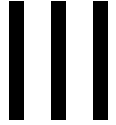


Policy Management



The following sections provide information about Novell® ZENworks® Linux Management Policy Management features and procedures:

- Chapter 11, “Policy Management Overview,” on page 71
- Chapter 12, “Understanding Policies,” on page 73
- Chapter 13, “Creating Policies,” on page 77
- Chapter 14, “Managing Policies,” on page 123

Policy Management Overview

11

Novell® ZENworks® Linux Management lets you configure operating system settings and select application settings through the use of policies. By applying a policy to multiple devices, you can ensure that the devices have the same configuration. In addition, if you change a policy after it has already been applied to a device, the policy is reapplied to the device according to the defined schedule.

The following sections contain additional information:

- [Section 11.1, “Understanding Policies,” on page 71](#)
- [Section 11.2, “Creating Policies,” on page 71](#)
- [Section 11.3, “Managing Policies,” on page 72](#)

11.1 Understanding Policies

Before you start creating policies, you should have a basic understanding of policies, know the basic terminology, and know the different types of policies available in ZENworks Linux Management. For more information, see [Chapter 12, “Understanding Policies,” on page 73](#).

11.2 Creating Policies

ZENworks Linux Management Policies give you the ability to define and lockdown configuration settings on managed devices (servers and workstations). ZENworks Linux Management provides policies for a number of popular applications, including the Novell Linux Desktop. It also includes a policy to execute script, binary, or Java files and a policy to apply changes to text files.

ZENworks Linux Management lets you create the following policies:

Table 11-1 ZENworks Linux Management Policies

Policy	Description
Epiphany Policy	Configures the Epiphany* Web browser. For step-by-step instructions to create this policy, see Section 13.1, “Epiphany Policy,” on page 77 .
Evolution Policy	Configures the Evolution™ e-mail client. For step-by-step instructions to create this policy, see Section 13.2, “Evolution Policy,” on page 83 .
Firefox Policy	Configures the Firefox* Web browser. For step-by-step instructions to create this policy, see Section 13.3, “Firefox Policy,” on page 90 .
Generic GNOME Policy	Configures the GNOME-based applications. For step-by-step instructions to create this policy, see Section 13.4, “Generic GNOME Policy,” on page 97 .
Novell Linux Desktop Policy	Configures the Novell Linux Desktop settings. For step-by-step instructions to create this policy, see Section 13.5, “Novell Linux Desktop Policy,” on page 103 .

Policy	Description
Remote Execute Policy	Executes a script, binary, or Java file. For step-by-step instructions to create this policy, see Section 13.6, “Remote Execute Policy,” on page 111 .
Text File Policy	Applies changes to a text file. For step-by-step instructions to create this policy, see Section 13.7, “Text File Policy,” on page 116 .

NOTE: The Epiphany, Evolution, Firefox, Generic GNOME, and Novell Linux Desktop policies are referred as GConf-based policies.

11.3 Managing Policies

In addition to creating policies, as described in [Chapter 13, “Creating Policies,” on page 77](#), you can create folders to organize policies, create policy groups to ease administration of policies, assign policies to devices, edit existing policies, and more.

For more information, see [Chapter 14, “Managing Policies,” on page 123](#).

Novell® ZENworks® Linux Management policies provide a mechanism of uniformly configuring applications. ZENworks policies let you configure system and application settings and then set them as Lockdown or Default. Lockdown lets you restrict users from changing settings, so the application must use the values that are configured in the policy. Default lets users change settings.

A policy applies to all users on assigned devices. You can use the Lockdown and Default mechanisms to configure applications in such a way that critical and important settings are locked and an appropriate default value is provided for other settings that might be relevant. Also, if you do not want to enforce a particular setting, you can exclude that setting while creating or editing a policy.

You can also use policies to modify configuration files and execute scripts or programs on managed devices.

Policies can be used to create a set of configurations that you can deploy on any number of managed devices, thereby providing the devices with a uniform configuration and eliminating the need to configure each device separately. You can also create policies with different settings and assign them appropriately to give a different configuration to a specific set of devices.

On managed devices, each policy type is enforced by a Policy Handler/Enforcer, which makes all the configuration changes necessary to enforce and unenforce the settings in a given policy. The Policy Handler/Enforcer executes with root privileges.

The following sections provide basic concepts you should understand as you begin using policies:

- [Section 12.1, “Types of Policies,” on page 73](#)
- [Section 12.2, “Assignments,” on page 74](#)
- [Section 12.3, “Schedules,” on page 74](#)
- [Section 12.4, “Groups,” on page 75](#)
- [Section 12.5, “System Requirements,” on page 75](#)
- [Section 12.6, “Effective Policies,” on page 76](#)

12.1 Types of Policies

ZENworks lets you create the following types of policies:

- **Epiphany policy:** Lets you disable certain Epiphany* Web browser settings, such as automatic downloading and opening of files, loading contents from unsafe protocols, and accessing the browser's History. The Epiphany policy also lets you configure a default home page, configure cookie settings, and more. For step-by-step instructions to create this policy, see [Section 13.1, “Epiphany Policy,” on page 77](#).
- **Evolution policy:** Lets you disable certain Evolution™ e-mail client settings, such as signatures, showing only subscribed folders, and overriding the server-supplied folder namespace. The Evolution policy also lets you configure image settings, junk e-mail settings, Mime types settings, and more. For step-by-step instructions to create this policy, see [Section 13.2, “Evolution Policy,” on page 83](#).

- **Firefox policy:** Lets you disable certain Firefox* Web browser settings, such as saving passwords and updating themes and extensions. The Firefox policy lets you configure pop-ups, JavaScript control, and more. For step-by-step instructions to create this policy, see [Section 13.3, “Firefox Policy,” on page 90](#).
- **Generic GNOME policy:** Lets you configure GConf-based applications. You can import settings from a device that is registered with the ZENworks Linux Management Server or you can define your own GConf settings. While importing settings from a device, the system imports all settings, including default settings, from that device. You must specify the name of a user on the device from where you are importing the GConf settings. Only those GConf settings are imported that are related to the user you have specified. For step-by-step instructions to create this policy, see [Section 13.4, “Generic GNOME Policy,” on page 97](#).
- **Novell Linux Desktop policy:** Lets you configure the Novell Linux Desktop settings. This policy lets you remove certain items from the system menu, program menu, and personal settings. It also lets you configure background image settings, shade settings, proxy settings, and more. For step-by-step instructions to create this policy, see [Section 13.5, “Novell Linux Desktop Policy,” on page 103](#).
- **Remote Execute policy:** Executes a script, binary, or Java file. The Remote Execute policy also lets you specify your own script to be executed on managed devices. For step-by-step instructions to create this policy, see [Section 13.6, “Remote Execute Policy,” on page 111](#).
- **Text File policy:** Applies changes to a text file. The Text File policy lets you append or prepend to a file and also lets you apply a search-based change in which a given string in the file can be replaced with another string, be deleted, and so forth. The search string can be specified using a regular expression.

This policy also allows you to execute a script, binary, or Java program before and after the text-file modification. It can be used for example, to change a configuration file. You might want to stop a service before the file is modified and restart the service after the file modification.

While creating a policy, only one file and one change can be specified. Editing a policy allows you to add multiple files and specify more than one change to a file. For step-by-step instructions to create this policy, see [Section 13.7, “Text File Policy,” on page 116](#).

12.2 Assignments

You can assign a policy directly to a device, or you can assign it to a folder or group in which the device is a member. As a general rule, you should try to assign policies to device groups rather than device folders.

12.3 Schedules

When assigning a policy to a device, you can specify the schedule for applying the policy. Depending on the type of policy being applied, the following schedules are available. Click the link in the left frame for details about each policy and its options, which vary, depending on the schedule.

Table 12-1 Available Schedules

Schedule Type	Description	Applicable For
No Schedule	Use this option to indicate no schedule; no action occurs.	All policies
Date Specific	Select one or more dates on which to enforce the policy on devices and set other restrictions that might apply.	Remote Execute and Text File policies
Day of the Week Specific	Select one or more days of the week on which to enforce the policy on devices and set other restrictions that might apply.	Remote Execute and Text File policies
Event	Select the event that triggers the enforcement of the policy.	Epiphany, Evolution, Firefox, Generic GNOME, and Novell Linux Desktop policies.
Monthly	Select the day of the month on which to enforce the policy on devices and set other restrictions that might apply.	Remote Execute and Text File policies
Relative to Refresh	Schedule when the policy is enforced, either immediately after the device refreshes or a specified amount of time after the device refreshes. You can also specify whether the policy's enforcement is repeated and specify a time period when you do not want the policy enforced to help minimize network traffic during that time. For more information, see Section 14.9, "Refreshing Policies," on page 142.	Remote Execute and Text File policies

12.4 Groups

A policy group is a collection of one or more policies. You can create policy groups and assign them to devices the same way you would assign individual policies.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see [Section 14.3, "Creating Policy Groups,"](#) on page 125.

12.5 System Requirements

System requirements specify the conditions that must be satisfied on the managed device for the policy to be effective. System requirements are specified for each policy to ensure that the conditions necessary for a proper enforcement of a policy are met.

The appropriate default system requirements are included in a policy when it is created. When you create or edit a policy, you can modify or remove the requirements. No default system requirement is available for the Text File and Remote Execute policies.

You can change the system requirement setting if the settings included in the policy are available on different versions or platforms. If not, all the settings configured in the policy are not effective. For example, if the Distribution \geq Novell Linux Desktop 9 requirement is removed from the Firefox policy and the policy is specified to be enforced on all platforms, the settings are not effective because the lockdown option for Firefox is available only for the Novell Linux Desktop.

You should remove the system requirement only if you are sure that it will not cause problems. For example, in a Generic GNOME policy created by importing settings from a device, the system requirement is set to the operating system of the device from which the settings were imported. If you have included settings in the policy that are available on other platforms, you can remove or change the system requirement.

IMPORTANT: Even if the requirements are removed and the application version or operating system is incompatible, the policy is enforced but a warning message is generated. If the appropriate application (Epiphany, Evolution, or Firefox) is not installed, the policy is not enforced and an error message is generated.




12.6 Effective Policies

A device inherits its policy assignments from its parent folders, its group memberships, and itself; when conflicting assignments occur, the assignments on the device override group assignments, which override folder assignments.

You can tell which policies are in effect for a device by viewing the Effective Policies section on the Device Summary page. To view the effective policies, click the *Devices* page, navigate the folders to find the device, click the device, then click the *Summary* tab.

All the effective policies are listed under the Effective Policies section on the Device Summary page. The following table provides a description of each icon that indicates the effectiveness of a policy:

Table 12-2 Policy Status Icons

Icon	Description
	The policy is effective and will be enforced on the device.
	The policy might be effective. The policy will be enforced if the system requirements are met. Otherwise, the policy will not be enforced.
	The policy is not effective and will not be enforced.

For GConf-based policies, the first policy amongst the effective policies, whose system requirements are met, is applied on the device.

For the Text File and Remote Execute policies, all policies whose system requirements are met are applied on the device.

Novell® ZENworks® Linux Management lets you configure operating system settings and select application settings through the use of policies. By applying a policy to multiple devices, you can ensure that the devices have the same configuration. In addition, if you change a policy after it has already been applied to a device, the policy is reapplied to the device as per the defined schedule.

The following sections contain additional information about the available ZENworks Linux Management policies:

- [Section 13.1, “Epiphany Policy,” on page 77](#)
- [Section 13.2, “Evolution Policy,” on page 83](#)
- [Section 13.3, “Firefox Policy,” on page 90](#)
- [Section 13.4, “Generic GNOME Policy,” on page 97](#)
- [Section 13.5, “Novell Linux Desktop Policy,” on page 103](#)
- [Section 13.6, “Remote Execute Policy,” on page 111](#)
- [Section 13.7, “Text File Policy,” on page 116](#)

13.1 Epiphany Policy

The Epiphany policy is used to configure the Epiphany Web browser.

To configure the Epiphany policy:

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

- 3 In the Policy type list, click *Epiphany Policy*, then click *Next* to display the Policy Name page.

Create New Epiphany Policy ?

Step 2: Policy Name

Specify the name of the new policy:

Policy Name: *

Folder: *

/Policies

Description:

Fields marked with a blue asterisk are required.

<< Back Next >> Cancel

- 4 Fill in the fields:

- **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.
- **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.
- **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

5 Click *Next* to display the Epiphany Lockdown Settings page.

Create New Epiphany Policy Epiphany ?

Step 3: Epiphany Lockdown settings

Select the Epiphany settings:

- ☐ Disable Javascript control of window chrome
- ☐ Hide menu bar
- ☐ Disable automatic download and opening of files
- ☐ Disable manual URL entry
- ☐ Disable bookmark editing
- ☐ Disable toolbar editing
- ☐ Disable history
- ☐ Disable loading of content from unsafe protocols. Default safe protocols are HTTP and HTTPS

Safe Protocols list:

^

...

v

Add ...

Remove

<< Back

Next >>

Cancel

6 Select the desired options (by default, all options are disabled):

Disable JavaScript control of window chrome: Select this option to disable the JavaScript control and modification of the Epiphany Web browser's window chrome.

The chrome is part of an application window that is positioned outside of the window's content area. A Web page can use JavaScript to control and modify the window chrome. Several elements such as the toolbar, menu bar, progress bar, and title bar are part of the chrome.

Hide menu bar: Select this option to hide the menu bar of the Epiphany Web browser.

Disable automatic download and opening of files: Select this option to prevent users from downloading and opening files automatically.

If you include this setting in the policy, users are always asked if they want to save a file or open it. For example, if users want to download a file, they are prompted to specify the location to save or open the file. If the user clicks *Open*, the file is downloaded and opened with the corresponding application.

Disable manual URL entry: Select this option to prevent users from manually entering URLs in the address bar.

Disable bookmark editing: Select this option to prevent users from editing a bookmark.

Disable toolbar editing: Select this option to prevent users from editing the toolbar. A toolbar can contain buttons with images and menus, or a combination of both.

Disable history: Select this option to prevent users from accessing the history, which contains links to pages recently visited.

Disable loading of contents from unsafe protocols. Default safe protocols are HTTP and HTTPS: Select this option to prevent the downloading of data that is transmitted using an unsafe protocol. Unsafe protocols do not encrypt the data sent across a network.

After you check this option, the following buttons are available:

- **Add:** To add a protocol to the *Safe protocol* list, click *Add*, specify a protocol name, then click *OK*.
- **Remove:** To remove a protocol from the *Safe protocol* list, select the protocol, then click *Remove*.

7 Click *Next* to display the Epiphany Configuration Settings page.

Create New Epiphany Policy Epiphany ?

Step 4: Epiphany Configuration settings

Select any Epiphany configuration settings you would like to provide.
For each setting you select, provide a value, and optionally, enable the lock to prevent the value from changing after it is set.

<input type="checkbox"/> Homepage URL		<input type="text"/>
<input type="checkbox"/> Download folder *		<input type="text"/>
<input type="checkbox"/> Allow Popups		Yes ▾
<input type="checkbox"/> Allow Java		Yes ▾
<input type="checkbox"/> Allow Javascript		Yes ▾
<input type="checkbox"/> Cookies		Always Accept ▾
<input type="checkbox"/> Disk space for temporary files		50 MB

Fields marked with a blue asterisk are required.

<< Back Next >> Cancel

8 Select the desired options (by default, all options are disabled).

For each option you enable, provide a value. When you enable an option, it is locked by default. You can unlock the option by clicking . The options that are not enabled are excluded from the policy and are not applied to the device.

Homepage URL: Specify the URL to automatically display when users launch the Epiphany Web browser.

Download folder: Specify the directory where you want users to download data. If the folder you specify does not exist, it is created relative to all users' home directories. If you specify an absolute path, ensure that it is at a location where all users have Read and Write access to files.

Allow popups: Select this option to allow or disallow pop-ups to be displayed in the Epiphany Web browser.

Allow Java: Select this option to allow or disallow Java applications to run on the Epiphany Web browser.

Allow JavaScript: Select this option to allow or disallow JavaScript applications to run on the Epiphany Web browser.

Cookies: Select this option to configure how the Epiphany Web browser handles cookies.

A cookie is a piece of information given to a Web browser by a Web server. The browser, in turn, stores this information in a file. The available options are *Always accept*, *Only from the sites you visit*, and *Never accept*.

Disk space for temporary files: Specify the amount of disk space to allow for storing temporary files for the browser.

- 9 Click *Next* to display the Default System Requirements for Epiphany Policy page.

Create New Epiphany Policy Epiphany ?

Step 5: Default system requirements for Epiphany policy

The following condition is added as a default system requirement to this policy.
If the minimum supported version requirement is removed or modified then the policy may not be fully applied and effective on the target device.

☒ Apply policy on devices with version of Epiphany >= 1.2.5 *

Fields marked with a blue asterisk are required.

<< Back Next >> Cancel

- 10 Specify the minimum system requirements that must be satisfied for the Epiphany Web browser policy settings to be effective.

The *Apply policy on devices with version of Epiphany* field displays the minimum version of the Epiphany Web browser required for all policy settings to be effective. Epiphany 1.2.5 is the minimum required version. Policy settings are applied only if the user has the same or later version of the Epiphany Web browser installed. If the user does not have the Epiphany Web browser installed or has an earlier version than the specified version, the policy does not apply.

Even if you do not include this system requirement in the policy, the system checks whether the Epiphany Web browser is installed on a managed device or not. If the system finds that the Epiphany Web browser is installed on a device, it also checks the version. If it finds an earlier version than the specified one, the policy is enforced but a warning message is generated. If the Epiphany Web browser is not installed on a managed device, the policy is not enforced and an error message is generated.

- 11 Click *Next* to display the Summary page.
- 12 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the Epiphany policy is created but it does not have devices assigned or a schedule specified. At some point in the future, you need to configure additional options for the policy by continuing with [Section 14.4, “Assigning Policies,” on page 128](#).


or

Click *Next* to display the Policy Assignment page to perform the following tasks:

- Specify assignments for this policy

- Specify the schedule for this policy
- Specify groups for this policy

Create New Epiphany Policy **Epiphany** ?

 **Step 7: Policy Assignments**

Specify the assignments for this policy:

Add Remove	
<input type="checkbox"/> Name	In Folder
No items selected, click add to select items	

13 Assign the policy to the devices.

13a Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.


13b Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

13c Click *OK*.

14 Click *Next* to display the Policy Schedule page.

Create New Epiphany Policy **Epiphany** ?

 **Step 8: Policy Schedule**

Select the schedule to apply to the policy assignments:

Schedule Type:

▼

15 Select the schedule to apply to the assignments from the drop-down list, then select the desired options, which vary, depending on the schedule type you select.

The settings you configure on this page determine when the policy is applied to devices.

See [Section 12.3, “Schedules,” on page 74](#) for information about the available schedules and their options.

- 16 Click *Next* to display the Policy Groups page.

Create New Epiphany Policy Epiphany ?

Step 9: Policy Groups

Specify the groups for this policy:

Add	Remove	Name	In Folder
No items selected, click add to select items			

<< Back Next >> Cancel

- 17 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the Name column to select the desired policy groups and display their names in the Selected list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see [Section 14.3, “Creating Policy Groups,” on page 125](#).

- 18 Click *Next* to display the Finish page.
- 19 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured according to the settings on the Finish page.

13.2 Evolution Policy

The Evolution policy is used to configure the Evolution e-mail client.

To configure the Evolution policy:

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

- 3 In the Policy Type list, click *Evolution Policy*, then click *Next* to display the Policy Name page.

Create New Evolution Policy www ?

Step 2: Policy Name

Specify the name of the new policy:

Policy Name: *

Folder: *

/Policies

Description:

Fields marked with a blue asterisk are required.

<< Back Next >> Cancel

- 4 Fill in the fields:

- **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.
- **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.
- **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

5 Click *Next* to display the Evolution Lockdown Settings page.

Create New Evolution Policy Evolution ?

Step 3: Evolution Lockdown Settings

Select the Evolution Mail Client settings that you do not want your users to change:

- ☐ Apply filters to new messages option
- ☐ Secure Socket Layer (SSL) option
- ☐ E-mail signature
- ☐ E-mail server authentication method
- ☐ Automatically check for new mail option
- ☐ Sent and draft mail folder locations
- ☐ Save password option
- ☐ Receive mail configuration
- ☐ Send mail configuration
- ☐ Show only subscribed folders (for IMAP Mail Accounts)
- ☐ Override server-supplied folder namespace (for IMAP Mail Accounts)

<< Back Next >> Cancel

6 Select the desired options (by default, all options are disabled):

The options on this page allow you to prevent users from changing the following Evolution e-mail client settings. Select an option to prevent users from changing that setting in the Evolution e-mail client.

Apply filter to new messages option: Applies the filter to all new messages users receive.

Secure Socket Layer (SSL) option: Specifies whether the Evolution e-mail client should connect to the server using SSL.

SSL is a protocol that provides encrypted communications on the network and enables secure communications between the Evolution client and the server.

E-Mail signature: Specifies whether an e-mail signature should be added to the contents of a message.

E-mail server authentication method: Specifies the kind of authentication to be used when users connect to the mail server.

Automatically check for new mail option: Specifies whether the Evolution client should automatically check for new mail.

Sent and draft mail folder locations: Specifies which folders users can select to store draft and sent mail.

Save password option: Specifies whether passwords should be saved so that users are not prompted for a password at every login.

Receive mail configuration: Configures the various options for receiving mail. For example, e-mail server and authentication details, checking for new mails, and applying filters.

Send mail configuration: Configures the various options for sending mail, for example, server and authentication details.

Show only subscribed folders (for IMAP mail accounts): Specifies that only the subscribed IMAP folders be shown to users. Internet Message Access Protocol (IMAP) lets users access e-mail messages that are stored on the mail server. Because the mail folders exist on the IMAP server and accessing them is time-consuming, Evolution lets users subscribe to certain IMAP folders.


Override server-supplied folder namespace (for IMAP mail accounts): Lets users change the IMAP name space that contains mail messages for the server.

NOTE: Users cannot create a new Evolution e-mail account if Receive Mail Configuration and Send Mail Configuration settings are included in the policy. These settings should be included in the policy only if the users' e-mail accounts have been created in the Evolution e-mail client.

- 7 Click *Next* to display the Evolution Configuration Settings page.








Create New Evolution Policy

Evolution

 **Step 4: Evolution Configuration Settings**

Select any e-mail configuration setting you would like to provide.

For each setting you select, provide a value, and optionally, enable the lock to prevent the value from changing after it is set.

<input type="checkbox"/>	Default character encoding for display		Western European (ISO-8859-1)
<input type="checkbox"/>	Default character encoding for composed mail		Western European (ISO-8859-1)
<input type="checkbox"/>	Empty Trash folders on exit		Never
<input type="checkbox"/>	Check inbox for junk mail		Yes
<input type="checkbox"/>	Include remote junk mail tests		No
<input type="checkbox"/>	Loading Images		Never load images off the net
<input type="checkbox"/>	Mime Types available for viewing Attachments		

Mime Types available

application/andrew-inset
application/msword
application/octet-stream
application/oda
application/pdf
application/pgp


Mime Types selected

<< Back

Next >>

Cancel

- 8 Select the desired options (by default, all options are disabled).

For each option you enable, provide a value. When you enable an option, it is locked by default. You can unlock the option by clicking . The options that are not enabled are excluded from the policy and are not applied to the device.

Default character encoding for display: Lets you choose a character interpretation set for displaying e-mail messages. The default character interpretation set is Western European (ISO-8859-1).

Default character encoding for composed mail: Lets you choose a character interpretation set for composing e-mail messages. The default character interpretation set is Western European (ISO-8859-1).

Empty trash folders on exit: Lets you specify when to empty the Trash folder. The available options are Never, Every time, Once per day, Once per week, and Once per month.

Check inbox for junk mail: Lets you specify if the incoming mail must be checked for junk mail.

Include remote junk mail tests: Lets you specify if the remote junk filtering option should be used for filtering incoming mail.

For example, the Evolution client stores a message in the Junk Mail folder if it finds the mail address a blacklisted address.

Loading Images: Lets you decide how images embedded in e-mail messages are loaded in the Evolution client.

The following options are available:

- **Never load images off the Internet:** If you select this option, the Evolution e-mail client never loads images. If you select this option users can still view the images in the message by selecting the appropriate menu options in the Evolution e-mail client.
- **Load images if sender is in address book:** If you select this option, images are loaded only if the sender of the e-mail message is in the receiver's address book.
- **Always load images off the Internet:** If you select this option, images are loaded regardless of their source.

Mime types available for viewing attachments: Lets you select the MIME types that Evolution allows to be viewed using available Bonobo controls.

Evolution provides built-in support for opening certain MIME types. Those MIME types that are not supported by Evolution can be viewed by using certain available Bonobo controls. Bonobo controls provide a means to view both the MIME types that are supported and those that are not supported by Evolution.

After you select this option, you can select items from the *Mime types available* list and then use the arrow button to move the selected item to the *Mime types selected* list.

- 9 Click *Next* to display the Default System Requirements for Evolution Policy page.

The screenshot shows a dialog box titled 'Create New Evolution Policy' with a sub-tab 'Evolution'. Below the title bar, it says 'Step 5: Default system requirements for Evolution policy'. The main text area contains the following information:

The following condition is added as a default system requirement to this policy.
If the minimum supported version requirement is removed or modified then the policy may not be fully applied and effective on the target device.

There is a checked checkbox followed by the text 'Apply policy on devices with version of Evolution >= ' and a text input field containing '2.0.1'. A blue asterisk is to the right of the input field.

Below this, it says 'Fields marked with a blue asterisk are required.'

At the bottom, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.

- 10 Specify the minimum system requirements that must be satisfied for the Evolution policy settings to be effective.

The *Apply policy on devices with version of Evolution* field displays the minimum version of the Evolution client required for all policy settings to be effective. Evolution 2.0.1 is the minimum required version. Policy settings are applied only if the user has the same or a later version of the Evolution e-mail client installed. If the user does not have the Evolution e-mail client installed or has an earlier version than the specified version, the policy does not apply.

Even if you do not include this system requirement in the policy, the system checks whether the Evolution client is installed on a managed device or not. If the system finds the Evolution client on a device, it also checks the version. If it finds an earlier version than the specified one, the policy is enforced but a warning message is generated. If the Evolution client is not installed on a managed device, the policy is not enforced and an error message is generated.

- 11 Click *Next* to display the Summary page.
- 12 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the Evolution policy is created but it does not have devices assigned or a schedule specified. At some point in the future, you need to configure additional options for the policy by continuing with [Section 14.4, “Assigning Policies,” on page 128](#).
- or

Click *Next* to display the Policy Assignment page to perform the following tasks:

- Specify assignments for this policy
- Specify the schedule for this policy
- Specify groups for this policy

Create New Evolution Policy

Evolution

?

Step 7: Policy Assignments

Specify the assignments for this policy:

Add	Remove
<input type="checkbox"/>	<div>Name</div> <div>In Folder</div>
No items selected, click add to select items	

<< Back

Next >>

Cancel

13 Assign the policy to the devices.

13a Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

13b Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

13c Click *OK*.

14 Click *Next* to display the Policy Schedule page.

Create New Evolution Policy

Evolution

?

Step 8: Policy Schedule

Select the schedule to apply to the policy assignments:

Schedule Type:

No Schedule

<< Back

Next >>

Cancel

15 Select the schedule to apply to the assignments from the drop-down list, then select the desired options, which vary, depending on the schedule type you select.

The settings you configure on this page determine when the policy is applied to devices.

See [Section 12.3, “Schedules,” on page 74](#) for information about the available schedules and their options.

- 16 Click *Next* to display the Policy Groups page.

Create New Evolution Policy Evolution ?

Step 9: Policy Groups

Specify the groups for this policy:

Add	Remove	Name	In Folder
No items selected, click add to select items			

<< Back Next >> Cancel

- 17 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the Name column to select the desired policy groups and display their names in the Selected list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see [Section 14.3, “Creating Policy Groups,” on page 125](#).

- 18 Click *Next* to display the Finish page.
- 19 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured according to the settings on the Finish page.

13.3 Firefox Policy

The Firefox policy is used to configure the Mozilla* Firefox* Web browser.

The Firefox policy is supported only if the lockdown version of Firefox is available on the Novell Linux Desktop.

To configure the Firefox policy:

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

3 In the Policy Type list, click *Firefox Policy*, then click *Next* to display the Policy Name page.

Create New Firefox Policy ?

Step 2: Policy Name

Specify the name of the new policy:

Policy Name: *

Folder: *

/Policies

Description:

Fields marked with a blue asterisk are required.

<< Back Next >> Cancel

4 Fill in the fields:

- **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.
- **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.
- **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

- 5 Click *Next* to display the Firefox Lockdown Settings page.

Create New Firefox Policy Firefox ?

Step 3: Firefox Lockdown settings

Select the Firefox settings:

- ☐ Disable Javascript control of window chrome
- ☐ Disable URL bar
- ☐ Disable web search
- ☐ Disable bookmark editing
- ☐ Hide bookmarks
- ☐ Disable toolbar editing
- ☐ Disable history
- ☐ Disable saving of passwords
- ☐ Disable updates to themes
- ☐ Disable updates to extensions

<< Back Next >> Cancel

- 6 Select the desired options (by default, all options are disabled):

Disable Javascript control of window chrome: Select this option to disable the JavaScript control and modification of the Firefox Web browser's window chrome.

The chrome is part of an application window that is positioned outside of the window's content area. A Web page can use JavaScript to control and modify the window chrome. Several elements such as the toolbar, menu bar, progress bar, and title bar are part of the chrome.

Disable URL bar: Select this option to prevent users from manually entering URLs in the address bar.

Disable web search: Select this option to prevent users from using the Web search bar to search the Web pages. If you select this option, the search bar and Add Engine option are disabled.

Disable bookmark editing: Select this option to prevent users from editing a bookmark.

Hide bookmarks: Select this option to hide bookmarks, including all the bookmarks listed in the Bookmark menu and bookmarks toolbar. Make sure that you select Disable Bookmark Editing if you select the Hide Bookmarks option.

Disable toolbar editing: Select this option to prevent users from editing the toolbar. A toolbar can contain buttons with images and menus, or a combination of both.

Disable history: Select this option to prevent users from accessing the History, which contains links to pages recently visited.

Disable saving of password: Select this option to prevent Firefox from saving users' passwords. Whenever a user enters a password in Firefox, it prompts the user and asks if the password should be saved. If the user clicks Yes, Firefox saves the password and fills it in automatically whenever the user visits that page again.

Disable updates to themes: Select this option to prevent users from updating a theme file.

The theme file contains the Control, Window Border, and Icons elements, which determine the appearance of user's browser. Themes are skins for Firefox, and they allow you to change the look and feel of the browser and personalize it to your taste. A theme can simply change the colors of Firefox or it can change the entire browser appearance.

Disable updates to extensions: Select this option to prevent users from updating the extensions to add a new functionality to Firefox.

Extensions are add-ons that add new functionality to Firefox. They can add anything from a toolbar button to a completely new feature. Extensions customize the browser to fit the personal needs of each user. For example, an extension can be used to add an IRC client to Firefox or to automatically copy highlighted content to the clipboard.

7 Click *Next* to display the Firefox Configuration Settings page.

Create New Firefox Policy Firefox ?

Step 4: Firefox Configuration settings

Select any Firefox configuration settings you would like to provide.
For each setting you select, provide a value, and optionally, enable the lock to prevent the value from changing after it is set.

☐ Homepage URL

☐ Allow Popups Yes ▾

☐ Allow Java Yes ▾

☐ Allow Javascript Yes ▾

☐ Allow sites to set cookies Yes ▾

☐ Keep Cookies ▾

☐ Allow loading of images Anywhere ▾

☐ Disk space for temporary files 50 MB

☐ Download Folder

☒ Ask the user where to save every file

☐ Save all files to this folder ▾

Folder path *

Fields marked with a blue asterisk are required.

<< Back Next >> Cancel

8 Select the desired options (by default, all options are disabled).

For each option you enable, provide a value. When you enable an option, it is locked by default. You can unlock the option by clicking . The options that are not enabled are excluded from the policy and are not applied to the device.

Homepage URL: Specify the URL to automatically display when users launch the Firefox Web browser.

Allow popups: Select this option to allow or disallow pop-ups to be displayed in the Firefox Web browser.

Allow Java: Select this option to allow or disallow Java applications to run on the Firefox Web browser.

Allow JavaScript: Select this option to allow or disallow JavaScript applications to run on the Firefox Web browser.

Allow sites to set cookies: Select this option to configure how Firefox handles cookies.

A cookie is a piece of information given to a Web browser by a Web server. The browser stores this information in a file.

You can select a value in the Keep Cookies drop-down list to specify if a Web server should be allowed to set cookies.

If you select Yes, specify how long to store the cookies:

- **Until they expire:** Firefox retains a cookie until it expires.
- **Ask me every time:** Firefox asks the user about the action to be taken with each cookie. Users can select *Allow*, *Allow for this session only*, or *Deny*.
- **Until I close Firefox:** Firefox retains cookies while the browser is open. When the browser is closed, Firefox removes all cookies.

Allow loading of images: Lets you specify the source from where images are loaded.

The following options are available:

- **Anywhere:** If you select this option, images are loaded regardless of their source.
- **From originating website only:** If you select this option, images are loaded only if the source of the images is the current site.
- **Never:** If you select this option, Firefox never loads images.

Disk space for temporary files: Specify the disk space allowed to store temporary files for the browser.

Download folder: Lets you specify the directory where you want users to save downloaded files.

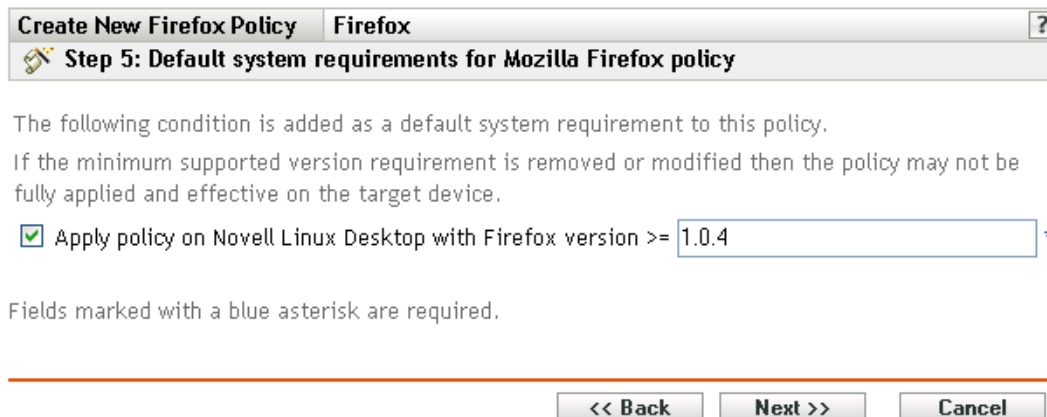
The following options are available:

- **Ask the user where to save every file:** If you select this option, Firefox asks the users where to save files every time files are downloaded.
- **Save all files to this folder:** If you select this option, specify a location to save files.

The following options are available:

- **Desktop:** Select Desktop to save downloaded files on the Desktop.
- **My Downloads:** Select My Downloads to save downloaded files in the My Downloads folder.
- **Home:** Select Home to save the downloaded files in a folder in the Home directory.
- **Other:** Select Other to store the downloaded files in a location of your choice. Specify the complete path, including the directory where the downloaded files should be saved.

- 9 Click *Next* to display the Default System Requirements for Mozilla Firefox policy page.



Create New Firefox Policy Firefox ?

Step 5: Default system requirements for Mozilla Firefox policy

The following condition is added as a default system requirement to this policy.

If the minimum supported version requirement is removed or modified then the policy may not be fully applied and effective on the target device.

☒ Apply policy on Novell Linux Desktop with Firefox version >= 1.0.4 *

Fields marked with a blue asterisk are required.

<< Back Next >> Cancel

- 10 Specify the minimum system requirements that must be satisfied for the Firefox Web browser policy settings to be effective.

The *Apply policy on Novell Linux Desktop with Firefox version* field displays the minimum version of Firefox required for all policy settings to be effective. Firefox 1.0.4 is the minimum required version. Policy settings are applied only if user has the same version or a later version of Firefox installed. If the user does not have Firefox installed or has an earlier version than the specified version, the policy does not apply.

Even if you do not include this system requirement in the policy, the system checks whether Firefox is installed on a managed device or not. If the system finds that Firefox is installed on a device, it also checks the version. If it finds an earlier version than the specified one, the policy is enforced but a warning message is generated. If Firefox is not installed on a managed device, the policy is not enforced and an error message is generated.

- 11 Click *Next* to display the Summary page.
- 12 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the Firefox policy is created but it does not have devices assigned or a schedule specified. At some point in the future, you need to configure additional options for the policy by continuing with [Section 14.4, “Assigning Policies,” on page 128](#).

or

Click *Next* to display the Policy Assignment page to perform the following tasks:

- Specify assignments for this policy
- Specify the schedule for this policy
- Specify groups for this policy

Create New Firefox Policy Firefox ?

Step 7: Policy Assignments

Specify the assignments for this policy:

Add	Remove	Name	In Folder
No items selected, click add to select items			

<< Back Next >> Cancel

13 Assign the policy to the devices.

13a Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

13b Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

13c Click *OK*.

14 Click *Next* to display the Policy Schedule page.

Create New Firefox Policy Firefox ?

Step 8: Policy Schedule

Select the schedule to apply to the policy assignments:

Schedule Type:
No Schedule

<< Back Next >> Cancel

15 Select the schedule to apply to the assignments from the drop-down list, then select the desired options, which vary, depending on the schedule type you select.

The settings you configure on this page determine when the policy is applied to devices.

See [Section 12.3, “Schedules,” on page 74](#) for information about the available schedules and their options.

- 16 Click *Next* to display the Policy Groups page.

Create New Firefox Policy Firefox ?

Step 9: Policy Groups

Specify the groups for this policy:

Add	Remove	Name	In Folder
No items selected, click add to select items			

<< Back Next >> Cancel

- 17 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the Name column to select the desired policy groups and display their names in the Selected list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see [Section 14.3, “Creating Policy Groups,” on page 125](#).

- 18 Click *Next* to display the Finish page.
- 19 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured according to the settings on the Finish page.

13.4 Generic GNOME Policy

The Generic GNOME policy is used to configure GConf- based applications on a device.

To configure the GNOME policy:

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

- 3 In the Policy Type list, click *Generic GNOME Policy*, then click *Next* to display the Policy Name page.

Create New Generic GNOME Policy ?

Step 2: Policy Name

Specify the name of the new policy:

Policy Name: *

Folder: *

/Policies

Description:

Fields marked with a blue asterisk are required.

<< Back Next >> Cancel

- 4 Fill in the fields:

- **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.
- **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.
- **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

- 5 Click *Next* to display the Source page.

Create New Generic GNOME Policy GNOME ?

Step 3: Generic GNOME Policy, Source Page

To create a new Generic GNOME Policy, you need to define some Gconf settings. You can define Gconf Settings using one of the following options:

☒ Import the settings from a device

☐ Define a setting on your own

<< Back Next >> Cancel

- 6 Select the desired option, then click Next.

Import the settings from a device: Use this option to import the existing GConf settings from any device that is registered with the ZENworks Linux Management Server. The system obtains all settings, including default settings, from that device. You can enforce these settings on a desired managed device or group of devices at a later time.

Before you import settings to your device, make sure the GConf settings are correct on the device you are importing from.

If you choose this option, continue with [Step 7 on page 99](#).

Define a setting on your own: Create a directory and corresponding key settings such as key names, types, and values. At a later time, you can enforce these settings on a managed device or on a group of devices.

Make sure that you specify the correct key names and types.

If you choose this option, continue with [Step 8 on page 100](#).

- 7 (Conditional) If you chose the *Import the settings from a device* option in [Step 6 on page 99](#), choose the device from which you want to import the Gconf settings.

Create New Generic GNOME Policy GNOME ?

Step 4: Generic GNOME Policy, Device Page

Choose the device from which you want to import the Gconf settings

Import settings from:

☐ Selected machine

☒ DNS Name / IP Address

User Name: *

Fields marked with a blue asterisk are required.

<< Back Next >> Cancel

7a Select one of the following options:

Selected machine: Browse to and select a device from which you want to import GConf settings, then click OK.

Only managed devices that are registered with the ZENworks Linux Management Server are displayed.

DNS name / IP address: Specify the DNS name or IP address of a managed device from which you are importing GConf settings. Ensure that the device is registered with the ZENworks Linux Management Server.


7b Specify the username of the managed device from which you are importing the GConf settings.

Only those GConf settings are imported that are related to the specified user. Ensure that the specified user has a valid account on the managed device from which you are importing the settings.


7c Click *Next* to import the top-level directories. The four top-level directories that are imported are Apps, Desktop, System, and GNOME.

7d Select one or more directory whose settings you want to import, then click *Next*.

7e (Optional) Add or delete the keys and their respective values from the imported GConf settings, then click *Next* and skip to [Step 9 on page 101](#).

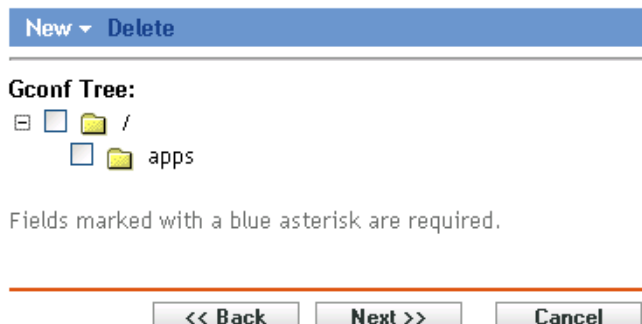
For detailed information about defining your own GConf settings, click the  button on the Built Gconf Tree page.

8 (Conditional) If you chose the *Define a setting on your own* in [Step 6 on page 99](#), define your own Gconf Settings by adding and deleting keys on the Gconf Tree, then click *Next*.

For detailed information about defining your own Gconf settings, click the  button on the Built Gconf Tree page.



You can define your own Gconf Settings by Adding / Deleting the keys on the Gconf Tree.
Deleting a directory, will delete all the sub-directories and keys in it.



- 9 Click *Next* to display the Default system requirements for Generic GNOME Policy page.

Create New Generic GNOME Policy GNOME ?

Step 5: Default system requirements for Generic GNOME policy

The following condition is added as a default system requirement to this policy.
If the minimum supported version requirement is removed then the policy may not be fully applied and effective on the target device.

☒ Apply policy on devices with distribution >= SUSE LINUX 9.3

<< Back Next >> Cancel

- 10 Specify the minimum system requirements for Generic GNOME policy settings to be effective.

The value you specify in the *Apply policy on devices with distribution* field indicates the distribution and minimum version that is required for the policy settings to be effective. The policy is applied if the device has the same version or a later version of the distribution.

If you chose the *Import from a device* option in [Step 6 on page 99](#), the default value is the operating system of a device from which you have imported GConf settings. If you have not included this setting in the policy, and if the operating system of a managed device (where the policy is to be applied) is different than the operating system of the device from which the settings have been imported, a warning message is generated. However, the policy settings are enforced.

If you chose the *Define a setting on your own* option in [Step 6 on page 99](#), and you want to include the default system requirement in the policy, you must specify the distribution and version of the operating system. If you do not include this setting in the policy, the system does not check for minimum operating system requirements and immediately enforces the policy.

Refer to the contents of the `/etc/SuSE-release` or `/etc/redhat-release` file to obtain the correct string for your platform.

- 11 Click *Next* to display the Summary page.
- 12 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the Generic GNOME policy is created but it does not have devices assigned or a schedule. At some point in the future, you need to configure additional options for the policy by continuing with [Section 14.4, “Assigning Policies,” on page 128](#).

or

Click *Next* to display the Policy Assignment page to perform the following tasks:

- Specify assignments for this policy
- Specify the schedule for this policy
- Specify groups for this policy

Create New Generic GNOME Policy

GNOME

?

Step 7: Policy Assignments

Specify the assignments for this policy:

Add	Remove
<input type="checkbox"/>	<div>Name</div> <div>In Folder</div>
No items selected, click add to select items	

<< Back

Next >>

Cancel

13 Assign the policy to the devices.

13a Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

13b Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

13c Click *OK*.

14 Click *Next* to display the Policy Schedule page.

Create New Generic GNOME Policy

GNOME

?

Step 8: Policy Schedule

Select the schedule to apply to the policy assignments:

Schedule Type:

No Schedule

<< Back

Next >>

Cancel

15 Select the schedule to apply to the assignments from the drop-down list, then select the desired options, which vary, depending on the schedule type you select.

The settings you configure on this page determine when the policy is applied to devices.

See [Section 12.3, “Schedules,” on page 74](#) for information about the available schedules and their options.

- 16 Click *Next* to display the Policy Groups page.

Create New Generic GNOME Policy GNOME ?

Step 9: Policy Groups

Specify the groups for this policy:

Add	Remove	Name	In Folder
No items selected, click add to select items			

<< Back Next >> Cancel

- 17 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the Name column to select the desired policy groups and display their names in the Selected list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see [Section 14.3, “Creating Policy Groups,” on page 125](#).

- 18 Click *Next* to display the Finish page.
- 19 Review the information on the *Finish* page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured according to the settings on the Finish page.

13.5 Novell Linux Desktop Policy

The Novell Linux Desktop policy is used to configure the GNOME Novell Linux Desktop settings on a device.

To configure the Novell Linux Desktop policy:

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

- 3 In the Policy Type list, click *Novell Linux Desktop Policy*, then click *Next* to display the Policy Name page.

The screenshot shows a window titled "Create New Novell Linux Desktop Policy" with a subtitle "Step 2: Policy Name". Below the title bar, it says "Specify the name of the new policy:". There are three input fields: "Policy Name: *" with an empty text box, "Folder: *" with a text box containing "/Policies" and a browse button (magnifying glass icon), and "Description:" with a large empty text area. At the bottom, a message states "Fields marked with a blue asterisk are required." Below this is a horizontal line and three buttons: "<< Back", "Next >>", and "Cancel".

- 4 Fill in the fields:

- **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.
- **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.
- **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

- 5 Click *Next* to display the Novell Linux Desktop Lockdown Settings page.

Create New Novell Linux Desktop Policy NLD ?

Step 3: Novell Linux Desktop Lockdown Settings

Selecting an item from the list below will disable or remove the associated feature on the users desktop. The user will be unable to access menu items or controls associated with the feature.

- ☐ Disable panel configuration
- ☐ Disable launcher creation
- ☐ Remove computer icon from desktop
- ☐ Remove trash icon from desktop
- ☐ Remove user's home icon from desktop

<< Back Next >> Cancel

- 6 Select the desired options (by default, all options are disabled):

Selecting an item from the list disables or removes the associated feature on the user's desktop. The user cannot access menu items or controls associated with the feature.

Disable panel configuration: Lets you prevent users from configuring a panel. If you select this option, users cannot add and remove the icons on the panel.

Disable launcher creation: Lets you prevent users from creating application launchers.

Remove computer icon from desktop: Lets you remove the computer icon from users' desktops.

Remove trash icon from desktop: Lets you remove the trash icon from users' desktops.

Remove user's home icon from desktop: Lets you remove the Home icon from users' desktops.

- 7 Click *Next* to display the Novell Linux Desktop Menu Lockdown page.

Create New Novell Linux Desktop Policy NLD ?

Step 4: Novell Linux Desktop Menu Lockdown

Selecting an item from the list below will remove the associated feature on the users desktop. The user will be unable to access menu items associated with the feature.

☐ Remove from system menu

System menu items

Log Off
Lock Screen
Run Program
Search for Files

Menu items to be removed. *

☐ Remove from program menu

Program menu items

Gnome Terminal
File Manager
Find Files
System Monitor

Menu items to be removed. *

Fields marked with a blue asterisk are required.

<< Back Next >> Cancel

- 8 Select the items that you want to remove from desktops so that users cannot access menu items associated with the feature (by default, all options are disabled):

Remove from System menu: Lets you remove items from the System menu of the Novell Linux Desktop. Select an item you want to remove and move it to the box on the right side. The item is removed from the users' System menus.

Remove from Program Menu: Lets you remove items from the Program menu of the Novell Linux Desktop. Select an item you want to remove and move it to the box on the right side. The item is removed from the users' Program menus.

- 9 Click *Next* to display the Novell Linux Desktop Personal Settings and Applets Lockdown page.

Create New Novell Linux Desktop Policy NLD ?

Step 5: Novell Linux Desktop Personal Settings and Applets Lockdown

Selecting an item from the list below will remove the associated feature on the users desktop. The user will be unable to access the items associated with the feature.

☐ Remove from personal settings

Personal settings

Menus
Shortcuts
Desktop Background
Fonts

Personal settings to be removed *

☐ Remove applets

Applets

Command Line
Stock Update
Sticky Notes
Volume Control

Applets to be removed *

Fields marked with a blue asterisk are required.

<< Back Next >> Cancel

- 10 Select the items that you want to remove from desktops so that users cannot access menu items associated with the feature (by default, all options are disabled):

Remove from personal settings: Lets you remove items from the Personal Settings of Novell Linux Desktop. Select an item you want to remove and move it to the box on the right side. The item is removed from the users' Personal Settings.


Remove applets: Lets you prevent the applets from being displayed on users' Novell Linux Desktop. Select an applet from the Applets list and move it to the box on the right side. Selected applets are not displayed on users' Novell Linux Desktop.

- 11 Click *Next* to display the Novell Linux Desktop Configuration Settings page.

Create New Novell Linux Desktop Policy

NLD


?

 Step 6: Novell Linux Desktop Configuration Settings

Click the checkboxes to select settings which will be enforced on the desktop.
For each setting you select, provide a value, and optionally, lock the setting to prevent the value from changing after it is set.

☐


Background image file name *



(eg. /opt/gnome/share/images/roses.jpeg)

☐

Background position




Centered

▼

☐

Background shade




Solid

▼

☐


Theme file name *



(eg. /opt/gnome/share/themes/metacity/index.theme)

☐

Proxy Settings



☐

Direct internet connection

☒

Manual proxy configuration

HTTP Proxy *

Port *

8080

Authentication

HTTP Secure Proxy

Port *

0

FTP Proxy

Port *

0

Socks Proxy

Port *

0

☐

Automatic proxy configuration

Autoconfiguration URL


Fields marked with a blue asterisk are required.

<< Back

Next >>

Cancel

- 12 Select the desired options (by default, all options are disabled).

For each option you enable, provide a value. When you enable an option, it is locked by default. You can unlock the option by clicking . The options that are not enabled are excluded from the policy and are not applied to the device.

Background image filename: Lets you specify the filename and complete location of a background image. This image file is displayed as a background on users' desktops. The file should exist on the managed device at the specified location.

Background position: Lets you specify background image display options. Center displays an image in the center of the screen, Fill Screen stretches the image to cover the entire screen, Scaled enlarges the image until the image meets the screen edges, and Tiled repeats the image

over the screen. Select No Background to prevent the image from being displayed on the desktop.

Background shade: Lets you choose an available shade to decorate the background. Select Solid to have the background image uniform across the desktop. Select Vertical to have the image become darker as you go up, and select Horizontal to have the image become darker as you go from left to right.

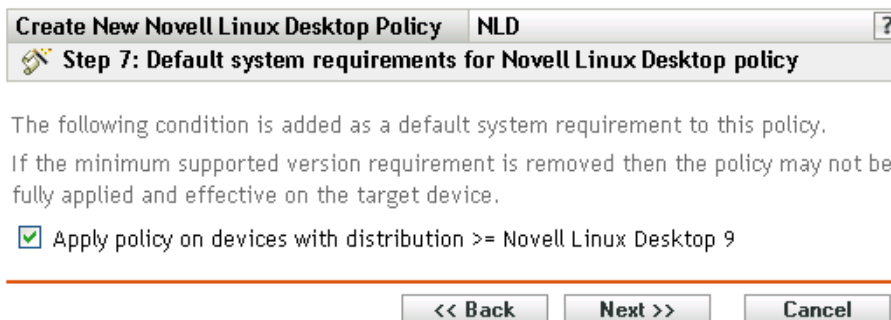
Theme filename: Lets you specify a theme file name and its complete location. The appearance of the windows, icons, buttons, and other graphical user interface controls are changed according to the selected theme.

Proxy settings: Specify a proxy setting:

- **Direct internet connection:** Lets users connect to the Internet without using the proxy server.
- **Manual proxy configuration:** Lets you manually configure the proxy. Specify the HTTP Proxy value, HTTP Secure Proxy value, FTP Proxy value, Socks Proxy value, and corresponding port numbers.

To authenticate the user before proxy configuration, click Authentication. In the HTTP Proxy Authentication dialog box, select Use Authentication, specify the username and password, then click OK.
- **Automatic proxy configuration:** Lets you automatically configure the proxy from a certain URL by specifying the URL.

- 13 Click *Next* to display the Default System Requirements for the Novell Linux Desktop Policy page.



- 14 Specify the minimum version of Novell Linux Desktop required for all policy settings to be effective. Policy settings are applied only if a device has the same version or a newer version of the Novell Linux Desktop. If a device does not have Novell Linux Desktop 9 or newer, the policy does not apply correctly.

Even if you do not include this setting in the policy, the system checks for Novell Linux Desktop. If it does not find Novell Linux Desktop, an error message is generated and the policy is not applied.

NOTE: To ensure successful enforcement of all configured items, you need Novell Linux Desktop 9 with Support Pack 2 with GNOME.

- 15 Click *Next* to display the Summary page.
- 16 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the Novell Linux Desktop policy is created but it does not have devices

assigned or a schedule specified. At some point in the future, you need to configure additional options for the policy by continuing with [Section 14.4, “Assigning Policies,” on page 128](#).

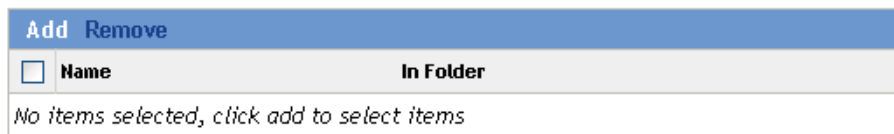
or

Click *Next* to display the Policy Assignment page to perform the following tasks:

- Specify assignments for this policy
- Specify the schedule for this policy
- Specify groups for this policy



Specify the assignments for this policy:



<< Back

Next >>

Cancel

17 Assign the policy to the devices.

17a Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

17b Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

17c Click *OK*.

18 Click *Next* to display the Policy Schedule page.



Select the schedule to apply to the policy assignments:

Schedule Type:

No Schedule

<< Back

Next >>

Cancel

- 19 Select the schedule to apply to the assignments from the drop-down list, then select the desired options, which vary, depending on the schedule type you select.

The settings you configure on this page determine when the policy is applied to devices.

See [Section 12.3, “Schedules,” on page 74](#) for information about the available schedules and their options.

- 20 Click *Next* to display the Policy Groups page.

Create New Novell Linux Desktop Policy NLD ?

Step 11: Policy Groups

Specify the groups for this policy:

Add	Remove	Name	In Folder
No items selected, click add to select items			

<< Back Next >> Cancel

- 21 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the Name column to select the desired policy groups and display their names in the Selected list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see [Section 14.3, “Creating Policy Groups,” on page 125](#).

- 22 Click *Next* to display the Finish page.
- 23 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured according to the settings on the Finish page.

13.6 Remote Execute Policy

The Remote Execute policy is used to execute any Script, Binary, or Java file.

To configure the Remote Execute policy:

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

- 3 In the Policy Type list, click *Remote Execute Policy*, then click *Next* to display the Policy Name page.

Create New Remote Execute Policy ?

Step 2: Policy Name

Specify the name of the new policy:

Policy Name: *

Folder: *

/Policies

Description:

Fields marked with a blue asterisk are required.

<< Back Next >> Cancel

- 4 Fill in the fields:

- **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.
- **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.
- **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

5 Click *Next*.

Create New Remote Execute Policy

Remote_Execute

?

Step 3: Remote Execute Policy

Executable Type:

Script

▼

Maximum Waiting Time:

☐ Do not wait

☒ Wait till the program completes the execution

☐ Wait For sec

Script to run:

Specify a file

▼

Script file name: *

(e.g. /usr/local/xyz.pl)

Script parameters:

(e.g. abc efg)

Script engine: *

(e.g. /usr/local/bin/perl)

Script engine parameters:

(e.g. -c abc -s efg)

Fields marked with a blue asterisk are required.

<< Back

Next >>

Cancel

6 Select the desired options:

Executable type: Select an executable type to run on a managed device (script, binary, or Java). Depending on the executable type you select, different options are available, as described below.

Maximum waiting time: Indicate the waiting time after starting the script, binary, or Java program. The following table explains the available options:

Option	Description
Do not wait	The Remote Execute enforcer does not wait for the program to be completed.
Wait till the program completes the execution	The Remote Execute enforcer waits for the program to be completed.
Wait for <n> sec	Indicates how many seconds the Remote Execute enforcer should wait after starting the program.

NOTE: The launched program is not terminated by the enforcer if you select the Do Not Wait or Wait for <n>Sec options.

(Conditional) If you chose Script in the Executable Type field in [Step 6 on page 113](#), the following options are available:

Script to run: Select an option from the drop-down list:

- **Specify a file:** Fill in the fields:

Script filename: Specify the complete path, including the filename, of the script you want to run on a managed device.

Script parameters: Specify any parameters to be passed to the specified script file.

Script engine: Specify the name and location of the script engine that runs the script. For example, `/user/bin/perl`.

Script engine parameters: Specify any parameters to be passed to the specified script engine.

- **Define your own script:** Type your script in the box.

(Conditional) If you chose Binary in the Executable Type field in [Step 6 on page 113](#), the following options are available:

Executable file name: Specify the complete path, including the filename, of the binary program you want to run on a managed device.

Executable file parameters: Specify any parameters to be passed to the specified binary program.

NOTE: You cannot perform shell operations, such as redirection using the executable type Binary. You can use *Executable file parameters* to pass only those parameters that are required by the executable specified in the *Executable file name* field. If you want to use shell operations, define your own script.

(Conditional) If you chose Java in the Executable Type field in [Step 6 on page 113](#), the following options are available:

Java program name: Specify the Java program you want to run on a managed device.

Program parameters: Specify any parameters to be passed to the specified Java program.

Java Runtime Executable (JRE): Specify the complete path, including the Java Runtime Executable (JRE) name. JRE is used to interpret the Java binary file.

JRE parameters: Specify the parameters to be passed to the Java Runtime Executable (JRE).

NOTE: The Own Defined Script specified in the Remote Execute policy is executed in the shell specified by the environment variable SHELL. The value of the variable SHELL is taken from the environment in which ZENworks Management daemon runs. If a value is not specified, then `/bin/sh` is used, which is a default value.

7 Click *Next* to display the Summary page.

8 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the Remote Execute policy is created but it does not have devices assigned or a schedule specified. At some point in the future, you need to configure additional options for the policy by continuing with [Section 14.4, “Assigning Policies,” on page 128](#).

or

Click *Next* to display the Policy Assignment page to perform the following tasks:

- Specify assignments for this policy
- Specify the schedule for this policy

- Specify groups for this policy

Create New Remote Execute Policy	Remote_Execute	?
Step 5: Policy Assignments		

Specify the assignments for this policy:

Add	Remove
<input type="checkbox"/>	Name
	In Folder
No items selected, click add to select items	

<< Back	Next >>	Cancel
---------	---------	--------

9 Assign the policy to the devices.

9a Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

9b Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

9c Click *OK*.

10 Click *Next* to display the Policy Schedule page, then select the schedule to apply to the assignments.

The settings you configure on this page determine when the policy is applied to devices.

See [Section 12.3, “Schedules,” on page 74](#) for information about the available schedules.

11 Click *Next* to display the Policy Groups page.

Create New Remote Execute Policy	Remote_Execute	?
Step 7: Policy Groups		

Specify the groups for this policy:

Add	Remove
<input type="checkbox"/>	Name
	In Folder
No items selected, click add to select items	

<< Back	Next >>	Cancel
---------	---------	--------

12 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the Name column to select the desired policy groups and display their names in the Selected list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see [Section 14.3, “Creating Policy Groups,” on page 125](#).

- 13 Click *Next* to display the Finish page.
- 14 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured per settings on the Finish page.

13.7 Text File Policy

The Text File policy is used to make changes to any text file on a device.

To configure the Text File policy:

- 1 In the ZENworks Control Center, click the *Policies* tab.
- 2 In the Policies list, click *New*, then click *Policy* to display the Create New Policy page.
- 3 In the Policy Type list, click *Text File Policy*, then click *Next* to display the Policy Name page.

Create New Text File Policy ?

Step 2: Policy Name

Specify the name of the new policy:

Policy Name: *

Folder: *

/Policies

Description:

Fields marked with a blue asterisk are required.

<< Back Next >> Cancel

- 4 Fill in the fields:
 - **Policy name:** (Required) Provide a unique name for the policy. The name you provide displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management.

- **Folder:** (Required) Type the name or browse to the folder that this policy will be created in. Folders display in the ZENworks Control Center.
- **Description:** Provide a short description of the policy. This description displays on the policy's Summary page in the ZENworks Control Center interface.

5 Click *Next* to display the General page.

Create New Text File Policy

Text_File

?

Step 3: Text File Policy, General Page

File details:

File Name: *
(e.g. /etc/samba/smb.conf)

Maximum number of version(s) to retain [1 to 25]: *

Change details:

Enter the search string as a regular (or) normal expression.
Refer the Administration document for further information on regular expressions.

Change Name: *

Change Mode:

Search String: *
(e.g. ^abc*\$)

Case Sensitive: ☒

Search Occurrence:

Result Action:

New String: *

Fields marked with a blue asterisk are required.

<< Back

Next >>

Cancel


6 Select the desired options:

Filename: Specify the name and the complete path of a file you want to change.

Maximum number of versions to retain: Specify the maximum number of backups to be maintained for a file that has been changed. If the maximum limit of backups is reached, the oldest backup of a file is deleted. The backup is created in the same location as the specified file.

Change name: Specify the name of the change you want to perform in the file. If you want to make more than one change in the same file, go to the Settings page.

Change mode: Select an option from the drop-down list:

- **Search file:** Lets you search for the given text in the entire file. Fill in the fields:
 - **Search string:** Specify the text you want to search for in a given file. The search string can be simple text or a regular expression. For detailed information on regular expressions, click the  button.
 - Case sensitive:** Select this option to distinguish between uppercase and lowercase characters. When Case Sensitive is selected, the system finds only those instances in which the capitalization matches the text you have specified in the search string.
 - Search occurrence:** Indicates the occurrence of the search text you have given. The available options are First Occurrence, Last Occurrence, and Find All Occurrences. For example, if you select First Occurrence, the system finds the first occurrence of the search string and performs the specified action on it.
 - Result action:** Select the operation from the drop-down list that you want perform on the specified search text.
- **Append lines to file:** Lets you append the given lines of text to the file
- **Prepend lines to file:** Lets you prepend the given lines of text to the file.

New string: Specify the text to be used for carrying out the specified action in the file. For example, you can select to replace a search string with a new string.

7 Click *Next* to display the Script Page.

Create New Text File Policy Text_File ?

Step 4: Text File Policy, Script Page

Pre-change action:
Execute the following before modifying the text file(s)

Executable Type: None

Action when the execution fails: Continue modifying the text files

Post-change action:
Execute the following after modifying the text file(s)

Executable Type: None

Fields marked with a blue asterisk are required.

<< Back Next >> Cancel

8 Fill in the fields:

Pre-change action: Specify the actions to perform before modifying the text files:

- **Executable type:** Select the executable type from the drop-down list that you want to run before modifying the file. The available options are None, Binary, Java, and Script.
(Conditional) If you chose Script in the *Executable type* field, the following options are available:

Script to run: Select an option from the drop-down list (Specify a File or Define Your Own Script):

- **Specify a file:** Fill in the fields:

Script filename: Specify the complete path, including the filename, of the script you want to run on a managed device.

Script parameters: Specify any parameters to be passed to the specified script file.

Script engine: Specify the name and location of the script engine that runs the script. For example, /user/bin/perl.

Script engine parameters: Specify any parameters to be passed to the specified script engine.

- **Define your own script:** Type your script in the box.

(Conditional) If you chose Binary in the *Executable type* field, the following options are available:

Executable file name: Specify the complete path, including the filename, of the binary program you want to run on a managed device.

Executable file parameters: Specify any parameters to be passed to the specified binary program.

(Conditional) If you chose Java in the *Executable type* field, the following options are available:

Java program name: Specify the Java program you want to run on a managed device.

Program parameters: Specify any parameters to be passed to the specified Java program.

Java Runtime Executable (JRE): Specify the complete path, including the Java Runtime Executable (JRE) name. JRE is used to interpret the Java binary file.

JRE parameters: Specify the parameters to be passed to the Java Runtime Executable (JRE).

NOTE: The Own Defined Script specified in the Remote Execute policy is executed in the shell specified by the environment variable SHELL. The value of the variable SHELL is taken from the environment in which ZENworks Management daemon runs. If a value is not specified, then `/bin/sh` is used, which is a default value.

Action when the execution fails: Select an action you want the system to perform when an execution fails. You can continue modifying the file by selecting *Continue modifying the text file* or you can stop the modifications in the file by selecting *Do not modify the text file*.

NOTE: The backup of the text file is taken after the pre-change action completes the execution and before the text file modification starts.

Post-change action: Specify the actions to perform after the actual changes are done in the file.

- **Executable type:** Select the executable type you want to run after modifying the file. Select Binary, Java, Script, or None from the drop-down list. Depending on which type you select, the available options vary. For more information about the specific options, see the descriptions in the Pre-Change Action section directly above.

9 Click *Next* to display the Summary page.

10 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the Text File policy is created but it does not have devices assigned or a schedule specified. At some point in the future, you need to configure additional options for the policy by continuing with [Section 14.4, “Assigning Policies,” on page 128](#).

or

Click *Next* to display the Policy Assignment page to perform the following tasks:

- Specify assignments for this policy
- Specify the schedule for this policy
- Specify groups for this policy

Create New Text File Policy Text_File ?

Step 6: Policy Assignments

Specify the assignments for this policy:

Add Remove	
<input type="checkbox"/> Name	In Folder
No items selected, click add to select items	

11 Assign the policy to the devices.

11a Click *Add* to browse for and select the appropriate Server or Workstation objects.

You can also select Folder or Group objects.

11b Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

11c Click *OK*.

12 Click *Next* to display the Policy Schedule page, then select the schedule to apply to the assignments.

The settings you configure on this page determine when the policy is applied to devices.

See [Section 12.3, “Schedules,” on page 74](#) for information about the available schedules.

13 Click *Next* to display the Policy Groups page.

Create New Text File Policy Text_File ?

Step 8: Policy Groups

Specify the groups for this policy:

Add Remove	
<input type="checkbox"/> Name	In Folder
No items selected, click add to select items	

14 (Optional) Click *Add* to open the Select Groups dialog box, then click the underlined links in the Name column to select the desired policy groups and display their names in the Selected list box.

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create. For more information, see [Section 14.3, “Creating Policy Groups,” on page 125](#).

- 15** Click *Next* to display the Finish page.
- 16** Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to create the policy as configured according to the settings on the Finish page.

Novell® ZENworks® Linux Management Policies give you the ability to define and lock down configuration settings of various applications on managed devices. ZENworks Linux Management provides policies for a number of popular applications, including the Novell Linux Desktop, plus powerful tools to create customized policies for other applications. In addition to creating policies, as described in [Chapter 13, “Creating Policies,” on page 77](#), you can create groups and folders to assign policies to, edit existing policies, and more.

The following sections contain additional information:

- [Section 14.1, “Creating Policies,” on page 123](#)
- [Section 14.2, “Creating Folders,” on page 124](#)
- [Section 14.3, “Creating Policy Groups,” on page 125](#)
- [Section 14.4, “Assigning Policies,” on page 128](#)
- [Section 14.5, “Removing Policy Assignments,” on page 130](#)
- [Section 14.6, “Adding Policies to Existing Groups,” on page 130](#)
- [Section 14.7, “Editing Policies,” on page 131](#)
- [Section 14.8, “Editing System Requirements,” on page 141](#)
- [Section 14.9, “Refreshing Policies,” on page 142](#)
- [Section 14.10, “Verifying Policy Enforcement,” on page 143](#)
- [Section 14.11, “Renaming, Copying, or Moving Policies,” on page 143](#)
- [Section 14.12, “Deleting Policies, Policy Groups, and Folders,” on page 144](#)
- [Section 14.13, “Unenforcing Policies,” on page 145](#)

14.1 Creating Policies

Step-by-step instructions to create policies are contained in [Chapter 13, “Creating Policies,” on page 77](#).

ZENworks lets you create seven types of policies:

- **Epiphany policy:** Configures the Epiphany Web browser. For step-by-step instructions to create this policy, see [Section 13.1, “Epiphany Policy,” on page 77](#).
- **Evolution policy:** Configures the Evolution™ e-mail client. For step-by-step instructions to create this policy, see [Section 13.2, “Evolution Policy,” on page 83](#).
- **Firefox policy:** Configures the Firefox Web browser. For step-by-step instructions to create this policy, see [Section 13.3, “Firefox Policy,” on page 90](#).
- **Generic GNOME policy:** Configures GConf applications. For step-by-step instructions to create this policy, see [Section 13.4, “Generic GNOME Policy,” on page 97](#).
- **Novell Linux Desktop policy:** Configures the Novell Linux Desktop settings. For step-by-step instructions to create this policy, see [Section 13.5, “Novell Linux Desktop Policy,” on page 103](#).

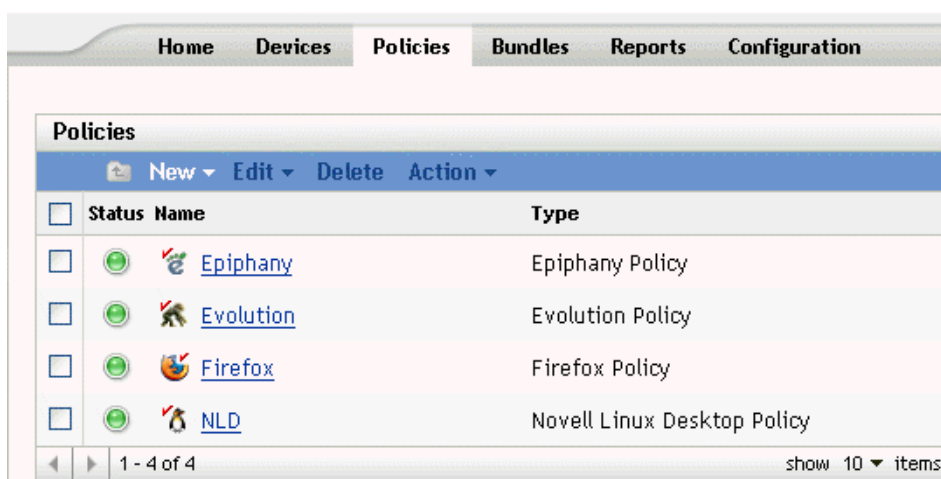
- **Remote Execute policy:** Executes a script, binary, or Java file. For step-by-step instructions to create this policy, see [Section 13.6, “Remote Execute Policy,” on page 111](#).
- **Text File policy:** Applies changes to a text file. For step-by-step instructions to create this policy, see [Section 13.7, “Text File Policy,” on page 116](#).

14.2 Creating Folders

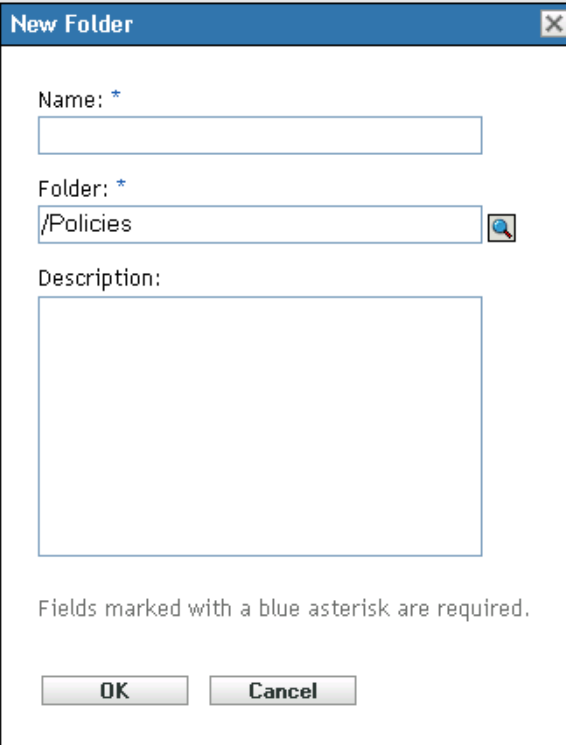
A folder is an organization object that displays in the ZENworks Control Center interface, which is the administrative tool for ZENworks Linux Management. A folder can contain various objects, including subfolders, Policy, and Policy Group objects.

To create a folder:

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



- 2 Click *New*, then click *Folder* to display the New Folder dialog box.

The image shows a 'New Folder' dialog box with a blue title bar and a close button. It contains three fields: 'Name: *' with an empty text box, 'Folder: *' with a text box containing '/Policies' and a browse button, and 'Description:' with a large empty text area. At the bottom, there is a note 'Fields marked with a blue asterisk are required.' and two buttons, 'OK' and 'Cancel'.

- 3 Fill in the fields:

- **Name:** Provide a unique name for your folder. This is a required field.
- **Folder:** Type the name or browse to the folder that contains this folder in the ZENworks Control Center interface.
- **Description:** Provide a short description of the folder's contents.

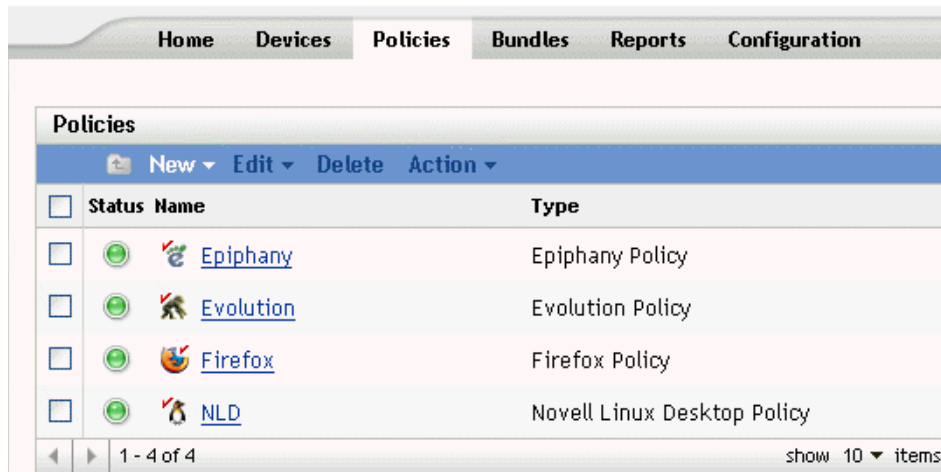
- 4 Click *OK*.

14.3 Creating Policy Groups

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

To create a policy group:

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



- 2 Click *New*, then click *Policy Group* to display the Basic Information page.

The screenshot shows the 'Create New Group' dialog box with the 'Step 1: Basic Information' tab selected. The dialog has a title bar 'Create New Group' with a help icon. The fields are:

- Group Name: * (required field, marked with a blue asterisk)
- Folder: * (required field, marked with a blue asterisk, containing the text '/Policies' and a browse button)
- Description: (text area)

Below the fields, it says 'Fields marked with a blue asterisk are required.' At the bottom, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.

- 3 Fill in the fields:

- **Group name:** (Required) Provide a unique name for your policy group. The name you provide displays in the ZENworks Control Center interface (the administrative tool for ZENworks Linux Management) and in the user interface.
- **Folder:** (Required) Type the name or browse to the folder that contains this policy group.

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

4 Click *Next* to display the Summary page.

Review the information on the Summary page, making any changes to the policy-group settings by using the *Back* button as necessary.

Depending on your needs, you can create the policy group now or you can specify members, assignments, and schedules for this policy group.

5 Click *Finish* to create the policy as configured according to the settings on the Summary page. If you click *Finish*, the policy group is created but it does not have members, devices assigned, a schedule, and so forth. At some point in the future, you need to configure additional options for the policy group by continuing with [Section 14.4, “Assigning Policies,” on page 128](#).

or

Click *Next* to display the Add Group Members page to perform the following tasks:

- Specify members for this policy group
- Specify assignments for this policy group
- Specify the schedule to apply the policy-group assignments

Create New Group	Policies	?
Step 3: Add Group Members		

Specify the members for this group:

Add	Remove
<input type="checkbox"/>	Name
	In Folder
No items selected, click add to select items	

<< Back	Next >>	Cancel
---------	---------	--------

6 Specify the policies to include in this policy group.

6a Click *Add* to browse for and select the appropriate policy objects.

6b Click the underlined link in the Name column to select the desired policies and display their names in the Selected list box.

6c Click *OK*.

- 7 Click *Next* to display the Add Assignments page.

Create New Group Policies ?

Step 4: Add Assignments

Specify the assignments for this group:

Add	Remove
<input type="checkbox"/>	Name In Folder

No items selected, click add to select items

<< Back Next >> Cancel

- 8 Assign the policy group to the desired devices.

- 8a Click *Add* to browse for and select the appropriate device objects.

You can also select Folder or Group objects.

- 8b Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.

Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.

- 8c Click *OK*.

- 9 Click *Next* to display the Schedule page.

- 10 Select the schedule to apply to the assignments.

The settings you configure on this page determine when the policies in the policy group are assigned to devices.

See [Section 12.3, “Schedules,” on page 74](#) for information about the available schedules.

- 11 Click *Next* to display the Summary page, then review the information, making any changes to the settings by using the Back button as necessary.

- 12 Click *Finish*.

14.4 Assigning Policies

When you assign policies, you specify device assignments and assignment schedules for an existing policy.

When you created policies, midway through the Create Policy Wizard, you were given the choice of clicking *Finish* or *Next*.

If you clicked *Finish*, the policy was created without assigning devices to it, specifying assignment schedules, or specifying groups for the policy. Before the policy can be applied to assigned devices,

you must complete the following steps. If you clicked *Next*, you have already performed the following procedure as part of the policy-creation process.

- 1 In the ZENworks Control Center, click the *Policies* tab, select the desired policy in the Policies list by checking the box next to its name, click *Action*, then click *Assign Policy* to display the Policy Assignments page.

The screenshot shows the 'Assign Policy' dialog box with the title bar 'Assign Policy' and a help icon. Below the title bar is a tab labeled 'Step 1: Devices to be Assigned'. The main area contains the instruction 'Select the devices to be assigned to the previously selected policies.' Below this is a table with two columns: 'Name' and 'In Folder'. The 'Name' column has a checkbox to its left. The table is currently empty, with a message 'No items selected, click add to select items' at the bottom. At the bottom of the dialog are three buttons: '<< Back', 'Next >>', and 'Cancel'.

Add Remove	
<input type="checkbox"/> Name	In Folder
No items selected, click add to select items	

- 2 Assign the policy to the desired devices.
 - 2a Click *Add* to browse for and select the appropriate Server or Workstation objects.
You can also select Folder or Group objects.
 - 2b Click the down-arrow next to Servers or Workstations to expand the list, then click the underlined link in the Name column to select the desired objects and display their names in the Selected list box.
Assigning a policy to a Group object is the preferred method of assigning the policy. Assigning the policy to a large number of objects (for example, more than 250) might cause increased server utilization.
 - 2c Click *OK*.
- 3 Click *Next* to display the Schedule page.

The screenshot shows the 'Assign Policy' dialog box with the title bar 'Assign Policy' and a help icon. Below the title bar is a tab labeled 'Step 2: Schedule'. The main area contains the instruction 'Specify the schedule to use for the assignments.' Below this is a label 'Schedule Type:' followed by a dropdown menu currently showing 'No Schedule'. At the bottom of the dialog are three buttons: '<< Back', 'Next >>', and 'Cancel'.

- 4 Select the schedule to apply to the assignments.
The settings you configure on this page determine when the policy is applied to devices. Depending on the type of policy you are assigning, the available schedules vary. See [Section 12.3, "Schedules," on page 74](#) for information about the available schedules.

- 5 Click *Next* to display the Finish page.
- 6 Review the information on the Finish page, making any changes to the policy settings by using the *Back* button as necessary. Click *Finish* to assign the policy as configured according to the settings on the Finish page.

In addition to the preceding steps to assign policies, the following are other options to assign a policy to devices:

- By selecting a policy and then using the Assignments section of the policy's Summary page.
- By selecting a device, device group, or folder and then selecting *Assign Policy* in the Action menu.
- By using the Effective Policy section on the device's Summary page.

14.5 Removing Policy Assignments

You can remove the policy assignments by selecting a policy and then removing the device from the Assignments section on the Policy Summary page. You can also do this by clicking the appropriate device on the Devices page and disassociating a policy by using the Effective Policies section.

After a policy is disassociated from a device, it is unenforced on the device. For more details on unenforcement of a policy, see [Section 14.13, “Unenforcing Policies,” on page 145](#).

You do not need to delete a policy to disassociate it from a device.

14.6 Adding Policies to Existing Groups

Using policy groups eases administration efforts by letting you group several policies so you can use common assignments, schedules, and so forth, rather than configuring these settings for each policy you create.

- 1 In the ZENworks Control Center, click the *Policies* tab, select the desired policy in the Policies list by selecting the box next to its name, click *Action*, then click *Add to Group* to display the Targets page.

Add To Group ?

Step 1: Targets

Select the groups that will contain the items.

Add	Remove	Name	In Folder
No items selected, click add to select items			

<< Back Next >> Cancel

- 2 Click *Add* to open the Select Groups dialog box, click the desired objects to add them to the Selected list, then click *OK* to display the selected groups in the list on the Targets page.
- 3 Click *Next* to display the Finish page.

- 4 Review the information on the Finish page, making any changes to the settings by using the *Back* button as necessary, then click *Finish* to add the policy to the group.

14.7 Editing Policies

You can edit an existing policy to change its description, add or remove assignments, add or remove the policy from existing policy groups, change configuration settings, and more.

Following sections describes how you can edit different types of policies:

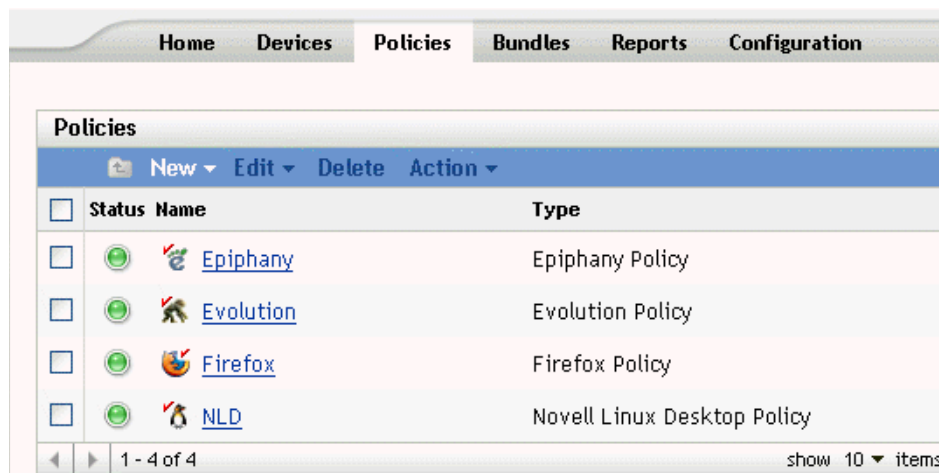
- [Section 14.7.1, “Editing Epiphany, Evolution, Firefox, and NLD Policies,” on page 131](#)
- [Section 14.7.2, “Editing Generic GNOME Policies,” on page 133](#)
- [Section 14.7.3, “Editing Remote Execute Policies,” on page 136](#)
- [Section 14.7.4, “Editing Text File Policies,” on page 138](#)
- [Section 14.7.5, “Viewing Policy Enforcement Status,” on page 140](#)

14.7.1 Editing Epiphany, Evolution, Firefox, and NLD Policies

You can edit, include, or remove lockdown settings, configuration settings, and system requirements of the application policies. Epiphany, Evolution, Firefox, and Novell Linux Desktop policies are the application policies.

To edit the application policies:

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



- 2 Click the policy's name to display the Summary page, then make the desired configuration changes.

If you do not want to edit any item on the Summary page, skip to [Step 3 on page 133](#).

Use the Summary page to view detailed information about the selected policy. This page provides general information about the policy, lists the individual devices that are assigned to the policy, displays an event log, shows upcoming events, and lists the groups that the policy belongs to.

You can also use this page to edit the policy's description, add or remove assignments for the policy, and change other configuration settings, as described below.

- 2a** Review the information in the General section, then make the desired configuration changes (you can edit only the Revision and Description options in this section).

Policy type: Displays the policy type (Novell Linux Desktop Policy, Firefox Policy, and so forth).

Revision: Displays the policy's revision number. To change the revision number, click Increment Revision.

Number of errors not acknowledged: Displays the number of errors not acknowledged.

Number of warnings not acknowledged: A warning is anything that does not cause the application of the policy to fail, but indicates minor problems. The number displayed indicates the number of unacknowledged warnings, which display in the Event Log section below.

GUID: Lists the selected object's GUID (global unique identifier), a randomly generated string that provides a unique identifier for the policy. You cannot edit the object's GUID.

Description: Displays the selected object's description, if one was provided when the policy was created. The description provides a short description of the policy's purpose.

Click *Edit* to change the description, if necessary.

- 2b** Review the information in the Assignments section, then make the desired configuration changes.

The Assignments section lists the devices, device groups, and device folders to which the selected policy is assigned. You can also view the folder to which the device belongs and the schedule. You can click the device object name to view information about that device object.

You can also use the following options:

Advanced: Click *Advanced* to display the Edit Assignments page to display a list of the devices that are assigned to the selected policy, the folder that contains each device, and each device's schedule. You can use the Edit Assignments page to edit certain settings, such as the schedule.

Add: Click *Add* to launch the Assign Policy Wizard to select the devices to be assigned to the selected policy. For more information, see [Section 14.4, "Assigning Policies," on page 128](#).

Remove: Select the device by selecting the check box next to the appropriate device name, then click *Remove* to remove the device's assignment from this policy.

- 2c** Review the information in the Event Log section, then make the desired changes.

The Event Log section lists all unacknowledged errors and warnings.

The Status column displays an icon indicating each item's status. Position the mouse pointer over each icon to display a short message describing the status of the item.

To acknowledge an error or warning, click its name in the Event Column, then click *Acknowledged* in the Message Detail Information dialog box that displays. You can also click *Advanced*, select the check box next to the appropriate event, then click *Acknowledge* (a check mark displays on the right side of the Date column to indicate that the item has been acknowledged).

- 2d** Review the information in the Upcoming Events section.

The Upcoming Events section lists events scheduled for the selected policy. You can click the calendar icon to display a calendar to view events for the desired date. You can also use the arrows to view events for the previous or next day, week, or month.

- 2e** Review the information in the Groups section, then make the desired configuration changes.

The Groups section lists the groups that contain the selected policy.

You can also use the following options:

Advanced: Click *Advanced* to display the Edit Groups page to display a list of the groups that contain the selected policy. You can click *Add* to open the Select Groups dialog box to add the selected policy to existing groups. You can also remove a group by selecting the check box next to the Name column, then clicking *Remove* to remove.

Add: Click *Add* to open the Select Groups dialog box, then click the blue arrow in the Select column to select the desired group and display its name in the Selected list box.

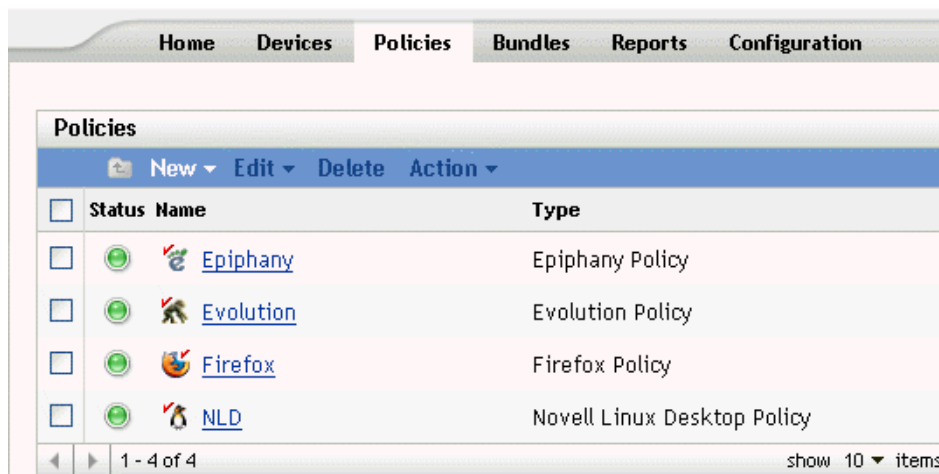
Remove: Select the check box next to the appropriate group name, then click *Remove* to remove the selected policy from the group.

- 3** Click the Details tab, then make the desired configuration changes. For more information about the available options, see the section about the appropriate policy in [Chapter 13, “Creating Policies,”](#) on page 77.
 - 3a** To edit the system requirements of a policy, see [Section 14.8, “Editing System Requirements,”](#) on page 141.
 - 3b** Click *Apply* to save any changes you have made.
- 4** After a policy is modified, the Revision field of the policy, which is available under the General section of the Summary page, must be incremented for the updated policy to be applied to associated devices. If the policy revision is not incremented, the changes made to the policy are not applied on the device.

14.7.2 Editing Generic GNOME Policies

To edit a Generic GNOME policy:

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



- 2 Click the policy's name to display the Summary page, then make the desired configuration changes.

If you do not want to edit any item on the Summary page, skip to [Step 3 on page 135](#).

Use the Summary page to view detailed information about the selected policy. This page provides general information about the policy, lists the individual devices that are assigned to the policy, displays an event log, shows upcoming events, and lists the groups that the policy belongs to.

You can also use this page to edit the policy's description, add or remove assignments for the policy, and change other configuration settings, as described below.

- 2a Review the information in the General section, then make the desired configuration changes (you can edit only the Revision and Description options in this section).

Policy type: Displays the policy type as Generic GNOME policy.

Revision: Displays the policy's revision number. To change the revision number, click *Increment Revision*.

Number of errors not acknowledged: Displays the number of errors that are not acknowledged.

Number of warnings not acknowledged: A warning is anything that does not cause the application of the policy to fail, but indicates minor problems. The number displayed indicates the number of unacknowledged warnings, which display in the Event Log section below.

GUID: Lists the selected object's GUID (global unique identifier), a randomly generated string that provides a unique identifier for the policy. You cannot edit the object's GUID.

Description: Displays the selected object's description, if one was provided when the policy was created. The description provides a short description of the policy's purpose. This description displays in the ZENworks Control Center interface.

Click *Edit* to change the description, if necessary.

- 2b Review the information in the Assignments section, then make the desired configuration changes.

The Assignments section lists the devices, device groups and device folders to which the selected policy is assigned. You can also view the folder to which the device belongs and the schedule. You can click the device object name to view information about that device object.

You can also use the following options:

Advanced: Click *Advanced* to display the Edit Assignments page to display a list of the devices that are assigned to the selected policy, the folder that contains each device, and each device's schedule. You can use the Edit Assignments page to edit certain settings, such as the schedule.

Add: Click *Add* to launch the Assign Policy Wizard to select the devices to be assigned to the selected policy. For more information, see [Section 14.4, "Assigning Policies," on page 128](#).

Remove: Select the device by clicking the check box next to the appropriate device name, then click *Remove* to remove the device's assignment from this policy.

- 2c Review the information in the Event Log section, then make the desired changes.

The Event Log section lists all unacknowledged errors and warnings.

The Status column displays an icon indicating each item's status. Position the mouse pointer over each icon to display a short message describing the status of the item.

To acknowledge an error or warning, click its name in the Event Column, then click *Acknowledged* in the Message Detail Information dialog box that displays. You can also click *Advanced*, select the check box next to the appropriate event, then click *Acknowledge* (a check mark displays on the right side of the Date column to indicate that the item has been acknowledged).

2d Review the information in the Upcoming Events section.

The Upcoming Events section lists events scheduled for the selected policy. You can click the calendar icon to display a calendar to view events for the desired date. You can also use the arrows to view events for the previous or next day, week, or month.

2e Review the information in the Groups section, then make the desired configuration changes.

The Groups section lists the groups that contain the selected policy.

You can also use the following options:

Advanced: Click *Advanced* to display the Edit Groups page to display a list of the groups that contain the selected policy. You can click *Add* to open the Select Groups dialog box to add the selected policy to existing groups. You can also remove a group by selecting the check box next to the Name column, then clicking *Remove* to remove.

Add: Click *Add* to open the Select Groups dialog box, then click the blue arrow in the Select column to select the desired group and display its name in the Selected list box.

Remove: Select the check box next to the appropriate group name, then click *Remove* to remove the selected policy from the group.

3 Click the Details tab, then make the desired configuration changes.

3a You can add a new key or directory by selecting the directory under which you want to add the new key or directory. You can use the New menu to add a new key or directory.

If you want to configure more application keys using the same policy, the Import From a Device option is more appropriate. You can configure the device, test it, and then import the settings to update the policy.

You can import from the same device that was used to create the original policy or you can import from any other device. When you import settings, you have additional options, such as the following:

Add the new imported settings that are not present in the policy: Adds only those GConf settings that are not part of existing policy settings. This is selected by default. Use this option to update the policy by including more directories and keys.

Override the settings that are already present in the policy with the imported settings: Overrides the existing settings with the imported policy settings. Use this option to use the newly imported settings instead of the ones configured in the policy.

Remove settings from the policy that are not present among the imported settings:

Removes those policy settings that are not present in the imported settings. Use this feature to discard any additional settings that might be present in the original policy and that you do not want as a part of the updated policy.

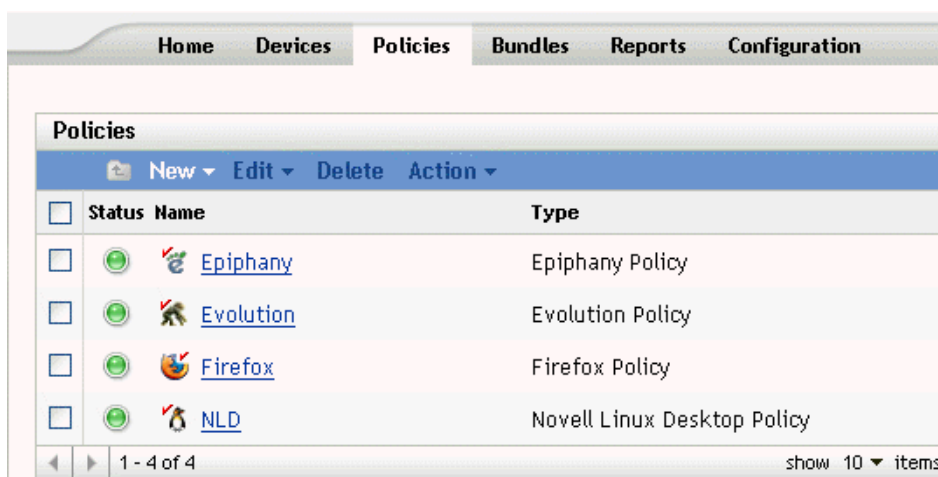
3b Edit the minimum system requirements according to your preferences. To edit the System Requirements of the Generic GNOME policy, see [Section 14.8, “Editing System Requirements,” on page 141](#).

- 3c Click *Apply* to save any changes you have made.
- 4 After a policy is modified, the Revision field of the policy (under the General section of the Summary page), must be incremented for the updated policy to be applied to associated devices. If the policy revision is not incremented, the changes made to the policy are not applied on the device.

14.7.3 Editing Remote Execute Policies

To edit the Remote Execute policy:

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



- 2 Click the policy's name to display the Summary page, then make the desired configuration changes.

If you do not want to edit any item on the Summary page, skip to **Step 3 on page 138**.

Use the Summary page to view detailed information about the selected policy. This page provides general information about the policy, lists the individual devices that are assigned to the policy, displays an event log, shows upcoming events, and lists the groups that the policy belongs to.

You can also use this page to edit the policy's description, add or remove assignments for the policy, and change other configuration settings, as described below.

- 2a Review the information in the General section, then make the desired configuration changes (you can edit only the Revision and Description options in this section).

Policy type: Displays the policy type as Remote Execute policy.

Revision: Displays the policy's revision number. To change the revision number, click *Increment Revision*.

Number of errors not acknowledged: Displays the number of unacknowledged errors.

Number of warnings not acknowledged: A warning is anything that does not cause the application of the policy to fail, but indicates minor problems. The number displayed indicates the number of unacknowledged warnings, which display in the Event Log section below.

GUID: Lists the selected object's GUID (global unique identifier), a randomly generated string that provides a unique identifier for the policy. You cannot edit the object's GUID.

Description: Displays the selected object's description, if one was provided when the policy was created. The description provides a short description of the policy's purpose. This description displays in the ZENworks Control Center interface.

Click *Edit* to change the description, if necessary.

- 2b** Review the information in the Assignments section, then make the desired configuration changes.

The Assignments section lists the devices, device groups and device folders to which the selected policy is assigned. You can also view the folder to which the device belongs and the schedule. You can click the device object name to view information about that device object.

You can also use the following options:

Advanced: Click *Advanced* to display the Edit Assignments page to display a list of the devices that are assigned to the selected policy, the folder that contains each device, and each device's schedule. You can use the Edit Assignments page to edit certain settings, such as the schedule.

Add: Click *Add* to launch the Assign Policy Wizard to select the devices to be assigned to the selected policy. For more information, see [Section 14.4, "Assigning Policies," on page 128](#).

Remove: Select the device by selecting the check box next to the appropriate device name, then click *Remove* to remove the device's assignment from this policy.

- 2c** Review the information in the Event Log section, then make the desired changes.

The Event Log section lists all unacknowledged errors and warnings.

The Status column displays an icon indicating each item's status. Position the mouse pointer over each icon to display a short message describing the status of the item.

To acknowledge an error or warning, click its name in the Event Column, then click *Acknowledged* in the Message Detail Information dialog box that displays. You can also click *Advanced*, select the check box next to the appropriate event, then click *Acknowledge* (a check mark displays on the right side of the Date column to indicate that the item has been acknowledged).

- 2d** Review the information in the Upcoming Events section.

The Upcoming Events section lists events scheduled for the selected policy. You can click the calendar icon to display a calendar to view events for the desired date. You can also use the arrows to view events for the previous or next day, week, or month.

- 2e** Review the information in the Groups section, then make the desired configuration changes.

The Groups section lists the groups that contain the selected policy.

You can also use the following options:

Advanced: Click *Advanced* to display the Edit Groups page to display a list of the groups that contain the selected policy. You can click *Add* to open the Select Groups dialog box to add the selected policy to existing groups. You can also remove a group by selecting the check box next to the Name column, then clicking *Remove*.

Add: Click *Add* to open the Select Groups dialog box, then click the blue arrow in the Select column to select the desired group and display its name in the Selected list box.

Remove: Select the check box next to the appropriate group name, then click *Remove* to remove the selected policy from the group.

- 3 Click the Details tab, then make the desired configuration changes. For more information about the available options, see [Section 13.6, “Remote Execute Policy,” on page 111](#).

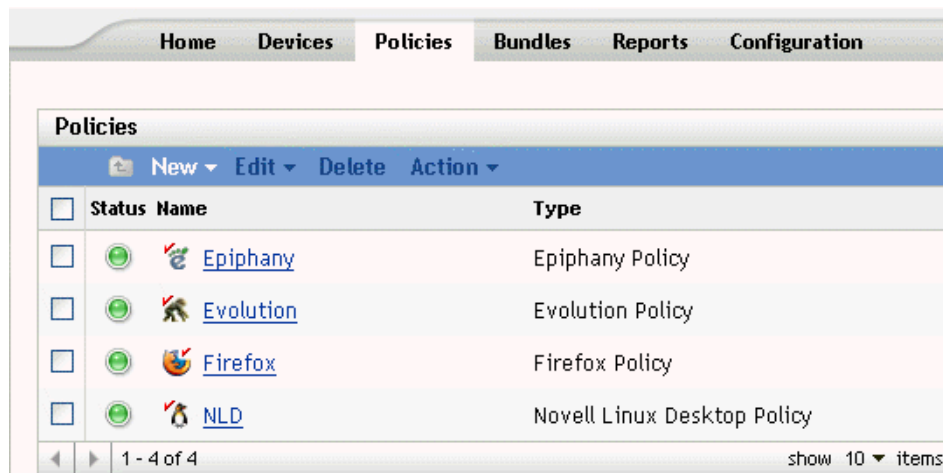
You can add system requirements to a policy. For more information, see [Section 14.8, “Editing System Requirements,” on page 141](#).

- 3a Click *Apply* to save any changes you have made.
- 4 After a policy is modified the Revision field of the policy (available under the General section of the Summary page), must be incremented for the updated policy to be applied to associated devices. If the policy revision is not incremented, the changes made to the policy are not applied on the device.

14.7.4 Editing Text File Policies

To edit the Text File Policy:

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



- 2 Click the policy's name to display the Summary page, then make the desired configuration changes.

If you do not want to edit any item on the Summary page, skip to [Step 3 on page 140](#).

Use the Summary page to view detailed information about the selected policy. This page provides general information about the policy, lists the individual devices that are assigned to the policy, displays an event log, shows upcoming events, and lists the groups that the policy belongs to.

You can also use this page to edit the policy's description, add or remove assignments for the policy, and change other configuration settings, as described below.

- 2a Review the information in the General section, then make the desired configuration changes (you can edit only the Revision and Description options in this section).

Policy type: Displays the policy type as Text File policy.

Revision: Displays the policy's revision number. To change the revision number, click *Increment revision*.

Number of errors not acknowledged: Displays the number of unacknowledged errors.

Number of warnings not acknowledged: A warning is anything that does not cause the application of the policy to fail, but indicates minor problems. The number displayed indicates the number of unacknowledged warnings, which display in the Event Log section below.

GUID: Lists the selected object's GUID (global unique identifier), a randomly generated string that provides a unique identifier for the policy. You cannot edit the object's GUID.

Description: Displays the selected object's description, if one was provided when the policy was created. The description provides a short description of the policy's purpose. This description displays in the ZENworks Control Center interface.

Click *Edit* to change the description, if necessary.

- 2b** Review the information in the Assignments section, then make the desired configuration changes.

The Assignments section lists the devices, device groups and device folders to which the selected policy is assigned. You can also view the folder to which the device belongs and the schedule. You can click the device object name to view information about that device object.

You can also use the following options:

Advanced: Click *Advanced* to display the Edit Assignments page to display a list of the devices that are assigned to the selected policy, the folder that contains each device, and each device's schedule. You can use the Edit Assignments page to edit certain settings, such as the schedule.

Add: Click *Add* to launch the Assign Policy Wizard to select the devices to be assigned to the selected policy. For more information, see [Section 14.4, “Assigning Policies,” on page 128](#).

Remove: Select the device by selecting the check box next to the appropriate device name, then click *Remove* to remove the device's assignment from this policy.

- 2c** Review the information in the Event Log section, then make the desired changes.

The Event Log section lists all unacknowledged errors and warnings.

The Status column displays an icon indicating each item's status. Position the mouse pointer over each icon to display a short message describing the status of the item.

To acknowledge an error or warning, click its name in the Event Column, then click *Acknowledged* in the Message Detail Information dialog box that displays. You can also click *Advanced*, select the check box next to the appropriate event, then click *Acknowledge* (a check mark displays on the right side of the Date column to indicate that the item has been acknowledged).

- 2d** Review the information in the Upcoming Events section.

The Upcoming Events section lists events scheduled for the selected policy. You can click the calendar icon to display a calendar to view events for the desired date. You can also use the arrows to view events for the previous or next day, week, or month.

- 2e** Review the information in the Groups section, then make the desired configuration changes.

The Groups section lists the groups that contain the selected policy.

You can also use the following options:

Advanced: Click *Advanced* to display the Edit Groups page to display a list of the groups that contain the selected policy. You can click *Add* to open the Select Groups dialog box to

add the selected policy to existing groups. You can also remove a group by selecting the check box next to the Name column, then clicking Remove to remove.

Add: Click *Add* to open the Select Groups dialog box, then click the blue arrow in the Select column to select the desired group and display its name in the Selected list box.

Remove: Select the check box next to the appropriate group name, then click *Remove* to remove the selected policy from the group.

- 3 Click the Details page. This page lets you perform the following actions:

Editing Item	Description
Edit the existing change(s) to be made	Lets you update the modifications to be made.
Add a new change to the same file	Lets you make multiple changes to the same file.
Add a new file to be changed and the corresponding changes	Lets you modify multiple files using the same policy.
Rename the change	Lets you keep the changed name consistent with the changes made.
Edit the file to be modified	Lets you edit the filename to apply the changes to another file or update the filename.
Delete files and changes	Lets you delete the files and changes.
Reorder files and changes	<p>A file is modified in the order of the changes shown in the ZENworks Control Center, you can use this option to order the sequence of changes. Because the second modification will be done on the updated file after the first modification is complete, and so on, ordering changes lets you perform logical operations.</p> <p>Ordering of files lets you modify files in a logical order.</p>
Edit the pre- and post-change actions	Lets you add, edit, or remove the pre- and post-change actions for the policy. You can also edit the action to be taken when a pre-change action fails.

You can add system requirements to a policy. For more information, see [Section 14.8, “Editing System Requirements,” on page 141](#).

3a Click *Apply* to save any changes you have made.

- 4 After a policy is modified, the Revision field of the policy (available under the General section of the Summary page) must be incremented for the updated policy to be applied to associated devices. If the policy revision is not incremented, the changes made to the policy are not applied on the device.

14.7.5 Viewing Policy Enforcement Status

You can view the status of a policy by looking at the icon located next to each policy. The following table describes each color code and its description:

Color Code	Policy Status
Green	Normal. The policy has been successfully enforced on all associated devices.
Yellow	Warning. A device has encountered a warning when trying to apply this policy.
Red Cross	Critical. A device has encountered an error when trying to apply this policy.

To view more information about a warning or error, click the policy to review the event log.

14.8 Editing System Requirements

The purpose of the system requirements is to limit some policies to run on devices that have the necessary requirements to enforce the policy. When more than one GConf-based policy of the same type is assigned, the first policy that meets the requirements is enforced on managed devices. All effective Remote Execute and Text File policies are enforced on managed devices.

You can specify the system requirements by defining certain conditions, called filters. You can set up simple system requirements that contain only one filter, or you can set up complex system requirements containing multiple filters or groups of filters. If you set up system requirements using more than one filter, you must also specify the logical relationship between the filters.

To set up a filter:

- 1 In the ZENworks Control Center, click the *Policies* tab.
- 2 Select a policy for which you want to edit the system requirements.
- 3 Click the *Details* tab.
- 4 In the Combine Filters Using field, select AND or OR.

This setting lets you specify the logical relationship between filter sets and filters. Select And to satisfy all the sets of filters and select Or to satisfy any one of the filter sets. By default, the filters are defined in one filter set. Within a filter set, select OR to satisfy any one of the filter conditions and select AND to satisfy all the filter conditions.

- 5 (Optional) Click *Add filter*. The new filter is added and it is applied based on the logical relationship you have defined in [Step 4 on page 141](#).
- 6 (Optional) Click *Add filter set* to add a new filter set. This filter is also applied based on the logical relationship you have defined in [Step 4 on page 141](#).
- 7 Select a value from the first drop-down list.

The operator list and other text boxes are displayed based on the value you have selected in the first drop-down list.

- 8 Specify a value in the text box. The following table describes values you can select in the first drop-down list and corresponding examples you can specify:

Criteria	Field 1	Field 2	Field 3
Date of File	Filename with complete path	Logical condition	Date
Distribution	Logical condition	Distribution name with version number	-

Criteria	Field 1	Field 2	Field 3
Environment	Environment Variable	Logical condition	Value
Find File	Filename with full path	Logical condition	-
Find RPM	RPM name Make sure that the RPM name you specify is case-sensitive.	Logical condition	-
Free Disk Space	File system. For example, /dev/hda1.	Logical condition	Value in KB
Kernel	Logical condition	Linux kernel_version. For example, Linux 2.6.5-7.111	-
Processor	Logical condition		-
Size of file	Filename with complete path	Logical condition	Size in bytes
Total Disk Space	File system. For example, /dev/hda1.	Logical condition	Value in KB
Used Disk Space	File System. For example, /dev/hda1	Logical condition	Value in KB
Version of RPM	RPM name Make sure that the RPM name you specify is case-sensitive.	Logical condition	Version (2.0.1)

9 Select an operator from the drop-down list.

The operator drop-down list is displayed based on the value you have selected in the first drop-down list. For example, if you select *Version of RPM*, the available operators are *Equal to*, *Not Equal to*, *Less Than*, *Greater than*, *Greater than or equal to*, and *Less than or equal to*. If you select *Size of file*, the available operators are *Less than*, *Greater than*, *Greater than or equal to*, and *Less than or equal to*. If you select *Date of file*, the available options are *On*, *After*, *On or after*, *Before*, and *On or before*. If you select *Date of file*, you can also select a specific date.

10 Click *Apply*.

14.9 Refreshing Policies

If you assign a new policy to a device or update a policy, you can ensure that the policy is updated on managed devices by refreshing the policies. Each device periodically refreshes its settings. It is not necessary to manually refresh each device after updating a policy. To ensure that the updated

policy is immediately pulled down, you can manually refresh the device using the following methods:

- In the ZENworks Control Center, go to the Devices page, select the appropriate device, click *Actions*, then click *Refresh Device*.
- On a managed device, start a console session and execute the following command: `/opt/novell/zenworks/bin/rug refresh`

Performing either action results in the managed device refreshing its policies and other settings. A newly assigned or updated policy is delivered to the device and is applied according to its schedule.

14.10 Verifying Policy Enforcement

ZENworks Linux Management lets you verify the enforcement of a policy after it has been assigned to a device or updated and the device has been refreshed (either manually or automatically by ZENworks). After a policy has been enforced, a message is logged indicating the success or failure of the policy enforcement. These messages can be seen in the Event log of the device on which the policy was applied or can be seen in the Event log of the policy that was applied.

To verify the enforcement of the GConf-based policies, you need to re-login to the assigned device. You can then start the application and verify that the policy has been enforced correctly.

If a desktop or user interface session is in progress on a managed device with GConf-based policies assigned to it, and an updated policy is enforced on that device by a console login or an `su` command, all updated settings may not be immediately applicable on the desktop session. The updated settings are reflected only when the user logs in via the user interface session again.

In the Novell Linux Desktop policy, some of the configuration settings are file-permission-based, and hence for a root user, these settings such as items in the Program menu and System menu will be accessible even if it is locked.

For the Remote Execute and Text File policies, the enforcement occurs according to the schedule. To verify the enforcement, check the managed device to ensure that the specified changes or actions have taken place.

You can also verify the enforcement status or check for errors by looking at the `zmd` log on the managed device (`/var/opt/novell/log/zenworks/zmd-messages.log`).

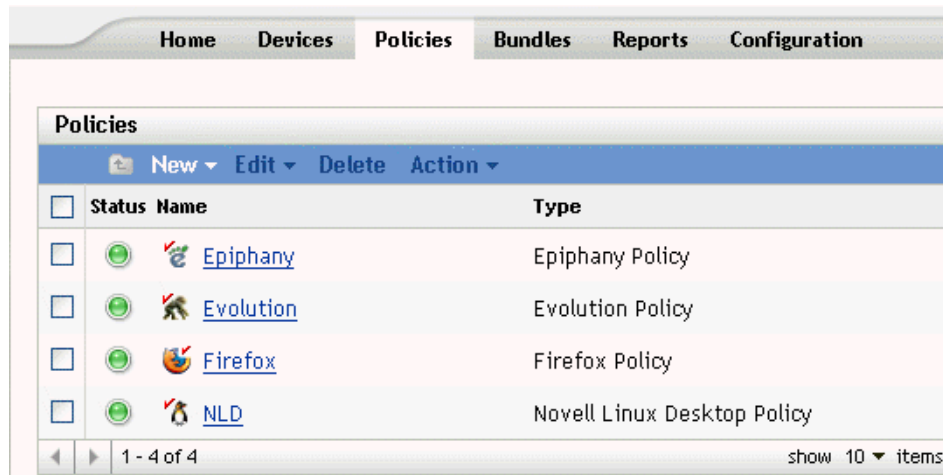
14.11 Renaming, Copying, or Moving Policies

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



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

- **Rename:** Click *Rename*, type a new name for the policy, then click *OK*.
- **Copy:** Click *Copy*, type a new name for the copy, then click *OK*.

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.

Only policy settings are copied; policy groups and assignments are not copied.

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

If you rename or move a policy, its assignments are still in place. ZENworks Linux Management does not reapply the policy to devices because of the name or location change.

14.12 Deleting Policies, Policy Groups, and Folders

Before you delete policies, policy groups, and folders from the ZENworks Control Center, review the following information to ensure that you obtain the desired results.

Deleting Policies: Depending on your needs, you can delete a policy from your ZENworks Linux Management system or remove a policy's assignments from devices.

If you delete a policy from your ZENworks Linux Management system, the policy does not display on the Policies or Devices pages in the ZENworks Control Center. When a policy is deleted, it is unassigned and unenforced from the device with which it was assigned. For more information, see [Section 14.13, "Unenforcing Policies," on page 145](#).

Deleting Policy Groups: The results of deleting a policy group is similar to that of deleting a policy.

If you delete a policy group from your ZENworks Linux Management system, the policy group does not display on the Policies page in the ZENworks Control Center and the policy group's assignments

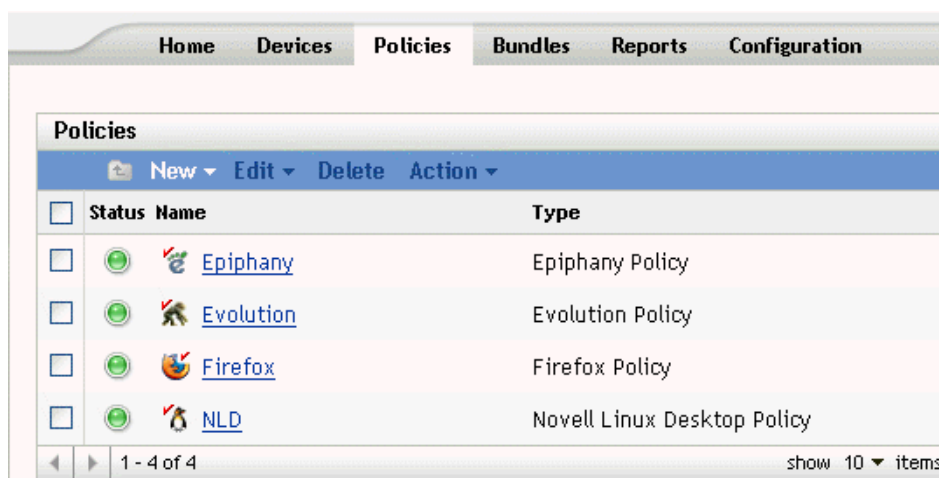
are removed. However, the individual policies contained in the group are not removed from the ZENworks Control Center and still display on the Policies page.

When a policy group is deleted, its member policies are not deleted, but the associations are removed. The policies of a policy group are unenforced from the devices to which the policy group was associated. For more information, see [Section 14.13, “Unenforcing Policies,” on page 145](#).

Deleting Folders: If you delete a folder that contains policies from your ZENworks Linux Management system, both the folder and its policies are removed from the ZENworks Control Center. The policies contained in the folder are unenforced from the device to which they were assigned. For more information, see [Section 14.13, “Unenforcing Policies,” on page 145](#).

To delete a policy, policy group, or folder:

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



- 2 In the Policies list, select the box next to the desired item's name, then click *Delete*.

If the item you are deleting is a folder, you are prompted whether or not to delete the folder and its contents.

When a policy folder is deleted, each of its policies and subfolders are also deleted.

14.13 Unenforcing Policies

Policies are unenforced when either a policy is deleted or it is unassigned from a device. On the next refresh, the policy data is removed from the managed device. For GConf-based policies, when a user logs in after a refresh, the configuration changes made by the policy are undone. Unenforcement is not supported for the Remote Execute and Text File policies.