opentext™

ZENworks
ZENworks Agent Guide

Legal Notice

Contents

About This Guide

This guide provides information about the ZENworks Agent, a component of ZENworks. For additional information about ZENworks and other Micro Focus products, visit www.novell.com (http://www.novell.com/products/zenworks).

The information in this guide is organized as follows:

Audience

This guide is intended for ZENworks end users (those with the ZENworks Agent on their devices).

Feedback

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

Additional Documentation

ZENworks is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the Zenworks documentation website.

1 Overview

The ZENworks Agent is a part of the ZENworks software that lets your administrator manage devices over the network. The ZENworks Agent provides services that help the administrator do the following without visiting your device:

- Manage policies that determine the behavior of your device.
- Deliver software, patches, and other files to your device.
- Take inventory of your device's hardware and software.
- Provide data encryption.
- Access your device from a remote location to troubleshoot and fix problems with hardware and software.

Each of these services is provided through the use of modules that plug in to the ZENworks Agent. Depending on the services implemented by the administrator, one or more of these modules might not be active on your device. For example, if your administrator does not intend to remotely access your workstation, the Remote Management module might not be installed on the device. Consequently, the Remote Management tab is not displayed in the ZENworks Agent page on the device. To view which modules are active on your device, see Status.

The ZENworks Agent connects to a ZENworks Primary Server. The Primary Server delivers policies and software for the agent to apply to your device, collects inventory information from the agent, and performs other services related to the management of your device. In some cases, your administrator might choose to have your device perform some of the duties of a Primary Server for other users in your system. As a result, your device might serve as one of the following:

- A satellite: Satellites can perform any of the following roles for a Primary Server: Authentication, Collection, Content, Imaging, and Join Proxy.
- A Windows Proxy: Windows Proxies perform discovery and deployment tasks that are Windows-based and cannot be performed by a Linux-based Primary Server.
- A Linux Proxy: Linux Proxies perform discovery and deployment tasks that are Linux-based and cannot be performed by a Windows-based Primary Server.

2 ZENworks Agent Update

The ZENworks Agent enables you to check for any available ZENworks software updates, snooze any update prompts, and resume the prompt to continue with the update. An *Update* is different than a *Refresh*. A *Refresh* updates the bundles and policies assigned to your computer, while an *Update* updates the ZENworks software itself.

The following sections contain more information:

2.1 Check for Updates

You can right-click the ZENworks icon 🔵 and select the **Check for Updates** option to check for any ZENworks software updates. This internally triggers a ZENworks Updater Service (ZeUS) refresh. If there are any pending updates, they will automatically start updating.

NOTE: In a terminal server, the **Check for Updates** option will be available only for a console session.

2.2 Snooze and Resume Update Prompts

When there is a system update, a ZENworks Update Available prompt is displayed denoting the action to be taken. You can snooze the prompt for a configured number of times before it starts updating automatically.

NOTE: If the Snooze option is not available, your ZENworks administrator has not enabled the option.

1. Click **Postpone** to postpone the prompt. If you want to start the update after some time, you can right-click the ZENworks icon 🔵, then select **Resume Updates** to display the update prompt. Click **Now** to start the update.

2. In the ZENworks icon menu, click the **Show Status** option to see the percentage completion of the update.

3. Select the **Exit** option if you do not want to receive any permission prompts or progress status messages. However, the update will still continue in the background.

3 Status

The ZENworks Agent provides information such as the last time it contacted a ZENworks Server, whether or not the Agent Modules are running, and the Closest Servers configured by the administrator in ZENworks Control Center.

The following sections contain more information:

3.1 Viewing the Agent's Status

1 Right-click the ZENworks icon 🔵 in the notification area, and select **Technician Application**.

2 In the left navigation pane, click **Agent**.

Status Field	Description
Device Address	The IP address of your device.
Device Name	The computer name for your device.
Network Environment	A network environment consists of services (gateways, DNS servers, DHCP servers, and so forth) that identify the environment.
Configuration Location	The device's location as determined by its current network environment. The configuration location determines which ZENworks server (or servers) the device connects to for authentication, configuration, content, and collection and Join Proxy service purposes.
Device State	The device's state: managed, unmanaged, retired, or unknown. Unknown displays only if there is an error.
Last Contact with Server	The last time the ZENworks Agent had contact with the ZENworks Server listed in the **Server DNS** field.
Next Contact with Server	The next time the ZENworks Agent is scheduled to contact (or be contacted by) the ZENworks Server.
HTTP Proxy	A proxy server lets a device connect indirectly to a ZENworks Server through the proxy server.
Join Proxy	Displays the *host name or IP port number* of the Join Proxy server to which the managed device is connected. If the managed device is not connected to Join Proxy server, the **Not Connected** status is displayed. If there is no Join Proxy server configured, the **Not Applicable** status is displayed.

Status Field	Description
Primary User	The most frequent user of the device. Frequency is determined by number of logins, amount of time logged in, or designated user; your administrator determines the method used to calculate the primary user.
ZENworks Agent Version	The version of the ZENworks Agent.
ZENworks Updater Service Version	The current highest version installed on your device.
ZENworks Updater Service Last Contact with Server	The last successful communication between ZENworks Updater Service and the Primary Server.
JRE Version	The version of the Java runtime environment used by the device. *This option is displayed only for Linux managed devices*.
Operating System Distribution	The type of operating system installed on the device. *This option is displayed only for Linux managed devices*.
Management Zone	The name of the ZENworks Management Zone in which your device is located.
Server DNS	The DNS name of the ZENworks Server that your device's ZENworks Agent communicates with to send and receive ZENworks content and information.
Server Address	The IP address of the ZENworks Server listed in the Server DNS field.
Registration Keys	The alphanumeric strings supplied during registration of the device in the Management Zone. Registration keys, which are defined by your administrator, help determine bundle and policy assignments.
Agent Security Settings	The Override Policy link displays the ZENworks Endpoint Security Agent About Box. You can use the About Box to override the current security policies. To do so, you must know the override password.
	If the ZENworks Endpoint Security Management Agent is not installed, the link displays the ZENworks Location Decider dialog box. You can use the Settings option to disable client self defense and the Agent Status option to view how the current Configuration location was determined. To do so, you must know the override password.
Agent Status	The status and versions of the Agent modules.

3.2 Registering with a Key

Your device must be registered in a ZENworks Management Zone in order to be managed. To facilitate this process, your administrator can create registration keys. A registration key is alphanumeric string that you optionally supply to the ZENworks Agent during registration of the device in order to automatically be assigned bundles and policies associated with the key.

Your administrator might provide you with a key and ask you to register (or reregister) your device. To do so:

1 Right-click the ZENworks icon in the notification area, and select Technician Application.

2 In the left navigation pane, click Agent.

3 In the Registration Keys field, type the registration key, then click Register.

The ZENworks Agent registers the device using the key you supplied.

Registration keys are cumulative, which means that when you register with more than one key, the device receives the bundles, policies, and group assignments associated with each of the keys. Each key used for registration is added to the list for future reference.

If you add a registration key to a device that is already registered in the Management Zone, the new key does not move the device to the folder specified by the new key.

To move a device to another folder, in ZENworks Control Center, click the Devices tab, click Servers or Workstations, click the check box next to the device that you want to move, click Edit, click Move, click the desired folder, then click OK. Moving a device by using the ZCC retains the device's existing assignments. You can also unregister then register the device, however, its existing assignments are removed.

3.3 Viewing the Closest Server Details

When you have multiple ZENworks Servers (Primary Servers and Satellites) in your Management Zone, the Closest Server rules determine which ZENworks Server a managed device contacts for each role (Collection, Content, Configuration, Authentication, and Join Proxy) defined by the administrator. You can view a list of the Closest Servers for the server roles configured by the administrator in ZENworks Control Center based on the location of the device, its network environment, or both.

1 Right-click the ZENworks icon in the notification area, and select Technician Application.

2 In the left navigation pane, click Servers.

The Closest Servers for Roles panel displays the Closest Server list based on the roles defined by the administrator.

Role	Description
Collection	Collects Inventory and message log information from each device to be listed in ZENworks Control Center and outputs the information to reports. Both ZENworks Primary Servers and Satellites can act as collection servers.
Configuration	Provides configuration settings and registration information to devices. Only ZENworks Primary Servers can act as configuration servers.

Role	Description
Content	Provides content to managed devices. Both ZENworks Primary Servers and Satellites can act as content servers.
Authentication	Authenticates managed devices to the Management Zone. Both ZENworks Primary Servers and Satellites can act as authentication servers. **NOTE:** The Authentication role is applicable only for the Windows managed devices.
JoinProxy	Helps in performing remote management operations on Windows managed devices that are in private network. Displays an URL with host name or IP port details.

NOTE: Linux or Mac devices cannot connect to Join Proxy. However you might find Join Proxy listed as the Closest Server in Z-icon Properties page of Linux or Mac devices when they are moved to a location that has Join Proxy.

4 Policies

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

You cannot change the policies applied by your administrator. However, it is helpful to understand the difference between user-assigned policies and device-assigned policies and how to see which policies are being applied.

The following sections contain more information:

- Section 4.1, "User-Assigned Versus Device-Assigned Policies," on page 17
- Section 4.2, "Viewing Policies," on page 17

4.1 User-Assigned Versus Device-Assigned Policies

Policies might be assigned to you or they might be assigned to your device. Policies assigned to you are referred to as user-assigned policies, and policies assigned to your device are referred to as device-assigned policies.

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

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

4.2 Viewing Policies

To view the policies assigned to you and your device:

1 Right-click the ZENworks icon 🔵 in the notification area.

2 Click **Technician Application**.

3 In the left navigation pane, click **Policies**.

If both user-associated and device-associated policies are effective for a device, only the policy that takes precedence according to the Policy Conflict Resolution settings is applied on the device. However, the **Effective** status for both policies is displayed as **Success** in the ZENworks Agent icon.

If the User Management Agent Feature is disabled or uninstalled in ZENworks Control Center (Agent Features panel on the ZENworks Agent page), the status for the DLU policy on the ZENworks Agent Policies page is displayed as **Success,** even though the policy is not effective on the device.

5 Windows Bundles

Software applications and other files are distributed to your device as bundles. A bundle consists of all the files, configuration settings, installation instructions, and so forth required to install the software on the device. This section is applicable only to ZENworks Configuration Management Windows devices.

The following sections contain more information:

5.1 Bundles Versus Applications

Bundles are different than standard applications, such as Windows Notepad, that already reside on your device. When you double-click a bundle to launch it, the ZENworks Agent might first complete a variety of distribution tasks before the application is launched, including installing the application files, running scripts, and changing the device's registry specific INI files, or environment variables. These tasks are all configured by your administrator to ensure that the application runs correctly on your device.

In some instances, a bundle's icon appears dimmed or grayed out. This indicates that your device does not meet the requirements that the administrator defined for the application, or the bundle is not scheduled to be available to you at that time. The ZENworks Agent does not distribute the application to your device until the requirements are met or the schedule is appropriate.

5.2 User-Assigned Versus Device-Assigned Bundles

The bundles that you see on your device might be assigned to you or they might be assigned to the device. Bundles assigned to you are referred to as user-assigned bundles, and bundles assigned to your device are referred to as device-assigned bundles.

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

The ZENworks Agent always displays the device-assigned bundles regardless of whether or not you are logged in. Device-assigned bundles can be launched by anyone who uses your device.

5.3 Accessing Bundles

There are three ways for accessing bundles on a ZENworks managed device assigned to you: the ZENworks Application, the ZENworks Explorer, and the ZENworks Agent.

5.3.1 ZENworks Application

The ZENworks Application is a standalone application that you can launch from the Start menu, or you can click the ZENworks icon 🔵 from the system tray.
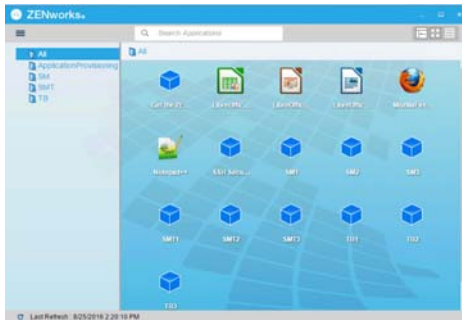
The ZENworks Window left pane displays the following:

- **[All] folder:** Contains all bundles that have been distributed to you, regardless of the folder in which they are located.
- **ZENworks folder:** Contains all bundles that have not been assigned to a different folder. The ZENworks folder is the default folder for bundles; however, your administrator can create additional folders in which to organize bundles, and can even rename the ZENworks folder.
- **Favorites:** Contains all bundles that have been set a favorite. This folder will be displayed only if the setting Enable Users to manage Favorites is enabled in the ZENworks Explorer Configuration Policy.

When you select a folder in the left pane, the right pane displays the bundles that the folder contains You can:

- Install a bundle or launch an application for an already installed bundle.

- View the properties of a bundle. The properties include a description of the bundle, information about people to contact for help with the bundle, the times when the bundle is available for use, and the system requirements established for the bundle.
- Repair an installed application.
- Uninstall an application. This is an administrator-controlled feature that might not be enabled.
- Postpone Operation. This feature allows a user to postpone the download of contents until the next refresh. The postpone operation appears only when the content being downloaded is fairly large in size.

5.3.2   ZENworks Explorer

ZENworks Explorer is an extension to Windows Explorer that enables bundles to be displayed in Windows Explorer, on the desktop, on the Start menu, on the Quick Launch toolbar, and in the notification area. The following graphic shows bundles displayed in Windows Explorer.
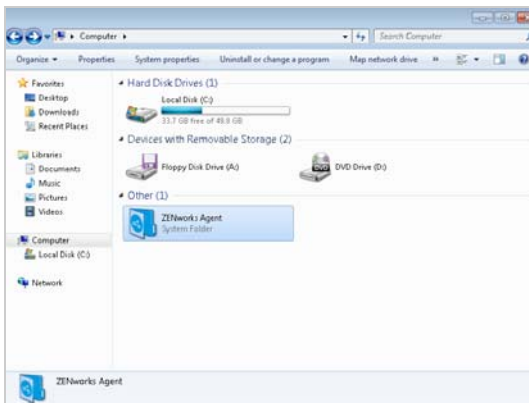
The following graphic shows bundles displayed on the desktop.
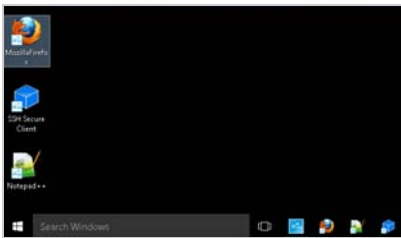
You can perform the same tasks on the bundles in the ZENworks Explorer as you can in the ZENworks Application. You can also view the Favorites folder in the ZENworks Explorer window, which will be displayed only if the setting Enable Users to manage Favorites is enabled in the ZENworks Explorer Configuration Policy.

5.3.3 ZENworks Agent

To open the ZENworks Agent on a Windows device, right-click the ZENworks icon in the notification area, and select **Technician Application**. This is an administrator-controlled feature that might not be enabled.

The **Bundles** link, located in the left navigation pane of the ZENworks Agent, lets you view the bundles that are assigned to your device.
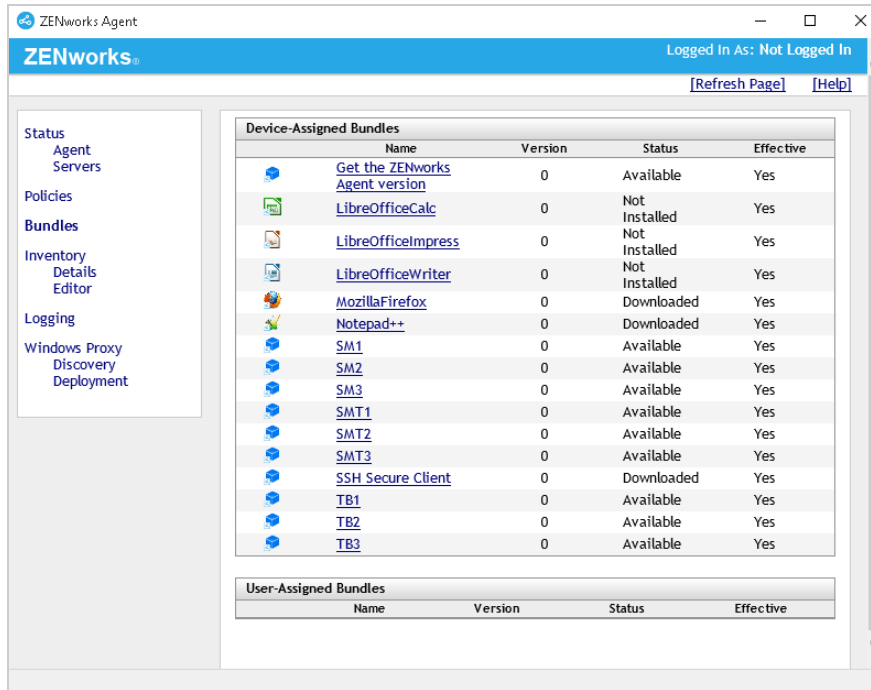
The bundle list includes the following information:

* **Name:** Displays the name of the bundle. Click the name to display the properties for the bundle, including such information as the version, folder, icon, help contacts, and the time schedules. Based on the configuration of the schedules for the bundle in ZENworks Control Center, the time schedules are as follows:

Time Schedule	Details
No Schedule / Default	No schedule is configured for the bundle
On a Specific Event	Runs the scheduled action when the specified event is triggered such as user login, user logout, or device boot
Relative	Runs the scheduled action relative to a specified number of days, hours, and minutes from when the device is refreshed
Daily	Runs the scheduled action daily at the specified time
Weekly	Runs the scheduled action on the selected day of the week
Monthly	Runs the scheduled action on the selected day of the month
Yearly	Runs the scheduled action on the selected day of the year

Time Schedule	Details
Specific Date and Time	Runs the scheduled action once on the date and time specified
Specific Time Interval	Repeatedly runs the scheduled action every xxx months, weeks, days, hours, and/or minutes from the start time
On Refresh	Runs the scheduled action on device refresh
Always	The scheduled action is always active.
Date Specific	Runs the scheduled action on the specified date
Day Range	Runs the scheduled action during the specified time interval

- **Status:** Displays the installation status for the bundle.
- **Effective:** Displays whether or not the bundle can be used on the device. If the Effective box is selected, the bundle meets all system requirements and schedule constraints to be used. You can click the bundle icon to launch the bundle.

   If the box is not selected, the bundle cannot be used. To find out why, click the bundle name to display the system requirements and schedule properties.

5.4 Understanding Bundle Icons

A bundle icon changes to reflect the current status of the bundle. The following table shows the bundle icons using the default light blue background icon. Your administrator might choose to use a different background icon; however, the status icons such as remain the same.

You can choose to hide or display the overlay icons that appear over the bundle icons in the agent. To change the overlay icon settings, in ZENworks Control Center, go to Configuration > Device Management > ZENworks Explorer Configuration, and select Disable Icon Overlays.

Icon	Status
	Available. You can launch the bundle.
	Unavailable. You cannot launch the bundle. Either the device does not meet the system requirements established for the bundle.
	Installing. The bundle is installing to the device. Downloading. The bundle is downloading from the network location where it is stored. Uninstalling. The bundle is being removed from the device. Running. The bundle is currently running.
	Downloaded: Downloaded but not installed: The bundle has been downloaded on the device. However, it has not been installed as yet.

Icon	Status
	Blocked. The bundle is blocked on the device. You cannot perform any of the actions on the bundle other than viewing its properties.
	Favorite: The bundle is set as a favorite.

NOTE: The bundle icons on the Start menu, Start menu tiles and Taskbar might not be consistent when the bundle status changes as this is an experimental feature for this release. After you sign out and sign into the device, the icons will become consistent.

5.5 Launching a Bundle

By default, the ZENworks Agent does not distribute (download and install) a bundle to your device until the first time you launch it. The distribution process might include installing the bundle's files, running scripts, and changing the device's registry, specific INI files, or environment variables. Or, the process might include nothing more than providing a shortcut to the application's executable file on your local device or a network server.

To launch a bundle:

1 Access the bundle in one of the following locations:

   ZENworks Window: From the **Start** menu, click **Programs** > **Novell ZENworks** > **ZENworks Application**.

   ZENworks Explorer: Open Windows Explorer and find the ZENworks Agent entry. Depending on how your ZENworks administrator configured the bundle, the bundle icon might also be displayed on the desktop, Start menu, Quick Launch toolbar, Start Menu Tiles, Task Bar, or notification area.

2 Double-click the bundle icon.

If the bundle has an Install MSI or Install Network MSI action, you might be prompted to enter the password when the bundle is launched on the device. To launch the bundle, you must log in to the device by using an user account that has a password configured.

5.6 Postponing a Bundle Download

If, after you launch a bundle, it begins to download and you need to stop the download, you can postpone the download to a later time. When you resume the download, it continues from the point where it previously stopped.

To postpone a bundle download:

1 Access the bundle in one of the following locations:

   ZENworks Window: From the **Start** menu, click **Programs** > **Novell ZENworks** > **ZENworks Application**.

ZENworks Explorer: Open Windows Explorer and find the ![icon] ZENworks Agent entry. Depending on how your ZENworks administrator configured the bundle, the bundle icon might also be displayed on the desktop, Start menu, Quick Launch toolbar, Start Menu Tiles, Task Bar, or notification area.

2 Right-click the bundle icon, then click **Postpone**.

5.7   Repairing a Bundle

If an installed application is not functioning correctly or you think it might be outdated, you can repair that the application's bundle information is still correct. If it is not, the ZENworks Agent reinstalls the bundle to your workstation.

To repair a bundle:

1 Access the bundle in one of the following locations:

ZENworks Window: From the **Start** menu, click **Programs** > **Novell ZENworks** > **ZENworks Application**.

ZENworks Explorer: Open Windows Explorer and find the ![icon] ZENworks Agent entry. Depending on how your ZENworks administrator configured the bundle, the bundle icon might also be displayed on the desktop, Start menu, Quick Launch toolbar, Start Menu Tiles, Task Bar, or notification area.

2 Right-click the bundle icon, then click **Repair**.

5.8   Viewing a Bundle's Properties

You can view a bundle's properties to see its version number, current installation status, and help contacts. In addition, if the bundle is unavailable, you can see if it is unavailable because of system requirements or schedule restrictions.

To view a bundle's properties:

1 Access the bundle in one of the following locations:

ZENworks Window: From the **Start** menu, click **Programs** > **Novell ZENworks** > **ZENworks Application**.

ZENworks Explorer: Open Windows Explorer and find the ![icon] ZENworks Agent entry. Depending on how your ZENworks administrator configured the bundle, the bundle icon might also be displayed on the desktop, Start menu, Quick Launch toolbar, Start Menu Tiles, Task Bar, or notification area.

2 Right-click the bundle icon, then click **Properties**.

5.9 Uninstalling a Bundle

Uninstall is an administrator-controlled feature. By default, uninstall is not enabled, which means that you can only uninstall bundles if your administrator has enabled the feature. Uninstall is enabled on a per-bundle basis. Depending on what your administrator enables, you might be able to uninstall some bundles but not others.

When you uninstall a bundle, the ZENworks Agent removes all files from your device and undoes all configuration settings made to your device during the bundle installation. Only files that the ZENworks Agent installs specifically for the bundle are removed. For example, the ZENworks Agent does not remove any shared files (files used by another application) or any user-created files such as word processing documents or spreadsheets.

After you uninstall a bundle, the bundle's icon remains on your device. This enables you to install the bundle again whenever necessary.

To uninstall a bundle:

1 Access the bundle in one of the following locations:

   ZENworks Window: From the **Start** menu, click **Programs** > **Novell ZENworks** > **ZENworks Application**.

   ZENworks Explorer: Open Windows Explorer and find the ZENworks Agent entry. Depending on how your ZENworks administrator configured the bundle, the bundle icon might also be displayed on the desktop, Start menu, Quick Launch toolbar, Start Menu Tiles, Task Bar, or notification area.

2 Right-click the bundle icon, then click **Uninstall**.

5.10 Managing Favorites

You can set a bundle as a favorite, to enable easy access to these bundles. You can set bundles as favorites from the desktop, from the file explorer, or from the ZENworks Application window. To add a bundle as a favorite, right-click the bundle icon and select **Set as Favorite**. A badge icon is appended to the bundle icon that is marked as a favorite. All bundles that are marked as favorites can be viewed in the **Favorites** folder displayed in the left pane of the ZENworks Application window and in the ZENworks Explorer window. You can also view a bundle as a favorite in the Start menu of your device (only if the bundle is pinned to the Start menu). Also, the bundles that are marked as favorites will be displayed as favorite bundles on other devices on which the user has logged in, if these bundles are available on those devices.

To remove the favorite tag from a bundle, right-click the bundle icon and select **Remove as Favorite**.

NOTE: The administrator can disable this feature in the ZENworks Explorer Configuration Policy.

6 Linux Bundles

Software applications and other files are distributed to your device as bundles. A bundle contains all of the content (such as files) and instructions (registry modifications, shortcut information, etc.) required to install the software on the device. This section is applicable only to ZENworks Configuration Management Linux devices.

The following sections contain more information:

6.1 Bundles Versus Applications

Bundles are different from standard applications, such as gedit, that already reside on your device. When you double-click a bundle to launch it, the ZENworks Agent might first complete a variety of distribution tasks before the application is launched, including installing the application files and running scripts and environment variables.These tasks are all configured by the administrator to ensure that the application runs correctly on your device.

In some instances, a bundle icon appears dimmed or grayed out. This indicates that your device does not meet the requirements that the administrator defined for the application or that the bundle is not scheduled to be available to you at that time. The ZENworks Agent does not distribute the application to your device until the requirements are met or the schedule is appropriate or the bundle is blocked.

6.2 Device-Assigned Bundles

The bundles that you see on your device are the bundles that are assigned to the device. Bundles assigned to your device are referred to as device-assigned bundles.

The ZENworks Agent always displays the device-assigned bundles regardless of whether you are logged in or not. Device-assigned bundles can be launched by users who have appropriate privilege access. To provide privilege access, the following zac commands need to be executed:

- `zac ua` to add local user to the privilege store.

- ◆ `zac ue` to edit the local user privileges
- ◆ `zac ul` to list all the users added to the privilege store.

For more information on these commands, see ZENworks Command Line Utilities Reference.

6.3 Accessing Bundles

There are two ways for accessing bundles on a ZENworks managed device: the ZENworks Window and the ZENworks Agent.

- ◆ Section 6.3.1, "ZENworks Window," on page 28
- ◆ Section 6.3.2, "ZENworks Agent," on page 30

6.3.1 ZENworks Window

The ZENworks Window is a standalone application that you can launch by using any one of the following options:

Option 1: In the notifications area of the Linux-managed device, right-click the ZENworks icon 🌐, and then select **ZENworks Window.**

Option 2: To launch the ZENworks Window on the managed device, follow the instructions provided for specific platforms supported by the device.

- ◆ **On GNOME desktops:**
  - ◆ RHEL 4: Select **Applications** > **System Settings** > **ZENworks Window**.
  - ◆ RHEL 5: Select **System** > **Administration** > **ZENworks Window**.
  - ◆ SUSE 10 or 11: Click **Computer**, then select **Applications** > **More Applications** > **System** > **ZENworks Window**.

    You do not need to select the **More Applications** tab if you have previously launched the ZENworks Window on the device.

- ◆ **On KDE desktops:**
  - ◆ RHEL 4: Right-click the Red Hat icon 🎩, then select **System Settings** > **ZENworks Window**.
  - ◆ RHEL 5: Right-click the Red Hat icon 🎩, then select **Administration** > **ZENworks Window**.
  - ◆ SUSE 10: Right-click the Application Launcher icon 🌐, then select **System** > **Configuration** > **ZENworks Window**.
  - ◆ SUSE 11: Right-click the Application Launcher icon 🌐, then select **Applications** > **System** > **Configuration** > **ZENworks Window**.
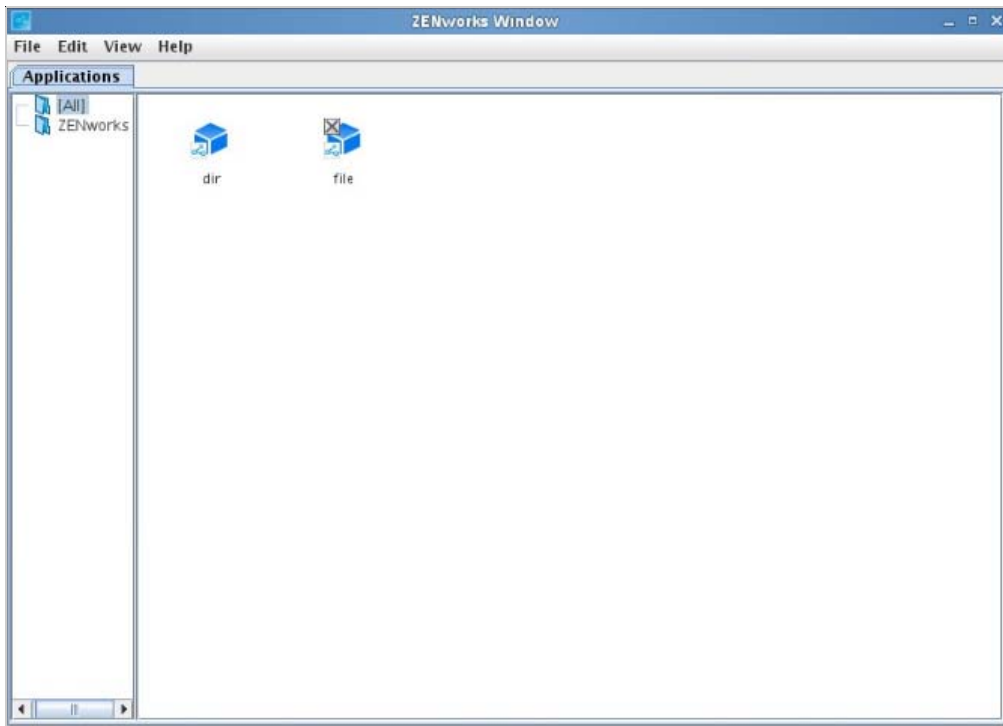
The ZENworks Window left pane displays the following:

 * **[All] folder:** Contains all bundles that have been distributed to you, regardless of the folder in which they are located.

 * **ZENworks folder:** Contains all bundles that have not been assigned to a different folder. The ZENworks folder is the default folder for bundles; however, the administrator can create additional folders for organizing bundles and even rename the ZENworks folder.

When you select a folder in the left pane, the right pane displays the bundles that the folder contains. You can:

 * Install a bundle or launch an application for an already installed bundle.

 * View the properties of the bundle. The properties include a description of the bundle, information about people to contact for help associated with the bundle, the times when the bundle is available for use, and the system requirements established for the bundle.

 * Repair an installed application.

 * Uninstall an application. This is an administrator-controlled feature that might not be enabled.

 * Postpone Operation. This feature allows a user to postpone the download of contents until the next refresh. The postpone operation appears only when the content being downloaded is fairly large in size.

6.3.2 ZENworks Agent

To open the ZENworks Agent on a Linux device, right-click the ZENworks icon ⬡ in the notification area, and select **Show Properties** or simply click the icon. The **Bundles** link, located in the left navigation pane of the ZENworks Agent, lets you view the bundles that are assigned to your device.

The bundle list includes the following information:

- **Name:** Displays the name of the bundle. Click the name to display the properties of the bundle, including information such as the version, folder, icon, help contacts, and the time schedules. Based on how the bundle is configured in ZENworks Control Center, you might see the following time schedules:

Time Schedule	Details
No Schedule/Default	Indicated that no schedule is configured for the bundle
On a Specific Event	Runs the scheduled action when the specified event is triggered, for example, user login, user logout, or device boot
Relative	Runs the scheduled action relative to a specified number of days, hours, and minutes from the time the device is refreshed
Daily	Runs the scheduled action daily at the specified time
Weekly	Runs the scheduled action on the selected day of the week
Monthly	Runs the scheduled action on the selected day of the month
Yearly	Runs the scheduled action on the selected day of the year
Specific Date and Time	Runs the scheduled action once on the date and time specified
Specific Time Interval	Repeatedly runs the scheduled action every xxx months, weeks, days, hours, and/or minutes from the start time
On Refresh	Runs the scheduled action on device refresh
Always	Indicates the scheduled action is always active
Date Specific	Runs the scheduled action on the specified date
Day Range	Runs the scheduled action during the specified time interval

- **Version:** Displays the version of the bundle assigned to the device.
- **Status:** Displays the installation status of the bundle.
- **Effective:** Displays whether or not the bundle can be used on the device. If the **Effective** box is selected, the bundle meets all system requirements and schedule constraints to be used. You can click the bundle icon 🖥 to launch the bundle.

  If the box is not selected, the bundle cannot be used. To find out why, click the bundle name to display the system requirements and schedule properties.

6.4 Understanding Bundle Icons

A bundle icon changes to reflect the current status of the bundle. The following table shows the bundle icons with the default light blue background icon. Your administrator might choose to use a different background icon; however, the status icons such as ⟳ and ☑ remain the same.

You can choose to hide or display the overlay icons that appear over the bundle icons in the agent. To change the overlay icon settings, in ZENworks Control Center, go to **Configuration** > **ZENworks Explorer Configuration,** and select **Disable Icon Overlays**.

Icon	Status
	Available. You can launch the bundle.
	Unavailable. You cannot launch the bundle. Either the device does not meet the system requirements established for the bundle or the bundle is not scheduled to be available at the current time.
	Downloading. The bundle is downloading from the network location where it is stored.s
	Installing. The bundle is being installed on the device.
	Running. The bundle is currently running.
	Uninstalling. The bundle is being removed from the device.
	Not Installed. The bundle failed to install. Right-click the icon, then click **Repair** to repair the bundle.
	Blocked. The bundle is blocked on the device. You cannot perform any of the actions on the bundle other than viewing its properties.

6.5 Launching a Bundle

By default, the ZENworks Agent does not distribute (download and install) a bundle to your device until the first time you launch it. The distribution process might include installing the bundle files, running scripts, and changing the environment variables.

To launch a bundle:

1 Access a bundle from the ZENworks Window. For more information, see Accessing Bundles.

2 To launch a bundle in the ZENworks Window, do one of the following:

 ◆ Right-click the bundle icon, then select **Open**.

- Double-click the bundle icon.
- Click **File** > **Open**, select a bundle, then click **Open**.

6.6 Postponing a Bundle Download

If you need to stop a bundle download after it begins, you can postpone the download to a later time. When you resume the download, it continues from the point where it previously stopped.

To postpone a bundle download:

1 Access a bundle from the ZENworks Window. For more information, see Accessing Bundles.

2 Right-click the bundle icon, then click **Postpone**.

or

Select a bundle(s) that you want to postpone then, click **File** > **Postpone**.

6.7 Verifying a Bundle

If an installed application is not functioning correctly or it is outdated, you can verify that the bundle information about the application is still correct. If it is not, the ZENworks Agent reinstalls the bundle on your workstation.

To verify a bundle:

1 Access a bundle from the ZENworks Window. For more information, see Accessing Bundles.

2 Right-click the bundle icon, then click **Verify**.

or

Select the bundle(s) you want to verify, then click **File** > **Verify**.

6.8 Viewing the Properties of a Bundle

You can view the properties of a bundle to see its version number, current installation status, and help contacts. In addition, if the bundle is unavailable, you can check if it is unavailable because of system requirements or schedule restrictions.

To view the properties of a bundle:

1 Access a bundle from the ZENworks Window. For more information, see Accessing Bundles.

2 Right-click the bundle icon, then click **Properties**.

or

Select the bundle(s), then click **File** > **Properties**.

6.9 Uninstalling a Bundle

Uninstalling is an administrator-controlled feature. By default, uninstalling is not enabled, which means that you can uninstall bundles only if your administrator has enabled this feature. Uninstalling is enabled on a per-bundle basis. Depending on what your administrator enables, you might be able to uninstall some bundles but not others.

When you uninstall a bundle, the ZENworks Agent removes all files from your device and reserves all configuration settings made to your device during bundle installation. Only the files that the ZENworks Agent installs specifically for the bundle are removed. For example, the ZENworks Agent does not remove any shared files (files used by another application) or any user-created files such as word processing documents or spreadsheets.

After you uninstall a bundle, the bundle icon remains on your device. This enables you to install the bundle again whenever necessary.

To uninstall a bundle:

1 Access a bundle from the ZENworks Window. For more information, see Accessing Bundles.

2 Right-click the bundle icon, then click **Uninstall**.

   or

   Select the bundle(s), then click **File** > **Uninstall**.

7 Bundle Locks

The ZENworks Agent allows you to create bundle lock rules for bundles on the managed devices for Linux, Macintosh, and Patch bundles to prevent them from being installed on the managed devices. This section is applicable only to Linux and Macintosh devices using ZENworks Configuration Management.

The following sections provide more information:

7.1 Configuring Bundle Locks

You can configure bundle locks only for Install Action set.

1 Right-click the ZENworks icon in the notification area.

2 Click **Technician Application**.

3 In the left navigation pane, click **Bundle Locks**, then fill in the following fields:

- **Bundle Name or Pattern:** Specify the bundle name or pattern that you want to lock.
- **Bundle Type:** Select the bundle type for which you want to set the lock. The available bundle types include:
  - **On a Linux device:** Bundle, Linux Bundle, and Linux Patch Bundle.
  - **On a Macintosh device:** Bundle, Macintosh Bundle, and Macintosh Patch Bundle.
- **Deny Install:** Select this check box to prevent the installation of the bundle on the managed device.

4 Click **Lock** to configure the bundle lock for the specified bundle.

7.2 Viewing the Bundle Lock Details

You can view the details of all the bundle locks in the Bundle Lock Manager panel.

To view the bundle lock details:

1 Right-click the ZENworks icon in the notification area.

2 Click **Technician Application**.

3 In the left navigation pane, click **Bundle Locks**.

The Bundle Lock Manager panel displays the following details:

Field	Description
Bundle Name or Pattern	Displays the bundle name or pattern created by the ZENworks Administrator.
Bundle Type	Displays the type of bundle selected by the administrator to lock.
Deny Install	Displays whether the bundle installation is allowed or not.

7.3 Deleting Bundle Locks

The Bundle Lock Manager panel displays the bundle locks that have been configured. To delete a bundle lock:

1 Right-click the ZENworks icon in the notification area.

2 Click **Technician Application**.

3 On the left navigation pane, click **Bundle Locks**.

4 In the Bundle Lock Manager panel, click **Remove Lock**.

8 Inventory

The ZENworks Agent scans your device for software and hardware information. This information is viewable by both you and your administrator.

The following sections contain more information:

8.1 What Is Inventory Information Used For?

The software and hardware inventory taken from your device might be used in a variety of ways. Your hardware information, for example, might be used by your administrator to see whether or not your device meets the system requirements for a bundle you need. Or, your software information might be used to validate compliance with company software standards.

You can use the inventory information to quickly find out details about your device, such as its asset tag number, IP address, total memory, and free disk space. You can view hardware details, such as the manufacturer and model of your hard drives, disk drives, and video card. You can also view software details, such as installed hot fixes and patches and the version numbers and locations of installed software products.

8.2 Scanning the Device

Unless your administrator has disabled the inventory scan schedule, the ZENworks Agent performs an inventory scan on your device on a regular basis. Your administrator determines the schedule; the default schedule is the first day of every month.

You can also initiate an inventory scan on your device, unless your administrator has disabled your ability to do so.

To initiate a scan:

1 Right-click the ZENworks icon in the notification area.

2 Click **Technician Application**.

3 From the left navigation pane, in the inventory menu, click **Details**.

4 Click **Scan Now**.

There is no indication that the scan is being performed. However, when you refresh the Inventory page, you know the scan occurred if the **Last Scan** field displays the current date and time. You can click **View Inventory Details** to see the results of the scan.

8.3 Viewing Inventory Information

You can use the inventory information to quickly find out details about your device, such as its asset tag number, IP address, total memory, and free disk space. You can view hardware details, such as the manufacturer and model of your hard drives, disk drives, and video card. You can also view software details, such as installed hot fixes and patches and the version numbers and locations of installed software products.

To view inventory information:

1 Right-click the ZENworks icon ⬡ in the notification area.

2 Click **Technician Application**.

3 From the left navigation pane, in the inventory menu, click **Details**.

4 Click **View Inventory Details**.

8.4 Completing a Collection Data Form

In addition to being able to schedule regular scans of your device, your administrator can create a collection data form to gather additional information from you. The information requested in the data form is determined by your administrator.

The collection data form appears as a dialog box on your desktop and remains until you submit the form. In addition, your administrator can configure the ZENworks Agent to display the form as an option when you right-click the ZENworks icon ⬡ in the notification area. In this case, the option remains even after you submit it; this allows you to resubmit the form when any of the requested information changes.

8.5 Working with the Inventory Collection Editor

You can use the collection editor to view and manage the inventory data. Any ZENworks administrator can access the collection editor by using login credentials. Only one administrator can log in to the collection editor at a time.

To log in to the collection editor:

1 Right-click the ZENworks icon ⬡ in the notification area.

2 Click **Technician Application**.

3 From the left navigation pane, in the inventory menu, click **Editor**.

After you have logged in as an administrator, you can edit the serial number and asset tag of the workstation and the hardware devices. You can also add new hardware. When you make changes, only a single undo is allowed. The value after an undo is the value that was loaded while you logged in to the editor.Clicking **Reset** removes all the manually added and edited information and restores the data from the collector. Clicking on **Update Collected Data** or clicking **Reset**, initiates a background inventory scan for hardware devices. You need to wait for the scan to complete before making any changes.

If you add new hardware, it appears at the bottom of the scanned report. Make sure to use the format in the examples provided below each field, because invalid data entries might not be added to the report.

The serial number and the asset tag for the newly added hardware devices are editable, and you can delete any manually added hardware entries. A collection editor session remains active for 300 seconds and then expires. Navigating to another tab logs you out of the collection editor.

9 Remote Management

The ZENworks Agent supports management of your device from a remote location. This enables your administrator or Help Desk personnel to remotely access or control your device in order to resolve problems with the device. This section is applicable only for Windows devices.

NOTE: If the device is connected through Remote Desktop Connection, the **Remote Management** tab is not displayed in the ZENworks Agent page on the device because remote management of terminal sessions is not supported.

The following sections contain more information:

9.1 Remote Management Operations

The ZENworks Agent supports the following Remote Management operations:

- **Remote Control:** Enables a remote operator (such as your administrator or a help desk operator) to control your device.
- **Remote View:** Enables a remote operator to view your device. This is a view-only mode; the operator cannot perform any actions on your device.
- **Remote Diagnostics:** Enables a remote operator to run specific administrative tools (such as Registry Editor, Computer Management, and Services) for diagnostic purposes.
- **File Transfer:** Enables a remote operator to transfer files to and from your device.
- **Remote Execute:** Enables a remote operator to run executables on your device.

The operations that are allowed on your device depend on which ones your administrator has enabled. For information about viewing which operations are available, see Viewing the Remote Management Policy.

9.2 Requesting a Remote Management Session

In some situations, you might want to request a Remote Management session with a remote operator, or you might be requested by a remote operator to initiate a session.

To request a session:

1 Right-click the ZENworks icon 🔗 in the notification area.

2 Click **Technician Application**.

3 In the left navigation pane, locate the **Remote Management** heading, then click **General**.

4 Click **Request Remote Management Session** to display the Request Session dialog box.

The ability to request a Remote Management session is controlled by your administrator, which means the option might be disabled, particularly if your company or department does not have dedicated help desk personnel to serve as on-call remote operators. If the **Request Remote Management Session** option is not displayed as linked text, the option is disabled.

5 In the **Listening Remote Operators** list, select the remote operator you want to open the remote session with.

or

If the remote operator is not listed, enter the operator's connection information in the **Request Connection** fields.

6 In the **Operation** field, select the type of operation (Remote Control, Remote View, Remote Diagnostics, File Transfer, or Remote Execute) you want to open. For information about each operation, see Remote Management Operations.

7 Click **Request** to launch the session.

9.3 Viewing Currently Connected Remote Operators

1 Right-click the ZENworks icon in the notification area.

2 Click **Technician Application**.

3 In the left navigation pane, locate the **Remote Management** heading, then click **General**.

4 Click **List Connected Remote Operators** to display the Request Operators dialog box.

The ability to view connected remote operators is controlled by your administrator. If the **List Connected Remote Operators** option is not displayed as linked text, the option is disabled.

9.4 Viewing the Remote Management Policy

The Remote Management operations that are enabled on your device, and the settings that apply to those operations, are controlled by your administrator through the use of a Remote Management policy.

You can view the policy settings. However, you cannot change any of the settings. To view the settings:

1 Right-click the ZENworks icon in the notification area.

2 Click **Technician Application**.

3 In the left navigation pane, locate the **Remote Management** heading, then click **Policy**.

4 In the **Category** list, select the policy category you want to view: General, Remote Control, Remote View, Remote Execute, File Transfer, Remote Diagnostics, or Security.

9.5 Using the Security Settings

The Remote Management security settings let you control the password required to perform remote operations on your device, re-enable operations after they have been suspended because of a detected intruder, display information about the Remote Management operations performed on your device, and display information about the self-signed certificate used for remote operations.

The security settings are controlled by your administrator and might not be available for you to use.

1 Right-click the ZENworks icon 🔵 in the notification area.

2 Click **Technician Application**.

3 In the left navigation pane, locate the **Remote Management** heading, then click **Security**.

4 Click the security setting you want to use:

   Set Password: You can set the password only if the **Allow user to set password on the managed device** option is enabled for the managed device. There are two types of password:

   - **ZENworks® password:** This password is used in ZENworks password-based authentication. It can be up to 255 characters long.

   - **VNC password:** This password is used in VNC password-based authentication. It can be up to 8 characters long.

      The ZENworks password authentication is recommended because it is more secure than the VNC password-based authentication. Use the VNC password-based authentication for interoperability with open source VNC viewers.

   Clear Password: Clears the selected password.

   Enable Accepting Connections if Currently Blocked Due to Intruder Detection: If a remote operator's attempt to log in fails a certain number of times (the default is 5), remote connections are disabled. Connections are automatically allowed again after a specific amount of time (the default is 10 minutes); however, you can click this option to manually enable connections.

   Display Audit Information: Displays the following information for the remote operations that have been performed on your device.

Field	Description
ZENworks User	Name of the ZENworks user logged in when the remote operation took place.
Remote Operator	Name of the remote operator who performed the operation.
Console Machine	Name of the device from which the remote operation was performed.
Console IP	IP address of the device from which the remote operation was performed.
Operation	The type of operation performed: Remote Control, Remote Execute, Remote View, Remote Diagnostics, File Transfer, or Security.
Start Time	The time when the remote operation began.
End Time	The time when the remote operation finished.
Status	The status of the remote operation: Success, Running, or Failure.

View Remote Management Certificate Details: Displays the device certificate. A remote operator might validate the device credentials before performing a remote operation on the device. The following certificate details are displayed:

Field	Description
Issued To	Name of the machine to which the certificate is issued.
Issued By	Name of the certificate issuing authority.
Validity	Period of certificate validity. The start and end date of validity.
Fingerprint	SHA-1 fingerprint of the certificate. The information can also be viewed by the user on the managed device from the z-icon and can be used by the remote operator to verify the certificate presented.

10 Full Disk Encryption

The information in this section applies only if ZENworks Full Disk Encryption is enabled on your device. To find out if it is enabled, right-click the ZENworks icon in the notification area, select **Technician Application**, and then look for **Full Disk Encryption** in the ZENworks Agent navigation menu. If **Full Disk Encryption** is not listed, your device is not using ZENworks Full Disk Encryption.

The following sections provide information to help you understand and use ZENworks Full Disk Encryption:

10.1 What Is ZENworks Full Disk Encryption?

ZENworks Full Disk Encryption uses disk encryption and pre-boot authentication to protect the data on your computer's local fixed volumes when the computer is powered-off or in hibernation mode.

10.1.1 Disk Encryption

ZENworks Full Disk Encryption encrypts local fixed volumes or partitions. For a single hard disk with multiple volumes, one or more of the volumes can be encrypted. All files on a volume are encrypted, including any temporary files, swap files, or operating system files. Because all files are encrypted, the data cannot be accessed when booting the computer from external media such as a CD-ROM, floppy disk, or USB drive.

ZENworks Full Disk Encryption only encrypts local fixed volumes. It does not encrypt removable volumes (USB drives and so forth) or network volumes.

10.1.2 Pre-Boot Authentication

Encrypted data is available after successful authentication. There are two levels of authentication that your ZENworks administrator can apply to your device:

- **Windows login:** This is the standard Windows login screen. If Windows login is the only required authentication, you gain access to encrypted data as soon as you successfully log in.
- **ZENworks Pre-Boot Authentication (PBA):** This added layer of access security uses MD5 checksums and strong key encryption, making it more secure than the Windows login. Before the Windows operating system boots, the ZENworks Pre-Boot Authentication screen is displayed. You gain access to encrypted data after you successfully log in to the ZENworks PBA. If your ZENworks administrator has not enabled single sign-on between the PBA and Windows login, you might also need to log in to Windows.

10.2   ZENworks Full Disk Encryption Agent

ZENworks Full Disk Encryption protects device data by applying a Disk Encryption security policy created by your ZENworks administrator. The ZENworks Agent downloads the security policy, but the enforcement of the policy on your device is performed by the ZENworks Full Disk Encryption Agent (commonly referred to as the Full Disk Encryption Agent).

Most of the Full Disk Encryption Agent functionality is exposed through the Full Disk Encryption Agent interface (rather than the ZENworks Agent interface). In addition, there is a separate Full Disk Encryption Agent Help file. To access the Full Disk Encryption Agent and its Help file:

1 Right-click the ZENworks icon in the notification area, and click **Technician Application**.

2 Click **Full Disk Encryption** in the ZENworks Agent navigation menu.

3 Under **Full Disk Encryption Agent Actions**, click one of the following:

   ◆ **Help:** Displays the Agent's Help file. The Help file provides information about how to use the Agent's features, such generating Emergency Recovery Information (ERI) files and diagnostic packages.

   ◆ **About:** Displays the Agent's About dialog box. This dialog box lets you access the ERI file and diagnostic package features as well as other features that your administrator might have enabled.

11 Endpoint Security

The information in this section applies only if ZENworks Endpoint Security Management is enabled on your device. To find out if it is enabled, right-click the ZENworks icon in the notification area, select **Technician Application**, and then look for **Endpoint Security** in the ZENworks Agent navigation menu. If **Endpoint Security** is not listed, your device is not using ZENworks Endpoint Security Management. This section is applicable only for Windows devices.

ZENworks Endpoint Security Management protects your computer against intruder attacks that can result in lost data, stolen data, and computer damage. The following sections provide information to help you understand and use ZENworks Endpoint Security Management:

- Section 11.1, "ZENworks Endpoint Security Agent," on page 47
- Section 11.2, "Security Locations," on page 48

11.1 ZENworks Endpoint Security Agent

ZENworks Endpoint Security Management protects your device by applying security policies (settings) created by your ZENworks administrator. In addition to using the ZENworks Agent to download security policies, ZENworks Endpoint Security Management uses the ZENworks Endpoint Security Agent to enforce the policies on your device. The ZENworks Endpoint Security Agent is commonly referred to as the Endpoint Security Agent.

Most of the ZENworks Endpoint Security Management functionality is exposed through the Endpoint Security Agent interface. In addition, there is a separate Endpoint Security Agent Help file. To access the Endpoint Security Agent and its Help file:

1 Right-click the ZENworks icon in the notification area, and click **Technician Application**.

2 Click **Endpoint Security** in the ZENworks Agent navigation menu.

3 Under **Endpoint Security Agent Actions**, click one of the following:

- **Help:** Displays the Agent's Help file. The Help file provides information about how to use the Agent's features, such as the encryption and diagnostic features.
- **About:** Displays the Agent's About dialog box. This dialog box lets you access the diagnostics feature as well as other features that your administrator might have enabled Encryption Management.

11.2 Security Locations

The Endpoint Security Agent enforces security policies on your device based on the security location of your device. The security location is determined from your surrounding network environment.

Depending on the security location, the applied security policies might be more or less restrictive. For example, if you are in the corporate office, your wireless access might be restricted to the corporate wireless network. One the other hand, if you are at home, your wireless access might allow you to connect to your home wireless network or other adhoc networks.

11.2.1 Viewing the Current Security Location

The current security location determines the security policies being applied to your device. To view the current location:

- Right-click the ZENworks icon ⊕ in the notification area, select **Technician Application**, and click **Security Location** in the ZENworks Agent. The current location is identified by a check mark.

  or

- Right-click the ZENworks icon in the notification area, click **Technician Application**, and click **Endpoint Security**. The current location is specified under **Security Location**.

11.2.2 Viewing the Available Security Locations

The ZENworks Agent selects your current security location from a list of locations provided by your ZENworks administrator. To view the available locations:

1. Right-click the ZENworks icon ⊕ in the notification area, and select **Technician Application**.

2. In the ZENworks Agent navigation menu, click **Endpoint Security**.

   The **Assignable Security Locations for the Device** box lists the locations that can be assigned to your device. There are two ways in which a location is assigned:

   - The ZENworks Agent assigns the location based on the current network environment. If the current network environment does not match any location that has been defined by your ZENworks administrator, Unknown Location is displayed.

   - You manually change the location assignment using the ZENworks icon menu in the notification area. This is possible only if the ZENworks administrator has enabled the location to be manually changed.

   The Allow Manual Change column indicates whether or not you can change to and from the location. For example, assume the list includes three locations. Location1 and Location2 can be manually changed, but Location3 cannot. If the ZENworks Agent determines the current location to be Location1, you can manually change to Location2 but not to Location3. This is because Location1 and Location2 both allow manual changes, but Location3 does not. If the ZENworks Agent determines that the location is Location3, you cannot change the location.

11.2.3 Changing Security Locations

You can change security locations only if additional locations are available and allow manual changes. See Section 11.2.2, "Viewing the Available Security Locations," on page 48.

When you change security locations, the ZENworks Agent applies the security policies associated with the new location. You should exercise caution when manually changing locations to ensure that you do not expose your device to unexpected security risks.

To change the security location:

Right-click the ZENworks icon in the notification area, select Security Location, and then click the new location.

12 Logging

While performing tasks on your device, the ZENworks Agent generates messages to track its activity. Each message is assigned a severity level: information, warning, error, or debug.

The following sections contain more information:

12.1 Changing the Message Log Level

By default, your ZENworks administrator controls what types of messages are stored in the local message log file. If your administrator needs to troubleshoot a ZENworks Agent issue on your device, he or she might direct you to change the log level setting so that additional information is logged. Otherwise, you probably never need to change the level.

To change the log level:

1 Click the ZENworks icon ⊕ in the system tray.

2 In the left navigation pane, click **Logging**.

3 In the **Applied Log Level** field, select one of the following options:

- **Use Global Setting:** Uses the message log level listed in the **Global Log Level** field.
- **Error:** Logs error messages only. Error messages are generated whenever the ZENworks Agent is unable to perform a requested task.
- **Errors, Warnings:** Logs error and warning messages. Warning messages are generated whenever the ZENworks Agent encounters a problem that might result in failure of a task.
- **Errors, Warning, Info:** Logs error, warning, and informational messages. Informational messages are generated whenever the ZENworks Agent performs a task to show that the normal process is taking place.
- **Errors, Warning, Info, Debug:** Logs all available messages to enable debug tracing of a problem. This level significantly increases the log file size and should be used only under the direction of your administrator.

4 Click **Apply** to apply the new severity level.

12.2 Clearing the Message Log File

Depending on how your ZENworks administrator has configured the log file backup option, the message log can become quite large. You can clear all messages from the current log file to free up disk space or to more easily view new messages.

To clear the log:

1 Click the ZENworks icon 🔵 in the system tray.

2 In the left navigation pane, click **Logging**.

3 Click **Clear Log**.

12.3 Viewing the Message Log File

The local log file, `zmd-messages.log`, is stored in the `program files\novell\zenworks\logs\localstore` directory on the root of the system drive (for example, `c:\program files\novell\zenworks\logs\local-store\zmd-messages.log`).

To view the log file:

1 Click the ZENworks icon 🔵 in the system tray.

2 In the left navigation pane, click **Logging**.

3 Click **View Log**.

Each entry in the file contains multiple fields. Each field begins with [and ends with]. For example, [ERROR]. The following table describes the fields.

Field Number	Example	Description
1	ERROR	The severity level. Possible values are ERROR, WARNING, INFORMATION, and DEBUG.
2	3/14/2007 4:21:35 PM	The date and time the message was generated.
3	JSmith	The user.
4	PolicyManager	The ZENworks Agent module that generated the message.
5	launcher configuration policy	The ID assigned to the message.
6	PolicyModule: Registering for events.	The message.
7		Additional information. Usually empty.
8	workstation1	Any objects related to the message.

12.4 Accessing the Backup Log Files

Backup log files are stored in the same directory as the current message log file. Each backup file is an incremented ZIP file (for example, `zmd-messages.log.1.zip` and `zmd-messages.log.2.zip`).

To access the backup log file:

1 Click the ZENworks icon 🔵 in the system tray.

2 In the left navigation pane, click **Logging**.

3 Click **Open Log Folder**.

13 Satellite Roles

A Windows device or a Linux device with satellite roles can perform certain roles that a ZENworks Primary Server normally performs. Any managed Windows or Linux device (server or workstation) can perform satellite roles. When the administrator configures the device, the administrator specifies the roles it performs. Satellite roles help to minimize WAN traffic in the ZENworks system.

Satellite roles include the following:

* **Authentication:** With the Authentication role, your device can be used as an Authentication server to help speed the authentication process by spreading the workload among various devices and by performing authentication locally to managed devices.

* **Collection:** To improve information roll-up access for a group of devices and to minimize traffic to the ZENworks Primary Server that is hosting the ZENworks database, the ZENworks administrator can enable the Collection role on a device and designate whether your device as a Collection Point.

* **Content:** ZENworks Configuration Management supports distributing bundles and policies from ZENworks Servers or from other devices that are designated as Distribution Points. Your administrator controls whether or not your device is a Distribution Point.

* **Imaging:** The Imaging role installs the Imaging services and adds the Imaging role to the device. With this role, the device can be used as an Imaging server to perform all Imaging operations, such as taking an image and applying the image within or across subnets by using unicast or multicast imaging. Your administrator controls whether or not your device has the imaging role.

* **Join Proxy:** You can use devices promoted to the Join Proxy role for performing remote management operations on Windows managed devices that are in a private network. You can promote only a ZENworks version 11.3 or later Windows or Linux managed device to the Join Proxy role.

The following sections contain more information:

13.1   General Satellite Role Information

You can view a device's general properties, including its current status, port, content replication schedule, and role status.

If your ZENworks administrator has specified that this device performs a satellite role, the information on this page lets you view the device's general information; however, you cannot edit the fields on this page.

To view general satellite role information:

1   Right-click the ZENworks icon 🔗 in the notification area.

2   Click **Technician Application**.

3   In the left navigation pane, under **Satellite**, click **General**.

Field	Description
Current Status	Displays whether your device is currently configured to perform a satellite role.
Port	Displays the port that the device is using.
SSL Port	If the device is performing the Authentication role, displays the SSL port being used for authentication purposes.
Satellite Role Status	Displays the roles that the device is performing (Collection, Content, Imaging, Authentication, and Join Proxy) and its current status.
Content Replication Details	Displays the content type, throttle rate (kb/sec) that the device uses to replicate content, how often the device's content is updated from the parent Primary Server, and the duration of the replication period. Your system administrator can change any of these settings.
	For example, by default, a Content role device checks for new or removed content every 5 minutes. Your ZENworks administrator can change this schedule. For example, your administrator might want to increase the time between cycles if the ZENworks system is not adding content to your system very often or if the connection between the Content role device and its parent Primary Server is slow.

13.2   Authentication

You can view a device's Authentication role properties, including its current status and the SSL port currently used for authentication; however, you cannot edit the fields on this page.

ZENworks Configuration Management lets your ZENworks administrator enable the Authentication role on a device. With this role, the device can be used as an Authentication server to help speed the authentication process by spreading the workload among various devices and by performing authentication locally to managed devices.

To view Authentication role information:

1 Right-click the ZENworks icon 🔗 in the notification area.

2 Click **Technician Application**.

3 In the left navigation pane, under **Satellite**, click **Authentication**.

Field	Description
Current Status	Displays whether your device is currently configured to perform Authentication operations. The current status is **Active** when the device is promoted to a satellite with the Authentication role.
SSL Port	Specifies the SSL port being used on the device for authentication purposes.

13.3 Imaging

You can view a device's imaging role properties, including its current status, PXE service status, image files, and imaging statistics; however, you cannot edit the fields on this page.

ZENworks Configuration Management lets your ZENworks administrator enable the Imaging role on a device. With this role, the device can be used as an Imaging server to perform all Imaging operations, such as taking an image and applying the image within or across subnets by using unicast or multicast imaging. Your administrator controls whether or not your device has the Imaging role.

To view imaging role information:

1 Right-click the ZENworks icon 🔗 in the notification area.

2 Click **Technician Application**.

3 In the left navigation pane, under **Satellite**, click **Imaging**.

Field	Description
Current Status	Displays whether your device is currently configured to perform Imaging operations. The current status is **Active** when the device is promoted to a satellite with the Imaging role.
PXE Service Status	Displays whether the Proxy DHCP service is enabled on the device.
View Image Files	Displays the image files stored in the `%ZENWORKS_HOME%\work\content-repo\images` directory.

Field	Description
Imaging Statistics	Displays the following information:
	◆ **PXE Requests:** The number of imaging requests of any kind that have been received by the Imaging Server since it was last started. This includes requests that failed, were denied, or were referred to other Imaging Servers. Information about each of these requests, such as the source, type, date/time, and results, is logged on the Imaging Server.
	◆ **Images Sent:** The number of images that the Imaging Server has sent to imaging clients since the Imaging Server was last started. This includes only images that were retrieved from this Imaging Server.
	◆ **Images Received:** The number of new images that have been received and stored on the Imaging Server since it was last started. This includes images that were received through client referrals.

13.4 Collection

You can view a device's collection role properties, including its current status, parent URLs, and collection schedule; however, you cannot edit the fields on this page.

ZENworks Configuration Management lets your ZENworks administrator enable the Collection role on a device. This improves information roll-up access for a group of devices and minimizes traffic to the ZENworks Primary Server that is hosting the ZENworks database. The information that is rolled up includes device inventory information, messages (errors, warning, informational, and so forth), and policy and bundle statuses. Your administrator controls whether or not your device is a Collection Point.

To view collection role information:

1 Right-click the ZENworks icon 🔗 in the notification area.

2 Click **Technician Application**.

3 In the left navigation pane, under **Satellite**, click **Collection**.

Field	Description
Current Status	Displays whether your device is currently configured to function as a Collection Point.
Parent URLs	Displays the URL for this device's parent ZENworks servers.
Collection Schedule	Displays how often the collected data is rolled up from the devices that use it as a collection device. Your ZENworks administrator can change this collection schedule.
Files Waiting to be Uploaded	Displays any files waiting to be uploaded and specifies the sender, type and filename.
Clients Uploading to this Satellite Collection Point	Lists any clients that can upload files to this device.

13.5   Content

ZENworks Configuration Management supports distributing bundles and policies from ZENworks Servers or from other devices that are designated as Distribution Points. Your administrator controls whether or not your device is a Distribution Point.

13.5.1   Viewing Distribution Point Information

If your device is serving as a Distribution Point, you can view statistical information about the number of times it has been accessed and the content (bundles and policies) that is stored on it.

1 Right-click the ZENworks icon 🔗 in the notification area.

2 Click **Technician Application**.

3 In the left navigation pane, under **Satellite**, click **Distribution Point**.

Field	Description
Current Status	The status of the Distribution Point module. If the **Stopped** status is displayed, your device is currently not serving as a Distribution Point.
Port	The port being used by the device to perform its Distribution Point function.
Content Replication Method	The replication method configured during the Satellite promotion.The Satellite performing the content role uses the configured replication method to replicate content from other Satellite content servers.
Repository Size	The amount of disk space being used by the repository.
Synchronization Status	The number and percentage of files synchronized.
Unique Device Accesses	The number of different devices that have accessed content from the repository on your device. This number represents the total unique accesses since the last time the **Clear History** option was used to reset the number to 0.
Number of Files Served	The number of bundle and policy files delivered to other devices. This number represents the total number of files transferred since the last time the **Clear History** option was used to reset the number to 0.
Size of Data Served	The total amount of data delivered to other devices. This amount represents the total number of files transferred since the last time the **Clear History** option was used to reset the amount to 0.
Number of Errors	The total number of errors encountered while transferring files. Click the **Export History** option to export transactions to a comma-separated values (CSV) file that you can use to examine the errors.
Actions	Click **Export History** to export the information from the **Recent Access History** list to a CSV file. Click **Clear History** to clear the information from the list and to reset the **Unique Device Accesses**, **Number of Files Transferred**, **Amount of Data Transferred**, and **Number of Errors** fields to 0.

Field	Description
Recent Access History	A listing of the last 10 devices to access the repository. The list shows only the 10 most recent accesses. However, all entries are saved until the history is cleared. To analyze all of the entries, click **Export History** to create a CSV file.
Content Repository Details	A listing of the bundles and policies stored in the repository.

13.5.2 Exporting the Recent Access History

The Recent Access History displays information about the 10 most recent repository accesses. This includes information about the device that performed the access, the total number of downloads that occurred, the amount of data that was transferred, and whether or not any errors occurred.

The list shows only the 10 most recent accesses. However, all entries are saved until the history is cleared. To analyze all of the entries, you can export the history to a comma-separated values (CSV) file.

1 Right-click the ZENworks icon 🔗 in the notification area.

2 Click **Technician Application**.

3 In the left navigation pane, under **Satellite**, click **Content**.

4 Click **Export History**, specify a location and name for the CSV file, then click **Save**.

5 To view the history file, open it in a text editor.

The history file contains two sections: Distribution Point Access History and Distribution Point Error History.

Distribution Point Access History: Contains an entry for each transaction in the **Recent Access History** list. Each entry is formatted as follows:

```
IP Address,DNS Name,Number of Files Transferred,Bytes
Transferred,Number of Errors,Last Access (UTC)
```

For example:

```
123.45.167.52,wks1.novell.com,3,544,0,3/20/2007 7:16:59 PM
```

Distribution Point Error History: Contains an entry for each transaction that included an error. Each entry is formatted as follows:

```
IP Address,DNS Name,Requested URI,Status Code,Access Time (UTC)
```

For example:

```
123.45.167.53,wks2.novell.com,/app.msi,404,3/22/2007 9:11:33 AM
```

13.5.3 Clearing the Recent Access History

You can clear the Recent Access History to remove all entries from the list and to reset the **Unique Device Accesses**, **Number of Files Transferred**, **Amount of Data Transferred**, and **Number of Errors** fields to 0.

1 Right-click the ZENworks icon ☁ in the notification area.

2 Click **Technician Application**.

3 In the left navigation pane, under **Satellite**, click **Content**.

4 Click **Clear History**, then click **Yes** to confirm deletion of the history.

13.6 Join Proxy

You can view the Join Proxy role properties of a devices which includes the current status of the device, port, maximum connections, and connection poll interval; however, you cannot edit the details on this page.

ZENworks Configuration Management lets your ZENworks administrator enable the Join Proxy role on a ZENworks version 11.3 or later Linux or Windows device to perform remote management operations on Windows managed devices that are in a private network.

To view Join Proxy role information:

1 Right-click the ZENworks icon ☁ in the notification area.

2 Click **Technician Application**.

3 In the left navigation pane, under **Satellite**, click **Join Proxy**.

Field	Description
Current Status	Displays one of the following statuses: ◆ Active: The Join Proxy service is running after the successful configuration of the Join Proxy role. ◆ Disabled: The Join Proxy role is not configured for the device. ◆ Stopped: The service is not starting, either because the port used for connection is not available or is already in use.
Port	Displays the port on which the Join Proxy listens for connections.
Maximum Connections	Displays the specified limit on the number of devices allowed to connect to the Join Proxy.
Connection poll interval	Displays the specified time interval for the Join Proxy to check if the devices are still connected to it.

14 Windows Proxy

The ZENworks Agent provides information on how your device performs the discovery and deployment activities when it acts as a Windows Proxy for the ZENworks Primary Server. This section is applicable only for Windows devices.

The following sections contain more information:

14.1 Viewing the Discovery Results

You can view the results of the discovery activities performed on your device when it acts as a Windows Proxy for the ZENworks Primary Server. Your device can act as a Windows Proxy for:

- Linux Primary Servers that cannot perform discovery tasks by using Windows-specific technologies such as WMI, WinAPI, and SNMP
- Windows Primary Servers if the devices to be discovered are in a different subnet than the Primary Server

To view the discovery results:

1 Right-click the ZENworks icon ⊕ in the notification area.

2 Click **Technician Application**.

3 In the left navigation pane, click **Discovery**.

   The Discovery Results panel displays the following details:

Field	Description
Discovery Task	Displays the discovery task name created by the ZENworks Administrator.
Discovery Target	Displays the target device's hostname or IP address.
Discovery Technologies	Displays the name and status of each discovery technology (WMI, WinAPI, SNMP) used for the discovery process.
	For more information on each discovery technology, see the ZENworks Discovery, Deployment, and Retirement Reference on ZENworks Documentation website.
Last Time Stamp	Displays the date and time when the discovery task was run.

4 (Optional) To remove all the discovery results from the Discovery Results panel, click **Clear Discovery Results**, then refresh the page.

14.2 Viewing the Deployment Results

You can view the results of the deployment activities performed on your device when it acts as a Windows Proxy for the ZENworks Primary Server. Your device can act as a Windows Proxy for:

- Linux Primary Servers that cannot perform deployment of ZENworks Agent to Windows target devices
- Windows Primary Servers if the devices to be deployed are in a different subnet than the Primary Server

To view the deployment results:

1 Right-click the ZENworks icon in the notification area.

2 Click **Technician Application**.

3 In the left navigation pane, click **Deployment**.

The Deployment Results panel displays the following details:

Field	Description
Deployment Task	Displays the deployment task name created by the ZENworks Administrator.
Deployment Target	Displays the target device's name or IP address.
Deployment Status	Displays the status of the deployment task.
Last Time Stamp	Displays the date and time when the deployment task was run.

4 (Optional) To remove all the deployment results from the Deployment Results panel, click **Clear Deployment Results**, then refresh the page.

15 Linux Proxy

15

Linux Proxy

The ZENworks Agent provides information on how your device performs the discovery and deployment activities when it acts as a Linux Proxy for the ZENworks Primary Server. This section is applicable only to ZENworks Configuration Management Linux devices.

- Section 15.1, "Viewing the Discovery Results," on page 67
- Section 15.2, "Viewing the Deployment Results," on page 68

15.1 Viewing the Discovery Results

You can view the results of the discovery activities performed on your device when it acts as a Linux Proxy for the ZENworks Primary Server. Your device can act as a Linux Proxy to perform the following actions:

- Enable Primary Servers that cannot perform discovery tasks by using Linux-specific discovery technologies like SSH.
- Discover Linux devices in a different subnet than the Primary Server.
- Discover Linux devices in a network enabled for NAT.

To view the discovery results:

1 Right-click the ZENworks icon in the notification area.

2 Click **Technician Application**.

3 In the left navigation pane, click **Discovery**.

The Discovery Results panel displays the following details:

Field	Description
Discovery Task	Displays the discovery task name created by the ZENworks Administrator.
Discovery Target	Displays the target device's hostname or IP address.
Discovery Technologies	Displays the name and status of the SSH discovery technology. For more information on SSH discovery technology, see "IP Discovery Technologies" in the ZENworks Discovery, Deployment, and Retirement Reference on the ZENworks Documentation website.
Last Time Stamp	Displays the date and time when the discovery task was run.

4 (Optional) To remove all the discovery results from the Discovery Results panel, click **Clear Discovery Results**, then refresh the page.

15.2 Viewing the Deployment Results

You can view the results of the deployment activities performed on your device when it acts as a Linux Proxy for the ZENworks Primary Server.

A Linux Proxy is primarily used for Primary Servers if you want to deploy to Linux devices in a different subnet than the Primary Server. When a Primary Server receives a deployment task that includes devices in a different subnet, it offloads the deployment tasks to the Linux Proxy. A Linux Proxy is also used for performing deployment tasks on Linux devices in a network enabled for NAT.

To view the deployment results:

1 Right-click the ZENworks icon 🔗 in the notification area.

2 Click **Technician Application**.

3 In the left navigation pane, click **Deployment**.

The Deployment Results panel displays the following details:

Field	Description
Deployment Task	Displays the deployment task name created by the ZENworks Administrator.
Deployment Target	Displays the target device's name or IP address.
Deployment Status	Displays the status of the deployment task.
Last Time Stamp	Displays the date and time when the deployment task was run.

4 (Optional) To remove all the deployment results from the Deployment Results panel, click **Clear Deployment Results**, then refresh the page.

16 External Services

The ZENworks Agent provides information on how to register external services such as YUM, ZYpp, and Mount to resolve dependencies and install or upgrade the required packages from the repositories in these services.

You can add the required properties to the service and register them. You can also view the list of registered services. This section is applicable only to ZENworks Configuration Management Linux devices.

The following sections provide more information:

16.1 Registering External Services

1 Select the type of service that you want to register. The available service types are YUM, ZYpp, and Mount.

2 Specify a local name for the service.

3 Specify the URL of the repository from where you want to download the packages.

4 If you want to synchronize the services with the External Package Management tools, select the **Synchronize with External Package Management Tools** check box.

NOTE: The ZYpp or Mount service do not synchronize with the YUM Package Management Tool on Red Hat devices.

---

5 (Optional) Specify the properties for the selected external service in the Add Property group. You can add multiple properties for a service.

  5a Click the **Specify Properties** link.

  5b Specify the property name and property value. The added properties are displayed in the Properties panel.

    The following table describes the supported properties:

Property Name	Description
username	Name of the user.
password	Password of the user.
recursive	This property is applicable only for Mount service type. Valid values are true or false. If true, adds the RPMs recursively from all the directories specified under the absolute path.

For example, to add authentication details such as username abc and password xyz for the selected repository, do the following:

1. Specify the property name as `username` and the property value as `abc`, then click **Add Property**.

2. Specify the property name as `password` and the property value as `xyz`, then click **Add Property**.

5c To delete a property, click **Remove Property**.

6 Click **Register** to register the external service.

The registered external service is displayed in the External Services panel.

16.2 Viewing the Registered External Services

You can view the external services that you registered in the External Services pane.

16.3 Deleting the Registered External Services

To delete a service, select the check box next to the service that you want to delete, then click **Delete**.

NOTE: An External Policy enforced service cannot be removed locally by a user.

16.4 Refreshing the Registered External Services

To refresh a service, select the check box next to the service that you want to refresh, then click **Refresh**.

17 Package Locks

The ZENworks Agent provides information on how to configure package locks on managed devices. You can use these package locks to prevent the removal or upgrade of packages on the managed devices. This section is applicable only to ZENworks Configuration Management Linux Devices.

The following sections contain more information:

* Section 17.1, "Configuring Package Locks," on page 73
* Section 17.2, "Deleting Package Locks," on page 74

17.1 Configuring Package Locks

1 Right-click the ZENworks icon in the notification area.
2 Click **Technician Application**.
3 On the left navigation pane, click **Package Locks**.
4 In the Add Package Locks panel:

    4a Specify the package lock name.

    4b Select a relational operator to be used to set the package lock. The following table explains the valid relational operators that can be used with the package:

Relational Operator	Functionality
Any	Locks any package.
=	Locks the specified package version.
<	Locks all versions of the package older than the specified version, excluding the specified version.
<=	Locks all versions of the package older than the specified version, as well as the specified version.
>	Locks all versions of the package later than the specified version, excluding the specified version.
>=	Locks all versions of the package later than the specified version, as well as the specified version.

    4c Specify the package version that you want to lock.

5 Click **Add Lock** to create the package lock.

17.2 Deleting Package Locks

The Package Locks panel displays the package locks that have been configured. To delete a package lock:

1 Right-click the ZENworks icon ⬡ in the notification area.

2 Click **Technician Application**.

3 On the left navigation pane, click **Package Locks**.

4 In the Package Locks panel, click **Remove Package Lock**.

18 ZENworks Terminology

The following terms are used throughout the ZENworks Agent documentation.

authentication role: A role that a managed device can perform to help speed the authentication process by spreading the workload among various devices and by performing authentication locally to managed devices.

bundle: The content and instructions required to install software on your device.

collection role: A role that a managed device can perform to improve information roll-up access for a group of devices and to minimize traffic to the ZENworks Primary Server that is hosting the ZENworks database.

content role: A role that a managed device can perform to help support distributing bundles and policies from ZENworks Servers or from other devices that are designated as Distribution Points.

device: A server or workstation.

device-assigned bundle or device-assigned policy: Bundles and policies that are assigned to a device so they are available to all users of the device.

Distribution Point: A device designated for the purpose of delivering bundles and policies to other devices.

imaging role: A role that installs the Imaging services and adds the Imaging role to a managed device. With this role, the device can be used as an Imaging server to perform all Imaging operations, such as taking an image and applying the image within or across subnets by using unicast or multicast imaging.

Join Proxy role: With this role, the device in a public network can be promoted as a Join Proxy Satellite Server for performing remote management operations on the managed devices in private network. ZENworks Satellites can act as Join Proxy servers while ZENworks Primary Servers have the Join Proxy role by default. Using a Join Proxy, you can remote control only a Windows managed device.

inventory: Data about your device's hardware and software.

Management Zone: A grouping of devices that belong to the same administrative domain.

policies: Rules that control a range of hardware and software configuration and security settings.

primary user: The most frequent user of the machine. Frequency is determined by number of logins, amount of time logged in, or designated user; your administrator determines the method used to calculate the primary user.

registration key: An alphanumeric string created by your administrator and used by the ZENworks Agent to register your device in the Management Zone.

Remote Management: The ability to remotely access or control your device in order to resolve problems with the device. The following remote management operations are available: Remote Control, Remote View, Remote Diagnostics, File Transfer, and Remote Execute.

Satellite: A device with satellite roles can perform certain roles that a ZENworks Primary Server normally performs. Any managed Windows or Linux device (server or workstation) can perform satellite roles. When the administrator configures the device, the administrator specifies the roles it performs. Satellites help to minimize WAN traffic in the ZENworks system. Satellite roles include the following: Authentication, Collection, Content, Imaging, and Join Proxy.

remote operator: The person who is remotely accessing or controlling your device.

user-assigned bundle or user-assigned policy: Bundles and policies that are assigned to a user. They are available only when the assigned user is logged in.

ZENworks Explorer: An extension to Windows Explorer that enables bundles to be displayed in Windows Explorer, on the desktop, on the Start menu, on the Quick Launch toolbar, and in the notification area.

ZENworks icon: The ZENworks icon ⬡ icon is located in the notification area of the Windows and Linux managed devices. Click the ZENworks icon to display the ZENworks Agent properties.

ZENworks Window: A standalone window that you can launch from the Start Menu (**Start Menu** > **Programs** > **Novell ZENworks** > **ZENworks Application**). The ZENworks Window displays all assigned bundles.

ZENworks Server: A server that your ZENworks Agent contacts in order to send information to and retrieve information from your Management Zone.

A   Troubleshooting

The following sections explain the issues that you might encounter on a managed device.

The ZENworks Application Fails to Launch on Windows 11 Managed Devices

Source: ZENworks Agent

Explanation: On the Windows 11 managed device, when you launch the ZENworks Application using the ZENworks icon, the following error is displayed:**The application was unable to start correctly (0xc0000135)**

Action: To resolve this issue:

1. On the **Turn Windows features on or off** window, select.**NET Framework 3.5** and then select the following:
   - Windows Communication Foundation HTP Activation
   - Windows Communication Foundation Non-HTP Activation
2. Click OK, and then restart the device.

Desktop Icons are Rearranged after the Reboot

Source: ZENworks Agent

Explanation: Due to Microsoft technical limitations, the NAL icons and default shortcut icons are placed in unexpected locations on the desktop.

Action: None

Installing ZENworks Agent on RHEL 8.x is registered as RHEL 8.1 Workstation

Source: ZENworks Agent

Explanation: When installing the ZENworks agent on an RHEL 8.x device, the device is registered as RHEL 8.1 workstation. For more information on the issue, see https://access.redhat.com/solutions/4203571

Action: Set the required role on the device by running the syspurpose command.

For example to set as a server, run the following command on the RHEL8.x device:

```
syspurpose set-role "Red Hat Enterprise Linux Server"
```

After upgrading the Operating System on ZENworks Satellite Server, ZENworks agent services might not start

Source: ZENworks; ZENworks Agent.

Action: After upgrading the Operating System on Satellite Servers, perform the following steps:

1   1.Stop all the ZENworks Agent services.

2   Backup contents of

3   Uninstall the ZENworks Agent by using the following command:

```
novell-zenworks-*.rpm with rpm -qa | grep 'novell-
zenworks-' | xargs rpm –e
```

4   Remove or rename directories and

5   Install the ZENworks Agent.

6   Check reconciliation with former object.

7   Stop ZENworks services by running the following command:

```
systemctl stop novell-zenworks-xplatzmd.service
```

8   Restore content-repo and /srv/tftp/ to respective folders.

9   Start ZENworks services by running the following command:

```
systemctl start novell-zenworks-xplatzmd.service
```

10   To verify the content, run `zac cdp-verify-content`.

11   Remint server certificate by running the following command:

```
zac rsc -u Administrator -p password
```

12   Disable and enable Imaging role for the satellite server

13   Restore the `/srv/tftp/` folder from the backup.

14   Replication contents of the tftp folder by running the following command:

```
zac cdp replicate
```

The ZENworks Agent UI shows both English and the local language chosen for viewing

Source: ZENworks; ZENworks Agent.

Explanation: ZENworks resources are loaded according to the locale of the process that retrieves them. When using regional settings, the ZENworks Windows service might be configured to use a different language than the user is configured to use. The result is that the strings from both languages are displayed.

Action: Do one of the following:

- Install the native language operating system
- Change the default user language to match the language displayed by the user

Standalone install or uninstall of individual components does not work on Windows managed devices

Source: ZENworks; ZENworks Agent.

Explanation: Standalone install or uninstall of individual components do not work on the ZENworks Agent. When you enable or disable individual components, the settings might not be applied and the following message is logged:

```
[CompMgmt] [] [Aborting InstallAndUninstallComponents
because of a pending reboot]
```

For example, if a bundle or policy component is disabled, you might continue seeing the bundle or policy component in effect on the ZENworks Agent.

Possible Cause: The Windows system might not be updated with the latest patches.

Action: Do the following:

- Apply the latest patches for Windows.
- Delete the registry key `HKEY_Local_Machine/Software/Novell/ZCM/volatile`.
- Reboot the system.

For more information, see TID 7006485 in the (http://www.novell.com/support/search.do?usemicrosite=true&searchString=7006485).

Unable to start zmd in debug mode on a RHEL 4 b4-bit managed device

Source: ZENworks; ZENworks Agent.

Explanation: When you try to run zmd in the debug mode on a RHEL 4 64-bit managed device, you might encounter the following error:

```
Native library not loaded
```

Possible Cause: The GLIBC version on the managed device is not 2.4 or later.

Action: On the managed device, upgrade the GLIBC version to 2.4 or later.

Locations configured in ZENworks Control Center may not apply to RHEL 5 devices

Source: ZENworks; ZENworks Agent.

Explanation: The Network Manager may not be running as a daemon on the RHEL 5 device. So, the `nm-tool` command output will be empty.

Action: Do one of the following:

- Run the Network Manager by using the `NetworkManager` command.
- Run the Network Manager as a daemon by using the `chkconfig` command.

  For example, `chkconfig --level 35 NetworkManager on` command runs the Network Manager as a daemon for levels 3 and 5.

On a Windows XP device, the installation of ZENworks Agent with the Remote Management component through Remote Desktop Connection fails

Source: ZENworks; ZENworks Agent.

Explanation: If you remotely connect to a managed device through Remote Desktop Connection (RDP), then download and install the ZENworks Agent, the installation does not complete and the Remote Desktop Connection program stops working.

Action: To fix the issue, download the patch from the Microsoft Support Web site (http://support.microsoft.com/kb/952132) and install it on the managed device..

ZEN CASA not storing Groupwise credentials

Source: Zenworks; ZENworks Agent.

Explanation: If the managed device is running with ZENworks Agent and Groupwise client, in which Groupwise client is enabled with single-sign-on (CASA) and remember password options. After closing and reopening of Groupwise client, it again prompts for password.

Action: Specify the password for Groupwise client and reboot the managed device.

Security vulnerabilities in .NET framework

Source: ZENworks; ZENworks Agent.

Explanation: There are a few critical vulnerabilities in the .Net framework.

Action: On the ZENworks agent, apply the following patches that have been released by Microsoft for .Net vulnerabilities:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0606
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0646