

Policy Management Reference

Novell® ZENworks® 10 Configuration Management SP3

10.3

November 17, 2011

www.novell.com



Legal Notices

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

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

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

Copyright © 2007 - 2011 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.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the [Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide	9
1 Overview	11
1.1 What Is a Policy?	11
1.2 What Is a Policy Group?	11
1.3 Understanding the Policy Types	12
1.4 Understanding the Features of a Policy	12
2 Creating Policies	15
2.1 Browser Bookmarks Policy	15
2.2 Dynamic Local User Policy	16
2.2.1 Rules for Workstations	19
2.2.2 Rules for Users	20
2.3 Local File Rights Policy	21
2.4 Printer Policy	23
2.5 Remote Management Policy	27
2.6 Roaming Profile Policy	28
2.7 SNMP Policy	29
2.8 Windows Group Policy	30
2.9 ZENworks Explorer Configuration Policy	33
2.10 Creating Policies by Using the zman Command Line Utility	34
2.10.1 Creating a Policy without Content	35
2.10.2 Creating a Policy with Content	37
2.10.3 Understanding the zman Policy XML File Format	38
3 Managing Policies	41
3.1 Policy Groups	41
3.2 Editing Policies	42
3.3 Deleting Policies	43
3.4 Adding Policies to Groups	43
3.5 Assigning a Policy to Devices	44
3.6 Assigning a Policy to Users	46
3.7 Assigning a Roaming Profile Policy that has the User Profile Stored on a Windows, Linux or NetWare Share	47
3.7.1 Creating a Default Profile Folder in a Shared Location	48
3.7.2 Copying the Default Profile from a Windows Vista, Windows 2008 or a Windows 7 device to the Default Profile Folder in the Shared Location	48
3.7.3 Configuring the Permissions for the Default Profile Registry Hive	48
3.7.4 Copying the Default Profile to User Folders	49
3.8 Assigning a Roaming Profile Policy that has the User Profile Stored on a Home Directory	49
3.9 Assigning the Local File Rights Policy to Devices Running Different Languages	50
3.10 Unassigning a Policy from Devices	50
3.11 Unassigning a Policy from Users	51
3.12 Adding System Requirements for a Policy	51
3.12.1 Filter Conditions	51

3.12.2	Filter Logic	55
3.13	Disabling Policies	56
3.14	Enabling the Disabled Policies	56
3.15	Copying a Policy to a Content Server	56
3.16	Incrementing the Policy Version	58
3.16.1	Using the Action Menu	58
3.16.2	Editing the Policy	59
3.17	Reviewing the Status of the Policies at the Managed Device	59
3.18	Policy Issues on a Windows 7, Windows Server 2008, or Windows Server 2008 R2 device	59
3.19	Viewing the Predefined Reports	60
4	Managing Policy Groups	63
4.1	Creating Policy Groups	63
4.2	Renaming or Moving Policy Groups	64
4.3	Deleting a Policy Group	64
4.4	Assigning a Policy Group to Devices	65
4.5	Assigning a Policy Group to Users	65
4.6	Adding a Policy to a Group	66
5	Managing Folders	67
5.1	Creating Folders	67
5.2	Renaming or Moving Folders	67
5.3	Deleting a Folder	68
A	Troubleshooting Policy Management	69
A.1	Browser Bookmarks Policy Errors	69
A.2	Browser Bookmarks Policy Troubleshooting	70
A.3	Dynamic Local User Policy Errors	71
A.4	Dynamic Local User Policy Troubleshooting	72
A.5	General Policy Troubleshooting	74
A.6	Local File Rights Policy Errors	76
A.7	Local File Rights Policy Troubleshooting	77
A.8	Printer Policy Errors	78
A.9	Printer Policy Troubleshooting	80
A.10	Roaming Profile Policy Errors	85
A.11	Roaming Profile Policy Troubleshooting	85
A.12	SNMP Policy Errors	86
A.13	Windows Group Policy Errors	86
A.14	Windows Group Policy Troubleshooting	89
A.15	ZENworks Explorer Configuration Policy Errors	95
B	iPrint Policy Management Utility	99
B.1	Installing the IPPman Utility	99
B.2	Using IPPman Commands to Configure iPrint Printers	100
B.2.1	Creating an iPrint Printer	100
B.2.2	Cloning an iPrint Printer	101
B.2.3	Renaming an iPrint Printer	102
B.2.4	Modifying an iPrint Printer	103

B.2.5	Deleting an iPrint Printer	104
B.2.6	Exporting iPrint Printer	105
B.2.7	Importing an iPrint Printer	105
B.3	Understanding the Format of the iPrint Printer Configuration File	107
B.3.1	Format of iPrint Printer Configuration File with Default Printing Preferences	107
B.3.2	[Example] iPrint Printer Configuration File with Some Printing Preferences Specified	107
B.4	Printing Preferences for an iPrint Printer	108
B.5	iPrint Printer List Import File Format	108
C	Best Practices	109
C.1	Local File Rights Policy	109
C.2	Dynamic Local User Policy	109
C.3	Roaming Profile Policy	109
C.4	SNMP Policy	109
C.5	Windows Group Policy	110
C.6	Printer Policy	110
D	Documentation Updates	111
D.1	November 17, 2011: Update to ZENworks 10 Configuration Management SP3 (10.3.4) ...	111
D.2	July 06, 2011: Update to ZENworks 10 Configuration Management SP3 (10.3.3)	112
D.3	January 17, 2011: Update to ZENworks 10 Configuration Management SP3 (10.3.2)	112
D.4	March 30, 2010: Update to ZENworks 10 Configuration Management SP3 (10.3)	113

About This Guide

This *Novell ZENworks 10 Configuration Management Policy Management Reference* includes information about Policy Management features and procedures to help you configure and maintain your Novell ZENworks 10 Configuration Management SP3 system. The information in this guide is organized as follows:

- ♦ Chapter 1, “Overview,” on page 11
- ♦ Chapter 2, “Creating Policies,” on page 15
- ♦ Chapter 3, “Managing Policies,” on page 41
- ♦ Chapter 4, “Managing Policy Groups,” on page 63
- ♦ Chapter 5, “Managing Folders,” on page 67
- ♦ Appendix A, “Troubleshooting Policy Management,” on page 69
- ♦ Appendix C, “Best Practices,” on page 109
- ♦ Appendix B, “iPrint Policy Management Utility,” on page 99
- ♦ Appendix D, “Documentation Updates,” on page 111

Audience

This guide is intended for Novell ZENworks administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Additional Documentation

ZENworks Configuration Management is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the [ZENworks 10 Configuration Management SP3 documentation \(http://www.novell.com/documentation/zcm10/\)](http://www.novell.com/documentation/zcm10/).

Overview

1

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

The following sections contain additional information:

- ♦ [Section 1.1, “What Is a Policy?,” on page 11](#)
- ♦ [Section 1.2, “What Is a Policy Group?,” on page 11](#)
- ♦ [Section 1.3, “Understanding the Policy Types,” on page 12](#)
- ♦ [Section 1.4, “Understanding the Features of a Policy,” on page 12](#)

1.1 What Is a Policy?

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

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

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

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

1.2 What Is a Policy Group?

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

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

1.3 Understanding the Policy Types

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

- ♦ **Browser Bookmarks Policy:** Lets you configure Internet Explorer favorites for Windows devices and users.
- ♦ **Dynamic Local User Policy:** Lets you create new users and manage existing users created on Windows 2000, Windows XP, and Windows Vista workstations; and Windows 2000, 2003, and Windows 2008 Terminal Server sessions after the users have successfully authenticated to the user source.
- ♦ **Local File Rights Policy:** Lets you configure rights for files or folders that exist on the NTFS file systems.

The policy can be used to configure basic and advanced permissions for both local and domain users and groups. It provides the ability for an administrator to create custom groups on managed devices.
- ♦ **Printer Policy:** Lets you configure Local, SMB, HTTP, and iPrint printers on a Windows machine.
- ♦ **Remote Management Policy:** Lets you configure the behavior or execution of Remote Management sessions on the managed device. The policy includes properties such as Remote Management operations and security.
- ♦ **Roaming Profile Policy:** Lets you to create a user profile that is stored in a network path.

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

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

1.4 Understanding the Features of a Policy

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

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

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

The Roaming Profile policy can be applied only to a user.
- ♦ A policy can be associated to groups and containers.

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

- ◆ A policy can be associated to query groups.

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

- ◆ Policies are chronologically ordered by default.

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

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

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

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

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

- ◆ Policies support management by exception.

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

- ◆ Policies support system requirements.

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

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

- ◆ ZENworks Configuration Management supports singular and plural policies.

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

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

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

The Browser Bookmarks policy, Local File Rights policy, Windows Group policy, and Printer policy are plural policies. However, the security settings in the Windows Group policy are not plural.

- ◆ Policies can be disabled.

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

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

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

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

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

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

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

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

Creating Policies

2

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

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

- ◆ [Section 2.1, “Browser Bookmarks Policy,” on page 15](#)
- ◆ [Section 2.2, “Dynamic Local User Policy,” on page 16](#)
- ◆ [Section 2.3, “Local File Rights Policy,” on page 21](#)
- ◆ [Section 2.4, “Printer Policy,” on page 23](#)
- ◆ [Section 2.5, “Remote Management Policy,” on page 27](#)
- ◆ [Section 2.6, “Roaming Profile Policy,” on page 28](#)
- ◆ [Section 2.7, “SNMP Policy,” on page 29](#)
- ◆ [Section 2.8, “Windows Group Policy,” on page 30](#)
- ◆ [Section 2.9, “ZENworks Explorer Configuration Policy,” on page 33](#)

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

- ◆ [Section 2.10, “Creating Policies by Using the `zman` Command Line Utility,” on page 34](#)

2.1 Browser Bookmarks Policy

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

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

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

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

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

- 4 Click *Next* to display the Bookmarks Tree Data Source page.
- 5 Create a browser bookmarks tree by importing a previously exported file or manually entering the data. Before you import a book marks file ensure that it is in UTF-8 format. To manually convert the bookmark file into UTF-8 format, use a text editor

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

- ♦ **Internet Explorer 6.x/8.x:** In the browser window, click *File > Import and Export*. Follow the instructions given in the Import/Export Wizard to create the `bookmark.htm` file.
 - ♦ **Internet Explorer 7:** In the browser window, click *Add to Favorites > Import and Export*. Follow the instructions given in the Import/Export Wizard to create the `bookmark.htm` file.
 - ♦ **Mozilla Firefox 2.x:** In the browser window, click *Bookmarks > Organize Bookmarks*, then click *File > Export* to create the `bookmarks.html` file.
 - ♦ **Mozilla Firefox 3.x:** In the browser window, click *Bookmarks > Organize Bookmarks*, then click *Import and Backup > Export HTML* to create the `bookmarks.html` file.
- 6 Click *Next* to display the Bookmarks Tree Configuration page, then use the options to configure the bookmarks tree.

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

Field	Details
<i>New</i>	<ul style="list-style-type: none"> ♦ Click <i>New > Folder</i> to display the Add Folder to Bookmarks dialog box, through which you can add a new folder to the bookmarks tree. ♦ Click <i>New > Bookmark</i> to display the Add Bookmark to Bookmarks dialog box, through which you can add a new bookmark to the bookmarks tree by specifying the bookmark name and a URL. Click the button next to the URL field to verify that the URL entered by you is correct and functional.
<i>Edit</i>	<ul style="list-style-type: none"> ♦ Select the bookmark name you want to change, click <i>Edit > Rename</i>, then specify a new name. ♦ Click <i>Edit > Sort</i> to organize the bookmarks in ascending or descending order. ♦ Click <i>Edit > Move Up</i>, <i>Move Down</i>, or <i>Move To</i> to relocate a bookmark. ♦ Click <i>Edit > Select All Children</i> to select all the subdirectories and bookmarks of the selected parent directory. ♦ Click <i>Edit > Deselect All Children</i> to deselect all the subdirectories and bookmarks of the selected parent directory. ♦ Click <i>Edit > Clear Selection</i> to clear the selections.
<i>Delete</i>	<ul style="list-style-type: none"> ♦ Click <i>Delete</i> to delete the selected bookmarks and the bookmarks folder from the bookmarks tree. However, you cannot delete the default bookmarks folder named <code>Bookmarks</code>.

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

2.2 Dynamic Local User Policy

The Dynamic Local User policy lets you create new users and manage existing users on the managed device after they have successfully authenticated to the user source.

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

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

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

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

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

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

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

Field	Details
<i>Use User Source Credentials</i>	Enables logging in through the user's authoritative source credentials instead of using the Windows credentials.
<i>Use the Credentials Specified Below (Always volatile)</i>	Allows you to specify the following user credentials for a volatile user: <ul style="list-style-type: none">◆ User Name: Specify the user's name.◆ Full Name: Specify the user's complete name.◆ Description: Provide any additional information that helps the administrator to further identify this user account. <p>If a user logs in to a device that has the Dynamic Local User policy applied and then logs out of the device when the device is disconnected from the network, the user is unable to log in to the disconnected device again. For information on this issue, see "Dynamic Local User Policy Troubleshooting" on page 72.</p>
<i>Manage Existing User Account (if any)</i>	Helps you to manage a user object that already exists. <p>If you select both the <i>Volatile User</i> and <i>Manage Existing User Account (If Any)</i> check boxes, and the user has a permanent local account that uses the same username specified in the user source, the permanent account is changed to a volatile (temporary) account and is removed when the user logs out.</p>
<i>Volatile User</i>	Specifies the use of a volatile user account for login. The user account that NWGINA creates on the local workstation can be either a volatile or a nonvolatile account.
Enable Volatile User Cache	Enables the caching of the volatile user account on the device for a specified period of time.

Field	Details
Cache Volatile User for Time Period (Days)	Allows you to specify the number of days to cache the volatile user account on the device. The default value is 5. You can specify a value from 1 to 999 days. This volatile user account is deleted after the expiry of the specified cache period when another DLU user logs out from the device.
<i>Not a Member Of</i>	Displays the available group to which a user can be assigned as a member.
<i>Member Of</i>	Displays groups a user is member of.
<i>Custom</i>	Click <i>Custom</i> to display the Custom Group Properties dialog box, through which you can add a new custom group and configure its rights.
<i>Edit</i>	Click <i>Edit</i> to view and edit the details of a custom group. You cannot edit the default Windows groups with this option.
<i>Delete</i>	Click <i>Delete</i> to delete a custom group. You cannot delete the default Windows groups with this option.

5 Click *Next* to display the Login Restrictions page, then fill in the fields to configure user access:

- ♦ **Included / Excluded Users:** Lists the users and containers that you want to include or exclude access to. For more information, see “[Rules for Users](#)” on page 20.
- ♦ **Included / Excluded Workstations:** Lists the workstations and containers that you want to include or exclude access to. For more information, see “[Rules for Workstations](#)” on page 19.

The *Excluded Workstations List* displays the workstations and containers that you want to exclude DLU access to. Workstations listed or workstations that are in the containers listed here cannot use DLU access. You can make exceptions for individual workstations by listing them in the *Included Workstations List*. This allows DLU access to those workstations only, and excludes DLU access to the remaining workstations in the container. If the user account is already on the workstation, the option to exclude the device from receiving the DLU policy is ignored.

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

For a DLU Policy, the timeout duration for enforcing file rights, if it is configured, is 120 seconds. For large directory structures, the DLU policy might not be enforced because of a timeout. To enforce the file rights, follow instructions in TID 7004171, in the [Novell Support Knowledgebase \(http://www.novell.com/support/knowledgebase/?usemicrosite=true&searchString=7004171\)](http://www.novell.com/support/knowledgebase/?usemicrosite=true&searchString=7004171).

The following table contains information about managing Dynamic Local User file system access on the managed device:

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

7 Click *Next* to display the Summary page.

8 Click *Finish* to create the policy now, or select *Define Additional Properties* to specify additional information, such as policy assignment, [system requirements](#), enforcement, status, and which group the policy is a member of.

2.2.1 Rules for Workstations

Be aware of the following:

- ◆ By default, all workstations are included.
- ◆ For an indirect association, if an object is in both lists, the closeness of the association is considered. A direct association is closer than a group association, which in turn is closer than a folder.

- ◆ If the closeness is the same, a workstation is directly added to Group A and Group B, and the *Included List* takes precedence.

Excluded List	Included List	Result
Workstation-A	Workstation-B	The policy is applied on all workstations except Workstation-A.
Workstation Group-1	Workstation-A	The policy is not applied on any workstations in Workstation Group-1, except for Workstation -A. The policy is applied on workstations that are not contained in Workstation Group-1.
Container-1	Workstation Group-1 or Workstation-A	The policy is not applied on any workstations in Container-1, except for Workstation Group-1 or Workstation-A. The policy is also applied on workstations that are not contained in Container-1.

2.2.2 Rules for Users

Be aware of the following:

- ◆ By default, all users are included.
- ◆ For an indirect association, if an object is in both the lists, the closeness of the association is considered. A direct association is closer than a group association, which in turn is closer than a folder.
- ◆ If the closeness is the same, a user is directly added to Group A and Group B, and the *Included List* takes precedence.

Excluded List	Included List	Result
User-A	User-B	The policy is applied on all users except User-A.
User Group-1	User-A	The policy is not applied on any users in User Group-1, except for User -A. The policy is also applied on users that are not contained in User Group-1.

Excluded List	Included List	Result
Container-1	User Group-1 or User-A	The policy is not applied on any users in Container-1, except for User Group-1 or User-A. The policy is also applied on users that are not contained in Container-1.

2.3 Local File Rights Policy

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

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

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

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

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

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

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

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

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

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

The following table contains information about configuring permissions:

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

NOTE: If the *Full Control* access right is denied for the Administrators or Authenticated Users group, the policy is successful only during the first enforcement. However, if the *Full Control* access right is denied for the Administrators or Authenticated Users group and the *Remove access control rules not configured by ZENworks* option is selected, the policy fails.

The unenforcement of the Local File Rights policy from a device fails if the Full Control access right is denied for the Administrators or Authenticated Users group in the policy.

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

2.4 Printer Policy

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

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

NOTE: Create and assign separate policies for different platforms for a printer.

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

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

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

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

Field	Details
<i>Name / Location</i>	<p>Specify the UNC path or URL name of the HTTP or an SMB printer.</p> <p>For example, it is <code>\\server-name\printer-name</code> for an SMB printer, and <code>http://server/printers/.myprinter/.printer</code> for a HTTP printer.</p> <hr/> <p>NOTE: Support for network printer that prompts for user credentials is not provided.</p>
<i>Driver</i>	<p>Browse to add and select a suitable driver for the Windows HTTP printer. You can ignore this for SMB printers.</p> <p>The driver must be digitally signed by Microsoft. However, if you choose to use a driver that is not digitally signed, see the Troubleshooting Scenario</p>
<i>Install a Driver</i>	<p>Use this option to install a driver on the target device. The driver installation is non-interactive and silent. The supported driver installation types is <code>.inf</code> and the <code>.inf</code> driver files can be bundled in <code>.zip</code> or <code>.tar</code> formats. The <code>.inf</code> file can be specified directly if it is already available on the target device. Ensure that the <code>.inf</code> file supports the installation of the driver.</p> <hr/> <p>NOTE: To add a new printer driver to the existing driver list:</p> <p>Edit the <code>zenworks_installdir\novell\zenworks\share\tomcat\webapps\zenworks\WEB-INF\conf\printerDriverDetails.conf</code> file to add the following line:</p> <pre>Printer_Manufacturername = Printer_Model</pre> <p>For example, if you want to add an HP Color LaserJet 4550 PCL printer, then add the following line:</p> <pre>HP = HP Color LaserJet 4550 PCL</pre>
<i>Model Name</i>	Browse to select the model name of the driver.
<i>Driver File Path</i>	<p>Specify the driver files either from a particular device where the browser is running or from a path in the managed device, such as <code>c:\temp\nip.zip</code>.</p> <hr/> <p>NOTE: While configuring the policy, if you are using a UNC path to access the Driver file, make sure the file you access must be on an anonymous share.</p>
<i>Supported Platforms</i>	Specify a platform for the driver. The platform information helps to select a suitable driver from the available drivers list, which is based on the installation platform.
<i>Language of Installation</i>	Select the installation language. Your choices are English (United States), French, German, Portugese, Spanish, Italian, Chinese (Traditional), Chinese (Simplified), or Japanese.
<i>Install Forcefully Even if the Driver is Already Installed</i>	Select this option to force the installation of the driver on the device every time the policy is applied on the device, even if the driver is already installed on the device.

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

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

Field	Details
<i>Name / Location</i>	Specify the URI name of the iPrint printer. For example, <code>ipp://acme.com/ipp/servername</code> .
<i>Update iPrint Printer while Installing the Driver</i>	Select this option to update the printer driver and to reinstall the printer driver from the iPrint server while installing the iPrint printer.
<i>Install iPrint Client</i>	Select this option to install the iPrint client on a target machine. The iPrint client is not supported on 64-bit versions of Windows Server 2003. The installation file can be either <code>nipp.zip</code> or <code>nipp-s.exe</code> , both of which are capable of carrying out non-interactive silent installation. These files can be uploaded from the machine where the browser is running. To install the iPrint client, you cannot use a <code>.exe</code> file that does not support a silent installation. For example, you cannot use a <code>nipp.exe</code> file to install iPrint client.
<i>iPrint Client Installer File Path</i>	Allows to specify the path to the iPrint Client Installer (which installs the iPrint client on the managed device). <ul style="list-style-type: none"> ◆ On the Managed Device: Select this option to specify the path to the iPrint client installer on the managed device. ◆ Select from this Device: Select this option to add the iPrint client installer as content with the policy. You can also distribute the iPrint client installer along with the policy.
<i>Install Forcefully Even if the Driver is Already Installed</i>	Select this option to force installation of the driver, even though it is already installed on the target device.
<i>Configure iPrint Client</i>	Select this option to configure the iPrint proxy server. If the workstations are located outside the physical firewall, you can use this option to specify the proxy address followed by a <code>(:)</code> and the port number.
<i>Proxy Server</i>	Specify the iPrint proxy server name. For example, <code>http://proxy.companyx.com:8080</code>

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

Field	Details
<i>Orientation</i>	Select this option to specify the paper layout for the printer, such as landscape or portrait.
<i>Duplex Printing</i>	Specify whether or not to print on both sides of the paper, if the printer has that capability.
<i>Collate</i>	Specify whether or not the printer should organize multiple copies of a document, if the printer has that capability.

Field	Details
<i>Print Quality</i>	Select the print quality. Select <i>High</i> quality, for the best possible resolution, or select <i>Low</i> quality for lower resolution and lower quality.
<i>Paper Source</i>	Specify the paper source for the printer. A source that is not listed in the standard available list can also be specified, but it must be supported by the printer. Information on supported paper sources is available in the printer documentation or in the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\printer-name\DsDriver\printBinNames on a Windows machine.
<i>Paper Size</i>	Specify the paper size for the printer. You can specify any paper size supported by the printer, in addition to the options listed in the menu. Information on supported sizes is available in the printer documentation or in the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\printer-name\DsDriver\printMediaSupported on a Windows machine, where a printer is locally installed.

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

Field	Details
<i>Set as Default Printer</i>	Select this option to specify a printer as the default printer to which the print requests are sent if no other printer is specified by the user. On a Windows 7 managed device, the assigned printer might be set as a default printer on the device even if the <i>Set as Default Printer</i> option is not selected in the policy.
<i>Remove all Printers not Specified by ZENworks Printer Policies</i>	Select this option to remove all printers that are not specified through the ZENworks Printer policy.

- 11** Click *Next* to display the Summary page.
This wizard allows you to configure only one printer. If you want to configure additional printers, then configure them in the Details page after creating the policy.
- 12** Click *Finish* to create the policy now, or select *Define Additional Properties* to specify additional information, such as policy assignment, [system requirements](#), enforcement, status, and which group the policy is a member of.
Only the preferences that are supported by the printer are configured on that printer.

2.5 Remote Management Policy

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

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

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

2.6 Roaming Profile Policy

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

IMPORTANT: Because of the security settings in Microsoft Vista, administrators must manually add the appropriate security rights to the user registry hive to enable roaming profiles. For more information, see [Section 3.7, “Assigning a Roaming Profile Policy that has the User Profile Stored on a Windows, Linux or NetWare Share,”](#) on page 47.

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

NOTE: If you log into Windows Vista or Windows 7 by using a domain account, Roaming Profile policy is not supported.

- 4 In the *Define Details* page fill in the following fields:

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

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

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

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

Field	Details
<i>Store User Profile in User’s Home Directory</i>	Select this option to load and save a user’s profile from the user’s home directory as specified in eDirectory. This option is applicable only if the user object is in eDirectory. However, it is currently not supported in Domain Services for Windows environment.
<i>User Profile Path</i>	Select a UNC path to a user’s roaming profile. If you want to administer the policy on more than one user object, use <code>%USERNAME%</code> as the environment variable. In this case, the environment variable is resolved with the logged-on username and the user profile is loaded from the specified path.

Field	Details
<i>Override Terminal Server Profile</i>	If a user is accessing a terminal server that has its own profile, enable this option to override the terminal server's profile.

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

2.7 SNMP Policy

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

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 In the *Policies* list, click *New*, then click *Policy* to display the Select Policy Type page.
- 3 Select *SNMP Policy*, click *Next* to display the Define Details page, then fill in the fields:
 - Policy Name:** Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in ZENworks Control Center.
 - Folder:** Type the name or browse to the ZENworks Control Center folder where you want the policy to reside. The default is `/policies`, but you can create additional folders to organize your policies.
 - Description:** Provide a short description of the policy's content. This description displays in ZENworks Control Center.
- 4 Click *Next* to display the SNMP Community Strings page. Refer to the following table for more information:

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

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

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

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

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

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

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

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

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

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

2.8 Windows Group Policy

The Windows Group Policy allows you to configure a Group Policy for Windows devices.

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

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

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

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

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

Field	Details
<i>Select the Type of Group Policy to Manage</i>	<p>With the Windows Group Policy, you can manage either a Local group or an Active Directory group policy.</p> <p>Before you can configure the Group Policy, you need to install a helper application. Click <i>Install the Group Policy Helper</i> to install the novell-zenworks-grouppolicyhelper-10.x.x.x.msi, which is a Windows installer package. This installation needs to be done only once. After the helper is installed, clicking <i>Configure</i> launches the helper, which you then use to configure or import a policy.</p> <ul style="list-style-type: none">♦ Local Group Policy: Select this option to configure a Local Group policy. To launch the group policy helper, click <i>Configure</i>. Configure or edit the settings in the Local Group policy, then upload the configured policy to the ZENworks Server.♦ Active Directory Group Policy: Select this option to use an Active Directory Group policy. To launch the group policy helper, click <i>Configure</i>. Import an Active Directory Group policy created from Windows Server 2003 or Windows Server 2008 Active Directory, then upload to the ZENworks Server. (You cannot edit an Active Directory policy through ZENworks Control Center.) <hr/> <p>NOTE: ZENworks Configuration Management SP3 supports importing an Active Directory Group policy created from Windows Server 2008 R2 Active Directory.</p>

Field	Details
<i>Select the Configuration Settings to Be Applied On the Managed Device</i>	<p>After you have adjusted the policy settings as you prefer, you can select how to apply the settings to the managed device.</p> <p>Computer Configuration Select this option to apply the computer configuration settings to the managed device.</p> <ul style="list-style-type: none"> ◆ Apply all settings: Select this option to apply all the computer configuration settings to the managed device. ◆ Apply only security settings: Select this option to apply only the security settings to the managed device. <p>However, if you select this option, the software restrictions in security settings are not enforced on the device. To enforce the software restrictions, select Apply all settings.</p> <ul style="list-style-type: none"> ◆ Apply all settings except security settings: Select this option to apply all the computer configuration settings except for security settings to the managed device. <p>User Configuration Select this option to apply the user configuration settings to the managed device.</p> <hr/> <p>NOTE:</p> <ul style="list-style-type: none"> ◆ The Computer Configuration settings from a user associated group policy are not applied when the user logs into a Windows 2000 or Windows 2003 Terminal Server. ◆ Group Policy Objects get assigned to a device on a general refresh. The Computer Configuration settings of a device-assigned Group Policy Object remains in-effect on user logout.

5 Click *Next* to display the Summary page.

6 Click *Finish* to create the policy now, or select *Define Additional Properties* to specify additional information, such as policy assignment, [system requirements](#), enforcement, status, and which group the policy is a member of.

If the login/logoff scripts are configured in a user-associated group policy and the *After enforcement, force a re-login on the managed device, if necessary* option in the *Apply Immediate* section of the *General Settings* is selected, then a relogin is forced and the login scripts run when the user logs into the managed device again. The startup scripts from a device-associated policy run only when the device reboots the next time.

The logoff scripts configured in the group policy does not run on Windows Server 2000, Windows Server 2003, and Windows Server 2008.

The Group policy login scripts do not support the environment variables for users on Windows Vista, Windows Server 2003, Windows Server 2008, Windows 7, and Windows Server 2008 R2.

The scripts configured through Active Directory group policy are not enforced on the device even though the policy displays success in the ZENworks Adaptive Agent Policies page. For more information see, [Section A.14, “Windows Group Policy Troubleshooting,” on page 89.](#)

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

2.9 ZENworks Explorer Configuration Policy

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

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

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

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

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

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

Field	Details
<i>Enable Folder View</i>	Use this option to display a folder list in the application window. The values are <i>Yes</i> , <i>No</i> , and <i>Unconfigured</i> . If you select the value as <i>Unconfigured</i> , the default value <i>Yes</i> is set on the managed device.
<i>Expand the Entire Folder Tree</i>	Use this option to expand the entire folder tree when the application window is opened. The values are <i>Yes</i> , <i>No</i> , and <i>Unconfigured</i> . If you select the value as <i>Unconfigured</i> , the default value <i>No</i> is set on the managed device.
<i>Display Applications in Windows Explorer</i>	Use this option to display the application list in Windows Explorer. The values are <i>Yes</i> , <i>No</i> , and <i>Unconfigured</i> . If you select the value as <i>Unconfigured</i> , the default value <i>Yes</i> is set on the managed device.
<i>Name of Root Folder</i>	Use this option to change the name of the root folder.
Hide the Zicon in the taskbar	Use this option to hide the ZENworks icon in the taskbar. The values are <i>Yes</i> , <i>No</i> , and <i>Unconfigured</i> . If you select the value as <i>Unconfigured</i> , the default value <i>No</i> is set on the managed device.

Field	Details
<i>Enable Manual Refresh</i>	<p>Use this option to specify whether manual refresh of applications is enabled after starting ZENworks Explorer.</p> <p>The values are <i>Yes</i>, <i>No</i>, and <i>Unconfigured</i>. If you select the value as <i>Unconfigured</i>, the default value <i>Yes</i> is set on the managed device.</p>
<i>Allow Logout / Login as a New User</i>	<p>Use this option to enable the user to log out and log in as a new user.</p> <p>The values are <i>Yes</i>, <i>No</i>, and <i>Unconfigured</i>. If you select the value as <i>Unconfigured</i>, the default value <i>Yes</i> is set on the managed device.</p>
<i>Show Progress</i>	<p>Use this option to specify whether the progress of the bundle operations should be displayed.</p> <p>The values are <i>Yes</i>, <i>No</i>, and <i>Unconfigured</i>. If you select the value as <i>Unconfigured</i>, the default value <i>Yes</i> is set on the managed device.</p>
<i>Show Default Notifications</i>	<p>Use this option to specify whether the default notification should be displayed. The notification is displayed when the content associated with a policy or a bundle is downloaded on the device. For example, during the enforcement of the Printer policy on a device, the following message is displayed in the notification area of the device:</p> <p>Downloading Files for Printer Policy</p> <p>The values are <i>Yes</i>, <i>No</i>, and <i>Unconfigured</i>. If you select the value as <i>Unconfigured</i>, the default value <i>Yes</i> is set on the managed device.</p>
<i>Start the ZENworks Explorer with the {All} Folder Displayed</i>	<p>Use this option to specify whether the [All] folder should be displayed when ZENworks Explorer starts.</p> <p>The values are <i>Yes</i>, <i>No</i>, and <i>Unconfigured</i>. If you select the value as <i>Unconfigured</i>, the default value <i>Yes</i> is set on the managed device.</p>

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

2.10 Creating Policies by Using the zman Command Line Utility

ZENworks Configuration Management allows you to create different types of policies, such as Browser Bookmarks policy, Dynamic Local User policy, Local File Rights policy, and Printer policy. Each policy has its own set of data and configuration settings. Because it is complex to pass the data as arguments in the command line, the zman utility takes XML files as an input to create policies. You can use exported XML files as a templates to create polices. To use the zman command line utility to create a policy, you must have a policy of the same type already created through ZENworks Control Center and export it to an XML file. For more information on creating policies by using ZENworks Control Center, see [Chapter 2, “Creating Policies,” on page 15](#).

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

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

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

- ♦ [Section 2.10.1, “Creating a Policy without Content,” on page 35](#)
- ♦ [Section 2.10.2, “Creating a Policy with Content,” on page 37](#)
- ♦ [Section 2.10.3, “Understanding the zman Policy XML File Format,” on page 38](#)

2.10.1 Creating a Policy without Content

1 Create a policy in ZENworks Control Center.

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

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

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

For example, export the google policy to google.xml by using the following command:

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

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

3 Modify the XML file according to your requirements.

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

```
<ns2:ActionSets>
  <Id>879de60b7591b6f6aefae09fcd83db54</Id>
  <Type>Enforcement</Type>
  <Version>1</Version>
  <Modified>>false</Modified>
  <Actions>
    <Id>0ab9a1785370bcd38bc862bd2817abac</Id>
    <Name>browserbookmarkspolicy</Name>
    <Type>browserbookmarkspolicy</Type>
    <Data>
      <PolicyData xmlns="http://novell.com/zenworks/datamodel/objects/policies">
        <BookmarksPolicyHandlerData xmlns="">
          <EnforcePolicy>
            <Bookmarks>
              <Bookmark Type="url_string">
                <Name>Google</Name>
                <Url>http://www.yahoo.com</Url>
                <Folder>/</Folder>
              </Bookmark>
            </Bookmarks>
          </EnforcePolicy>
        </PolicyData>
      </Data>
    </Actions>
  </ActionSets>
```

```

        </Bookmark>
    </Bookmarks>
</EnforcePolicy>
</BookmarksPolicyHandlerData>
</PolicyData>
</Data>
<ContinueOnFailure>true</ContinueOnFailure>
<Enabled>true</Enabled>
<Properties>StandaloneName=browserbookmarksenf;Impersonation=SYSTEM;</
Properties>
</Actions>
</ns2:ActionSets>
<ns2:ActionSets xmlns:ns2="http://novell.com/zenworks/datamodel/objects/
actions" xmlns="http://novell.com/zenworks/datamodel/objects/actions">
    <Id>4efa37c827cf0e8a8ac20b23a3022227</Id>
    <Type>Distribution</Type>
    <Version>1</Version>
    <Modified>>false</Modified>
    <Actions>
        <Id>27c4a42544210b3ac3b067ff6aff2d5c</Id>
        <Name>Distribute Action</Name>
        <Type>Distribute Action</Type>
        <ContinueOnFailure>true</ContinueOnFailure>
        <Enabled>true</Enabled>
        <Properties />
    </Actions>
</ns2:ActionSets>
<ApplyImmediate>>false</ApplyImmediate>
<PolicyData>
    <BookmarksPolicyHandlerData>
        <EnforcePolicy>
            <Bookmarks>
                <Bookmark Type="url_string">
                    <Name>Google</Name>
                    <Url>http://www.yahoo.com</Url>
                    <Folder></Folder>
                </Bookmark>
            </Bookmarks>
        </EnforcePolicy>
    </BookmarksPolicyHandlerData>
</PolicyData>

```

4 Create a new policy by using the following command:

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

For example, to create the yahoo policy, use the following command:

```
zman policy-create yahoo google.xml
```

2.10.2 Creating a Policy with Content

- 1 Create a policy in ZENworks Control Center.

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

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

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

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

For example, export iPrintPolicy to `iPrintPolicy.xml` by using the following command:

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

The `iPrintPolicy.xml` and `iPrintPolicy_ActionContentInfo.xml` files are created. For more information about `ActionContentInfo.xml`, see [Section 2.10.3, “Understanding the zman Policy XML File Format,”](#) on page 38.

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

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

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

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

A sample `iPrintPolicy_actioncontentinfo.xml` is shown below.

```
<ActionInformation>
  <ActionSet type="Enforcement">
    <Action name="printer policy" index="1">
      <Content>
        <ContentFilePath>driver.zip</ContentFilePath>
      </Content>
    </Action>
  </ActionSet>
</ActionInformation>
```

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

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

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

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

2.10.3 Understanding the zman Policy XML File Format

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

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

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

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

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

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

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

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

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

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

- ◆ If you want to modify the `<Data>` element of actions in the exported XML file, ensure that the new data is correct and that it conforms to the schema. The `zman` utility does a minimal validation of the data and does not check for the errors. Hence, the policy might be successfully created, but with invalid data. Such a policy fails when deployed on a managed device.

- ◆ File content is associated with a particular action in an Action Set. The Action Content Information XML file should contain the path of the file to which the file content is to be associated and the index of the action in the Action Set.

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

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

```
<ActionInformaion>
  <ActionSet type="Enforcement">
    <Action name="printer policy" index="1">
      <Content>
        <ContentFilePath>driver1.zip</ContentFilePath>
      </Content>
      <Content>
        <ContentFilePath>driver2.zip</ContentFilePath>
      </Content>
    </Action>
  </ActionSet>
</ActionInformation>
```


Managing Policies

3

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

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

- ◆ [Section 3.1, “Policy Groups,” on page 41](#)
- ◆ [Section 3.2, “Editing Policies,” on page 42](#)
- ◆ [Section 3.3, “Deleting Policies,” on page 43](#)
- ◆ [Section 3.4, “Adding Policies to Groups,” on page 43](#)
- ◆ [Section 3.5, “Assigning a Policy to Devices,” on page 44](#)
- ◆ [Section 3.6, “Assigning a Policy to Users,” on page 46](#)
- ◆ [Section 3.7, “Assigning a Roaming Profile Policy that has the User Profile Stored on a Windows, Linux or NetWare Share,” on page 47](#)
- ◆ [Section 3.8, “Assigning a Roaming Profile Policy that has the User Profile Stored on a Home Directory,” on page 49](#)
- ◆ [Section 3.9, “Assigning the Local File Rights Policy to Devices Running Different Languages,” on page 50](#)
- ◆ [Section 3.10, “Unassigning a Policy from Devices,” on page 50](#)
- ◆ [Section 3.11, “Unassigning a Policy from Users,” on page 51](#)
- ◆ [Section 3.12, “Adding System Requirements for a Policy,” on page 51](#)
- ◆ [Section 3.13, “Disabling Policies,” on page 56](#)
- ◆ [Section 3.14, “Enabling the Disabled Policies,” on page 56](#)
- ◆ [Section 3.15, “Copying a Policy to a Content Server,” on page 56](#)
- ◆ [Section 3.16, “Incrementing the Policy Version,” on page 58](#)
- ◆ [Section 3.17, “Reviewing the Status of the Policies at the Managed Device,” on page 59](#)
- ◆ [Section 3.18, “Policy Issues on a Windows 7, Windows Server 2008, or Windows Server 2008 R2 device,” on page 59](#)
- ◆ [Section 3.19, “Viewing the Predefined Reports,” on page 60](#)

3.1 Policy Groups

A policy group consists of two or more policies. Creating policy groups eases administration efforts by letting you assign the group, rather than each individual policy, to devices and users. You can create a policy group with a single policy and then add policies to the group as and when required.

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

2 In the *Policies* list, click *New*, click *Policy Group* to display the Basic Information page, then fill in the fields:

Group Name: Provide a unique name for your policy group. The name you provide displays in the ZENworks Control Center interface.

Folder: Type the name or browse to and select the folder that contains this policy group

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

3 Click *Next* to display the Add Group Members page. You can add any number of policies to the group. You cannot add other policy groups to the group.

To add a policy:

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

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

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

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

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

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

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

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

4 Click *Next* to display the Summary page.

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

3.2 Editing Policies

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

Task	Steps	Additional Details
Edit the content of a policy	<ol style="list-style-type: none">1. Click the policy whose content you want to edit.2. Click the <i>Details</i> tab, then edit the settings according to your requirements.3. Click <i>Apply</i>.4. Click the <i>Summary</i> page.5. Increment the version of the policy to enforce the changes made to the policy on the managed device.	

Task	Steps	Additional Details
Rename a policy	<ol style="list-style-type: none"> 1. Select the check box next to the policy. 2. Click <i>Edit > Rename</i>, then specify the new name. 	<p>If more than one check box is selected, the <i>Rename</i> option is not available in the <i>Edit</i> menu.</p> <p>If you rename a policy, ensure to increment the version of the policy to deliver it to assigned devices and users that already have this policy.</p>
Create a copy of the policy	<ol style="list-style-type: none"> 1. Select the check box next to the policy. 2. Click <i>Edit > Copy</i>, then specify a new name. 	<p>If more than one check box is selected, the <i>Copy</i> option is not available in the <i>Edit</i> menu.</p> <p>The copy option is useful to create a new policy that is similar to an existing policy. You can copy a policy and then edit the new policy's settings.</p>
Move a policy to a different folder	<ol style="list-style-type: none"> 1. Select the check box next to the policy (or policies). 2. Click <i>Edit > Move</i>, then select the target folder. 	
Copy the system requirements of one policy to another policy	<ol style="list-style-type: none"> 1. Select the check box next to the policy. 2. Click <i>Edit > Copy System Requirements</i>. 3. Select <i>Policies</i>, then click <i>Add</i> to select the policies to which you want to copy the selected policy's system requirements. 	<p>If more than one check box is selected, the <i>Copy System Requirements</i> option is not available in the <i>Edit</i> menu.</p>

3.3 Deleting Policies

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

3.4 Adding Policies to Groups

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

- 5** (Conditional) If you are adding selected items to an existing group, the Targets page is displayed. Select the groups to which you want to add the objects (users, devices, bundles, policies).

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

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

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

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

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

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

- 5b2** Click the underlined link in the *Name* column to select the policy and display its name in the *Selected* list.

- 5b3** (Optional) Repeat [Step 5a](#) and [Step 5b](#) to add additional policies to the *Selected* list.

- 5b4** Click *OK* to add the selected policies to the group.

- 5c** Click *Next* to skip to [Step 7](#).

- 6** (Conditional) If you are creating a new group to contain the selected items, the Basic Information page is displayed. Fill in the following fields, then click *Next* to continue with [Step 7](#).

Group Name: Provide a unique name for your policy group. The name you provide displays in the ZENworks Control Center interface.

Folder: Type the name or browse to and select the folder that contains this policy group

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

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

- 8** Click *Finish*.

3.5 Assigning a Policy to Devices

Certain key points that you must be aware of before you assign a policy to a device are as follows:

- ♦ If you are assigning a Local File Rights policy to a network made up of devices running different languages, see [Section 3.9, “Assigning the Local File Rights Policy to Devices Running Different Languages,”](#) on page 50.
- ♦ The Dynamic Local User policy and The Roaming Profile policy are not supported on a 64-bit Windows Server 2003 device.

Perform the following steps to assign a policy to a device:

- 1** In ZENworks Control Center, click the *Policies* tab.
- 2** In the *Policies* list, select the check box next to the objects such as policies or policy groups.
- 3** Click *Action* > *Assign to Device*.

- 4 Browse for and select the devices, device groups, and device folders to which you want to assign the group. To do so:
 - 4a Click  next to a folder (for example, the `Workstations` folder or `Servers` folder) to navigate through the folders until you find the device, group, or folder you want to select.
If you are looking for a specific item, such as a `Workstation` or a `Workstation Group`, you can use the *Items of type* list to limit the types of items that are displayed. If you know the name of the item you are looking for, you can use the *Item name* box to search for the item.
 - 4b Click the underlined link in the *Name* column to select the device, group, or folder and display its name in the *Selected* list box.
 - 4c Click *OK* to add the selected devices, folders, and groups to the *Devices* list.
- 5 Click *Next* to display the Policy Conflict Resolution page.
- 6 Set the priority between device-associated policies and user-associated policies for resolving conflicts that arise when policies of the same type are associated to both devices and users.
 - ♦ **User Last:** Select this option to apply policies that are associated to devices first and then the users.
 - ♦ **Device Last:** Select this option to apply policies that are associated to users first and then the devices.
 - ♦ **Device Only:** Select this option to apply policies that are associated only to devices.
 - ♦ **User Only:** Select this option to apply policies that are associated only to users.
- 7 Click *Next* to display the Finish page, review the information and, if necessary, use the *Back* button to make changes to the information.
If you want the policies to be immediately enforced on all the assigned devices, select *Enforce Policies Immediately on all Assigned Devices*.
- 8 Click *Finish*.

The following points are applicable when you assign a policy to a device:

- ♦ If you assign a DLU policy to a device on which a user has logged in, the user is prompted to log in to the device again. Unless the user logs in to the device again, no new policies are enforced on the device.
- ♦ When you assign a ZENworks Explorer Configuration Policy to a device, the settings configured in the policy are not immediately reflected on the device. For example, even if *Hide the Z icon in the taskbar* is enabled in the policy, the ZENworks icon is displayed for a few seconds on the device after the policy is assigned to the device.
- ♦ If both user-associated and device-associated policies are effective for a device, only the policy that takes precedence according to the Policy Conflict Resolution settings is applied on the device. However, the *Effective* status for both policies is displayed as *Success* in the ZENworks Adaptive Agent icon.
- ♦ User settings of a device associated Group policy cannot be enforced in console sessions of a Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2 device.

- ♦ On a managed device, if you launch a published application that is installed on a Citrix server having iPrint policy configured, it might take considerable time for the policy to be enforced on the server. During this period, the iPrint functionality is not available for the application.

The iPrint policy is not enforced on the device if you set the `ZENUserDaemon` and the `DisableUserDaemonHealing` registry keys on the device to enable the user configuration settings configured in the Group policy to be applied in terminal sessions of Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 devices. For more information, see the Policy Management issue in [the ZENworks 10 Configuration Management SP3 Readme \(http://www.novell.com/documentation/zcm10/\)](http://www.novell.com/documentation/zcm10/).

3.6 Assigning a Policy to Users

Certain key points that you must be aware of before you assign a policy to a user are as follows

- ♦ There are two types of users: users in the corporate directory and local users on managed devices. Policies can be associated to users in the corporate directory. ZENworks assumes that a mapping exists between users in the corporate directory and users on a device. When a user logs in to the corporate directory, ZENworks obtains the policies for the corporate user and caches them on the device.
- ♦ If a mapping exists between a corporate user and a local user, ZENworks also associates the cached policies with the local user. When a user logs in to the device, the previously cached policies are enforced for the local user. When the user also logs in to the corporate directory, the policies for the corporate user are refreshed, then enforced.
- ♦ The set of policies, both directly assigned and inherited, is called as a set of assigned policies for a device or a user. When calculating the set of assigned policies, filters such as multiplicity or system requirements are not applied. Groups and containers also have assigned policies. Policies that are disabled are not included in the set of assigned policies.
- ♦ If you are assigning a Local File Rights policy to a network made up of devices running different languages, see [Section 3.9, “Assigning the Local File Rights Policy to Devices Running Different Languages,”](#) on page 50.
- ♦ Before assigning a Roaming Profile policy to a user on a Windows Vista device or Windows Server 2008 device, make sure a user profile with correct registry hive permissions is available on the device. See [Section 3.7, “Assigning a Roaming Profile Policy that has the User Profile Stored on a Windows, Linux or NetWare Share,”](#) on page 47.

Perform the following steps to assign a policy to a user:

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

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

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

The following points are applicable when you assign a policy to a user:

- ♦ When you assign a ZENworks Explorer Configuration Policy to a user, the settings configured in the policy are not immediately reflected on the device on which the user logs on. For example, even if *Hide the Z icon in the taskbar* is enabled in the policy, the ZENworks icon is displayed for a few seconds on the device after the policy is assigned to the user.
- ♦ User assigned policies are not enforced in the console sessions of Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 device.
- ♦ If you launch a published application from a Citrix server on to the device, it might take some considerable time for the list of the iPrint printers to be displayed on the device.
- ♦ If you launch a published application installed on a Citrix server that has iPrint printer policy configured, it might take some considerable time for the policy to be enforced on the server. During this period, the iPrint functionality is not available for the application.

3.7 Assigning a Roaming Profile Policy that has the User Profile Stored on a Windows, Linux or NetWare Share

If a Roaming Profile policy is assigned to a user on a Windows Vista, Windows 2008 or a Windows 7 device, the policy fails if the user profile is stored on a shared location. This is because the registry hive of the user profile does not have permissions to load the profile to other devices. For more information, see the [Microsoft TechNet Web site \(http://technet.microsoft.com/en-us/library/cc766489.aspx\)](http://technet.microsoft.com/en-us/library/cc766489.aspx).

If a default profile already exists in a shared location, start with [Step 3](#). If you do not yet have a default profile, start with [Step 1](#).

Before assigning a roaming profile policy to users on a Windows Vista, Windows 2008 or a Windows 7 device, do the following:

- 1** Create a default profile folder in a shared location.
For information on creating the default profile folder, see [Section 3.7.1, “Creating a Default Profile Folder in a Shared Location,”](#) on page 48.
- 2** Copy the default profile from a Windows Vista, Windows 2008 or a Windows 7 device to the default profile folder in the shared location.
For information on copying the default profile to the shared location, see [Section 3.7.2, “Copying the Default Profile from a Windows Vista, Windows 2008 or a Windows 7 device to the Default Profile Folder in the Shared Location,”](#) on page 48.
- 3** Configure the registry hive permissions for the default profile.
For information on configuring the registry hive permissions, see [Section 3.7.3, “Configuring the Permissions for the Default Profile Registry Hive,”](#) on page 48.

3.7.1 Creating a Default Profile Folder in a Shared Location

Create a default profile folder in a shared location depending on where you want to store the user profile. For example:

- ♦ **User Profile Path:** \\DNS_name_of_file_server\profiles\DefaultProfile.V2

3.7.2 Copying the Default Profile from a Windows Vista, Windows 2008 or a Windows 7 device to the Default Profile Folder in the Shared Location

Ensure that the user profile you want to copy as a default profile already exists on the device. If the desired profile is not available, create a new user account and then log in to the device with the new account credentials to create the profile.

Perform the following steps to copy the default profile to the default profile folder in the shared location:

- 1 Log in to the device as an administrator.
- 2 Right-click *Computer*, click *Properties* > *Advanced system settings*.
- 3 In the User Profiles section, click *Settings*.
- 4 Select a profile on the device to store as a default profile.
- 5 Click *Copy To*.
- 6 Browse to and select the default profile folder you created in [Section 3.7.1, “Creating a Default Profile Folder in a Shared Location,”](#) on page 48.
- 7 Click *Change* in the Permitted to Use section.
- 8 Specify *Everyone* in the *Enter the object name to select* option to provide permissions, then click *OK*.
- 9 Click *OK* to copy the profile to the shared location, then click *OK*.
- 10 Click *OK*.

3.7.3 Configuring the Permissions for the Default Profile Registry Hive

- 1 To open the Registry Editor when the shared location is on a Windows device, run `regedit`.
or
To open the Registry Editor when the shared location is on a Linux or NetWare device, map the location from a Windows device, and then open the Registry Editor on the Windows device.
- 2 Select `HKEY_USERS`, then click *File* > *Load Hive*.
- 3 Open the `NTUSER.DAT` file from the default profile folder created in [Section 3.7.1, “Creating a Default Profile Folder in a Shared Location,”](#) on page 48.

The `NTUSER.DAT` file might be hidden. To unhide the file:

1. Open the default profile folder in Windows Explorer.
2. Click *Tools* > *Folder Options* > *View*
3. Deselect *Hide protected operating system files*.

- 4 In the Load Hive dialog box, specify the *Key Name* for the hive. For example, Vista.
- 5 Right-click the *Vista* hive, then click *Permissions*.
- 6 Ensure that the following groups or usernames have Full Control permissions:
 - ♦ Administrators
 - ♦ SYSTEM
 - ♦ Users
- 7 Click *Advanced*.
- 8 Select the *Replace permission entries on all child objects with entries shown here that apply to child objects* option and click *OK*, then click *Yes*.
- 9 Click *OK*.
- 10 Ensure to unload the hive. To unload the hive, select the *Vista* registry hive that you created, then click *File > Unload Hive*.

3.7.4 Copying the Default Profile to User Folders

Ensure that you copy the default profile to the user folders before assigning the Roaming Profile policy to the users. Depending on the user profiles stored, these user folders are:

- ♦ **User Profile Path:** `\\DNS_name_of_file_server\profiles\Username.V2`

3.8 Assigning a Roaming Profile Policy that has the User Profile Stored on a Home Directory

If a Roaming Profile policy is assigned to a user, the policy fails if the user profile is stored on Linux or NetWare Home Directory. This is because the registry hive of the user profile does not have permissions to load the profile to other devices. If a default profile already exists at a shared location, you need to configure the permissions for the default profile registry hive.

For more information, see TID 7007207 in the [Novell Support Knowledgebase \(http://www.novell.com/support/search.do?usemicrosite=true&searchString=7007207\)](http://www.novell.com/support/search.do?usemicrosite=true&searchString=7007207).

To Configure the Permissions for the Default Profile Registry Hive

- 1 At the shared location, run `regedit` to open the Registry Editor.
If the shared location is on a Netware or Linux device, map the location from a Windows device and open the Registry Editor on the Windows device.
- 2 Select `HKEY_USERS`, then click *File > Load Hive*.
- 3 Open the `NTUSER.DAT` file from the default profile folder.
The `NTUSER.DAT` file might be hidden. To unhide the file:
 1. Open the default profile folder in Windows Explorer.
 2. Click *Tools > Folder Options > View*
 3. Deselect *Hide protected operating system files*.
- 4 In the Load Hive dialog box, specify the *Key Name* for the hive. For example, Vista.
- 5 Right-click the *Vista* hive, then click *Permissions*.

- 6 Ensure that the following groups or usernames have Full Control permissions:
 - ♦ Administrators
 - ♦ SYSTEM
 - ♦ Users
- 7 Click *Advanced*.
- 8 Select the *Replace permission entries on all child objects with entries shown here that apply to child objects* option and click *OK*, then click *Yes*.
- 9 Click *OK*.
- 10 Ensure to unload the hive. To unload the hive, select the *Vista* registry hive that you created, then click *File > Unload Hive*.

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

- 1 Create a separate Local File Rights policy for each language. For more information on creating the policy, see [Section 2.3, “Local File Rights Policy,” on page 21](#).
- 2 Add a filter for each policy:
 - 2a Click the policy, then click *Requirements*.
 - 2b Click *Add Filter*, select the *Registry Key Value* condition, then specify the following:

Key:

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

Value: language.dll

Comparator: = (String Type)

Value Data: *language*

For example, on a device with the English language, *language* is *English (American)*. You can use the registry editor to determine the value data of the language.
 - 2c Click *Apply*.
- 3 Assign the policy to the device. For more information on assigning a policy to a device, see [Section 3.5, “Assigning a Policy to Devices,” on page 44](#).
or
Assign the policy to the user. For more information on assigning a policy to a user, see [Section 3.6, “Assigning a Policy to Users,” on page 46](#).

3.10 Unassigning a Policy from Devices

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 In the *Policies* list, click the policy you want to unassign.
- 3 Click *Relationships*.
- 4 In the Device Assignments panel, select the devices from which you want to unassign the policy.

- 5 Click *Remove*.

On a Windows Server 2008 device, the Group policy user settings associated to a user are not unenforced when the user logs out.

3.11 Unassigning a Policy from Users

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 In the *Policies* list, click the policy you want to unassign.
- 3 Click *Relationships*.
- 4 In the User Assignments panel, select the users from whom you want to unassign the policy.
- 5 Click *Remove*.

When you unassign a printer policy that is assigned to a user, the printer permissions for the user are removed from the device. However, the printer continues to be configured on the device.

3.12 Adding System Requirements for a Policy

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

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

To create system requirements for a policy:

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 Click the underlined link for the desired policy to display the policy's Summary page.
- 3 Click the *Requirements* tab.
- 4 Click *Add Filter*, select a filter condition from the drop-down list, then fill in the fields.

As you construct filters, you need to know the conditions you can use and how to organize the filters to achieve the desired results. For more information, see [Section 3.12.1, "Filter Conditions,"](#) on page 51 and [Section 3.12.2, "Filter Logic,"](#) on page 55.

- 5 (Conditional) Add additional filters and filter sets.
- 6 Click *Apply* to save the settings.

3.12.1 Filter Conditions

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

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

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

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

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

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

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

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

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

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

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

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

File Version: Determines the version of a file. The condition you use to set the requirement includes the filename, an operator, and a version. The filename can be any file name supported by the operating system. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=).

Be aware that file version numbers contain four components: Major, Minor, Revision, and Build. For example, the file version for `calc.exe` might be 5.1.2600.0. Each component is treated independently. For this reason, the system requirements that you set might not provide your expected results. If you do not specify all four components, wildcards are assumed.

For example, if you set the condition to `calc.exe <= 5`, you are specifying only the first component of the version number (Major). As a result, versions 5.0.5, 5.1, and 5.1.1.1 also meet the condition.

However, because each component is independent, if you set the condition to `calc.exe <= 5.1`, the `calc.exe` file must be less than or equal to version 5.1 to meet the requirement.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.12.2 Filter Logic

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

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

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

Filters, Filter Sets, and Logical Operators

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

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

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

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

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

Nested Filters and Filter Sets

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

3.13 Disabling Policies

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

To disable a policy:

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

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

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

3.14 Enabling the Disabled Policies

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

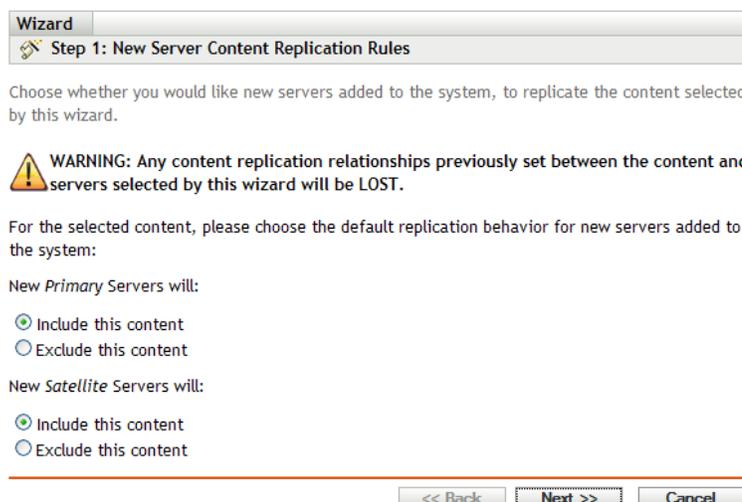
In the Policies list, the status of the *Enabled* column for the policy (or policies) is changed to *Yes*.

3.15 Copying a Policy to a Content Server

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

To specify a content server:

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



4 Specify the default replication behavior for new servers added to the system:

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

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

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

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

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

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

Excluded Primary Servers
 /Devices/Servers/krobinson2
 /Devices/Servers/Primary Server 1
 /Devices/Servers/Primary Server 2

Included Primary Servers

Excluded Satellite Servers
 /Devices/Servers/Satellite Server 1
 /Devices/Servers/Satellite Server 2
 /Devices/Servers/DP 1
 /Devices/Servers/DP 2

Included Satellite Servers

<< Back Next >> Cancel

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

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

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

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

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

5b Click the button to move the selected content server to the *Included Primary Servers* or *Included Satellite Servers* list.

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

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

3.16 Incrementing the Policy Version

The policy version number should be incremented whenever the policy is updated. This ensures that the latest policy is enforced on the managed device.

3.16.1 Using the Action Menu

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

- 2 Select the check box next to the policy (or policies) for which you want to increment the version.
- 3 Click *Action > Increment Version*.
- 4 In the Confirm Version Increment dialog box, click *Yes*.

3.16.2 Editing the Policy

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 In the *Policies* list, click a Policy's underlined link in the *Name* column to display its Summary page.
- 3 Click *Increment Version*.
- 4 In the Confirm Version Increment dialog box, click *Yes*.

3.17 Reviewing the Status of the Policies at the Managed Device

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

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

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

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

To view the policies assigned to you and your device:

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

3.18 Policy Issues on a Windows 7, Windows Server 2008, or Windows Server 2008 R2 device

- ♦ Roaming Profile policy with the home directory option is not enforced in a terminal session of a Windows Server 2008 or Windows Server 2008 R2 device if you have launched the terminal session from a Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device. This is because the Novell Client login dialog box is not displayed on the device and only the Remote Desktop login is performed on the device.

To display the Novell Client login dialog box, do the following:

1. Open the registry editor.
 2. Go to HKEY_LOCAL_MACHINE\SOFTWARE\Novell\Login.
 3. Create a string called TSCClientAutoAdminLogon, and set its value to 1.
 4. Create a string called DefaultLoginProfile, and set its value to Default.
 5. Close the registry editor.
 6. From a Windows Vista or Windows 7 device, launch a Remote Desktop session to the Windows Server 2008 R2 device and specify the Windows user credentials.
 7. A Novell Client window is displayed. Click *Cancel*.
 8. In the next screen, click *Novell Logon* to display the Novell Client login dialog box.
- ♦ Dynamic Local User Profile policy is not enforced in a terminal session of a Windows Server 2008 or Windows Server 2008 R2 device if you have launched the terminal session from a Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device. This is because Novell Client login dialog box is not displayed on the device and only the Remote Desktop login is performed on the device.

For information on resolving this issue, search for the Using Dynamic Local User Policy in Windows Server 2008 R2 Remote Desktop Session Host article at the [ZENworks Cool Solutions Community \(http://www.novell.com/communities/cool solutions/zenworks\)](http://www.novell.com/communities/cool solutions/zenworks)

- ♦ If a Roaming Profile user logs in to a Windows Server 2008 or Windows Server 2008 R2 device and then logs out, the user cannot log in to a Windows 7 device or to other Windows Server 2008 or Windows Server 2008 R2 devices.
- ♦ A Roaming Profile policy cannot be enforced on a Windows 7, Windows Server 2008, or Windows Server 2008 R2 device if the user profile is stored on a Windows Server 2003 shared location. For more information, see the troubleshooting scenario “Unable to enforce a Roaming Profile policy on a Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device if the user profile is stored in a shared folder on a Windows Server 2003 device” on page 85.

3.19 Viewing the Predefined Reports

You must have installed ZENworks Reporting Server to view the Predefined reports. For more information on how to install ZENworks Reporting Server, see [ZENworks 10 Configuration Asset Management Reporting Server Installation Guide](#)

To view the Predefined reports for Policies, do the following:

- 1 In the ZENworks Control Center, click *Reports*.
- 2 In the ZENworks Reporting Server Reporting panel, click *ZENworks Reporting Server InfoView* to launch the ZENworks Reporting Server InfoView.
- 3 Navigate to the *Novell ZENworks Reports* folder > *Predefined Reports* > *Bundles and Policies* folder.
- 4 The following Predefined reports are included for Policies:
 - ♦ **Assigned Bundles and Policies by Device:** Displays information on all the policies that are assigned to a particular device.
 - ♦ **Content By Server:** Displays the content information for the selected server. The information includes the content name, content type, replication state, and the disk space.

- ♦ **Content By Bundle and Policy:** Displays the content information for the bundles and policies. This information includes the content server, content type, replication state, and disk space.

For more information on creating and managing reports, see the [ZENworks 10 Configuration Management Asset Management System Reporting Reference](#) documentation.

Managing Policy Groups

4

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

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

- ♦ [Section 4.1, “Creating Policy Groups,”](#) on page 63
- ♦ [Section 4.2, “Renaming or Moving Policy Groups,”](#) on page 64
- ♦ [Section 4.3, “Deleting a Policy Group,”](#) on page 64
- ♦ [Section 4.4, “Assigning a Policy Group to Devices,”](#) on page 65
- ♦ [Section 4.5, “Assigning a Policy Group to Users,”](#) on page 65
- ♦ [Section 4.6, “Adding a Policy to a Group,”](#) on page 66

4.1 Creating Policy Groups

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

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

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

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

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

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

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

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

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

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

- 4b** Browse for and select the policies you want to add to the group. To do so:
- 4b1** Click  next to a folder to navigate the folders until you find the policy you want to select.
If you know the name of the policy you are looking for, you can also use the *Item name* box to search for the bundle.
 - 4b2** Click the underlined link in the *Name* column to select the policy and display its name in the *Selected* list.
 - 4b3** (Optional) Repeat [Step 4a](#) and [Step 4b](#) to add additional policies to the *Selected* list.
 - 4b4** Click *OK* to add the selected policies to the group.
- 5** Click *Next* to display the Summary page, review the information and, if necessary, use the *Back* button to make changes to the information.
- 6** (Optional) Select the *Define Additional Properties* option to display the group's properties page after the group is created. You can then configure additional policy properties.
- 7** Click *Finish* to create the group.

Before the bundle group's contents are distributed to devices or users, you must continue with [Section 3.5, "Assigning a Policy to Devices," on page 44](#) or [Section 3.6, "Assigning a Policy to Users," on page 46](#).

4.2 Renaming or Moving Policy Groups

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

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

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

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

4.3 Deleting a Policy Group

Deleting a policy group does not delete its policies. It also does not unenforce the policies from devices where they have already been enforced. To unenforce the policy from devices, remove the assignment of each policy from the devices or users before deleting the policy group.

For information on unassigning policy from a user, see [Section 3.11, "Unassigning a Policy from Users," on page 51](#).

For information on unassigning policy from a device, see [Section 3.10, "Unassigning a Policy from Devices," on page 50](#).

To delete the policy group:

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

4.4 Assigning a Policy Group to Devices

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

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

4.5 Assigning a Policy Group to Users

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

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

4.6 Adding a Policy to a Group

For more information, see [Section 3.4, “Adding Policies to Groups,”](#) on page 43.

Managing Folders

5

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

The following sections contain additional information:

- ♦ [Section 5.1, “Creating Folders,” on page 67](#)
- ♦ [Section 5.2, “Renaming or Moving Folders,” on page 67](#)
- ♦ [Section 5.3, “Deleting a Folder,” on page 68](#)

5.1 Creating Folders

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

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

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

5.2 Renaming or Moving Folders

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

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

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

- 1 In ZENworks Control Center, click the *Policies* tab.
- 2 In the *Policies* list, select the box next to the folder's name, then click *Edit*.
- 3 Select an option:
 - ♦ **Rename:** Click *Rename*, provide a new name for the folder, then click *OK*.

- ♦ **Move:** Click *Move*, choose a destination folder for the selected objects, then click *OK*.

5.3 Deleting a Folder

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

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

Troubleshooting Policy Management

A

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

- ◆ Section A.1, “Browser Bookmarks Policy Errors,” on page 69
- ◆ Section A.2, “Browser Bookmarks Policy Troubleshooting,” on page 70
- ◆ Section A.3, “Dynamic Local User Policy Errors,” on page 71
- ◆ Section A.4, “Dynamic Local User Policy Troubleshooting,” on page 72
- ◆ Section A.5, “General Policy Troubleshooting,” on page 74
- ◆ Section A.6, “Local File Rights Policy Errors,” on page 76
- ◆ Section A.7, “Local File Rights Policy Troubleshooting,” on page 77
- ◆ Section A.8, “Printer Policy Errors,” on page 78
- ◆ Section A.9, “Printer Policy Troubleshooting,” on page 80
- ◆ Section A.10, “Roaming Profile Policy Errors,” on page 85
- ◆ Section A.11, “Roaming Profile Policy Troubleshooting,” on page 85
- ◆ Section A.12, “SNMP Policy Errors,” on page 86
- ◆ Section A.13, “Windows Group Policy Errors,” on page 86
- ◆ Section A.14, “Windows Group Policy Troubleshooting,” on page 89
- ◆ Section A.15, “ZENworks Explorer Configuration Policy Errors,” on page 95

A.1 Browser Bookmarks Policy Errors

- ◆ “The folder cannot be created to add bookmark as Internet Explorer does not allow such folder” on page 69
- ◆ “The bookmark cannot be created as the bookmark name is not proper. Internet Explorer does not allow such bookmarks” on page 70
- ◆ “Unable to apply the Browser Bookmark Policy. For more information, see the ZENworks error message online documentation at <http://www.novell.com/documentation>” on page 70
- ◆ “On a managed device, empty folders cannot be created in a user’s favorites folder” on page 70
- ◆ “The Browser Bookmarks policy fails on a Windows Vista managed device” on page 70

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

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

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

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

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

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

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

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

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

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

Action: Ensure that the Browser Bookmark policy has been correctly created. For more information, see [Section 2.1, “Browser Bookmarks Policy,” on page 15](#).

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

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

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

Action: None.

The Browser Bookmarks policy fails on a Windows Vista managed device

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

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

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

Action: Refresh the managed device.

A.2 Browser Bookmarks Policy Troubleshooting

- ♦ [“The Browser Bookmarks policy settings are not removed from the user’s Favorites when the ZENworks Adaptive Agent is uninstalled” on page 71](#)
- ♦ [“The bookmark file exported in .json file format is not yet supported” on page 71](#)

The Browser Bookmarks policy settings are not removed from the user's Favorites when the ZENworks Adaptive Agent is uninstalled

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

Explanation: If a Browser Bookmarks policy is assigned to a user or the managed device, the Browser Bookmarks policy settings are not removed from the user's Favorites when the ZENworks Adaptive Agent is uninstalled.

Action: To remove the Browser Bookmarks policy settings from the user's Favorite, unassign the policy from the device or the user and refresh the managed device before uninstalling the ZENworks Adaptive Agent.

The bookmark file exported in .json file format is not yet supported

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

Explanation: On Mozilla Firefox 3.0 or above, if you click *Bookmarks > Organize Bookmarks > Import and Backup > Backup* to export the bookmarks, the bookmarks are exported to a .json file. However, the .json file format is not yet supported in ZENworks.

Action: Export the bookmarks to a html file. Click *Bookmarks > Organize Bookmarks > Import and Backup > Export HTML* to export the bookmarks.

A.3 Dynamic Local User Policy Errors

- ♦ [“The policy policy_name was failed in include/exclude list calculation” on page 71](#)
- ♦ [“There was an error while applying settings for the group group_name” on page 71](#)
- ♦ [“There was an error while applying settings for the file filename” on page 72](#)
- ♦ [“Unable to enforce the policy_name policy because the policy data is empty” on page 72](#)

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

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

Explanation: This error occurs if the Include/Excluded workstation or the user list is configured, and the workstation or user did not qualify.

Action: Remove the user or device from the Excluded list configured in the policy and increment the version of the policy to enforce the policy updates to the managed device.

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

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

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the “[Message Logging](#)” in *ZENworks 10 Configuration Asset Management System Administration Reference*.

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

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

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

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the “[Message Logging](#)” in *ZENworks 10 Configuration Asset Management System Administration Reference*.

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

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

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

Possible Cause: The ZENworks Adaptive Agent did not receive any data to be configured on the managed device.

Action: Review the policy content in ZENworks Control Center. For more information about the Dynamic Local User Policy, see [Section 2.2, “Dynamic Local User Policy,”](#) on page 16.

A.4 Dynamic Local User Policy Troubleshooting

- ♦ [“Unable to update the group membership of the user on the managed device”](#) on page 72
- ♦ [“Dynamic Local User is unable to log on to the managed device”](#) on page 73
- ♦ [“Subsequent to the first login, the DLU user is prompted to provide the credentials when he or she tries to log into the device again during the cache period specified in the policy”](#) on page 73
- ♦ [“After logging out of a managed device that is disconnected from the network, a Dynamic Local User is unable to log in to the device again”](#) on page 73
- ♦ [“The DLU policy does not delete user profiles if the Roaming Profile policy is applied”](#) on page 74

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

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

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

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

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

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

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

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

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

Action: Do one of the following:

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

Subsequent to the first login, the DLU user is prompted to provide the credentials when he or she tries to log into the device again during the cache period specified in the policy

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

Explanation: If the *Use the credential specified below* and *Enable Volatile User cache* settings are configured in the Dynamic Local User policy, then subsequent to the first login, the DLU user is prompted to provide the credentials when he or she tries to log into the device again during the cache period specified in the policy.

Action: To enable the user to log into the device without being prompted on subsequent logins, ensure that the *Manage existing user account* option is enabled in the policy. This ensures that the ZENworks Agent manages the password on behalf of the user.

After logging out of a managed device that is disconnected from the network, a Dynamic Local User is unable to log in to the device again

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

Explanation: If a Dynamic Local User policy that has *Use the credential specified below*, *Manage existing user account*, and *Enable Volatile User Cache* options enabled is assigned to a device and a user logs out of the device when the device is disconnected from the network, the user is unable to log in to the disconnected device again.

Action: Before the policy is assigned to the device or the device is disconnected from the network, perform the following steps on the managed device to use the user source password for logging in to the device:

- 1 Open the Registry Editor.
- 2 Go to \HKLM\SOFTWARE\Novell\NWGINA\Dynamic Local User\.
- 3 Create a DWORD called `EnableEDirPasswordForFA`, and set the value to 1.

The DLU policy does not delete user profiles if the Roaming Profile policy is applied

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

Explanation: User profiles created with a volatile DLU (Dynamic Local User) that has a Roaming Profile policy in effect are sometimes not deleted on user logoff.

Action: Set the `DeleteRoamingCache` registry key value. For details on setting the key value, see the [Microsoft Support Web site \(http://technet.microsoft.com/en-us/library/cc957394.aspx\)](http://technet.microsoft.com/en-us/library/cc957394.aspx).

For more information, see TID 7006386 in the [Novell Support Knowledgebase \(http://www.novell.com/support/search.do?usemicrosite=true&searchString=7006386\)](http://www.novell.com/support/search.do?usemicrosite=true&searchString=7006386).

A.5 General Policy Troubleshooting

- ♦ “The user is prompted to log in again immediately after logging in to ZENworks by using ZENworks icon” on page 74
- ♦ “Unable to view the newly added user source in all the other concurrent sessions of ZENworks Control Center” on page 75
- ♦ “The Wake-on-LAN policy is not available in ZENworks Configuration Management” on page 75
- ♦ “The `zman pvst` command might not display the correct status of the policy assignment and deployment on a managed device” on page 75
- ♦ “The enforcement of policies such as DLU policy, Roaming Profile policy, or Group Policy fails on the managed device” on page 76
- ♦ “Closing a published application or logging out of the shared desktop of a Citrix server fails to terminate the session on the Citrix server” on page 76

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

Source: ZENworks 10 Configuration Management; Policy Management.

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

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

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

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

Source: ZENworks 10 Configuration Management; Policy Management.

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

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

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

Source: ZENworks 10 Configuration Management; Policy Management.

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

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

The zman pvst command might not display the correct status of the policy assignment and deployment on a managed device

Source: ZENworks 10 Configuration Management; Policy Management.

Explanation: If you assign a policy to a user or device and run the `zman pvst` command on the device, the assignment status and the overall deployment status of the policy might not be displayed correctly.

Action: Refresh the device.

The enforcement of policies such as DLU policy, Roaming Profile policy, or Group Policy fails on the managed device

Source: ZENworks 10 Configuration Management; Policy Management.

Possible Cause: If a user logs into a managed device by authenticating with a eDirectory user account that has trailing space characters, policies such as DLU policy, Roaming Profile policy, or Group Policy are not enforced on the managed device.

Action: Ensure that the eDirectory user account does not have trailing space characters.

Closing a published application or logging out of the shared desktop of a Citrix server fails to terminate the session on the Citrix server

Source: ZENworks 10 Configuration Management; Policy Management.

Explanation: Even after closing a published application or logging out of the shared desktop of a Citrix server, a user remains logged in to ZENworks. Consequently, some of the policies might not be unenforced on the device.

Action: Perform the following steps on the device:

- 1 Open the Registry Editor.
- 2 Go to
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI.
- 3 Change the value of LogoffCheckSysModules from ZCMUMHelper.exe to ZenUserDaemon.exe, ZCMUMHelper.exe
- 4 Reboot the device.

A.6 Local File Rights Policy Errors

- ♦ [“The file/folder filename or folder_name was not found while enforcing policy policy_name” on page 76](#)
- ♦ [“There was an error while unenforcing the policy” on page 77](#)
- ♦ [“There was an error while applying the policy policy_name” on page 77](#)

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

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

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

Action: On the managed device, do the following:

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

There was an error while unenforcing the policy

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

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the “[Message Logging](#)” in [ZENworks 10 Configuration Asset Management System Administration Reference](#).

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

There was an error while applying the policy *policy_name*

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

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the “[Message Logging](#)” in [ZENworks 10 Configuration Asset Management System Administration Reference](#).

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

A.7 Local File Rights Policy Troubleshooting

- ♦ “[The user permissions configured in the Local File Rights policy are not effective on the device](#)” on page 77

The user permissions configured in the Local File Rights policy are not effective on the device

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

Possible Cause: The user permissions configured in the Local File Rights policy might conflict with the user permissions configured in the Dynamic Local User policy. The permissions configured for the user or group in the Dynamic Local User policy take precedence over the permissions configured in the Local File Rights policy.

Action: Ensure that the user permissions configured in the Local File Rights policy are not conflicting with the user permissions configured in Dynamic Local User policy.

A.8 Printer Policy Errors

- ♦ “Printer driver installation failed for *printer_name*. The provided driver install file type is not supported” on page 78
- ♦ “Printer driver installation failed for *printer_name*. File extraction failed for *filename*” on page 78
- ♦ “Printer driver installation failed for *printer_name*. Check if provided drivers *inf* file is in proper format” on page 79
- ♦ “Unable to get *iprint* install file from the specified location in managed device, please check if file is there in specified location” on page 79
- ♦ “Unable to extract *iprint* client installer from the content” on page 79
- ♦ “Bad *iprint* install file. Unable to extract *setupipp.exe* file. Expectation is for a *zip* file which extracts *setupipp.exe* on the root. check the file mentioned for install” on page 79
- ♦ “*iPrint* client install failed. Check if the provided *iprint* client supports silent install” on page 79
- ♦ “Failed to add *smb* printer *printer_name*” on page 80
- ♦ “Failed to add *iprint* printer *printer_name*” on page 80
- ♦ “An incorrect error message that the *iPrint* policy could not be enforced is displayed on the managed device” on page 80

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Unable to extract iprint client installer from the content

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

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

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

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

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

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

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

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

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

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

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

Failed to add smb printer *printer_name*

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

Possible Cause: The SMB printer connection is not valid.

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

Failed to add iprint printer *printer_name*

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

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

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

An incorrect error message that the iPrint policy could not be enforced is displayed on the managed device

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

Explanation: The iPrint policy might take some time to install an iPrint printer on a device, depending on the size of the iPrint printer driver and the network connectivity. In such a scenario, even if the iPrint printer is successfully installed on the device, an incorrect message that the iPrint policy could not be enforced is displayed on the managed device.

Action: Ignore the error message and refresh the device.

The correct message indicating that the policy has been successfully enforced is displayed on the device after a manual or automatic refresh.

A.9 Printer Policy Troubleshooting

- ♦ [“Unable to install a printer driver on Windows managed devices through the Printer Policy” on page 81](#)
- ♦ [“Unable to install the printer driver on a Windows Vista SP1 device” on page 81](#)
- ♦ [“Changing the iPrint printer driver on a server does not update the driver on the managed device” on page 82](#)
- ♦ [“Unable to install or update the printer drivers on re-enforcing the policy” on page 82](#)
- ♦ [“Unable to install iPrint printer on a Windows 2000 managed device” on page 82](#)

- ◆ “Unable to install iPrint printer on a Windows XP managed device” on page 82
- ◆ “Uninstall does not roll back the previously enforced Printer policies” on page 83
- ◆ “Installation of the iPrint printer fails on a device if the printer does not have the supported drivers” on page 83
- ◆ “Installation of the network printer might fail on a Windows Server 2008 R2 device” on page 83
- ◆ “Unable to enforce a printer policy on a managed device if the printer driver that is installed on the device is unsigned” on page 84
- ◆ “The Printer policy might fail to install an iPrint printer on a managed device if iPrint printer drivers are configured in the policy” on page 84
- ◆ “The Printer policy fails because of a handler timeout” on page 84

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Unable to install iPrint printer on a Windows 2000 managed device

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

Explanation: If a printer policy that is configured to install an iPrint printer on a managed device is assigned to a user who logs in to a Windows 2000 managed device, the iPrint printer is not installed on the device.

Action: Assign the printer policy to the device.

Unable to install iPrint printer on a Windows XP managed device

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

Explanation: If a printer policy that is configured to install an iPrint printer on a managed device is assigned to a user who logs in to a Windows XP device that has an iPrint Client 4.x installed, the iPrint printer is not installed on the device.

Action: Do the following:

- 1 Uninstall the iPrint Client 4.x from the device.

- 2 Download the iPrint Client 5.x from the [Novell Downloads site \(http://download.novell.com/index.jsp\)](http://download.novell.com/index.jsp).
- 3 Install the iPrint Client 5.x on the managed device.
For more information on installing the iPrint Client, see [Step 8 in Section 2.4, “Printer Policy,” on page 23](#)

Uninstall does not roll back the previously enforced Printer policies

- Source: ZENworks 10 Configuration Management; Policy Management; Windows Configuration Policy.
- Explanation: The previously enforced printer policies does not roll back when ZENworks is uninstalled.
- Action: Before uninstalling ZENworks, disassociate the Printer policy from the users or devices to unenforce the policy.

Installation of the iPrint printer fails on a device if the printer does not have the supported drivers

- Source: ZENworks 10 Configuration Management; Policy Management; Windows Configuration Policy.
- Explanation: If a printer configured in the iPrint policy has assigned drivers that are not supported by the operating system on the managed device, then the Installation of the printer fails.
- For example, if a printer that has Windows XP and Windows Vista drivers is configured in a iPrint policy and the policy is assigned to a Windows 7 device, the installation of the printer on the Windows 7 device fails.
- Action: Before assigning a iPrint policy to a device, ensure that the drivers assigned to the printer configured in the policy are supported by the operating system on the device.

Installation of the network printer might fail on a Windows Server 2008 R2 device

- Source: ZENworks 10 Configuration Management; Policy Management; Windows Configuration Policy.
- Explanation: If you assign a Printer policy that has a Network printer configured for a Windows Server 2008 R2 device, the installation of the printer might fail if the Internet Printing Client is not installed on the device.
- Action: Perform the following steps to install the Internet Printing Client on the device:
- 1 Click *Start > All Programs > Administrative Tools > Server Manager*.
 - 2 In the Server Manager window, click *Features > Add Features*.
 - 3 Select *Internet Printing Client*.
 - 4 Click *Install*.
 - 5 Restart the device.

Unable to enforce a printer policy on a managed device if the printer driver that is installed on the device is unsigned

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

Explanation: The printer driver that is installed on the device has not been digitally signed by Microsoft.

Action: Enable using unsigned drivers in the printer policy:

- 1 On the device, right-click *My Computers > Properties*.
- 2 In the System Properties window, click *Hardware > Driver Signing*.
- 3 Select *Ignore - Install the software anyway and don't ask for my approval*.

The Printer policy might fail to install an iPrint printer on a managed device if iPrint printer drivers are configured in the policy

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

Explanation: The iPrint policy might fail to install the iPrint printer on a device if iPrint printer drivers are configured in the policy. You must not add iPrint printer drivers in the Printer Driver Installation panel of a printer policy details page because the iPrint drivers are automatically downloaded from the iPrint servers when the iPrint printer is installed on the device.

Action: Edit the policy to remove the iPrint printers from the Driver List in the Printer Driver Installation panel of the printer policy details page.

The Printer policy fails because of a handler timeout

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

Explanation: The printers that are being installed or configured might take a considerable amount of time because the devices need to access and then install the related printer drivers. This could result in a printer handler time-out.

Action: To set a default value that forces the Printer policy handler to wait for a set amount of time:

- 1 On a Windows managed device, open the Registry Editor.
- 2 Go to `HKLM\Software\Novell\ZCM\PrinterPolicy`.
- 3 Create the `MaxZenPrinterProcessingTimeOut` registry key with an appropriate timeout value, in seconds, depending on the number of printers to be configured.

A.10 Roaming Profile Policy Errors

- ♦ “The policy `policy_name` could not be successfully enforced as policy data was empty” on page 85

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

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

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the “[Message Logging](#)” in [ZENworks 10 Configuration Asset Management System Administration Reference](#).

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

A.11 Roaming Profile Policy Troubleshooting

- ♦ “Unable to enforce a Roaming Profile policy on a Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device if the user profile is stored in a shared folder on a Windows Server 2003 device” on page 85

Unable to enforce a Roaming Profile policy on a Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device if the user profile is stored in a shared folder on a Windows Server 2003 device

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

Explanation: If a Roaming Profile policy is assigned to a user who has not logged into a Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device at least once before the policy was assigned, enforcing the policy fails on the device. This is because of insufficient permissions configured for the shared folder containing the user profile on the Windows Server 2003 device.

Action: Perform the following steps on the Windows Server 2003 device:

- 1 Create a local user account with the same credentials that the user specifies to log in to the Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device.

For example, if the username is `user1`, create a local account with `user1` credentials.

- 2 Create a folder named `username.v2`.

For example, `user1.v2`.

- 3 Right-click the folder, then click *Properties*.

- 4 Click *Sharing* and share the folder.

- 5 Click *Permissions* to provide Full Control permissions for the user, click *Apply*, then click *OK*.
- 6 Click *Security*.
- 7 In the Group or user names panel, click *CREATOR OWNER*, then click *Advanced*.
- 8 In the Advanced Security Settings box, click *Owner*.
- 9 Click *Other Users or Groups*.
- 10 In the Select User or Group dialog box, click *Advanced* to add this user as the current owner of the folder.
- 11 Click *OK*.
- 12 Provide Full Control permissions for the *CREATOR OWNER*.
- 13 Click *Apply*, then click *OK*.

A.12 SNMP Policy Errors

- ♦ “The policy *policy_name* could not be successfully enforced due to an error” on page 86
- ♦ “The policy *policy_name* could not be successfully enforced as policy data was empty” on page 86

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

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

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

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the “[Message Logging](#)” in *ZENworks 10 Configuration Asset Management System Administration Reference*.

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

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

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

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

Action: Review the policy content in ZENworks Control Center.

A.13 Windows Group Policy Errors

- ♦ “There was an error while enforcing the policy *policy_name*. Please refer the managed device log for details” on page 87
- ♦ “The policy *policy_name* was not applied” on page 87

- ◆ “The security settings in policy *polycname* were not applied” on page 87
- ◆ “The Windows Hotfix "KB897327" required for exporting and applying Group policy security settings on Windows XP was not found. Computer configuration security settings could not be exported/applied” on page 88
- ◆ “There was an error while unenforcing Group policy settings” on page 88
- ◆ “There was an error while cleaning up Group policy settings at logout for user *username*” on page 88
- ◆ “There was an error while accessing content for policy *policy_name*.” on page 88
- ◆ “Some security settings could not be configured” on page 89
- ◆ “To operate on security settings, Windows XP Hotfix KB897327 is required” on page 89
- ◆ “Failure importing group policy settings” on page 89

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

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

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the “[Message Logging](#)” in *ZENworks 10 Configuration Asset Management System Administration Reference*.

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

The policy *policy_name* was not applied

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

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

The security settings in policy *polycname* were not applied

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

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

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

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

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

Possible Cause: This message is logged if the Hotfix KB897327 is not applied on Windows XP SP1 or SP2 device before the policy is applied. The Hotfix is required for security settings to be configured on the managed device.

Action: Install Windows Hotfix KB897327 on the Windows XP SP1 or SP2 managed device from the [Microsoft Support Web site \(http://support.microsoft.com/KB/897327\)](http://support.microsoft.com/KB/897327).

There was an error while unenforcing Group policy settings

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

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the “[Message Logging](#)” in *ZENworks 10 Configuration Asset Management System Administration Reference*.

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

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

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

Action: Turn on debug logging on the managed device and refer the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see “[Message Logging](#)” in *ZENworks 10 Configuration Asset Management System Administration Reference*.

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

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

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

Possible Cause: The error occurs if the managed device is immediately refreshed after the policy was created and assigned. Hence, the content for the policy might have not been completely processed at the server.

Action: Wait for five minutes and refresh the managed device.

Some security settings could not be configured

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

Possible Cause: This message is logged if some of the security settings of a policy are not applied on the managed device.

Action: Contact [Novell Support \(http://www.novell.com/support\)](http://www.novell.com/support).

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

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

Explanation: The error message might occur while creating or editing group policies for Windows XP SP1 or SP2 managed device.

Possible Cause: The Windows Hotfix KB897327 is not installed on the Windows XP SP1 or SP2 managed device.

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

Action: Install Windows Hotfix KB897327 on the Windows XP SP1 or SP2 managed device from the [Microsoft Support Web site \(http://support.microsoft.com/KB/897327\)](http://support.microsoft.com/KB/897327).

Failure importing group policy settings

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

Explanation: When `gpedit.msc` is closed, the GPHelper displays the error message with the ID `POLICYHANDLERS.WinGPPolicy.ExportFailure`.

Possible Cause: The Windows Hotfix KB897327 is not installed on the Windows XP SP1 or SP2 managed device.

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

Action: Install Windows Hotfix KB897327 on the Windows XP SP1 or SP2 managed device from the [Microsoft Support Web site \(http://support.microsoft.com/KB/897327\)](http://support.microsoft.com/KB/897327).

A.14 Windows Group Policy Troubleshooting

- ♦ [“The Group Policy Helper tool is not backward compatible with the earlier versions of ZENworks Configuration Management releases” on page 90](#)
- ♦ [“Favorites configured by using the Group policy are not cleared when the group policy is unenforced” on page 90](#)
- ♦ [“Internet Explorer Settings configured in the Group policy are not applied on the Internet Explorer” on page 90](#)
- ♦ [“Security settings of the Windows Group policy are not effective on the device” on page 91](#)

- ◆ “The Security settings configured in the Windows Group policy are not applied on a Windows XP SP1 or SP2 managed device” on page 91
- ◆ “Unable to launch the Group Policy Helper tool on a 32-bit Windows Vista or Windows 7 device” on page 91
- ◆ “Policy Enforcement status is not properly displayed” on page 92
- ◆ “Unable to export Group Policy content” on page 92
- ◆ “Unable to view the 64 bit snap-ins in the Group Policy Helper tool” on page 92
- ◆ “Log-on and Log-off scripts that launch GUI applications do not functional properly on terminal server and Windows Vista devices” on page 93
- ◆ “Assigning an Active Directory Group policy to a user or a device might generate some application event logs on the device” on page 93
- ◆ “Group Policy created on a device with a specific operating system is not enforced on a device with a different operating system” on page 93
- ◆ “Configuring Group Policy on a 64-bit version of Windows Vista device, Windows Server 2008, and Windows 7 device is not yet supported” on page 93
- ◆ “Scripts configured through Active Directory Group policy are not enforced on a device.” on page 94
- ◆ “Security settings that have not been configured in a ZENworks Group Policy are also enforced on a managed device when the ZENworks Group Policy is enforced on the managed device” on page 94
- ◆ “Partial failure of Group Policy unenforcement settings” on page 94
- ◆ “Users need to log in again on a managed device, even though the setting for a forced login is not selected” on page 95

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The Security settings configured in the Windows Group policy are not applied on a Windows XP SP1 or SP2 managed device

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

Action: On the Windows XP SP1 or SP2 managed device, install Windows Hotfix KB897327 from the [Microsoft Support Web site \(http://support.microsoft.com/KB/897327\)](http://support.microsoft.com/KB/897327).

Unable to launch the Group Policy Helper tool on a 32-bit Windows Vista or Windows 7 device

Source: ZENworks 11 Configuration Management; Policy Management; Windows Configuration Policy.

Explanation: The Group Policy Helper tool does not launch on a 32-bit Windows 7/Vista device if the User Account Control (*Start > Settings > Control Panel > User Accounts*) is enabled and Mozilla Firefox or any other browser is used.

Action: Configure the Internet Explorer or Mozilla Firefox browser to run with administrator credentials.

- ◆ To configure Internet Explorer or Mozilla Firefox for a session, right-click the selected browser's shortcut icon on the desktop, then select *Run as administrator*.
- ◆ To configure the Internet Explorer or Mozilla Firefox browser permanently:
 1. On the desktop, right-click the selected browser's shortcut icon and select *Properties*. Click the *Shortcut* tab, then click the *Advanced* button. In the Advanced Properties dialog box, select *Run as administrator*.

or

In Windows Explorer, navigate to the Internet Explorer or Mozilla Firefox executable file, right-click the file, then select *Properties*. Click the *Compatibility* tab, then select *Run this program as an administrator*.

2. Restart the browser.

Policy Enforcement status is not properly displayed

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

Explanation: If you assign more than one policy to a user or a device, the policy enforcement status is not properly displayed. The consolidated status of a Group policy is displayed in the ZENworks icon only for the last enforced policy. That is, if any of the Group policies fail, the last effective policy is displayed in the ZENworks icon as *Failed* and rest of the policies are displayed as *Success*.

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

Action: None.

Unable to export Group Policy content

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

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

Action: Perform the following steps:

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

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

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

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

Action: None.

Log-on and Log-off scripts that launch GUI applications do not functional properly on terminal server and Windows Vista devices

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

Explanation: On the terminal server and Windows Vista devices, the log-on and log-off scripts launching GUI applications do not functional properly because the Graphical User Interface is not launched on the desktop.

Action: Use Directive bundles to launch the GUI applications:

- 1 Create a Directive bundle.
- 2 Add a Launch Windows Executable action to launch a GUI application, such as mspaint.
- 3 Assign the bundle to a device.
- 4 Select *Launch Schedule*, then select the schedule type as *Event*.
- 5 Select the *User Login* or *User Logout* event to trigger the schedule.

Assigning an Active Directory Group policy to a user or a device might generate some application event logs on the device

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

Explanation: If you configure an Active Directory Group policy and assign the policy to a user or a device, some application event logs might be generated on the device even if the policy is successfully enforced on the device.

Action: Ignore the application event logs.

Group Policy created on a device with a specific operating system is not enforced on a device with a different operating system

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

Explanation: The Windows Group policy containing the local group policy settings is not applied on a device if the operating system of the device where the policy is applied is different from the operating system of the device where the policy is created.

Action: Remove the Operating System specific System Requirement from the Windows Group policy and then apply the policy.

However, the security settings are applied only if the operating system version of the device where the policy is applied is later than the operating system version of the device where the policy is created.

Configuring Group Policy on a 64-bit version of Windows Vista device, Windows Server 2008, and Windows 7 device is not yet supported

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

Explanation: You cannot configure Group policy on 64-bit version of Windows Vista device, Windows Server 2008, and Windows 7 device. However, you can enforce Group policy on these devices.

Action: To enforce Group Policy on 64-bit version of a device, configure a Group policy on a corresponding 32-bit version of the device and assign it to the 64-bit device. For example, create a Group policy on a 32-bit Windows 7 device and assign it to a 64-bit Windows 7 device.

Scripts configured through Active Directory Group policy are not enforced on a device.

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

Explanation: The scripts configured through Active Directory group policy are not enforced on a device even though the policy displays success in the ZENworks Adaptive Agent Policies page. However, the other settings if any configured in the policy are enforced on the device.

Action: Configure scripts through Local Group policy.

Security settings that have not been configured in a ZENworks Group Policy are also enforced on a managed device when the ZENworks Group Policy is enforced on the managed device

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

Explanation: If you create a Windows Group Policy through the ZENworks Control Center of a device that already has some security settings configured and assign this policy to a managed device, the security settings that were configured on the device, on which you created the group policy, are also applied on the managed device.

Action: To remove all the previously configured security settings on a device, run the following command before you launch the ZENworks Control Center on the device to create the Group policy:

```
secedit /configure /cfg %windir%\repair\secsetup.inf /db  
secsetup.sdb /verbose
```

Partial failure of Group Policy unenforcement settings

Source: ZENworks 11 Configuration Management; Policy Management; Windows Configuration Policy.

Explanation: When Group Policy settings are unenforced on a device, URLs added in Favourites and Links do not get removed.

Action: To unenforce the Group Policy settings and restore the system to a clean state, make sure you select the option *Delete existing Favourites and Links, if present*, when the system is in the default state prior to applying any policies.

Users need to log in again on a managed device, even though the setting for a forced login is not selected

Source: ZENworks 11 SP2 Configuration Management; Policy Management; Windows Configuration Policy.

Explanation: After applying an updated Windows Group Policy on a managed device, logged-in users are forced to log out even though the *After enforcement, force a re-login on the managed device, if necessary* setting is not selected.

Action: To ensure that a user does not need to log in again to the managed device, deselect the *After enforcement, force a re-login on the managed device, if necessary* option on any Roaming Profile Policy that is associated with the same user or device.

For more information, see TID 7007600 in the [Novell Support Knowledgebase](http://www.novell.com/support/search.do?usemicrosite=true&searchString=7007600) (<http://www.novell.com/support/search.do?usemicrosite=true&searchString=7007600>).

A.15 ZENworks Explorer Configuration Policy Errors

- ♦ “There was an error while unenforcing the policy” on page 95
- ♦ “There was an error while enforcing the policy policy_name. Please refer the managed device log for details” on page 96
- ♦ “There was an error while setting the desktop icon name” on page 96
- ♦ “The policy policy_name could not be successfully enforced as policy data was empty” on page 96
- ♦ “There was an error while configuring the setting "Enable manual refresh"" on page 96
- ♦ “There was an error while configuring the setting "Enable folder view"" on page 97
- ♦ “There was an error while configuring the setting "Expand the entire folder tree"" on page 97
- ♦ “There was an error while configuring the setting "Display applications in windows explorer"" on page 97
- ♦ “There was an error while configuring the setting "Allow logout/login as new user"" on page 97

There was an error while unenforcing the policy

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

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the “[Message Logging](#)” in *ZENworks 10 Configuration Asset Management System Administration Reference*.

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

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

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

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the “[Message Logging](#)” in *ZENworks 10 Configuration Asset Management System Administration Reference*.

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

There was an error while setting the desktop icon name

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

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

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the “[Message Logging](#)” in *ZENworks 10 Configuration Asset Management System Administration Reference*.

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

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

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

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the “[Message Logging](#)” in *ZENworks 10 Configuration Asset Management System Administration Reference*.

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

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

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

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the “[Message Logging](#)” in *ZENworks 10 Configuration Asset Management System Administration Reference*.

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

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

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

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the “[Message Logging](#)” in *ZENworks 10 Configuration Asset Management System Administration Reference*.

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

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

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

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the “[Message Logging](#)” in *ZENworks 10 Configuration Asset Management System Administration Reference*.

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

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

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

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the “[Message Logging](#)” in *ZENworks 10 Configuration Asset Management System Administration Reference*.

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

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

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

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more information on how to turn on debug logging, see the “[Message Logging](#)” in *ZENworks 10 Configuration Asset Management System Administration Reference*.

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

iPrint Policy Management Utility

B

The iPrint Policy Management (IPPman) utility allows you to perform repetitive and mass operations on printer policies that have an iPrint printer matching a specific iPrint URI or a specific search criteria. You can use this utility to migrate the iPrint printers from one iPrint server to another.

The IPPman utility enables you to create, clone, rename, modify, and delete the iPrint objects by editing the existing printer policies that have iPrint printers. You can also export and import the iPrint printer configurations for all the policies that match specific printer URI criteria.

The following sections contain more information on this utility:

- ♦ [Section B.1, “Installing the IPPman Utility,” on page 99](#)
- ♦ [Section B.2, “Using IPPman Commands to Configure iPrint Printers,” on page 100](#)
- ♦ [Section B.3, “Understanding the Format of the iPrint Printer Configuration File,” on page 107](#)
- ♦ [Section B.4, “Printing Preferences for an iPrint Printer,” on page 108](#)
- ♦ [Section B.5, “iPrint Printer List Import File Format,” on page 108](#)

B.1 Installing the IPPman Utility

The IPPman utility is installed by default in the ZENworks installation directory of the ZENworks Configuration Management server. However, you might need to manually install the utility on a device in the following scenarios:

- ♦ Migrate an iPrint printer from one device to another.
- ♦ Install the utility on a device that is not a ZENworks Server.

1 Copy the `ippmanagement.zip` file from the `ZENworks_installation_directory\novell\zenworks\install\downloads\tools` directory to a temporary location.

or

Download the file from ZENworks Control Center (in the Common Tasks, click *Download ZENworks Tools > Administrative Tools*).

- 2** Extract the `ippmanagement.zip` file to a temporary location.
- 3** Set the `IPPMAN_HOME` environment variable to the directory where you extracted IPPman.
- 4** Set the `JAVA_HOME` environment variable to the JDK installation directory.

For information related with JAVA version specifications, see “[Administration Browser Requirements](#)” in the *ZENworks 10 Configuration Management Installation Guide*.

- 5** At the command prompt of the device, go to the directory where the `.zip` contents are extracted and run `ippman.bat` from the `bin` folder.

B.2 Using IPPman Commands to Configure iPrint Printers

You can configure iPrint printers by using ZENworks Control Center or by using the `zman` command line utility. In addition, you can use the IPPman utility to perform repetitive and mass operations on printer policies that have an iPrint printer matching a specific iPrint URI or matching a specific search criteria.

For more information on creating printer policies by using ZENworks Control Center, see [Section 2.4, “Printer Policy,” on page 23](#).

For more information on creating printer policies by using `zman` command line utility, see [“ZENworks Command Line Utilities”](#).

Review the following sections for more information on using the IPPman commands:

- ◆ [Section B.2.1, “Creating an iPrint Printer,” on page 100](#)
- ◆ [Section B.2.2, “Cloning an iPrint Printer,” on page 101](#)
- ◆ [Section B.2.3, “Renaming an iPrint Printer,” on page 102](#)
- ◆ [Section B.2.4, “Modifying an iPrint Printer,” on page 103](#)
- ◆ [Section B.2.5, “Deleting an iPrint Printer,” on page 104](#)
- ◆ [Section B.2.6, “Exporting iPrint Printer,” on page 105](#)
- ◆ [Section B.2.7, “Importing an iPrint Printer,” on page 105](#)

B.2.1 Creating an iPrint Printer

To create a new iPrint printer configuration for all the policies that match specific printer URI criteria:

- 1 Create the iPrint printer configuration file.

For information on creating the iPrint printer configuration file, see [Section B.3, “Understanding the Format of the iPrint Printer Configuration File,” on page 107](#).

- 2 Use the `ippman create` command to create a new iPrinter printer for all the printer policies that have an iPrint printer with the URI specified in the command.

The printer name and the printing preferences for the new iPrinter printer are specified in the iPrint printer configuration file.

- ◆ On a ZENworks server, enter the command as follows:

```
ippman create -uri iprint_printer_uri -conf iprint_printer_configuration_file
-username username -password password
```

Example:

```
ippman create -uri ipp://10.0.0.0/ipp/Printer1 -conf
"c:\printerdata.xml" -username Administrator -password xxxxxx
```

- ◆ On a device other than the ZENworks server, enter the command as follows:

```
ippman create -uri iprint_printer_uri -conf iprint_printer_configuration_file
-server ZENworks_server_ip -port port_number -username username -password
password
```

Example:

```
ippman create -uri ipp://10.0.0.0/ipp/Printer1 -conf
"c:\\printerdata.xml" -server 10.0.0.0 -port 80 -username
Administrator -password xxxxx
```

Table B-1 Options Used with the Create Command

Option	Description
uri	URI of the iPrint printer to search.
conf	iPrint printer configuration file containing the printer name and the printing preferences.
username and password	Credentials of the ZENworks administrator.
server	IP address of the ZENworks server.
port	Port of the ZENworks server. The default port is 80.

To refer to the online help for the command, enter the following command:

```
ippman create -help
```

B.2.2 Cloning an iPrint Printer

To clone the iPrint printer configuration for all policies that match specific printer URI criteria, use the `ippman clone` command.

This command creates a new iPrinter printer for all the printer policies that have an iPrint printer with the URI specified in the command. The URI of the new iPrint printer is also specified in the command. The cloned printer has the same printing preferences as the original printer.

- ◆ On a ZENworks server, enter the command as follows:

```
ippman clone -uri iprint_printer_uri -uri2 iprint_printer_uri_for_clone -
default true/false -updatedriver true/false -username username -password
password
```

Example:

```
ippman clone -uri ipp://10.0.0.0/ipp/Printer -uri2 ipp://10.0.0.0/ipp/Printer1
-default true -updatedriver true -username Administrator -password xxxxx
```

- ◆ On a device other than the ZENworks server, enter the command as follows:

```
ippman clone -uri iprint_printer_uri -uri2 iprint_printer_uri_for_clone -
default true/false -updatedriver true/false -server ZENworks_server_ip -port
port_number -username username -password password
```

Example:

```
ippman clone -uri ipp://10.0.0.0/ipp/Printer -uri2 ipp://10.0.0.0/ipp/Printer1
-default true -updatedriver true -server 10.0.0.0 -port 80 -username
Administrator -password xxxxx
```

Table B-2 Options Used with the Clone Command

Option	Description
uri	URI of the iPrint printer to search.
uri2	URI of the iPrint printer to clone.
default	Whether this is the default printer. The available options are true or false.
updatedriver	Update the printer driver. The available options are true or false.
username and password	Credentials of the ZENworks administrator.
server	IP address of the ZENworks server.
port	Port of the ZENworks server. The default port is 80.

To refer to the online help for the command, enter the following command:

```
ippman clone -help
```

After cloning an iPrint printer, you can choose to delete the original iPrint printer. For more information on deleting the iPrint printer, see [Section B.2.5, “Deleting an iPrint Printer,” on page 104](#).

B.2.3 Renaming an iPrint Printer

To rename the iPrint printer configuration for all policies that match specific printer URI criteria, use the `ippman rename` command.

- ◆ On a ZENworks server, enter the command as follows:

```
ippman rename -uri iprint_printer_uri -uri2 renamed_iprint_printer_uri -  
default true/false -updatedriver true/false -username username -password  
password
```

Example:

```
ippman rename -uri ipp://10.0.0.0/ipp/Printer -uri2 ipp://10.0.0.0/ipp/  
Printer1 -default true -updatedriver true -username Administrator -password  
xxxxx
```

- ◆ On a device other than the ZENworks server, enter the command as follows:

```
ippman rename -uri iprint_printer_uri -uri2 renamed_iprint_printer_uri -  
default true/false -updatedriver true/false -server ZENworks_server_ip -port  
port_number -username username -password password
```

Example:

```
ippman rename -uri ipp://10.0.0.0/ipp/Printer -uri2 ipp://10.0.0.0/ipp/  
Printer1 -default true -updatedriver true -server 10.0.0.0 -port 80 -username  
Administrator -password xxxxx
```

Table B-3 Options Used with the Rename Command

Option	Description
uri	URI of the iPrint printer to search.
uri2	URI of the iPrint printer to rename.
default	Whether this is the default printer. The available options are true or false.
updatedriver	Update the printer driver. The available options are true or false.
username and password	Credentials of the ZENworks administrator.
server	IP address of the ZENworks server.
port	Port of the ZENworks server. The default port is 80.

To refer to the online help for the command, enter the following command:

```
ippman rename -help
```

B.2.4 Modifying an iPrint Printer

To create a new iPrint printer configuration for all policies that match specific printer URI criteria, and modify the default settings:

- 1 Create the iPrint printer configuration file.

For information on creating the iPrint printer configuration file, see [Section B.3, “Understanding the Format of the iPrint Printer Configuration File,”](#) on page 107.

- 2 Use the `ippman modify` command.

- ◆ On a ZENworks server, enter the command as follows:

```
ippman modify -uri iprint_printer_uri -conf iprint_printer_configuration_file -username username -password password
```

Example:

```
ippman modify -uri ipp://10.0.0.0/ipp/Printer1 -conf "c:\\printerdata.xml" -username Administrator -password xxxxx
```

- ◆ On a device other than the ZENworks server, enter the command as follows:

```
ippman modify -uri iprint_printer_uri -conf iprint_printer_configuration_file -server ZENworks_server_ip -port port_number -username username -password password
```

Example:

```
ippman modify -uri ipp://10.0.0.0/ipp/Printer1 -conf "c:\\printerdata.xml" -server 10.0.0.0 -port 80 -username Administrator -password xxxxx
```

Table B-4 Options Used with the Modify Command

Option	Description
uri	URI of the iPrint printer to search.
conf	iPrint Printer Configuration file containing the printer name and the printing preferences.
username and password	Credentials of the ZENworks administrator.
server	IP address of the ZENworks server.
port	Port of the ZENworks server. The default port is 80.

To refer to the online help for the command, enter the following command:

```
ippman modify -help
```

B.2.5 Deleting an iPrint Printer

To delete a new iPrint printer configuration for all policies that match specific printer URI criteria, use the `ippman delete` command.

- ◆ On a ZENworks server, enter the command as follows:

```
ippman delete -uri iprint_printer_uri -username username -password password
```

Example:

```
ippman delete -uri ipp://10.0.0.0/ipp/Printer1 -username Administrator -password xxxxx
```

- ◆ On a device other than the ZENworks server, enter the command as follows:

```
ippman delete -uri iprint_printer_uri -server ZENworks_server_ip -port port_number -username username -password password
```

Example:

```
ippman delete -uri ipp://10.0.0.0/ipp/Printer1 -server 10.0.0.0 -port 80 -username Administrator -password xxxxx
```

Table B-5 Options Used with the Delete Command

Option	Description
uri	URI of the iPrint printer to delete.
username and password	Credentials of the ZENworks administrator.
server	IP address of the ZENworks server.
port	Port of the ZENworks server. The default port is 80.

To refer to the online help for the command, enter the following command:

```
ippman delete -help
```

B.2.6 Exporting iPrint Printer

To export the iPrint printer configuration for all policies that match a specific printer URI criteria, use the `ippman export` command.

- ♦ On a ZENworks server, enter the command as follows:

```
ippman export -uri iprint_printer_uri -folder export_folder -username username -password password
```

Example:

```
ippman export -uri ipp://10.0.0.0/ipp/Printer1 -folder "c:\\export" -username Administrator -password xxxxx
```

- ♦ On a device other than the ZENworks server, enter the command as follows:

```
ippman export -uri iprint_printer_uri -folder export_folder -server ZENworks_server_ip -port port_number -username username -password password
```

Example:

```
ippman export -uri ipp://10.0.0.0/ipp/Printer1 -folder "c:\\export" -server 10.0.0.0 -port 80 -username Administrator -password xxxxx
```

Table B-6 Options Used with the Export Command

Option	Description
uri	URI of the iPrint printer to search.
folder	Folder to which the XML files containing the iPrint printer configuration is exported. For every printer policy that matches the search criteria, an XML file is created. The XML file is named <i>polycyname_policyUID</i> . where <i>polycyname</i> is the name of the printer policy and <i>policyUID</i> is the unique ID of the printer policy.
username and password	Credentials of the ZENworks administrator.
server	IP address of the ZENworks server.
port	Port of the ZENworks server. The default port is 80.

To refer to the online help for the command, enter the following command:

```
ippman export -help
```

B.2.7 Importing an iPrint Printer

To import the iPrint printer configuration to a printer policy, you must use the XML file that contains the exported iPrint printer configuration information

For information on the format of the file, see [Section B.5, “iPrint Printer List Import File Format,” on page 108.](#)

- 1 (Conditional) Depending on the requirements, modify the XML file created when you export the iPrint printer.

For more information on exporting the iPrint printer, see [“Exporting iPrint Printer” on page 105.](#)

- 2 Use the `ippman import` command to import the iPrint printer configuration to all the printer policies matching a specific iPrint URI or a specific search criteria.

- ♦ On the ZENworks server, enter the command as follows:

```
ippman import -uri iprint_printer_uri -folder import_folder -username username
-password password
```

Example:

```
ippman import -uri ipp://10.0.0.0/ipp/Printer1 -folder "c:\\export" -
username Administrator -password xxxxx
```

- ♦ On the device other than the ZENworks server, enter the command as follows:

```
ippman import -uri iprint_printer_uri -folder import_folder -server
ZENworks_server_ip -port port_number -username username -password password
```

Example:

```
ippman import -uri ipp://10.0.0.0/ipp/Printer1 -folder "c:\\export" -
server 10.0.0.0 -port 80 -username Administrator -password xxxxx
```

Table B-7 Options Used with the Import Command

Option	Description
uri	URI of the iPrint printer to search.
folder	Folder from which the iPrint printer configuration is imported. This folder contains the exported iPrint printer configuration saved in an XML file named <i>policyname_policyUID</i> . where <i>policyname</i> is the name of the printer policy and <i>policyUID</i> is the unique ID of the printer policy.
username and password	Credentials of the ZENworks administrator.
server	IP address of the ZENworks server.
port	Port of the ZENworks server. The default port is 80.

To refer to the online help for the command, enter the following command:

```
ippman import -help
```

B.3 Understanding the Format of the iPrint Printer Configuration File

The iPrint printer configuration file contains information about the iPrint printer such as printer name, iPrint URI, and the printing preferences.

- ♦ [Section B.3.1, “Format of iPrint Printer Configuration File with Default Printing Preferences,” on page 107](#)
- ♦ [Section B.3.2, “\[Example\] iPrint Printer Configuration File with Some Printing Preferences Specified,” on page 107](#)

B.3.1 Format of iPrint Printer Configuration File with Default Printing Preferences

```
<?xml version="1.0" encoding="utf-8"?>
<Printer name="ipp://10.0.0.0/ipp/Printer2" type="iPrint"
updateiPrintDriver="true">
  <DefaultPrintingPreferences/>
</Printer>
```

For information on the default printing preferences, see [Section B.4, “Printing Preferences for an iPrint Printer,” on page 108](#).

B.3.2 [Example] iPrint Printer Configuration File with Some Printing Preferences Specified

You can specify printing preferences in the iPrint printer configuration file. For more information on the available printing preferences, see [Section B.4, “Printing Preferences for an iPrint Printer,” on page 108](#).

A sample of the iPrint printer configuration file with some printing preferences specified is as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<Printer name="ipp://10.0.0.0/ipp/Printer2" type="iPrint"
updateiPrintDriver="true">
  <DefaultPrintingPreferences>
    <PrinterOrientation>Portrait</PrinterOrientation>
    <PaperSource>Envmanual</PaperSource>
    <Duplex>true</Duplex>
    <Collate>true</Collate>
    <PaperSize>Ledger</PaperSize>
    <PrintQuality>High</PrintQuality>
    <IsDefault>true</IsDefault>
```

```

    </DefaultPrintingPreferences>
</Printer>

```

B.4 Printing Preferences for an iPrint Printer

Table B-8 *iPrint Printer Printing Preferences*

Printing Preference	Possible Values	Default Value
PrinterOrientation	Portrait, Landscape	Portrait
Duplex	true, false	true
Collate	true, false	true
PrintQuality	High, Low	high
PaperSource	Auto, Cassette, Envelope, Envmanual, Formsourc, Largecapacity, Lower, Largefmt, Largecapacity, Manual, Onlyone, Tractor, Smallfmt, Tray 1, Tray 2, Tray 3, Tray 4	No default value
PaperSize	Letter, Letter Small, Tabloid, Ledger, Legal, Statement, Executive, 11x17,16K, 8K, A3, A4, A4 Small, A5, B4, B5	No default value

B.5 iPrint Printer List Import File Format

To import the iPrint printer configuration to all the policies that match specific printer URI, use the XML file created when you exported the iPrint printer. For more information on exporting the iPrint printer, see [Section B.2.6, “Exporting iPrint Printer,” on page 105](#).

The format of the iPrint printer list import file that is used with the printer policy import command is as follows.

```

<?xml version="1.0" encoding="UTF-8"?>
  <PrinterList removeOthers="false">
    <Printer name="ipp://164.99.147.66/ipp/Printer2" type="iPrint "
updateiPrintDriver="true">
      <DefaultPrintingPreferences />
    </Printer>
    <Printer name="ipp://164.99.147.66/ipp/Printer3" type="iPrint "
updateiPrintDriver="false">
      <DefaultPrintingPreferences/>
    </Printer>
  </PrinterList>

```

Best Practices

C

The following sections contain information on the best practices to follow when using the Novell ZENworks 11 Configuration Management policies:

- ♦ [Section C.1, “Local File Rights Policy,” on page 109](#)
- ♦ [Section C.2, “Dynamic Local User Policy,” on page 109](#)
- ♦ [Section C.3, “Roaming Profile Policy,” on page 109](#)
- ♦ [Section C.4, “SNMP Policy,” on page 109](#)
- ♦ [Section C.5, “Windows Group Policy,” on page 110](#)
- ♦ [Section C.6, “Printer Policy,” on page 110](#)

C.1 Local File Rights Policy

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

C.2 Dynamic Local User Policy

- ♦ Ensure that the latest version of the Novell Client is installed on the managed device before the Dynamic Local User policy is enforced. To obtain the latest version of Novell Client, see the [Novell Download Web site \(http://download.novell.com/index.jsp\)](http://download.novell.com/index.jsp).
- ♦ If a Dynamic Local User policy that has no login restrictions configured is assigned to a managed device, the time taken to log in to the managed device can be significantly improved by adding a DonotFetchUserGroups registry key as follows:
 1. Open the Registry Editor.
 2. Go to HKLM\Software\Novell\ZCM\AgentSettings.
 3. Create a String called DonotFetchUserGroups and set its value to True.

C.3 Roaming Profile Policy

- ♦ The local user account must have the same username and password on both the managed device and the shared server that has the user profile stored because Windows authenticates the user before loading or saving the profile across the devices.
- ♦ Provide the necessary permission on the shared location to users whose profile is configured for roaming.

C.4 SNMP Policy

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

C.5 Windows Group Policy

- ◆ Do not apply the Windows Group policy on Windows 2000 or Windows 2003 domain controllers.
- ◆ Do not apply the Windows Group policy to a Windows managed device that is a part of the Microsoft domain and has a group policy from the Windows domain controller applied. The ZENworks Windows Group policy must be applied only if the group policy from the Windows domain controller is not applied.
- ◆ If you want the Windows Group policy settings to be applied to all users of a device, the settings must be configured as a part of a device-assigned policy. The user-assigned policies must contain only the configuration settings specific to the user to whom the policy is assigned.
- ◆ If you apply Local Group policies on a managed device that has ZENworks Group policies already applied, some of the settings might not work correctly.

C.6 Printer Policy

You must not edit the Printer policy to add iPrint printer drivers in the Printer Driver Installation panel of a printer policy details page. This is because the iPrint drivers are automatically downloaded from the iPrint servers when the iPrint printer is installed on a device. However, you can add local or network printer drivers to the drivers list if the policy has local or network printers configured.

Documentation Updates

D

This section contains information on documentation content changes that were made in this *ZENworks Policy Management Reference* for Novell ZENworks 10 Configuration Management SP3. The information can help you to keep current on updates to the documentation.

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

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

The following updates were made to the document:

- ♦ [Section D.1, “November 17, 2011: Update to ZENworks 10 Configuration Management SP3 \(10.3.4\),” on page 111](#)
- ♦ [Section D.2, “July 06, 2011: Update to ZENworks 10 Configuration Management SP3 \(10.3.3\),” on page 112](#)
- ♦ [Section D.3, “January 17, 2011: Update to ZENworks 10 Configuration Management SP3 \(10.3.2\),” on page 112](#)
- ♦ [Section D.4, “March 30, 2010: Update to ZENworks 10 Configuration Management SP3 \(10.3\),” on page 113](#)

D.1 November 17, 2011: Update to ZENworks 10 Configuration Management SP3 (10.3.4)

Updates were made to the following sections.

Location	Change
Section 2.2, “Dynamic Local User Policy,” on page 16	Added an update on the timeout duration for enforcing file rights in DLU policies in Step 6 on page 18 .
Section 2.2, “Dynamic Local User Policy,” on page 16	Added the update, if the user account is already on the workstation, the option to exclude the device from receiving the DLU policy is ignored in Step 5 on page 18 .
Section A.14, “Windows Group Policy Troubleshooting,” on page 89	Added the following troubleshooting scenario: “Users need to log in again on a managed device, even though the setting for a forced login is not selected” on page 95
Section A.4, “Dynamic Local User Policy Troubleshooting,” on page 72	Added the following troubleshooting scenario: “After logging out of a managed device that is disconnected from the network, a Dynamic Local User is unable to log in to the device again” on page 73
Section A.9, “Printer Policy Troubleshooting,” on page 80	Added the following troubleshooting scenario: “The Printer policy fails because of a handler timeout” on page 84.

Location	Change
Chapter 3, "Managing Policies," on page 41	Updated the following troubleshooting scenario: "Assigning a Roaming Profile Policy that has the User Profile Stored on a Windows, Linux or NetWare Share" on page 47.
Section A.4, "Dynamic Local User Policy Troubleshooting," on page 72	Added the following troubleshooting scenario: "The DLU policy does not delete user profiles if the Roaming Profile policy is applied" on page 74.

D.2 July 06, 2011: Update to ZENworks 10 Configuration Management SP3 (10.3.3)

Updates were made to the following sections.

Location	Change
Section 3.7, "Assigning a Roaming Profile Policy that has the User Profile Stored on a Windows, Linux or NetWare Share," on page 47	Updated section for Linux and Netware share.
Section 3.8, "Assigning a Roaming Profile Policy that has the User Profile Stored on a Home Directory," on page 49	Added section for Home Directory

D.3 January 17, 2011: Update to ZENworks 10 Configuration Management SP3 (10.3.2)

Updates were made to the following sections.

Location	Change
Section 2.4, "Printer Policy," on page 23	Added a note in Step 6 .
Section 2.8, "Windows Group Policy," on page 30	Added a note in Step 4 .
Section 2.9, "ZENworks Explorer Configuration Policy," on page 33	Updated default values in table.
Section A.14, "Windows Group Policy Troubleshooting," on page 89	Added the following scenario: "Unable to launch the Group Policy Helper tool on a 32-bit Windows Vista or Windows 7 device" on page 91.
Section A.14, "Windows Group Policy Troubleshooting," on page 89	Added the following scenario: "Partial failure of Group Policy unenforcement settings" on page 94.

Location	Change
Appendix B, "iPrint Policy Management Utility," on page 99	Updated the information in Step 3 to Step 5 .

D.4 March 30, 2010: Update to ZENworks 10 Configuration Management SP3 (10.3)

Updates were made to the following sections.

Location	Change
Section 2.2, "Dynamic Local User Policy," on page 16	Updated the information in Step 4 and Step 5 .
Section 2.3, "Local File Rights Policy," on page 21	Added a note in Step 5 .
Section 2.4, "Printer Policy," on page 23	Updated the information in Step 7 and Step 8 .
Section 2.4, "Printer Policy," on page 23	Added the following information in the row " Set as Default Printer " on page 27 : On a Windows 7 managed device, the assigned printer might be set as a default printer on the device even if the <i>Set as Default Printer</i> option is not selected in the policy.
Section 2.8, "Windows Group Policy," on page 30	Updated the information.
Section 3.5, "Assigning a Policy to Devices," on page 44	Updated the section.
Section 3.6, "Assigning a Policy to Users," on page 46	Updated the section.
Section 3.18, "Policy Issues on a Windows 7, Windows Server 2008, or Windows Server 2008 R2 device," on page 59	Added the section.
Section A.2, "Browser Bookmarks Policy Troubleshooting," on page 70	Added the section.
Section A.4, "Dynamic Local User Policy Troubleshooting," on page 72	Updated the section.
Section A.8, "Printer Policy Errors," on page 78	Added the following scenario: "An incorrect error message that the iPrint policy could not be enforced is displayed on the managed device" on page 80 .
Section A.9, "Printer Policy Troubleshooting," on page 80	Updated the section.

Location	Change
Section A.9, "Printer Policy Troubleshooting," on page 80	<p>Added the following scenarios:</p> <ul style="list-style-type: none"> ◆ "Unable to enforce a printer policy on a managed device if the printer driver that is installed on the device is unsigned" on page 84. ◆ "The Printer policy might fail to install an iPrint printer on a managed device if iPrint printer drivers are configured in the policy" on page 84. ◆ Installation of the network printer might fail on a Windows Server 2008 R2 device.
Section A.11, "Roaming Profile Policy Troubleshooting," on page 85	<p>Added the following scenario:</p> <p>"Unable to enforce a Roaming Profile policy on a Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2 device if the user profile is stored in a shared folder on a Windows Server 2003 device" on page 85.</p>
Section A.14, "Windows Group Policy Troubleshooting," on page 89	<p>Updated the section.</p>
Section C.2, "Dynamic Local User Policy," on page 109	<p>Updated the section.</p>
Section C.3, "Roaming Profile Policy," on page 109	<p>Updated the section.</p>
Section C.6, "Printer Policy," on page 110	<p>Added the section.</p>
Appendix B, "iPrint Policy Management Utility," on page 99	<p>Added the section.</p>