opentext™

ZENworks
Discovery, Deployment, and Retirement Reference

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.microfocus.com/en-us/legal.

© Copyright 2008 - 2023 Open Text

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

About This Guide **7**

Part I Device Discovery **9**

1 Basic Concepts **11**

Discovery Methods 11
IP and LDAP Discovery Tasks 11
IP Discovery Technologies 12
LDAP Discovery Technology 17
Advertised Devices 17
Discovered Devices 18
Searching Discovered Devices 19
Deployable Devices 19

2 Discovering Devices By Using IP Addresses **21**

Configuring Discovery Settings 21
Designating a Discovery and Deployment Proxy Server 23
Designating a Windows Proxy Server 23
Designating a Linux Proxy Server 24
Creating an IP Discovery Task 24

3 Discovering Devices in LDAP Directories **33**

4 Importing Devices from CSV Files **39**

5 Advertised Discovery **41**

Configuring the Advertised Discovery Settings 41
Discovering Advertised Devices 42

6 Viewing or Updating Device Details **43**

7 Geolocating Windows 10 Devices **45**

Part II ZENworks Agent Deployment **47**

8 Basic Concepts **49**

Deployment Methods 49
Deployment Packages 49
ZENworks Agent Versus Inventory-Only Module 50

9 Managing Deployment Packages **51**

Package Types and Architectures. 51
Package Types and Architectures for Windows. 51
Package Types and Architectures for Linux 52
Package Types and Architectures for Macintosh. 53
Default System Packages Versus Custom Packages 53
Customizing Packages. 54
Rebuilding Packages 56
Rebuilding the Default Packages 57
Rebuilding the Custom Packages 58

10 Registering Devices **59**

What Happens During Registration 59
Creating Registration Keys and Rules 60
Creating a Registration Key 61
Creating a Registration Rule 63
Creating Authorization Key. 67
Modifying the Device Naming Template Used During Registration 68
Enabling Dynamic Renaming of Devices During Registration 69
Enabling the Setting at the Management Zone. 69
Enabling the Setting for a Device Folder 69
Reconciling Devices with existing Device Objects During Registration. 70
Creating Dummy Device Objects 70
Reconciling the Devices. 72
Importing Managed Devices. 80
Disabling the Use of Registration Rules. 81
Adding Pre-approved Devices 82
Adding the Pre-approved Devices Manually 83
Importing Pre-approved Devices from CSV File 83
Adding the Pre-approved Devices using Action 84
Adding the Pre-approved Devices while Deleting Devices. 84
Manually Registering a Device 85
Performing an Initial Registration. 85
Reregistering a Device with an Additional Registration Key. 86
Unregistering a Device 86

11 Deploying the ZENworks Agent **89**

Coexisting with the ZENworks Desktop Management Agent 89
Customizing the Agent Features 90
Customizing Features before Deployment 91
Customizing Features after Deployment 91
Configuring the Agent Security 92
Customizing Security before Deployment 92
Customizing Security after Deployment 93
Changing the Target Installation Directory 93
Using a Task to Deploy the Agent 94
Prerequisites for Deploying to Windows Devices 94
Prerequisites for Deploying to Linux Devices 98
Deploying to a Discovered Device 99
Deploying to a Non-Discovered Device 109

Manually Deploying the Agent on Windows 119
Reboot-less Agent 121
Manually Deploying the Agent on Linux 122
Manually Deploying the Agent on a Macintosh Device 123
Agent Deployment in VDI environment 127
Upgrading the Agent in a Citrix VDI Environment 129
Agent Deployment on Citrix Server 129
Package Options for Windows, Linux, and Macintosh 129
Installing the Agent as an Add-on Product in SLES/SLED 131
Installing the ZENworks Agent on SLES/SLED 11, 12 and 15 131
Installing the Agent by Using YUM on RHEL 132

12 Viewing and Updating the Managed Device Details 135

13 Uninstalling the Agent 139

14 Deploying the Inventory-Only Module 141

Prerequisites 141
Downloading the Module from a ZENworks Server 142
Installing Inventory-Only Agent (IOA) on Linux. 142
Installing Inventory-Only Agent (IOA) on Windows 143
Installing Inventory-Only Agent (IOA) on Macintosh OS X 144
Uninstalling the Inventory-Only Module 145
Upgrading Inventory-Only Agent 146
Re-registering Inventory-Only Devices 146
Re-registering Inventory-Only Devices for All Platforms 146
Re-registering Inventory-Only Devices for Individual Platforms 146
Running Scannow on an Inventory-Only Device. 148

Part III Device Removal and Retirement 149

15 Deleting Devices from Your ZENworks System 151

16 Retiring or Unretiring Devices 153

17 Exporting Details to CSV Format 155

Part IV Appendixes 157

A Viewing the Predefined Reports 159

B Schedules 161

Now 161
No Schedule. 161
Date Specific 161
Start Dates 161

Run Event Every Year 161
Select When Schedule Execution Should Start 161
Use Coordinated Universal Time (UTC) 162
Recurring 162
Days of the Week 162
Monthly 162
Fixed Interval 163

C Configuring NMAP for ZENworks 165

D Troubleshooting Discovery, Deployment, and Retirement 167

About This Guide

This *ZENworks Discovery, Deployment, and Retirement Reference* helps you add devices to your ZENworks Management Zone and then install the ZENworks Agent or Inventory Only Module to the devices.

The information in this guide is organized as follows:

- Part I, “Device Discovery,” on page 9
- Part II, “ZENworks Agent Deployment,” on page 47
- Part III, “Device Removal and Retirement,” on page 149
- Part IV, “Appendixes,” on page 157

Audience

This guide is intended for anyone who configures and manages a ZENworks system.

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.

Device Discovery

The following sections provide information and instructions to help you add devices to your ZENworks database. After a device is added to the database, a ZENworks Server can automatically deploy the ZENworks Agent to the device. If you face issues with any of the Discovery and Deployment tasks, then check the following logs:

- **On the server:** loader-messages.log and services-messages.log.
- **On the target device:** Event viewer logs (on Windows) and /var/log/messages (on Linux)
- **(If proxy is used) On the proxy device:** zmd-messages.log

---

NOTE: Device discovery and deployment tasks for Agent are not supported for a Mac platform. In this case, the agent needs to be installed manually using a standalone installer.

- Chapter 1, “Basic Concepts,” on page 11
- Chapter 2, “Discovering Devices By Using IP Addresses,” on page 21
- Chapter 3, “Discovering Devices in LDAP Directories,” on page 33
- Chapter 4, “Importing Devices from CSV Files,” on page 39
- Chapter 5, “Advertised Discovery,” on page 41
- Chapter 6, “Viewing or Updating Device Details,” on page 43
- Chapter 7, “Geolocating Windows 10 Devices,” on page 45

1 Basic Concepts

Device discovery is the process of adding workstation and server information to the ZENworks database so that you can use that information to automatically deploy the ZENworks Agent from a ZENworks Server to the devices. The following sections provide information to help you understand the discovery terminology and concepts:

- "Discovery Methods" on page 11
- "IP and LDAP Discovery Tasks" on page 11
- "IP Discovery Technologies" on page 12
- "LDAP Discovery Technology" on page 17
- "Advertised Devices" on page 17
- "Discovered Devices" on page 18
- "Deployable Devices" on page 19

Ensure that the Discovery Rights are enabled, which are required to perform discovery operation. For more information, see Discovery Rights in ZENworks Administrator Accounts and Rights Reference.

Also, the device discovery feature for agents is not applicable for a Mac platform. The agent on a Mac platform needs to be installed manually using a standalone installer.

Discovery Methods

There are four discovery methods you can use:

- **IP discovery:** Use the ZENworks discovery engine to collect information about devices on your network. The engine uses various protocols and standards (WMI, WinAPI, MAC Address, NMAP, ZENworks, SNMP, SSH) to discover and collect information from devices that you identify through IP address ranges.
- **LDAP directory discovery:** Use the ZENworks discovery engine to search Novell eDirectory or Microsoft Active Directory for device objects. You specify the contexts to search and the filter to use for the search.
- **CSV import:** Import device information from a comma-separated values (CSV) file. At the minimum, the file must contain the IP address or DNS name for each device.
- **Advertised discovery:** Use the ZENworks discovery engine to collect information about devices that have the ZENworks preagent installed.

IP and LDAP Discovery Tasks

IP and LDAP discoveries are performed through discovery tasks. You create a discovery task in ZENworks Control Center. LDAP discovery requires Novell eDirectory or Microsoft Active Directory to search for devices.

IP Discovery Technologies

The ZENworks discovery engine can utilize a variety of different technologies for IP-based discoveries. When more than one technology is used, the discovery engine initiates a discovery request for each technology. This is done for each target IP address. For example, if you use MAC Address, SNMP, and WMI, the discovery engine creates three requests for each target IP address. The requests are queued and the discovery engine processes five requests at a time until no requests remain. Five requests is the default. You can change the default if necessary (see "Configuring Discovery Settings" on page 21) or override the settings in the discovery task.

Using fewer discovery technologies reduces the time required to complete the discovery task but might also reduce the amount of information received.

NOTE: We do not support using SSH or ZENworks ping to discover Macintosh devices.

By default, the MAC Address, SSH, WinAPI, and ZENworks technologies are enabled; the SNMP, WMI, and NMAP technologies are disabled. You can change the default if necessary; see "Configuring Discovery Settings" on page 21.

If more than one technology request returns information for a discovered device, the information is merged together. In the case of conflicting information, the discovery process chooses the best information. If a high priority discovery technology is successful and returns the information, then the other lower priority discovery technologies are aborted for better performance. For example, if WinAPI or WMI is successful, then MAC address and NMAP technologies are aborted.

IP discovery tasks require the following information:

- The range of IP addresses for the devices you want discovered.
- The credentials required for the SSH, WMI, WinAPI, and SNMP discovery technologies to retrieve information from devices. The NMAP, MAC Address, and ZENworks technologies do not require credentials.

  Not all technologies use the same credentials, and all devices might not have the same credentials, so you might need to specify multiple credentials to cover all targeted devices and to utilize all discovery technologies. For example, WMI and WinAPI require Windows credentials, and SNMP requires SNMP credentials.
- The schedule for running the task. You can schedule it to run immediately or at a specified date and time. Optionally, you can choose to not set a schedule, in which case the task is not run until you manually initiate it or schedule a time.
- The ZENworks Server that you want to run the task.

The following table provides detailed information about the IP discovery technologies:

Table 1-1 *IP Discovery Technologies*

IP Discovery Technology	Functionality	Requirements	Prerequisites
WMI (Windows Management Instrumentation)	WMI is the infrastructure for management data and operations on Windows-based operating systems. Discovery issues a remote request to the WMI service on the devices identified by the IP-based discovery task to obtain information. Retrieves the OS type and version, MAC address, Network Adapters, and CPU details of the device. For more information on WMI, see the MSDN Web site (http://msdn.microsoft.com/en-us/library/aa384642%28VS.85%29.aspx).	Because WMI is a Windows-specific technology, the requests generated from a ZENworks Server running on Linux must be routed to a Windows Proxy for processing. For more information, see "Designating a Discovery and Deployment Proxy Server" on page 23.	◆ Microsoft Windows Management Instrumentation Service to be installed and running on the target Windows device. ◆ Credentials of an administrator account on the target device should be specified as Windows credentials in the discovery task. This is required for connecting to the WMI Service. ◆ To authenticate by using the Windows credentials, set the value of the **Network access: Sharing and security model for local accounts** Local Security setting to **Classic - local users authenticate as themselves**. For more information on how to configure the Local Security settings, see "Enabling Classic File Sharing" on page 97. ◆ Since the Remote WMI connection establishes a RPC connection with the target Windows device, the TCP ports 139 and 445 must be allowed by the Windows Firewall of the target device for the WMI discovery technology. For more information on how to open these ports, see "Enabling File and Printer Sharing through Windows Firewall" on page 95. ◆

IP Discovery Technology	Functionality	Requirements	Prerequisites
WinAPI	Issues a request to the registry on the devices identified by the IP-based discovery task to retrieve the OS type and version, and CPU details.	Because WinAPI is a Windows-specific technology, the requests generated from a ZENworks Server running on Linux must be routed to a Windows Proxy for processing. For more information, see "Designating a Discovery and Deployment Proxy Server" on page 23.	◆ Microsoft Remote Registry Service to be installed and running on the target Windows device. ◆ Credentials of an administrator account with read privileges on the Windows registry of the target device should be specified as Windows credentials in the discovery task. This is required for connecting to the Remote Registry Service. ◆ The **File and Printer Sharing for Microsoft Networks** option must be enabled. For more information, see "Enabling File and Printer Sharing for Microsoft Networks" on page 94. ◆ To authenticate by using the Windows credentials, set the value of the **Network access: Sharing and security model for local accounts** Local Security setting to **Classic - local users authenticate as themselves**. For more information on how to configure the Local Security settings, see "Enabling Classic File Sharing" on page 97. ◆ Since the Remote Registry connection establishes a RPC connection with the target Windows device, the TCP ports 139 and 445 must be allowed by the Windows Firewall of the target device. For more information on how to open these ports, see "Enabling File and Printer Sharing through Windows Firewall" on page 95. If the target device is in a different subnet than the Windows Proxy or the Primary server running the task, then the scope of the Firewall exception should include them.

IP Discovery Technology	Functionality	Requirements	Prerequisites
MAC Address	Retrieves the MAC Address of the discovered device. Uses the `ping` and `arp` (Address Resolution Protocol) commands to map the IP addresses of the devices identified by the IP-based discovery task to their associated MAC addresses. The MAC Address discovery gets only the MAC address of the device and does not give any OS information.		◆ For the `arp` command to be successful, the target devices must reside in the same network as the ZENworks Server that performs the discovery request. ◆ For the `ping` command to be successful, the incoming ICMP echo requests (ping) must be enabled on the device, and the ICMP echo requests and echo responses must be allowed on the network.
NMAP	Uses NMAP (Network Mapper) to retrieve the OS type and version details of the devices identified by the IP-based discovery task. **IMPORTANT:** NMAP has certain known limitations. For more information on these limitations, see the NMAP Web site (http://www.nmap.org).		◆ NMAP must be installed on the ZENworks Server that is processing the discovery request. NMAP is freely available from InSecure.org (http://www.insecure.org). For more information on how to configure NMAP for ZENworks, see Appendix C, "Configuring NMAP for ZENworks," on page 165.

IP Discovery Technology	Functionality	Requirements	Prerequisites
ZENworks	Issues a request to the ZENworks Agent or ZENworks preagent on the devices identified by the IP-based discovery task. If the device has the ZENworks Agent, the agent responds with the OS type and version, MAC Address, Network Adapters, CPU, managed device GUID, Management Zone GUID, Management Zone name, ZENworks AgentZENworks Agent version, disk space, and memory details. If the device has the ZENworks preagent installed, the preagent responds with the OS type, CPU, disk space, memory, and the GUID details that should be used to register the device in the Management Zone.		◆ The preagent is only installed on OEM devices or on devices whose registration was removed from the zone.
SNMP	Issues a request to the SNMP service on the devices identified by the IP-based discovery task. SNMP versions 2 and 1 are supported, with SNMP version 2 tried first. Retrieves the OS type and version, MAC address, Network Adapters, and CPU details.	Because the discovery process uses a Windows-based SNMP technology, requests generated from a ZENworks Server running on Linux must be routed to a Windows Proxy for processing. For more information, see "Designating a Discovery and Deployment Proxy Server" on page 23.	◆ To query a device using SNMP, the device must have SNMP enabled. ◆ The SNMP community string must be specified as a SNMP credential in the Discovery Task. ◆ SNMP uses the UDP Port 161. The firewall must be configured to allow access through this port.

IP Discovery Technology	Functionality	Requirements	Prerequisites
SSH	Uses the SSH protocol to communicate with the SSH server on the devices identified by the IP-based discovery task. Depending on the device OS (Linux or NetWare), the device retrieves the OS type, OS or Kernel version, CPU, Network Adapters, and memory details.		◆ To query a device using SSH, the device should have SSH enabled, and the username and password must be specified as General or Linux credentials in the Discovery task. For more information on how to open port 22, see "Prerequisites for Deploying to Linux Devices" on page 98.

LDAP Discovery Technology

For LDAP discoveries, the ZENworks discovery engine issues an LDAP request to the LDAP server. The LDAP request contains the LDAP server name, LDAP port, credentials, the context or group to search, and whether or not to recursively search subcontainers or subgroups.

Device objects that are found are queried for well-known attributes (dnsHostName, OperatingSystem, wmNameDNS, wmNameOS, and so forth) to attempt to determine the OS version and DNS name of the device. If the request specifies a recursive search, the context is searched for well-known container objects. For each container object found, a new LDAP request is created for the container object and appended to the search context of the current request.

LDAP discovery tasks require the following information:

- The connection information (address and port) for the LDAP server.
- The credentials required for reading information from the LDAP directory.
- The directory contexts to search for devices.
- The schedule for running the task. You can schedule it to run immediately or at a specified date and time. Optionally, you can choose to not set a schedule, in which case the task is not run until you manually initiate it or schedule a time.
- The ZENworks Server that you want to run the task.

Advertised Devices

The ZENworks discovery engine allows you to discover devices that have the ZENworks preagent installed, such as OEM devices or devices whose registration was removed from the Management Zone. Only those devices that have the preagent installed respond to an advertised discovery; devices that have the ZENworks Agent do not respond to an advertised discovery.

Discovered Devices

As devices are discovered, they are added to the ZENworks database and listed in the appropriate device type folder in the Discovered panel on the Discovered Devices page.

Each discovered device is categorized by type.

- **All Types:** All discovered devices, regardless of type.
- **Servers:** All discovered devices that have been identified as servers.
- **Workstations:** All discovered devices that have been identified as workstations.
- **Printers:** All discovered devices that have been identified as printers. ZENworks does not manage printers; therefore, you cannot deploy the ZENworks Agent to them.
- **DRAC Devices:** All discovered devices that have been identified as Dell Remote Access Controllers (DRAC).
- **Intel AMT Devices:** All discovered devices that have the Intel Active Management Technology (AMT) capability.
- **Network Equipment:** All discovered devices that have been identified as network equipment. This includes such devices as routers. ZENworks does not manage network equipment; therefore, you cannot deploy the ZENworks Agent to network equipment.
- **Thin Clients:** All discovered devices that have been identified as thin clients.
- **Embedded Workstations:** All discovered devices that have been identified as embedded workstations.
- **Other Devices:** All discovered devices that have been identified but do not fit into one of the other categories. This category includes devices that already have the ZENworks Agent installed.
- **Unknown Devices:** All discovered devices whose operating system cannot be identified. The devices might be listed as unknown because the firewall configuration of the device may block the usage of discovery technologies, or invalid credentials are provided to the discovery technology. You can deploy the ZENworks Agent to these devices if you can manually ensure that the agent is supported on these devices. For more information on list of supported devices, see Managed Device Requirements in *ZENworks System Requirements*.
- **Apple DEP Devices (Settings):** All discovered devices that have been identified as DEP devices. The Device Enrollment Program (DEP) intends to automate MDM enrollment and enables over-the-air configuration of iOS and iPadOS devices purchased from Apple or authorized resellers. Click Settings to configure the DEP device enrollment settings at the device folder level.
- **Deployable Types:** All discovered devices that have been identified as types to which you can deploy the ZENworks Agent.
- **Devices Created Via ZENworks Migration:** All devices that were migrated from ZENworks 7 through the ZENworks Migration utility.
- **Devices Created Via ZENworks Asset Management:** All devices that were migrated from ZENworks Asset Management through the ZENworks Asset Management Migration utility.

Searching Discovered Devices

The search operation for discovered devices works a bit different when compared to other search operations in ZENworks Control Center.

- To search a device that contains a specific word, prefix * before the word.

  Example: Specify *sap in the search field, all discovered devices that contains sap will be listed.
- To search a device that starts with a word, suffix * after the keyword or just mention the keyword.

  Example: Either specify sap or sap* in the search field, all discovered devices that starts with sap will be listed.

Deployable Devices

Devices that meet the requirements for the ZENworks Agent are displayed in ZENworks Control Center in the Deployable Devices panel on the Deployment page.

Using this panel, you can deploy the ZENworks Agent to devices, remove them from the ZENworks database, or ignore them by filtering them out of the list.

2 Discovering Devices By Using IP Addresses

You can perform an IP-based discovery of your network to add devices to your ZENworks database. With an IP discovery, the ZENworks Server uses a set of technologies (WMI, WinAPI, MAC Address, NMAP, ZENworks, SNMP, SSH) to discover as much information about the target devices as possible. The target devices are determined by the IP address range you specify.

- "Configuring Discovery Settings" on page 21
- "Designating a Discovery and Deployment Proxy Server" on page 23
- "Creating an IP Discovery Task" on page 24

Configuring Discovery Settings

IP discoveries use the following configuration settings that can be modified, if necessary:

- Number of discoveries that can be processed concurrently (default is 5)
- IP subnets or address ranges that are to be excluded from the discovery
- Discovery technologies that are used (the default is LDAP, MAC Address, WinAPI, ZENworks, and SSH)

1. In ZENworks Control Center, click the **Configuration** tab.
2. In the Management Zone Settings panel, click **Discovery and Deployment**, then click the **Discovery** option.
3. In the Discovery Process Settings panel, modify the following settings as necessary:

   Maximum Concurrent Discoveries: A discovery task consists of one or more discovery requests. For IP-based discovery tasks, a request is created for each discovery technology and each IP address in the specified range. Therefore, if you use six technologies to discover 10 IP addresses, 60 requests are created. For LDAP-based discovery tasks, a request is created for each context or group to be searched.

   You use this field to specify the maximum number of discovery requests that the ZENworks Server can process at one time. A smaller number eases the traffic load on the network but requires more time to complete the discovery task; you should use a smaller number if you schedule discovery tasks during peak network load times. A larger number has the opposite effect; heavier traffic load with less time to complete the task.

   For more information on the IP discovery process, see "IP Discovery Technologies" on page 12.

   Discovery Technologies: The discovery process can utilize a variety of different technologies. When more than one technology is used, the discovery process initiates a discovery request for each technology, with all technology requests running simultaneously. This is done for each target IP address. For example, if you use MAC Address, SNMP, and WMI, the discovery process creates three requests for each target IP address. The requests are queued and run according to the **Maximum Concurrent Discoveries** setting.

If more than one technology request returns information for a discovered device, the information is merged together. In the case of conflicting information, the discovery process chooses the best information.

Using fewer discovery technologies reduces the time required to complete the discovery task but might also reduce the amount of information received.

For detailed information about each technology, see "IP Discovery Technologies" on page 12.

4 In the IP Addresses to be Excluded panel, specify the IP subnets or address ranges to be excluded from the discovery.

NOTE: All the discovery tasks inherit the IP address ranges specified at the Management Zone level. If the IP address range is specified at a task level, the combined ranges of the Management Zone and discovery task are excluded from the discovery.

You can manually add the IP addresses to be excluded or import the IP addresses to be excluded from a CSV file.

- To manually add the IP address to be excluded:
  1. In the **Range** field, enter the IP address range in one of the following formats:

     xxx.xxx.xxx.xxx: Standard dotted-decimal notation for a single address. For example, `123.45.167.100`.

     xxx.xxx.xxx.xxx - xxx.xxx.xxx.xxx: Standard dotted-decimal notation for a range of addresses. For example, `123.45.167.100 - 123.45.167.125`.

     xxx.xxx.xxx.xxx/n: Standard CIDR (Classless Inter-Domain Routing) notation. With CIDR, the dotted decimal portion of the IP address is interpreted as a 32-bit binary number that has been broken into four 8-bit bytes. The number following the slash (/n) is the prefix length, which is the number of shared initial bits, counting from the left side of the address. The /n number can range from 0 to 32, with 8, 16, 24, and 32 being commonly used numbers. For example, `123.45.167.100/24` matches all IP addresses that start with `123.45.167`. When you add the IP address range to the **Selected IP Ranges** list (see the next step), it is automatically expanded to show the range of addresses in dotted-decimal notation.
  2. To add the IP address range to the **Selected IP Ranges** list, click **Add**.
- To use a CSV list to import an IP address to be excluded:
  1. In the **Selected IP Ranges** list, click **Import**.

     The Import CSV File dialog box is displayed.
  2. Click **Browse** to browse for and select a file that contains a comma-separated or columnar list of IP addresses.
  3. Click **OK**.

5 In the Network Discovery Settings panel, modify the following settings as necessary:

IP Settings: These settings apply when using the WMI and SNMP discovery technologies.

- **Initial ping timeout:** Specifies how long the discovery technology waits for a response to an ICMP query (ping).
- **Maximum ping retries:** Specifies the number of times a ping is repeated before giving up.

- **Increment ping timeout on retries by:** Adds the specified amount of time to each retry. For example, if the initial ping timeout is 200 milliseconds, the maximum ping retries is 3, and the increment is 200 milliseconds, the first retry timeout is 400, the second retry timeout is 600, and the third retry timeout is 800.
- **Perform name lookups:** Uses a reverse lookup to associate the target IP address with a DNS name. Deselect this option if you do not want the DNS name discovered.

SNMP Settings: These settings apply when using the SNMP discovery technology.

- **Initial SNMP timeout:** Specifies how long the discovery technology waits for a response to an SNMP query before assuming that the packet is lost.
- **Maximum SNMP retries:** Specifies the number of times an SNMP query is repeated before giving up.
- **Increment SNMP timeout on retries by:** Adds the specified amount of time to each retry. For example, if the initial SNMP timeout is 500 milliseconds, the maximum SNMP retries is 3, and the increment is 1000 milliseconds, the first retry timeout is 1500, the second retry timeout is 2500, and the third retry timeout is 3500.

SSH Settings: These settings apply when using the SSH discovery technology.

- **SSH connection timeout:** Specifies how long the discovery technology waits to establish a SSH connection with the Linux device.

6 Click **OK** to save the changes.

Designating a Discovery and Deployment Proxy Server

ZENworks Servers running on Linux cannot perform discovery tasks that use Windows-specific technologies such as WMI and WinAPI. Linux servers also cannot perform deployment of ZENworks Agents to Windows devices, as deployment uses Windows-specific technologies. In order to enable the execution of discovery and deployment tasks by Linux ZENworks Servers, you can designate a Windows managed device in your zone to function as a discovery and deployment proxy server. The managed device can be either a Windows server or workstation.

When a Linux ZENworks Server receives a discovery task that includes Windows-specific technologies, it processes the non-Windows discovery technologies and offloads the Windows-specific technologies to the proxy. The proxy performs the discoveries and returns the results to the Linux ZENworks Server. The deployment task is totally offloaded to the Windows Proxy.

If you have only Linux servers in your environment, you must first manually install ZENworks Agent on a Windows device by downloading the agent from `https://IP_address_of_the_ZENworks_Server/zenworks-setup`, then designate the device as a proxy for discovery and deployment tasks.

Designating a Windows Proxy Server

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

2 In the Management Zone Settings panel, click **Discovery and Deployment**, then click the **Windows Proxy** option.

3 Fill in the following fields:

Windows Proxy: Click to browse for and select a Windows managed device (server or workstation) to be used as a Windows Proxy for performing the discovery and deployment tasks instead of a ZENworks Server. The Windows Proxy must reside in the same network as the target devices.

Windows Proxy Timeout: Specify the number of seconds you want the ZENworks Server to wait for a response from the Windows Proxy.

4 Click **OK** to save the changes.

Designating a Linux Proxy Server

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

2 In the Management Zone Settings panel, click **Discovery and Deployment**, then click the **Linux Proxy** option.

3 Fill in the following fields:

Linux Proxy: Click to browse for and select a Linux managed device (server or workstation) to be used as a Linux Proxy for performing the discovery and deployment tasks instead of a ZENworks Server. The Linux Proxy must reside in the same network as the target devices.

Linux Proxy Timeout: Specify the number of seconds you want the ZENworks Server to wait for a response from the Linux Proxy.

4 Click **OK** to save the changes.

Creating an IP Discovery Task

You use the Create New Discovery Task Wizard to create and schedule the tasks used by ZENworks Servers to discover devices on your network and add them to the ZENworks database.

When a discovery task runs, the ZENworks Server creates a discovery request for each IP address and discovery technology (WMI, WinAPI, MAC Address, NMAP, ZENworks, SNMP, SSH) used. For example, if you specify one IP address and use all seven discovery technologies, the ZENworks Server initiates seven discovery requests. Therefore, the more IP addresses you specify and the more discovery processes you use, the longer the discovery task takes to complete. For fastest results, you should create tasks that target smaller ranges of IP addresses and, if possible, assign different ZENworks Servers to process the tasks.

NOTE: For NMAP to work correctly, you need to first configure NMAP for ZENworks. For more information, see Appendix C, “Configuring NMAP for ZENworks,” on page 165.

---

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

2 In the Discovery Tasks panel, click **New** to launch the New Discovery Task Wizard.

3 Complete the wizard by using information from the following table to fill in the fields.

Wizard Page	Details
Select Discovery Type page	Select **IP Discovery Task**. Specify a name for the task. The name cannot include any of the following invalid characters: / \ * ? : " ' < > | ` % ~
Discovery Settings page > **Override Zone Discovery Settings** field	Chose whether to override the discovery settings configured at the Management Zone. If you want to configure the settings on a device folder or a device, you must select **Override Zone Discovery Settings** before you can modify the settings.
Discovery Settings page > **Discovery Technologies**	The discovery process can utilize a variety of different technologies. When more than one technology is used, the discovery process initiates a discovery request for each technology, with all technology requests running simultaneously. This is done for each target IP address. For example, if you use MAC Address, SNMP, and WMI, the discovery process creates three requests for each target IP address. The requests are queued and run according to the **Maximum Concurrent Discoveries** setting. If more than one technology request returns information for a discovered device, the information is merged together. In the case of conflicting information, the discovery process chooses the best information. Using fewer discovery technologies reduces the time required to complete the discovery task but might also reduce the amount of information received. For more information about each technology, see "IP Discovery Technologies" on page 12.

Wizard Page	Details
Enter IP Discovery Settings page > **Range** field	To specify a range of IP addresses for the discovery task: 1. In the **Range** field, specify an IP address range using one of the following formats: **xxx.xxx.xxx.xxx:** Standard dotted-decimal notation for a single address. For example, 123.45.167.100. **xxx.xxx.xxx.xxx - xxx.xxx.xxx.xxx:** Standard dotted-decimal notation for a range of addresses. For example, 123.45.167.100 - 123.45.167.125. **xxx.xxx.xxx.xxx/n:** Standard CIDR (Classless Inter-Domain Routing) notation. With CIDR, the dotted decimal portion of the IP address is interpreted as a 32-bit binary number that has been broken into four 8-bit bytes. The number following the slash (/n) is the prefix length, which is the number of shared initial bits, counting from the left side of the address. The /n number can range from 0 to 32, with 8, 16, 24, and 32 being commonly used numbers. For example, 123.45.167.100/24 matches all IP addresses that start with 123.45.167. When you add the IP address range to the **Selected IP Ranges** list (see the next step), it is automatically expanded to show the range of addresses in dotted-decimal notation. You are recommended to specify an IP address range that does not contain more than 50,000 devices. A task that has a large IP address range does not get started. For more information, see the troubleshooting scenario "Troubleshooting Discovery, Deployment, and Retirement" on page 167. 2. To add an IP address range to the **Selected IP Ranges** list, click **Add**. 3. (Optional) To exclude the IP subnets or address ranges from the discovery, click **Exclude**. The Excluded Addresses dialog box is displayed. For more information on how to exclude the IP subnets or address ranges, see "Device Discovery" on page 9. 4. To add additional ranges, repeat Step 1 and Step 2.

Wizard Page	Details
Enter IP Discovery Settings page > Excluded Addresses dialog box	To specify the IP subnets or address ranges to be excluded from the IP discovery. These ranges are added to the ranges specified in the Management Zone, and the combined ranges are excluded while running the discovery task. To specify the IP subnets or address ranges to be excluded from the discovery, do one of the following: ◆ Manually add the IP address to be excluded: 1. In the **Range** field, enter the IP address range using one of the following formats: **xxx.xxx.xxx.xxx:** Standard dotted-decimal notation for a single address. For example, 123.45.167.100. **xxx.xxx.xxx.xxx - xxx.xxx.xxx.xxx:** Standard dotted-decimal notation for a range of addresses. For example, 123.45.167.100 - 123.45.167.125. **xxx.xxx.xxx.xxx/n:** Standard CIDR (Classless Inter-Domain Routing) notation. With CIDR, the dotted decimal portion of the IP address is interpreted as a 32-bit binary number that has been broken into four 8-bit bytes. The number following the slash (/n) is the prefix length, which is the number of shared initial bits, counting from the left side of the address. The /n number can range from 0 to 32, with 8, 16, 24, and 32 being commonly used numbers. For example, 123.45.167.100/24 matches all IP addresses that start with 123.45.167. When you add the IP address range to the **Selected IP Ranges** list (see the next step), it is automatically expanded to show the range of addresses in dotted-decimal notation. 2. To add an IP address range to the **Selected IP Ranges** list, click **Add**. ◆ Use a CSV file to import an IP address to be excluded: 1. In the **Selected IP Ranges** list, click **Import**. The Import CSV File dialog box is displayed. 2. Click **Browse t**o browse for and select a file that contains a comma-separated or columnar list of IP addresses. 3. Click **OK**.

Wizard Page	Details
Enter IP Discovery Settings page > **Save Credentials to DataStore** field	In order for the SSH, WMI, WinAPI, and SNMP discovery technologies to retrieve information from devices, you must provide credentials that the discovery technologies can use. The NMAP, MAC Address, and ZENworks technologies do not require credentials. Unless you save the credentials, they are stored only in memory. Saved credentials are encrypted in the database for increased security. Credentials that are not saved are cleared from memory when the ZENworks Server is restarted. If you are creating a scheduled deployment task, you might want to save the credentials to ensure that they are still available when the deployment is performed. **NOTE:** Credentials are not saved in the credential vault.

Wizard Page	Details
Enter IP Discovery Settings page > **Credentials** field	Not all technologies use the same credentials, and all devices might not have the same credentials, so you might need to specify multiple credentials to cover all targeted devices and to utilize all discovery technologies. To add a credential: 1. In the Credentials panel, click **Add** to display the Enter Credential Information dialog box. 2. In the **Type** field, select the type of credentials you are defining: **General:** Specifies credentials to be used by all discovery technologies except for SNMP. **Linux:** Specifies credentials for the SSH technology to communicate with the SSH server on a Linux device. **Windows:** Specifies credentials for the WMI and WinAPI technology to access the WMI service and Windows registry on a Windows device. **SNMP:** Specifies community strings for the SNMP technology to access the SNMP service on a device. For example, `public` as the community string. 3. If you selected **General**, **Linux**, or **Windows**, fill in the username and password. You can enter the username for Windows devices in one of the following formats: *username* *domain_name\username* *username@domain_name* *username@fully_qualified_domain_name* **NOTE:** Windows Server 2008 does not support the *username @domain_name* format. 4. If you selected **SNMP**, fill in a community string. 5. Click **OK** to add the credentials to the Credentials panel. 6. Repeat Step 1 through Step 5 to add additional credentials. If you add multiple credentials of the same type (for example, multiple Windows credentials), the technologies that require those credentials use them in the order they are displayed in the Credentials panel, moving from top to bottom. Therefore, you should make sure that you place the most common credentials first in order to speed up the discovery process.

Wizard Page	Details
Set the Discovery Schedule page	Choose whether you want the task to run as soon as it is created (the **Now** option) or if you want to schedule the task to run at a future date and time. If you select **On a Schedule**, choose one of the following schedules: **No Schedule:** Indicates that no schedule has been set. The task does not run until a schedule is set or it is manually launched. This is useful if you want to create the task and come back to it later to establish the schedule or run it manually. **Date Specific:** Specifies one or more dates on which to run the task. **Recurring:** Identifies specific days each week, month, or a fixed interval on which to run the task. See Appendix B, "Schedules," on page 161 or click the **Help** button for more information on the schedules.
Select Primary Server page > *Primary Server* field	Select the ZENworks Server that you want to perform the discovery task. If you are using any Windows-specific discovery technologies (WMI, WinAPI), you must select a ZENworks Server on Windows (not Linux) or you must have already designated a Windows ZENworks Server as a discovery proxy for your Linux servers. For information on discovery proxies, see "Designating a Discovery and Deployment Proxy Server" on page 23.
Select or Edit a Proxy Device page	The Select or Edit a Proxy Device page lets you choose whether you want to use a proxy device to perform the discovery task.

Wizard Page	Details
Select or Edit a Proxy Device page > **Windows Proxy**	If you want to use a Windows Proxy instead of the Primary Server to perform the discovery tasks on Windows devices, click the **Windows Proxy** option and configure the settings in the Select Windows Proxy dialog box. A Windows Proxy is used to perform the following actions: ◆ Enable Linux Primary Servers to perform discovery tasks that use Windows-specific discovery technologies (such as WMI, WinAPI, and SNMP). ◆ Discover Windows devices that are in a different subnet than the Primary Server. ◆ Discover Windows devices in a network enabled for NAT. Discovery through WMI, WinAPI and SNMP requires certain ports to be reachable on the target devices, so the Primary Server can send Remote Registry, WMI, or SNMP requests to the target devices. Ports are opened by adding them as an exception in the Windows Firewall configuration settings. By default, the scope of the exception applies only to the local subnet. If the target device is in a different subnet than the Primary Server from which the discovery is run, you need to add the IP address of the Primary Server as an exception. However, if you use a Windows Proxy in the same subnet as a target device, you do not need to change the scope of the Windows Firewall exception. The connection between the ZENworks Server and the Windows Proxy is secured through SSL. **Override Zone Window Proxy Settings:** Select this option if you want to override the Windows Proxy settings configured at the Management Zone and configure new settings for the task. **Windows Proxy:** Select a Windows managed device (server or workstation) to be used as a Windows Proxy for performing the discovery tasks instead of a ZENworks Server. The Windows Proxy must reside in the same network as the target devices. **Windows Proxy Timeout:** Specify the number of seconds you want the ZENworks Server to wait for a response from the Windows Proxy.

Wizard Page	Details
Select or Edit a Proxy Device page > **Linux Proxy**	If you want to use a Linux Proxy instead of the Primary Server to perform the discovery tasks on Linux devices, click the **Linux Proxy** option and configure the settings in the Select Linux Proxy dialog box. A Linux Proxy is used to perform the following actions: ◆ Enable Primary Servers that cannot perform discovery tasks that use 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. The SSH discovery requires port 22 to be reachable in order to enable the Primary Server to connect to the target device. If the SSH port is blocked in the Network Firewall, you use a Linux managed device in the same subnet as the target device. The connection between the ZENworks Server and Linux Proxy is secured through SSL. For more information on how to open port 22, see "Prerequisites for Deploying to Linux Devices" on page 98. **Override Zone Linux Proxy Settings:** Select this option if you want to override the Linux Proxy settings configured at the Management Zone and configure new settings for the task. **Linux Proxy:** Select a Linux managed device (server or workstation) to be used as a Linux Proxy for performing the discovery tasks instead of a ZENworks Server. The Linux Proxy must reside in the same network as the target devices. **Linux Proxy Timeout:** Specify the number of seconds you want the ZENworks Server to wait for a response from the Linux Proxy.

When you finish the wizard, the discovery task is added to the list in the Discovery Tasks panel. You can use the panel to monitor the status of the task. As devices are discovered, they are listed in the Deployable Devices panel. If you have specified IP addresses to be excluded from a discovery task, then the discovery is not run for those IP addresses and the excluded IP addresses are not included in the **Results** tab.

3 Discovering Devices in LDAP Directories

You can search an LDAP directory for devices to add to your ZENworks database. The directory can be one that is already defined as a user source in your Management Zone, or it can be a new directory.

You can recursively search for device in all the directories from the root context. Or, you can limit the search by specifying one or more contexts to search. Device objects that are found are queried for well-known attributes (dnsHostName, OperatingSystem, wmNameDNS, wmNameOS, and so forth) to attempt to determine the OS version and DNS name of the device.

Before performing an LDAP discovery, make sure the following prerequisites are satisfied:

- An LDAP search requires the ZENworks Server to provide credentials that give read access to the contexts being searched. When accessing Novell eDirectory, the account also requires read rights to the WM:NAME DNS attributes on the workstation and server objects.
- An LDAP search of Active Directory requires the ZENworks Server to use a DNS server to resolve the device DNS name (as recorded on the object DNS name attribute in Active Directory) to its IP address. Otherwise, the device is not added as a discovered device.

You use the Create New Discovery Task Wizard to create and schedule an LDAP discovery task:

1. In ZENworks Control Center, click the **Deployment** tab.
2. In the Discovery Task panel, click **New** to launch the New Discovery Task Wizard.
3. Complete the wizard by using information from the following table to fill in the fields.

Wizard Page	Details
Select Discovery Type page	Select **LDAP Discovery Task**. Specify a name for the task. The name cannot include any of the following invalid characters: / \ * ? : " ' < > | ` % ~
Enter LDAP Settings page > **Search pre-configured LDAP source** field	The Enter LDAP Settings page lets you identify the LDAP directory and contexts where you want to perform the discovery task. A preconfigured LDAP source is one that has already been defined as a user source in your Management Zone. If you want to select a new source, see "Enter LDAP Settings page > Specify an LDAP Source field" on page 35. To use a preconfigured source: 1. Select **Search pre-configured LDAP source**, then select the desired source. 2. If you do not want to search the entire LDAP directory, you can identify specific search contexts/groups. To do so: a. In the LDAP Search Contexts/Groups panel, click **Add** to display the **Enter Context or Group Information** dialog box. b. Fill in the following fields: **Context/Group DN:** Click **Browse** to locate and select the context/group you want to search. **Recursive Search:** Select this option to search all subcontexts/subgroups. c. Click **OK** to save the search context/group. 3. If necessary, modify the LDAP search filter. By default, the filter searches for the computer objectClass or server objectClass. When modifying the filter, you can use the standard filter syntax for your LDAP directory.

Wizard Page	Details
Enter LDAP Settings page > **Specify an LDAP Source** field	You can create a new connection to a LDAP directory in order to discover devices in the directory. If you want to use an existing connection, see Enter LDAP Settings page > Search pre-configured LDAP source field above. To create a new connection to an LDAP directory: 1. Select **Specify an LDAP source**, then fill in the following fields: **LDAP Server:** Specify the IP address or DNS hostname of the server where the LDAP directory resides. **LDAP Port/Use SSL:** The default is standard SSL port (636) or non-SSL port (389), depending on whether the **Use SSL** option is enabled or disabled. If your LDAP server is listening on a different port, select that port number. **Root Context:** Establishes the entry point in the directory; nothing located above the entry point is available for searching. Specifying a root context is optional. If you do not specify a root context, the directory root container becomes the entry point. **Save Credentials to Datastore:** Unless you save the credentials (defined in the **Credentials** list), they are stored only in memory. Saved credentials are encrypted in the database for increased security. Credentials are cleared from memory when the ZENworks Server is restarted. If you want to permanently retain the credentials, you should save them. **Credentials:** Click **Add** to specify a username and password that provides read-only access to the directory. The user can have more than read-only access, but read-only access is all that is required and recommended. When accessing Novell eDirectory, the user account also requires read rights to the WM:NAME DNS attributes on the workstation and server objects. For Novell eDirectory access, use standard LDAP notation. For example, `cn=admin_read_only,ou=users,o=mycompany` For Microsoft Active Directory, use standard domain notation. For example, `AdminReadOnly@mycompany.com` 2. If you do not want to search the entire LDAP directory, you can identify specific search contexts/groups. To do so: a. In the LDAP Search Contexts/Groups panel, click **Add** to display the **Enter Context or Group Information** dialog box. b. Fill in the following fields: **Context/Group DN:** Click **Browse** to locate and select the context/group you want to search. **Recursive Search:** Select this option to search all subcontexts/subgroups. c. Click **OK** to save the search context/group. 3. If necessary, modify the LDAP search filter. By default, the filter searches for the computer objectClass or server objectClass.

Wizard Page	Details
Discovery Settings page	LDAP discovery retrieves the hostname, operating system type and version, and IP address of a discovered device from the LDAP source. Based on the selected discovery technologies, you can obtain the following additional information on a device: ◆ ZENworks Management Status ◆ Operating System Suites ◆ MAC Address ◆ Network Adapters ◆ CPU ◆ Memory and Disk Space To obtain additional information on a device: 1. Select the **Use the IP discovery technologies to gather more information** option. 2. Select **Override Zone Discovery Settings**, then select the discovery technologies. 3. In the Credentials panel, add the credential information. For more information on how to add the credential information, click the **Help** button.
Set the Discovery Schedule page	Choose whether you want the task to run as soon as it is created (the **Now** option) or if you want to schedule the task to run at a future date and time. If you select **Scheduled**, choose one of the following schedules: **No Schedule:** Indicates that no schedule has been set. The task does not run until a schedule is set or it is manually launched. This is useful if you want to create the task and come back to it later to establish the schedule or run it manually. **Date Specific:** Specifies one or more dates on which to run the task. **Recurring:** Identifies specific days each week, month, or a fixed interval on which to run the task. For more information about the schedules, click the **Help** button.
Select Primary Server page	Select the ZENworks Server that you want to perform the deployment task.
Select or Edit a Proxy Device page	The Select or Edit a Proxy Device page lets you choose whether you want to use a proxy device to perform the discovery task.

Wizard Page	Details
Select or Edit a Proxy Device page > **Windows Proxy**	If you want to use a Windows Proxy instead of the Primary Server to perform the discovery tasks on Windows devices, click the **Windows Proxy** option and configure the settings in the Select Windows Proxy dialog box. A Windows Proxy is used to perform the following actions: ◆ Enable Linux Primary Servers to perform discovery tasks that use Windows-specific discovery technologies (such as WMI, WinAPI, and SNMP). ◆ Discover Windows devices that are in a different subnet than the Primary Server. ◆ Discover Windows devices in a network enabled for NAT. Discovery through WMI, WinAPI and SNMP requires certain ports to be reachable on the target devices, so the Primary Server can send Remote Registry, WMI, or SNMP requests to the target devices. Ports are opened by adding them as an exception in the Windows Firewall configuration settings. By default, the scope of the exception applies only to the local subnet. If the target device is in a different subnet than the Primary Server from which the discovery is run, you need to add the IP address of the Primary Server as an exception. However, if you use a Windows Proxy in the same subnet as a target device, you do not need to change the scope of the Windows Firewall exception. The connection between the ZENworks Server and Windows Proxy is secured through SSL. **Override Zone Window Proxy Settings:** Select this option if you want to override the Windows Proxy settings configured at the Management Zone and configure new settings for the task. **Windows Proxy:** Select a Windows managed device (server or workstation) to be used as a Windows Proxy for performing the discovery tasks instead of a ZENworks Server. The Windows Proxy must reside in the same network as the target devices. **Windows Proxy Timeout:** Specify the number of seconds you want the ZENworks Server to wait for a response from the Windows Proxy.

Wizard Page	Details
Select or Edit a Proxy Device page > **Linux Proxy**	If you want to use a Linux Proxy instead of the Primary Server to perform the discovery tasks on Linux devices, click the **Linux Proxy** option and configure the settings in the Select Linux Proxy dialog box. A Linux Proxy is used to perform the following actions: ◆ Enable Primary Servers that cannot perform discovery tasks that use 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. The SSH discovery requires port 22 to be reachable in order to enable the Primary Server to connect to the target device. If the SSH port is blocked in the Network Firewall, you use a Linux managed device in the same subnet as the target device. The connection between the ZENworks Server and Linux Proxy is secured through SSL. For more information on how to open port 22, see "Prerequisites for Deploying to Linux Devices" on page 98. **Override Zone Linux Proxy Settings:** Select this option if you want to override the Linux Proxy settings configured at the Management Zone and configure new settings for the task. **Linux Proxy:** Select a Linux managed device (server or workstation) to be used as a Linux Proxy for performing the discovery tasks instead of a ZENworks Server. The Linux Proxy must reside in the same network as the target devices. **Linux Proxy Timeout:** Specify the number of seconds you want the ZENworks Server to wait for a response from the Linux Proxy.

When you finish the wizard, the discovery task is added to the list in the Discovery Tasks panel. You can use the panel to monitor the status of the task. As devices are discovered, they are listed in the Deployable Devices panel.

4 Importing Devices from CSV Files

You can add devices to the ZENworks database by importing their information from a CSV (comma-separated values) file. When you import information from a CSV file, you map the CSV fields to ZENworks database fields. At a minimum, the CSV file must contain the DNS name or IP address for each device you want to import. The CSV file can contain the information in any order. An option to choose the column (which contains a valid number that is to be mapped with the selected device field) is provided while importing devices from a CSV file.

IMPORTANT: While importing network devices, ensure that you specify **networkdevicedata** in the first line of the CSV file. If **networkdevicedata** is not specified, then the Administrator-Defined Fields defined for Network Devices are not displayed while importing devices from the CSV file.

The imported network devices are listed in the **Devices** > **Discovered** > **Network Equipment** page.

To import devices from a CSV file:

1. In ZENworks Control Center, click the **Deployment** tab.
2. In the **Deployment Activities** list in the left navigation panel, click **Import Deployable Devices** to launch the Import Devices from CSV File Wizard.
3. Complete the wizard by using information from the following table to fill in the fields.

Wizard Page	Details
Select File to Import page	Browse for and select the CSV file that contains the devices you want to import. At a minimum, the CSV file must contain the DNS name or IP address for each device you want to import.
Configure Import	Map the columns in the CSV file to the device fields in the ZENworks database. At a minimum, you must map the CSV file's DNS name or IP address to the ZENworks database DNS Name field or IP Address field. To create the information mappings: 1. Click **Add** to display the Specify Import Columns dialog box. 2. Fill in the following fields: **Field:** Select the device field you want to map to a column in the CSV file. **Column:** Specify a column and then number it to match the selected device field. ***Example 4-1*** *For example* If the first column in a CSV file contains IP address information, the second column contains DNS name information while the third column contains operating system information, then the values of the above fields would be: Field: IP Address, Column:1 Field: DNS Name, Column: 2 Field: Operating System, Column: 3 3. Click **OK** to create the information mapping and add it to the list. 4. To verify that the field is mapped to the correct column, click **Verify**. 5. Repeat the above steps to create and verify additional information mappings.

When you finish the wizard, the devices are added to the list in the Deployable Devices panel.

5 Advertised Discovery

The ZENworks discovery engine allows you to collect information about advertised devices on your network.

- "Configuring the Advertised Discovery Settings" on page 41
- "Discovering Advertised Devices" on page 42

Configuring the Advertised Discovery Settings

Advertised discovery uses the following configuration settings that can be modified, if necessary:

- Advertised discovery interval.
- IP addresses and subnets to scan for advertised devices. By default, only the local subnet is scanned.

1. In ZENworks Control Center, click the **Configuration** tab.
2. In the Management Zone Settings panel, click **Discovery and Deployment**, then click **Advertised Discovery Settings**.
3. In the Advertised Discovery Interval panel, modify the following settings as necessary:

   Allow the system to check for advertised devices: Select this option to enable advertised discovery. All ZENworks Servers perform the discovery. When a preagent receives a discovery request, it responds to the ZENworks Server that initiated the request.

   Days, Hours, Minutes: Specify how often you want to perform the advertised discovery.
4. In the Advertised Discovery Subnets panel, specify subnets for the advertised discovery. By default, the ZENworks Server that performs the discovery scans on its local subnet only.

   To specify a subnet:

   4a To specify a subnet, fill in the following fields:

   IP Address: Specify an IP address located within the subnet. Use the standard dotted-decimal notation. For example, 123.45.167.100.

   Optional CIDR Subnet Mask: Specify the subnet by using the standard CIDR (Classless Inter-Domain Routing) notation. With CIDR, the dotted decimal portion of the IP address (in the IP Address field) is interpreted as a 32-bit binary number that has been split into four 8-bit bytes. You can use this field to enter the prefix length, which is the number of shared initial bits, counting from the left side of the address. The prefix length can range from 0 to 32, with 8, 16, 24, and 32 being commonly used numbers. For example, 123.45.167.100 with an optional CIDR subnet mask (or prefix length) of 24 matches specifies the 123.45.167 subnet.

   4b To add the subnet to the list, click **Add**.

   4c (Optional) To add additional subnets, repeat Step 4a and Step 4b.

4d (Optional) To reorder the list, select a subnet, then click **Move Up** or **Move Down**.

The subnets are scanned in the order listed, from top to bottom.

5 Click **OK**.

Discovering Advertised Devices

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

2 In the **Deployment Activities** list located in the left pane, click **Discover Advertised Devices**.

The ZENworks Server sends an advertised discovery request to all the devices on the network. On receiving the request, the preagent responds to the ZENworks Server.

The discovered advertised devices are listed in the Deployable Devices panel.

6 Viewing or Updating Device Details

After a device is discovered, its details are listed in ZENworks Control Center, based on the information available for a discovered device. For example, if the SNMP information is not available for a discovered device, then the SNMP Information panel is not displayed.

If the discovered information for a device is incorrect or insufficient, administrators with the Edit Discovered Device rights can manually change the details for the fields that have the **Edit** button next to them. However, except for the Asset information, manually updated information is overwritten with the discovered information when a discovery is run again for the same IP address.

You can view the following information about the discovered device:

- **Discovery Information:** Displays the identification information, device type, discovery process status, deployment process status, mode of the discovery, and network type of the device.
- **Network Information:** Displays the IP address, MAC address, and DNS name of the device.
- **Management Information:** Displays the ZENworks Agent version and Management Zone name. For a managed device that belongs to the same zone from which a discovery is run, you can also view the Summary page and hardware and software inventory information of the associated managed device.

  These details are displayed for managed devices only.
- **Asset Information:** Displays the description, manufacturer, model, serial number, and asset tag number of the device.

  For routers, hubs, and switches, the number of ports and firmware revision details are also displayed.

  For printers, the number of pages and firmware revision details are displayed.
- **OS Information:** Displays the operating system type and version, memory, disk space, and hardware information.
- **SNMP Information:** Displays the SNMP object identification, SNMP system name, and up-time of the SNMP service.

To view or update the device details:

1. In ZENworks Control Center, click **Devices** > **Discovered**.
2. In the Discovered panel, click a device type, then click a discovered device for which you want to view or update the details.

   The Details page lists information about the discovered devices.
3. (Conditional) If the discovered information for a device is incorrect or insufficient, click **Edit**, then manually change the details for the fields.

   Your manual changes are overwritten the next time a discovery is run for this device.

7 Geolocating Windows 10 Devices

Use the Geolocation page to find the physical location of a selected Windows device. This ZENworks feature uses the Windows 10 location service to geographically locate devices that operate on Windows 10 version 1709 and later Windows 10 operating systems.

When you successfully execute a remote-find from the ZENworks Control Center using this feature, the coordinates and accuracy of the device's location are displayed on the page. This also starts the dynamic indicator for Last Located, which will reflect the last time you located this device if you re-open the Geolocation page with the device selected.

Click **View on map** to graphically pin-point the location on a Google Maps page.

For information about what determines location accuracy or how the Windows 10 location service works, see https://privacy.microsoft.com/en-us/windows-10-location-and-privacy.

II ZENworks Agent Deployment

The following sections provide information and instructions to help you deploy the ZENworks Agent to devices so that you can manage them. If you face issues with any of the Discovery and Deployment tasks, then check the following logs:

- **On the server:** loader-messages.log and services-messages.log.
- **On the target device:** Event viewer logs (on Windows) and /var/log/messages (on Linux)
- **(If proxy is used) On the proxy device:** zmd-messages.log

---

NOTE: Device discovery and deployment tasks for Agent are not supported for a Mac platform. In this case, the agent needs to be installed manually using a standalone installer.

IMPORTANT: To support legacy Windows devices as mentioned below, weak cipher suites are used to communicate between Servers and Managed Devices and these ciphers might be added into the server configuration. To use strong ciphers, use a newer version of Windows in the zone.

Following are the legacy Windows devices:

- Windows 7 SP1
- Windows Embedded 7 SP1
- Windows Server 2008 SP2
- Windows Server 2008 R2
- Windows 2008 R2 SP1
- Windows 2012
- Windows 2012 R2 Server

- Chapter 8, “Basic Concepts,” on page 49
- Chapter 9, “Managing Deployment Packages,” on page 51
- Chapter 10, “Registering Devices,” on page 59
- Chapter 11, “Deploying the ZENworks Agent,” on page 89
- Chapter 12, “Viewing and Updating the Managed Device Details,” on page 135
- Chapter 13, “Uninstalling the Agent,” on page 139
- Chapter 14, “Deploying the Inventory-Only Module,” on page 141

8 Basic Concepts

Deployment is the process of installing the ZENworks Agent on devices and registering the devices within your Management Zone. The following sections provide information to help you understand the deployment terminology and concepts:

- "Deployment Methods" on page 49
- "Deployment Packages" on page 49
- "ZENworks Agent Versus Inventory-Only Module" on page 50

Ensure that the Deployment Rights are enabled, which are required to perform discovery operation. For more information, see Deployment Rights in ZENworks Administrator Accounts and Rights Reference.

Deployment Methods

There are several deployment methods you can use:

- **Deployment task:** The ZENworks Server can deliver the ZENworks Agent to devices and initiate the installation of the agent. This requires that you create a task, called a deployment task, for the ZENworks Server. The task identifies the target devices, the credentials required to perform an installation on the devices, the registration key to use (optional), and other tasks you want performed on the devices either before or after the installation. You can have a ZENworks Server immediately perform the task, or you can schedule the task for a specific date and time.
- **Manual deployment:** You can manually download the ZENworks Agent deployment package from a ZENworks Server to a device and initiate the installation.
- **Automated deployment:** You can automate deployment by using any method that can launch the ZENworks Agent deployment package. For example, you can use a login script, or, if you have a previous version of ZENworks, you can distribute the ZENworks Agent deployment package as an Application object through Novell Application Launcher.

Installation instructions are provided in Chapter 11, "Deploying the ZENworks Agent," on page 89.

Deployment Packages

Deployment packages contain the files and information needed to install the ZENworks Agent on devices and register the devices in the Management Zone. There are fourteen default system packages that are included on each ZENworks Server. These packages provide for local or network installation of the ZENworks Agent (full agent or partial agent) on various operating system architectures (32-bit and 64-bit).

If necessary, you can modify a deployment package to change the ZENworks Server address or registration key included in the package. For example, assume that you want to use the same package to deploy the agent to devices on your private network and to devices on the other side of a

firewall or router that is using NAT (Network Address Translation). You could modify a package in order to list the ZENworks Server private network address (IP address, DNS name, or both) and also list its NAT address.

For more information about the deployment packages and how to use them, see Chapter 9, “Managing Deployment Packages,” on page 51.

ZENworks Agent Versus Inventory-Only Module

You can fully manage devices on which the ZENworks Agent is deployed. This includes distributing software, enforcing policies, remotely managing the device, and so forth. The ZENworks Control Center displays managed devices on the Managed tab in the Device page.

Deployment instructions for the ZENworks Agent are provided in Chapter 11, “Deploying the ZENworks Agent,” on page 89.

If a Windows device does not meet the requirements for deploying the ZENworks Agent or if you want to inventory a Linux or a Macintosh device, you can deploy the Inventory-Only module.

For details see System Requirements in the *ZENworks System Requirements* for details.

After you deploy the module, the device is added to the ZENworks database. The ZENworks Control Center displays inventoried-only devices on the **Inventoried** tab in the Device page.

NOTE: The inventory-only module only collects and sends the inventory data. It does not perform any of the other tasks associated with the ZENworks Agent.

Deployment instructions for the Inventory-Only module are provided in Chapter 14, “Deploying the Inventory-Only Module,” on page 141.

9 Managing Deployment Packages

Deployment packages contain the files and information needed to install the ZENworks Agent on devices and register the devices in the Management Zone.

Each ZENworks Server contains nine default system packages. These packages are built during installation and system update of the ZENworks Server. In addition to the ZENworks Agent files, each default system package includes the ZENworks Server address and (optionally) a key to use when registering. You cannot change which files a default system package includes, but you can customize the ZENworks Server address and registration key (which is blank unless you specify one).

For example, assume that you are deploying the ZENworks Agent to devices on your private network and to devices on the other side of a firewall or router that is using NAT (Network Address Translation). You could modify a package in order to list the ZENworks Server private network address (IP address, DNS name, or both) and also list its NAT address.

The following sections provide information and instructions to help you manage your deployment packages:

- "Package Types and Architectures" on page 51
- "Default System Packages Versus Custom Packages" on page 53
- "Customizing Packages" on page 54
- "Rebuilding Packages" on page 56

Package Types and Architectures

- "Package Types and Architectures for Windows" on page 51
- "Package Types and Architectures for Linux" on page 52
- "Package Types and Architectures for Macintosh" on page 53

In order to support deployment of the ZENworks Agent from files on either local or network media, there are various types of deployment packages for Windows, Linux and Macintosh operating systems.There are three versions of each of these packages: x86, x86_64, and x86/x86_64. The x86 and x86_64 packages are used in deployments to 32-bit and 64-bit devices, while the x86/x86_64 version is used in deployments to either 32-bit or 64-bit devices.

Package Types and Architectures for Windows

The following packages are available for installing the ZENworks Agent on Windows:

- **Network:** Contains the `web-installer.exe` and configuration file, which downloads the ZENworks Agent files from a ZENworks Server and installs the agent on the device.
- **Standalone:** Contains the pre-agent, all the ZENworks Agent module files, and the Microsoft .NET 4.8 installables. The ZENworks Agent is installed to the device, but no registration or management occurs until the device connects to the network.

- **Web:** The `web-installer.exe` will install the ZENworks Agent. The web installer does not include any zone specific information and is signed by Micro Focus to prevent the antivirus from blocking the install as potential malware.

To support the various Windows architectures, there are three versions of each package:

- **x86 version:** You use the x86 version for manual deployment to 32-bit Windows devices.

  The x86 package (`PreAgentPkg_AgentCompleteDotNet.exe`) is located in the following directory on the ZENworks Server:

  %ZENSERVER_HOME%`\install\downloads\setup\x86` on Windows and `/opt/microfocus/zenworks/install/downloads/setup/x86` on Linux.

- **x86_64 version:** You use the x86_64 version for manual deployment to 64-bit Windows devices.

  The x86_64 package (`PreAgentPkg_AgentCompleteDotNet.exe`) is located in the following directory on the ZENworks Server:

  %ZENSERVER_HOME%`\install\downloads\setup\x86_64` on Windows and `/opt/microfocus/zenworks/install/downloads/setup/x86_64` on Linux.

- **All Architectures version:** This package is used by the ZENworks Server when completing a deployment task. It contains files for both 32-bit and 64-bit Windows devices.

  The All Architectures packages (`PreAgentPkg_Agent.zip`, `PreAgentPkg_AgentCompleteDotNet.exe`, and `web-installer.exe`) are located in the following directory on the ZENworks Server:

  %ZENSERVER_HOME%`\install\downloads\setup\_all` on Windows and `/opt/microfocus/zenworks/install/downloads/setup/_all` on Linux.

Package Types and Architectures for Linux

The following packages are available for installing the ZENworks Agent on Linux:

To support the various Linux architectures, there are three versions of each package:

- **x86 version:** You use the x86 version for manual deployment to 32-bit Linux devices.

  The x86 package (`PreAgentPkg_AgentLinuxComplete.bin`) is located in the following directory on the ZENworks Server:

  %ZENSERVER_HOME%`\install\downloads\setup\x86` on Windows and `/opt/microfocus/zenworks/install/downloads/setup/x86` on Linux.

- **x86_64 version:** You use the x86_64 version for manual deployment to 64-bit Linux devices.

  The x86_64 package (`PreAgentPkg_AgentLinuxComplete.bin`) is located in the following directory on the ZENworks Server:

  %ZENSERVER_HOME%`\install\downloads\setup\x86_64` on Windows and `/opt/microfocus/zenworks/install/downloads/setup/x86_64` on Linux.

- **All Architectures version:** This package is used by the ZENworks Server when completing a deployment task. It contains files for both 32-bit and 64-bit Linux devices.

The All Architectures packages (`PreAgentPkg_AgentLinux.zip`, `PreAgentPkg_AgentLinuxComplete.bin` and `web-installer.bin`) are located in the following directory on the ZENworks Server:

%ZENSERVER_HOME%`\install\downloads\setup\_all` on Windows and `/opt/microfocus/zenworks/install/downloads/setup/_all` on Linux.

Package Types and Architectures for Macintosh

The following packages are available for installing the ZENworks Agent on Macintosh devices:

- **Network:** Contains only the pre-agent, which downloads the ZENworks Agent files from the ZENworks Server.
- **Standalone:** Contains the pre-agent and all the ZENworks Agent module files.

The architecture of the agent to be installed depends upon the architecture of Java installed on the device. To support the various Macintosh architectures, there are three versions of each package:

- **x86 version:** You use the x86 version for manual deployment to Macintosh devices having 32-bit Java installed on the device.

  The x86 packages (`PreAgentPkg_AgentMac.bin` and `PreAgentPkg_AgentMacComplete.bin`) are located in the following directory on the ZENworks Server:

  %ZENSERVER_HOME%`\install\downloads\setup\x86` on Windows and `/opt/microfocus/zenworks/install/downloads/setup/x86` on Linux and Macintosh devices.
- **x86_64 version:** You use the x86_64 version for manual deployment to 64-bit Macintosh devices.

  The x86_64 packages (`PreAgentPkg_AgentMac.bin` and `PreAgentPkg_AgentMacComplete.bin`) are located in the following directory on the ZENworks Server:

  %ZENSERVER_HOME%`\install\downloads\setup\x86_64` on Windows and `/opt/microfocus/zenworks/install/downloads/setup/x86_64` on Linux and Macintosh devices.

Default System Packages Versus Custom Packages

You can customize any of the default system packages to change the package or to create a new custom package. When you do so, you can modify the ZENworks Server address and registration key; you cannot modify, add, or remove the ZENworks Agent files.

Only the All Architectures packages are used by the ZENworks Server when completing a deployment task. Therefore, any custom packages you create, or any modifications you make to the x86 or x86_64 system packages, are used only during manual deployments of the ZENworks Agent.

Customizing Packages

1. In ZENworks Control Center, click the **Deployment** tab.
2. Click **Edit Deployment Package** (located in **Deployment Activities** list in the left navigation pane) to launch the Edit Deployment Package Wizard.
3. Complete the wizard by using information from the following table to fill in the fields.

Wizard Page	Details
Select Deployment Package to Edit page	In the **Target Operating System** field, select the operating system of the package that you want to edit.oIn the **Target Architecture** list, select the architecture of the package you want to edit. ◆ **x86 Architecture (32-bit):** Used in manually deploying the agent to 32-bit devices. ◆ **x86_64 Architecture (64-bit):** Used in manually deploying the agent to 64-bit devices. ◆ **All Supported Architectures:** Used by the ZENworks Server to complete deployment tasks for either 32-bit or 64-bit devices. In the **Package Install Type** list, select the installation type of the package that you want to edit. The packages in the list are determined by the **Target Operating System** that you selected for the device. The following packages are available for Windows: ◆ **Network Installation** Contains the web installer and configuration file, which downloads the ZENworks Agent files from a ZENworks Server. The following packages are available for Linux: ◆ **Network Installation** Contains the web installer and configuration file, which downloads the ZENworks Agent files from the ZENworks Server and the JRE installables. ◆ **Standalone Installation:** Contains the pre-agent, all the ZENworks Agent module files, and the JRE installables. In the **Package Name** list, select the name of the package that you want to edit. The names in the list are determined by the architecture and installation type you selected. The list displays the names of any packages with the selected architecture and installation type. By default, the system package is always displayed. The system package is the predefined deployment package that meets the architecture and installation type criteria you specified.

Wizard Page	Details
	Other package names are displayed only if you have edited the system package and saved the customized version as a new package. You can specify any name for the customized package. The name must not contain any of the following invalid characters: / \ * ? : " ' < > | ` % ~. The directory, used to store the package, is given the specified name and the package name remains the same.
Provide Primary Server Information page	Specify the addresses that can be used to access the ZENworks Server. A device needs to access the ZENworks Server when the deployment is a network installation (the pre-agent must download the ZENworks Agent files from the ZENworks Server) and when it registers as a managed device. All addresses you specify must belong to the same ZENworks Server. For example, assume that you are deploying the ZENworks Agent to devices on your private network and to devices on the other side of a firewall or router that is using NAT (Network Address Translation). You would list the ZENworks Server private network address (IP address, DNS name, or both) and also list its NAT address.
Add Registration Key page	Select a registration key to use during the registration portion of the deployment process. A registration key provides information about the folders and groups to which a device is assigned during registration. Selecting a registration key is optional; if you do not select one, registration rules are used to determine the folder and group assignments. To deploy to servers or workstations, choose a server registration key or a workstation registration key respectively. For more information about registration keys and rules, see Chapter 10, “Registering Devices,” on page 59.
Additional Language Selection page	On Windows, select additional language packages to be included with the deployment package. The progress and message logs for the deployment process are displayed in English by default. If you want to receive the messages in the language of the machine locale, then you must add the necessary additional language packs to the deployment package.

Wizard Page	Details
Select Destination for the New Deployment Package page	Select whether you want to overwrite the existing package or save the edited package as a custom package. The two options are: **Overwrite Original Deployment Package:** Replace the original package with this edited package. **Select a Name for the New Deployment Package** Saves the edited package as a new custom package. The original package remains unchanged. You can specify any name you want for the new custom package. The name must not contain any of the following invalid characters: / \ * ? : " ' < > | ` % ~. The name that you specify is used to identify the updated packages on the zenworks-setup page. The package name remains the same and the directory used to store the package is given the name you specify.  All new packages are saved in the ZENworks Server: *%ZENSERVER_HOME%*`\install\downloads\custom` directory on Windows and `/opt/microfocus/zenworks/install/downloads/custom` on Linux. For example, if you modify the x86 version of the `PreAgentPkg_Agent.exe` package and save it with a name of `ExternalPack`, the file is stored as follows:  *%ZENSERVER_HOME%*`\MicroFocus\ZENworks\install\downloads\custom\ExternalPack\x86\PreAgentPkg_Agent.exe` on Windows and `/opt/microfocus/zenworks/install/downloads/custom/ExternalPack/x86/PreAgentPkg_Agent.exe` on Linux. **NOTE:** If you want to delete custom deployment packages, you must manually delete the directory containing the packages.

Rebuilding Packages

You must rebuild the default and custom deployment packages in the following scenarios:

- If the Primary Server port has been changed or is incorrect in the package.
- To include all the new and updated `MSI` or `RPM` files that are provided as patches.

  The new and updated `MSI` files are located in the *%ZENSERVER_HOME%*`\install\downloads\msi` directory on Windows and in the `/opt/microfocus/zenworks/install/downloads/msi` directory on Linux.

  The new and updated `RPM` files are located in the *%ZENSERVER_HOME%*`\install\downloads\rpm` directory on Windows and in the `/opt/microfocus/zenworks/install/downloads/rpm` directory on Linux.
- If the server certificate has been changed.

The following sections provide instructions for rebuilding the default and custom packages:

- "Rebuilding the Default Packages" on page 57
- "Rebuilding the Custom Packages" on page 58

Rebuilding the Default Packages

The default packages are the system packages that are included on each ZENworks Server to deploy the agent to your device. For more information on the default packages, see "Deployment Packages" on page 49.

To rebuild the default packages:

1. Do one of the following:
   - **On Windows:** At the command prompt, enter:

     `microfocus-zenworks-configure -Z -c CreateExtractorPacks`
   - **On Linux:** At the console prompt, change to the `/opt/microfocus/zenworks/bin` directory, then enter:

     `./microfocus-zenworks-configure -Z -c CreateExtractorPacks`
2. When prompted to select the packages to be rebuilt, (by default, only the `Agent Network Package - Windows` is selected), do one of the following:
   - To rebuild only the default package, press Enter.
   - To rebuild additional packages, type the number corresponding to a package, then press Enter twice.

     For example, if you type 2, then press Enter twice, the `Agent Network Package - Windows` (default) and `Agent Complete Package - Windows` are rebuilt.
   - To rebuild all the packages, type `2,3,4,5,6,7` then press Enter twice.
   - To rebuild all the packages, type `2,3,4` then press Enter twice.

NOTE: Choosing the following 6 and 7 options will not rebuild the Mac pre-agent installer packages.

- 6-[ ] Agent Network Package - Mac
- 7-[ ] Agent Complete Package - Mac

IMPORTANT: Ensure that you do not use the `zman surp` command to rebuild deployment packages. This command is used to complete a partially completed system update activity and not to rebuild packages. Therefore, when you run the `zman surp` command, any updates made in the system, such as changes in the server's hostname, is not picked up by the command. It reads the hostnames that are already present in the deployment package and reuses them. For example, if you have a server with hostname A, then the current deployment package will also have the hostname as A. If you change the hostname of the server to B, and run the `zman surp` command, then the agent package will still have the hostname as A. When you try to install the agents with this deployment package, they will try to register to hostname A, due to which registration might fail. However, if you run the `CreateExtractorPacks` configure action, then the latest hostname is retrieved and updated in the deployment packages.

Rebuilding the Custom Packages

The custom packages are created by customizing any of the default system packages. For more information on the custom packages, see "Default System Packages Versus Custom Packages" on page 53.

NOTE: From ZENworks 2020 Update 3, only All Architecture is supported for the network packages. During the system update, ZENworks uses the configuration of all architecture or x86_64 (64-bit) or x86 (32-bit) to rebuild an All Architecture version, and the existing x86 (32-bit) and x86_64 (64-bit) will be removed for custom packages. Precedence for choosing the existing custom package for rebuilding will be in the order of all architecture, x86_64 (64-bit) and then x86 (32-bit).

From ZENworks 2020 Update 3, only the Standalone (.NET included) package is available. During the system update, ZENworks uses the configuration of either Standalone (.NET included) or Standalone (.NET required) to rebuild the Standalone (.NET included) package. Standalone (.NET included) takes higher precedence for rebuilding. The existing Standalone (.NET required) package will be removed.

To rebuild the custom packages:

1. Do one of the following:
   - **On Windows:** At the command prompt, enter:

     ```
     microfocus-zenworks-configure -Z -c RebuildCustomPacks
     ```
   - **On Linux:** At the console prompt, change to the `/opt/microfocus/zenworks/bin` directory, then enter:

     ```
     ./microfocus-zenworks-configure -Z -c RebuildCustomPacks
     ```
2. When prompted to select whether to rebuild the custom packages, press Enter.

10 Registering Devices

When you install the ZENworks Agent to a device, the device is registered in your Management Zone and becomes a managed device. The following sections provide information to help you understand and manage the registration process:

- "What Happens During Registration" on page 59
- "Creating Registration Keys and Rules" on page 60
- "Creating Authorization Key" on page 67
- "Modifying the Device Naming Template Used During Registration" on page 68
- "Enabling Dynamic Renaming of Devices During Registration" on page 69
- "Reconciling Devices with existing Device Objects During Registration" on page 70
- "Disabling the Use of Registration Rules" on page 81
- "Adding Pre-approved Devices" on page 82
- "Manually Registering a Device" on page 85
- "Unregistering a Device" on page 86

IMPORTANT: If you have freshly installed ZENworks, then by default, TLS1.3 will be enabled in the zone and when you try to register an older OS version device with Microsoft .NET version older than 4.7, then the device registration fails. However, the agent will be installed on the device.

If you are upgrading an existing zone, TLS1.3 will not be enabled by default. If you are enabling TLS1.3 in the zone, then some of the features on the already registered devices might not work as expected and new device registration may fail if Microsoft .NET 4.7 is not installed on all the devices in the zone. For more information, see Securing ZENworks by Disabling Older Security Protocols in the ZENworks Best Practices Guide.

What Happens During Registration

The ZENworks Agent includes a service that performs all registration tasks. The tasks performed by the Registration service depend on whether the device is registering for the first time, performing a scheduled refresh, or reregistering with a new registration key. The following table lists the tasks performed in each scenario.

Table 10-1 *Registration tasks*

Task	Initial Registration	Refresh	Reregistration [1]
Create device object in ZENworks database	Yes	No	No
Name device object according to device naming template	Yes	Yes [2]	Yes [2]

Task	Initial Registration	Refresh	Reregistration [1]
Add device to folder	Yes	No	No
Add device to groups [3]	Yes	No	Yes
Add site, department, and location information [3]	Yes	No	Yes
Update device attributes (GUID, IP address, DNS name, last contact time, etc.)	Yes	Yes	Yes

[1] Reregistration assumes that the device object has not been removed from the ZENworks database and that the device is simply being reregistered using a new registration key.

[2] Occurs only if the **Device Dynamic Rename** option is enabled. See "Enabling Dynamic Renaming of Devices During Registration" on page 69 for more information.

[3] Occurs only if the key or rule being used for registration includes this information. See "Creating Registration Keys and Rules" on page 60 for more information.

During registration, if you configure the `SendRegKeyOnEveryRefresh` registry key on the agent, after every refresh, the agent will send the registration key in the `initial-web-service` file, and the group membership will be updated after every refresh. For more information, see the *ZENworks Registry Keys Reference*.

Creating Registration Keys and Rules

The first time a device registers, it is added to a folder. By default, it is added to either the `/Servers` folder or the `/Workstations` folder, depending on the device type.

You can use registration keys and registration rules to override the default folder assignment and specify another folder, and to assign the device to groups. Although you can manually move a device to another folder and add it to groups after the device registers, this can become burdensome if you have a large number of devices or if you are consistently adding new devices. The best way to manage a large number of devices is to use registration keys and rules to automatically add them to the correct folders and groups during registration.

- **Registration key:** A registration key is an alphanumeric string that you manually define or randomly generate. During deployment of the ZENworks Agent on a device, the registration key must be provided. When the device connects to a ZENworks Server for the first time, the device is added to the folder and groups defined within the key.
- **Registration rule:** A registration rule is a set of predefined criteria (for example, operating system type, CPU, or IP address) that you define. If the device meets the criteria, the rule is used for registration. You can create multiple rules; all rules are checked before the default folder is used. Registration rules are applied only if a registration key is not used.

The following sections provide instructions for creating registration keys and rules:

- "Creating a Registration Key" on page 61
- "Creating a Registration Rule" on page 63

Creating a Registration Key

The steps in this section explain how to create a registration key. After you have created a key, you can use the key in the following ways:

- Include the key in a deployment task so that it is used during installation of the ZENworks Agent. See Chapter , "Using a Task to Deploy the Agent," on page 94.
- Add the key to a deployment package so that when the package is used in either a deployment task or a manual installation, the registration key is applied. See "Deployment Packages" on page 49.
- Use the key with the ZENworks Agent command line utility (`zac`) to initially register a device within a zone (`zac register` command), or to manually reregister the device with an additional key (`zac add-reg-key` command). See "Manually Registering a Device" on page 85.

To create a registration key:

1. In ZENworks Control Center, click the **Configuration** tab, then click the **Registration** tab.
2. In the Registration Keys panel, click **New** > **Registration Key** to launch the Create New Registration Key Wizard.
3. Complete the wizard by using information from the following table to fill in the fields.

Wizard Page	Details
Basic Information page	Define the registration key name and folder location, add information to describe the key, and specify the number of times the key can be used. **Key Code:** Provide a key code for the registration key. When devices register during installation, this is the key code the device provides to be assigned to the folder and groups associated with this registration. Any device that presents this key code is given the assignments associated with this registration. Choose something simple for reduced security, or click **Generate** to generate a complex registration string that is difficult to guess. Use the **Generate** option along with a registration key limit for increased security. If you manually enter a name, the name must be different than any other registration key names and must not use any of the following invalid characters: / \ * ? : " ' < > | ` % ~. **Folder:** Specify the folder for this registration key. This is for organizational purposes only. Devices do not need to know where a registration key is located in order to use it to register, they simply need to know the key name. **Description:** Use this field to provide information about the new registration key. This is for your benefit. This field appears only in ZENworks Control Center. **Number of Times This Key Can Be Used:** For security purposes, this enables you to limit the number of times the devices can use this key to register.

Wizard Page	Details
Containment Rules page	Specify the folder in which to place the devices. As a general rule, devices with similar configuration settings (refresh intervals, logging settings, remote management settings, and so forth) should be grouped in the same folder so that you can specify the configuration settings on the folder and have the devices in the folder inherit them. You should not use the same folder for devices that require different configuration settings; doing so prohibits you from using the folder to define the settings and forces you to define them on each individual device.
Device Fields	Specify the department, site, and location information you want entered on a device details page when it registers. For example, if you enter `Accounting` in the **Department** field, then `Accounting` is entered in the **Department** field on the device details page.
Group Membership page	Specify the groups that devices will become members of when they register. Adding groups causes registering devices to receive any assignments provided by membership in the groups. Assignments from group membership are additive, so if a device is assigned to both groups A and B, the device receives all assignments from both groups. You can only add groups that are valid for the type of device folder you specified on the previous page of the wizard. For example, if you specified the `/Devices/Workstations` folder, you can only choose workstation groups. To specify a group: 1. Click **Add** to display the Groups dialog box. 2. Browse for and select the group (or groups) to which you want to add the devices. To do so: a. Click next to a folder (for example, the `Workstations` folder or `Servers` folder) to navigate through the folders until you find the group you want to select. or Search for the group by entering its name in the **Item name** box. You can use an asterisk (*) as a wildcard. For example, entering P* finds all groups that start with P, or entering *Accounting finds all groups that end with Accounting. b. Click the underlined link in the **Name** column to select the group and display its name in the **Selected** list box. c. Repeat steps 2a and 2b until you have selected all groups to which you want to assign membership. d. Click **OK** to add the selected groups to the list.

Wizard Page	Details
Reconcile Settings page	Specify how you want the to reconcile the existing devices with the new devices that come for registration in the Management Zone. For information, see "Reconciling the Devices" on page 72. Enable reconcile setting if ZENworks Agents are deployed in VDI environment. This device reconcile setting take precedence over zone level device reconcile settings.

When you complete the wizard, the key is added to the Registration Keys panel.

You can also use the `registration-create-key` command in the zman utility to create a registration key. For more information, see "Registration Commands" in the *ZENworks Command Line Utilities Reference*.

Creating a Registration Rule

1. In ZENworks Control Center, click the **Configuration** tab, then click the **Registration** tab.
2. In the Registration Rules panel, click **New** to launch the Create New Registration Rule Wizard.
3. Complete the wizard by using information from the following table to fill in the fields.

Wizard Page	Details
Basic Information page	Define the rule name and add information to describe the rule. **Name:** Provide a name for the rule. Users never see the rule name; it displays only in ZENworks Control Center. The name must be different than any other registration key names and must not use any of the following invalid characters: / \ * ? : " ' < > | ` % ~. **Description:** Provide information about the new registration rule. The information appears only in ZENworks Control Center.

Wizard Page	Details

Device Criteria page	Define the criteria that must be met for the registration rule to be applied to a device. The criteria are defined through the use of filters. At least one filter must be defined.
	1. Click **Add Filter** to add a filter line.
	2. Create the filter expression.
	An expression consists of a criteria option, operator, and value.
	Example 1:
	`IPAddress Equal to 123.45.67.89`
	`IPAddress` is the criteria option, `Equal to` is the operator, and `123.45.67.89` is the value. In the above example, the registration rule is applied only to devices whose IP addresses is equal to 123.45.67.89.
	Example 2:
	`NOT IPAddress Equal to 123.45.67.89`
	You can use NOT to perform a logical negation of the expression.
	In the above example, the registration rule is applied only to devices whose IP addresses is not equal to 123.45.67.89.
	Example 3:
	`IPAddress Within 123.45.67.89-123.45.67.99`
	You can use the `Within` operator to specify the IP address range. Two types of IP address ranges are supported:
	◆ Standard dotted-decimal notation
	Example: 123.45.67.89-123.45.67.99
	◆ CIDR notation
	Example: 123.45.67.89/24, where /24 represents the prefix length, which is the number of shared initial bits, counting from the left side of the address.
	The criteria options you can use are listed below, along with possible values. The format for all values, with the exception of CPU, Language, Device Type and OS, are free form string.
	◆ Azure AD Tenant ID: d7878af8-383c-4161-8b76-e8fc4566b42e
	◆ CPU: Intel(R) Pentium(R) M processor 1600MHz
	◆ DNS: abc.xyz.com
	◆ Device Carrier: T-mobile
	◆ Device Manufacturer: Apple
	◆ Device Model: MD439LL/A
	◆ Device Type: Workstation or Server
	◆ GUID: 5bf63fb9b1ed4cd880e1a428a1fcf737
	◆ Hostname: zenserver
	◆ IMEI: 2436262256
	◆ IPAddress: 123.45.67.89
	◆ Language: Portuguese (Brazil)
	◆ MAC Address: 00-0c-29-e8-cd-3a
	◆ OS: win2003-se-sp1-x86
	3. If necessary, click **Add Filter** to create another filter.
	Filters are combined with the AND operator, which means that the criteria defined in each filter must be met before the registration rule is applied to a device. For example, OS Equal to Windows Server 2003 AND

Wizard Page	Details

Device Criteria page (continued)	You can add filters individually or in sets. Logical operators, either **AND** or **OR**, are used to combine each filter and filter set. By default, filters are combined using **OR** (as determined by the **Combine Filters Using** field) and filter sets are combined using **AND**.
	
	You can change the default and use **AND** to combined filters, in which case filter sets are automatically combined using **OR**. In other words, the logical operator that is to combine individual filters (within in a set) must be the opposite of the operator that is used between filter sets.
	
	You can easily view how these logical operators work. Click both the **Add Filter** and **Add Filter Set** options a few times each to create a few filter sets, then switch between **AND** and **OR** in the **Combine Filters Using** field and observe how the operators change.
	
	As you construct filters and filter sets, you can think in terms of algebraic notation parentheticals, where filters are contained within parentheses, and sets are separated into a series of parenthetical groups. Logical operators (**AND** and **OR**) separate the filters within the parentheses, and the operators are used to separate the parentheticals.
	
	For example, "(u AND v AND w) OR (x AND y AND z)" means "match either uvw or xyz." In the filter list, this looks like:
	
	`u AND`
	`v AND`
	`w`
	`OR`
	`x AND`
	`y AND`
	`z`

Containment Rules page	Specify the folder in which to place the devices. As a general rule, devices with similar configuration settings (refresh intervals, logging settings, remote management settings, and so forth) should be grouped in the same folder so that you can specify the configuration settings on the folder and have the devices in the folder inherit them. You should not use the same folder for devices that require different configuration settings; doing so prohibits you from using the folder to define the settings and forces you to define them on each individual device.
Device Fields	Specify the department, site, and location information you want entered on a device details page when it registers. For example, if you enter `Accounting` in the **Department** field, then `Accounting` is entered in the **Department** field on the device details page.

Wizard Page	Details
Group Membership page	Specify the groups that devices will become members of when they register. Adding groups causes registering devices to receive any assignments provided by membership in the groups. Assignments from group membership are additive, so if a device is assigned to both groups A and B, the device receives all assignments from both groups. You can only add groups that are valid for the type of device folder you specified on the previous page of the wizard. For example, if you specified the `/Devices/Workstations` folder, you can only choose workstation groups. To specify a group: 1. Click **Add** to display the Groups dialog box. 2. Browse for and select the group (or groups) to which you want to add the devices. To do so: a. Click next to a folder (for example, the `Workstations` folder or `Servers` folder) to navigate through the folders until you find the group you want to select. or Search for the group by entering its name in the **Item name** box. You can use an asterisk (*) as a wildcard. For example, entering P* finds all groups that start with P, or entering *Accounting finds all groups that end with Accounting. b. Click the underlined link in the **Name** column to select the group and display its name in the **Selected** list box. c. Repeat steps 2a and 2b until you have selected all groups to which you want to assign membership. d. Click **OK** to add the selected groups to the list.
Reconcile Settings page	Specify how you want the to reconcile the existing devices with the new devices that come for registration in the Management Zone. For information, see "Reconciling the Devices" on page 72. Enable reconcile setting if ZENworks Agents are deployed in VDI environment. This device reconcile setting take precedence over zone level device reconcile settings.

When you complete the wizard, the rule is added to the Registration Rules panel. Rules are applied from the top down. You want to list the more restrictive rules first, followed by the more general rules. If no rules apply, the default server and workstation rules are applied.

4 If you want to reorder the rules, click **Advanced** (located in the upper right corner of the Registration Rules panel).

5 Select the check box in front of the rule you want to move.

6 Click **Move Up** or **Move Down** to reposition the rule.

You can also use the `ruleset-create` command in the zman utility to create a registration rule. For more information, see "Ruleset Commands" in the *ZENworks Command Line Utilities Reference*.

Creating Authorization Key

From ZENworks 2020 Update 2 onwards, the Authorization Key will be used to authorize devices while registering the devices to the Management Zone. While registering the device, the key will be used to validate if the device is authorized to register with the zone. Ensure that you have Configure Authorization Key and View Authorization Key rights to create or view the authorization key. Authorization key is one of the methods to securely register the device, you can also add the devices to the pre-approved list. For more information, see "Adding Pre-approved Devices" on page 82.

If you have enabled the Security setting on a ZENworks Update 2 server to which the devices will be registered, then you need to use the Authorization key to register the device. For more information on enabling the Security setting, see Security Commands in the ZENworks Command Line Utilities Reference.

To create an authorization key, perform the following:

1. In ZCC, click Configuration > Registration
2. In the Authorization Keys panel, click New > Authorization Key.
3. In the New Authorization Key window, perform the following:
   - Authorization Key: You can either specify the key-value or click Generate to populate the field with a unique system-generated value.

     If you are specifying the value, ensure that the key-value includes alphanumeric characters and hyphens, and key length are between 6 and 10 characters, by default.
   - Usage Limit: You can either select Unlimited or select Limit to and specify how many times the authorization key can be used to register devices to the zone.

     Based on whether you want to allow the key to be used for an unlimited number of times or whether you want it to be limited to a specific number of uses, select Unlimited or select Limit to and specify the related value.

     The limit value should be a positive integer and the value can range from 1 to 2147483647.
   - Key Expiry Date: You can either select Does Not Expire or select Expire on, and then click the calendar icon to select a date after which the authorization key should be invalid. Ensure that you select a date that is later than the current date.
   - Usage Notes: Specify a note that provides information related to the usage of the key.
4. Click Add.

NOTE: ◆By default, the usage limit will be set to 1, and the key will expire on the same day at 23:59:59.

- The fields cannot be modified if the key is revoked.
- The Authorization Key cannot be modified if the key is used at least once.

Following are some of the additional actions that can be performed on the Authorization Key:

Task	Steps
Edit a key	1. Click the key name. 2. Modify the fields as required, and then click **Save**. If you need help with the options, click the **Help** button.
Delete a key	1. Select the check box next to the key or folder that you want to delete. 2. Click **Action** > **Delete**.
Revoke a key	1. Select the check box next to the key or folder that you want to revoke. 2. Click **Action** > **Revoke**.
Create a folder	1. Click New > Folder to display the New Folder dialog box. 2. In the Name field, specify a unique name for the folder. 3. In the Folder field, click to browse and select the folder where you want the new folder created. 4. Click OK to create the folder.
Move a Key	1. Select the check box next to the key. 2. Click **Edit** > **Move**. 3. In the Select Folder dialog box, browse for the folder to which you want to move the key, and then click OK..

Modifying the Device Naming Template Used During Registration

The device naming template determines how devices are named when they register. By default, a device hostname is used. You can change it to use any combination of the following machine variables: ${HostName}, ${GUID}, ${OS}, ${CPU}, ${DNS}, ${IPAddress}.

If the naming template causes conflicting device object names, another machine variable is automatically appended to make the second name unique. For example, if you are using the hostname for the name and you have two devices with the same hostname, the GUID is added to the hostname to create a unique name.

To modify the template:

1. In ZENworks Control Center, click the **Configuration** tab.
2. In the Management Zone Settings panel, click **Device Management**, then click **Registration** to display the Registration page.
3. In the Device Naming Template panel, click , then select the desired machine variable from the list.

   You can use any combination of one or more variables. For example:

   `${HostName}${GUID}`

NOTE: When you use `${IPAddress}` as device name, then IPv4 address will be used while renaming the device. If the device has only IPv6 address, then IPv6 address will be used as device name, but all ":" will be replaced with "_".

4 Click **OK** to save the changes.

Enabling Dynamic Renaming of Devices During Registration

The Device Dynamic Rename setting lets you enable devices to be renamed, if necessary, whenever they refresh their registration information. A device might need to be renamed for the following reasons:

- The naming template settings have changed. For example, the name template is now using both the Hostname and GUID variables rather than only the Hostname.
- A different naming template is now being applied to the device. For example, a folder naming template is now being applied rather than the Management Zone naming template.
- The device variable being used for the name changed. For example, the device hostname is being used for the name, and the device actual hostname changed.

Because a device GUID and not its name is used to establish relationships with other ZENworks objects (folders, groups, and so forth), renaming the device does not affect anything other than the name that is displayed in ZENworks Control Center.

By default, the Device Dynamic Rename setting is disabled. You can enable the setting at the Management Zone, in which case all devices inherit the setting, or you can enable it on a device folder, in which case only the devices in the folder inherit the setting.

- "Enabling the Setting at the Management Zone" on page 69
- "Enabling the Setting for a Device Folder" on page 69

Enabling the Setting at the Management Zone

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

2 In the Management Zone Settings panel, click **Device Management**, then click **Registration** to display the Registration page.

3 In the Device Dynamic Rename panel, click **Enable automatic renaming of devices**.

4 Click **OK** to save the changes.

Enabling the Setting for a Device Folder

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

2 Browse to find the device folder for which you want to change the setting, then click **Details** to display the folder details.

3 Click the **Settings** tab.

4 In the Settings panel, click **Device Management**, then click **Device Dynamic Rename** to display the Device Dynamic Rename page.

5 Click **Override settings** to activate the Device Dynamic Rename panel.

6 In the Device Dynamic Rename panel, click **Enable automatic renaming of devices**.

7 Click **OK** to save the changes.

Reconciling Devices with existing Device Objects During Registration

ZENworks enables you to create a device object in the zone prior to actually registering the device with the zone. This feature allows you to pre configure all the variables and other configurations for a given device prior to booting the device.

You can create dummy device objects and register them in the Management Zone by importing their information from a comma-separated value (CSV) file. This creates managed workstation device objects in the database. Later, when the Primary Agent is deployed to these devices, the ZENworks Reconcile settings (hostname, serial number, and MAC address) are used to reconcile the new Primary Agent to the device object that has already been registered in the database. This helps you to avoid the possibility of duplicates in the database during the registration of the devices in the Management Zone.

Review the following sections:

- "Creating Dummy Device Objects" on page 70
- "Reconciling the Devices" on page 72
- "Importing Managed Devices" on page 80

Creating Dummy Device Objects

You can create dummy device objects that are added to the ZENworks database in one of the following ways:

- "Manually Creating a Dummy Device Object" on page 70
- "Creating Dummy Device Objects by Using a CSV File" on page 71

Manually Creating a Dummy Device Object

1 Ensure that you have created registration keys as explained in "Creating a Registration Key" on page 61.

2 In ZENworks Control Center, click the **Devices** tab.

3 In the Devices Tasks panel, click **Add Device**.

The Add Device wizard is displayed.

4 On the Device Attributes and Registration Key page, provide the following information used to identify and register the device in the ZENworks database:

Registration Key: Select a registration key to use when registering the device. The key must already exist.

Host Name: Specify a hostname for the device. For example: workstation1.

The hostname appears as the first part of the DNS name (for example, workstation1.company.com. Because of DNS limitations, the maximum number of characters that can be used in the hostname is 63.

Serial Number: Specify the device serial number if you want to later reconcile a managed device with this dummy device object based on the serial number.

MAC Address: Specify the device MAC address if you want to later reconcile a managed device with this dummy device object based on the serial number. MAC address is a 12-digit alphanumeric string in which you can use a hyphen (-) or a colon (:) as separator. You can specify the MAC address in one of the following formats.

- *xxxxxxxxxx*
- *xx-xx-xx-xx-xx-xx*
- *xx:xx:xx:xx:xx:xx*

5 Review the information and, if necessary, use the **Back** button to make changes to the information. Click **Finish** to add the device.

A workstation device object with the hostname that you specified in Step 4 on page 70 is created in the ZENworks database and is registered in the Management Zone. To view the device object in ZENworks Control Center, click **Devices** > **Managed** > the **Workstations** folder.

Creating Dummy Device Objects by Using a CSV File

1 Using a text editor, create a CSV file with the following fields as an entry for each device objects:

- WS_1.0. This is the first field that must be specified for each entry. You must not change it.
- hostname
- serial number
- MAC address

Use the following format to list the devices in the file:

`WS_1.0,` *hostname of the device being registered or imported, serial number, MAC address*

The value for hostname is mandatory, and the values for serial number and MAC address are optional.

A sample CSV file is as follows:

```
WS_1.0,img-linux1,121456125622,000C298062A8
WS_1.0,img-linux2,121456125623,000C29935FF8
```

2 Log into ZENworks Control Center.

3 Click the **Devices** tab.

4 In the Device Tasks panel, click **Import Managed Devices**.

The Import Devices dialog box is displayed.

5 Specify or click to browse for and select a key to use when registering the device. The key must already exist.

To create a registration key in ZENworks Control Center, see "Creating Registration Keys and Rules" on page 60.

6 In the **File Path** option, browse for and select the CSV file that you created in Step 1.

7 Click **OK**.

The device entries listed in the CSV file are created as workstation device objects in the database and are registered in the Management Zone. To view the device objects in ZENworks Control Center, click **Devices** > **Managed** > the **Workstations** folder.

Reconciling the Devices

You can reconcile a new device that is being registered to an existing device object with its own bundles and policies. Reconciliation occurs only if the GUID of the new device that is getting registered does not match the GUID of the existing device object. Reconciliation does not occur with every refresh or registration call.

NOTE: By default, Serial Number and MAC Address are selected with differentiation enabled. If you have enabled the AllowNonActiveNIC registry key, then the device can be reconciled with the MAC address of the non-active adapters.

For more information on AllowNonActiveNIC, see ZENworks Registry Keys Reference.

Device Reconciliation Settings

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

2 In the Management Zone Settings panel, click **Device Management**, then click **Registration** to display the Registration page.

3 Indicate the device attributes that are used in reconciliation.

You can choose to reconcile the new devices with the existing device objects by using one or more of the following attributes:

- **Serial Number**
- **MAC Address**
- **Machine Name** (hostname)

3a **Enable Differentiation:**

- If differentiation is enabled, it uses **AND** logic, meaning that all the selected attributes must match for a device to reconcile.
- If differentiation is disabled, it uses **OR** logic, meaning that any one of the selected attributes must match for a device to reconcile.

Differentiation disabled: If multiple device objects with matching attributes (such as Mac address or hostname) are found, the device object with the matching serial number gets the first preference, even if none of the attributes are selected.

4 Click **Apply**.

By default, Serial Number and MAC Address are selected with differentiation enabled.

NOTE: For accurate reconciliation, we recommend that you select at least two attributes with differentiation enabled.

Sample Illustrations - Enable Differentiation and Reconciliation

Scenario 1

Serial Number and MAC Address are selected with differentiation enabled: For a device to reconcile to the existing device object, the Serial Number and MAC address of the existing device must match the Serial Number and MAC address of the new device.

Scenario 2

MAC Address and Machine Name selected with differentiation disabled: For a device to reconcile to the existing device object, the MAC Address or the Machine name of the existing device must match the MAC address or Machine name of the new device

Scenario 3

Serial Number and MAC Address selected with differentiation enabled and with device having multiple MAC addresses: The existing device object has multiple MAC addresses and the new device has multiple MAC addresses, which includes two new and one old. In this case, the new device object will still reconcile to the existing device object if any one of the MAC addresses and the Serial Number match the existing object.

Scenario 4

The new device and the existing device object have the same GUID but different passwords:

Devices getting registered with new passwords, but with same device GUID was less secure option where password of any device can be updated. In order to provide security, by default, the password update of a device with same device GUID is not allowed. If this setting is set to false, by default, then a -34 is sent back to the device, when a registration request is received with incorrect credentials. If the device registration is failed due to this reason, it can be fixed by running the zac reg -r command where administrator credentials are required.

The default settings are as follows:

- `authreconcile disableAuthfailure = false [true: in case if above behavior is not desired]`
- `enableReconcileignore = true [false: in case if configured reconcile settings are to be considered]`
- `disableClientID = true [false: in case if device GUID needs to be considered for reconciliation]`
- `createNewDevice = true [false: not to create new device object in case of  reconciliation failure]`

Devices getting registered with new passwords but with the same GUID is less secure. The option where the password of any device can be updated. To provide security, by default, the password update of a device with the same GUID is not allowed. This can be achieved by setting the disableAuthFailure flag to false.

In some scenarios, administrator credentials are required to update the password using the zac reg -r command.

NOTE: The `authreconcile.xml` file and it's settings that could be customized are considered only when there is a device which has the same GUID as the existing device object but with a different password.

The following table shows how different settings can help or fail device reconciliation:

	Serial number (SN)	Mac Address	Hostname	Expected
Differentiation Enabled	✓	✓	✓	**Success:** The attributes of the new device must match all attributes of the existing object for successful reconciliation. **Failure:** If there is no match with even a single attribute, reconciliation fails and a new device object is created.
	✗	✗	✗	The reconciliation settings are not set and thus, a new device object is created for every new device.
	✓	✓	✗	**Success:** The Serial Number, as well as MAC address of the new device, must match the Serial Number and MAC address of the existing device object. **Failure:** If only one of the two attributes match, then reconciliation of the new device with the existing object fails.
	✓	✗	✓	**Success:** The Serial Number, as well as the Hostname of the new device, must match the Serial Number and Hostname of the existing device object. **Failure:** If only one of these two attributes match, then reconciliation of the new device with the existing object fails.
	✗	✓	✓	**Success:** The MAC address, as well as Hostname of the new device, must match the MAC address and Hostname of the existing device object. **Failure:** If only one of these two attributes match, then reconciliation of the new device with the existing object fails.
	✓	✗	✗	**Success:** The Serial Number of the new device must match the Serial Number of the existing device object. **Failure:** If the Serial Number doesn't match, then reconciliation of the new device with the existing object fails.

	Serial number (SN)	Mac Address	Hostname	Expected
Differentiation Enabled	✗	✓	✗	**Success:** The MAC address of the new device must match the MAC address of the existing device object. **Failure:** If the MAC address doesn't match, then reconciliation with the existing object fails.
	✗	✗	✓	**Success:** The Hostname of the new device must match the Hostname of the existing device object. **Failure:** If the Hostname doesn't match, then reconciliation of the new device with the existing object fails.
	✗	✓ ***(multiple≥2)***	✓	**Success:** If a device consists of multiple MAC addresses, all of them are queried and stored with the reconciliation request. Any one of the multiple MAC addresses and the Hostname of the existing device must match with any one of the MAC addresses and the Hostname of the new device for successful reconciliation. **Failure:** If none of the MAC addresses match, reconciliation fails.
	✓	✓ ***(same≥2)***	✗	**Success:** If two or more devices have the same MAC addresses, then devices are distinguished by the Serial Number, and the device with the matching Serial Number is reconciled with the existing object.
	✓	✗	✓ ***(same≥2)***	If two or more devices have the same Hostname, then the devices are distinguished by the Serial Number. The new device with the matching Serial Number is reconciled with the existing object.

	Serial number (SN)	Mac Address	Hostname	Expected
Differentiation Disabled	✅	✅	✅	**Success:** New device attributes must match with either the attributes of the existing object for successful reconciliation. **Failure:** If none of the attributes match, reconciliation fails and a new device object is created.
	❌	❌	❌	If the settings for device reconciliation are not set, then a new device object is created for every new device. **NOTE:** If multiple device objects with matching attributes (such as MAC address or hostname) are found, the device object with the matching serial number gets the first preference, even if none of the attributes are selected.
	✅	✅	❌	**Success:** Either the Serial Number or the MAC address of the new device must match the Serial Number or the MAC address of the existing device object. **Failure:** If neither of these two attributes match, then reconciliation of the new device with the existing object fails.
	✅	❌	✅	**Success:** Either the Serial Number or the Hostname of the new device must match the Serial Number or the Hostname of the existing device object. **Failure:** If neither of these two match, then reconciliation of the new device with the existing object fails.

	Serial number (SN)	Mac Address	Hostname	Expected
Differentiation Disabled	✗	✓	✓	**Success:** Either the MAC address or the Hostname of the new device must match the MAC address or the Hostname of the existing device object. **Failure:** If neither of these two match, then reconciliation of the new device with the existing object fails.
	✓	✗	✗	**Success:** The Serial Number of the new device must match the Serial Number of the existing device object. **Failure:** If the Serial Number of the new device doesn't match, then reconciliation of the new device with the existing object fails.
	✗	✓	✗	**Success:** The MAC address of the new device must match the MAC address of the existing device object. **Failure:** If the MAC address of the new device doesn't match, then reconciliation of the new device with the existing object fails.
	✗	✗	✓	**Success:** The Hostname of the new device must match the Hostname of the existing device object. **Failure:** If the Hostname of the new device doesn't match, then reconciliation of the new device with the existing object fails.

IMPORTANT: For better management of VDI devices in the management zone use registration keys or rules, since reconciliation settings are included as part of Registration Keys and Rules from ZENworks 11 SP4 release onwards.

In VDI environment, if you are using Citrix XenDesktop 7.x or VMware view 5.2 (the recompose of Desktop pools) onwards, you must set the reconcile settings to Machine Name with Enable Differentiation.

Undoing /Resetting Device Reconciliation Settings

The changes in reconciliation settings will not reset or un-reconcile the device, because reconciliation is triggered only when a new device GUID is found.

To undo device reconciliation, do the following on the device after selecting the appropriate settings in ZENworks Control Center:

1. Unregister the device by using the `zac unr` command.
2. Clear the Workstation GUID by using the `zac fsg –d` command.
3. Run the following commands:
   - 3a **On Windows:** Open the command prompt as an administrator, go to `%ZENworks_Home%\bin\preboot` folder, then run the `ZISWIN.exe -w` command to clear Image-safe Data.
   - 3b **On Linux:** Run the commands `export LD_LIBRARY_PATH=/opt/novell/zenworks/preboot/lib:${LD_LIBRARY_PATH}` and `/opt/novell/zenworks/preboot/bin/novell-zislnxd clearISD`.
4. Clear the cache by using the `zac cc` command.
5. Register the agent `zac reg <server url>`.

Importing Managed Devices

You can use the Import Devices dialog box to register one or more devices in the Management Zone by importing the information from a comma-separated value (CSV) file. Before importing the managed device, ensure that the registry keys have been created. Also ensure that there are limited and unlimited usage registration keys. You are allowed to execute the Import Managed Devices action regardless of whether you have registration rights or not, if you select an unlimited usage registration key.

1. In ZENworks Control Center, click the **Devices** tab.
2. In the Device Tasks panel, click **Import Managed Devices** to display the Import Devices dialog box.
3. Click to browse for and select a key in the Registration Key dialog box.

   The key must already exist. For more information on creating registration keys, see Section 9.2.1, “Creating a Registration Key,” on page 66.
4. Click **OK**.
5. In the **File Path** option, browse for and select the CSV file that you created earlier. For more information see “Creating Dummy Device Objects by Using a CSV File” on page 71.
6. Click **OK.**

Choose an unlimited usage registration key to execute **Import Managed Devices** action, even when you do not have registration rights.

If you choose a limited registration key and if you do not have registration rights, the following error message is displayed:

```
Unable to proceed as you do not have sufficient rights on /~keys~. Contact
your ZENworks Administrator.
```

Disabling the Use of Registration Rules

By default, the registration rules feature is enabled. This ensures that devices that register without a registration key are at least added to the correct folder, which is the `/servers` or `/workstations` folder, depending on the device type.

If you want to rely completely on registration keys, you can disable registration rules. You have two options when you disable registration rules:

- **Disable the default registration rules only:** Any device that attempts to register without a registration key or that does not meet the criteria in a custom registration rule is rejected. The default registration rules are ignored.
- **Disable all registration rules:** Any device that attempts to register without a registration key is rejected.

To disable registration rules:

1. In ZENworks Control Center, click the **Configuration** tab.
2. In the Management Zone Settings panel, click **Device Management**, then click **Registration** to display the Registration page.
3. In the Registration Rules panel, deselect one of the following options:

   Enable Use of Device Management Registration Rules: Disable this option to force devices to use a registration key when registering. Any devices that attempt to register without a key are rejected.

   Enable Use of Device Management default Registration Rules: Disable this option to force devices to use a registration key or meet the criteria defined in a custom registration rule. Any devices that do not are rejected.

   Disable Use of Registration Keys sent by Managed Devices: Enable this option if you want the registration keys sent by the managed device to be considered by the server only when the device is being registered for the first time.

   During registration, if you configure the `SendRegKeyOnEveryRefresh` registry key on the agent, after every refresh, the agent will send the registration key in the `initial-web-service` file, and the group membership will be updated after every refresh. For more information, see the *ZENworks Registry Keys Reference*.

   The following table provides information about the behavior of this feature in various scenarios:

ZENworks Control Center Setting - Disable Use of Registration Keys sent by Managed Devices	Agent-side Registry Key - SendRegKeyOnEveryRefresh	Behavior
Enabled	Enabled	The group membership will be updated only when the device is registered for the first time.
Enabled	Disabled	The group membership will be updated only when the device is registered for the first time.
Disabled	Enabled	The group membership will be updated during a network connect or disconnect, when the device is registered for the first time, when the zac `add-reg-key` command is executed. and on every refresh.
Disabled	Disabled	The group membership will be updated during a network connect or disconnect, the first time the device is registered, when the zac `add-reg-key` command is executed.

4 Click **OK** to save the changes.

Adding Pre-approved Devices

From ZENworks 2020 Update 2 onwards, you can add the devices to the pre-approved devices list. The pre-approved devices are approved by the administrators to be part of the zone. You can pre-approve devices while bulk registering a known set of devices. It can also be used to allow known devices to reconcile if required. The Pre-Approved Enrollment feature lets you import devices, even before the enrollment is completed. This feature can be used only when you enable the enhanced security feature. For more information on enabling the security feature, see Security Commands in the ZENworks Command Line Utilities Reference.

Assume that a managed device or an inventory-only device (IOA agents) that was previously registered to the zone using the authorization key gets deleted or unregistered from the Management Zone. The next time, if the device must register back to the zone without having the hassle of using or entering the authorization key again, then the devices should be added to the pre-approved devices list. Including the devices in the pre-approved list with specific device details help devices to register back to the zone.

The pre-approved devices can be added manually, imported using a CSV file or using device action (Add to pre-approved devices).

- "Adding the Pre-approved Devices Manually" on page 83
- "Importing Pre-approved Devices from CSV File" on page 83

- "Adding the Pre-approved Devices using Action" on page 84
- "Adding the Pre-approved Devices while Deleting Devices" on page 84

Adding the Pre-approved Devices Manually

If you have obtained a list of devices through your OEM vendor, then you can manually add the pre-approved devices by perform the following steps:

1. In ZCC, click Devices > Discovered
2. Click Pre-approved Devices.
3. In the Pre-approved devices page, click Add.
4. Specify the following information, and then click Next:
   - Serial Number
   - Mac Address
   - DNS Name
   - Product Name
   - Manufacturer
   - Asset Tag Number
   - Device Type
   - Expiry Date
5. In the Device Match Setting page, select the attributes that will be used to uniquely identify a device. At least one attribute should be selected. If multiple attributes are selected, then the attributes are matched in the following order:
   - Serial Number
   - MAC Address
   - DNS Name

     If required, you can click override, and based on requirements, you can modify the settings.
6. Click Finish.

Importing Pre-approved Devices from CSV File

To import the pre-approved devices using a CSV file, perform the following steps:

1. In ZCC, click Devices.
2. In the Devices Tasks panel, click Import Pre-approved Devices.
3. Click Browse and select a CSV file that includes details of the devices that you want to import as pre-approved devices, and then click Next.
4. Click Add, in the pop-up select the field, associate column name in the CSV file, and then click OK.

   Ensure that you at least associate the Device Type field, and the MAC address, Serial Number, or DNS Name field.

   After associating all the fields, click Ok.

If required, you can click Verify to check for the associated fields.

5. Click Finish.

The imported devices will be displayed in the Pre-approved Devices page.

IMPORTANT: You can also import devices to the pre-approved devices list using the zman discovered-import-preapproved-devices command. For more information on the command, see the ZENworks Command Line Utilities Reference.

Adding the Pre-approved Devices using Action

To add the already registered devices to the per-approved devices list, perform the following steps:

1. In ZCC, click Devices.
2. Click Servers or Workstations.
3. Select the required devices, and then click Action > Add to pre-approved devices.

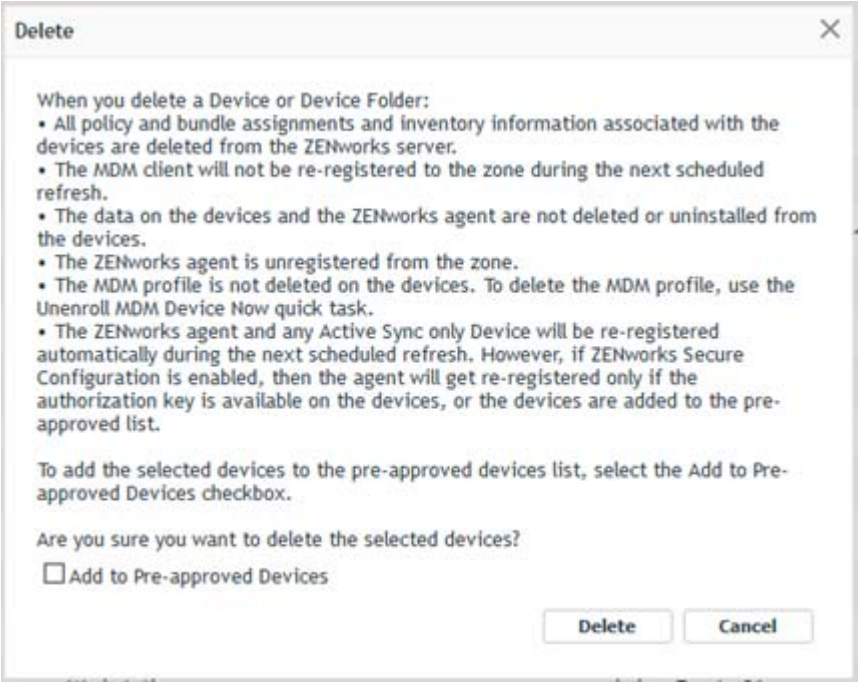
NOTE: If device already exists in the pre-approved devices list, expiry of the device is changed to the default expiry date (2 days), if existing expiry is less than default expiry date or device was already expired.

Adding the Pre-approved Devices while Deleting Devices

In ZENworks, the devices that are already managed (registered to the zone) can be added to the Pre-approved devices list while deleting from the zone. The managed device can either be a server or a workstation.

To delete a Server or Workstation, perform the following:

1. In ZCC, click Devices > Workstations / Servers.
2. In the Workstations page, select the required devices.
3. Click Delete.
4. After clicking Delete, a pop-up is displayed as shown in the below image:



5. To add devices to the pre-approved devices, select the Add to Pre-approved Devices check box.
6. Click Delete.

Manually Registering a Device

A device is automatically registered when the ZENworks Agent is installed. You should only need to manually register a device in the following situations:

- The device was unregistered.
- The device object was deleted from the ZENworks database. The ZENworks Agent is still installed on the device and you now want to register the device again.
- You want to reregister an already registered device with an additional registration key.

Manual registration of a device must be done at the device using the ZENworks Agent command line utility (zac).

The following sections provide instructions:

- "Performing an Initial Registration" on page 85
- "Reregistering a Device with an Additional Registration Key" on page 86

Performing an Initial Registration

1 At the device, open a command prompt.

2 Enter the following command:

```
zac reg [-a <authorization key>][-k key] [-u ZENworks Administrator
username -p ZENworks Administrator password] [server_url:port]
```

For example:

```
zac reg -k acct -u zadmin -p novell https://zserver.novell.com
```

The `-k`, `-u`, and `-p` parameters are optional. If you do not use the `-u` and `-p` parameters, you are prompted to enter a username and password. For the `server_url:port` parameter, you can also use an IP address; the port is required only if the ZENworks Server is not using the default port (443).

If you have enabled the Security setting on a ZENworks server to which the devices will be registered, then you need to use the Authorization key to register the device.

NOTE: ◆The `-g` and `-k` options are meant only for the initial registration of a device. On subsequent registration requests, `-g` and `-k` options will not be honored because of the reconciliation of the device with an existing device object.

- When you modify or update the GUID using the -g option, then audit and messages generated with the old GUID will be lost.

Reregistering a Device with an Additional Registration Key

1. At the device, open a command prompt.
2. Enter the following command:

   ```
   zac add-reg-key registration_key
   ```

   For example:

   ```
   zac add-reg-key acct
   ```

   Registration keys are additive. If you register with more than one key, the device receives all group memberships associated with each registration key.

Unregistering a Device

A device is automatically unregistered when the ZENworks Agent is uninstalled. You can manually unregister a device if necessary.

Unregistering a device by using zac

Unregistration of a device can be done at the device using ZENworks Agent command line utility (zac):

1. At the device, open a command prompt.
2. Enter the following command:

   ```
   zac unr [-f] [-u ZENworks Administrator username -p ZENworks
   Administrator password]
   ```

   For example:

```
zac unr -u zadmin -p novell
```

The `-f`, `-u`, and `-p` parameters are optional. If you do not use the `-u` and `-p` parameters, you are prompted to enter a username and password. The `-f` parameter ignores the ZENworks database and forces the device to be unregistered locally; this option is only necessary if the device object has already been deleted from the ZENworks database or if the device cannot connect to the database.

Unregistering a device by using the Unregister Device action

To manually unregister a device, do the following:

1. Log in to ZENworks Control Center.
2. Click **Devices** > **Managed**.
3. Select either **Servers** or **Workstations** as the type of the device, then select the devices you want to unregister from the Management zone.

   You will not be able to reregister the unregistered device through ZCC. However, you can use the `zac reg` command to reregister the device.
4. Click **Action** > **Unregister Device**.

11 Deploying the ZENworks Agent

Devices that you want to manage through ZENworks must have the ZENworks Agent deployed to them. The ZENworks Agent performs all ZENworks management tasks on the managed device.

For detailed information about the supported platforms and system requirements for a managed device, see “Managed Device Requirements” in the *ZENworks System Requirements*.

There are several ways to deploy the agent. The following sections provide instructions:

- “Coexisting with the ZENworks Desktop Management Agent” on page 89
- “Customizing the Agent Features” on page 90
- “Configuring the Agent Security” on page 92
- “Changing the Target Installation Directory” on page 93
- “Using a Task to Deploy the Agent” on page 94
- “Manually Deploying the Agent on Windows” on page 119
- “Reboot-less Agent” on page 121
- “Manually Deploying the Agent on Linux” on page 122
- “Manually Deploying the Agent on a Macintosh Device” on page 123
- “Agent Deployment in VDI environment” on page 127
- “Upgrading the Agent in a Citrix VDI Environment” on page 129
- “Agent Deployment on Citrix Server” on page 129
- “Package Options for Windows, Linux, and Macintosh” on page 129
- “Installing the Agent as an Add-on Product in SLES/SLED” on page 131
- “Installing the Agent by Using YUM on RHEL” on page 132

Coexisting with the ZENworks Desktop Management Agent

This section applies only if you want to deploy the ZENworks Agent to devices that have the traditional ZENworks Desktop Agent installed. The traditional ZENworks Desktop Agent is included with ZENworks 7 Desktop Management.

The ZENworks Agent and the traditional ZENworks Desktop Agent can coexist on the same device, but only to support the use of ZENworks Asset Management or ZENworks Patch Management with traditional ZENworks Desktop Management. ZENworks Configuration Management cannot be used on the same device as traditional ZENworks Desktop Management.

When Configuration Management is activated in your Management Zone, either through a full license or an evaluation license, the following ZENworks Agent features are available for installation:

- Bundle Management

- Image Management
- Policy Management
- Remote Management
- User Management

The *Bundle Management*, *Image Management*, and *User Management* features overlap with the ZENworks Desktop Management features. Therefore, when you deploy the ZENworks Agent to a device that has the traditional ZENworks Desktop Agent installed, if you install any of these three feature modules (Bundle, Image, or User Management), the ZENworks Agent removes the ZENworks Desktop Agent before installing the features.

During deployment, the pre-agent is installed first. It then contacts the ZENworks Management Zone to identify which ZENworks Agent features should be installed. If the Bundle Management, Image, Management, or User Management features are selected to be installed, the pre-agent uninstalls the ZENworks Desktop Agent before installing the features. If the pre-agent is unable to contact the server, it stops installation of the ZENworks Agent and does not uninstall the traditional ZENworks Desktop Agent.

Customizing the Agent Features

The ZENworks Agent is used with the following ZENworks products: Asset Management, Configuration Management, Endpoint Security, Full Disk Encryption, and Patch Management.

To provide support for each of these products, the agent utilizes feature modules. Each feature module provides functionality for one or more products, as shown in the following table:

Product	Feature Modules
Asset Management	◆ Asset Management ◆ User Management
Configuration Management	◆ Bundle Management ◆ Image Management ◆ Policy Management ◆ Remote Management ◆ User Management
Endpoint Security Management	◆ Endpoint Security Management ◆ User Management
Full Disk Encryption	◆ Full Disk Encryption
Patch Management	◆ Patch Management

By default, the ZENworks Agent is configured to be installed with the feature modules associated with the products that are active (either full or evaluation license) in the Management Zone. For example, if Configuration Management and Endpoint Security Management are both active, the Bundle Management, Image Management, Policy Management, Remote Management, User Management, and Endpoint Security Management feature modules are installed and enabled by default.

Each feature module can be installed or uninstalled. If it is installed, it can either be enabled or disabled. The following sections explain how to customize the feature modules both before the ZENworks Agent is deployed and after:

- "Customizing Features before Deployment" on page 91
- "Customizing Features after Deployment" on page 91

Customizing Features before Deployment

The ZENworks Agent is deployed with the feature modules that are enabled in the ZENworks Agent settings in the Management Zone Settings. If you do not want to deploy the agent with the default feature modules installed and enabled, you should customize the features before performing any of the following tasks:

- Creating and starting a new deployment task
- Starting an existing deployment task
- Downloading or deploying the agent manually

To customize which feature modules are installed and enabled:

1. In ZENworks Control Center, click the **Configuration** tab.
2. In the Management Zone Settings panel, click **Device Management**, then click **ZENworks Agent**.
3. In the Agent Features panel:
   - If you do not want to install a feature, deselect **Installed** next to a feature. The selected feature is not installed on the device. If you choose to deselect all the features, then only the core agent is installed.
   - If you want to install but disable a feature, select **Installed** and **Disabled** next to a feature.The disabled feature is not uninstalled from the currently managed devices. The feature is installed on the device, but it is nonfunctional.
4. To save the changes, click **OK**.

   The installation of Bundle Management, Remote Management, or User Management features requires a reboot of your device. The installation of Image Management feature requires a reboot only on Windows 2008, Windows Vista, Windows 7, and Windows 10. The user is prompted to reboot the device based on the selected reboot option.

Customizing Features after Deployment

The ZENworks Agent is deployed with the security settings selected at the Management Zone level. After deploying the agent to a device, you can do any of the, following:

- Change the security settings configured at the Management Zone level
- Override the Management Zone settings at the device folder or device level

The new settings are applied to the agent on a device refresh.

For more information on how to override and configure the settings for an existing agent, see "Configuring ZENworks Agent Settings after Deployment"in the *ZENworks Agent Reference*.

Configuring the Agent Security

You can configure whether or not to allow users to uninstall the ZENworks Agent. In addition, you can require a password for the uninstall, define an override password to provide access to restricted administrative features in the agent, and enable self-defense to protect agent files from being removed.

The following sections explain how to configure the security settings both before the ZENworks Agent is deployed and after:

- "Customizing Security before Deployment" on page 92
- "Customizing Security after Deployment" on page 93

Customizing Security before Deployment

1. In ZENworks Control Center, click the **Configuration** tab.
2. In the Management Zone Settings panel, click **Device Management**, then click **ZENworks Agent**.
3. In the Agent Security panel:
   - **Allow Users to Uninstall the ZENworks Agent:** Enable this option to allow users to perform a local uninstall of the ZENworks Agent. If this option is disabled, the agent can only be uninstalled through the ZENworks Control Center.

   The following settings apply only to the ZENworks 11 SP2 and newer versions of the ZENworks Agent. For older versions of the agent, use the Security Settings policy (one of the Windows Endpoint Security policies) to configure these settings.

   - **Require an Uninstall Password for the ZENworks Agent:** Enable this option to require users to enter a password in order to uninstall the ZENworks Agent. Click **Change** to set the password.

     To avoid distributing the uninstall password to users, we recommend that you use the Password Key Generator utility to generate a key for the uninstall password. The key, which is based on the uninstall password, functions the same as the uninstall password but can be tied to a single device or user so that its use is limited.

     You access the Password Key Generator utility in the **Configuration Tasks** list in the left navigation pane.
   - **Enable an Override Password for the ZENworks Agent:** An override password can be used in the ZENworks Agent to:
     - Access information about the device current location and how the location was assigned.
     - Access the Administrative options in the Endpoint Security Agent. These options let you disable the currently applied security policies (with the exception of the Data Encryption policy), view detailed policy information, and view agent status information.
     - Access the Administrative options in the Full Disk Encryption Agent. These options let you view detailed policy information, view agent status information, and perform functions such as
     - Uninstall the ZENworks Agent.

To enable an override password, select the check box, then click **Change** to set the password.

To avoid distributing the override password to users, we recommend that you use the Password Key Generator utility to generate a key for the override password. The key, which is based on the override password, functions the same as the override password but can be tied to a single device or user and can have a usage or time limit.

You access the Password Key Generator utility in the **Configuration Tasks** list in the left navigation pane

- **Enable Self Defense for the ZENworks Agent** Currently, self-defense functionality protects only the ZENworks Endpoint Security Agent. It does not protect the other ZENworks Agent modules.

  Self defense protects the Endpoint Security Agent from being shut down, disabled, or tampered with in any way. If a user performs any of the following activities, the device is automatically rebooted to restore the correct system configuration:

  - Using Windows Task Manager to terminate any Endpoint Security Agent processes.
  - Stopping or pausing any Endpoint Security Agent services.
  - Removing critical files and registry entries. If a change is made to any registry keys or values associated with the Endpoint Security Agent, the registry keys or values are immediately reset.
  - Disabling NDIS filter driver binding to adapters.

  Select the check box to enable self defense.

4 To save the changes, click **OK**.

Customizing Security after Deployment

The ZENworks Agent is deployed with the features selected at the Management Zone level. After deploying the agent to a device, you can do any of the, following:

- Change the agent settings configured at the Management Zone level
- Override the Management Zone settings at the device folder or device level

The new settings are applied to the agent on a device refresh.

For more information on how to override and configure the settings for an existing agent, see "Configuring ZENworks Agent Settings after Deployment"in the *ZENworks Agent Reference*.

Changing the Target Installation Directory

On Windows

By default, the ZENworks Agent is installed to the following locations:

- **On a Windows 32-bit device:** `Windows_drive:\Program Files\Novell\ZENworks`
- **On a Windows 64-bit device:** `Windows_drive:\Program Files(x86)\Novell\ZENworks`

To install the agent to a different location, you can create a ZENWORKS_HOME system environment variable on the device prior to deployment and set the variable to the new target installation directory. Some examples of acceptable paths are:

```
c:\
```

```
c:\Program Files\Corporate\
```

```
d:\Applications\Novell\ZENworks
```

On Linux

You cannot change the target installation directory.

Using a Task to Deploy the Agent

The ZENworks Server can deploy the ZENworks Agent to devices. This requires that you create a task, called a deployment task, for the ZENworks Server. The task identifies the target devices, the credentials required to perform an installation on the devices, the registration key to use (optional), the date and time to perform the installation, and other tasks you want performed on the devices either before or after the installation.

This form of deployment is only supported on Windows and Linux devices.

The steps for creating a deployment task vary slightly depending on whether or not the target devices are already listed as discovered devices in your Management Zone (see Part I, "Device Discovery," on page 9):

- "Prerequisites for Deploying to Windows Devices" on page 94
- "Prerequisites for Deploying to Linux Devices" on page 98
- "Deploying to a Discovered Device" on page 99
- "Deploying to a Non-Discovered Device" on page 109

Prerequisites for Deploying to Windows Devices

Before the ZENworks Server can deploy the ZENworks Agent to a device, make sure the following prerequisites are satisfied:

- "Enabling File and Printer Sharing for Microsoft Networks" on page 94
- "Enabling File and Printer Sharing through Windows Firewall" on page 95
- "Enabling Classic File Sharing" on page 97

In addition to these requirements, ensure that the date and time are correct on both the ZENworks Server and on managed devices.

Enabling File and Printer Sharing for Microsoft Networks

You need to enable the **File and Printer Sharing for Microsoft Networks** option to allow other computers on a network to access resources on your computer by using a Microsoft network.

Windows XP

1 Right-click **My Network Places** > **Properties**.

   The Networks Connections window is displayed.

2 Right-click **Local Area Connection** > **Properties**.

   The Local Area Connection Properties dialog box is displayed.

3 In the **General** tab, ensure that the **File and Printer Sharing for Microsoft Networks** option is selected.

4 Click **OK**.

For more information, see File and Printer Sharing for Microsoft Networks (http://technet.microsoft.com/en-us/library/cc779133.aspx).

Windows Server 2008

1 Right-click **Network** > **Properties**.

   The Network and Sharing Center window is displayed.

2 In the left pane, click **Manage network connections**.

3 Right-click **Local Area Connection** > **Properties**.

   The Local Area Connection Properties dialog box is displayed.

4 In the **Networking** tab, ensure that the **File and Printer Sharing for Microsoft Networks** option is selected.

5 Click **OK**.

Windows 7, Windows 8, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2

1 Right-click **Network** > **Properties**.

   The Network and Sharing Center window is displayed.

2 Right-click **Local Area Connection** > **Properties**.

   The Local Area Connection Properties dialog box is displayed.

3 In the **Networking** tab, ensure that the **File and Printer Sharing for Microsoft Networks** option is selected.

4 Click **OK**.

Enabling File and Printer Sharing through Windows Firewall

Any target device that is using Windows Firewall needs to be configured to allow file and printer sharing through the firewall. This is done by enabling the **File and Printer Sharing** exception in the Windows Firewall configuration settings. You can access Windows Firewall through the Control Panel or through the Windows Security Center.

By default, the scope of the exception applies only to a local subnet. If the target device is in a different subnet than the Primary Server from which the deployment is run, you must add the IP address of the Primary Server to the Windows Firewall along with the local subnet.

Windows Server 2008

1. From the desktop **Start** menu, click **Settings** > **Control Panel**.
2. Double-click **Windows Firewall**.

   The Windows Firewall window is displayed.
3. Click the **Exceptions** tab.
4. In the **Programs and Services** list, select **File and Printer Sharing**, then click **Edit**.

   The Edit a Service window is displayed.
5. Click **Change Scope** to include the IP address of the Primary Server and the local subnet.
6. Click **OK**.

Windows 7, Windows 8, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2

1. From the desktop **Start** menu, click **Settings** > **Control Panel**.
2. Double-click **Windows Firewall**.

   The Windows Firewall window is displayed.
3. In the left pane, click **Allow a program or feature through Windows Firewall**.
4. In the **Allowed Programs and Features** list, select **File and Printer Sharing**.
5. Click **OK**.

Windows 10

1. From the desktop **Start** menu, click **Settings** > **Control Panel**.
2. Double-click **Windows Firewall**.

   The Windows Firewall window is displayed.
3. In the left pane, click **Allow a program or feature through Windows Firewall**.
4. In the **Allowed Programs and Features** list, select **File and Printer Sharing**.
5. Enable **Windows Management Instrumentation** (WMI).
6. Click **OK**.

Windows XP

You can allow WMI through Windows firewall.

1. At the command prompt, run the following command:

   ```
   netsh firewall set service RemoteAdmin enable
   ```

   For more information on WMI, see Connecting Through Windows Firewall (http://msdn.microsoft.com/en-us/library/aa389286%28v=VS.85%29.aspx).

Enabling Classic File Sharing

The ZENworks Server needs classic file sharing access to the administrative share (displayed as Admin$) on target devices.

- "Windows XP" on page 97
- "Windows Server 2008" on page 97
- "Windows 7, Windows 8, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2" on page 97
- "Windows 10" on page 98

To know in detail about the ports that are opened when you enable Classic File sharing, see IP Discovery Technologies.

Windows XP

Windows XP uses simple file sharing by default. You need to disable simple file sharing to enable classic file sharing.

1. On the Windows XP device, right-click the **My Computer** icon, then click **Open**.
2. Click the **Tools** menu > **Folder Options** to display the Folder Options dialog box.
3. Click the **View** tab.
4. In the **Advanced Settings** list, deselect the **Use simple file sharing** option, then click **OK** to save the change.

Disabling this option changes the setting for the **Network access: Sharing and security model for local accounts** option in the Local Security Policy (**Local Policies** > **Security Options**) to **Classic - local users authenticate as themselves**. You can also use a Windows Group Policy to change the setting.

Windows Server 2008

1. Open the Windows Registry and access the following:

   `HKLM/Software/Microsoft/Windows/CurrentVersion/Policies/System/LocalAccountTokenFilterPolicy`

   If the registry key does not exist, you need to create it.
2. Change its DWORD (32-bit) value to 1.

   This allows remote users to log in and not be forced to be guest.
3. Close the registry to save the change.
4. Open the Services window and set the Remote Registry service to start automatically, then start it.
5. Click the desktop **Start** menu > **Settings** > **Control Panel**.
6. Double-click **Network and Sharing Center**.
7. Select **Turn on File Sharing**, then click **Apply**.

Windows 7, Windows 8, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2

1. Open the Windows Registry and access the following:

`HKLM/Software/Microsoft/Windows/CurrentVersion/Policies/System/LocalAccountTokenFilterPolicy`

If the registry key does not exist, you need to create it.

2 Change its DWORD (32-bit) value to 1.

This allows remote users to log in and not be forced to be guest.

3 Close the registry to save the change.

4 Open the Services window and set the Remote Registry service to start automatically, then start it.

5 Click the desktop **Start** menu > **Settings** > **Control Panel**.

6 Double-click **Network and Sharing Center**.

7 In the left pane, click **Change advanced sharing settings**.

8 Select **Turn on file and printer sharing**, then click **Save Changes**.

Windows 10

1 Open the Windows Registry and access the following:

`HKLM/Software/Microsoft/Windows/CurrentVersion/Policies/System/LocalAccountTokenFilterPolicy`

If the registry key does not exist, you need to create it.

2 Change its DWORD (32-bit) value to 1.

This allows remote users to log in and not be forced to be guest.

3 Close the registry to save the change.

4 Open the Services window and set the Remote Registry service to start automatically, then start it.

5 Click the desktop **Start** menu > **Settings** > **Control Panel**.

6 Double-click **Network and Internet > Network and Sharing Center**.

7 In the left pane, click **Change advanced sharing settings**.

8 Select **Turn on file and printer sharing**, then click **Save Changes**.

Prerequisites for Deploying to Linux Devices

Before the ZENworks Server can deploy the ZENworks Agent to a Linux device, make sure that SSH Port 22 is open. To open SSH port 22 use the following procedures to add SSH as an allowed service on the target device.

To add SSH as an allowed service on Red Hat Enterprise Linux (RHEL):

1 Edit `vi/etc/sysconfig/iptables` to append the following rule:

```
-A RH-Firewall-1-INPUT -m state –state NEW -m tcp -p tcp –dport 22 -j ACCEPT
```

2 Save the iptables file.

3 Restart the ip tables service by running either the service iptables restart command or the `/etc/init.d/iptables` restart command.

To add SSH as an allowed service on Red Hat Enterprise Linux (RHEL) 7.6 and later:

1 Add SSH port 22 by executing the following command:

```
firewall-cmd --permanent --zone=public --add-port=22/tcp
```

or

Add the service SSH to the firewall config by executing the following command:

```
firewall-cmd --permanent --zone=public --add-service=ssh
```

2 Restart the firewall service by running the following command:

```
systemctl restart firewalld.service
```

IMPORTANT: For Linux devices ensure that you copy the `ZENworks11-gpg-pubkey.asc` key on to the device and execute the `import rpm --import ZENworks11-gpg-pubkey.asc` command to avoid errors. The `ZENworks11-gpg-pubkey.asc` is key is available in the `ZENworks 2020 iso`.

To add SSH as an allowed service on SUSE Linux Enterprise Server (SLES) and SUSE Linux Enterprise Desktop (SLED) 11 and 12:

1 Edit the following file:

```
/etc/sysconfig/SuSEfirewall2
```

2 Add SSH to the list of ports under `FW_SERVICES_<Firewall Zone>_TCP`.

For example, for an external zone, add SSH under `FW_SERVICES_EXT_TCP="ssh"`.

3 Run the following command:

```
/sbin/SuSEfirewall2.
```

To add SSH as an allowed service on SUSE Linux Enterprise Server (SLES) and SUSE Linux Enterprise Desktop (SLED) 15 and OpenSUSE 15:

1 Add the service SSH to firewall config by executing the following command:

```
/usr/bin/firewall-cmd --permanent --zone=public --add-service=ssh
```

2 Restart the firewall service by running:

```
systemctl restart firewalld.service
```

Deploying to a Discovered Device

This section assumes that you have already performed a discovery task to add the target devices to your ZENworks database. If you have not, you can perform the discovery task before continuing (see Part I, “Device Discovery,” on page 9) or you can perform the discovery as part of the deployment task (see “Deploying to a Non-Discovered Device” on page 109).

To deploy the ZENworks Agent to a discovered device:

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

The Deployable Device panel lists all the devices (imported or discovered) to which you can deploy the ZENworks Agent.

2 In the Deployment Tasks panel, click **New** to launch the Deploy Device Wizard.

3 Complete the wizard by using information from the following table to fill in the fields.

Wizard Page	Details
Enter Deployment Task page	Specify a name for the task. The name cannot include any of the following invalid characters: / \ * ? : " ' < > | ` % ~
Select Devices page	Allows you to identify the devices to which you want to deploy the ZENworks Agent. Click **Add** to display the Discovered Device Browser dialog box. You can deploy to the target devices by using one of the following options: ◆ DNS Name ◆ IP Address If you select **IP Address** and if the target device is not reachable by using the IP address, the deployment uses the DNS name. If you select **DNS Name** and if the target device is not reachable by using the DNS name, the deployment uses the IP address. If the deployment uses a proxy, the target device is only connected by using the option provided.
Discovered Device Browser dialog box > **Source** > **IP Address**	1. In the **Source** list, select **IP Address**. 2. Fill in the **IP Address Range/Host Name** field. The address can use any of the following formats: xxx.xxx.xxx.xxx: Standard dotted-decimal notation for a single address. For example, 123.45.167.100. xxx.xxx.xxx.xxx - xxx.xxx.xxx.xxx: Standard dotted-decimal notation for a range of addresses. For example, 123.45.167.100 - 123.45.167.125. xxx.xxx.xxx.xxx/n: Standard CIDR (Classless Inter-Domain Routing) notation. For example, 123.45.167.100/24 matches all IP addresses that start with 123.45.167. hostname: Standard device hostname. For example, workstation1. 3. To add the device to the **Selected Devices** list, click **Add**. 4. When you are finished selecting devices, click **OK**.

Wizard Page	Details
Discovered Device Browser dialog box > **Source** > **Add New CSV File**	1. In the **Source** list, select **Add New CSV File** to display the Add New Source dialog box. 2. Fill in the following fields: **CSV File:** Browse for and select the CSV file containing the devices to which you want to deploy the agent. **DNS Name Column:** Select the number of the column that contains the DNS name information. **IP Address Column:** Select the number of the column that contains the IP address information. If you want the IP address to be resolved from the DNS name rather than imported from the file, select the **Resolve IP from DNS name** option. **OS Type Column:** Select the number of the column that contains the operating system information. If you want to specify a default OS type rather than importing it from the file, select the **Use default OS for all selections** option, then select the default operating system in the **Default OS Type** field. 3. Click OK to display the devices in the source list. 4. Click ➡ to move a device to the **Selected Devices** list. 5. When you are finished selecting devices, click **OK**.
Discovered Device Browser dialog box > **Source** > existing user source	1. In the **Source** list, select the existing user source. The root of the user source is displayed in the source list. 2. Browse the directory to find the desired device. 3. Click ➡ to move the device to the **Selected Devices** list. 4. When you are finished selecting devices, click **OK**.

Wizard Page	Details
Discovered Device Browser dialog box > **Source** > **Add New LDAP Source**	1. In the **Source** list, select **Add New LDAP Source** to display the Add New Source dialog box. 2. Fill in the following fields: **LDAP Source Name:** Provide a name for the LDAP source. **LDAP Server:** Specify the IP address or DNS hostname of the LDAP server. **LDAP Port/Use SSL:** Defaults to the standard SSL port (636) or non-SSL port (389) depending on whether the **Use SSL** option is enabled or disabled. If your LDAP server is listening on a different port, select that port. **LDAP Root Context:** Establishes the point in the directory where you can begin to browse. If you do not specify a base DN, the directory root container becomes the entry point. **Save Credentials to Data store:** Unless you save the credentials (defined in the **Credentials** list), they are stored only in memory. Saved credentials are encrypted in the database for increased security. Credentials are cleared from memory when the ZENworks Server is restarted. If you want to permanently retain the credentials as part of the deployment task, you should save the credentials. **Credentials:** Click Add to enter a username and password that provides read-only access to the directory. The user can have more than read-only access, but read-only access is all that is required and recommended. For Novell eDirectory access, use standard LDAP notation. For example: cn=admin_read_only,ou=users,o=mycompany For Microsoft Active Directory, use standard domain notation. For example: AdminReadOnly@mycompany.com 3. Click **OK** to display the LDAP directory in the source list. 4. Browse the directory to find the desired device. 5. Click ➡ to move the device to the **Selected Devices** list. 6. When you are finished selecting devices, click **OK**.
Enter Credentials page > **Save Credentials to DataStore** field	The Enter Credentials page lets you provide the usernames and passwords required to deploy the ZENworks Agent to the devices included in the task. Unless you save the credentials, they are stored only in memory. Saved credentials are encrypted in the database for increased security. Credentials that are not saved are cleared from memory when the ZENworks Server is restarted. If you are creating a scheduled deployment task, you should save the credentials to ensure that they are still available when the deployment is performed.

Wizard Page	Details
Enter Credentials page > **Credentials** field	To add a credential on Windows: 1. Click **Add** to display the Enter Credential Information dialog box. 2. In the **Type** list, select the type of operating system for which you want to enter the credential. 3. In the **Username** field, specify the appropriate username. To deploy the agent, the ZENworks Server must be able to map a drive to the device administrative share (ADMIN$). This requires the following credentials: ◆ **If the device is a member of a domain:** You can use a domain or local Administrator group credential. If you use the local credential, you must specify the username as `workstation_name\username` to distinguish it from domain credentials. ◆ **If the device is not a member of a domain:** You must use a local Administrator group credential. 4. In the **Password** and **Reenter Password** fields, enter the user password. 5. Click **OK** to save the credential. Depending on your environment, one credential might not provide access to all of the devices where you want to deploy the ZENworks Agent. In this case, you need to add as many credentials as necessary to cover the devices included in the task. The ZENworks Server uses the first credential that works. Specify only the root credential to deploy the ZENworks Agent on Linux.
Select Schedule page	The Select Schedule page lets you choose whether you want the task to run as soon as it is created (the **Now** option) or if you want to schedule the task to run at a future date and time. If you select **Scheduled**, choose one of the following schedules: **No Schedule:** Indicates that no schedule has been set. The task does not run until a schedule is set or it is manually launched. This is useful if you want to create the task and come back to it later to establish the schedule or run it manually. **Date Specific:** Specifies one or more dates on which to run the task. **Recurring:** Identifies specific days each week, month, or a fixed interval on which to run the task. See Appendix B, "Schedules," on page 161 or click the **Help** button for more information about the schedules.
Select Primary Server page > *Primary Server* field	Select the ZENworks Server that you want to perform the deployment task.

Wizard Page	Details
Select or Edit a Proxy Device page	The Select or Edit a Proxy Device page lets you choose whether you want to use a proxy device to perform the deployment task.
Select or Edit a Proxy Device page > **Windows Proxy**	If you want to use a Windows Proxy instead of the Primary Server to perform the deployment tasks on Windows devices, click the **Windows Proxy** option and configure the settings in the Select Windows Proxy dialog box. A Windows Proxy is used to perform the following actions: ◆ Enable Linux Primary Servers to perform deployment tasks on Windows devices. ◆ Deploy Windows devices that are in a different subnet than the Primary Server. ◆ Deploy Windows devices in a network enabled for NAT. The connection between the ZENworks Server and the Windows Proxy is secured through SSL. For deployment, you need to add File and Printer Sharing as an exception in the Windows Firewall configuration settings. By default, the scope of the exception applies only to a local subnet. If the target device is in a different subnet than the Primary Server from which the deployment is run, you also need to add the IP address of the Primary Server as an exception. However, if you use a Windows Proxy in the same subnet as a target device, you do not need to change the scope of the Windows Firewall exception. **Override Zone Windows Proxy Settings:** Select this option if you want to override the Windows Proxy settings configured at the Management Zone and configure new settings for the task. **Windows Proxy:** Select a Windows managed device (server or workstation) to be used as a Windows Proxy for performing the deployment tasks instead of a ZENworks Server. The Windows Proxy must reside in the same network as the target devices. **Windows Proxy Timeout:** Specify the number of seconds you want the ZENworks Server to wait for a response from the Windows Proxy.

Wizard Page	Details
Select or Edit a Proxy Device page > **Linux Proxy**	If you want to use a Linux Proxy instead of the Primary Server to perform the deployment tasks on Linux devices, click the **Linux Proxy** option and configure the settings in the Select Linux Proxy dialog box. A Linux Proxy is used to perform the following actions: ◆ Enable Primary Servers to offload a deployment task to a Linux Proxy if the task includes devices in a different subnet. ◆ Deploy Linux devices in a different subnet than the Primary Server. ◆ Deploy Linux devices in a network enabled for NAT. The SSH discovery requires port 22 to be reachable in order to enable the Primary Server to connect to the target device. If the SSH port is blocked in the Network Firewall, you use a Linux managed device in the same subnet as the target device. **Override Zone Linux Proxy Settings:** Select this option if you want to override the Linux Proxy settings configured at the Management Zone and configure new settings for the task. **Linux Proxy:** Select a Linux managed device (server or workstation) to be used as a Linux Proxy for performing the deployment tasks instead of a ZENworks Server. The Linux Proxy must reside in the same network as the target devices. **Linux Proxy Timeout:** Specify the number of seconds you want the ZENworks Server to wait for a response from the Linux Proxy.

Wizard Page	Details
Windows Options page > **Reboot Option** field	After installation of the ZENworks Agent, a device must reboot to make the agent functional. Do the following: 1. Select the desired reboot option. ◆ **Immediate:** To reboot immediately after installation of the ZENworks Agent, select **Immediate** to force the device ◆ **Manual:** To allow the user to manually reboot the device at his or her convenience, select **Manual**. ◆ **Scheduled:** To reboot the device at a specified time, select **Scheduled**. Fill in the schedule fields. ◆ **Start Date:** Click to display a calender you can use to select a date for the event. ◆ **Start Time:** Specify the time at which the event must start. ◆ **Use Coordinated Universal Time (UTC):** The Start Time is converted to Universal Coordinated Time (UTC). Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you do not select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours. 2. (Optional) Select the **Do Not Prompt for Reboot** option if you do not want the reboot prompt message to be displayed. ◆ **Start ZENworks Agent with limited functionality:** (Optional) This is enabled only if you select **Manual** reboot option. Select this option to start ZENworks Agent with limited functionality and without rebooting a device. **IMPORTANT:** If you select **Immediate** or **Manual** reboot option, and **Do not prompt for reboot** option, then **Cancel** the reboot after agent install, a prompt is displayed to start the ZENworks agent with limited functionality. If user selects **Yes**, the agent service starts with limited functionality until a reboot is done. **NOTE:** The Windows Options page is displayed only if you have provided Windows credentials on the Enter Credentials page.

Wizard Page	Details
Windows Options page > **Permission Prompt Options** fields	After deployment, you can use these options to postpone the agent installation on the target machine: ◆ **Show Permission Prompt:** Select **On** to display a dialog box on the agent when the installation is ready to begin. Users can cancel, postpone, or allow the installation to begin based on the Permission Prompt options configured by the Zone administrator. **NOTE:** By default, this setting is set to **Off**, so users cannot cancel or postpone the installation. The installation begins immediately without any prompt. If you select On, the following options are enabled: ◆ **Prompt Max Postpone:** Specify how many times a user can postpone or snooze the installation. Select **Unlimited** to let the user postpone the installation an unlimited number of times, or select **Limit To**, then specify the number of times the user can postpone the installation. ◆ **Prompt Timeout:** Specify how long to wait for an answer before the installation begins. To display the permission prompt until the user responds, select **No Timeout**. Or, select **Timeout after _ mins** and specify the number of minutes you want an unanswered prompt to remain on the user's screen before the installation starts. By default, the user has five minutes to respond to the prompt. ◆ **Prompt Nag Time:** Specify, in minutes, how often the prompt should appear to let a user know that an installation is waiting to start. By default, this prompt displays every 15 minutes. ◆ **Prompt Max Wait Time:** Specify the maximum timeout for which the agent installation can be postponed. When this timeout is reached, the agent installation starts even if there are other prompt messages remaining. ◆ **Agent Message Overrides:** Customize the text for agent installation messages that display in dialog boxes during the installation. Click **Add** to display the Edit Agent Installation Message dialog box. Select a Message Key from the drop-down list, type the desired text, then click **OK**.
Windows Options page > **Deployment Package** field	Depending upon the processor architecture of the managed device, select the deployment package to be used for installing ZENworks Agent on the device. If you are not sure about the device's processor architecture, choose the package with target architecture as **All**, which applies to 32-bit and 64-bit platforms. If the selected package has been deleted from the Primary Server, then the default deployment package is deployed.

Wizard Page	Details
Windows Options page > **Agent Installation Folder** field	Specify the directory on the managed device where you want to install ZENworks Agent. By default, the agent is installed to the directory specified in the *%ZENWORKS_HOME%* system environmental variable or to the `%ProgramFiles%\novell\zenworks` directory if the variable is not set on the managed device. Ensure that the installation path does not contain spaces. **NOTE:** If the directory you specify cannot be created, then the agent is installed in the default location.
Linux Options page	The Linux Options page lets you configure the installation options to make the ZENworks Agent functional after the installation of the agent on the Linux devices. **Deployment Package:** Depending upon the processor architecture of the managed device, select the deployment package to be used for installing ZENworks Agent on the device. If you are not sure about the device's processor architecture, choose the package with target architecture as All, which applies to 32-bit and 64-bit platforms. If the selected package has been deleted from the Primary Server, then the default deployment package is deployed. **Installation Options:** Configure the following options for deploying the ZENworks Agent: ◆ **Do Not Install the GUI Packages:** Select this option if you do not want to install the RPMs that provide a GUI interface for the ZENworks Agent such as the icon. ◆ **Disable SELinux for Red Hat Devices:** Select this option to disable SELinux (Security-Enhanced Linux). SELinux provides limited access control on Linux. Select this option to disable SELinux if the agent is unable to open the ports required by ZENworks. SELinux is temporarily disabled only if the agent is unable to open the ports, and is automatically enabled again after the agent installation. **NOTE:** The Linux Options page is displayed only if you have provided Linux credentials on the Enter Credentials page.
Add Registration Key page	Select a registration key to use during the registration portion of the deployment process. A registration key provides information about the folders and groups to which a device is assigned during registration. Selecting a registration key is optional; if you do not select one, registration rules are used to determine the folder and group assignments. To deploy to servers or workstations, choose a server registration key or a workstation registration key respectively. For more information about registration keys and rules, see Chapter 10, “Registering Devices,” on page 59.

Wizard Page	Details
Pre/Post Deployment page	Specify commands that you want to run before and after the agent is installed on a device. For example, you can execute operating system commands, run scripts, and launch executables. The commands are passed to the pre-agent as part of the deployment task package. The pre-agent executes the commands in the system space, so you must specify commands that do not require user interaction. For more information about predeployment and post-deployment commands, click the **Help** button.

When you finish the wizard, the deployment task is added to the list in the Deployment Tasks panel. You can use the panel to manage current tasks and create new tasks for deploying the ZENworks Agent to devices. The panel includes the following information for each task:

- **Name:** Displays the name given to the task. If **Credentials Cleared** is displayed below the task name, the credentials required to perform the task on the targeted devices have been cleared from the ZENworks Server memory and must be entered again. To avoid having credentials lost when they are cleared from memory, you must store them in the ZENworks database.
- **Schedule:** Displays the dates on which the task is scheduled to run.
- **Status:** Displays the following status information: **Scheduled**, **Pending**, **Installing**, **Registering**, **Inactive**, **Finished**, or **Error**. You can mouse over certain statuses to receive more information about the status.

  If an error occurred, the error is also recorded for the target device in the Deployable Devices panel. You can click the target device in the Deployable Devices panel to receive more information about the error.

Deploying to a Non-Discovered Device

If a target device has not been added to your ZENworks database through a discovery task, you can select the device while you are creating the deployment task. The following sections explain how to create the deployment task depending on whether you want to identify the target device by its IP address/hostname, from a CSV file, or from an LDAP directory.

1. In ZENworks Control Center, click the **Deployment** tab.
2. In the Deployment Tasks panel, click **New** to launch the Deploy Device Wizard.
3. Complete the wizard by using information from the following table to fill in the fields.

Wizard Page	Details
Enter Deployment Task page	Specify a name for the task. The name cannot include any of the following invalid characters: / \ * ? : " ' < > | ` % ~

Wizard Page	Details
Select Devices page	Allows you to identify the devices to which you want to deploy the ZENworks Agent. Click **Add** to display the Discovered Device Browser dialog box. You can deploy to the target devices by using one of the following options: ◆ DNS Name ◆ IP Address If you select **IP Address** and if the target device is not reachable by using the IP address, the deployment uses the DNS name. If you select **DNS Name** and if the target device is not reachable by using the DNS name, the deployment uses the IP address. If the deployment uses a proxy, the target device is only connected by using the option provided.
Discovered Device Browser dialog box > **Source** > **IP Address**	1. In the **Source** list, select **IP Address**. 2. Fill in the **IP Address Range/Host Name** field. The address can use any of the following formats: xxx.xxx.xxx.xxx: Standard dotted-decimal notation for a single address. For example, 123.45.167.100. xxx.xxx.xxx.xxx - xxx.xxx.xxx.xxx: Standard dotted-decimal notation for a range of addresses. For example, 123.45.167.100 - 123.45.167.125. xxx.xxx.xxx.xxx/n: Standard CIDR (Classless Inter-Domain Routing) notation. For example, 123.45.167.100/24 matches all IP addresses that start with 123.45.167. hostname: Standard device hostname. For example, workstation1. 3. To add the device to the **Selected Devices** list, click **Add**. 4. When you are finished selecting devices, click **OK**.

Wizard Page	Details
Discovered Device Browser dialog box > **Source** > **Add New CSV File**	1. In the **Source** list, select **Add New CSV File** to display the Add New Source dialog box. 2. Fill in the following fields: **CSV File:** Browse for and select the CSV file containing the devices to which you want to deploy the agent. **DNS Name Column:** Select the number of the column that contains the DNS name information. **IP Address Column:** Select the number of the column that contains the IP address information. If you want the IP address to be resolved from the DNS name rather than imported from the file, select the **Resolve IP from DNS name** option. **OS Type Column:** Select the number of the column that contains the operating system information. If you want to specify a default OS type rather than importing it from the file, select the **Use default OS for all selections** option, then select the default operating system in the **Default OS Type** field. 3. Click OK to display the devices in the source list. 4. Click ➡ to move a device to the **Selected Devices** list. 5. When you are finished selecting devices, click **OK**.
Discovered Device Browser dialog box > **Source** > existing user source	1. In the **Source** list, select the existing user source. The root of the user source is displayed in the source list. 2. Browse the directory to find the desired device. 3. Click ➡ to move the device to the **Selected Devices** list. 4. When you are finished selecting devices, click **OK**.

Wizard Page	Details
Discovered Device Browser dialog box > **Source** > **Add New LDAP Source**	1. In the **Source** list, select **Add New LDAP Source** to display the Add New Source dialog box. 2. Fill in the following fields: **LDAP Source Name:** Provide a name for the LDAP source. **LDAP Server:** Specify the IP address or DNS hostname of the LDAP server. **LDAP Port/Use SSL:** Defaults to the standard SSL port (636) or non-SSL port (389) depending on whether the **Use SSL** option is enabled or disabled. If your LDAP server is listening on a different port, select that port. **LDAP Root Context:** Establishes the point in the directory where you can begin to browse. If you do not specify a base DN, the directory root container becomes the entry point. **Save Credentials to Datastore:** Unless you save the credentials (defined in the **Credentials** list), they are stored only in memory. Saved credentials are encrypted in the database for increased security. Credentials are cleared from memory when the ZENworks Server is restarted. If you want to permanently retain the credentials as part of the deployment task, you should save the credentials. **Credentials:** Click Add to enter a username and password that provides read-only access to the directory. The user can have more than read-only access, but read-only access is all that is required and recommended. For Novell eDirectory access, use standard LDAP notation. For example: cn=admin_read_only,ou=users,o=mycompany For Microsoft Active Directory, use standard domain notation. For example: AdminReadOnly@mycompany.com 3. Click **OK** to display the LDAP directory in the source list. 4. Browse the directory to find the desired device. 5. Click ➡ to move the device to the **Selected Devices** list. 6. When you are finished selecting devices, click **OK**.
Enter Credentials page > **Save Credentials to DataStore** field	The Enter Credentials page lets you provide the usernames and passwords required to deploy the ZENworks Agent to the devices included in the task. Unless you save the credentials, they are stored only in memory. Saved credentials are encrypted in the database for increased security. Credentials that are not saved are cleared from memory when the ZENworks Server is restarted. If you are creating a scheduled deployment task, you should save the credentials to ensure that they are still available when the deployment is performed.

Wizard Page	Details
Enter Credentials page > **Credentials** field	To add a credential: 1. Click **Add** to display the Enter Credential Information dialog box. 2. In the **Type** list, select the type of operating system for which you want to enter the credential. 3. In the **Username** field, specify the appropriate username. To deploy the agent, the ZENworks Server must be able to map a drive to the device administrative share (ADMIN$). This requires the following credentials: ◆ **If the device is a member of a domain:** You can use a domain or local Administrator group credential. If you use the local credential, you must specify the username as `workstation_name\username` to distinguish it from domain credentials. ◆ **If the device is not a member of a domain:** You must use a local Administrator group credential. 4. In the **Password** and **Reenter Password** fields, enter the user password. 5. Click **OK** to save the credential. Depending on your environment, one credential might not provide access to all of the devices where you want to deploy the ZENworks Agent. In this case, you need to add as many credentials as necessary to cover the devices included in the task. The ZENworks Server uses the first credential that works.
Select Schedule page	The Select Schedule page lets you choose whether you want the task to run as soon as it is created (the **Now** option) or if you want to schedule the task to run at a future date and time. If you select **Scheduled**, choose one of the following schedules: **No Schedule:** Indicates that no schedule has been set. The task does not run until a schedule is set or it is manually launched. This is useful if you want to create the task and come back to it later to establish the schedule or run it manually. **Date Specific:** Specifies one or more dates on which to run the task. **Recurring:** Identifies specific days each week, month, or a fixed interval on which to run the task. See Appendix B, "Schedules," on page 161 or click the **Help** button for more information about the schedules.
Select Primary Server page > *Primary Server* field	Select the ZENworks Server that you want to perform the deployment task.
Select or Edit a Proxy Device page	The Select or Edit a Proxy Device page lets you choose whether you want to use a proxy device to perform the deployment task.

Wizard Page	Details
Select or Edit a Proxy Device page > **Windows Proxy**	If you want to use a Windows Proxy instead of the Primary Server to perform the deployment tasks on Windows devices, click the **Windows Proxy** option and configure the settings in the Select Windows Proxy dialog box. A Windows Proxy is used to perform the following actions: ◆ Enable Linux Primary Servers to perform deployment tasks on Windows devices. ◆ Deploy Windows devices that are in a different subnet than the Primary Server. ◆ Deploy Windows devices in a network enabled for NAT. The connection between the ZENworks Server and Windows Proxy is secured through SSL. For deployment, you need to add File and Printer Sharing as an exception in the Windows Firewall configuration settings. By default, the scope of the exception applies only to a local subnet. If the target device is in a different subnet than the Primary Server from which the deployment is run, you also need to add the IP address of the Primary Server as an exception. However, if you use a Windows Proxy in the same subnet as a target device, you do not need to change the scope of the Windows Firewall exception. **Override Zone Windows Proxy Settings:** Select this option if you want to override the Windows Proxy settings configured at the Management Zone and configure new settings for the task. **Windows Proxy:** Select a Windows managed device (server or workstation) to be used as a Windows Proxy for performing the deployment tasks instead of a ZENworks Server. The Windows Proxy must reside in the same network as the target devices. **Windows Proxy Timeout:** Specify the number of seconds you want the ZENworks Server to wait for a response from the Windows Proxy.

Wizard Page	Details
Select or Edit a Proxy Device page > **Linux Proxy**	If you want to use a Linux Proxy instead of the Primary Server to perform the deployment tasks on Linux devices, click the **Linux Proxy** option and configure the settings in the Select Linux Proxy dialog box. 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. The SSH discovery requires port 22 to be reachable in order to enable the Primary Server to connect to the target device. If the SSH port is blocked in the Network Firewall, you use a Linux managed device in the same subnet as the target device. **Override Zone Linux Proxy Settings:** Select this option if you want to override the Linux Proxy settings configured at the Management Zone and configure new settings for the task. **Linux Proxy:** Select a Linux managed device (server or workstation) to be used as a Linux Proxy for performing the deployment tasks instead of a ZENworks Server. The Linux Proxy must reside in the same network as the target devices. **Linux Proxy Timeout:** Specify the number of seconds you want the ZENworks Server to wait for a response from the Linux Proxy.

Wizard Page	Details
Windows Options page > **Reboot Option** field	After installation of the ZENworks Agent, a device must reboot to make the agent functional. Do the following: 1. Select the desired reboot option. ◆ **Immediate:** To reboot immediately after installation of the ZENworks Agent, select **Immediate** to force the device ◆ **Manual:** To allow the user to manually reboot the device at his or her convenience, select **Manual**. ◆ **Scheduled:** To reboot the device at a specified time, select **Scheduled**. Fill in the schedule fields. ◆ **Start Date:** Click to display a calender you can use to select a date for the event. ◆ **Start Time:** Specify the time at which the event must start. ◆ **Use Coordinated Universal Time (UTC):** The Start Time is converted to Universal Coordinated Time (UTC). Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you do not select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours. 2. (Optional) Select the **Do Not Prompt for Reboot** option if you do not want the reboot prompt message to be displayed. ◆ **Start ZENworks Agent with limited functionality:** (Optional) This is enabled only if you select **Manual** reboot option. Select this option to start ZENworks Agent with limited functionality and without rebooting a device. **IMPORTANT:** If you select **Immediate** or **Manual** reboot option, and **Do not prompt for reboot** option, then **Cancel** the reboot after agent install, a prompt is displayed to start the ZENworks agent with limited functionality. If user selects **Yes**, the agent service starts with limited functionality until a reboot is done. **NOTE:** The Windows Options page is displayed only if you have provided Windows credentials on the Enter Credentials page.

Wizard Page	Details
Windows Options page > **Permission Prompt Options** fields	After deployment, you can use these options to postpone the agent installation on the target machine: ◆ **Show Permission Prompt:** Select **On** to display a dialog box on the agent when the installation is ready to begin. Users can cancel, postpone, or allow the installation to begin based on the Permission Prompt options configured by the Zone administrator. **NOTE:** By default, this setting is set to **Off**, so users cannot cancel or postpone the installation. The installation begins immediately without any prompt. If you select On, the following options are enabled: ◆ **Prompt Max Postpone:** Specify how many times a user can postpone or snooze the installation. Select **Unlimited** to let the user postpone the installation an unlimited number of times, or select **Limit To**, then specify the number of times the user can postpone the installation. ◆ **Prompt Timeout:** Specify how long to wait for an answer before the installation begins. To display the permission prompt until the user responds, select **No Timeout**. Or, select **Timeout after _ mins** and specify the number of minutes you want an unanswered prompt to remain on the user's screen before the installation starts. By default, the user has five minutes to respond to the prompt. ◆ **Prompt Nag Time:** Specify, in minutes, how often the prompt should appear to let a user know that an installation is waiting to start. By default, this prompt displays every 15 minutes. ◆ **Prompt Max Wait Time:** Specify the maximum timeout for which the agent installation can be postponed. When this timeout is reached, the agent installation starts even if there are other prompt messages remaining. ◆ **Agent Message Overrides:** Customize the text for agent installation messages that display in dialog boxes during the installation. Click **Add** to display the Edit Agent Installation Message dialog box. Select a Message Key from the drop-down list, type the desired text, then click **OK**.
Windows Options page > **Deployment Package** field	Depending upon the processor architecture of the managed device, select the deployment package to be used for installing ZENworks Agent on the device. If you are not sure about the device's processor architecture, choose the package with target architecture as **All**, which applies to 32-bit and 64-bit platforms. If the selected package has been deleted from the Primary Server, then the default deployment package is deployed.

Wizard Page	Details
Windows Options page > **Agent Installation Folder** field	Specify the directory on the managed device where you want to install ZENworks Agent. By default, the agent is installed to the directory specified in the *%ZENWORKS_HOME%* system environmental variable or to the `%ProgramFiles%\novell\zenworks` directory if the variable is not set on the managed device. Ensure that the installation path does not contain spaces. **NOTE:** If the directory you specify cannot be created, then the agent is installed in the default location.
Linux Options page	The Linux Options page lets you configure the installation options to make the ZENworks Agent functional after the installation of the agent on the Linux devices. **Deployment Package:** Depending upon the processor architecture of the managed device, select the deployment package to be used for installing ZENworks Agent on the device. If you are not sure about the device's processor architecture, choose the package with target architecture as All, which applies to 32-bit and 64-bit platforms. If the selected package has been deleted from the Primary Server, then the default deployment package is deployed. **Installation Options:** Configure the following options for deploying the ZENworks Agent: ◆ **Do Not Install the GUI Packages:** Select this option if you do not want to install the RPMs that provide a GUI interface for the ZENworks Agent such as the icon. ◆ **Disable SELinux for Red Hat Devices:** Select this option to disable SELinux (Security-Enhanced Linux). SELinux provides limited access control on Linux. Select this option to disable SELinux if the agent is unable to open the ports required by ZENworks. SELinux is temporarily disabled only if the agent is unable to open the ports, and is automatically enabled again after the agent installation. **NOTE:** The Linux Options page is displayed only if you have provided Linux credentials on the Enter Credentials page.
Add Registration Key page	Select a registration key to use during the registration portion of the deployment process. A registration key provides information about the folders and groups to which a device is assigned during registration. Selecting a registration key is optional; if you do not select one, registration rules are used to determine the folder and group assignments. To deploy to servers or workstations, choose a server registration key or a workstation registration key respectively. For more information about registration keys and rules, see Chapter 10, “Registering Devices,” on page 59.

Wizard Page	Details
Pre/Post Deployment page	Specify commands that you want to run before and after the agent is installed on a device. For example, you can execute operating system commands, run scripts, and launch executables. The commands are passed to the pre-agent as part of the deployment task package. The pre-agent executes the commands in the system space, so you must specify commands that do not require user interaction. For more information about predeployment and post-deployment commands, click the **Help** button.

When you finish the wizard, the deployment task is added to the list in the Deployment Tasks panel. You can use the panel to manage current tasks and create new tasks for deploying the ZENworks Agent to devices. The panel includes the following information for each task:

- **Name:** Displays the name given to the task. If **Credentials Cleared** is displayed below the task name, the credentials required to perform the task on the targeted devices have been cleared from the ZENworks Server memory and must be entered again. To avoid having credentials lost when they are cleared from memory, you must store them in the ZENworks database.
- **Schedule:** Displays the dates on which the task is scheduled to run.
- **Status:** Displays the following status information: **Scheduled**, **Pending**, **Installing**, **Registering**, **Inactive**, **Finished**, or **Error**. You can mouse over certain statuses to receive more information about the status.

  If an error occurred, the error is also recorded for the target device in the Deployable Devices panel. You can click the target device in the Deployable Devices panel to receive more information about the error.

Manually Deploying the Agent on Windows

IMPORTANT: To support legacy Windows devices as mentioned below, weak cipher suites are used to communicate between Servers and Managed Devices and these ciphers might be added into the server configuration. To use strong ciphers, use a newer version of Windows in the zone.

Following are the legacy Windows devices:

- Windows 7 SP1
- Windows Embedded 7 SP1
- Windows Server 2008 SP2
- Windows Server 2008 R2
- Windows 2008 R2 SP1
- Windows 2012
- Windows 2012 R2 Server

NOTE: From ZENworks 23.4 onwards, agent installation and agent update are not supported on Windows 7.

Rather than having a ZENworks Server deliver the ZENworks Agent to a device, you can manually download the ZENworks Agent deployment package from the server and install the agent.

1. Make sure the device meets the necessary requirements. For details see "Managed Device Requirements" in the *ZENworks System Requirements*.
2. On the target device, open a Web browser to the following address:

   https://*server*:*port*/zenworks-setup

   Replace *server* with the DNS name or IP address of a ZENworks Server and replace the *port* only if the ZENworks Server is not using the default port (443).

   The Web browser displays a list of deployment packages. For each architecture (32-bit and 64-bit), there are three types of packages:

   - **Network:** Contains the `web-installer.exe` and configuration file, which downloads the ZENworks Agent files from a ZENworks Server and installs the agent on the device.
   - **Standalone:** Contains the pre-agent, all the ZENworks Agent module files, and the Microsoft .NET 4.8 installables. The ZENworks Agent is installed to the device, but no registration or management occurs until the device connects to the network.
   - **Web:** The `web-installer.exe` will install the ZENworks Agent. The web installer does not include any zone specific information and is signed by Micro Focus to prevent the antivirus from blocking the install as potential malware.

     NOTE: The web installer automatically connects to the following URLs:

     - `zenserver.<agent machine's domain name>`
     - `zenworks.<agent machine's domain name>`
     - `zen.<agent machine's domain name>`

     For example, If an agent device is on the `microfocus.com` domain, the auto connect URLs wil be:

     - `zenserver.microfocus.com`
     - `zenworks.microfocus.com`
     - `zen.microfocus.com`

     If the above mentioned URLs are not available for the web installer to connect, then you will be prompted to enter the server details.

   Custom: The package name, Default Agent, refers to the predefined deployment packages. The custom deployment packages created through **Deployment** > **Edit Deployment Package** are shown with the name given during the creation of the package.
3. Click the required deployment package you want to use, then save the package to the local drive of the device or run it from the ZENworks Server.
4. If you downloaded the package, launch the package on the device.

   For information about the options you can use with the package, see Package Options for Windows, Linux, and Macintosh (page 129).

IMPORTANT: If you choose to install a complete package, the installation of Windows Installer or .NET Framework might require a reboot after you launch the package. If you did not select a reboot option during agent deployment, a message is displayed showing various options on the reboot. Select one of the following options:

- Do nothing. Auto-reboot will occur after 5 minutes.
- Click **Cancel**. You will need to reboot later.
- Click **OK** to reboot immediately.

When the device reboots, the installation automatically resumes.

If you selected the **Manual** and the **Do not prompt for reboot** option during the agent installation, and if .NET or Windows Installer requires a reboot, then you need to manually reboot the device to resume the agent installation.

5 Upon completion of the installation, the device reboots automatically if you have already rebooted the device while installing Windows Installer or .NET Framework.

When the device reboots, it is registered in the Management Zone and the ZENworks icon is placed in the notification area (system tray).

In ZENworks Control Center, the device appears in the `\Servers` folder or `\Workstation` folder on the Devices page.

Reboot-less Agent

When ZENworks Agent is installed or an existing managed device is updated to ZENworks 2020, the administrator can select an option not to reboot the device after completing the installation. Additionally, the administrator can select to start the Microfocus ZENworks Adaptive Agent services on the managed device. If the services are selected to be started without a reboot, the ZENworks Agent works with limited functionality until a reboot is performed by user.

The following does not work without Reboot:

- **Agent Fresh Install:** ZENworks Endpoint Security Management (ZESM) and ZENworks Full Disk Encryption (ZFDE) policies including the locations will not be functional until a reboot is performed. Alternatively location lite can be used to detect locations on the managed devices with out reboot.

  Dynamic Local User (with and without Novell Client) and Roaming profile policies are not effective on Windows XP devices.
- **Agent System Update:** New ZESM and FDE Policies and Newly assigned locations does not work, while the previous policies assigned works. After agent is updated it goes to the last known location, which was detected by the agent before the update started. It stays at this location until the device is rebooted.
- **Start ZENworks Services:** This option starts ZENworks services in case reboot is suppressed while deploying the update to the device. It is not applicable for Primary Servers.
- ZENworks Explorer Configuration Policy (ZECP) with "`Name of the root folder`" setting will not be effective.

Manually Deploying the Agent on Linux

Instead of having a ZENworks Server deliver the ZENworks Agent to a device, you can manually download the ZENworks Agent deployment package from the server and install the agent.

1. Make sure the device meets the necessary requirements. For details, see "Managed Device Requirements" in the *ZENworks System Requirements*.
2. Before deploying the agent, ensure that you install all the dependent RPMs on the device. For more information, see RPMs for the Linux ZENworks Agent in the ZENworks Agent Reference .
3. On the target device, open a Web browser and access the following address:

   https://*server*:*port*/zenworks-setup

   Replace *server* with the DNS name or IP address of a ZENworks Server and replace the *port* only if the ZENworks Server is not using the default port (443).

   The Web browser displays a list of deployment packages. For each architecture (32-bit and 64-bit), there are two types of packages:

   Network: The network package installs only the pre-agent on the target device; the pre-agent then downloads and installs the ZENworks Agent from the ZENworks Server. The network package requires that JRE is installed on the device prior to the deployment of the agent on the device.

   NOTE: It is required to install only Sun's Java Runtime Environment (JRE)on the Linux managed devices for the ZENworks Agent to work.

   Standalone: The standalone package installs the pre-agent and extracts all executable files required for ZENworks Agent installation, including the JRE installer on the target device. The pre-agent then installs the ZENworks Agent from the local device. The standalone package is useful when you need to install the ZENworks Agent on a device that is currently disconnected from the network. You can save the package to removable media (CD, USB flash drive, and so on) and have the standalone device run the package from the media. The ZENworks Agent is installed on the device, but no registration or management occurs until the device connects to the network.

   Custom: The package name, Default Agent, refers to predefined deployment packages. The custom deployment packages created through **Deployment** > **Edit Deployment Package** are shown with the name assigned during the creation of the package.
4. At the command prompt, specify executable permissions to the downloaded `.bin` file by running the `chmod +x <file_name>` command.

   For more information on the options that you can use with the package, see "Package Options for Windows, Linux, and Macintosh" on page 129.
5. Click the required deployment package you want to use, save the package to the local drive of the device, then assign executable permissions to the file by running the command `chmod 755 filename`.

   For information on the options that you can use with the package, see "Package Options for Windows, Linux, and Macintosh" on page 129.
6. (Optional) On a RHEL device, run the following command:

   ```
   chcon -u system_u -t rpm_exec_t filename
   ```

7 In the terminal window, go to the directory where you have downloaded the package, then launch the package on the device by running the command `./filename`, where **filename** is the name of the package you downloaded in Step 5.

NOTE: A root user has to run the agent installer.

---

8 (Conditional) If you want to view the ZENworks notify icon in the notification area after agent installation for the Linux device, log out of and log in to the device.

In ZENworks Control Center, the device appears in the `\Servers` folder or `\Workstation` folder on the Devices page.

NOTE: ◆After deploying the ZENworks Agent on Linux device, `/opt/novell/zenworks/bin` is not added to the PATH variable and hence the commands in that directory cannot be used directly. Do any of the following on the Linux device to run the commands from `/opt/novell/zenworks/bin`:

— Relogin to the device.

— Specify the complete path to access the command.

For example: `/opt/novell/zenworks/bin/zac`.

◆ To configure RHEL devices as Servers or workstations, set the RHEL System Role on the device as required. If no role is configured, then by default, ZENworks recognize devices as Workstations.

Manually Deploying the Agent on a Macintosh Device

You can deploy the ZENworks Agent to a Macintosh device by downloading the agent installer from the server.

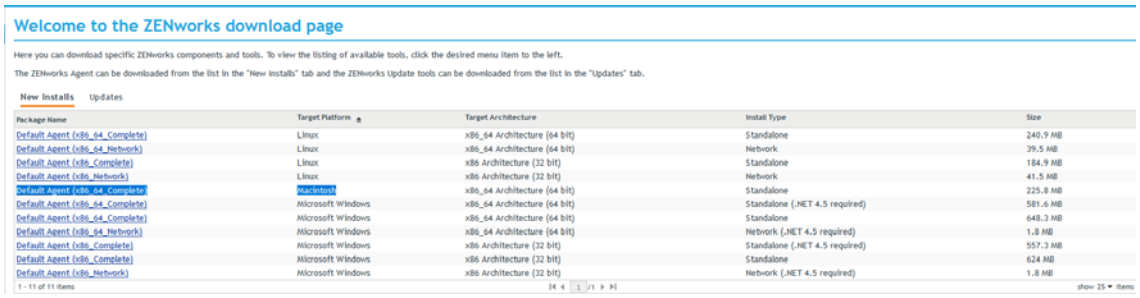
1 Before installing the agent on the device, ensure that the device meets the system requirements. For more information, see Managed Device Requirements in the ZENworks 2020 Update 1 System Requirements.

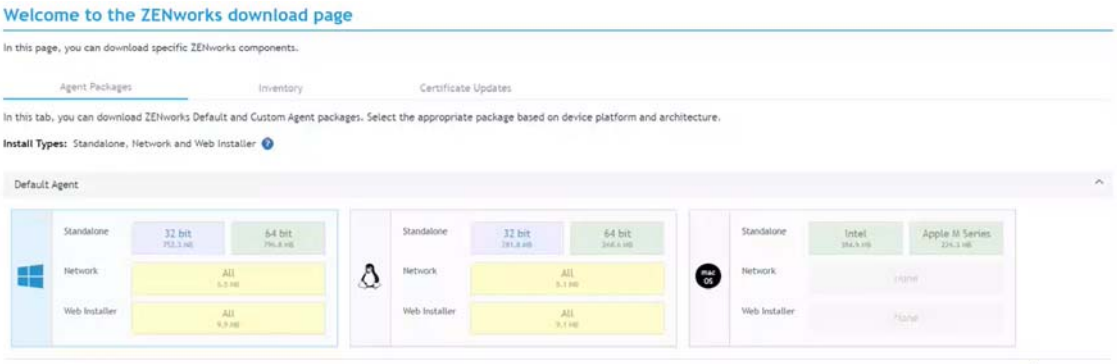
2 On the target device, open the following address to open the ZENworks download page.

https://server:port/zenworks-setup

Replace server with the DNS name or IP address of a ZENworks 2020 Update 1 or later server and replace the port only if the ZENworks Server is not using the default port (443).

3 Click the name of the agent installer with target platform Macintosh, and then save the file to the local drive of the device.





4 Double-click the downloaded installer:

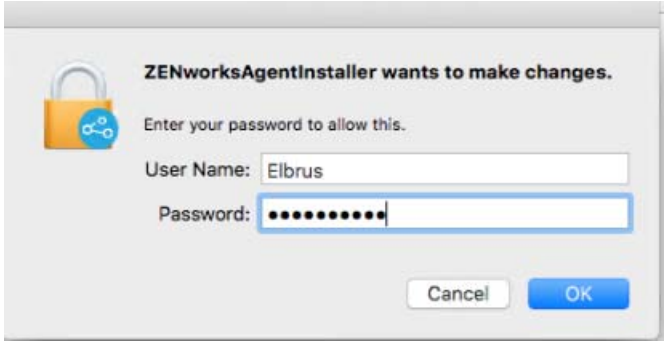
- For Intel: `ZENworksAgentInstaller.dmg` which is available as `IntelAgentInstaller.app`
- For Apple M-series: `ZENworksAgentInstaller-ARM64.dmg`, which is available as `ArmAgentInstaller.app`

NOTE: Apple M-series includes both Apple M1 and M2.

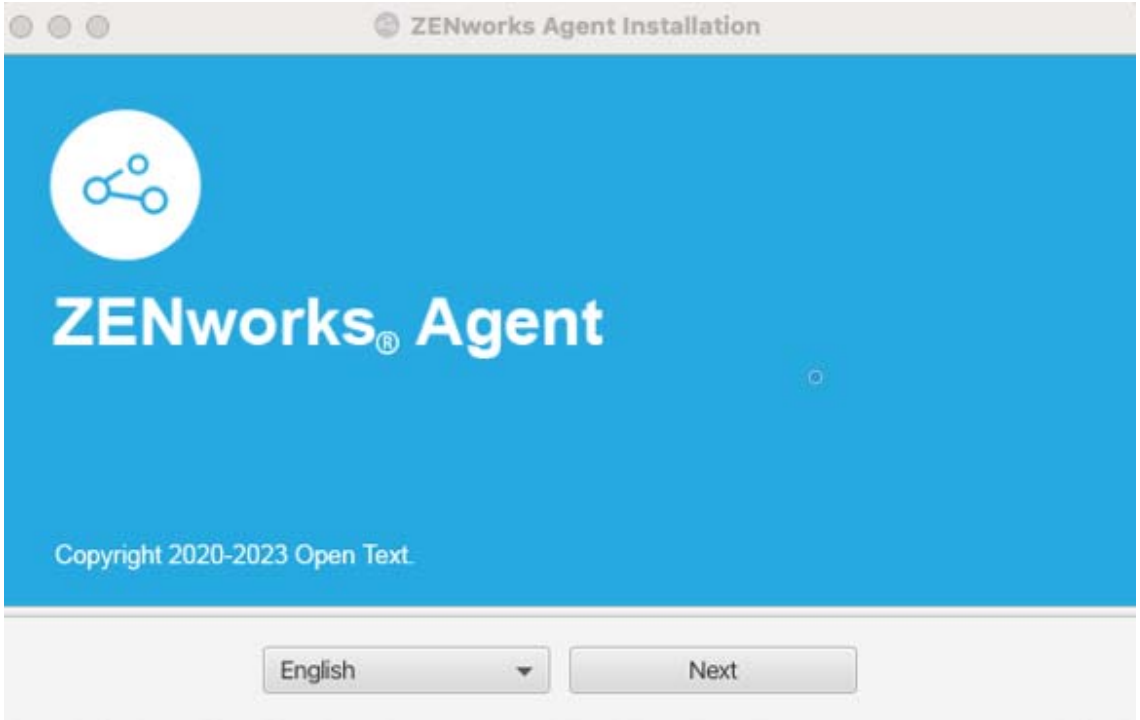
5 It extracts and opens a window with the installer (*ZENworksAgentInstaller*).

6 Click the installer, and specify the administrator credentials.

NOTE: Only users with administrator privilege rights can install the agent.



7 Select the required language and click Next.



8 Specify the ZENworks server name, port number, and then click Next.

NOTE: ◆Ensure that you specify the server details to which the agent should be registered.

- Ensure that the specified ZENworks server is up and running with 2020 update1.

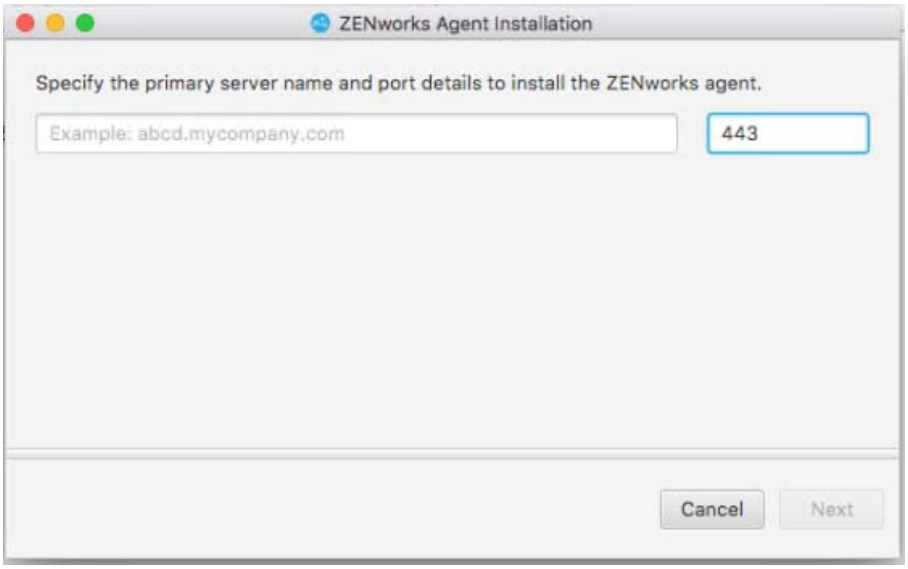
You can Provide the ZENworks Primary Server DNS Name or IPAddress along with the port 443.

Example:

Server name: primary1.dns.com

Port: 443

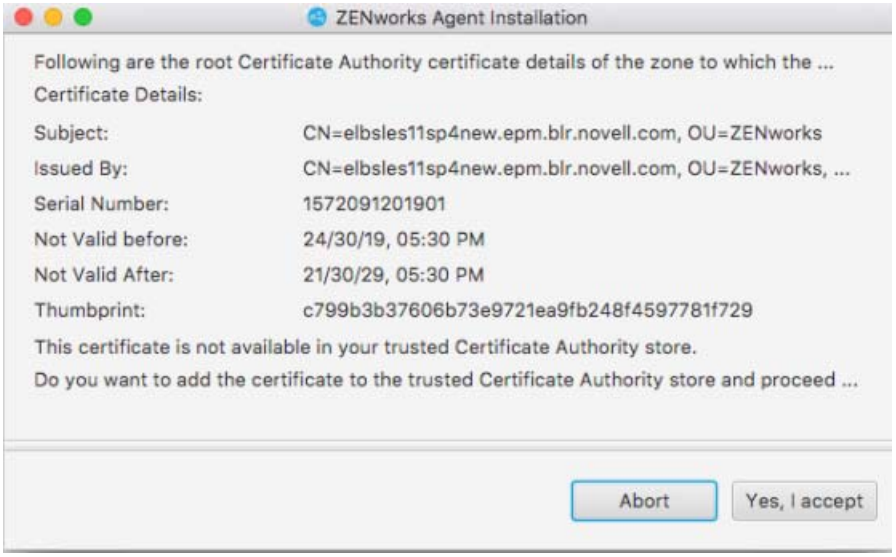
If you are using any non-default port, then specify the non-default port.



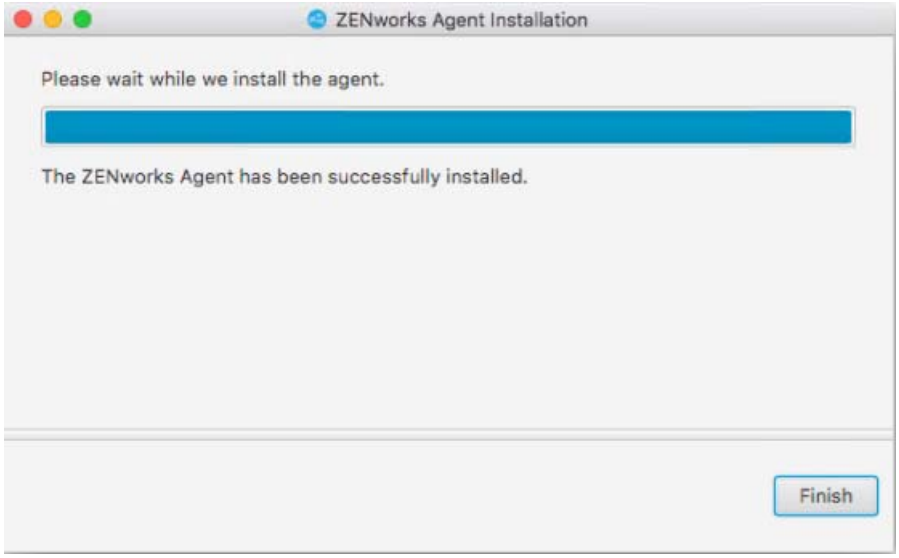
9 The root certificate of the server is displayed, click *Yes, I accept* to add this certificate to the trusted Certificate Authority store.

NOTE: ◆The Root Certificate validation prompt is displayed only for the Internal certificates that are not trusted and are not provided by any well-known external Certificate Authority (CA).

- If the certificate is already trusted certificate and is provided by an external Certificate Authority (CA), then the certificate validation prompt window will not be displayed.
- If the certificate is already expired, then only the **Abort** button is enabled. The **Yes, I accept** button is displayed as disabled.



10 After successfully installing the agent, click **Finish**.



NOTE: If you are installing the agent on a Mac device using VMware Fusion, then a blank page might be displayed. Installing the agent using a virtual machine is not supported.

Agent Deployment in VDI environment

Perform the following steps to prepare Master image:

1 Install the Agent manually.

NOTE: From ZENworks 2020 onwards, if ZENworks security configuration is enabled on the server to which the device will be registered, then ensure that you specify the authorization key during the agent installation.

2 Back up the `initial-web-service` file from the `%ZENworks_Home%\conf` location.

3 If you want to add a registration key, you can add in the `initial-web-service` file.

The first line of the `initial-web-service` file contains the list of IP addresses and host names of the server to which this device has registered. Add the registration key in the second line.

4 Unregister the device by using the `zac unr` command.

5 Clear the Workstation GUID by using zac `fsg -d` command.

6 Open the command prompt as an administrator, go to `%ZENworks_Home%\bin\preboot` folder, then run the `ZISWIN.exe -w` command to clear Image-safe Data.

7 Clear the cache by using the `zac cc` command.

8 Copy the backed up `initial-web-service` file to `%ZENworks_Home%\conf` location.

IMPORTANT: Enable the `Hostname` Reconcile settings to ensure that the agent registration and reconciliation works in VDI environment.

For more information, see "Reconciling the Devices" on page 72.

Perform the following steps to create Master Image for linked clone desktop pool:

NOTE: If you are creating a full clone image, then skip the following steps.

8a Perform *Step 1* to *Step 8* as mentioned in the *"Agent Deployment in VDI environment" on page 127*.

8b Stop the and change the **Startup type** to **Manual**.

8c Create a batch file (for example, `zenworks.bat`) with the following commands:

```
sc config "Novell ZENworks Agent Service" start= auto
sc start "Novell ZENworks Agent Service"
```

8d Copy the created batch file (`zenworks.bat`) to any location.

8e Shutdown the device and take a snapshot.

8f Specify the batch script path in the **Post -synchronization script name**, while creating the linked clone desktop pool. For example: `C:\zenworks.bat`

The path of the batch file must be the same location that you copied in *Step 8d*.

9 Shutdown the device and take a snapshot.

IMPORTANT: For the existing pool, before recomposing perform *Step 8a* to *Step 8e*, then add the **Post -synchronization script** (**Guest Customization** > **Post -synchronization script**).

If VDI Solution is Citrix XenDesktop 7.x or later versions, perform the following to create Master Image:

1 Install Citrix Virtual Delivery Agent on Windows devices.

2 During installation, select **Create Master Image**.

3 Reboot the device after Virtual Delivery Agent installation.

4 Create a Custom Deployment Package with Registration Keys that enables **Machine Name** attribute under **Reconcile Settings**.

To create registration keys with reconcile settings see, *"Creating a Registration Key" on page 61*.

5 Download and install the Custom Deployment Package that is created in *Step 4* and reboot the device.

6 Log in to the device as an administrator.

7 Verify that the device is not registered to the zone.

NOTE: Agent service will not be started in the Master Image. In order to upgrade the VDI setup, install the agent once again on the Master Image.

8 Go to `%ZENWORKS_HOME%\conf` and delete the `DeviceData` and `DeviceGUID` files.

9 Clear ISD by using `%ZENWORKS_HOME%\bin\preboot\ziswin.exe`

10 Shutdown the device and take a snapshot.

Upgrading the Agent in a Citrix VDI Environment

To upgrade the Agent in a Citrix VDI environment:

1. Install the latest agent on the base machine.
2. Go to `%ZENWORKS_HOME%\conf` and delete the `DeviceData` and `DeviceGUID` files.
3. Clear ISD (Image Safe Data) by using `%ZENWORKS_HOME%\bin\preboot\ziswin.exe`
4. Shutdown the device and take a snapshot.
5. In the Citrix Studio, go to **Machine Catalog** and click **Update Machines**.
6. Select the latest snapshot that was taken in Step 4 on page 129, and then complete the on screen instructions.

Agent Deployment on Citrix Server

On a Citrix server, after deploying the ZENworks agent, you need to perform certain tasks. For details, see "Tasks to be Performed after Deploying the Agent on Citrix Servers" in the *ZENworks Best Practices Guide*.

Package Options for Windows, Linux, and Macintosh

You can use the following options when launching a deployment package from the command line on Windows, Linux, and Macintosh. The syntax is:

```
package name option1 option2 ...
```

An example for Windows:

```
PreAgentPkg_Agent.exe -q -v -k regkey1
```

An example for Linux:

```
PreAgentPkg_AgentLinux.bin -S -k regkey1
```

An example for Macintosh:

```
PreAgentPkg_AgentMAC.bin -k regkey1
```

The command accepts the following options:

On Linux

-G: Do not install packages which require X or GUI.

-S: Disable SELinux if the agent is unable to open the ports required by ZENworks.

-k: The registration key used to register the device in the management zone.

-ak: The Authorization Key when deploying agent in a zone that has Agent to Server secure communication enabled.

On Windows

-x: Do not reboot after installation.

-q: Suppress the reboot prompt.

-Z: Log the ZESM installation information.

-U: Force uninstall of older ZENworks Desktop Management Agent.

-K: Installs drivers for ZENworks Endpoint Security Management (ZESM), Full Disk Encryption (FDE), Full Location Awareness (FLA) and Agent Self Defense (ASD) based on the argument passed.

For more information, see:

- **ZESM:** ZENworks Endpoint Security Agent Reference
- **FDE:** ZENworks - Full Disk Encryption Overview
- **FLA:** Configuring the Location Awareness Mode for the Zone
- **ASD:** Configuring Agent Self Defense

For example: If this `PreAgentPkg_Agent.exe –K 1111` parameter is passed, then all drivers (ZESM, FDE, FLA and ASD) will be installed.

-b: Blocks installation of component. Component can be a single component or a comma separated list of ZENworks components.

Supported component names: FDE, ZESM, Asset Management, Policies, Bundles, Patches, Users, Remote Management and Imaging.

On Linux and Windows

The following options are applicable only to the web-installer package in ZENworks 2020 Update 3:

-server: The IP address or hostname of the primary server.

-port: The port configured for the primary server. The default port is 443.

-cacert: The CA certificate for the server and its path.

-sslignore: Ignores the SSL warning of the untrusted CA certificate.

-s: Prevents the display of the summary screen.

On Linux, Macintosh, and Windows

-d *target_path*: Extract the files to the specified target path. The default target path for Windows is `c:\windows\novell\zenworks\stage`.

The default target path for Linux and Macintosh is `/opt/novell/zenworks/stage`.

-h: Display help information.

-k: The registration key used to register the device in the management zone.

-l: List the contents of the package only. Do not extract the package and run the installation.

-n: Extract the package but do not run the installation.

-v: Turn on verbose screen logging.

In addition to the options listed above, there are two additional BUILDTIME options (-f *file* and -o *output_file*) that are used when building packages. These options should only be used under the direction of Micro Focus Customer Support.

Installing the Agent as an Add-on Product in SLES/SLED

You can install the ZENworks Agent on SUSE Linux Enterprise Server (SLES) and Desktop (SLED) devices by using YaST.

You need to manually install the ZENworks certificates to the OS trust store before configuring the software repository in YaST. Adding the `?ssl_verify=no` at the end of the URL will allow you to bypass the SSL handshake.

The ZENworks Server hosts a repository, which is used as add-on media by YaST to install the ZENworks Agent at the following URL:

`https://<server_ip>/zenworks-agent-addon/zenworks-agent-addon-sle11/?ssl_verify=no`

`https://<server_ip>/zenworks-agent-addon/zenworks-agent-addon-sle12/?ssl_verify=no`

`https://<server_ip>/zenworks-agent-addon/zenworks-agent-addon-sle15/?ssl_verify=no`

Replace *server_ip* with the DNS name or IP address of a ZENworks Server.

You need to manually register the installed agent with the ZENworks Management Zone.

NOTE: ◆This URL https:/<*server_ip*>:<port>/zenworks-agent-addon might not list any repositories if server is configured with non-default ports.

- The ZENworks Agent cannot be installed by using the Auto YaST installation process.
- When a ZENworks server is added as a YaST2 repository in a SLED or SLES machine, you will see a warning message: **Cannot assess installation media. Check whether the server is accessible**.

  Ignore the warning and proceed with adding the repository.

Installing the ZENworks Agent on SLES/SLED 11, 12 and 15

To install the ZENworks Agent on SLES/SLED 11,12 and 15 by using YaST:

1. Launch YaST Control Center.
2. Click the **Software** tab, then click **Add-on Products**.
3. In the Installed Add-on Products window, click **Add**.
4. Select the **Media Type** as **HTTPS**, then click **Next**.
5. Provide the necessary repository and server details for the selected media, then click **Next**.
6. Accept the **License Agreement**.

   The Software Management wizard is displayed.

7 In the **Filter** drop-down list, select **Patterns**.

   In the Patterns panel under **Add-on**, select **ZENworks Agent All**.

8 Click **Accept** to install the ZENworks Agent.

Installing the Agent by Using YUM on RHEL

You can install the ZENworks Agent on Red Hat Enterprise Linux (RHEL) devices by using YUM.

IMPORTANT: Currently installing the agent by using YUM is not supported for Scientific Linux.

The ZENworks Server hosts a repository, which is used by YUM to install the ZENworks Agent at the following URL:

```
https://<server_ip>/zenworks-agent-addon/zenworks-agent-yum-repo-rhel7/
?ssl_verify=no
```

```
https://<server_ip>/zenworks-agent-addon/zenworks-agent-yum-repo-rhel8/
?ssl_verify=no
```

```
https://<server_ip>/zenworks-agent-addon/zenworks-agent-yum-repo-rhel9/
?ssl_verify=no
```

NOTE: This URL https:/<*server_ip*>:<port>/zenworks-agent-addon might not list any repositories if server is configured with non-default ports.

You need to manually register the installed agent with the ZENworks Server.

To install the ZENworks Agent on RHEL, perform the following steps:

1 Add a new repository file named `zenworks.repo` to the `/etc/yum.repos.d/` directory with the following content:

   For a 32-bit device:

```
[zenworks-agent-addon]
name=zenworks-agent-addon
baseurl=https://<server_ip>/zenworks-agent-addon/<repo_url>/

gpgcheck=0
```

   For a 64-bit device:

```
[zenworks-agent-addon]
name=zenworks-agent-addon
exclude=*.i386 novell-zenworks-zislnx*.i586 xinetd*.i386 xinetd*.i686
novell-zenworks-xplat-zennotifyicon*.i586 novell-zenworks-xplat-
jsvc*.i586 novell-zenworks-xplat-imaging-native*.i586 jre*.i586 novell-
zenworks-zmg*.i586
baseurl=https://<server_ip>/zenworks-agent-addon/<repo_url>/
sslverify=0
```

`gpgcheck=0`

Replace *server_ip* with the DNS name or IP address of a ZENworks Server and *repo_url* with zenworks-agent-yum-repo-rhel7 for RHEL 7, and zenworks-agent-yum-repo-rhel8 for RHEL 8and zenworks-agent-yum-repo-rhel9 for RHEL 9.

NOTE: By default, YUM installs 32-bit RPMs on 64-bit devices. If multiple architectures for the same RPM are available in the YUM repository, both the 32-bit and 64-bit RPMs are installed on 64-bit devices. The exclude attribute ensures that conflicting 32-bit RPMs are not installed on the 64-bit devices.

---

2 Ensure you disable SELinux before installing the agent. To install the agent, run the `yum groupinstall zenworks-agent-addon` command.

SELinux provides limited access control on Linux. Select this option to disable SELinux if the agent is unable to open the ports required by ZENworks. SELinux is temporarily disabled only if the agent is unable to open the ports, and is automatically enabled again after the agent installation.

3 If the security is enabled in the zone, run the `zac reg -a <auth key>` zac command to register RHEL agent to the zone.

4 If security is enabled in the zone, then run the `zac reg -a <auth key>`zac command to register the RHEL agent to the zone.

NOTE: On RHEL devices, if the ZENworks Agent is installed using the `yum groupinstall`, to uninstall it, you need to use the `novell-zenworks-xplat uninstall` located at `/opt/novell/zenworks/bin`. The `yum groupremove` is not supported.

---

12 Viewing and Updating the Managed Device Details

After the ZENworks Agent is deployed, its details are listed in ZENworks Control Center, based on the information available for a managed device.

If the discovered information for a device is incorrect or insufficient, administrators with the Modify Device rights can manually change the details for the fields that have the **Edit** button next to them.

You can view the following information about a managed device:

- **Alias**: Displays the name assigned to the device when it registered. The name is determined by the Device Naming Template, which is a configuration setting available on devices, device folders, and the Management Zone.
- **Hostname**: Displays the device's host name.
- **IP Address**: Displays the device's IP address.
- **Test Device:** Displays if the device is a test device or a non-test device.

  If the device is not a test device, you can click **Set** to set the device as a test device. If the device is a test device, you can click **Reset** to reset the device as a non-test device.
- **Last Full Refresh**: Displays the last time that the device refreshed its information (bundles, policies, configuration information, registration information, and so forth). A refresh can be manually initiated by the device's user, manually initiated by an administrator using the Refresh Device Quick Task, or scheduled. The refresh schedule is determined by the Device Refresh Schedule configuration setting available on devices, device folders, and the Management Zone.
- **Last Contact**: Displays the last time the agent contacted the ZENworks Server.
- **Last Boot Time:** Displays the date and time when the device was rebooted the last time. For more information, hover on the displayed date. The value will be unavailable if the server is at ZENworks 2020 Update 2 or lower versions.
- **Reboot Pending Since:** Displays the date and time since when the device reboot is pending. This field will be displayed only when you have postponed the device reboot after applying a patch, update, or any other action that requires a device reboot. The value will be unavailable if the device reboot is completed, or if the server is at ZENworks 2020 Update 2 or lower versions, or if the server OS is Linux or Macintosh.
- **Network Location:** Displays the network location name to which the device was connected. Along with the name, time and date of connection will also be displayed. The value will be unavailable if the server is at ZENworks 2020 Update 2 or lower versions.
- **Network Environment:** Displays the network environment name to which the device was connected. Along with the name, the time and the date of connection will also be displayed. The value will be unavailable if the server is at ZENworks 2020 Update 3 or lower versions.
- **ZENworks Agent Version**: Displays the version of the ZENworks Agent software on the device. Click the underlined version number to display a list of the ZENworks Agent modules that are installed on the device along with their version numbers.

You can uninstall, enable, or disable the ZENworks modules by using the ZENworks Agent settings on the device's Settings page. Click the **Settings** tab > click **Device Management** > click **ZENworks Agent** > in the **Enable/Disable Agents** section, click **Installed**, **Enabled**, or **Disabled** for each agent, select the reboot behavior, then click **Apply**. If you are configuring the ZENworks Agent settings on a device folder or a device, you need to click **Override settings** before you can modify the settings.

NOTE: For upgrading or troubleshooting purposes, you can use the Advanced Search feature to display a list of devices in your ZENworks Management Zone that have a specified version of the ZENworks Agent software installed.

1. Depending on whether you want to search for all devices (servers and workstations), for servers, or for workstations that have the specified version of the ZENworks Agent installed, do one of the following in ZENworks Control Center:
   - To search for all devices, click the **Devices** tab.
   - To search for all servers, click the **Devices** tab > **Servers**.
   - To search for all workstations, click the **Devices** tab > **Workstations**.
2. In the Search section, click **Advanced Search**.
3. Click **Add** to display the Search Criteria dialog box.
4. Click **Add Filter**, click **Device/AgentVersion** from the drop-down list, then click **OK**.

- **ZENworks Updater Service Last Contact Time**: Displays the time at which the ZENworks Updater Service (ZeUS) last contacted the ZENworks server.
- **ZENworks Agent Status**: Monitors and displays the status of the ZENworks Updater Service (ZeUS) and the ZENworks Agent. It might take a while for the status to be displayed.
  - Indicates that both ZeUS and ZENworks Agent are reachable.
  - Indicates that ZeUS is up but the ZENworks Agent is not reachable.
  - Indicates that ZeUS is not reachable.
  - Unknown; indicates that status determination is in progress
- **MDM Enrolled**: Displays if the device is enrolled using MDM.

  Displays Yes if the device is enrolled via MDM, else No is displayed.
- **MDM Agent Version**: Displays the version of the MDM agent.
- **MDM Sync Time**: Displays the time stamp at which the MDM agent synced with the ZENworks server.
- **Operating System**: Displays the device's operating system.
- **Number of errors not acknowledged**: An error is any action that fails so the ZENworks Agent cannot complete the action on the device. The number displayed indicates the number of unacknowledged errors, which are any errors that you have not specifically marked as acknowledged. Unacknowledged errors are displayed in the Message Log panel.

- **Number of warnings not acknowledged**: A warning is any action that encounters a problem; the problem might or might not result in the ZENworks Agent completing the action on the device. The number displayed indicates the number of unacknowledged warnings, which are any warnings that you have not specifically marked as acknowledged. Unacknowledged warnings are displayed in the Message Log panel.
- **Primary User**: Displays the primary user associated with the device. If no user is associated, the field is empty.

  Associating a primary user with the device enables you to establish bundle system requirements and policies based on the primary user.

  To change the primary user association, click **Edit**. You can manually select the primary user, or you can have ZENworks automatically select the user based on the **Primary User** setting (**Configuration** tab > **Configuration** > **Device Management** > **Primary User**).
- **Owner**: Displays the person who should be contacted with issues or questions about the device. Click **Edit** to change the owner.
- **Serial Number**: Displays the device's serial number. A device has a serial number if the device object was manually created in the ZENworks Management Zone and a serial number was specified (in ZENworks Control Center > click the **Devices** tab > click **Add Device** under **Device Tasks** in the left navigation pane). If the device is registered automatically using a registration key or rule, then the serial number of the device is set.

  If no serial number is specified during manual creation, the serial number is set using the GUID.

  Click **Edit** to change the serial number.
- **GUID**: Displays the device's GUID (global unique identifier), a randomly generated string that provides a unique identifier for the device. You cannot edit the GUID. The GUID remains the same as long as the device exists. The GUID, rather than the modifiable device name, is used when creating relationships between the device and other ZENworks objects such as bundles, policies, groups, folders, and configuration settings.
- **Department, Site, Location**: Provides information fields for you to further identify the owner or location of the device. Click **Edit** to change the information in any of the fields.

13 Uninstalling the Agent

For information on how to uninstall the ZENworks Agent, see:

- **Windows:** "Uninstalling ZENworks Software from Windows Devices" in the *ZENworks Uninstall Guide*.
- **Linux:** "Uninstalling ZENworks Software from Linux Devices" in the *ZENworks Uninstall Guide*.
- **Macintosh:** "Uninstalling ZENworks Software from Macintosh Devices" in the *ZENworks Uninstall Guide*.

14 Deploying the Inventory-Only Module

If you want to only inventory a Windows, Linux or Macintosh OS X device, you can deploy the Inventory-only module. The inventory-only module only collects and sends the inventory data. It does not perform any of the other tasks associated with the ZENworks Agent. See "Operating System: Servers" in the *ZENworks System Requirements* for information about the platform versions on which the Inventory-Only module is supported.

NOTE: From the ZENworks 2020 Update 2 release onwards, SSL certificates are distributed to Inventory-only devices during the registration process, to secure communication between the ZENworks server and the Inventory-only device. During a server certificate remint, if for any reason the registered Inventory-only device does not receive the new certificate, then you will have to re-register the device. For more information on re-registering the device, see Re-registering Inventory-Only Devices.

The following sections provide instructions:

- "Prerequisites" on page 141
- "Downloading the Module from a ZENworks Server" on page 142
- "Installing Inventory-Only Agent (IOA) on Linux" on page 142
- "Installing Inventory-Only Agent (IOA) on Windows" on page 143
- "Installing Inventory-Only Agent (IOA) on Macintosh OS X" on page 144
- "Uninstalling the Inventory-Only Module" on page 145
- "Upgrading Inventory-Only Agent" on page 146
- "Re-registering Inventory-Only Devices" on page 146
- "Running Scannow on an Inventory-Only Device" on page 148

Prerequisites

- From the ZENworks 2020 Update 2 release onwards, new enhancements have been introduced to secure communication between the Inventory-only devices and the ZENworks server. After you upgrade to ZENworks 2020 from the previous release, these enhancements are disabled by default. To turn on these enhancements, see Security Reference Guide.

  If you do not turn on these enhancements, the existing procedure of registering Inventory-Only Agent (IOA) devices applies.
- As a part of these enhancements, you need to have the following in place to register Inventory-only devices:
  - **Authorization Key:** Procure an Authorization Key and specify this key, while executing the `zac ioa cfg` command to register the device.

- **Pre-approved Device:** If you do not have an Authorization key, then you can add the device in the list of pre-approved devices and then execute the `zac ioa cfg` command to register the device.

- The network (.NET required) package requires that Microsoft .NET 4.8 or later is installed on the device prior to registering the device.

Downloading the Module from a ZENworks Server

1. On the target device, open a Web browser to the following address:

   http://*server*/zenworks-setup

   where *server* is the DNS name or IP address of a ZENworks Server.

   IMPORTANT: The Inventory-Only module uses the default port (7443 and 443) and not the customized port configured on the ZENworks Server.

   ---

2. .

   The Inventory-Only Module for each platform is listed on

3. Click the required file in the desired platform and download the file.
4. Skip to one of the following sections to continue with installation of the module:
   - "Installing Inventory-Only Agent (IOA) on Linux" on page 142
   - "Installing Inventory-Only Agent (IOA) on Windows" on page 143
   - "Installing Inventory-Only Agent (IOA) on Macintosh OS X" on page 144

Installing Inventory-Only Agent (IOA) on Linux

1. Log in as a user with installation rights on the device.
2. Make sure you have downloaded the correct Inventory-Only module package (based on the architecture) to the target device. If you have not, see "Downloading the Module from a ZENworks Server" on page 142.
3. In the terminal go to the location of the downloaded Inventory-Only module package file.
4. Unpack the Inventory-Only module package by running the following commands:
   - `gunzip` and the package name

     Example:

     ```
     gunzip ZENworks_Inventory_Only_Agent_Linux_x86.tar.gz
     ```

   - `tar -xopf` and the package name

     Example:

     ```
     tar -xopf ZENworks_Inventory_Only_Agent_Linux_x86.tar
     ```

   or run the following command:

   `tar -zxvf` and the package name

   Example:

   ```
   tar -zxvf ZENworks_Inventory_Only_Agent_Linux_x86.tar.gz
   ```

The package will be extracted to a new directory with the same name.

5 In the terminal, browse to the location of the extracted package in Step 4 and install the Inventory-Only module by running the `./install.sh` command. The relevant Inventory-Only Agent (IOA) packages will be installed on the device.

The installation program requires no user interaction.

6 After the installation program completes its execution, register the Inventory-Only Agent (IOA) device to the server by running the following command:

```
zac ioa cfg <server_ip:port_number>
```

- If you are using the default port, then specify only the IP address.

  For example,

  - **IPv4:** zac ioa cfg <*server_ip:port_number*>
  - **IPv6:** zac ioa cfg <[*server_ip]:port_number*>

  In the above command, replace the <*server_ip*> with the actual IP address.

The Inventory-Only module is started and the device is added to the Inventoried devices page in ZENworks Control Center (**Devices tab** > **Inventoried tab** > **Workstations or Servers** folder).

For details see "Inventory-Only Commands"in the "*ZENworks Command Line Utilities Reference*".

NOTE: To debug any issues that you might face while registering the device, see the `zmd-messages.log` in `\novell\zenworks\logs\localstore` on the device that you want to register to the zone. You can also refer to `service-messages.log` on the server to which you are registering the device.

Installing Inventory-Only Agent (IOA) on Windows

1 Make sure you have downloaded to the target Windows device. If you have not, see "Downloading the Module from a ZENworks Server" on page 142.

2 Make sure the location of `msiexec.exe` on the target machine is in the path variable of the target machine.

3 At a command prompt, run to launch the installation program.

4 After the installation program completes its execution, register the Inventory-Only Agent (IOA) device. In the command line go to `C:\Program Files (x86)\Novell\ZENworks\bin` and run the following command:

```
zenioa register
```

- To run this command, either specify an authorization key for the secure registration of the device or ensure that the device is added in the list of pre-approved devices.

  For example, if the device is pre-approved: `zenioa register`

  For example, if you are using an Authorization Key:

  ```
  zenioa register --authkey <xyz>
  ```

- Credentials of an administrator account need to be provided while running this command.

- While registering the device to the zone, you need to trust the root certificate. A prompt to trust the root certificate will be displayed during device registration. If you do not trust the certificate, then you will not be able to register the device.

  You also have the option of auto accepting the certificate while running the command:

  For example, to auto accept the certificate:

  ```
  zenioa register --authkey <xyz> --autoAcceptCert
  ```

NOTE: ◆Ensure that you do not provide the Admin port while installing the Inventory-Only Agent.

- To view the imported certificate, navigate to `regedit->local_machine->software->wow6432-> microsoft-> system certificate -> Root`.

  To debug any issues that you might face while registering the device, see the `zmd-messages.log` in `\novell\zenworks\logs\localstore` on the device that you want to register to the zone. You can also refer to `service-messages.log` on the server to which you are registering the device.

Installing Inventory-Only Agent (IOA) on Macintosh OS X

1. Make sure you have downloaded the `ZENworks_Inventory_Only_Agent_OSX.dmg` disk image to the target Macintosh device.

   For more information on how to download the `ZENworks_Inventory_Only_Agent_OSX.dmg` disk image, see "Downloading the Module from a ZENworks Server" on page 142.

2. Double-click the `ZENworks_Inventory_Only_Agent_OSX.dmg` file.

   Or,

   Run the `hdiutil attach filename.dmg` command to mount the disk on all versions of macOS mini.

3. Double-click the `ZENworks_Adaptive_Agent_OSX` file, so that it gets mounted.

4. Browse to the mounted drive and locate the extracted folder.

   For example, `/Volumes/ZENworks_Inventory_Only_Agent_OSX`

5. Run the `install.sh` script.

6. After the installation is complete, log out and log in to the terminal.

7. After the installation program completes its execution, register the Inventory-Only Agent (IOA) device to the server by running the following command:

   ```
   zac ioa cfg <server_ip:port_number>
   ```

   NOTE: Ensure that you do not provide the Admin port while installing the Inventory-Only Agent.

   - To run this command, either specify an authorization key for the secure registration of the device or ensure that the device is added in the list of pre-approved devices.

     For example, if the device is pre-approved:

     ```
     zac ioa cfg <server_ip:port_number>
     ```

     For example,

```
zac ioa cfg <server_ip:port_number> --authkey <xyz>
```

- While registering the device to the zone, you need to trust the root certificate. A prompt to trust the root certificate will be displayed during device registration. If you do not trust the certificate, then you will not be able to register the device. You also have the option of auto accepting the certificate while running the command:

  For example, to auto accept the certificate:

  ```
  zac ioa cfg <server_ip:port_number> --authkey <xyz> --autoAcceptCert
  ```

- If you are using the default port, then specify only the IP address.

  For example:

  - **IPv4:** zac ioa cfg <*server_ip:port_number*>
  - **IPv6:** zac ioa cfg <*[server_ip]:port_number*>

  In the above command, replace the <*server_ip*> with the actual IP address.

8 The Inventory-Only module is added to the Inventoried Devices page in ZENworks Control Center (**Devices** tab > **Inventoried** tab > **Workstations** folder).

NOTE: To debug any issues that you might face while registering the device, see the `zmd-messages.log` in `\novell\zenworks\logs\localstore` on the device that you want to register to the zone. You can also refer to `service-messages.log` on the server to which you are registering the device.

Uninstalling the Inventory-Only Module

To uninstall the Inventory-Only module for the supported platforms, use the following instructions:

Linux

1 Go to the `/opt/novell/zenworks/bin` directory.

2 Execute the `novell-zenworks-ioa-uninstall` script.

Windows

1 From the Windows Start menu, select **Settings** > **Control Panel** > **Add or Remove Programs.**

2 Select ZENworks Adaptive Agent Service, then click **Remove**.

Macintosh OS X

1 Go to the `cd /opt/novell/zenworks/bin` directory.

2 Execute the `novell-zenworks-ioa-uninstall` script.

NOTE: ◆To remove the Inventory-Only module from ZENworks Control Center (ZCC), go to ZCC and manually delete the object.

- You cannot upgrade the 11.3 and earlier versions of Linux Inventory-Only Agent (IOA) devices to 2020.Therefore you need to first uninstall the existing zenumia agents, and then make a fresh install of the 2020 agents.

Upgrading Inventory-Only Agent

Macintosh OS X

To upgrade to a newer version of Inventory-Only Agent (IOA) on the Macintosh OS Device:

1. Uninstall the existing Inventory-Only agent. For more information, see "Uninstalling the Inventory-Only Module" on page 145.
2. Install the new Inventory-Only agent. For more information, see "Downloading the Module from a ZENworks Server" on page 142.

Linux

The Inventory-only agents on Linux devices are automatically upgraded, after the ZENworks server is upgraded to the newer version and the scheduled device refresh is performed.

Alternatively, you can also run the following command before the scheduled device refresh, in the command prompt:

```
zac su
```

Windows

The Inventory-only agents on Windows devices are automatically upgraded, after the ZENworks server is upgraded to the newer version and the scheduled device refresh is performed.

Re-registering Inventory-Only Devices

There are two options you can use for re-registering Inventory-Only devices.

- "Re-registering Inventory-Only Devices for All Platforms" on page 146
- "Re-registering Inventory-Only Devices for Individual Platforms" on page 146

Re-registering Inventory-Only Devices for All Platforms

This procedure is common to re-register the Inventory-Only devices for all the supported platforms.

1. Uninstall the existing agent from the device by following the instructions provided for the selected platform in "Uninstalling the Inventory-Only Module" on page 145.
2. Download the executable agent from the latest module on the ZENworks Server.

   For more information, see "Downloading the Module from a ZENworks Server" on page 142.

Re-registering Inventory-Only Devices for Individual Platforms

This procedure can be used for re-registering Inventory-Only devices for the specified platforms.

Linux

1. Execute the following command:

`zac ioa cfg <server_ip:port_number>`

-

  For example, if the device is pre-approved:

  `zac ioa cfg <server_ip:port_number>`

  For example,

  `zac ioa cfg <server_ip:port_number> --authkey`

- While registering the device to the zone, you need to trust the root certificate. A prompt to trust the root certificate will be displayed during device registration. If you do not trust the certificate, then you will not be able to register the device.

  You also have the option of auto accepting the certificate while running the command:

  For example, to auto accept the certificate:

  `zac ioa cfg <server_ip:port_number> --authkey <xyz> --autoAcceptCert`

- If you are using the default port, then specify only the IP address.

  For example:

  - **IPv4:** zac ioa cfg <*server_ip:port_number*>
  - **IPv6:** zac ioa cfg <*[server_ip]:port_number*>

  In the above command, replace the <*server_ip*> with the actual IP address.

Windows

1. Go to the `C:\Program Files\Novell\ZENworks\bin` `C:\Program Files (x86)\Novell\ZENworks\bin` directory.
2. In the service manager, stop the Microfocus ZENworks Agent Adaptive Agent.
3. Edit the `uiaconfig.xml` file.
4. Replace the existing Server IP address with the new ZENworks Server IP address.
5. Save and close the inventory config file.
6. (Conditional) If necessary modify the register key `HKLM\Software\Novell\ZCM` to change the default values for server, port, and secure port.

   By default, the server is the DNS name or IP address of the ZENworks Server and the default numbers for the port and secure port is 443.
7. To restart the service in the service manager, start Microfocus ZENworks Adaptive Agent Service.

Macintosh OS X

1. Execute the following command:

   `zac ioa cfg <server_ip:port_number>`

   -

     For example, if the device is pre-approved:

     `zac ioa cfg <server_ip:port_number> --authkey`

- While registering the device to the zone, you need to trust the root certificate. A prompt to trust the root certificate will be displayed during device registration. If you do not trust the certificate, then you will not be able to register the device.

  You also have the option of auto accepting the certificate while running the command:

  For example, to auto accept the certificate:

  `zac ioa cfg <server_ip:port_number> --authkey <xyz> --autoAcceptCert`
- If you are using the default port, then specify only the IP address.

  For example:

  - **IPv4:** zac ioa cfg <*server_ip:port_number*>
  - **IPv6:** zac ioa cfg <*[server_ip]:port_number*>

  In the above command, replace the <*server_ip*> with the actual IP address.

Running Scannow on an Inventory-Only Device

To run a scan on an Inventory-Only device, follow the steps provided for the supported platforms:

Linux

1. Open the terminal and run the following command:

   `zac inv scannow`

Windows

1. At the command prompt, go to the `cd "C:\Program Files\Novell\ZENworks\bin" cd "C:\Program Files (x86)\Novell\ZENworks"` bin directory.
2. Enter the `zenioa scannow` command.

Macintosh OS X

1. Open the terminal and run the following command:

   `zac inv scannow`

III Device Removal and Retirement

The following sections provide information and instructions to help you delete or retire devices from your ZENworks system.

If you delete a server or workstation device, the selected device is removed from your ZENworks system.

Retiring a device is different from deleting a device. When you retire a device, its GUID is retained (as opposed to when you delete a device, which also deletes its GUID). As a result of retiring a device, all inventory information is retained and is assessable but all policy and bundle assignments are removed. A retired device is in a holding state until you unretire or delete the device. If you unretire the device in the future, its assignments are restored. You can retire both managed and inventoried devices.

- Chapter 15, “Deleting Devices from Your ZENworks System,” on page 151
- Chapter 16, “Retiring or Unretiring Devices,” on page 153
- Chapter 17, “Exporting Details to CSV Format,” on page 155

15 Deleting Devices from Your ZENworks System

If you delete a server or workstation device, the selected device is removed from your ZENworks system, its GUID is deleted, all inventory information is removed, and all policy and bundle assignments are removed.

NOTE: Enrolled mobile devices cannot be deleted from ZENworks. You need to unenroll these devices. Mobile devices that are in wipe pending, retired, or enrollment pending states can be deleted from ZCC. For more information, see Unenrolling Devices.

---

1. In ZENworks Control Center, click the **Devices** tab.
2. Click the underlined link next to the **Servers** or **Workstations** folder to display the list of servers or workstations in your ZENworks system.
3. Select the check box in front of the server or workstation (you can select multiple devices).
4. Click **Delete**.

NOTE: In ZENworks Control Center, if you delete Windows or Linux devices, the devices are automatically registered again after the next refresh.

You cannot delete a ZENworks Primary Server and Satellite Server from the **Devices** tab. If you select a Primary Server in Step 3 and click **Delete**, then the following error message displays:

```
Error: The object "vm232w2k3ent" is a Primary Server and cannot be
deleted. To delete a Primary Server, go to Configuration, Server Hierarchy,
(select a Primary Server), Action, Delete ZENworks Server.
```

If you select a Satellite Server in Step 3 and click Delete, then the following error message displays:

```
Error: The object "windows-10-x64" is a Satellite Server and cannot be
deleted. The roles on a satellite server should be removed before it can be
deleted.
```

For more information about deleting a ZENworks Primary Server, see "Deleting a ZENworks Primary Server"in the *ZENworks Primary Server and Satellite Reference*.

16 Retiring or Unretiring Devices

If you retire a server or a workstation device, the selected device is retired from the ZENworks zone. Retiring a device is different from deleting a device. When you retire a device, the device GUID is retained. However, when you delete a device, the device GUID is also deleted. Also when a device is retired, all policy and bundle assignments, and inventory information are retained. A retired device is in a holding state until you unretire or delete the device. If you unretire the device in the future, its assignments are restored. You can retire both managed and inventoried devices.

To retire or unretire a device, you must have Device Modify rights. For more information, see "Device Rights"in the *ZENworks Administrator Accounts and Rights Reference*.

To retire or unretire a managed device:

1. In ZENworks Control Center, click the **Devices** tab.
2. Click the underlined link next to the **Servers** or **Workstations** folder to display the list of servers or workstations in your ZENworks system.
3. Select the check box in front of the server or workstation (you can select multiple devices).

   Before you can retire a ZENworks Primary Server, you must first demote it. For more information, see "Changing the Parent-Child Relationships of Primary Servers"in the ZENworks Primary Server and Satellite Reference (https://www.novell.com/documentation/zenworks-23.3/zen_sys_servers/data/bookinfo.html).
4. Click **Action** > Retire Device to retire the device upon its next refresh.

   or

   Click **Action** > **Unretire** to unretire the device upon its next refresh.

   The icon displays in the **Status** column in the **Servers** or **Workstations** list for retired devices. You can mouse over the time to see the full date and time.

   NOTE: To retire a device immediately, select the check box in front of the servers or workstations, then click **Quick Tasks** > **Retire Device Now**.

   To unretire a device immediately, select the check box in front of the servers or workstations, then click **Quick Tasks** > **Unretire Device Now**.

To retire or unretire an inventoried device:

1. In ZENworks Control Center, click **Devices > Inventoried**.
2. Click the underlined link next to the **Servers** or **Workstations** folder to display the list of servers or workstations in your ZENworks system.
3. Select the check box in front of the server or workstation you want to retire or unretire (you can select multiple devices).
4. Click **Action** > **Retire Device**.

   or

   Click **Action** > **Unretire Device**.

The icon displays in the **Status** column in the **Servers** or **Workstations** list for retired devices. You can mouse over the time to see the full date and time.

After a device has been retired the inventory management status shows as **Disabled**. You can continue to view the inventory reports of the last inventory scan or search for all retired devices in your ZENworks system.

To search for retired servers and workstations:

1. In ZENworks Control Center, click the **Devices** tab.
2. (Conditional) To search for both retired servers and workstations, skip to Step 3.

   or

   To search for only retired servers, click the underlined link next to the **Servers** folder to display the list of servers.

   or

   To search for only retired workstations, click the underlined link next to the **Workstations** folder to display the list of workstations.
3. In the Search box, select **Retired** from the **Device State** drop-down list.
4. Click **Search**.

17 Exporting Details to CSV Format

To export the server or workstation data to comma separated value (CSV) format:

1. Click **Devices** > **Servers** or **Workstations**.
2. Click **Export**, then select **As csv**.

For all the listed servers, the following details are listed in the CSV file:

- Name
- Type
- Operating System
- Server Type
- Last Contact
- Lost
- Retired
- Message Status
- Compliance

IV Appendixes

- Appendix A, “Viewing the Predefined Reports,” on page 159
- Appendix B, “Schedules,” on page 161
- Appendix C, “Configuring NMAP for ZENworks,” on page 165
- Appendix D, “Troubleshooting Discovery, Deployment, and Retirement,” on page 167

A Viewing the Predefined Reports

The ZENworks Reporting is a powerful, flexible, and customizable reporting tool that is installed and configured separately from the ZENworks system. For information on how to install ZENworks Reporting, see the *ZENworks Appliance Deployment and Administration Reference*.

To view the predefined reports for discovered devices and ZENworks Systems:

1. Log in to ZENworks Reporting.
2. Navigate to the **View** > Repository > Folders > Organization > Reports > ZENworks > Predefined Reports folder.
3. Click **Discovered Devices**.

   The following predefined reports are included for discover devices:

   - **CISCO Routers:** Displays information on the discovered Cisco routers in the zone.
   - **Deployable Devices:** Displays all the discovered devices that have been identified as types to which you can deploy the ZENworks Agent.
   - **Managed Devices by ZENworks Management Zone:** Displays all the discovered devices that have the ZENworks Agent installed on them. It also displays the ZENworks Management Zone information of all the discovered devices.
   - **Printed Page Count by Printer:** Displays the discovered printers and the number of pages printed by each printer.
   - **Printer Alerts:** Displays printer alerts and the alerting units of the discovered printers.
   - **Printer Supply Levels:** Displays the supply levels for units, including toner, waste toner, and fuser of the discovered printers.
   - **Unmanaged Servers:** Displays all the discovered devices that have been identified as servers to which you can deploy the ZENworks Agent.
   - **Unmanaged Workstations:** Displays all the discovered devices that have been identified as workstations to which you can deploy the ZENworks Agent.
   - **Managed Device Listing:** Displays the discovered, inventoried, and managed devices in the Management Zone. This report is included in the **ZENworks System** folder (**Novell ZENworks Reports** > **Predefined Reports** folder).
   - **Non-Compliant Devices:** Displays the number of non-compliant devices that are present in a zone.This report is included in the **ZENworks System** folder (**Novell ZENworks Reports** > **Predefined Reports** folder).

For more information about ZENworks Reporting, see the *ZENworks Reporting System Reference* documentation.

B Schedules

The following schedules are available for discovery and deployment tasks:

- "Now" on page 161
- "No Schedule" on page 161
- "Date Specific" on page 161
- "Recurring" on page 162

Now

Runs the task immediately after completing the task wizard.

No Schedule

Indicates that no schedule has been set. The task does not run until a schedule is set or it is manually launched. This is useful if you want to create the task and come back to it later to establish the schedule or run it manually.

Date Specific

The **Date Specific** scheduling option lets you specify one or more dates on which to run the task.

Start Dates

Click ⊕ to display a calendar you can use to select a date for the task. You can add multiple dates one at a time.

Run Event Every Year

Select this option to run the task every year on the dates shown in the **Start Date(s)** list.

Select When Schedule Execution Should Start

Select one of the following options:

- **Start Immediately at Start Time:** Starts the task at the time you specify in the **Start Time** field.
- **Start at a Random Time between Start Time and End Time:** Starts the task at a randomly selected time between the time you specify in the **Start Time** and **End Time** fields. You can use this option to avoid possible network overload from concurrently scheduled tasks.

Use Coordinated Universal Time (UTC)

The Start Time is converted to Universal Coordinated Time (UTC). Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you do not select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.

Recurring

The **Recurring** scheduling option lets you repeat the task at a specified interval.

Days of the Week

This schedule lets you specify the days during the week that you want the event to run. The event is run on these same days each week.

Select **Days of the Week**, then fill in the following fields:

- **Sun ... Sat:** Specifies the days of the week you want to run the event.
- **Start Time:** Specifies the time you want to run the event.
- **Use Coordinated Universal Time:** The Start Time is converted to Universal Coordinated Time (UTC). Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you do not select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.
- **Start at a Random Time between Start Time and End Time:** Starts the event at a randomly selected time between the time you specify in the **Start Time** and **End Time** fields. You can use this option to avoid possible network overload from concurrently scheduled events.
- **Restrict Schedule Execution to the Following Date Range:** Limits running the event to the time period specified by the starting and ending dates.

Monthly

This schedule lets you specify one or more days during the month to run the event.

Select **Monthly**, then fill in the following fields:.

- **Day of the Month:** Specifies the day of the month to run the event. Valid entries are 1 through 31. If you specify 29, 30, or 31 and a month does not have those days, the event does not run that month.
- **Last Day of the Month:** Runs the event on the last day of the month, regardless of its date (28, 30, or 31).
- ***First Sunday*:** Specifies a specific day of a week. For example, the first Monday or the third Tuesday. Click ⊞ to add multiple days.
- **Start Time:** Specifies the time you want to run the event.

- **Use Coordinated Universal Time:** The Start Time is converted to Universal Coordinated Time (UTC). Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you do not select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.
- **Start at a Random Time between Start Time and End Time:** Starts the event at a randomly selected time between the time you specify in the Start Time and End Time boxes. You can use this option to avoid possible network overload from concurrently scheduled events.
- **Restrict Schedule Execution to the Following Date Range:** Limits running of the event to the time period specified by the starting and ending dates.

Fixed Interval

This schedule lets you specify an interval between days to run the event. For example, you can run the event every 14 days.

Select **Fixed Interval**, then fill in the following fields:.

- **Months, Weeks, Days, Hours, Minutes:** Specifies the interval between times when the event is run. You can use any combination of months, weeks, days, hours, and minutes. For example, both *7 days, 8 hours* and *1 week, 8 hours* provide the same schedule.
- **Start Date:** Specifies the initial start date for the interval.
- **Start Time:** Specifies the initial start time for the interval.
- **Use Coordinated Universal Time:** The Start Time is converted to Universal Coordinated Time (UTC). Select this option to indicate that the Start Time you entered is already in Coordinated Universal Time and should not be converted. For example, suppose you are in the Eastern time zone. If you enter 10:00 a.m. and select this option, the Start Time is scheduled for 10:00 UTC. If you do not select this option, the Start Time is scheduled for 14:00 UTC because Eastern time is UTC - 4 hours.
- **Restrict Schedule Execution to the Following Date Range:** Limits running of the event to the time period specified by the start date, end date, and end time.

C Configuring NMAP for ZENworks

The following section lets you know how to configure NMAP for ZENworks:

Configuring NMAP for ZENworks on Linux

Until ZENworks 2020 Update 3, configuring NMAP for ZENworks on Linux had prerequisites. From ZENworks 23.3 onwards, those requirements are no longer required. For more information, see Configuring NMAP for ZENworks on Linux in ZENworks 2020 Update 3 documentation.

Configuring NMAP for ZENworks on Windows

On a Windows Primary Server, the NMAP (`nmap.exe`) is installed in the `%ProgramFiles%\nmap` directory and added to the PATH variable of the user who installs it. While installing NMAP, PATH variable is added only to the user variable. You have to manually add it to system environment variable.

You must append the location of the NMAP installation directory (`%ProgramFiles%\nmap`) to the system environment variable PATH of Windows. You have to manually restart the Novell ZENworks Loader service in order to discover the devices.

D Troubleshooting Discovery, Deployment, and Retirement

The following sections provide solutions to the problems you might encounter while discovering devices, deploying the ZENworks Agent to devices, and retiring devices:

- "IOA Version not Getting Updated on macOS Devices While Updating to ZENworks 23.3" on page 168
- "Unable to Install ZENworks Agent on Windows Managed Device" on page 168
- "Unable to Update ZENworks Agent on OES Devices" on page 169
- "Delay while retrieving ZENworks Agent status" on page 169
- "SNMP discovery detects the latest Windows operating system as Windows 8.1" on page 169
- "Device reconciliation fails with invalid authentication" on page 169
- "If ZENworks Agent is installed on SLE12 after running the SuSEfirewall start command then ZENworks Agent fails to communicate with the ZENworks Server" on page 170
- "An error occurs while installing the ZENworks Agent through a deployment task" on page 170
- "Manual installation of the ZENworks Agent hangs with the status as starting" on page 170
- "NMAP discovery does not run from a Windows Primary Server that has NMAP installed" on page 171
- "How do I enable debug logging?" on page 171
- "Where do I find the PreAgent log files?" on page 171
- "Refreshing the Deployment page causes the discovery tasks to be repeated" on page 172
- "Orphaned and deleted files are not cleaned up from a deployment task that uses a proxy" on page 172
- "Discovery task remains in a pending state if it has a large IP address range" on page 172
- "The device that has the ZENworks Agent installed is not registered in the Management Zone" on page 173
- "Windows XP devices on which ZENworks 11.x Agents are installed cannot be registered to a ZENworks Management Zone" on page 173
- "Unable to remove or uninstall a registered Macintosh device from the Management Zone" on page 174
- "ZENworks Agent installation fails because of a ZENPreAgent and ZPA_Ifacetype initialization exception" on page 174
- "After installing the ZENworks Agent, you cannot find the /opt directory in the Mac OS X Finder" on page 175
- "ZENworks Agent installation fails on a Mac OS X Lion (version 10.7) device or later" on page 175
- "Push deployment fails on a WinXP device with a generic error message" on page 175

- "Agent Installation is incomplete" on page 176
- "ZENworks Agent does not work if Macintosh device is upgraded from 10.8 to 10.9" on page 176
- "ZENworks Agent installation fails when the Windows Imaging Component is not installed on the device" on page 176
- "Unable to install ZENworks Agent on Windows 2012 Server R2" on page 176
- "Duplicate Device Objects are created when Device Authentication fails during Reconciliation" on page 177
- "When a Mac patch policy bundle fails, the xauth messages that are launched are not terminated" on page 177
- "Effective location settings on the managed devices do not work after clearing the cache and refreshing the managed devices" on page 177
- "Device Serial Number not getting updated on the Device Summary Page" on page 178
- "ZCC displays lost and retired devices in the Devices Logged Into list" on page 178
- "An error was displayed when you try to re-enroll a ZENworks agent" on page 178

IOA Version not Getting Updated on macOS Devices While Updating to ZENworks 23.3

Source: ZENworks 2020 Update 3

Explanation: The Inventory-Only Agent (IOA) version on macOS devices does not get updated when you run the `zac su` command to update from ZENworks 2020 Update 3 to ZENworks 23.3.

Possible Cause: The `zac su` command is not supported on the macOS 10.13 and macOS 10.14 versions.

Action: To update the IOA version on macOS devices:

1. Uninstall the existing IOA.
2. Download the required IOA module for the macOS platform. For more information, see Downloading the Module from a ZENworks Server.
3. Re-install the downloaded IOA. For more information, see Installing IOA on Macintosh.

NOTE: IOA is not supported on the macOS 10.15 version onwards.

Unable to Install ZENworks Agent on Windows Managed Device

Source: ZENworks 2020 Update 3

Explanation: While updating the ZENworks agent on a Windows managed device, the Primary Agent MSI encounters an error:

```
MSI (s) (84:74) [00:42:10:857]: Product: ZENworks Primary
Agent -- Error 1923. Service 'Novell ZENworks Agent Service'
(Novell ZENworks Agent Service) could not be installed.
Verify that you have sufficient privileges to install system
services
```

Action: Restart the device and apply the system updates.

Unable to Update ZENworks Agent on OES Devices

Source: ZENworks 2020 Update 3

Explanation: While updating the ZENworks agent on an OES device, the update process stops abruptly or crashes.

Possible Cause: An issue with the OES client version.

Action: Ensure that you install client for Open Enterprise Server `OES client 2SP7 IR2` or a later version.

Delay while retrieving ZENworks Agent status

Explanation: At times there is a considerable delay while retrieving the ZENworks Agent Status in the Device Summary page.

Possible Cause: As the server has to contact both the ZENworks Updater Service (ZeUS) as well as the ZENworks Agent, there is a delay in retrieving the status.

Action: In ZCC, navigate to **Configuration** > **Device Management** > **System Variable**, add the system variable PING_DEVICE_TO_SEND_QUICKTASK and set the value as True. This system variable will bypass ZeUS and directly obtain the status from the ZENworks Agent.

NOTE: If the system variable is set to True, quick tasks from ZCC are also sent to the agent instead of through ZeUS.

SNMP discovery detects the latest Windows operating system as Windows 8.1

Explanation: Microsoft has deprecated SNMP, so when you perform SNMP discovery from ZENworks it might detect the latest Windows operating system as Windows 8.1.

Action: None

Device reconciliation fails with invalid authentication

Explanation: While updating an older version of the ZENworks Agent to ZENworks 2020, using the Standalone Agent Updater, when you reboot the device, the device is registered as a new device in ZCC.

Action: Manually unregister the device from the zone and add it again to the zone.

If ZENworks Agent is installed on SLE12 after running the SuSEfirewall start command then ZENworks Agent fails to communicate with the ZENworks Server

Source: ZENworks; Discovery, Deployment, and Retirement..

Explanation: The `SuSEfirewall` start command does not start the firewall. So, during agent installation the check assumes that the firewall is disabled and it will not open the port (expected behavior). But the `SuSEfirewall` start command changes the `iptables` and causes the server and agent communication failure.

Action: Stop the firewall using the `rcSuSEfirwall stop` command.

IMPORTANT: To manage the firewall services on SLE12 devices use the `rcSuSEfirwall stop` or `rcSuSEfirwall start` command instead of `SuSEfirewall start` or `SuSEfirewall stop`.

An error occurs while installing the ZENworks Agent through a deployment task

Source: ZENworks; Discovery, Deployment, and Retirement.

Explanation: If the ZENworks Agent is installed through a deployment task on a managed device that has .NET Framework 3.5 SP1 installed, you might encounter the following error message:

```
An unhandled exception (System.Security.SecurityException)
occurred in
micasad.exe.
Additional Information: Ecall methods must be packaged into
a system module.
```

Action: On the managed device, uninstall .NET Framework 3.5 SP1 and reinstall it. For more information on how to uninstall .NET Framework 3.5 SP1 and reinstall it, see the Microsoft .NET Framework 2.0 Solution Center Web site (http://support.microsoft.com/ph/8291).

Manual installation of the ZENworks Agent hangs with the status as starting

Source: ZENworks; Discovery, Deployment, and Retirement.

Explanation: The manual installation of ZENworks Agent abruptly stops on the managed device after the MSI packages are downloaded. Following are the symptoms:

- The icon displays the installation status as "`Starting...`" for a considerable amount of time.
- The status of Novell ZENworks PreAgent service is not **Started** in the Windows Service Control Manager.

- The *%SystemRoot%*\novell\zenworks\bin\zenpreagent.installerr file contains the following error message:

  ```
  Exception during start: Cannot start service ZENPreAgent
  on computer.
  ```

Possible Cause: The Novell ZENworks PreAgent service was terminated by the Windows Service Manager because it failed to respond to the start request in a timely fashion. This issue is likely to occur if the device is slow and heavily loaded.

Action: Do the following:

1. Start the Novell ZENworks PreAgent service:
   - **1a** From the Windows desktop Start menu, click **Settings** > **Control Panel**.
   - **1b** Double-click **Administrative Tools** > **Services**.
   - **1c** Start the Novell ZENworks PreAgent service.

     This automatically resumes the ZENworks Agent installation.
2. (Conditional) If the problem persists, do the following:
   - **2a** Kill the zenpreagent.exe and zpa_iface.exe processes.
   - **2b** Start the ZENworks Agent installation. For more information, see "Manually Deploying the Agent on Windows" on page 119.

NMAP discovery does not run from a Windows Primary Server that has NMAP installed

Source: ZENworks; Discovery, Deployment, and Retirement.

Possible Cause: On a Windows Primary Server, the NMAP (nmap.exe) is installed in the *%ProgramFiles%*\nmap directory and added to the PATH variable of the user who installs it. Consequently, the ZENworks user is unable to locate nmap.exe by using the PATH variable.

Action: Append the location of the NMAP installation directory (*%ProgramFiles%*\nmap) to the system environment variable PATH of Windows.

How do I enable debug logging?

Source: ZENworks; Discovery, Deployment, and Retirement.

Action: To enable the logs, see TID 3418069 in the Novell Support Knowledgebase (http://support.novell.com/search/kb_index.jsp).

Where do I find the PreAgent log files?

Source: ZENworks; Discovery, Deployment, and Retirement.

Action: Following are the PreAgent log files located in %SystemRoot%\novell\zenworks\bin\

zenpreagent.installerr

`zenpreagent.installlog`

`zenpreagent.installstate`

`ZPA.status`

`cmdline.txt` (The command line executed when the managed agent package was launched.)

After the PreAgent service is installed, all logging information is available in the system application event log.

Refreshing the Deployment page causes the discovery tasks to be repeated

Source: ZENworks; Discovery, Deployment, and Retirement.

Possible Cause: It is normal for a Web browser to resend information in order to refresh a page. ZENworks auto-updates the data on a Deployment page every 5 seconds, so you should not need to refresh the Deployment page after running a discovery task. If you refresh the Deployment page in ZENworks Control Center after running a discovery task, you are asked to confirm the resend in order to refresh the page. If you do so, the discovery task runs again.

Action: Do not refresh the Deployment page after running a discovery task. Instead, exit the page and return to see any changes.

Orphaned and deleted files are not cleaned up from a deployment task that uses a proxy

Source: ZENworks; Discovery, Deployment, and Retirement.

Explanation: Orphaned or to-be-deleted files from a pre-task or post-task action during a deployment task that uses a proxy are not cleaned up.

For example, if you run the deployment task from a Linux server through a Windows Proxy, there is a folder created in the *`zenworks_installation_directory`*`\novell\zenworks\bin\_rfu_cache` directory on the Windows device that contains the pre-task or post-task command file. If you delete the task in ZENworks Control Center, the command file is left on the Windows Proxy device. However, all command files older than five days are removed when another deployment task is run by using the same Windows Proxy.

Action: To immediately delete the orphaned files from the *`zenworks_installation_directory`*`\novell\zenworks\bin\_rfu_cache` directory, you must manually delete it.

Discovery task remains in a pending state if it has a large IP address range

Source: ZENworks; Discovery, Deployment, and Retirement.

Explanation: If a discovery task has an IP address range with more than 50,000 devices, the task is not started. The status of the task remains as **Pending**. If any other discovery or loader task is running simultaneously, it might take a considerable time to complete.

Possible Cause: The ZENworks Loader has insufficient memory to run a task that has a large IP address range.

Action: Do the following:

1. Stop the discovery task that has a large IP address range:
   1a. In the Discovery Tasks panel, select the discovery task that has a large IP address range.
   1b. Click **Action** > **Abort Discovery Task**.
2. Create multiple tasks with the IP address ranges that have fewer than 50,000 devices.
3. (Conditional) If any other discovery or loader task takes a considerable time to complete, restart the ZENworks Loader.
   - **On Windows:** Do the following:
     1. From the Windows desktop **Start** menu, click **Settings** > **Control Panel**.
     2. Double-click **Administrative Tools** > **Services**.
     3. Restart the **Novell ZENworks Loader Service**.
   - **On Linux:** At the console prompt, enter `/etc/init.d/novell-zenloader restart`.
4. Restart the ZENworks Loader.

The device that has the ZENworks Agent installed is not registered in the Management Zone

Source: ZENworks; Registration.

Possible Cause: The device has more than one DNS suffix configured.

Action: Do the following on the device that is not registered in the Management Zone:

1. Reconfigure the device with only one DNS suffix.
2. Manually register the device to the Management Zone.

   For more information on how to manually register the device, see "Manually Registering a Device" on page 85.

Windows XP devices on which ZENworks 11.x Agents are installed cannot be registered to a ZENworks Management Zone

Source: ZENworks; Registration.

Possible Cause: The required cipher suites are not enabled on ZENworks

Action: On the Primary Server, perform the following steps:

1. Add the following ciphers to the `/opt/microfocus/zenworks/share/tomcat/conf/server.xml` file:

TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA

2 Remove the 3DES_EDE_CBC cipher from the `/opt/novell/zenworks/share/jdk/jre/lib/security/java.security` file, by changing the following line:

From

```
jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, DH keySize < 1024, \
    EC keySize < 224, DES40_CBC, RC4_40, 3DES_EDE_CBC
```

To

```
jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, DH keySize < 1024, \
    EC keySize < 224, DES40_CBC, RC4_40
```

3 Restart all the ZENworks services.

Unable to remove or uninstall a registered Macintosh device from the Management Zone

Source: ZENworks; Discovery, Deployment, and Retirement.

Explanation: Uninstalling or removing a previously registered Macintosh agent from the Management Zone gives the following errors:

```
Permission denied.
```

or

```
Not enough privileges to perform the operation.
```

Action: A user needs to have root privileges before running the uninstall script.

1 Log in as `root` or use the `sudo -i` command.
2 Run the uninstall script.

ZENworks Agent installation fails because of a ZENPreAgent and ZPA_Ifacetype initialization exception

Source: ZENworks; Discovery, Deployment, and Retirement

Explanation: When you download and install the pre-agent package, installation fails because of a `ZENPreAgent` and `ZPA_Iface type` initialization exception.

You might get the following error message in the ZENPreAgent.exe-Common Language Runtime Debugging Services window:

```
Application has generated an exception that could not be handled
```

You might get the following error message in the Visual Studio Just-In-Time Debugger window:

```
An unhandled
exception(System.TypeInitializationException)occurred in
ZPA_Iface.exe
```

Possible Cause: A corrupted .NET framework.

Action: To successfully install the pre- agent on the device:

1. Use the .NET clean up utility to uninstall the .NET framework.
2. Re-install the .NET framework.

After installing the ZENworks Agent, you cannot find the /opt directory in the Mac OS X Finder

Source: ZENworks; Discovery, Deployment, and Retirement

Explanation: After installing the ZENworks Agent on a Mac OS X Lion device, you cannot find the `/opt` directory in the Mac OS X Finder.

Action: To make the `/opt` directory visible in the Mac OS X Finder, run the following command:

```
/usr/bin/chflags nohidden /opt
```

ZENworks Agent installation fails on a Mac OS X Lion (version 10.7) device or later

Source: ZENworks; Discovery, Deployment, and Retirement

Explanation: If you install the ZENworks Agent on a Mac OS X Lion (version 10.7) device or later, the installation fails.

Possible Cause: Java 1.6 might not have been installed on the machine.

Action: To install Java 1.6, run the following command:

```
java -version
```

Push deployment fails on a WinXP device with a generic error message

Source: ZENworks; Discovery, Deployment, and Retirement

Explanation: The push deployment fails on a WinXP device, with the following error message:

```
Error: Credentials invalid. Please ensure that Classic file
sharing is enabled on the target device
```

Possible Cause: The failure could be because of one of the following:

- You might have entered wrong credentials and have not enabled the classic file sharing option on the target device.
- A Microsoft issue. For more information, see the CAUSE section in (http://support.microsoft.com/?id=281308).

Action: Do the following:

- Enter correct credentials and ensure that you have enabled classic file sharing on the target device.
- If the generic error message is displayed even after the above conditions are met, you need to add a registry key. For more information, see (http://support.microsoft.com/?id=281308).

Agent Installation is incomplete

Source: ZENworks; Discovery, Deployment, and Retirement.

Explanation: Agent installation fails to complete when you have selected the **Manual** and the **Do not prompt for reboot** option.

Possible Cause: .NET or Windows Installer requires a reboot.

Action: Reboot the device to resume the agent installation.

ZENworks Agent does not work if Macintosh device is upgraded from 10.8 to 10.9

Source: ZENworks; Discovery, Deployment, and Retirement.

Explanation: If ZENworks Agent is installed on Macintosh 10.8 device and Macintosh device is upgraded from 10.8 to 10.9, then ZENworks Agent does not work. Since, Apple's jdk 1.6 have been removed after upgrade.

Action: On Macintosh 10.9 device install Apple's jdk 1.6 and log in again.

ZENworks Agent installation fails when the Windows Imaging Component is not installed on the device

Source: ZENworks; Discovery, Deployment, and Retirement

Explanation: ZENworks agent installation fails with the following error message:

```
Windows Imaging Component, a prerequisite for.NET 4.0 should
be installed manually before the ZENworks Agent
installation.
```

Possible Cause: The Windows Imaging Component which is a prerequisite for .NET 4.0 is not installed on the device.

Action: Install Windows Imaging Component on your device manually and restart the ZENworks agent installation.

Unable to install ZENworks Agent on Windows 2012 Server R2

Source: ZENworks; Discovery, Deployment, and Retirement

Explanation: When you install the ZENworks Agent on a Windows 2012 Server R2 machine, the installation fails with the following error messages:

```
ZENPreAgent.exe has stopped working.
```

```
ZPA_Iface.exe - Application Error.
```

Action: To install the ZENworks Agent, do the following:

1. On the Windows desktop, click **Start** > **Control Panel** > **System and Security** > **System** > **Advanced system settings**.
2. In the System Properties dialog box, click **Advanced** > **Performance Settings**.
3. In the Performance Options dialog box, click **Data Execution Prevention** > **Turn on DEP for essential Windows programs and services only**.
4. Click **OK**, then **Apply**.

Duplicate Device Objects are created when Device Authentication fails during Reconciliation

Source: ZENworks; Discovery, Deployment, and Retirement

Explanation: During device registration if a device is not reconciled due to device authentication failure, duplicate device objects are created for the device in the management zone.

Action: Prevent creation of duplicate device objects for the managed device:

- Ensure that the network adapters of the managed device are connected and have a valid IP address.
- Execute the following zac command on the managed device:

  ```
  zac reregister <GUID of original device object>
  ```

When a Mac patch policy bundle fails, the xauth messages that are launched are not terminated

Source: ZENworks; Discovery, Deployment, and Retirement

Explanation: If you launch a Mac patch policy bundle several times, the policy fails each time with a pop-up message to install xauth. These xauth messages are not terminated even after the bundle error messages disappear. This is because X11 is no longer included as a default install, starting with OS X Mountain Lion 10.8.3.

Action: Before upgrading a ZENworks agent to an OS X Mountain Lion 10.8.3 (or later) device, or before installing ZENworks agent on an OS X Mountain Lion 10.8.3 (or later) device, you need to install the X11 application.

Effective location settings on the managed devices do not work after clearing the cache and refreshing the managed devices

Source: ZENworks; Discovery, Deployment, and Retirement

Explanation: When you clear the cache by using the `zac cc` command and refresh the managed devices by using the `zac ref` command, the effective location settings on the managed devices might not work.

Action: Restart the ZENworks Agent on the managed devices.

Device Serial Number not getting updated on the Device Summary Page

Explanation: After correcting the serial numbers on the managed device, the updated values are not getting updated on the Device Summary page in ZENworks Control Center.

Action: Modify the setting below on all configuration servers in the zone to allow the Serial Number update through a refresh of the managed devices:

1. In the config file, modify the value of the setting "AllowSerialNumberUpdate" from "false" to "true". The config file can be accessed from the following location:
   - **On Windows Servers:** %ZENSERVER_HOME%\services\zenclient-mgmt\conf\registration\
   - **On Linux Servers:** /etc/opt/microfocus/zenworks/tomcat-conf/zenclient-mgmt/registration/
2. Restart the ZENServer service for the changes to take effect.

NOTE: After the device serial numbers are updated in ZCC, it is recommended to reset the value of the `AllowSerialNumberUpdate` setting to `false`. This ensures that the database is not updated during every device refresh, thereby improving the performance of ZENworks.

ZCC displays lost and retired devices in the Devices Logged Into list

Explanation: Devices that are lost or have been retired, are listed in the **Devices Logged Into** panel in ZENworks Control Center, even though users have not logged into these devices for a considerable time period.

Action: To ignore missing and retired devices from the **Devices Logged Into** list in ZCC, add the following Opaque Data Entry in the database:

```
INSERT INTO ZOPAQUEDATA VALUES ((SELECT zuid FROM
zzone),'IGNORE_LOST_AND_RETIRED_DEVICES','true')
```

An error was displayed when you try to re-enroll a ZENworks agent

Explanation: An InternalDataModel exception error message was displayed when you try to re-enroll a ZENworks agent within five minutes of the agent unregistration.

Action: Users can update or delete a ZENworks agent after an interval time of five minutes of unregistration.