devices

The administrator or remote users can now perform Remote View or Remote Control operations with the IP-enabled Windows CE devices by configuring the WinCE Remote Management policy, and initiating a remote session with the devices.

**Remote View:** Lets you connect with a handheld device so you can view the device instead of controlling it. Remotely viewing a handheld device helps you troubleshoot problems that the user encountered. For example, you can observe how the user at a handheld device performs certain tasks to ensure that the user performs a task correctly.

**Remote Control:** Lets you control a handheld device from the ConsoleOne® to provide user assistance. With Remote Control connections, the administrator or remote users can go beyond viewing the handheld device to taking control of it

To perform Remote View or Remote Control operations, perform the following tasks:

- ♦ [Section 6.1, “Configuring WinCE Remote Management Policy,” on page 125](#)
- ♦ [Section 6.2, “Setting a VNC Password on the Handheld Device,” on page 125](#)
- ♦ [Section 6.3, “Initiating a Remote View or a Remote Control Session,” on page 126](#)

## 6.1 Configuring WinCE Remote Management Policy

For detailed information on how to configure the WinCE Remote Management policy, see [Section 2.4.13, “WinCE Remote Management Policy,” on page 66](#).

## 6.2 Setting a VNC Password on the Handheld Device

- 1 On the Handheld device, click *Start*, click *Programs*, click *Communication*, then click *VNC Password*.
- 2 Enter a password.

---

**IMPORTANT:** Ensure that the password is unique and it is not the eDirectory™ password.

---

- 3 Click *OK*.

## 6.3 Initiating a Remote View or a Remote Control Session

This section contains the following information:

- ♦ [Section 6.3.1, “Initiating a Remote View or a Remote Control Session from a Device Object,” on page 126](#)
- ♦ [Section 6.3.2, “Initiating a Remote View or a Remote Control Session from a User Object,” on page 127](#)

### 6.3.1 Initiating a Remote View or a Remote Control Session from a Device Object

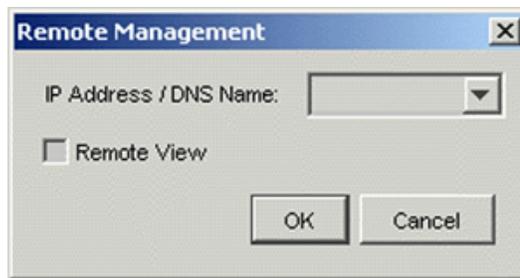
- 1 In ConsoleOne, right-click the Windows CE device object that you want to remotely view or control, click *Actions*, then click *Remote Control*.

---

**NOTE:** We recommend you to initiate a Remote View or Remote Control session in a secure network environment.

---

The Remote Management dialog box is displayed.



- 2 In the Remote Management dialog box, do the following:

- 2a Select the IP address or the DNS name of the handheld device.

---

**IMPORTANT:** Ensure that the IP address or the DNS name of the device you want to remotely control is correct.

---

- 2b (Conditional) If you only want to initiate a Remote View session, select the *Remote View* option.

- 2c Click *OK*.

- 2d If prompted, enter the VNC password of the device (which is set in [Section 6.2, “Setting a VNC Password on the Handheld Device,” on page 125](#)).

---

**NOTE:** If the password contains more than eight characters, only the first eight characters are validated.

---

## 6.3.2 Initiating a Remote View or a Remote Control Session from a User Object

You can initiate a Remote View or a Remote Control session from a user object if a user is associated to a handheld device.

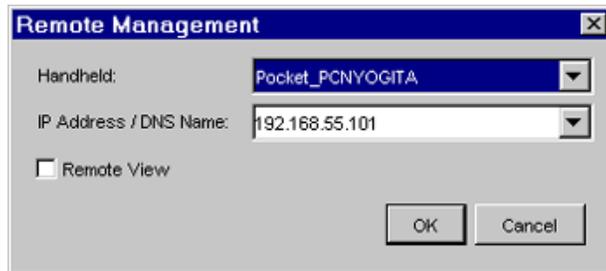
- 1 In ConsoleOne, right-click user object, click *Actions*, then click *Remote Control a Handheld*.

---

**NOTE:** We recommend you to initiate a Remote View or Remote Control session in a secure network environment.

---

The Remote Management dialog box is displayed.



- 2 In the Remote Management dialog box, do the following:
  - 2a Select the handheld device that you want to remotely view or control.
  - 2b Select the IP address or the DNS name of the handheld device.

---

**IMPORTANT:** Ensure that the IP address or the DNS name of the device you want to remotely control is correct.

---

- 2c (Conditional) If you only want to initiate a Remote View session, select the *Remote View* option.
- 2d Click *OK*.
- 2e If prompted, enter the VNC password of the device (which is set in [Section 6.2, “Setting a VNC Password on the Handheld Device,”](#) on page 125).

---

**NOTE:** If the password contains more than eight characters, only the first eight characters are validated.

---



# Making System Configuration Changes

# 7

This section discusses how to make configuration changes to your Novell® ZENworks® 7 Handheld Management system.

The following sections contain additional information:

- ♦ [Section 7.1, “Configuring User Authentication,” on page 129](#)
- ♦ [Section 7.2, “Configuring the Proxy Service,” on page 131](#)
- ♦ [Section 7.3, “Converting to Microsoft SQL Server,” on page 136](#)
- ♦ [Section 7.4, “Compacting and Repairing the Database,” on page 138](#)
- ♦ [Section 7.5, “Configuring the ZENworks Handheld Management Access Point and the Desktop Synchronization Integration,” on page 140](#)
- ♦ [Section 7.6, “Configuring the ZENworks Handheld Management IP Clients,” on page 141](#)

## 7.1 Configuring User Authentication

You can manage by both device and user (similar to ZENworks Desktop Management). If user-based management is enabled, users are prompted for their credentials and ZENworks Handheld Management authenticates the users using LDAP to log in to the directory.

During installation, you can configure user-based management of all of your handheld devices in your ZENworks Handheld Management system. For more information, see [“Installing the ZENworks Handheld Management Server”](#) in the *Novell ZENworks 7 Handheld Management Installation Guide*.

You can also configure user-based management by following the procedure in this section to edit the properties of the ZENworks Handheld Management Service object.

---

**NOTE:** If you do not want to enable user authentication for all handheld devices in your ZENworks Handheld Management system, you can choose to not enable global user authentication during installation or by following the procedure in this section. You can then configure either the [Palm Client Configuration policy](#) or the [WinCE Client Configuration policy](#) to target only specific handheld devices or groups of handheld devices.

---

If user authentication is enabled, the user is prompted for his or her credentials (username and password) the first time the device connects/synchronizes. ZENworks Handheld Management then authenticates the user using LDAP to login to the directory. After the user is authenticated, you can target policies and applications to the user of the handheld device.

The user must enter the credentials only once; ZENworks Handheld Management does not prompt the user for the credentials again. If a user who has been authenticated gives the device to another person, you should reconfigure the user on the device using ZENworks Handheld Management console on the device.

If the device uses the Palm\* IP or Windows\* IP client to connect, the user-authentication dialog box displays on the handheld device. If the device uses Palm HotSync, the user-authentication dialog box displays on the desktop computer during synchronization.

When the user is prompted for authentication, if he or she clicks *Cancel*, the handheld device can be managed by device, but user-based management does not function because the user is not authenticated. If the user mis-types the username or password, he or she is immediately prompted for the credentials again.

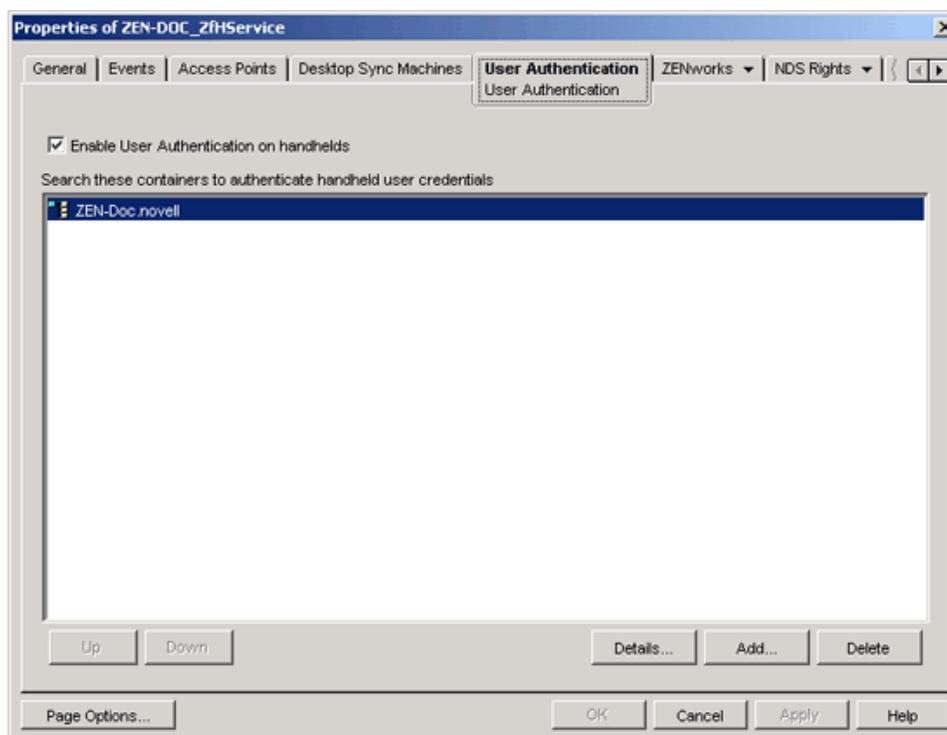
---

**NOTE:** There are two places in ZENworks Handheld Management where users can be required to enter a password: to authenticate to the directory as part of the Palm Client Configuration policy and to power on a handheld device as part of the Palm Security policy. These two passwords are independent of each other. For more information about the password users must enter to power on a device, see [“Palm Security Policy” on page 48](#).

---

To configure user authentication for all handheld devices in your system after installation:

- 1 In Novell ConsoleOne<sup>®</sup>, right-click the ZENworks Handheld Management Service object, then click *Properties*.
- 2 Click the *User Authentication* tab.



- 3 Select the *Enable User Authentication on Handhelds* check box.

Checking this option forces all managed handheld devices to prompt users for user credentials when the handheld device connects/synchronizes. After user credentials are entered, the ZENworks Handheld Management Access Point (on the ZENworks Handheld Management Server or on another machine) authenticates the user with the directory.

- 4 Click *Add* to open the Select Objects dialog box.

- 5 Specify the containers that the ZENworks Handheld Management Access Point should search when authenticating users, then click *OK*.  
Be aware that subcontainers are not searched. You must specify each user container or subcontainer individually.
- 6 Click the *General* tab, then click *Scan Now* to immediately force a scan so that the changes you made to the Service object are sent to the ZENworks Handheld Management Server.
- 7 Click *OK*.

## 7.2 Configuring the Proxy Service

The proxy service is installed along with the ZENworks Handheld Management Access Point Software and the Desktop Synchronization Software. The proxy service manages application delivery, monitors application distributions sent by the ZENworks Handheld Management server, and sends the results of those distributions back to the server. The proxy service also queues the policies and ensures that they are delivered to handheld devices.

The proxy service starts and runs in the background each time the computer is started. On Windows 2000/XP machines, the proxy service runs as a service.

You can use the Proxy Console utility to configure the communication mechanism that the proxy uses to talk to the Zenworks Handheld Management Server. The proxy service has configuration settings for which ZENworks Handheld Management server it should communicate with and options for dial-up networking and message transfers.

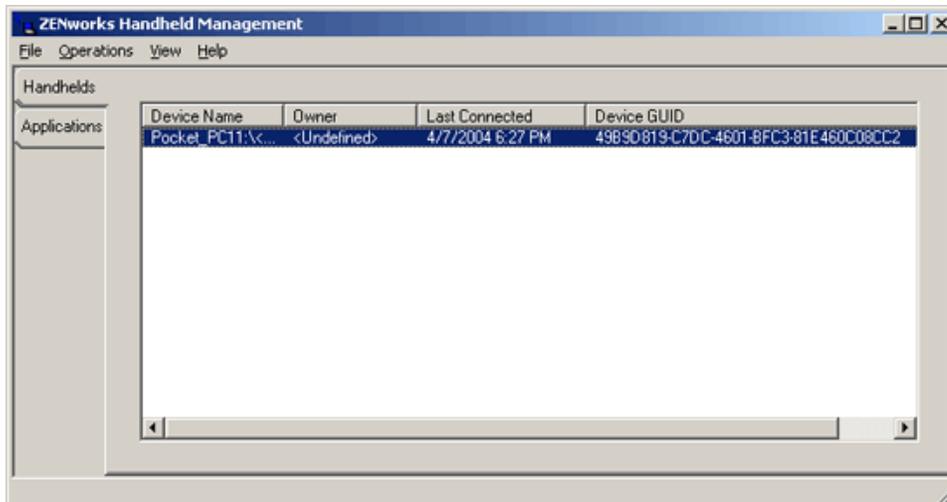
To make configuration changes to a proxy service on a Windows 2000 machine, the user must be at least a Power User on the machine.

The following sections contain additional information:

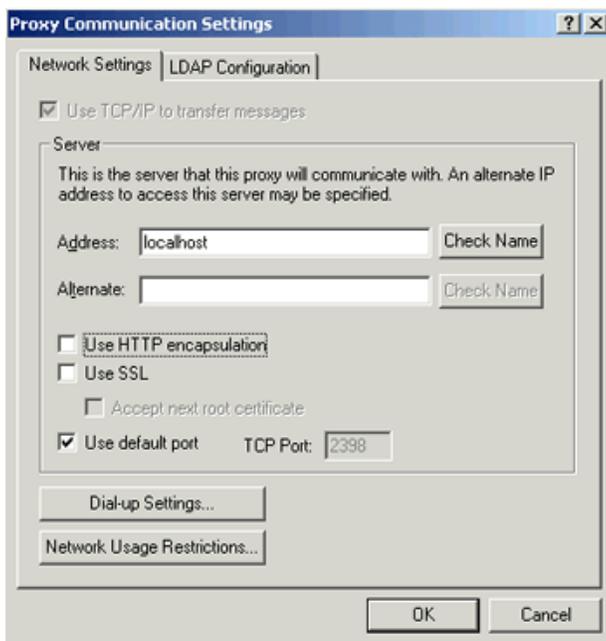
- ♦ [Section 7.2.1, “Configuring Network Settings,” on page 131](#)
- ♦ [Section 7.2.2, “Configuring Network Usage Restrictions,” on page 132](#)
- ♦ [Section 7.2.3, “Configuring Dial-Up Communications,” on page 134](#)
- ♦ [Section 7.2.4, “Enabling or Disabling Message Transfers,” on page 135](#)
- ♦ [Section 7.2.7, “Connecting to the ZENworks Handheld Management Server,” on page 136](#)

### 7.2.1 Configuring Network Settings

- 1 Run `console.exe` from the `zfhap` directory (by default, `program files\novell\zfhap`).



2 Click *Operations > Configure > Server Communications*.



Alternate addresses can be defined for the server when the server is on a network that defines one set of IP addresses for internal traffic and another set of IP addresses for traffic from outside of the firewall, for instance when you are using Network Address Translation (NAT).

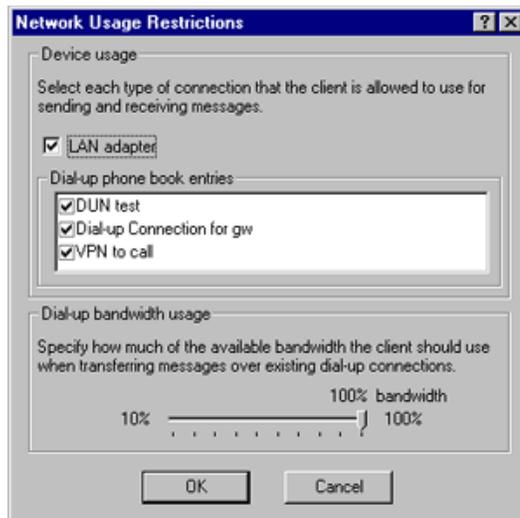
To configure HTTP/SSL settings, see [Appendix B, "Configuring SSL and HTTP Settings,"](#) on page 153.

## 7.2.2 Configuring Network Usage Restrictions

Network usage restrictions allow you to pick how TCP/IP connections are made by the proxy service and to set bandwidth limitations. In most situations, the default settings should be sufficient.

To configure network usage restrictions:

- 1 Run `console.exe` from the `zfhap` directory (by default, `program files\novell\zfhap`).
- 2 Click *Operations > Configure Communications*.
- 3 Click *Network Usage Restrictions* in the Network Settings page.



- 4 Specify the settings in the fields:

**LAN Adapter:** The proxy service tries to make a TCP/IP connection to the ZENworks Handheld Management server using the installed LAN adapter (this is how a normal connection would be made by a proxy service directly connected to the LAN).

Because the proxy service periodically tries to connect to the server, this option should be disabled if there is no way to connect to the ZENworks Handheld Management server via the LAN. For example, if the user is in a remote office that never directly connects to the LAN but has a LAN adapter installed.

**Dial-Up Phone Book Entries:** Lists the current dial-up networking connections that have been configured on the proxy service.

You might want to disable a dial-up connection in order to limit the bandwidth used by a specific connection. For example, you might not want ZENworks Handheld Management to use a dial-up connection that is used strictly for a cellular modem.

**Dial-Up Bandwidth Usage:** Allows you to set how much bandwidth ZENworks Handheld Management can use when transferring messages over dial-up connections. By default, proxy services uses the maximum bandwidth available.

On occasion, the user might want to limit the bandwidth ZENworks Handheld Management uses, especially if other processes are using the dial-up connection at the same time ZENworks Handheld Management is transferring messages.

For example, if users are downloading large files from the network, they might want to limit the amount of bandwidth ZENworks Handheld Management is using so that the file download finishes faster. If necessary, you can also disable message transfers to keep ZENworks Handheld Management from sending messages. For more information, see [“Enabling or Disabling Message Transfers” on page 135](#).

## 7.2.3 Configuring Dial-Up Communications

You can configure the proxy service to automatically attempt to connect to the server using a dial-up connection.

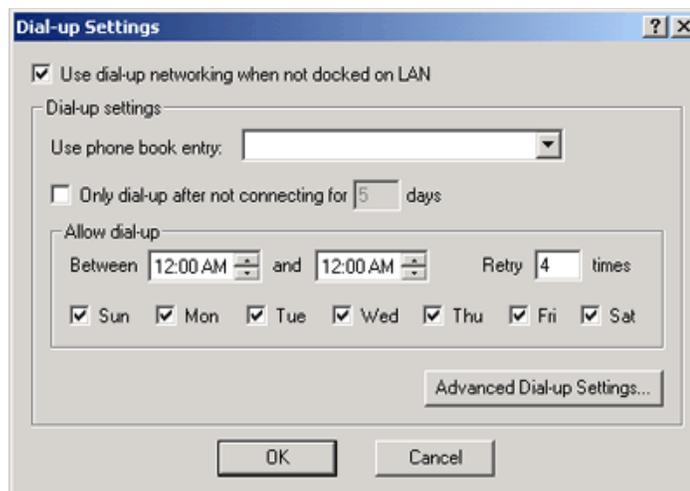
When dial-up networking is configured, the proxy service automatically attempts to dial up the ZENworks Handheld Management server to exchange messages. You can configure the frequency of dial-ups and how long to wait for the next dial-up after the client has connected.

Before setting up the proxy service to use dial-up networking, the proxy service must have a valid phone book entry in the Dial-Up Networking folder on the client. This entry should connect you to a server that gives you access to the server.

To configure the proxy service to use dial-up networking:

- 1 Run `console.exe` from the `zfhap` directory (by default, `program files\novell\zfhap`).
- 2 Click *Operations > Configure > Server Communications*.
- 3 Click *Dial-Up Settings*.

The Dial-Up Settings page is displayed.



- 4 Select the *Use Dial-Up Networking When Not Docked on LAN* check box.
- 5 Select a phone book entry from the drop-down list.
- 6 To configure how frequently the proxy service attempts to dial up the server, select *Only Dial Up After Not Connecting for \_ Days*, then specify the number of days.
- 7 To configure when the proxy service should attempt to dial up the server, configure the schedule in the *Allow Dial-Up* group box.
- 8 To configure details of the dial-up, such as logon information, select *Advanced Dial-Up Settings*, make any configuration settings, then click *OK*.
- 9 Click *OK*.

## 7.2.4 Enabling or Disabling Message Transfers

Message transfers enable the proxy service to send messages to the ZENworks Handheld Management server. Normally, you should always leave message transfers enabled.

To enable or disable message transfers:

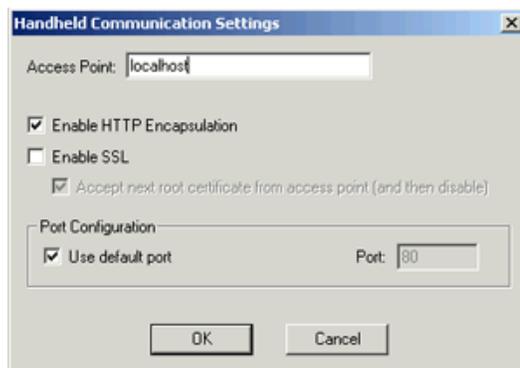
- 1 Run `console.exe` from the `zfhap` directory (by default, `program files\novell\zfhap`).
- 2 To enable transfers, click *Operations*, then click *Enable Message Transfers*.  
or  
To disable transfers, click *Operations*, then click *Disable Message Transfers*.

By default, message transfer is enabled and new messages are automatically placed in the proxy service's message queue or out box.

## 7.2.5 Configuring Handheld Communications

You can configure the settings used by the IP client on the handheld to communicate with the ZENworks Handheld Management Access Point.

- 1 Start `console.exe` from the `zfhap` directory.



- 2 Click *Options > Configure > Handheld Communications*.
- 3 In the Handheld Communication Settings dialog box, configure the following options:
  - ♦ If you want the handheld to use HHTTP, select the *Enable HTTP Encapsulation* check box.
  - ♦ If you want the handheld to use SSL, select the *Enable SSL* check box.
  - ♦ If you want the handheld to communicate with SSL over HTTP, select both the *Enable HTTP Encapsulation* and the *Enable SSL* check boxes.
  - ♦ If you want the handheld to connect to a port other than the default, deselect the *Use Default Port* check box and specify the port the handheld should use to connect to the ZENworks Handheld Management Access Point.

## 7.2.6 Configuring IP Communication for the ZENworks Handheld Management Access Point

To configure the Access Point communication, click *Options > Configure > Access Point Communications*. Alternatively, you can configure Access Point communication by launching `cfgip.exe` from the `zfhap` directory. For more information, see [Section B.1, “Configuring the SSL and HTTP Communication between the ZENworks Handheld Management Server and the ZENworks Handheld Management Access Point,”](#) on page 154.

## 7.2.7 Connecting to the ZENworks Handheld Management Server

You can ensure that the proxy service can locate the ZENworks Handheld Management server and exchange messages by using the *Connect to Server* option in the *Operations* menu of the proxy service console.

When you use this option, the proxy service attempts to connect to its assigned server, and, if the server is found, it forwards any pending messages to the server.

To force a connection to the ZENworks Handheld Management server:

- 1 Run `console.exe` from the `zfhap` directory (by default, `program files\novell\zfhap`).
- 2 Click *Operations*, then click *Connect to Server*.

---

**TIP:** If the *Connect to Server* option is not available, the proxy server will not be running.

---

If the server cannot be found, ensure that the ZENworks Handheld Management server service is running on the ZENworks Handheld Management server machine and that you are properly connected to the network.

## 7.3 Converting to Microsoft SQL Server

If you configured the ZENworks Handheld Management Server to use the internal ODBC-compatible database, you can upgrade to a Microsoft\* SQL Server database if you have Microsoft SQL Server installed.

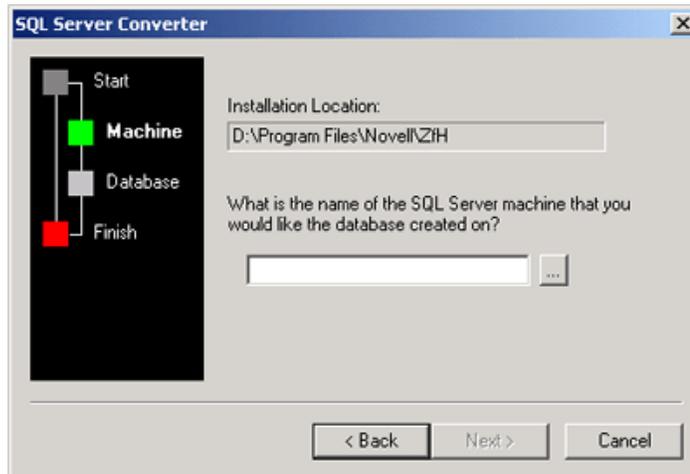
To convert the internal ODBC-compatible database to Microsoft SQL Server:

- ♦ The ZENworks Handheld Management Server machine must be able to access the Microsoft SQL Server machine on the network.
- ♦ The person logged in when running the SQL conversion tool must have a server role of System Administrator to convert the database.

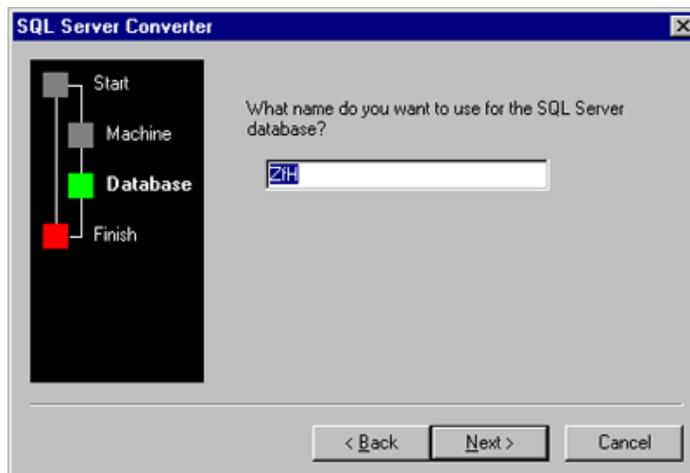
After the database is successfully upgraded, the System Administrator permission can be removed. The ZENworks Handheld Management Server user and the user running the ZENworks Handheld Management console just need database access of `db_datareader` and `db_datawriter`.

To convert the database to Microsoft SQL Server:

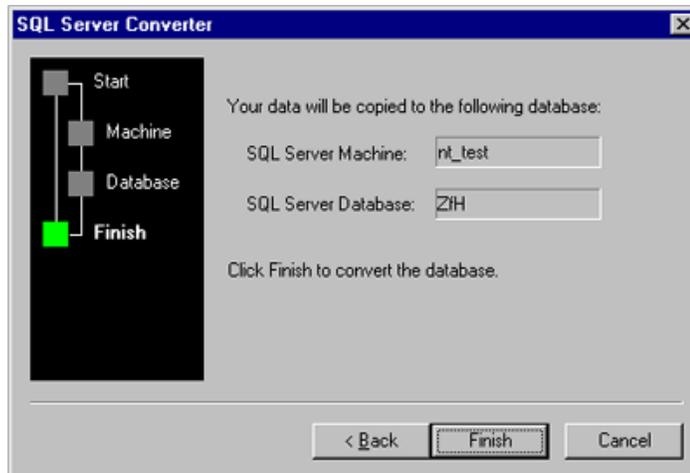
- 1 Use either Windows Explorer or the command prompt on the ZENworks Handheld Management installation machine to access the ZENworks Handheld Management Server installation directory.
- 2 From the installation directory, run `sqlconv.exe` (by default, in `program files\novell\zfh`) to open the SQL Server Converter wizard.
- 3 Click *Next*.



- 4 Type the name of the machine where Microsoft SQL Server is installed, then click *Next*.



- 5 Type the name you want to assign to the ZENworks Handheld Management database when it is created in SQL, then click *Next*.



This page shows the name of the SQL Server machine and the name you are assigning to the database.

- 6 Click *Finish* to convert your current ZENworks Handheld Management database to an SQL Server database.

The time it takes for the database conversion depends on the size of the database and number of records to process.

## 7.4 Compacting and Repairing the Database

As the number of distributions you run increases, the size of the databases at the server and on the proxy service computers grows.

ZENworks Handheld Management provides separate tools to reduce the size of the server and proxy service databases.

The ZENworks Handheld Management tools to compact and repair the server database are for the internal ODBC-compatible databases only. If you have configured ZENworks Handheld Management to use Microsoft SQL Server, use the utilities provided with Microsoft SQL Server to perform database maintenance.

The following sections contain additional information:

- ♦ [Section 7.4.1, “Compacting the Server Database,” on page 138](#)
- ♦ [Section 7.4.2, “Compacting the Proxy Service Database,” on page 139](#)
- ♦ [Section 7.4.3, “Compacting and Repairing the Database,” on page 139](#)

### 7.4.1 Compacting the Server Database

Before performing database operations, you should back up the ZENworks Handheld Management installation directory (specifically `serverdata.mdb`).

Before compacting a server database, make sure to shut down all ZENworks Handheld Management applications, including ConsoleOne.

Make sure that no other computer is accessing the database (for example, a remote copy of ConsoleOne).

If another computer has the database locked, you receive an error message if you try the operation. Shut down the ConsoleOne on that computer and retry the operation.

To compact the server database:

- 1 Use either Windows Explorer or the command prompt on the ZENworks Handheld Management installation machine to access the ZENworks Handheld Management Server installation directory.
- 2 From the installation directory, run `dbtool.exe`.
- 3 If you are sure no other process is accessing the database (for example, a remote installation of ConsoleOne), click *OK*.

The database is compacted and the service is restarted.

## 7.4.2 Compacting the Proxy Service Database

The proxy service database can be compacted by using `dbtool.exe` from the command line in the client installation directory (`program files\novell\zfhap`).

To compact a proxy service database:

- 1 Use the command prompt on the ZENworks Handheld Management proxy service machine to access the ZENworks Handheld Management client installation directory.
- 2 From the installation directory, run `dbtool.exe/proxy /compact`.  
You are reminded that the ZENworks Handheld Management client is stopped and restarted after the database is compacted.
- 3 Click *OK*.

## 7.4.3 Compacting and Repairing the Database

If the server internal ODBC-compatible database or proxy service database cannot be opened when ZENworks Handheld Management or the proxy service starts, you might need to compact and repair the database.

If the database is corrupt, you might see a message in the log file that indicates that the database could not be opened. To compact and repair the database, you need to use the `dbtool` command with the `/compact` option. Other `dbtool` options are described below.

**Table 7-1** *DBtool options*

Option	Function
<code>/compact</code>	Compact and repair a database
<code>/proxy</code>	Perform on a proxy service database
<code>/server</code>	Perform on a server database

For example, to repair a proxy service database, enter `dbtool /proxy /compact`.

`Dbtool.exe` is installed in the `zfh` and `zfhap` installation directories.

## 7.5 Configuring the ZENworks Handheld Management Access Point and the Desktop Synchronization Integration

The IP conduit is used by ZENworks Handheld Management IP service clients to transfer messages. It is installed when the ZENworks Handheld Management Server or ZENworks Handheld Management Access Point is installed. For more information, see “[Installing the ZENworks Handheld Management Access Point on Additional Computers](#)” in “[Installing ZENworks Handheld Management Server Components](#)” in the *Novell ZENworks 7 Handheld Management Installation Guide*.

You can configure how much bandwidth ZENworks Handheld Management should allow when the handheld IP client connects to the IP conduit and how often clients should try to connect to the IP conduit after failing to connect.

These settings are found in the registry on the IP conduit machine (the sync machine).

The following sections contain additional information:

- ♦ [Section 7.5.1, “Configuring Bandwidth Usage,” on page 140](#)
- ♦ [Section 7.5.2, “Configuring Client Retries and Power Down \(or Suspend\),” on page 140](#)

### 7.5.1 Configuring Bandwidth Usage

If you have a very limited bandwidth (for example, a wireless network where multiple applications use the TCP/IP connection), you can limit how much bandwidth the ZENworks Handheld Management handheld IP client should use.

On the IP conduit machine (the sync machine where the Desktop Synchronization Integration is installed), the throttle setting is found in the value name Throttle in the following registry entry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\ZENworks for Handhelds  
Proxy\Current Version\IP Conduit\Throttle
```

By default, ZENworks Handheld Management is configured to use 100 percent of available bandwidth, which is a setting of 100 (decimal) in the Throttle value. If you set it to 50, ZENworks Handheld Management uses just 50 percent of available bandwidth.

If you change this setting, you should test how it works in your environment. Lowering the throttle value causes ZENworks Handheld Management messages (that is, applications) to take longer to download to the handheld device.

### 7.5.2 Configuring Client Retries and Power Down (or Suspend)

Windows CE devices power down or suspend by default after a predefined number of minutes of inactivity. This counter is reset if there is any activity on the device (for example, a synchronization, using the keyboard, and so forth).

Because the IP client periodically attempts to connect to the IP conduit after a failed connection, the counter is reset whenever the IP client attempts to connect to the server. To prevent this, the IP client uses a default retry connection interval of 60 seconds plus whatever the battery power off setting is (by default, 3 minutes).

Without this default, the device might never power down or go into suspend mode.

On the other hand, if your users only connect for short periods of time, the interval might be set too high for the client to connect to the IP conduit and therefore your users might not connect to the IP conduit frequently enough.

If your users connect for short periods of time and you are concerned that they might not be getting their ZENworks Handheld Management messages because the minimum connection interval is set too high, you can change the Minimum Connect Retry value in the registry.

This value is found in the registry on the IP conduit machine in:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Novell\ZENworks for Handhelds  
Proxy\Current Version\IP Conduit\Minimum Connect Retry
```

The setting at the server applies to all handheld devices.

By default, the registry value is 0. This default behavior means that the IP client on the handheld device waits 60 seconds plus the battery power auto shutoff setting on the handheld device (by default, 3 minutes) to connect to the IP conduit.

The values are in seconds. If you set the value to 25, ZENworks Handheld Management waits 25 seconds between retry attempts.

## 7.6 Configuring the ZENworks Handheld Management IP Clients

The ZENworks Handheld Management IP clients connect directly to the IP conduit on the ZENworks Handheld Management Server or ZENworks Handheld Management Access Point computer, allowing management of Palm OS and Windows CE devices without requiring any third-party synchronization software. For more information, see “[Installing the Handheld Clients](#)” in “[Installing ZENworks Handheld Management](#)” in the *Novell ZENworks 7 Handheld Management Installation Guide*.

The following sections contain additional information:

- ♦ [Section 7.6.1, “Configuring the ZENworks Handheld Management Palm OS IP Client,”](#) on page 141
- ♦ [Section 7.6.2, “Configuring the ZENworks Handheld Management Windows CE IP Client,”](#) on page 143

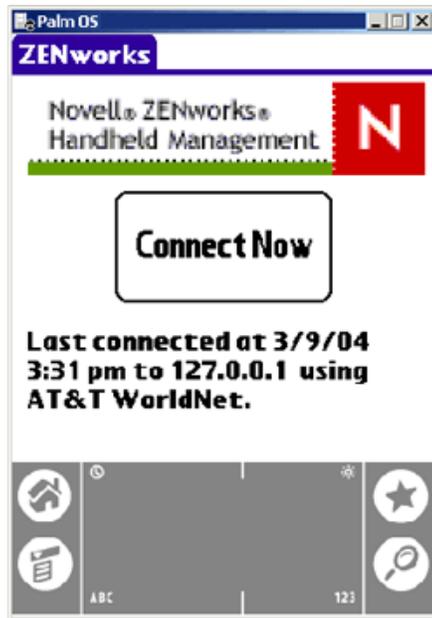
### 7.6.1 Configuring the ZENworks Handheld Management Palm OS IP Client

The ZENworks Handheld Management Palm OS IP client has a console (the ZENworks Handheld Management console) that allows you to do the following:

- ♦ Configure the address of the IP conduit and port number to use
- ♦ Stop and start the proxy service
- ♦ View the log
- ♦ Force a connection to the IP conduit

To start the ZENworks Handheld Management Palm OS IP client console:

- 1 Click the *ZENworks Handheld Management* console from the Palm OS device's Application Launcher screen.
- 2 Click *Connect Now*.



or

Click *ZENworks Handheld Management* console at the top of the screen to open the drop-down list, then click an option.



The following table describes the available options:

**Table 7-2** ZENworks Handheld Management Palm OS IP Client Console Options

Click	To
Configure	Configure the handheld server address or port number
View Log	View the client log file and enable diagnostic logging
About	View the Palm IP client version number and copyright information.

## 7.6.2 Configuring the ZENworks Handheld Management Windows CE IP Client

The ZENworks Handheld Management Windows CE IP client has a console (`console.exe`) that allows you to do the following:

- ◆ Configure the address of the IP conduit and port number to use
- ◆ Stop and start the proxy service
- ◆ View the log
- ◆ Force a connection to the IP conduit

To start the ZENworks Handheld Management Windows CE IP client console:

- 1 Click `console.exe` on the Windows CE device.

Depending on the type of Windows CE device you have, the console looks similar to the figure below:



The following table describes the available options:

**Table 7-3** *ZENworks Handheld Management Windows CE Client Console Options*

<b>Click</b>	<b>To</b>
Configure	Configure the handheld server address or port number
Log	View the client log file and enable diagnostic logging
Connect Now	Force a connection to the IP conduit
Stop/Start Client	Stop/start the client

# Troubleshooting

# A

The following sections contain troubleshooting tips and frequently asked questions about Novell® ZENworks® 7 Handheld Management:

- ♦ [Section A.1, “Error Logs,” on page 145](#)
- ♦ [Section A.2, “ConsoleOne Status Pages,” on page 145](#)
- ♦ [Section A.3, “Error Messages,” on page 146](#)
- ♦ [Section A.4, “Troubleshooting Strategies,” on page 147](#)
- ♦ [Section A.5, “Contacting Technical Support,” on page 152](#)

## A.1 Error Logs

If you are experiencing a problem, examine the following error logs for insight into errors, warnings, or informational messages recorded by ZENworks Handheld Management:

**Table A-1** ZENworks Handheld Management Error Logs

Log	Description
Windows 2000/XP Event Viewer	Check the Windows NT*/2000 Event Viewer log for errors, warnings, and alerts logged by the ZENworks Handheld Management Server service.
Server Error Log ( <code>statuslog.txt</code> )	Check the log file in the ZENworks Handheld Management Server installation directory for errors or informational messages logged by ZENworks Handheld Management.
Client Error Log	Check the log file in the ZENworks Handheld Management Access Point installation directory for errors or informational messages logged by the proxy service.

## A.2 ConsoleOne Status Pages

If you are experiencing problems with policies not being enforced, query-based groups not being updated, or handheld applications not being distributed, you can view status pages in Novell ConsoleOne® to help you troubleshoot these problems.

ZENworks Handheld Management lets you view the following types of status information:

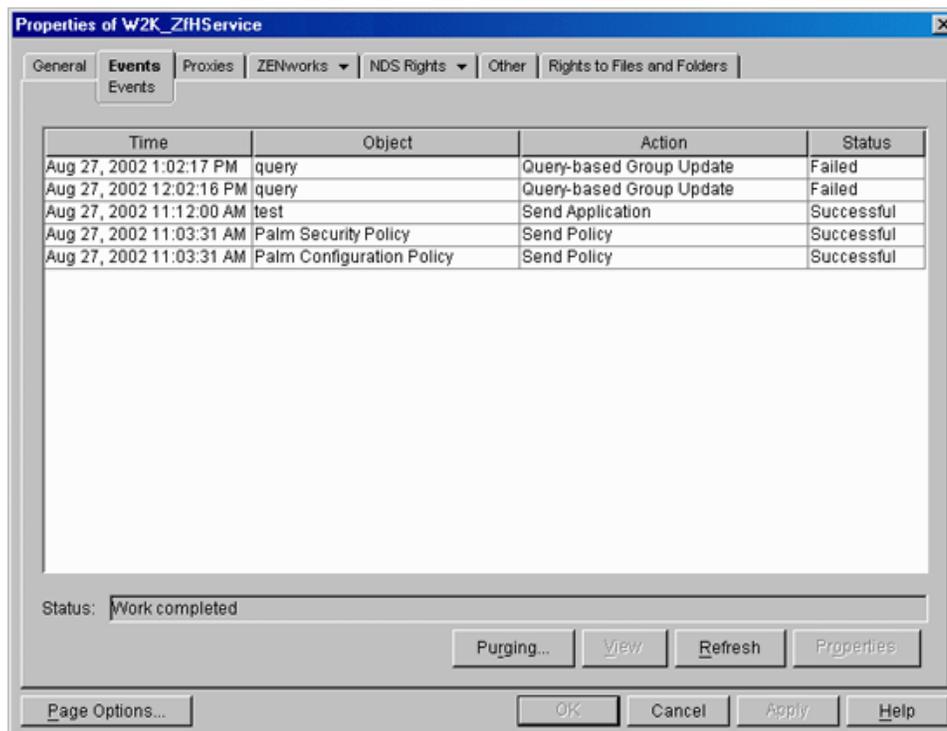
**Policy Status:** You can view policy status information for each enabled policy, including a list of all handheld devices that a policy is associated with, the status of each policy, and the date and time that the policy was last enforced. You can also view status information about all policies associated with a specific handheld device. For more information, see [Section 2.6, “Viewing Policy Status Information,” on page 76](#).

**Handheld Group Status:** You can view the status of handheld groups, including a list of all handheld devices that are members of a specific group, a list of policy packages that are associated with a particular Handheld Group object, and a list of Handheld Application objects that are associated to a particular Handheld Group object. For more information, see [Section 3.2.2, “Viewing the Properties of a Group,”](#) on page 89.

**Handheld Application Status:** You can view a list of all the Handheld Application objects distributed by the selected ZENworks Handheld Management Service object, the status of each object, and the version number of each Handheld Application object. For more information, see [Section 4.3, “Displaying Handheld Application Object Status,”](#) on page 104.

**ZENworks Handheld Management Service Object Events:** You can view event information about policy packages, updates to query-based groups, or Handheld Application objects that the ZENworks Handheld Management server has sent (or, in the case of unsuccessful distributions, tried to send) to associated handheld devices.

- 1 In ConsoleOne, right-click the ZENworks Handheld Management service object, then click *Properties*.
- 2 Click the *Events* tab.



## A.3 Error Messages

- ♦ “Failed to connect to server” on page 147
- ♦ “Shortcut is not created on the device. Policy status shows error as “The device has already maximum number of shortcuts” on page 147
- ♦ “Unable to configure button <Button X>. The button was not found” on page 147

### Failed to connect to server

Possible Cause: The Remote Management policy has not been configured for the Windows CE device you want to remotely control or remotely view.

Action: Configure the Remote Management policy. For detail information on how to configure the policy, see [Section 6.1, “Configuring WinCE Remote Management Policy,” on page 125](#).

Possible Cause: The Windows CE device you want remotely control or remotely view does not have a network IP address.

Action: Ensure that the Windows CE device you want remotely control or remotely view has a network IP address.

### Shortcut is not created on the device. Policy status shows error as “The device has already maximum number of shortcuts

Possible Cause: Some PPC devices limit shortcut creation to the seven files in the Start menu.

Action: Click *Start > Settings > Menu*. Deselect some of the selected shortcuts and enforce the policy.

### Unable to configure button <Button X>. The button was not found

Possible Cause: The button name configured in the policy is not same as the button name that appears on the device. For example, on some devices the button names contain spaces, such as Button 1 and Button 2. However, on other devices button names appear without space, such as Button 1 and Button 2.

Action: While configuring the policy, make sure the button name in the policy is identical to the button name on the device. The button names on the device are found under Settings on the Button Configuration page.

## A.4 Troubleshooting Strategies

The following sections provide suggestions and troubleshooting tips to problems you might encounter when using ZENworks 7 Handheld Management:

- ♦ [“Why doesn’t my handheld device display in ConsoleOne or in the ZENworks Handheld Management Inventory Viewer?” on page 148](#)
- ♦ [“Why are policies that I have configured and enabled not being enforced on individual handheld devices?” on page 148](#)
- ♦ [“Why are handheld applications not being installed on individual handheld devices?” on page 149](#)
- ♦ [“Why don’t I see ZENworks Handheld Management inventory information for my registered handheld devices?” on page 150](#)
- ♦ [“How does ZENworks Handheld Management manage handheld devices that synchronize at multiple computers?” on page 150](#)
- ♦ [“My backup program reports that the ZENworks Handheld Management database files cannot be backed up because they are open. Is there a way to shut them down for the backup?” on page 150](#)
- ♦ [“The ZENworks Handheld Management Client is not Pushed to the Palm Device” on page 151](#)

- ◆ “Unable to Remotely Control or Remotely View a Windows CE Device” on page 151
- ◆ “Even though the WinCE Configuration Access Point Policy, WinCE Remote Management Policy, or WinCE Configuration Policy for Uninstalling Applications is not Enforced on the Windows CE Device, the Policy Status is Reported as Enforced” on page 152
- ◆ “How to Change the User Account in Novell eDirectory After Installing ZENworks 7 Handheld Management Server?” on page 152
- ◆ “A Handheld device’s software inventory information in ConsoleOne is not updated.” on page 152
- ◆ “Even though the device is connected all the time, the last connected time in ConsoleOne is not updated.” on page 152

### Why doesn't my handheld device display in ConsoleOne or in the ZENworks Handheld Management Inventory Viewer?

**Action:** Before handheld device objects are displayed in ConsoleOne, you need to set up the Handheld Import policy. For more information, see [Chapter 1, “Setting Up Handheld Import,”](#) on page 11.

**Possible Cause:** You did not associate the Handheld Import policy correctly.

**Action:** The Handheld Import policy you configured and enabled is not in effect until you associate its policy package with a ZENworks Handheld Management service object or a container object that contains the ZENworks Handheld Management service objects. For more information, see [Section 1.3, “Associating the Handheld Service Package,”](#) on page 16.

**Possible Cause:** You enabled and associated the Handheld Import policy after the handheld devices connected to the ZENworks Handheld Management Access Point.

**Action:** Resynchronize or connect the devices to import them into ZENworks Handheld Management.

**Action:** If you are using the sync client, the handheld device needs to synchronize (possibly three times) after the ZENworks Handheld Management Desktop Synchronization Integration is installed on the computer it synchronizes with.

### Why are policies that I have configured and enabled not being enforced on individual handheld devices?

**Action:** Policies can be scheduled to run at a certain time. During creation, all policy packages are given a default run schedule (EventHandheldSync, by default). This means that all applicable policies in this package are enforced every time a handheld device connect/synchronizes.

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

You can change the default schedule for an entire policy package or for individual policies. For more information, see [“Scheduling Packages and Policies”](#) on page 74.

---

**NOTE:** Be aware that changing the policy package’s schedule or an individual policy’s schedule to run too frequently affects performance, depending on your environment. The default schedule should be adequate for most situations.

---

If you have configured and enabled policies, but they have not been enforced on individual handheld devices, consider the following:

1. When you configure and enable policies, ConsoleOne records the new information in the directory.
2. The ZENworks Handheld Management Server scans for new information hourly, by default. You must wait for up to one hour to ensure that the Handheld Management Server has received the policy changes, depending on when the last scan was performed. Or, you can force an immediate directory scan to ensure that the Handheld Management Server receives the new policy changes by right-clicking the ZENworks Handheld Management Service object, clicking *Actions*, then clicking *Scan Now*.
3. For Palm OS and Windows CE devices, the default Policy Package Schedule is EventHandheldSync (whenever the handheld device connects/synchronizes); for BlackBerry devices, the default Policy Package Schedule is once per day. If you have changed the default Policy Package Schedule, it might take longer to enforce the policy changes on the associated handheld devices. In addition, if the handheld devices were unable to connect to the ZENworks Handheld Management system (because of connectivity problems, for example), you might need to reconnect/resynchronize the devices.

Possible Cause: The ZENworks Handheld Management proxy service has not yet connected to the ZENworks Handheld Management server.

Action: You can force an immediate connection to the ZENworks Handheld Management server using the ZENworks Handheld Management Proxy Console on the proxy service machine (the Windows machine that the handheld device synchronizes with).

To force an immediate connection to the ZENworks Handheld Management server: from the ZENworks Handheld Management Access Point service installation directory  
(program files\novell\zfhap by default), run  
console.exe, click *Operations*, then click *Connect to Server*.

### **Why are handheld applications not being installed on individual handheld devices?**

Possible Cause: The Handheld Application object is not configured properly.

Action: Configure the Handheld Application object properly. For more information, see [“Configuring a Handheld Application Object” on page 98](#).

Possible Cause: The application has already been installed on the handheld device. ZENworks Handheld Management does not re-install an application that is already installed on the device.

Action: You can force an application to be installed, even if it has already been installed on the device, by using the *Resend* button on the Application Status page of the application object. You cannot force ZENworks Handheld Management to resend an application by deleting the application from the handheld device; you must use the *Resend* button.

Possible Cause: The storage device is not available for a Palm OS device. When you configure the Handheld Application object, you can specify that the files be installed on a storage card on a Palm OS device. If you selected the *Install Files on Storage Card* option in **Step 11 on page 100**, ZENworks Handheld Management installs the files only to a storage card. If the storage card is not available, the installation fails; ZENworks Handheld Management does not install the files in the Palm OS device's main memory.

### **Why don't I see ZENworks Handheld Management inventory information for my registered handheld devices?**

Action: If you are using the ZENworks Handheld Management sync client, for most synchronization packages, inventory is collected by ZENworks Handheld Management every time the device synchronizes. The ZENworks Handheld Management client on the handheld device must be run manually before synchronizing for ZENworks Handheld Management to get the latest inventory information.

If the handheld device is new to the ZENworks Handheld Management system, you might need to synchronize the device three times. The first time the device synchronizes with the proxy service computer, the handheld client is installed. The second time, the handheld device registers with the ZENworks Handheld Management server. The third time, inventory information is sent to the proxy service for forwarding to the ZENworks Handheld Management server.

### **How does ZENworks Handheld Management manage handheld devices that synchronize at multiple computers?**

Action: ZENworks Handheld Management allows handheld devices to synchronize at multiple computers. If you are using the ZENworks Handheld Management sync client and you want to be sure software is distributed and inventory collected whenever a device synchronizes, you should install the ZENworks Handheld Management Access Point on every computer where a handheld device synchronizes. For more information, see "[Installing the ZENworks Handheld Management Access Point on Additional Computers](#)" in "[Installing ZENworks Handheld Management Server Components](#)" in the *Novell ZENworks 7 Handheld Management Installation Guide*.

### **My backup program reports that the ZENworks Handheld Management database files cannot be backed up because they are open. Is there a way to shut them down for the backup?**

Action: The ZENworks Handheld Management server keeps the ZENworks Handheld Management database files open so that they can record any result information they receive. You can shut down the ZENworks Handheld Management server and messenger services before the backup and restart them after the backup.

If your backup program supports pre- and post-backup commands, you can have the backup program perform the work of stopping and starting the services. Otherwise, you need manually start and stop the services and back up the information.

Before stopping the services, close the ZENworks Handheld Management console and ensure that no remote administrators are accessing the installation.

To stop the services from the command line, enter:

```
net stop "ZENworks Handheld Management Server"
```

To restart the services from the command line, enter:

```
net start "ZENworks Handheld Management Server"
```

### **The ZENworks Handheld Management Client is not Pushed to the Palm Device**

**Action:** Ensure that ZENworks 7 Handheld Management Access Point or Desktop Synchronization Integration Software is installed.

**Possible Cause:** The Palm device has been synchronized to Palm HotSync only after the installation of ZENworks 7 Handheld Management Access Point or Desktop Synchronization Integration Software.

**Action:** Do the following:

- 1** Run `console.exe` from Access Point or Desktop Synchronization Integration Software installation directory. By default, ZENworks Handheld Management Access Point is installed in `c:\program files\novell\zfhap`, and Desktop Synchronization Integration Software is installed in `c:\program files\novell\zfhds`.

The ZENworks Handheld Management dialog box is displayed.

- 2** Click *Operations*, then click *Scan for Palm OS Handhelds*.

The following confirmation message is displayed:

*Count of the Palm handhelds* new Palm OS handhelds have been identified.

- 3** Synchronize the device again.

### **Unable to Remotely Control or Remotely View a Windows CE Device**

**Possible Cause:** The Remote Management policy has not been configured for the Windows CE device you want to remotely control or remotely view.

**Action:** Configure the Remote Management policy. For detail information on how to configure the policy, see [Section 6.1, "Configuring WinCE Remote Management Policy," on page 125](#)

**Possible Cause:** The Windows CE device you want remotely control or remotely view does not have a network IP address.

**Action:** Ensure that the Windows CE device you want remotely control or remotely view has a network IP address.

**Possible Cause:** The Windows CE device that you want to remotely control or remotely view is already being remotely managed.

**Action:** Do the following:

- 1** Terminate the existing Remote Control or Remote View session.

- 2** Start the Remote Control or the Remote View session.

**Even though the WinCE Configuration Access Point Policy, WinCE Remote Management Policy, or WinCE Configuration Policy for Uninstalling Applications is not Enforced on the Windows CE Device, the Policy Status is Reported as Enforced**

Possible Cause: The handheld client has ZENworks 6.5 Handheld Management installed, and the Handheld Management server has ZENworks 7 Handheld Management installed.

Action: Upgrade the handheld client to ZENworks 7 Handheld Management.

For more information on to how upgrade the client, see “[Upgrading the Windows CE or Palm OS IP Clients](#)” in the *Novell ZENworks 7 Handheld Management Installation Guide*.

**How to Change the User Account in Novell eDirectory After Installing ZENworks 7 Handheld Management Server?**

Action: Do the following:

- 1 Run `cfgsrvr.exe` from the `ZENworks_Handheld_Management_Server_installation_directory\program_files\novell\zfh`
- 2 In the Directory User Information page, enter the new user account name and password.
- 3 Complete the wizard.

**A Handheld device’s software inventory information in ConsoleOne is not updated.**

Possible Cause: By default, a device’s software inventory is collected every 24 hours. If the device is not cradled for more than 24 hours, software inventory cannot be collected. As a result, the software inventory that displays in ConsoleOne is not updated and is out of date. When the device is reconnected to the cradle, the information in ConsoleOne is updated. The frequency that software inventory is collected cannot be changed from the 24-hour default.

**Even though the device is connected all the time, the last connected time in ConsoleOne is not updated.**

Possible Cause: By default, a device makes a connection to the ZENworks Handheld Management server every hour. Some PPC devices in idle mode do not make the connection.

Action: Use the WinCE Configuration Policy to change the power settings on the device so it doesn’t go into idle mode. While configuring the WinCE policy, select *Disabled* for the *On battery power* and *On external power* settings on the Power tab of the WinCE Configuration Policy. For more information on WinCE Configuration Policy, see [Section 2.4.10, “WinCE Configuration Policy,” on page 55](#).

## A.5 Contacting Technical Support

If your troubleshooting efforts do not provide an answer to your questions, [Novell Support](#) (<http://www.novell.com/support>) provides a range of support options to access top-quality technical support.

# Configuring SSL and HTTP Settings

# B

By default, Novell® ZENworks® Handheld Management uses TCP/IP for communications between the ZENworks Handheld Management Access Point and ZENworks Handheld Management Server and between the handheld device and the ZENworks Handheld Management Access Point.

If you have just one ZENworks Handheld Management Access Point (installed as part of the ZENworks Handheld Management Server), there is no reason to turn on HTTP or SSL because the traffic between the ZENworks Handheld Management Access Point and the ZENworks Handheld Management Server is not going over the network. But you can enable HTTP and SSL for communication between handheld devices and the ZENworks Handheld Management Access Point.

If you configure SSL at the client and the server, additional encryption and verification is done on the data and the data source.

If you have installed the ZENworks Handheld Management Access Point on additional computers outside your firewall or if you have handheld devices connecting from outside a firewall, you might want to enable HTTP or SSL so that you do not need to open a port in the firewall or if you want all ZENworks Handheld Management communications to be encrypted.

If you enable HTTP at the ZENworks Handheld Management Server or ZENworks Handheld Management Access Point, these services listen to both TCP/IP and HTTP protocols.

SSL is supported on Palm OS devices running Palm OS 5.1 or later, and on Windows CE devices running Windows CE 3.0 or later. HPC 2.11 is not supported for SSL communication.

To use SSL communication in PPC 2000 devices, you must install the High Encryption pack for Pocket PC 1.0. You must reinstall the pack on every Hard-reset of the device. For more information about the High Encryption pack, see [Microsoft's High Encryption Pack for Pocket PC Web site \(http://www.microsoft.com/downloads/\)](http://www.microsoft.com/downloads/).

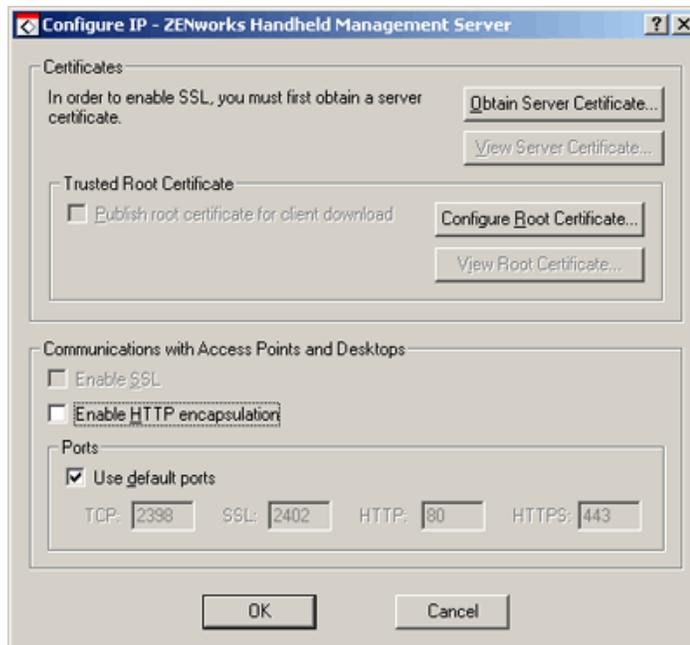
This section includes the following:

- ◆ [Section B.1, “Configuring the SSL and HTTP Communication between the ZENworks Handheld Management Server and the ZENworks Handheld Management Access Point,” on page 154](#)
- ◆ [Section B.2, “Configuring SSL and HTTP Communication between the ZENworks Handheld Management Access Point and the Handheld Devices,” on page 156](#)
- ◆ [Section B.3, “Changing the Default Ports on the ZENworks Handheld Management Server and ZENworks Handheld Management Access Point Communication,” on page 159](#)
- ◆ [Section B.4, “Changing the Default Ports for the ZENworks Handheld Management Access Point and the Handheld Devices Communication,” on page 159](#)

## B.1 Configuring the SSL and HTTP Communication between the ZENworks Handheld Management Server and the ZENworks Handheld Management Access Point

You can configure the SSL and HTTP settings using the `cgfip.exe` file.

- 1 Run `cgfip.exe` in the ZENworks Handheld Management installation directory.
- 2 Obtain a server certificate before using SSL.



- 2a In the Configure IP dialog box, click *Obtain Server Certificate*.
  - 2b Review the information in the Certificate Wizard page, then click *Next*.
  - 2c Specify the common name for the computer in the text box, then click *Next*.
  - 2d Specify information for your geographic location in the *Country/Region*, *State/Providence*, and *City/Locality* text boxes, then click *Next*.
  - 2e Specify information about your organization and organizational unit, then click *Next*.
  - 2f Specify the location in which you want to save the certificate request, then click *Next*.
  - 2g Click *Finish*, then click *OK*.
  - 2h Have the certificate signed by a Certificate Signing Authority, such as Novell Certificate Services (NCS) or VeriSign\*.

---

**NOTE:** To use NCS: In ConsoleOne<sup>®</sup>, click *Tools*, click *Issue Certificate*, then follow the prompts. When having the certificate signed (if given a choice), have it saved in Base64 format.

Handheld PCs running Windows CE 3.0 and Pocket PC 2000 devices do not support certificates originating from NCS.

---

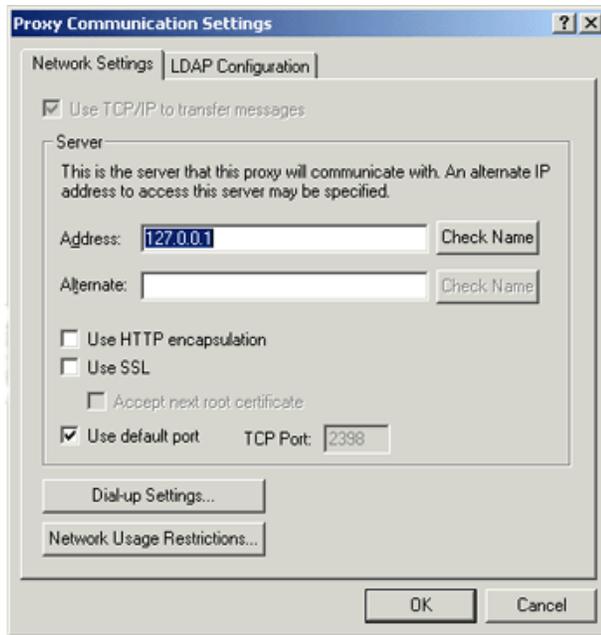
- 3** Import a server certificate before using SSL:
  - 3a** In the Configure IP dialog box, click *Import Server Certificate*.
  - 3b** Click *Next*.
  - 3c** Ensure that the *Process the Pending Request and Install the Certificate* option is enabled, then click *Next*.
  - 3d** Browse to the location where you saved the certificate during **Step 2h on page 154**, then click *Open*.
  - 3e** Click *Next*.
  - 3f** Click *Finish*.
- 4** You can publish a trusted SSL root certificate that desktop sync machines or remote ZENworks Handheld Management Access Points automatically download when they connect. This should be the root certificate of the Certificate Authority used to sign your server certificate.

If you are using a third-party Certificate Signing Authority and the root certificate does not already exist on the PC or handheld device (for example, a root certificate from NCS), you can publish the root certificate so that is automatically downloaded.

To publish a trusted SSL root certificate:

  - 4a** In the Configure IP dialog box, click *Configure Root Certificate*.
  - 4b** Browse to and select the signed root certificate, then click *Open*.

The root certificate that you get from a Certificate Authority (CA) must be in Base64 format.
  - 4c** Click *OK* twice.
- 5** To enable SSL on the ZENworks Handheld Management server, select the *Enable SSL* check box.
- 6** To enable HTTP on the ZENworks Handheld Management server, select the *Enable HTTP* check box.
- 7** To enable SSL/HTTP on the Access Point:
  - 7a** Run the `console.exe` file from the `zfhap` directory.
  - 7b** Select *Operations > Configure > Server Communications*.



- 7c To select SSL, select the *Use SSL* check box. If the server certificate is signed by non-standard certificate authority, then select the *Accept Next Root Certificate* check box.
- 7d To enable HTTP, select the *Use HTTP Encapsulation* check box.
- 7e Click *OK*.

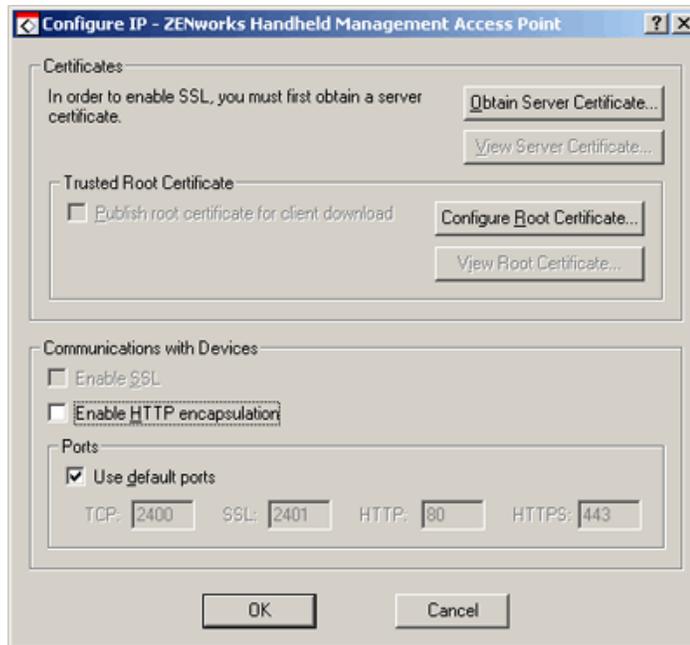
## B.2 Configuring SSL and HTTP Communication between the ZENworks Handheld Management Access Point and the Handheld Devices

You can configure the SSL and HTTP communication between the ZENworks Handheld Management Access Point and the Handheld devices by using `cfgip.exe` from the `zfhap` directory.

We recommend you to use SSL for communication between the ZENworks Handheld Management Access Point and the Handheld devices because SSL provides the following primary security services:

- ♦ **Message Privacy:** All transmissions after the initial handshake between the ZENworks Handheld Management Access Point and the Handheld device are encrypted.
- ♦ **Session Integrity:** A secure channel is opened between the ZENworks Handheld Management Access Point and the Handheld device.
- ♦ **Mutual Authentication:** The ZENworks Handheld Management Access Point and the Handheld device can establish their authenticity.

- 1 Launch `cfgip.exe` from `zfhap` directory.



## 2 Obtain a server certificate before using SSL.

---

**NOTE:** Palm devices do not support adding root certificates that are bundled with them by default.

---

- 2a** In the Configure IP - ZENworks Handheld Management Access Point dialog box, click *Obtain Server Certificate*.
- 2b** Review the information on the Certificate Wizard page, then click *Next*.
- 2c** Specify the common name for the computer in the text box, then click *Next*.

---

**NOTE:** If you want to connect your PPC 2000 device using SSL, you must keep in mind the following points:

1. The server address is stored as the IP address because the Domain Name Resolution does not work on PPC 2000 devices.
  2. If the PPC 2000 device is connected using IP client through wireless, you must specify the IP address of the ZENworks Handheld Management Access Point instead of the common name when you create the Certificate Signing Request (CSR). This enables the device to validate the Certificate server. But if the device cradle syncs, you can use the common name by selecting the Use Desktop sync settings check box in the ZENworks Console that is available on the device.
- 

- 2d** Specify information for your geographic location in the *Country/Region*, *State/Providence*, and *City/Locality* text boxes, then click *Next*.
- 2e** Specify information about your organization and organizational unit, then click *Next*.
- 2f** Specify the location in which you want to save the certificate request, then click *Next*.
- 2g** Click *Finish*, then click *OK*.
- 2h** Have the certificate signed by a Certificate Signing Authority, such as Novell Certificate Services (NCS) or VeriSign.

---

**NOTE:** To use NCS: In ConsoleOne, click *Tools*, click *Issue Certificate*, then follow the prompts. When having the certificate signed (if given a choice), have it saved in Base64 format.

Handheld PCs running Windows CE 3.0 and Pocket PC 2000 devices do not support certificates originating from NCS.

---

- 3** To import a server certificate before using SSL:
  - 3a** In the Configure IP - ZENworks Handheld Management Access Point dialog box, click *Import Server Certificate*.
  - 3b** Click *Next*.
  - 3c** Ensure that the *Process the Pending Request and Install the Certificate* option is enabled, then click *Next*.
  - 3d** Browse to the location where you saved the certificate during [Step 2h on page 157](#), then click *Open*.
  - 3e** Click *Next*.
  - 3f** Click *Finish*.
- 4** You can publish a trusted SSL root certificate that Windows CE clients automatically download when they connect. This should be the root certificate of the Certificate Authority used to sign your server certificate.

If you are using a third-party Certificate Signing Authority and the root certificate does not already exist on the PC or handheld device (for example, a root certificate from NCS), you can publish the root certificate so that is automatically downloaded.

To publish a trusted SSL root certificate:

  - 4a** In the Configure IP - ZENworks Handheld Management Access Point dialog box, click *Configure Root Certificate*.
  - 4b** Browse to and select the signed root certificate, then click *Open*.

The root certificate that you get from a Certificate Authority (CA) must be in Base64 format.
  - 4c** Click *OK* twice.
- 5** To enable the SSL on the ZENworks Handheld Management Access Point, select the *Enable SSL* check box.
- 6** To enable HTTP on the ZENworks Handheld Management Access Point, select the *Enable HTTP Encapsulation* check box.
- 7** To enable SSL/HTTP on a handheld device, open the ZENworks console and do the following:
  - 7a** For PalmOS devices, select the server from the drop-down list and select *Use SSL*.

or

For Windows CE devices, click *Configure*, then click *Use SSL*.

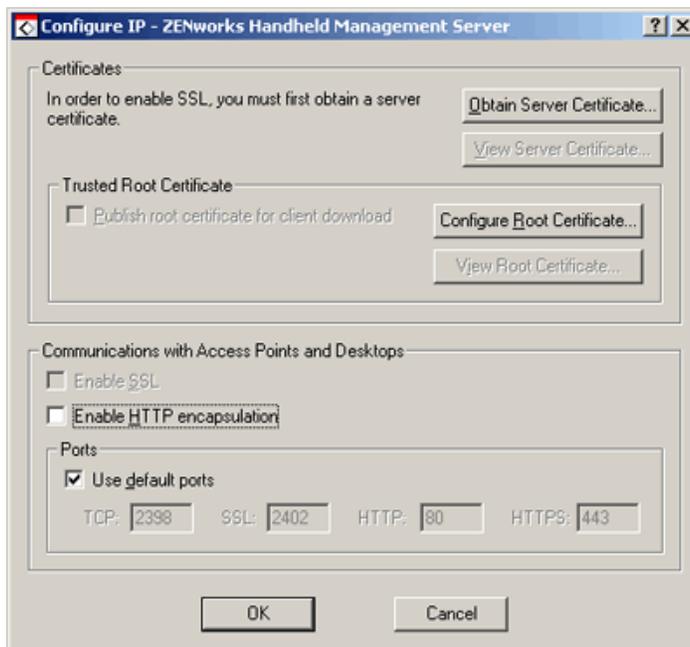
If you are publishing a root certificate, click *Accept Next Root Certificate*.
  - 7b** To enable HTTP for Palm devices, select *Server* from the drop-down list, then click *Use HTTP encapsulation*.

or

For Windows CE devices, click *Configure*, then click *Use HTTP Encapsulation*.

## B.3 Changing the Default Ports on the ZENworks Handheld Management Server and ZENworks Handheld Management Access Point Communication

- 1 Run `cfgip.exe` from the ZENworks Handheld Management Server installation directory.
- 2 In the Configure IP - ZENworks Handheld Management Server dialog box, do the following:
  - 2a Deselect the *Use Default* check box.
  - 2b Type the desired TCP, SSL, HTTP, and HTTPS ports that you want the ZENworks Handheld Management Server to use.
  - 2c Click *OK*.

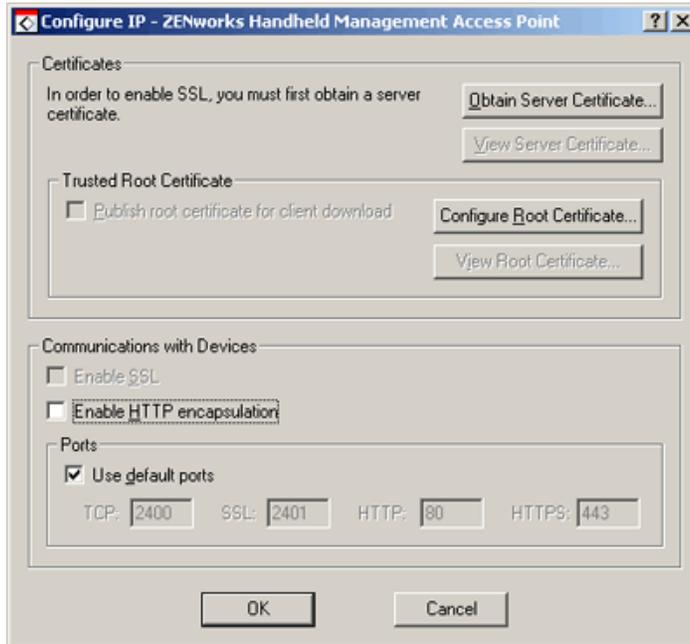


- 3 Configure the ZENworks Handheld Management Access Point to connect to the new ports.
  - 3a Run `console.exe` from the `zfhap` directory.
  - 3b Select *Operations > Configure > Server Communication*.
  - 3c Deselect the *Use Default Port* check box.
  - 3d Specify the desired port that you want the ZENworks Handheld Management Access Point to use for communicating with the ZENworks Handheld Management server.
  - 3e Click *OK*.

## B.4 Changing the Default Ports for the ZENworks Handheld Management Access Point and the Handheld Devices Communication

- 1 Launch `cfgip.exe` from `zfhap` directory.

- 2 In the Configure IP - ZENworks Handheld Management Access Point dialog box, do the following:
  - 2a Deselect the *Use Default Ports* check box
  - 2b Specify the desired TCP, SSL, HTTP, and HTTPS ports that you want the ZENworks Handheld Management Access Point to use.
  - 2c Click *OK*.



- 3 On the Handheld device, open the ZENworks console and do the following:

For PalmOS devices, click the *ZENworks* menu > *Server*, then deselect the *Use Default Port* check box. Specify the port that you want the device to use for connecting to the ZENworks Handheld Management Access Point

or

For Windows CE devices, click *Configure* > *Use SSL*, then deselect the *Use Default Port* check box. Specify the port that you want the device to use when connecting to the ZENworks Handheld Management Access Point.

# Security Considerations

# C

To ensure the security of your ZENworks Handheld Management System, you should use the following best practices:

- ◆ Make sure the database is protected, because it contains system information that is vulnerable to hacking.
- ◆ Use SSL to communicate between a device and the ZENworks Handheld Management Access Point, and between the Access Point and the Handheld Management Server, in order to protect the data on a wired or wireless network. For detail information on how to enable SSL, see [B.0 Configuring SSL and HTTP Settings](#).
- ◆ Use the ZENworks Handheld Management Remote Control VNC software behind the firewall in a protected environment.
- ◆ Use a strong ZENworks Handheld Management Remote Control VNC software password.

---

**NOTE:** Do not use an eDirectory password as the ZENworks Handheld Management Remote Control VNC software password for security of eDirectory password.

---



# Documentation Updates

# D

This section contains information on documentation content changes that have been made in the *Administration Guide* after the initial release of Novell® ZENworks® 7 Handheld Management. The information helps you to keep current on updates to the documentation.

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

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

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

The documentation was updated on the following dates:

- ♦ [Section D.1, “July 14, 2006,” on page 163](#)
- ♦ [Section D.2, “December 9, 2005,” on page 163](#)
- ♦ [Section D.3, “October 7, 2005,” on page 164](#)

## D.1 July 14, 2006

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

- ♦ [Section D.1.1, “Appendix C: Security Considerations,” on page 163](#)

### D.1.1 Appendix C: Security Considerations

The following changes were made in this section:

Location	Change
<a href="#">Appendix C, “Security Considerations,” on page 161</a>	Added Appendix C-Security Considerations. It lists the security considerations for ZENworks 7 Handheld Management.

## D.2 December 9, 2005

Page design of the entire guide was reformatted to comply with revised Novell documentation standards.

## D.3 October 7, 2005

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

- ♦ [Section D.3.1, “Using Inventory and Reports,” on page 164](#)
- ♦ [Section D.3.2, “Using ZENworks Handheld Management Policies,” on page 164](#)

### D.3.1 Using Inventory and Reports

The following changes were made in this section:

---

Location	Change
<a href="#">Section 5.2, “Viewing Hardware Inventory,” on page 118</a>	Added the following note:  “For Java-based BlackBerry devices, the Password Enabled field value is not scanned for and the value is always displayed as “No”. The value of Power Save Mode is always “Off”. The serial number is same as the PIN value of the device.”

---

### D.3.2 Using ZENworks Handheld Management Policies

The following changes were made in this section:

---

Location	Change
<a href="#">“BlackBerry Configuration Policy” on page 30</a>	Added the following note:  “This policy is not supported for Java-based BlackBerry devices.”
<a href="#">“BlackBerry Security Policy” on page 34</a>	Added the following note:  “This policy is not supported for Java-based BlackBerry devices.”
<a href="#">“Scheduling Packages and Policies” on page 74</a>	Deleted the following text from the second point, which is one of the considerations that you must ensure if you have configured and enabled policies, but not yet enforced on individual handheld devices:  “To change the value, right-click the ZENworks Handheld Management Service object in ConsoleOne, click Properties, in the General page, set the Directory Scan Interval value.”

---