opentext™

ZENworks

Management Zone Settings Reference

Legal Notices

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).

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.

About This Guide

This *ZENworks Management Zone Settings Reference* contains information about Management Zone settings that let you control a wide range of functionality for your zone.

Audience

This guide is intended for ZENworks administrators.

Feedback

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

Additional Documentation

ZENworks 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 Web site.

Contents

1 Accessing Configuration Settings

Management Zone settings that apply to devices are inherited by all devices in the zone. You can override zone settings by configuring them on device folders or on individual devices. This allows you to establish zone settings that apply to the largest number of devices and then, as necessary, override the settings on folders and devices.

By default, your zone settings are preconfigured with values that provide common functionality. You can, however, change the settings to best adapt them to the behavior you need in your environment.

- Section 1.1, "Modifying Configuration Settings at the Zone," on page 7
- Section 1.2, "Modifying Configuration Settings on a Folder," on page 8
- Section 1.3, "Modifying Configuration Settings on a Device," on page 9

1.1 Modifying Configuration Settings at the Zone

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

2 In the Management Zone Settings panel, click the settings category (**Content**, **Device Management**, **Discovery and Deployment**, **Event and Messaging**, and so forth) whose settings you want to modify.

3 Click the setting to display its details page.

4 Modify the setting as desired.

For information about the settings, click the **Help** button in ZENworks Control Center or see the following sections:

- "Bundle, Policy and Content" on page 11
- "Device Management Settings" on page 13
- "Discovery and Deployment Settings" on page 15
- "Event and Messaging Settings" on page 17
- "Infrastructure Management Settings" on page 19
- "Inventory Settings" on page 23
- "Asset Management Settings" on page 25
- "Service Desk Registration Settings" on page 27
- "Audit Management" on page 29
- "Security Settings" on page 31
- "Telemetry Settings" on page 35
- "Push Notifications" on page 33

5 When you have finished modifying the setting, click **OK** (or **Apply**) to save your changes.

If the configuration setting applies to devices, the setting is inherited by all devices in the zone unless the setting is overridden at a folder level or a device level.

By default, Management Zone settings are cached on the ZENworks Server and the cache is updated every 10 minutes. Because of this, if a change is made to a zone setting, devices don't receive the changes until the next cache update, which might be as long as 10 minutes.

If you change any of these settings and you want to apply them immediately to a device, you must use the zac command line utility on the device to bypass the ZENworks Server cache and retrieve the new settings. To do so, run the following command on the device:

```
zac ref general bypasscache
```

1.2 Modifying Configuration Settings on a Folder

1. In ZENworks Control Center, click the **Devices** tab.
2. In the Devices panel (on the **Managed** tab), browse for the folder whose settings you want to modify.
3. When you find the folder, click **Details** next to the folder name to display the folder's details.
4. Click the **Settings** tab.
5. In the Settings panel, click the settings category (**Content**, **Device Management**, **Infrastructure Management**, and so forth) whose settings you want to modify.
6. Click the setting to display its details page.
7. Modify the setting as desired.

   For information about the setting, click the **Help** button in ZENworks Control Center or see the following sections:

   - "Bundle, Policy and Content" on page 11
   - "Device Management Settings" on page 13
   - "Discovery and Deployment Settings" on page 15
   - "Event and Messaging Settings" on page 17
   - "Infrastructure Management Settings" on page 19
   - "Inventory Settings" on page 23
   - "Asset Management Settings" on page 25
   - "Service Desk Registration Settings" on page 27
   - "Security Settings" on page 31
   - "Audit Management" on page 29
   - "Telemetry Settings" on page 35
   - "Push Notifications" on page 33
8. When you have finished modifying the setting, click **OK** (or **Apply**) to save your changes.

   The configuration setting is inherited by all devices in the folder, including any devices contained in subfolders, unless the setting is overridden on a subfolder or individual device.

1.3 Modifying Configuration Settings on a Device

1. In ZENworks Control Center, click the **Devices** tab.
2. In the Devices panel (on the **Managed** tab), browse for the device whose settings you want to modify.
3. When you find the device, click the device name to display the its details.
4. Click the **Settings** tab.
5. In the Settings panel, click the settings category (**Content**, **Device Management**, **Infrastructure Management**, and so forth) whose settings you want to modify.
6. Click the setting to display its details page.
7. Modify the setting as desired.

   For information about the setting, click the **Help** button in ZENworks Control Center or see the following sections:

   - "Bundle, Policy and Content" on page 11
   - "Device Management Settings" on page 13
   - "Discovery and Deployment Settings" on page 15
   - "Event and Messaging Settings" on page 17
   - "Infrastructure Management Settings" on page 19
   - "Inventory Settings" on page 23
   - "Asset Management Settings" on page 25
   - "Service Desk Registration Settings" on page 27
   - "Audit Management" on page 29
   - "Security Settings" on page 31
   - "Telemetry Settings" on page 35
   - "Push Notifications" on page 33
8. When you have finished modifying the setting, click **OK** (or **Apply**) to save your changes.

2 Bundle, Policy and Content

The Bundle, Policy and Content section contains the following settings:

Content Blackout Schedule: Define times when content (bundles, policies, configuration settings, and so forth) is not delivered to devices. For more information, see Content Blackout Schedule.

Content Replication: Determine how often content (bundle and policy files) is updated on the ZENworks Primary Servers and Satellites. For more information, see Content Replication.

Primary Server Replication: Lets you specify whether or not new Primary Servers added to the Management Zone include or exclude the content and lets you include or exclude a content server.

Satellite Server Replication: Lets you specify whether or not new Satellite devices added to the Management Zone include or exclude the content and lets you include or exclude a content server.

Older Bundle Version Retain Setting Using this setting, you can configure the maximum number of bundle versions to be retained in the Management Zone. For more information, see Older Bundle Version Retain Settings.

Older Policy Version Retain Setting Using this setting, you can configure the maximum number of policy versions to be retained. For more information, see Older Policy Version Retain Settings.

NOTE: The Bundle, Policy and Content settings are not applicable for mobile devices.

2.1 Older Bundle Version Retain Settings

Using this page, you can configure the number of older bundle versions that you want to retain in ZENworks. The available options include:

- **Retain all versions** Select this option to retain all versions of the bundle. This includes the Published and Sandbox versions.
- **Retain the specified number of older versions** Select this option to specify the number of older versions of the bundle to be retained. The number that you specify should be a positive integer and it should not include the Published and Sandbox versions as they are retained by default.

  For example: If a bundle has 5 versions and if you specify 2, then only the 2 versions prior to the currently published version will be retained along with Published and Sandbox versions. The remaining versions will be deleted.
- **Do not retain any older versions** Select this option if you do not want to retain any older versions. This option retains only the Published and Sandbox versions.

NOTE: The bundle version retention setting can be configured at the zone, folder and bundle levels. The order of precedence is bundle, folder and then zone.

2.2 Older Policy Version Retain Settings

Using this page, you can configure the number of older policy versions that you want to retain in ZENworks. The available options include:

- **Retain all versions:** Select this option to retain all versions of the policy. This includes the Published and Sandbox versions.
- **Retain the specified number of older versions:** Select this option to specify the number of older versions of the policy to be retained. The number that you specify should be a positive integer and it should not include the Published and Sandbox versions as they are retained by default.

  For example: If a policy has 5 versions and if you specify 2, then only the 2 versions prior to the currently published version will be retained along with Published and Sandbox versions. The remaining versions will be deleted.
- **Do not retain any older versions:** Select this option if you do not want to retain any older versions. This option retains only the Published and Sandbox versions.

NOTE: The policy version retention setting can be configured at the zone, folder and policy levels. The order of precedence is policy, folder and then zone.

3 Device Management Settings

The Device Management section contains the following settings:

Local Device Logging: Configure logging of messages to a managed device's local drive. You can determine what severity level messages are logged and when the log file is backed up. You can also determine what severity level messages are sent to the ZENworks server for viewing in ZENworks Control Center. For more information, see Local Device Logging.

Device Refresh and Removal Schedule: Specify how often a device contacts a ZENworks Server to update bundle, policy, configuration, and registration information. You can also specify what to do with a device when it has not contacted a ZENworks Server within a certain number of days. For more information, see Device Refresh Schedule.

iOS Device Settings: Configure the iOS device settings such as Active Lock Bypass. For more information, see Managing Mobile Devices.

ZENworks Agent: Configure uninstall and caching settings for the ZENworks Agent as well as enable or disable specific Agent modules. For more information, see ZENworks Agent.

System Update Agent: Configure System Update behavior on ZENworks Agents. For more information, see System Update Agent.

Registration: Control the settings used when registering devices, including how registered devices are named, whether registration rules are enabled, and whether device objects in ZENworks Control Center can be renamed as they update their registration information. For more information, see Registration.

ZENworks Explorer Configuration: Configure common settings for ZENworks Explorer component of the ZENworks Agent. You can select whether or not you want a bundle to be uninstalled after it is no longer assigned to a device or the device's user. You can also rename the default folder in Windows Explorer, on the Start menu, and in the ZENworks Window where all bundles are placed. For more information, see ZENworks Explorer Configuration.

System Variables: Define variables that can be used to replace paths, names, and so forth as you enter information in ZENworks Control Center. For more information, see System Variables.

Preboot Services: Configure settings for devices that use Preboot Services. For more information, see Preboot Services.

Primary User: Determine how and when a device's primary user is calculated. For more information, see Primary User.

Primary Workstation: Determine how and when a device's primary workstation is calculated. You can also disable the calculation by selecting the **None (Do not calculate, this affects both Primary Workstation and Primary User)** option. For more information, see Primary Workstation.

Dynamic Group Refresh Schedule: Determine how often a dynamic group's criteria are applied to devices in order to update membership in the group. Membership in a dynamic group is determined by applying the dynamic group's criteria to devices. If a device meets the criteria, it is added to the group; you cannot manually add devices to a dynamic group or remove them from a dynamic group. For more information, see Dynamic Group Refresh Schedule.

Power Management Settings: Configure the power management schedule for Intel AMT devices.

Wake-on-LAN: Configure the number of retry attempts to wake up a device and the time interval between the retry attempts. For more information, see Wake-on-LAN.

Remote Management: Configure Remote Management settings, which are a set of rules that determine the behavior or the execution of the Remote Management service on the managed device. For more information, see Remote Management.

NOTE: **Local Device Logging**, **Device Refresh and Removal Schedule**, **iOS Device Settings**, and **Dynamic Group Refresh Schedule** are the only settings that are applicable for mobile devices as well.

4 Discovery and Deployment Settings

The Discovery and Deployment section contains the following settings:

Advertised Discovery Settings: Specify how often you want your ZENworks system to attempt to discover devices on your network that have the ZENworks pre-agent installed. For more information, see Advertised Discovery Settings.

Discovery: Control the settings used during the discovery processes, including the maximum number of discovery requests that can be running at one time and the technologies to use for the discovery. You can also specify IP and SNMP settings used by the WMI (Windows Management Instrumentation) and SNMP discovery technologies. For more information, see Discovery.

Windows Proxy: Specify a managed Windows device in your zone to perform discovery and deployment tasks in place of a ZENworks Server. This is designed primarily to enable ZENworks Servers running on Linux to offload discovery tasks that use Windows-specific discovery technologies such as WMI and WinAPI and deployment tasks that involve Windows managed devices. For more information, see Windows Proxy.

Linux Proxy: Specify a managed Linux device in your zone to perform discovery and deployment tasks in place of a ZENworks Server. This is designed primarily to enable ZENworks Servers running on Windows to offload discovery tasks that use Linux-specific discovery technology such as SSH and deployment tasks that involve Linux managed devices. For more information, see Linux Proxy

Apple Device Enrollment Program: Add a DEP server to link the ZENworks MDM Server with your Apple Deployment Programs account to automate MDM enrollment of multiple corporate-owned iOS devices. For more information, see Enrolling devices using the Apple Device Enrollment Program.

NOTE: **Apple Device Enrollment Program** is the only setting that is applicable for Mobile Devices.

5 Event and Messaging Settings

The Event and Messaging section contains the following settings:

Centralized Message Logging: Configure the settings related to message logging performed by the Primary Server, including automatic message cleanup, e-mail notification, SNMP traps, and UDP forwarding. For more information, see Centralized Message Logging.

Notification Servers: Configure the SMTP server for sending the e-mail notifications to ZENworks administrators. For more information, see SMTP Settings.

Email Notifications: Edit email notifications that are to be sent to mobile devices, in your preferred language. For more information, see ZENworks Mobile Management Reference.

NOTE: **Notification Servers** and **Email Notifications** are the only settings that are applicable for mobile devices as well.

6 Infrastructure Management Settings

The Infrastructure Management section contains the following settings:

Closest Server Default Rule: Define the rule that is used by a device to determine the closest collection, content, and configuration servers when no Closest Server rules have been defined or when none apply. This rule is simply a listing of the servers in the order you want devices to contact them. You cannot add or remove servers from the lists. For more information, see Closest Server Default Rule.

Closest Server Rules: These settings are not applicable for the ZENworks 2020 release.

MDM Servers: Define an MDM Server to allow all mobile devices to communicate with the server at all times. For more information, see Configuring an MDM Server.

HTTP Proxy Settings: Define proxy servers you want to use. In ZENworks, proxy server settings can be configured for the following:

- **ZENworks Agent:** The device's ZENworks Agent connects to the proxy server, then requests resources from a ZENworks Server. The proxy provides the resource either by connecting to the ZENworks Server or by serving it from a cache. To define a proxy server:
  1. Click **Add** to display the Configure HTTP Proxy Settings dialog box.
  2. Fill in the following fields:

     Proxy Address: Specify the IP address of the proxy server.

     Use the supported IP address notation. For example, 172.16.0.0 for IPv4, or 2001:db8::ff00:42:8329 for IPv6.

     Port: Specify the port number on which the proxy server is listening.

     Network Segment (in CIDR notation): Specify the network segment in CIDR notation.

     For example:

     IPv4: 123.45.67.12/16 represents all IP addresses that start with 123.45.

     IPv6: 2001:db8::0/48 represents range of IPv6 addresses from 2001:db8:0:0:0:0:0:0 to 2001:db8:0:ffff:ffff:ffff:ffff:ffff.
- **MDM Servers:** A ZENworks Mobile Device Management (MDM) server communicates with enrolled mobile devices by connecting to a proxy server. For more information, see Configuring an MDM Server in ZENworks Mobile Management Reference.

System Update Settings: Configure how you want to use the System Updates feature, including how often to check for updates, specifying a download schedule, configuring e-mail notifications, and more. For more information, see System Update Settings.

ZENworks News Settings: Configure the server and the schedule for downloading the ZENworks News. For more information, see ZENworks News Settings.

Zone Sharing Settings: Configure the zone sharing settings. For more information, see Zone Sharing Settings

Subscription Settings: Configure the settings for subscriptions. For more information, see Subscription Settings.

YUM Service Settings: Configure the YUM Service Refresh Schedule. For more information, see YUM Service Settings.

Purge Vertica Data Settings: Configure the settings to remove historical trending data for bundle and patch from Vertica. For more information, see Vertica Reference.

OpenID Settings: Configure the settings related to you to an OpenID, For more information, see OpenID Settings

User Source Settings: Configure the settings related to user sources. For more information, see User Source Settings

Adapter Settings: Configure network adapter definitions for use in locations and security policies. For more information, see Adapter Settings

Assignment Optimization Settings: Configure the usage of precomputed assignments for managed devices.

- Assignment Optimization increases the server performance by using precomputed assignments for managed devices. You can run the precomputation by using the zman area command, or specify a schedule.
- You can perform the following configuration on the Assignment Optimization:
  - Enable or Disable the usage of precomputed assignments for managed devices.
  - Specify the interval to compute effective assignments for managed devices.
  - Select a server on which the effective assignments are computed.

    By default, any available server in the Management Zone is used to compute the effective assignment.

NOTE: **MDM Server** is the only setting that is applicable for mobile devices.

IPv6 Usage Settings: Configure the setting for servers to communicate with managed devices through the IPv6 network.

In the IPv6 Usage Settings page, you can either enable or disable the usage of IP v6 addresses in the Closest Server Rules.

1. Log into **ZENworks Control Center**, and then click **Configuration**.
2. In the **Management Zone Settings** panel, click **Infrastructure Management**, and then click the **IPv6 Usage Settings** link.
3. In the **IPv6 Usage Settings** panel, select the **Include servers IPv6 addresses in the Closest Server Rules** check-box.

   NOTE:

   - This setting is applicable only for Primary Servers and Satellite Servers.
   - Primary Server or Satellite Server IPv6 addresses will be added during the next Closest Server Rules computation.
   - If the setting is enabled at zone level, then IPv6 addresses of all Primary Servers and Satellite Servers will be used in the Closest Servers.

- If the setting is enabled at the folder level, then IPv6 addresses will be included for all servers available in that folder.
- By modifying this setting, deployment packages will not be built automatically, you have to rebuild them manually. For more information, see Rebuilding Packages in the ZENworks Discovery, Deployment, and Retirement Reference guide.

4. In the **Preferred Protocol for Communication** drop-down list, select **IPv6**, and click **OK**.

   NOTE:

   - If you select IPv6, the agents will first try using IPv6 addresses available in the Closest Server Rules to communicate with servers, before trying IPv4 addresses.
   - The **Preferred Protocol for Communication** setting can be overridden in the **Locations** page and in the **Network Environments** page.

7 Inventory Settings

The Inventory section contains the following settings:

Inventory: Configure inventory scanning settings, including on-demand scans, first scans, and recurring scans. You can also specify directories to skip when performing scans and identify software applications that are not contained in the ZENworks Knowledgebase. For more information, see Inventory.

Inventory Schedule: Specify when to run an inventory scan, including specifying that scans do not run automatically or specifying a date-specific, recurring, or event-driven scan. For more information, see Inventory Schedule.

Mobile Device Inventory Schedule an inventory scan to collect the mobile device inventory data. For more information see, Collecting Mobile Device Inventory.

Collection Data Form: Configure which demographic data to collect for a device or devices, such as a user's name or telephone, which department the user belongs to, and so on. For more information, see Collection Data Form.

Collection Data Form Schedule: Configure how you send out the Collection Data Form. You can schedule it as part of a regular inventory scan, you can use a Device Quick Task, or you can use the Collection Data Form Schedule. For more information, see Collection Data Form Schedule.

Inventory Only: Configure inventory scan settings for devices in the zone that don't have the ZENworks Agent installed but do have the Inventory Module installed. This type of scan is useful for devices running Windows NT, Windows 95, Windows 98, Windows Me, NetWare, and Mac OS X. For more information, see Inventory Only.

Inventory Only Schedule: Configure when to run an Inventory Only scan. For more information, see Inventory Only Schedule.

Inventory Only Reconciliation: Control whether and how new workstations are reconciled to avoid the possibility of duplicates in the database. When a scan is made of a workstation that is new to the Management Zone, it is assigned an identifier. If the identifier is lost, such as by a disk crash, it is assigned a new identifier during the next scan. Reconciliation allows you to check whether the workstation is already in the database. If it is, the identifier in the database is changed to match the new identifier. For more information, see Inventory Only Reconciliation.

Purge Inventory History: Configures the inventory history purge settings, which allows you to remove the inventory history and application usage data as necessary. For more information, see Purge Inventory History

Inventory Report Rights Configures the default rights at the Management Zone level. These rights are assigned to users according to the default settings. For more information, see Inventory Reports Rights

PRU Schedule: Configure a schedule for PRU availability check, download and deployment. For more information, see PRU Schedule.

Out-of-Band Inventory Reconciliation: Configures how the inventory information from devices that are discovered by out-of-band means must be reconciled. Applies only to devices that have the Inventory module installed and not the entire ZENworks Agent. For more information, see Out-of-Band Inventory Reconciliation

NOTE: Inventory settings are not applicable for mobile devices.

8 Asset Management Settings

The Asset Management section contains the following settings:

Reports: Configure report settings for Asset Management. For more information, see Reports.

Compliance: Set the time of day that license compliance data is refreshed. For more information, see Compliance.

Usage Monitoring: Enable software usage monitoring. For more information, see Usage Monitoring (../../resources/help/am_usagemonitor.html).

Usage Display: Configure whether or not usage data is displayed on License Management pages (Asset Management > License Management tab) in the ZENworks Control Center. For more information, see Usage Display.

User Source: Determines the source (Inventory user data or authoritative user source) from which you can select users to associate with product licenses. For more information, see User Source

Asset Management Report Rights: Configures the default rights at the Management Zone level. These rights are assigned to the user according to the default settings. For more information, see Asset Management Report Rights

License Collection Schedule: Determines the schedule during which the license usage information is collected periodically for the products for which the sources are configured in asset management. For more information see, License Collection Schedule

9 Service Desk Registration Settings

Lets you configure settings related to the registration of Micro Focus Service Desk with ZENworks.

9.1 Register Service Desk Server

Select the **Register Service Desk server** option to register the Micro Focus Service Desk Server with ZENworks.

The registration process requires you to import the Micro Focus Service Desk certificate. You can import the certificate either by directly contacting the Micro Focus Service Desk Server or by manually downloading the certificate to a file and then importing it.

To import the Micro Focus Service Desk certificate, do one of the following:

- **Import NSD certificate by directly contacting the server:**
  1. Select the **Import NSD Certificate by directly contacting the server** option to import the certificate by directly contacting the NSD Server.
  2. In the **Server name/IP address** box, specify the Server name or the IP address.
  3. In the **Port** box, specify the port number.

     NOTE: The default value for the Port is:

     - **443:** If you select the **Use SSL** option
     - **80:** If you do not select the **Use SSL** option

  4. If Micro Focus Service Desk is configured with SSL, select the **Use SSL** option.
  5. Click **Import Certificate**. The certificate is displayed in the Service Desk Certificate panel.
- **Import Certificate from a File:**
  1. Select the **Import Certificate from a file** option if Service Desk has not been enabled with SSL.
  2. Download the certificate from the following URL and save it to a file:

     ```
     http://<ip_address:port>/LiveTime/WebObjects/LiveTime.woa/wa/
     DownloadAction/downloadCertificate
     ```

     NOTE: In the above URL, replace <*ip_address:port*> with the IP address and port of the NSD Server.

  3. Browse to the download location and select the file to import the certificate.
  4. Click on **Import Certificate**. The certificate is displayed in the Service Desk Certificate panel.

10 Audit Management

Audit Management enables you to record various changes and actions that occur in the zone. Once recorded, this information can be audited later for compliance. Audit enables you to centrally monitor activities pertaining to all Primary Servers, Satellite Servers and managed devices.

All these changes and actions are captured as audit events. Each audit event captures information in the form of who did what and when.

- Events Configuration: Lets you configure audit events in ZENworks.
- Local Audit Logging: Lets you enable message logging to local audit files. This feature is available only on Primary Servers.
- Audit Purge Schedule: Lets you configure the audit purge schedule.

For more information about Audit Management, see the ZENworks Audit Management Reference.

11 Security Settings

The Security section contains the following settings:

Security Dashboard: Configure patch compliance criteria and the malware status unknown threshold. For more information, see Security Dashboard.

Patch Subscription Service Settings: Allows you to control the subscription service, define proxy settings, and enter subscription credentials for 3rd-party patch content. For more information, see Patch Subscription Service Settings.

Subscription Service Content Download: Allows you choose and filter what patch content is downloaded. For more information, see Subscription Service Content Download.

Email Notification: Set up the e-mail notification options when the Patch Management Server detects a new patch. For more information, see Email Notification.

Vulnerability Detection Schedule: Allows you to set the default schedule for vulnerability detections. For more information, see Vulnerability Detection Schedule.

Patch Policy Settings: Allows you to set the default settings for patch policy distribution, enforcement, and reboot behavior. For more information, see Patch Policy Settings.

Patch Policy Pre-Install Behavior: Allows you to define when patches are distributed to the agents and how end users are notified of patch installations. For more information, see Patch Policy Pre-Install Behavior.

CVE and Patch Cleanup: Allows you to specify the time period after which CVE and Patch content are deleted. Using this setting you can also control the delaying of superseded and non-superseded patches. For more information, see CVE and Patch Cleanup.

Zone Policy Settings: Specify the default security policies that the ZENworks Agent uses when no other policies settings are available. For more information, see Zone Policy Settings.

Endpoint Security Reporting Settings: Configure how often effective policy reports are uploaded from the Endpoint Security Agent to the ZENworks Server. For more information, see Endpoint Security Reporting Settings.

Antimalware Agent Schedules: Configure zone settings for malware scan schedules and updates to the Antimalware Agent on managed devices. For more information, see Antimalware Agent Schedules.

Antimalware Agent Notifications: Configure the settings for Antimalware generated notifications on managed devices in the management zone. For more information, see Antimalware Agent Notifications.

Antimalware Configuration: Configure the Antimalware Server and the maintenance schedule for malware cleanup and agent installation. For more information, see Antimalware Configuration.

12 Push Notifications

This setting is applicable for only mobile devices. Push notifications can be sent to Android Devices and Apples Devices which will enable communication between the ZENworks Server and the ZENworks Mobile App (for Android devices) or with the MDM profile (for iOS devices) installed on the device. For more information, see Enabling Push Notifications.

13 Telemetry Settings

Telemetry enables Novell to collect statistical data about your usage of ZENworks, thereby ensuring that you have the best possible experience with ZENworks. This chapter provides information on:

13.1 Configuring Telemetry

To configure Telemetry:

1. Log into ZENworks Control Center and navigate to **Configuration > Management Zone Settings > Telemetry Configuration**.
2. (Optional) Click **view** to view the last collected data as an XML.
3. (Optional) Click **download** to download the last collected data as an encrypted file.
4. (Optional) Click **Gather Now** to collect the Telemetry data immediately without waiting for the schedule and upload to Novell.
5. Configure the following settings:
   - **Select the server that will be used to collect and send Telemetry data:** Browse to the server that will be used to collect and send Telemetry to Novell.

     NOTE: It is recommended that you allow an outbound connection for the ZENworks Telemetry server to collect and send Telemetry data to Novell. To send the Telemetry data, you need to ensure that the productfeedback.microfocus.com URL is white-listed for FTP access.

   - **Telemetry Schedule:** Select the day and time to run Telemetry. By default, it is scheduled to run once a week.
   - **Send mandatory data to Novell:** When the super administrator logs into ZENworks, the mandatory data is shared with Novell based on the schedule. Click the mandatory data hyperlink, to view the mandatory information that is collected.
   - **I agree to send optional data as part of the Telemetry scan:** Select this option to send optional data to Novell. Click the optional data hyperlink, to view the additional information that is sent to Novell as part of the Telemetry data.
   - **Name of the organization:** If you want to include your company’s identity information along with the telemetry data, specify your company name.
   - **Email IDs:** Specify email IDs each separated by commas.

- **Server does not have outward connectivity, manually upload the data using these instructions:** If the Telemetry server does not have outward connectivity, or if you want to upload the data manually, then select this check box. This will ensure that ZENworks does not attempt to send the collected information to Novell. Click the instructions hyperlink, follow the steps, and upload the data manually.

13.2 Mandatory Data

The following information is mandatory and it is collected by default from the ZENworks Primary Server and database and sent to Novell:

- Primary Server count by ZENworks version, Docker version and platform (OS, Version, Service Pack)
- Satellite Server count by ZENworks version and platform (OS, Version, Service Pack)
- Agent count by ZENworks version and platform (OS, Version, Service Pack)
- User source type and user count
- Licensed products in the zone
- Mobile device count by OS, Version, Enrollment type and Enrollment mode
- Number of Windows MDM devices enrolled
- ZENworks Reporting Information (ZRSCustomerUniqueID, ZENworksReportingVersion, ZENworksVersion, DomainNames, DomainDBType , DomainVerion, ApplianceRAM, NumberOfAdhocViews, NumberOfReports, NumberOfDashboards, NumberOfActiveReportingUsers)
- Number of Windows workstations with an assigned Antimalware Enforcement policy
- Number of Windows servers with an assigned Antimalware Enforcement policy
- Is Antimalware Enabled
- Number of Primary Servers on which the Security Setting is Enabled
- Is Vertica enabled, node count, vertica usage data, and compliance status

13.3 Optional Data

The following information is optional and to send this information as Telemetry data to Novell, in the Telemetry Configuration page, in ZCC, you need to select the I agree to send optional data as part of the Telemetry scan option:

- Primary Server count by RAM range
- Satellite Server count by RAM range
- Agent count by RAM range
- Database Information - database type, size, top 10 row counts
- Bundles - Number of each type of bundle, number of each type of action
- Policies - Number of each type of policy
- ZAM License Product Count
- ZAM Contract Count

- ZAM Document Count
- ZPM Patch Count
- ZPM Patch Policy Count, preferably with number of patches per policy
- Number of devices on which ZPM is enabled
- Number of patch and CVE dashlets configured
- Location Count
- Network Environment Count
- Location awareness modes (Lite or Full) in the zone
- Client self-defense state in the zone
- Products that are enabled and their license state
- Agent componentsthat are enabled in the zone, and the number of devices on which the components are enabled
- Number of shared bundles and policies
- Number of subscriptions by type
- Type of CA
- Apple Volume Purchase Program and Android Enterprise app counts
- ActiveSync Servers
- Managed device details
- Number of users using non-proxy email server
- Number of users using ZENworks Server as proxy email server
- Number of DEP Servers
- Number of Azure MDM applications
- Number of Windows MDM devices enrolled using Provisioning Package
- Number of Windows MDM devices enrolled using Azure AD
- Number of Windows MDM devices having both ZENworks agent and MDM agent
- Count of Content and Collection Satellite servers based on SSL enabled/disabled
- ZENworks Reporting Information (ApplianceHeapMemory, IsSMTPConfigured, IsLDAPConfigured, NumberOfLDAPAdminGroups , NumberOfScheduledReportsOrJobs)
- Antimalware Database Usage
- Antimalware Database Distribution (Size)
- Number of Malware Threats in last 30 days
- Number of Advanced Authentication Servers
- Number of Administrators with Multi-Factor Authentication Enabled
- Number of Administrator Groups with Multi-Factor Authentication Enabled

13.4 Manually Uploading the Telemetry Data

If you want to manually upload the Telemetry data to the Novell FTP server, perform the following steps:

1. Download the file by clicking the download link in the Telemetry Settings page.
2. Using any FTP client connect to `productfeedback.microfocus.com` with the following credentials:
   - username: anonymous
   - password: blank (optionally, use your email-id).
3. Upload the file to the `stats/zentelemetry` folder.

14 Intune App Management Settings

The Intune App Management section contains the following settings:

Intune App Management: Enables ZENworks to apply protection policies on apps that use the Intune Software Development Kit (SDK). For more information, see Protecting Intune Apps.

Policy Sync Schedule: Configure the schedule to enable ZENworks to sync Intune App Protection policy with Azure. For more information, see Policy Sync Schedule.

15 Windows 10 MDM

The Windows 10 MDM section contains the following settings:

Configure Windows 10 MDM: Enables you to create a provisioning package that is required to enroll Windows 10 devices. For more information, see Windows 10 MDM.