

OpenText™ Endpoint Management 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>.

© Copyright 2008 - 2025 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.

About This Guide

This *OpenText™ Endpoint 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 Endpoint Management 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

Endpoint Management is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the [Endpoint Management documentation Web site](#).

Contents

About This Guide	3
1 Accessing Configuration Settings	7
1.1 Modifying Configuration Settings at the Zone.....	7
1.2 Modifying Configuration Settings on a Folder.....	7
1.3 Modifying Configuration Settings on a Device	8
2 Bundle, Policy and Content	9
2.1 Older Bundle Version Retain Settings	9
2.2 Older Policy Version Retain Settings.....	10
3 Device Management Settings	11
4 Event and Messaging Settings	13
5 Infrastructure Management Settings	15
6 Inventory Settings	17
7 Audit Management	19

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 7](#)
- ♦ [Section 1.3, “Modifying Configuration Settings on a Device,” on page 8](#)

1.1 Modifying Configuration Settings at the Zone

- 1 In Endpoint Management Console, click the **Configuration** tab.
- 2 In the Management Zone Settings panel, click the settings category (**Bundle, Policy and Content, 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 Endpoint Management Console or see the following sections:

- ♦ [“Bundle, Policy and Content” on page 9](#)
 - ♦ [“Device Management Settings” on page 11](#)
 - ♦ [“Event and Messaging Settings” on page 13](#)
 - ♦ [“Infrastructure Management Settings” on page 15](#)
 - ♦ [“Inventory Settings” on page 17](#)
 - ♦ [“Audit Management” on page 19](#)
- 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.

1.2 Modifying Configuration Settings on a Folder

- 1 In Endpoint Management Console, 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 Endpoint Management Console or see the following sections:

- ♦ [“Bundle, Policy and Content” on page 9](#)
- ♦ [“Device Management Settings” on page 11](#)
- ♦ [“Event and Messaging Settings” on page 13](#)
- ♦ [“Infrastructure Management Settings” on page 15](#)
- ♦ [“Inventory Settings” on page 17](#)
- ♦ [“Audit Management” on page 19](#)

- 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 Endpoint Management Console, 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 Endpoint Management Console or see the following sections:

- ♦ [“Bundle, Policy and Content” on page 9](#)
- ♦ [“Device Management Settings” on page 11](#)
- ♦ [“Event and Messaging Settings” on page 13](#)
- ♦ [“Infrastructure Management Settings” on page 15](#)
- ♦ [“Inventory Settings” on page 17](#)
- ♦ [“Audit Management” on page 19](#)

- 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](#).

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 Endpoint Management. 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 Endpoint Management. 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 cloud server for viewing in Endpoint Management Console. For more information, see [Local Device Logging](#).

Device Refresh and Removal Schedule: Specify how often a device contacts a cloud 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 cloud Server within a certain number of days. For more information, see [Device Refresh Schedule](#).

Endpoint Agent: Configure uninstall and caching settings for the Endpoint Agent as well as enable or disable specific Agent modules. For more information, see [Endpoint Agent](#).

Configure Agent Update: Configure System Update behavior on Endpoint Agents. For more information, see [Configure Agent Update](#).

Registration: Control the settings used when registering devices, including how registered devices are named, whether registration rules are enabled, and whether device objects in Endpoint Management Console can be renamed as they update their registration information. For more information, see [Registration](#).

Application Explorer Configuration: Configure common settings for Application Explorer component of the Endpoint 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 Endpoint Management Window where all bundles are placed. For more information, see [Application Explorer Configuration](#).

System Variables: Define variables that can be used to replace paths, names, and so forth as you enter information in Endpoint Management Console. For more information, see [System Variables](#).

4 Event and Messaging Settings

The Event and Messaging section contains the following settings:

Centralized Message Logging: Configure the settings such as, when to clean up message logs and how to forward error messages to OpenText™ Endpoint Management administrators via e-mail notifications, SNMP traps, and UDP.. For more information, see [Centralized Message Logging](#).

5 Infrastructure Management Settings

The Infrastructure Management section contains the following settings:

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

- ♦ **Endpoint Agent:** The device's Endpoint Agent connects to the proxy server, then requests resources from a cloud Server. The proxy provides the resource either by connecting to the cloud 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 to 2001:db8:0:ffff:ffff:ffff:ffff:ffff.

Agent Update Settings: Configure how you want to use the Agent Updates feature, including how stage timeout settings and reboot behavior. For more information, see [System Update Settings](#).

Session Management Settings: Configure the Endpoint Management Console session timeout. If an administrator is not active for the configured value (in minutes), then the session times out.

Throttle Settings: Configure the upload and download throttle value for the Endpoint Agents.

6 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 Endpoint Management 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](#).

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](#).

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](#).

7 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 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 Endpoint Management.
- ♦ Local Audit Logging: Lets you enable message logging to local audit files.

For more information about Audit Management, see the [Endpoint Management Audit Management Reference](#).

