Novell ZENworks® Configuration Management

10

www.novell.com

POLICY MANAGEMENT REFERENCE

January 10, 2008

Novell®

Legal Notices

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

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

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (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.

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

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

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

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (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

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 system. The information in this guide is organized as follows:

Audience

This guide is intended for Novell ZENworks administrators.

Feedback

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

Additional Documentation

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

Documentation Conventions

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

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

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

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:

1.1 What Is a Policy?

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

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

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

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

1.2 What Is a Policy Group?

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

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

1.3 Understanding the Policy Types

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

- **Browser Bookmarks Policy:** Lets you configure Internet Explorer favorites for Windows* devices and users.
- **Dynamic Local User Policy:** Lets you create new users and manage existing users created on Windows 2000, Windows XP, and Windows Vista* workstations; and Windows 2000 and Windows 2003 Terminal Server sessions after the users have successfully authenticated to Novell eDirectory™.
- **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.
- **Login Restriction Policy:** Lets you restrict user access to one or more workstations.
- **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, ZENworks Explorer Configuration policy, and Windows Group 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, and Printer policy are plural policies.

- Policies can be disabled.

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

- ZENworks Configuration Management allows you to resolve policy conflicts.

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

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

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

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

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

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

Creating Policies

2

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

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

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

2.1 Browser Bookmarks Policy

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

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

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

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

   Description: Provide a short description of the policy’s content. This description displays in ZENworks Control Center.
4. Click *Next* to display the Bookmarks Tree Data Source page.
5. Create a browser bookmarks tree by exporting the bookmarks to a file in UTF-8 format or by manually entering the data source.

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

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

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

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

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

Field	Details
New	◆ Click *New* > *Folder* to display the Add Folder to Bookmarks dialog box, through which you can add a new folder to the bookmarks tree. ◆ Click *New* > *Bookmark* 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.
Edit	◆ Select the bookmark name you want to change, click *Edit* > *Rename*, then specify a new name. ◆ Click *Edit* > *Sort* to organize the bookmarks in ascending or descending order. ◆ Click *Edit* > *Move Up*, *Move Down*, or *Move To* to relocate a bookmark.
Delete	◆ Click *Delete* to delete a bookmark from the bookmarks tree.

7 Click *Next* to display the Summary page.

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

2.2 Dynamic Local User Policy

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

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
Use User Source Credentials	Enables logging in through the user's authoritative source credentials instead of Windows 2000, Windows XP, or Windows Vista credentials.
Volatile User (Remove User After Logout)	Specifies the use of a volatile user account for login. The user account that NWGINA creates on the local workstation can be either a volatile or a nonvolatile account.
Use the Credentials Specified Below (Always volatile)	Allows you to specify the following user credentials for a volatile user: ◆ **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.
Manage Existing User Account (if any)	Helps you to manage a user object that already exists. If you select both the *Volatile User (Remove User After Logout)* and *Manage Existing User Account (If Any)* check boxes, the existing user account is removed when the user logs out.
Not a Member Of	Displays the available group to which a user can be assigned as a member.
Member Of	Displays groups a user is member of.

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

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

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

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

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

Field	Details
Add	Allows you to select and assign appropriate file rights. To add a file/folder: 1. Click *Add*, 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 *Restrict inheritance to immediate child files/folders only*. 4. Click *OK*.
Edit	*Copy*: Allows you to copy and add a file rights setting to the list. 1. Select a file or folder, then click *Edit*. 2. Click *Copy*. 3. Specify a new name. 4. Click *OK*. *Rename*: Allows you to edit only the filename. 1. Select a file or folder, then click *Edit*. 2. Click *Rename*. 3. Specify a new filename. 4. Click *OK*.
Move Up or *Move Down*	Allows you to reorder the files or folders. 1. Select the check box in front of the file or folder you want to move. 2. Click *Move Up* and *Move Down* to relocate it.
Remove	Allows you to delete a file or a folder. 1. Select the check box in front of the file or folder. 2. Click *Remove*.

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, enforcement, status, and which group the policy is a member of.

2.3 Local File Rights Policy

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

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

2 In the *Policies* list, click *New*, then click *Policy* to display the Select Policy Type page.

3 Select *Local File Rights Policy*, click *Next* to display the Define Details page, then fill in the fields:

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

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

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

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

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

Field	Details
File / Folder Path	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 *Configuration* tab > the *Content* setting in the Management Zone Settings panel > *System Variables*. Click the *Help* button for details about configuring system variables.
Attributes	Allows you to specify the attributes of a file or folder, such as *Read only* and *Hidden*.

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
Permission for Users or Groups	Allows you to configure permissions for users or groups. 1. Click *Add*, then Click *User* or *Group* to select a user or a group from the appropriate drop-down list. 2. Select the type of permission you want to configure as *Simple NTFS Permissions* or *All NTFS Permissions*. 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 *Restrict inheritance to immediate child files/folders only*. 4. Click *OK*.
Create Groups on the Managed Device if they Do not Exist	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.

Field	Details
Remove Access Control Rules not Configured by ZENworks	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.
Inherit Applicable Access Rights Configured on Parent Folders	Select *Yes* if you want a file or folder to inherit applicable access control rules from its parent object. If you select *No*, inherited rules are removed. If you do not want to make any changes, select *not configured* on the managed device.At least one attribute, permission, or inheritance setting must be configured to create a policy. Without configuring any settings, you cannot create a policy.

6 Click *Next* to display the Summary page.

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

2.4 Printer Policy

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

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

2 In the *Policies* list, click *New*, then click *Policy* to display the Select Policy Type page.

3 Select *Printer Policy*, click *Next* to display the Define Details page, then fill in the fields:

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

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

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

4 Click *Next* to display the Printer Identification page, then select the type of printer to be installed on the managed device.

5 Click *Next*, then skip to the appropriate step, depending on which printer type you chose in Step 4:

- **Local Printer:** Continue with Step 6.
- **Network Printer:** Skip to Step 7.
- **iPrint Printer:** Skip to Step 8.

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

Field	Details
Name	Specify the name of the local printer that you want to configure on the target device.
Port	Select the physical port to which the printer is added, such as LPT1 or COM1.
Driver	Browse to and select a suitable driver for the printer. If the driver is not contained in the browser list, type in the correct model name. The driver must either be installed on the target device or specified in the installed policies.
Install a Driver	Select this option to install a driver on the target device. The driver installation is non-interactive and silent, and the supported driver installation type is `.inf`. 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.
Model Name	Browse to select the model name of the driver. The `.inf` file should support installation of the driver with a similar name.
Driver File Path	Specify the driver files either from a particular device where the browser is running or from a path in the managed device, such as `C:\temp\nipp.zip`.
Platform	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.
Language of Installation	Select the installation language. Your choices are English (United States), French, German, Portugese, Spanish, Italian, Chinese (Traditional), Chinese (Simplified), or Japanese.
I*nstall Forcefully Even if the Driver is Already Installed*	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
Name / Location	Specify the UNC path or URL name of the HTTP or an SMB printer. For example, it is `\\server-name\printer-name` for an SMB printer, and `http://server/printers/.myprinter/.printer` for a HTTP printer.
Driver	Browse to add and select a suitable driver for the Windows HTTP printer. You can ignore this for SMB printers.
Install a Driver	Use this option to install a driver on the target device. The driver installation is non-interactive and silent. The supported driver installation types are `.inf` and `.exe`. For the `.inf` type, the 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.
Model Name	Browse to select the model name of the driver. The `.inf` file should support installation of the driver with a similar name.

Field	Details
Driver File Path	Specify the driver files either from a particular device where the browser is running or from a path in the managed device, such as `c:\temp\nip.zip`.
Supported Platforms	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.
Language of Installation	Select the installation language. Your choices are English (United States), French, German, Portugese, Spanish, Italian, Chinese (Traditional), Chinese (Simplified), or Japanese.
Install Forecefully Even if the Driver is Already Installed	Select this option to force installation of the driver, even though it is already installed on the target device.

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

Field	Details
Name / Location	Specify the URI name of the iPrint printer. For example, `ipp://acme.com/ipp/servername`.
Update iPrint Printer while Installing the Driver	Select this option to update the printer driver and to reinstall the printer driver from the iPrint server while installing the iPrint printer.
Install iPrint Client	Select this option to install the iPrint client on a target machine. The installation file can be either `nipp.zip` or `nipp-s.exe`, 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.
i*Print Client Installer File Path*	Allows to specify the path to the iPrint Client Installer (which installs the iPrint client on the managed device). ◆ **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.
Install Forcefully Even if the Driver is Already Installed	Select this option to force installation of the driver, even though it is already installed on the target device.
Configure iPrint Client	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 (:) and the port number.
Proxy Server	Specify the iPrint proxy server name. For example, `http://proxy.companyx.com:8080`

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
Orientation	Select this option to specify the paper layout for the printer, such as landscape or portrait.
Duplex Printing	Specify whether or not to print on both sides of the paper, if the printer has that capability.
Collate	Specify whether or not the printer should organize multiple copies of a document, if the printer has that capability.
Print Quality	Select the print quality. Select *High* quality, for the best possible resolution, or select *Low* quality for lower resolution and lower quality.
Paper Source	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.
Paper Size	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` for 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
Set as Default Printer	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.
Remove all Printers not Specified by ZENworks Printer Policies	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, 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 settings for Remote Management operations such as Remote Control, Remote View, Remote Execute, Remote Diagnostics, and File Transfer, and also allows you to control settings for security.

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 *Remote Management Policy*, click *Next* to display the Define Details page, then fill in the fields:

   Policy Name: Provide a unique 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.

   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 the summary page of the policy in ZENworks Control Center.
4. Click *Next* to display the Remote Management General Settings page. To accept the default settings, proceed to the next step, or use the information specified in the following table to change the default settings.

Field	Details
Allow User to Request a Remote Session	Enables the user on the managed device to request a remote operator to perform a remote session. The remote operator must ensure that the Remote Management Listener is running.
Terminate the Remote Session When Permission Is Required from a New User Logging In to the Managed Device	Terminates an ongoing remote session when permission is required from a new user who has logged into a remotely managed device.
Display Remote Session Audit Information to the User on the Managed Device	Allows the user on the managed device to view the audit information for remote sessions from the ZENworks icon.
Display Remote Management Properties in the ZENworks Icon	Allows the user on the managed device to view the properties associated with the Remote Management policy in the ZENworks icon.
Edit	To edit the message displayed to the user on the managed device before starting a remote session: 1. Click *Edit* to display the Edit Message dialog box. 2. Edit the message. 3. Click *OK*.
Restore default	To restore the default message: 1. Click *Restore default* to revert to the default message.

Field	Details
Add a Remote Listener	To add a Remote Listener: 1. Click *Add*. 2. In the Add Remote Listener dialog box, specify the DNS name or IP address of the management console and the port number on which the Remote Management Listener will listen for remote session requests. 3. Click *OK*.
Delete a Remote Listener	To delete a Remote Listener: 1. Select the Remote Listener you want to delete. 2. Click *Remove*.

5 Click *Next* to display the Remote Control Settings page. To accept the default settings, proceed to the next step, or use the information specified in the following table to change the default settings.

Field	Details
Allow Managed Device to be Controlled Remotely	Allows Remote Control sessions on the managed device. Selecting this option enables the subsequent options on the page. Deselecting the option disables the Remote Control operation on the device.
Ask Permission from User on Managed Device Before Starting Remote Control	Allows you to request permission from the user on the managed device before starting a Remote Control session.
Give Visible Signal to User on Managed Device During Remote Control	Displays a visible signal in the top right corner of the managed device desktop during the Remote Control session. The visible signal lets the user on the managed device know that a Remote Control session is in progress.
Give Audible Beep to User on Managed Device Every [ ] Seconds During Remote Control	Generates a beep on the managed device during a Remote Control session. The beep is generated periodically after the specified number of seconds.
Allow Managed Device Screen to be Blanked During Remote Control	Enables blanking of the screen of the managed device during a Remote Control session. Selecting this option locks the keyboard and the mouse controls of the managed device.
Allow Managed Device Mouse and Keyboard to be Locked During Remote Control	Enables locking of the managed device mouse and keyboard during a Remote Control session.
Allow Screen Saver to be Automatically Unlocked During Remote Control	Enables the unlocking of a password-protected screen saver from the Remote Control Viewer before the start of a Remote Control session on the managed device.
Automatically Terminate Remote Control Session After Inactivity of [ ] Minutes	Terminates a Remote Control session on the managed device if it has been inactive for the specified duration.

6 Click *Next* to display the Remote View Settings page. To accept the default settings, proceed to the next step, or use the information specified in the following table to change the default settings.

Field	Details
Allow Managed Device to be Viewed Remotely	Allows Remote View sessions on the managed device. Selecting this option enables the subsequent options on the page. Deselecting the option disables the Remote View operation on the device.
Ask Permission from User on Managed Device Before starting Remote View	Allows you to request permission from the user on the managed device before starting a Remote View session.
Give Visible Signal to User on Managed Device During Remote View	Displays a visible signal in the top right corner of the managed device desktop during the Remote View session.The visible signal lets the user on the managed device know that a Remote View session is in progress.
Give Audible Beep to User on Managed Device Every [ ] Seconds During Remote View	Generates a beep on the managed device during the Remote View session. The beep is generated periodically after the specified number of seconds.

7 Click *Next* to display the Remote Diagnostics Settings page. To accept the default settings, proceed to the next step, or use the information specified in the following table to change the default settings.

Field	Details
Allow Managed Device to be Diagnosed Remotely	Allows Remote Diagnostics sessions on the managed device. Selecting this option enables the subsequent options on the page. Deselecting the option disables the Remote Diagnostics operation on the device.
Ask Permission from User on Managed Device Before starting Remote Diagnostics	Ensures that the remote operator requests permission from the user on the managed device before starting a Remote Diagnostics session.
Give Visible Signal to User on Managed Device During Remote Diagnostics	Displays a visible signal in the top right corner of the managed device desktop during the Remote Diagnostics session.The visible signal lets the user on the managed device know that a Remote Diagnostics session is in progress.
Give Audible Beep to User on Managed Device Every [ ] Seconds During Remote Diagnostics	Generate a beep on the managed device during the Remote Diagnostics session. The beep is generated periodically after the specified number of seconds.
Allow Managed Device Screen to be Blanked During Remote Diagnostics	Enables blanking of the screen of the managed device during a Remote Diagnostics session. The managed device keyboard and mouse are always locked during a Remote Diagnostics session. Selecting this option disables the visible signal on the managed device.

Field	Details
Show Warning Message Before Reboot for [ ] Seconds	Displays a warning message on the managed device at the start of the Remote Diagnostics session, reminding the user to save all existing applications. This warning message is displayed for the specified duration to prevent the user from losing any unsaved data, because the remote operator might initiate a system reboot during the Remote Diagnostics session.
Automatically Terminate Remote Diagnostics Session After Inactivity of [ ] Minutes	Terminates the Remote Diagnostics session if it is inactive for the specified duration.

8 Click *Next* to display the Remote Execute Settings page. To accept the default settings, proceed to the next step, or use the information specified in the following table to change the default settings.

Field	Details
Allow programs to be remotely executed on the managed device	Allows programs to be executed remotely on the managed device. Selecting this option enables the subsequent options on the page. Deselecting the option disables the Remote Execute operation on the device.
Ask permission from User on Managed Device Before Starting Remote Execute	Ensures that the remote operator requests permission from the user on the managed device before starting a Remote Execute session.
Give Visible Signal to User on Managed Device During Remote Execute	Displays a visible signal in the top right corner of the managed device desktop during the Remote Execute session. The visible signal lets the user on the managed device know that a Remote Execute session is in progress.
Automatically Terminate Remote Diagnostics Session After Inactivity of [ ] Minutes	Terminates the Remote Execute session if it is inactive for the specified duration.

9 Click *Next* to display the File Transfer Settings page. To accept the default settings, proceed to the next step, or use the information specified in the following tables to change the default security settings.

Field	Details
Allow Transferring Files on Managed Device	Enables transfer of files between the management console and the managed device. Selecting this option enables the subsequent options on the page. Deselecting the option disables the File Transfer operation on the device
Ask permission from User on Managed Device Before Starting File Transfer	Ensures that the remote operator requests permission from the user on the managed device before starting a File Transfer session.
Give Visible Signal to User on Managed Device During File Transfer	Displays a visible signal in the top right corner of the managed device desktop during the File Transfer session. The visible signal lets the user on the managed device know that a File Transfer session is in progress.

Field	Details
Allow Files to be Downloaded from Managed Device	Allows a remote operator to open files on the managed device and transfer them to the management console. If this option is not selected, the remote operator can only transfer files from the management console to the managed device.
File Transfer Root Directory	Specify the managed device directory to be seen by the remote operator during a File Transfer session. The remote operator can only transfer files to and from this directory and its subdirectories. The default directory is My Computer, which means that the remote operator can see and transfer files in the entire file system of the managed device.

10 Click *Next* to display the Security Settings page. To accept the default settings, proceed to the next step, or use the information specified in the following tables to change the default security settings.

Password Authentication

Field	Details
Enable Password Based Authentication	Allows the remote operator to use a password to authenticate to the managed device. Select this option to configure the password type settings.
Minimum Password Length	Allows you to specify the minimum length for the password. By default, it is 6 characters.
Session Password	Select this option to prompt the user on the managed device to set a password before the start of a new remote session. This option is recommended because the password is not stored on the managed device and is valid only for the current session.
Persistent Password	Select this option to set the ZENworks and VNC passwords. Setting the ZENworks Password is recommended because it is safer and more secure than the VNC Password. This password can be set by the administrator through the Remote Management policy or by the managed device user from the ZENworks icon. Selecting this option enables the subsequent options. To enable the user to set the password through ZENworks icon, select the *Allow user to override default passwords on managed device* option.
ZENworks Password	To clear the ZENworks password: 1. Click *Clear Password*. 2. Click *Apply*, then click *OK*. To set the ZENworks password: 1. Click *Set Password*. 2. Enter the password. The maximum length of the password is 255 characters. 3. Click *Apply*, then click *OK*.

Field	Details
VNC Password	To clear the VNC password: 1. Click *Clear Password*. 2. Click *Apply*, then click *OK*. To set the VNC password: 1. Click *Set Password*. 2. Enter the password. The maximum length of the password is 8 characters. 3. Click *Apply*, then click *OK*.

Intruder Detection

Field	Details
Enable Intruder Detection	Select this option to enable the detection of invalid or unauthorized attempts to launch a remote session on the managed device. Selecting this option enables the subsequent options in the Intruder Detection section.
Suspend Accepting Connections After [ ] Successive Invalid Attempts	Specify the maximum number of consecutive invalid attempts a remote operator can make before the Remote Management service on the managed device is blocked. By default, it is five attempts.
Automatically Start Accepting Connections After [ ] Minutes	Specify the time in minutes after which the Remote Management Agent automatically accepts a connection to the managed device. To manually unblock the Remote Management service, double-click the ZENworks Adaptive Agent icon, click *Security Settings*, then click *Enable Accepting Connections if Currently Blocked Due to Intruder Detection.* By default, it is 10 minutes.

Session Security

Field	Details
Enable Session Encryption	Enables session encryption using SSL encryption (TLSv1 protocol). Selecting this option enables the subsequent options in the Session Security section.
Allow Connection When Remote Management Console Does Not Have SSL Certificate	When a remote session is launched from the ZENworks Control Center, a certificate is automatically generated for a remote operator. This certificate is used during authentication. Select this option to allow connections from a Remote Management console launched outside ZENworks Control Center that might not have an SSL certificate.

Field	Details
Allow up to [ ] levels in Viewer certificate chain	The Novell rights-based and password-based authentication schemes are played over an SSL encrypted channel. The establishment of this channel requires the viewer to present a certificate. This certificate can be signed by an intermediate or a root certificate authority, thereby creating a certificate chain. This property defines the maximum number of levels that are allowed in the viewer's certificate chain. When the ZENworks internal certificate authority is employed (it is installed by default), a two-level viewer certificate chain is automatically created while launching a remote session from ZENworks Control Center.

Abnormal Termination

Field	Details
Lock Device	Locks the managed device when the remote session is terminated abnormally.
Log Off User	Logs off the user on the managed device when the remote session is terminated abnormally.

11 Click *Next* to display the Summary page.

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

2.6 Roaming Profile Policy

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

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

2 In the *Policies* list, click *New*, then click *Policy* to display the Select Policy Type page.

3 Select *Roaming Profile Policy*, click *Next* to display the Define Details page, then fill in the fields:

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

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

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

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

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

5 Click *Next* to display the Summary page.

6 Click *Finish* to create the policy now, or select *Define Additional Properties* to specify additional information, such as policy assignment, 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
Add a Community String	Allows you to add a community string.
Community String	Specify the name of the SNMP community string to be added.
Community Rights	Allows you to administer rights for a selected community, such as Read Only, Read & Write, Read & Create, and Notify.
Remove All SNMP Community Strings not specified by ZENworks SNMP Policies	Select this option to remove all the community strings that are not specified through ZENworks SNMP policy.

Field	Details
Send SNMP Authentication Trap	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
Allow SNMP Communication	Select this option to specify whether SNMP communication is allowed from any host or a list of predefined hosts.
Remove All SNMP Allowed Hosts not Specified by ZENworks SNMP Policies	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
Add a Trap Target	Allows you to add a trap target for the SNMP service.
IP Address / Host Name	Specify an IP address or host name of the target device.
Community String	Specify a community string for the trap target defined in *IP address/ Host name*.
Remove All SNMP Trap Targets Not Specified by ZENworks SNMP Policies	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
Apply Policy Only if SNMP Service Exists On the Target Device	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, enforcement, status, and which group the policy is a member of.

2.8 Windows Group Policy

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

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

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

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

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

Field	Details
Select the Type of Group Policy to Manage	With the Windows Group policy, you can manage either a Local group or an Active Directory group policy. Before you can configure the Group policy, you need to install a helper application. Click *Install the Group Policy Helper* to install the `novell-zenworks-grouppolicyhelper-10.0.0.0.msi`, which is a Windows installer package. This installation needs to be done only once. After the helper is installed, clicking *Configure* launches the helper, which you then use to configure or import a policy. ◆ **Local Group Policy:** Select this option to configure a Local Group policy. To launch the group policy helper, click *Configure*. 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 *Configure*. Import an Active Directory Group policy, then upload the ZENworks Server. (You cannot edit an Active Directory policy through ZENworks Control Center.)
Select the Configuration Settings to Be Applied On the Managed Device	After you have adjusted the policy settings as you prefer, you can select how to apply the settings to the managed device. **NOTE:** The Computer Configuration settings from a user associated group policy are not applied when the user logs into a Windows 2000 or Windows 2003 Terminal Server.

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, enforcement, status, and which group the policy is a member of.

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

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

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
Enable Folder View	Use this option to display a folder list in the application window. The values are *Yes*, *No*, and *Unconfigured*. The default value is *Yes*. If you select *Unconfigured*, the existing settings of the managed device are retained.
Expand the Entire Folder Tree	Use this option to expand the entire folder tree when the application window is opened. The values are *Yes*, *No*, and *Unconfigured*. The default value is *Yes*. If you select *Unconfigured*, the existing settings of the managed device are retained.

Field	Details
Display Applications in Windows Explorer	Use this option to display only the application list in Windows Explorer. The values are *Yes*, *No*, and *Unconfigured*. The default value is *Yes*. If you select *Unconfigured*, the existing settings of the managed device are retained.
Name of Root Folder	Use this option to change the name of the root folder.
Enable Manual Refresh	Use this option to specify whether manual refresh of applications is enabled after starting ZENworks Explorer. The values are *Yes*, *No*, and *Unconfigured*. The default value is *Yes*. If you select *Unconfigured*, the existing settings of the managed device are retained.
Allow Logout / Login as a New User	Use this option to enable the user to log out and log in as a new user. The values are *Yes*, *No*, and *Unconfigured*. The default value is *Yes*. If you select *Unconfigured*, the existing settings of the managed device are retained.
Show Progress	Use this option to specify whether the progress of the bundle operations should be displayed. The values are *Yes*, *No*, and *Unconfigured*. The default value is *Yes*. If you select *Unconfigured*, the existing settings of the managed device are retained.
Start the ZENworks Explorer with the {All} Folder Displayed	Use this option to specify whether the [All] folder should be displayed when ZENworks Explorer starts. The values are *Yes*, *No*, and *Unconfigured*. The default value is *Yes*. If you select *Unconfigured*, the existing settings of the managed device are retained.

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, enforcement, status, and which group the policy is a member of.

2.10 Creating Policies by Using the zman Command Line Utility

ZENworks Configuration Management allows you to create different types of policies, such as Browser Bookmarks policy, Dynamic Local User policy, Local File Rights policy, and Printer policy. Each policy has its own set of data and configuration settings. Because it is complex to pass the data as arguments in the command line, the zman utility takes XML files as an input to create policies. You can use the exported XML file as a template to create 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 13.

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

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

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

- Section 2.10.1, “Creating a Policy without Content,” on page 34
- Section 2.10.2, “Creating a Policy with Content,” on page 36
- Section 2.10.3, “Understanding the zman Policy XML File Format,” on page 37

2.10.1 Creating a Policy without Content

1. Create a policy in ZENworks Control Center.

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

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

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

   For example, export the google policy to `google.xml` by using the `zman policy-export-to-file google google.xml` command.

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

3. Modify the XML file according to your requirements.

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

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

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

4 Create a new policy by using the following command:

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

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

2.10.2 Creating a Policy with Content

1. Create a policy in ZENworks Control Center.

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

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

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

   This creates *`policy_filename`*`.xml` and *`policy_filename`*`_ActionContentInfo.xml` files.

   For example, export iPrintPolicy to `iPrintPolicy.xml` by using the `zman policy-export-to-file iPrintPolicy iPrintPolicy.xml` command. The `iPrintPolicy.xml` and `iPrintPolicy_ActionContentInfo.xml` files are created. For more information about `ActionContentInfo.xml`, see Section 2.10.3, "Understanding the zman Policy XML File Format," on page 37.

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

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

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

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

   A sample `iPrintPolicy_actioncontentinfo.xml` is shown below.

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

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

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

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

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

2.10.3 Understanding the zman Policy XML File Format

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

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

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

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

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

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

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

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

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

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

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

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

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

- The Action Set is specified by the type attribute in `<ActionSet>` element. It should be the same as the Action Set type of the policy XML file.

- The `<Action>` element has a name attribute, which is optional, for user readability.

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

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

Managing Policies

3

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

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

3.1 Policy Groups

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

1. In ZENworks Control Center, click the *Policies* tab.
2. In the *Policies* list, click *New*, click *Policy Group* to display the Basic Information page, then fill in the fields:

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

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

   Description: Provide a short description of the policy group's content. This description displays in ZENworks Control Center.
3. Click *Next* to display the Add Group Members page. You can add any number of policies to the group. You cannot add other policy groups to the group.

   To add a policy:

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

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

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

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

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

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

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

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

4 Click *Next* to display the Summary page.

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

3.2 Editing Policies

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

Task	Steps	Additional Details
Edit the content of a policy	1. Click the policy whose content you want to edit. 2. Click the *Details* tab, then edit the settings according to your requirements. 3. Click *Apply*. 4. Click the *Summary* page. 5. Increment the version of the policy to enforce the changes made to the policy on the managed device.	
Rename a policy	1. Select the check box in front of the policy. 2. Click *Edit* > *Rename*, then specify the new name.	If more than one check box is selected, the *Rename* option is not available in the *Edit* menu.
Create a copy of the policy	1. Select the check box in front of the policy. 2. Click *Edit* > *Copy*, then specify a new name.	If more than one check box is selected, the *Copy* option is not available in the *Edit* menu. 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.
Move a policy to a different folder	1. Select the check box in front of the policy (or policies). 2. Click *Edit* > *Move*, then select the target folder.	

Task	Steps	Additional Details
Copy the system requirements of one policy to another policy	1. Select the check box in front of the policy. 2. Click *Edit* > *Copy System Requirements*. 3. Select *Policies*, then click *Add* to select the policies to which you want to copy the selected policy's system requirements.	If more than one check box is selected, the *Copy System Requirements* option is not available in the *Edit* menu.

3.3 Deleting Policies

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

3.4 Adding Policies to Existing Groups

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

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

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

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

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

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

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

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

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

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

5c Click *Next* to skip to Step 7.

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

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

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

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

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

8 Click *Finish*.

3.5 Assigning a Policy to Devices

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

2 In the *Policies* list, select the check box in front of the policy (or policies).

3 Click *Action* > *Assign to Device*.

4 Browse for and select the devices, device groups, and device folders to which you want to assign the group. To do so:

4a Click next to a folder (for example, the `Workstations` folder or `Servers` folder) to navigate through the folders until you find the device, group, or folder you want to select.

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

4b Click the underlined link in the *Name* column to select the device, group, or folder and display its name in the *Selected* list box.

4c Click *OK* to add the selected devices, folders, and groups to the *Devices* list.

5 Click *Next* to display the Policy Conflict Resolution page.

6 Set the priority between device-associated policies and user-associated policies for resolving conflicts that arise when policies of the same type are associated to both devices and users.

- **User Last:** Select this option to apply policies that are associated to devices first and then the users.
- **Device Last:** Select this option to apply policies that are associated to users first and then the devices.
- **Device Only:** Select this option to apply policies that are associated only to devices.
- **User Only:** Select this option to apply policies that are associated only to users.

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

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

8 Click *Finish*.

3.6 Assigning a Policy to Users

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

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

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

1 In ZENworks Control Center, click the *Policies* tab.
2 In the *Policies* list, select the check box in front of 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*.

3.7 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 in front of 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.

3.8 Enabling the Disabled Policies

1. In ZENworks Control Center, click the *Policies* tab.
2. Select the check box in front of 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*.

3.9 Copying a Policy to a Content Server

You can copy only the content associated with the Printer policy or Windows Group policy to a content server.

1. In ZENworks Control Center, click the *Policies* tab.
2. In the *Policies* list, select the check box in front of the Printer policy or the Windows Group policy.
3. Click *Action* > *Specify Content Server*.
4. On the New Servers Added to the System page, specify whether the content (bundles and policies) is replicated to new content servers (ZENworks Servers and Content Distribution Points) that are added to the Management Zone. Choose one of the following two options.
   - **Included:** Replicates the content to any content servers created in the future.
   - **Excluded:** Excludes the content from being replicated to any content servers created in the future.
5. Click *Next* to display the Include or Excluded Content Servers/Distribution Points page.

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

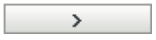
   The relationships between content and content servers that you create using this wizard override any existing relationships.

   To host the content on a content server:

   5a. In the *Excluded Devices* 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 Distribution Point without including it on the Distribution Point's parent ZENworks Server. You must select both the Distribution Point and its parent.

   5b. Click the  button to move the selected content servers to the *Included Devices* 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.

3.10 Incrementing the Policy Version

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

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

3 Click *Action* > *Increment Version.*

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

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

3.11 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*.

Managing Policy Groups

4

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

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

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 Appendix B, "Naming Conventions in ZENworks Control Center," on page 69.

   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 42 or Section 3.6, "Assigning a Policy to Users," on page 43.

4.2 Renaming or Moving Policy Groups

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

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

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

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

2 In the *Policies* list, select the box next to the policy group's name, click *Edit*, then click an option:

Rename: Click *Rename*, provide a new name for the policy group, then click *OK*.

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

4.3 Copying a Policy Group's System Requirements

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

2 In the *Policies* list, select the check box in front of the policy group.

3 Click *Edit* > *Copy System Requirements*.

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

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

4.4 Deleting a Policy Group

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

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

4.5 Assigning a Policy Group to Devices

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

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

4.6 Assigning a Policy Group to Users

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

     If you are looking for a specific item, such as a User or a User Group, you can use the *Items of type* list to limit the types of items that are displayed. If you know the name of the item you are looking for, you can use the *Item name* box to search for the item.
   - **4b** Click the underlined link in the *Name* column to select the user, group, or folder and display its name in the *Selected* list box.

4c Click *OK* to add the selected devices, folders, and groups to the *Users* list.

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

6 Click *Finish*.

4.7 Adding a Policy to a Group

For more information, see Section 3.4, “Adding Policies to Existing Groups,” on page 41.

Managing Folders

5

A folder is an organizational object. You can use folders to structure your polices 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:

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

5.2 Renaming or Moving Folders

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

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

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

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

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

5.3 Copying a Folder's System Requirements

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

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

5.4 Deleting a Folder

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

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

Troubleshooting Policy Management

6

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

6.1 Browser Bookmarks Policy Error Messages

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

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

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

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

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

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

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

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

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

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

Action: Ensure that the Browser Bookmark policy has been correctly created. For more information, see Section 2.1, "Browser Bookmarks Policy," on page 13.

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

6.2 Dynamic Local User Policy Error Messages

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

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

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

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

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

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

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

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

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

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

Action: Turn on debug logging on the managed device and refer to the `zmd-messages.log` file to obtain more details about the error. For more

information on how to turn on debug logging, see the *ZENworks 10 Configuration Management Message Logging Reference*.

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

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

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

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

Action: Review the policy content in ZENworks Control Center. For more information about the Dynamic Local User Policy, see Section 2.2, "Dynamic Local User Policy," on page 14.

6.3 Local File Rights Policy Error Messages

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

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

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

Action: Do the following:

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

There was an error while unenforcing the policy

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

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

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

There was an error while applying the policy *policy_name*

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

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

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

6.4 Printer Policy Error Messages

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Unable to extract iprint client installer from the content

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

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

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

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

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

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

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

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

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

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

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

Failed to add smb printer *printer_name*

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

Possible Cause: The SMB printer connection is not valid.

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

Failed to add iprint printer *printer_name*

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

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

6.5 Printer Policy Troubleshooting Strategies

- "Unable to install a printer driver on Windows managed devices through the Printer Policy" on page 58

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

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

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

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

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

6.6 Roaming Profile Policy Errors

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

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

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

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

6.7 SNMP Policy Errors

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

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

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

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

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

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

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

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

Action: Review the policy content in ZENworks Control Center.

6.8 Windows Group Policy Errors

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

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

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

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

The policy *policy_name* was not applied

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

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

The security settings in policy *policyname* were not applied

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

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

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

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

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

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

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

There was an error while unenforcing Group policy settings

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

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

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

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

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

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

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

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

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

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

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

Some security settings could not be configured

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

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

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

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

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

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

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

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

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

Failure importing group policy settings

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

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

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

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

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

6.9 ZENworks Explorer Configuration Policy Errors

- “There was an error while configuring the setting \" Allow logout/login as new user \"” on page 65

There was an error while unenforcing the policy

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

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

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

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

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

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

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

There was an error while setting the desktop icon name

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.10 Dynamic Local User Policy Troubleshooting Strategies

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

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

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

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

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

Best Practices

A

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

A.1 Local File Rights Policy

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

A.2 Dynamic Local User Policy

- For better results, always use the latest version of Novell Client™. To obtain the latest version, see the Novell Download Web site (http://download.novell.com/index.jsp).

A.3 Roaming Profile Policy

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

A.4 SNMP Policy

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

A.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.

Naming Conventions in ZENworks Control Center

B

When you name an object in ZENworks® Control Center (folders, policies, policy groups, and so forth), ensure that the name adheres to the following conventions:

- The name must be unique in the folder.
- Depending on the database being used for the ZENworks database, uppercase and lowercase letters might not create uniqueness for the same name. The embedded database included with ZENworks Configuration Management is case insensitive, so Folder 1 and FOLDER 1 are the same name and cannot be used in the same folder. If you use an external database that is case-sensitive, Folder 1 and FOLDER 1 are unique.
- If you use spaces, you must enclose the name in quotes when entering it on the command line. For example, you must enclose bundle 1 in quotes (“policy 1”) when entering it in the zman utility.
- The following characters are invalid and cannot be used: / \ * ? : " ' < > | ` % ~

Documentation Updates

C

This section contains information on documentation content changes that were made in this *Administration Guide* after the initial release of Novell® ZENworks® Configuration Management. The information can help you to keep current on updates to the documentation.

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

The documentation update information is grouped according to the date the changes are published. Within a dated section, the changes are alphabetically listed by the names of the main table of contents sections in the guide.

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

The documentation was updated on the following dates:

C.1 January 02, 2007 (Update 1)

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

C.1.1 Creating Polices

The following changes were made in this section:

Location	Change
Section 2.1, “Browser Bookmarks Policy,” on page 13	The file to which the bookmarks are exported should be in UTF-8 format.

C.1.2 Troubleshooting Policy Management

The following changes were made in this section:

Location	Change
Section 6.10, “Dynamic Local User Policy Troubleshooting Strategies,” on page 65	Unable to update the group membership of the user in the Dynamic Local User Policy