

OpenText™ Endpoint Management

Endpoint Agent 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>.

© 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.

Contents

About This Guide	5
1 Overview	7
2 Registering Devices	9
2.1 Creating Registration Keys and Rules	9
2.1.1 Creating a Registration Key	10
2.1.2 Creating a Registration Rule	12
2.2 Creating Enrollment Token	16
2.3 Modifying the Device Naming Template Used During Registration	18
2.4 Enabling Dynamic Renaming of Devices During Registration	19
2.4.1 Enabling the Setting at the Management Zone	19
2.4.2 Enabling the Setting for a Device Folder	19
2.5 Reconciling Devices with existing Device Objects During Registration	20
2.5.1 Reconciling the Devices	20
2.6 Disabling the Use of Registration Rules	28
2.7 Manually Registering a Device	29
2.7.1 Performing an Initial Registration	29
2.7.2 Reregistering a Device with an Additional Registration Key	30
2.8 Unregistering a Device	30
2.9 Configuring the Agent Security	31
2.9.1 Customizing Security before Deployment	31
2.10 Changing the Target Installation Directory	31
2.11 Manually Deploying the Agent on Windows	32
3 Endpoint Agent Configuration	33
3.1 Viewing the Version of the Endpoint Agent Software and Modules on a Device	33
3.2 Searching for a Specified Version of the Endpoint Agent	33
3.3 Configuring Endpoint Agent Settings after Deployment	34
3.3.1 Configuring Agent Settings on the Management Zone Level	34
3.3.2 Configuring Agent Settings on the Device Folder Level	34
3.3.3 Configuring Agent Settings on the Device Level	34
3.3.4 Endpoint Agent Settings	35
3.4 Configuring Application Explorer	37
3.4.1 Configuring Application Explorer Settings on the Management Zone Level	37
3.4.2 Configuring Application Explorer Settings on the Device Folder Level	38
3.4.3 Configuring Application Explorer Settings on the Device Level	38
3.4.4 Application Explorer General Settings	38
3.5 Configuring the Update Behavior of the Endpoint Agent	39
3.6 Customizing the Look and Feel of the Agent Tray Icon	39
3.6.1 Replacing the Default Agent Tray Icons with the New Customized Icons	40
3.6.2 Replacing the Customized Icons with the Default Agent Tray Icons	40

4	Applications Portal	41
4.1	Overview	41
4.1.1	Launching Applications Portal	41
4.1.2	Launching help	42
4.1.3	About Endpoint Management	42
4.1.4	Launching Applications Portal using the Command Line Switches	42
4.1.5	Launching Technician Portal	43
4.1.6	Refreshing the Agent	43
4.1.7	Searching bundles and folders	44
4.1.8	Viewing bundles and folders using the icons	44
4.1.9	Viewing the bundle progress status	44
4.1.10	Viewing and using the bundle actions	44
4.1.11	Cleaning up the Bundle Shortcuts	45
4.1.12	Accessing options through shortcuts	45
4.1.13	Creating Applications Portal as Shell	45
4.1.14	Managing Favorites	46
5	Technician Portal	47
5.1	Agent	47
5.1.1	Viewing the Agent's Status	47
5.1.2	Registering with a Key	48
5.2	Policies	49
5.2.1	Viewing Policies	49
5.3	Windows Bundles	49
5.3.1	Bundles Versus Applications	49
5.3.2	Accessing Bundles	50
5.3.3	Understanding Bundle Icons	53
5.3.4	Launching a Bundle	54
5.3.5	Postponing a Bundle Download	55
5.3.6	Repairing a Bundle	55
5.3.7	Viewing a Bundle's Properties	55
5.3.8	Uninstalling a Bundle	56
5.3.9	Managing Favorites	56
5.4	Inventory	57
5.4.1	What Is Inventory Information Used For?	57
5.4.2	Scanning the Device	57
5.4.3	Viewing Inventory Information	58
5.4.4	Completing a Collection Data Form	58
5.5	Logging	58
5.5.1	Changing the Message Log Level	58
5.5.2	Clearing the Message Log File	59
5.5.3	Viewing the Message Log File	59
5.5.4	Accessing the Backup Log Files	60
6	Uninstalling Endpoint Agent from Windows Devices	61
6.1	Uninstalling Endpoint Agent from a Windows Device	61
7	Endpoint Management Terminology	63
A	Troubleshooting	65

About This Guide

This guide provides information about the Endpoint Agent, a component of OpenText™ Endpoint Management. For additional information about OpenText™ Endpoint Management and other OpenText products, visit www.opentext.com.

The information in this guide is organized as follows:

- ♦ [Chapter 1, “Overview,” on page 7](#)
- ♦ [Chapter 2, “Registering Devices,” on page 9](#)
- ♦ [Chapter 3, “Endpoint Agent Configuration,” on page 33](#)
- ♦ [Chapter 4, “Applications Portal,” on page 41](#)
- ♦ [Chapter 5, “Technician Portal,” on page 47](#)
- ♦ [Chapter 6, “Uninstalling Endpoint Agent from Windows Devices,” on page 61](#)
- ♦ [Chapter 7, “Endpoint Management Terminology,” on page 63](#)
- ♦ [Appendix A, “Troubleshooting,” on page 65](#)

Audience

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

Feedback

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

Additional Documentation

OpenText 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 [Online documentation website](#).

1 Overview

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

- ♦ Manage policies that determine the behavior of your device.
- ♦ Deliver software, and other files to your device.
- ♦ Take inventory of your device's hardware and software.

Each of these services is provided through the use of modules that plug in to the Endpoint Agent. Depending on the services implemented by the administrator, one or more of these modules might not be active on your device.

The Endpoint Agent connects to a cloud server. The server delivers policies and software for the agent to apply to your device, collects inventory information from the agent, and performs other services related to the management of your device.

2 Registering Devices

When you install the Endpoint 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:

- ♦ [Section 2.1, “Creating Registration Keys and Rules,” on page 9](#)
- ♦ [Section 2.2, “Creating Enrollment Token,” on page 16](#)
- ♦ [Section 2.3, “Modifying the Device Naming Template Used During Registration,” on page 18](#)
- ♦ [Section 2.4, “Enabling Dynamic Renaming of Devices During Registration,” on page 19](#)
- ♦ [Section 2.5, “Reconciling Devices with existing Device Objects During Registration,” on page 20](#)
- ♦ [Section 2.6, “Disabling the Use of Registration Rules,” on page 28](#)
- ♦ [Section 2.7, “Manually Registering a Device,” on page 29](#)
- ♦ [Section 2.8, “Unregistering a Device,” on page 30](#)
- ♦ [Section 2.9, “Configuring the Agent Security,” on page 31](#)
- ♦ [Section 2.10, “Changing the Target Installation Directory,” on page 31](#)
- ♦ [Section 2.11, “Manually Deploying the Agent on Windows,” on page 32](#)

2.1 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 Endpoint Agent on a device, the registration key must be provided. When the device connects to a cloud 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:

- ♦ [Section 2.1.1, “Creating a Registration Key,” on page 10](#)
- ♦ [Section 2.1.2, “Creating a Registration Rule,” on page 12](#)

2.1.1 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:

- ♦ Use the key with the Endpoint 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 [Section 2.7, “Manually Registering a Device,” on page 29](#).

To create a registration key:

- 1 In Endpoint Management Console, 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	<p>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.</p> <p>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.</p> <p>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: <code>/ \ * ? : " ' < > ` % ~</code>.</p> <p>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.</p> <p>Description: Use this field to provide information about the new registration key. This is for your benefit. This field appears only in Endpoint Management Console.</p>
Containment Rules page	<p>Specify the folder in which to place the devices.</p> <p>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.</p>

Wizard Page	Details
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	<p>Specify the groups that devices will become members of when they register.</p> <p>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.</p> <p>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.</p> <p>To specify a group:</p> <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> 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	<p>Specify how you want the to reconcile the existing devices with the new devices that come for registration in the Management Zone.</p> <p>For information, see Section 2.5.1, "Reconciling the Devices," on page 20.</p> <p>Enable reconcile setting if Endpoint Agents are deployed in VDI environment. This device reconcile setting take precedence over zone level device reconcile settings.</p>

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 [Endpoint Management Command Line Utilities Reference](#).


2.1.2 Creating a Registration Rule

- 1 In Endpoint Management Console, 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	<p>Define the rule name and add information to describe the rule.</p> <p>Name: Provide a name for the rule. Users never see the rule name; it displays only in Endpoint Management Console. The name must be different than any other registration key names and must not use any of the following invalid characters: / \ * ? : " ' < > ` % ~.</p> <p>Description: Provide information about the new registration rule. The information appears only in Endpoint Management Console.</p>
Device Criteria page	<p>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.</p> <p>Click Add Filter to add a filter line.</p>

Wizard Page	Details
	<p>Create the filter expression.</p> <p>An expression consists of a criteria option, operator, and value.</p> <p>Example 1:</p> <pre>IPAddress Equal to 123.45.67.89</pre> <p>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.</p> <p>Example 2:</p> <pre>NOT IPAddress Equal to 123.45.67.89</pre> <p>You can use NOT to perform a logical negation of the expression.</p> <p>In the above example, the registration rule is applied only to devices whose IP addresses is not equal to 123.45.67.89.</p> <p>Example 3:</p> <pre>IPAddress Within 123.45.67.89-123.45.67.99</pre> <p>You can use the Within operator to specify the IP address range. Two types of IP address ranges are supported:</p> <ul style="list-style-type: none"> ♦ 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. <p>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.</p> <ul style="list-style-type: none"> ♦ 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

Wizard Page	Details
	<p>If necessary, click Add Filter to create another filter.</p> <p>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 equals Windows Server 2003 AND IPAddress Equal to 123.45.67.89</p> <p>In the above example, the registration rule is applied only to devices whose operating system is Windows 2003 and whose IP address is equal to 123.45.67.89.</p>
Device Criteria page (continued)	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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:</p> <pre> u AND v AND w OR x AND y AND z </pre>
Containment Rules page	<p>Specify the folder in which to place the devices.</p> <p>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.</p>
Device Fields	<p>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.</p>

Wizard Page	Details
Group Membership page	<p>Specify the groups that devices will become members of when they register.</p> <p>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.</p> <p>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 <code>/Devices/Workstations</code> folder, you can only choose workstation groups.</p> <p>To specify a group:</p> <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> a. Click  next to a folder (for example, the <code>Workstations</code> folder or <code>Servers</code> 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 <code>P*</code> finds all groups that start with P, or entering <code>*Accounting</code> 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	<p>Specify how you want the to reconcile the existing devices with the new devices that come for registration in the Management Zone.</p> <p>For information, see Section 2.5.1, “Reconciling the Devices,” on page 20.</p>

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.

2.2 Creating Enrollment Token

The Enrollment Token will be used to authorize devices while registering the devices to the zone. While registering the device, the token will be used to validate if the device is authorized to register with the zone.

To create an Enrollment Token, perform the following:

1. In Endpoint Management Console, click Configuration > Registration
2. In the Enrollment Tokens panel, click New > Enrollment Token.
3. In the New Enrollment Token window, perform the following:
 - ♦ Token Name: Specify a name for the enrollment token.
 - ♦ Enrollment Token: This is an auto-generated 32-character token.
By default, the enrollment token is hidden. Click the eye icon to view the token and click the copy icon to copy the token.
 - ♦ Usage Limit: You can specify how many times the enrollment token can be used to register devices to the zone
 - ♦ Token Expiry Date: You can click the calendar icon to select a date after which the enrollment token should be invalid. Ensure that you select a date that is lesser than six months from the current date.
 - ♦ Usage Notes: Specify a note that provides information related to the usage of the token.
4. Click Add.

NOTE:

- ♦ By default, the usage limit will be set to 1, and the token will expire on the same day at 23:59:59.
 - ♦ The fields cannot be modified if the token is revoked.
 - ♦ The Enrollment Token cannot be modified if the token is used at least once.
-

The following table explains the column information:


Table 2-1 Column Description

Column Name	Description
Enrollment Token Name	Displays the name of the enrollment token.

Column Name	Description
Status	<p>Displays the status of the token. The status can be any one of the following:</p> <ul style="list-style-type: none"> ♦ Active: Indicates that the token is active and can be used to register devices to the zone. ♦ Expired: Indicates that the token has expired and it cannot be used to register devices to the zone. ♦ Limit Utilized: Indicates that the usage limit has been reached and the token cannot be used to register more devices to the zone. ♦ Revoked: Indicates that the token has been revoked and it cannot be used to re-register devices or register new devices to the zone.
Usage Limit	Displays the number of times the token can be used to register devices to the zone. The Usage Limit can be between 1 and 999.
Used Count	Displays the number of times the token was used to register devices to the zone.
Expiry Date	Displays the date and time when the token will expire. The key can have a specific expiry date and it should not be more than six months from the date of token creation.
Usage Note	Displays the usage note, if it was added while creating or editing the token.

Following are some of the additional actions that can be performed on the Enrollment Token:

Task	Steps
Edit token	<ol style="list-style-type: none"> 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 token	<ol style="list-style-type: none"> 1. Select the check box next to the token or folder that you want to delete. 2. Click Action > Delete.
Revoke a key	<ol style="list-style-type: none"> 1. Select the check box next to the token or folder that you want to revoke. 2. Click Action > Revoke.


Task	Steps
Create a folder	<ol style="list-style-type: none"> 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 token	<ol style="list-style-type: none"> 1. Select the check box next to the token. 2. Click Edit > Move. 3. In the Select Folder dialog box, browse for the folder to which you want to move the token, and then click OK.

2.3 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 Endpoint Management Console, 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.

2.4 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 Endpoint Management objects (folders, groups, and so forth), renaming the device does not affect anything other than the name that is displayed in Endpoint Management Console.

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.

- ♦ [Section 2.4.1, “Enabling the Setting at the Management Zone,” on page 19](#)
- ♦ [Section 2.4.2, “Enabling the Setting for a Device Folder,” on page 19](#)

2.4.1 Enabling the Setting at the Management Zone

- 1 In Endpoint Management Console, 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.

2.4.2 Enabling the Setting for a Device Folder

- 1 In Endpoint Management Console, 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.

2.5 Reconciling Devices with existing Device Objects During Registration

Endpoint Management 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 endpoint agent is deployed to these devices, the Endpoint Management Reconcile settings (hostname, serial number, and MAC address) are used to reconcile the new endpoint 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:

- ♦ [Section 2.5.1, “Reconciling the Devices,” on page 20](#)

2.5.1 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 [Endpoint Management Registry Keys Reference](#).

Device Reconciliation Settings

- 1 In Endpoint Management Console, 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 its 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				<p>Success: The attributes of the new device must match all attributes of the existing object for successful reconciliation.</p> <p>Failure: If there is no match with even a single attribute, reconciliation fails and a new device object is created.</p>
				The reconciliation settings are not set and thus, a new device object is created for every new device.
				<p>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.</p> <p>Failure: If only one of the two attributes match, then reconciliation of the new device with the existing object fails.</p>
				<p>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.</p> <p>Failure: If only one of these two attributes match, then reconciliation of the new device with the existing object fails.</p>
				<p>Success: The MAC address, as well as Hostname of the new device, must match the MAC address and Hostname of the existing device object.</p> <p>Failure: If only one of these two attributes match, then reconciliation of the new device with the existing object fails.</p>
				<p>Success: The Serial Number of the new device must match the Serial Number of the existing device object.</p> <p>Failure: If the Serial Number doesn't match, then reconciliation of the new device with the existing object fails.</p>

	Serial number (SN)	Mac Address	Hostname	Expected
Differentiation Enabled				<p>Success: The MAC address of the new device must match the MAC address of the existing device object.</p> <p>Failure: If the MAC address doesn't match, then reconciliation with the existing object fails.</p>
				<p>Success: The Hostname of the new device must match the Hostname of the existing device object.</p> <p>Failure: If the Hostname doesn't match, then reconciliation of the new device with the existing object fails.</p>
		 (multiple≥2)		<p>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.</p> <p>Failure: If none of the MAC addresses match, reconciliation fails.</p>
		 (same≥2)		<p>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.</p>
			 (same≥2)	<p>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.</p>

	Serial number (SN)	Mac Address	Hostname	Expected
Differentiation Disabled				<p>Success: New device attributes must match with either the attributes of the existing object for successful reconciliation.</p> <p>Failure: If none of the attributes match, reconciliation fails and a new device object is created.</p>
				<p>If the settings for device reconciliation are not set, then a new device object is created for every new device.</p> <p>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.</p>
				<p>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.</p> <p>Failure: If neither of these two attributes match, then reconciliation of the new device with the existing object fails.</p>
				<p>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.</p> <p>Failure: If neither of these two match, then reconciliation of the new device with the existing object fails.</p>

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

2.6 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 Endpoint Management Console, 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 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 [Endpoint Management Registry Keys Reference](#).

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

Endpoint Management Console 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 <code>zac add-reg-key</code> 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 <code>zac add-reg-key</code> command is executed.

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

2.7 Manually Registering a Device

A device is automatically registered when the Endpoint 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 Endpoint Management database. The Endpoint 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 Endpoint Agent command line utility (`zac`).

The following sections provide instructions:

- ♦ [Section 2.7.1, “Performing an Initial Registration,” on page 29](#)
- ♦ [Section 2.7.2, “Reregistering a Device with an Additional Registration Key,” on page 30](#)

2.7.1 Performing an Initial Registration

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

```
register (reg) [-g] [-k <key>] <Cloud Server URL>
```

Examples:

To register a device using the enrollment token and subscription name, run the following command:

```
zac register -a <EnrollmentToken> -sn <subscriptionname> https://abcd.opentext.com
```

If you run the command without specifying the parameters, then you will be prompted to provide enrollment token and subscription name.

To register using a key, run the following command:

```
zac register -k mykey https://abcd.opentext.com
```

To generate a new device GUID and then register, run the following command:

```
zac register -g https://abcd.opentext.com
```

2.7.2 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.

2.8 Unregistering a Device

A device is automatically unregistered when the Endpoint 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 Endpoint Agent command line utility (zac):

- 1 At the device, open a command prompt.

- 2 Enter the following command:

```
zac unr [-f]
```

For example:

To force a device to unregister locally when a server cannot be contacted:

```
zac unr -f
```

Unregistering a device by using the Unregister Device action

To manually unregister a device, do the following:

- 1 Log in to Endpoint Management Console.
- 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 Endpoint Management Console. However, you can use the `zac reg` command to reregister the device.
- 4 Click **Action** > **Unregister Device**.

2.9 Configuring the Agent Security

You can configure whether or not to allow users to uninstall the Endpoint 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 Endpoint Agent is deployed and after:

- ♦ [Section 2.9.1, “Customizing Security before Deployment,” on page 31](#)

2.9.1 Customizing Security before Deployment

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

2.10 Changing the Target Installation Directory

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

On a Windows device: `Windows_drive:\Program Files\OpenText\Endpoint Agent\bin`

To install the agent to a different location, you can create an `%ENDPOINT_AGENT_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:\Program Files\Corporate\`

`d:\Applications\OpenText\EndpointAgent`

2.11 Manually Deploying the Agent on Windows

The Endpoint agent can be manually download from the server and installed on the device.

- 1 Make sure the device meets the necessary requirements. For details see “Managed Device Requirements” in the [Endpoint Management System Requirements](#).
- 2 On the target device, open and log into the Endpoint Management Console.
- 3 Click Home, and then click Download Admin Tools.
- 4 Click Endpoint Agent, and then click 64 bit to download the agent package.
- 5 Launch the package on the device.
- 6 In the Device Registration page, specify the Endpoint Management server details.

Example: abcd.opentext.com

- 7 In the Registration Details page, specify the Subscription Name and Enrollment Token details and then click Next.

If you do not have Subscription Name and Enrollment Token details, then click Skip to install the agent.

If you specify invalid subscription name or enrollment token, the following error will be displayed:

You have specified invalid registration details. Check the Subscription Name and Enrollment Token.

If you exceed the number of attempts, then you will not be able to register the device in the zone.

- 8 After completing the installation, you will be prompted to reboot the device.

The following 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, it is registered in the Management Zone and the Endpoint Management icon is placed in the notification area (system tray).

3 Endpoint Agent Configuration

- ♦ Section 3.1, “Viewing the Version of the Endpoint Agent Software and Modules on a Device,” on page 33
- ♦ Section 3.2, “Searching for a Specified Version of the Endpoint Agent,” on page 33
- ♦ Section 3.3, “Configuring Endpoint Agent Settings after Deployment,” on page 34
- ♦ Section 3.4, “Configuring Application Explorer,” on page 37
- ♦ Section 3.5, “Configuring the Update Behavior of the Endpoint Agent,” on page 39
- ♦ Section 3.6, “Customizing the Look and Feel of the Agent Tray Icon,” on page 39

3.1 Viewing the Version of the Endpoint Agent Software and Modules on a Device

- 1 In Endpoint Management Console, click the **Devices** tab.
- 2 Click **Workstations**, and then click the underlined link for the desired device to view the Endpoint Agent software version on a workstation.
- 3 In the General section, view the version in the **Endpoint Agent Version** row.

3.2 Searching for a Specified Version of the Endpoint Agent

For upgrading or troubleshooting purposes, you can use the Advanced Search feature to display a list of devices in your zone that have a specified version of the Endpoint 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 Endpoint Agent installed, do one of the following in Endpoint Management Console:
 - ♦ To search for all devices, click the **Devices** tab.
 - ♦ 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/Agent Version** from the drop-down list, then click **OK**.

3.3 Configuring Endpoint Agent Settings after Deployment

By default, the Endpoint Agent is deployed with the features selected at the Management Zone level in the Agent Features panel of Endpoint Management Console. After the deployment, you can configure the agent's cache, set retry settings, and select whether to let users uninstall the agent. The User Management feature is only supported on Windows managed devices across all the OpenText Endpoint Management products.

You can configure settings at three levels:

- **Management Zone:** The setting applies to all devices in the Management Zone.
- **Device Folder:** The setting applies to all devices contained within the folder or its subfolders. It overrides the Management Zone setting.
- **Device:** The setting applies only to the device for which it is configured. It overrides the settings established at the Management Zone and folder levels.

The following sections contain more information:

- [Section 3.3.1, “Configuring Agent Settings on the Management Zone Level,” on page 34](#)
- [Section 3.3.2, “Configuring Agent Settings on the Device Folder Level,” on page 34](#)
- [Section 3.3.3, “Configuring Agent Settings on the Device Level,” on page 34](#)
- [Section 3.3.4, “Endpoint Agent Settings,” on page 35](#)

3.3.1 Configuring Agent Settings on the Management Zone Level

- 1 In Endpoint Management Console, click the **Configuration** tab.
- 2 In the **Management Zone Settings** panel, click **Device Management**.
- 3 Click **Endpoint Agent**.
- 4 Fill in the fields. For more information, see [Section 3.3.4, “Endpoint Agent Settings,” on page 35](#).
- 5 Click **OK** to apply the changes.

3.3.2 Configuring Agent Settings on the Device Folder Level

- 1 In Endpoint Management Console, click the **Devices** tab.
- 2 Click the **Servers** or **Workstations** folder.
- 3 Click **Details** next to the folder for which you want to configure settings.
- 4 Click the **Settings** tab, click **Device Management**, then click **Endpoint Agent**.
- 5 Fill in the fields. For more information, see [Section 3.3.4, “Endpoint Agent Settings,” on page 35](#).
- 6 Click **OK** to apply the changes.

3.3.3 Configuring Agent Settings on the Device Level

- 1 In Endpoint Management Console, click the **Devices** tab.
- 2 Click the **Servers** or **Workstations** folder.
- 3 Click the device for which you want to configure settings.

- 4 Click the **Settings** tab, click **Device Management**, then click **Endpoint Agent**.
- 5 Fill in the fields. For more information, see [Section 3.3.4, “Endpoint Agent Settings,” on page 35](#).
- 6 Click **OK** to apply the changes.

3.3.4 Endpoint Agent Settings

The following sections provide details about the configuration settings available for the Endpoint Agent. Each section assumes that you have accessed the settings at the level where you want the settings applied.

- ♦ [“Agent Security” on page 35](#)
- ♦ [“General” on page 35](#)
- ♦ [“Agent Preferences” on page 37](#)

Agent Security

You can configure whether or not to allow users to uninstall the Endpoint 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.

If you are configuring the Endpoint Agent settings on a device folder or a device, click **Override settings** to activate the settings.

The following setting applies to all versions of the Endpoint Agent:

- ♦ **Allow Users to Uninstall the Endpoint Agent:** Enable this option to allow users to perform a local uninstall of the Endpoint Agent. If this option is disabled, the agent can only be uninstalled through the Endpoint Management Console.

General

You can configure the Endpoint Agent’s cache and agent retry settings.

If you are configuring the Endpoint Agent settings on a device folder or a device, click **Override settings**.

The following settings can be configured:

- ♦ **Cache Life:** The Endpoint Agent’s cache directory contains content data used by the agent. Each piece of data, referred to as a cache entry, is stored in the cache database.

When a cache entry is added to the cache database, it is assigned a creation time and an expiration time. The creation time is simply the time it was added to the database. The expiration time is the creation time plus the number of hours specified by the **Cache Life** setting (by default, 336 hours or 14 days). For example, suppose that a cache entry is added on June 10 at 3:00 p.m. With the default **Cache Life** setting, the expiration time is set to June 24 at 3:00 p.m.

The agent does not attempt to update a cache entry until after the entry’s expiration time. At that point, the agent updates the cache entry the next time it contacts the cloud server to refresh its information.

NOTE: Updates to expired cache entries occur only for cache entries that are content-related (bundles, policies, configuration settings, registration settings, and so forth). Updates to cache entries that are event-related (remote management, inventory, reporting, and so forth) only occur at the time the event takes place on the device.

A higher **Cache Life** setting reduces the traffic load on your network because cache entries are refreshed less frequently. A lower setting provides newer information but increases the traffic load.

This setting affects only how often the agent requests updates to a cache entry. Cache entries can also be updated before their expiration time if information is changed in Endpoint Management Console that causes the information to be pushed from the cloud server to the agent.

- ♦ **Cache Orphaning Threshold:** Over a period of time, it is possible for entries to be inserted in the cache database but not removed. This can cause the cache to grow unnecessarily.

An orphan is an entry that is inserted into the cache but not accessed within the number of days specified by the **Cache Orphaning Threshold** setting. For example, suppose that a cache entry is accessed on July 1 at 10:00 a.m. Without the default **Cache Orphaning Threshold** setting (30 days), the entry becomes an orphan if it is not accessed again before July 31 at 10:00 a.m.

A higher **Cache Orphaning Threshold** setting ensures that infrequently accessed information is not removed from the cache database. A lower setting can reduce the cache size.

- ♦ **Times to Retry Requests to a Busy Server:** Lets you specify the number of times that the agent retries a request to a busy server before considering the server as bad instead of busy.

The default value is 15. The maximum value that you can specify is 20.

- ♦ **Initial Retry Request Wait:** The **Initial Retry Request Wait** setting lets you specify the initial amount of time that the agent waits before retrying a Web service request after receiving a busy response from the server. The wait time increases by one second with every busy response. The default setting is four seconds. The maximum value that you can set is ten seconds. Each subsequent request is incremented by one second.

For example, suppose that you leave this setting at the default (four seconds). After receiving a busy response from the server, the agent waits four seconds for the first retry attempt. If the server is still busy, the agent waits five additional seconds ($4 + 1$) before making the second retry attempt. The third retry attempt is 15 seconds after the initial retry attempt ($4 + 5 + 6$). The time increments until the value specified in the **Maximum Retry Request Wait** setting is reached. The retry attempts stop when the value specified in the **Times to Retry Requests to a Busy Server** setting is reached.

- ♦ **Maximum Retry Request Wait:** Lets you specify the maximum amount of time to wait before retrying a Web service request after receiving a busy response from the server.

The default setting is 16 seconds. The maximum value that you can specify is 20 seconds.

Agent Preferences

To provide optimal performance the default status upload frequency of the Endpoint Agent is 30 minutes. You can choose to override the default status upload frequency by configuring the following preferences on a Windows managed device:

- ♦ [“Changing the Default Status Upload Frequency of the Endpoint Agent on a Windows Managed Device” on page 37](#)

Changing the Default Status Upload Frequency of the Endpoint Agent on a Windows Managed Device

- 1 On a Windows managed device, create the `StatusSenderConfig.xml` file in `<CONF_DIR>`.
- 2 Open `<CONF_DIR>/StatusSenderConfig.xml` in a text editor.
- 3 Provide the following values:

```
<configuration>
<StatusSender>
  <Parameter Name="SleepTime" Value="milliseconds"/>
</StatusSender>
</configuration>
```

3.4 Configuring Application Explorer

You can configure common settings at three levels for the Application Explorer component of the Endpoint Agent:

- ♦ **Management Zone:** The settings are inherited by all device folders and devices.
- ♦ **Device Folder:** The bundle settings are inherited by all devices contained within the folder or its subfolders.
- ♦ **Device:** The bundle settings apply only to the device for which they are configured.

The following sections contain more information:

- ♦ [Section 3.4.1, “Configuring Application Explorer Settings on the Management Zone Level,” on page 37](#)
- ♦ [Section 3.4.2, “Configuring Application Explorer Settings on the Device Folder Level,” on page 38](#)
- ♦ [Section 3.4.3, “Configuring Application Explorer Settings on the Device Level,” on page 38](#)
- ♦ [Section 3.4.4, “Application Explorer General Settings,” on page 38](#)

3.4.1 Configuring Application Explorer Settings on the Management Zone Level

- 1 In Endpoint Management Console, click the **Configuration** tab.
- 2 Click the **Device Management** tab.
- 3 Click **Application Explorer Configuration**.

- 4 Fill in the fields. For more information, see [Section 3.4.4, “Application Explorer General Settings,” on page 38.](#)
- 5 Click **OK** to apply the changes.

3.4.2 Configuring Application Explorer Settings on the Device Folder Level

- 1 In Endpoint Management Console, click the **Devices** tab.
- 2 Click the **Servers** or **Workstations** folder.
- 3 Click **Details** next to the folder for which you want to configure settings.
- 4 Click the **Settings** tab, click **Content**, then click **Application Explorer Configuration**.
- 5 Click **Override Settings**.
If you are configuring the settings on a device folder or a device, you need to click **Override Settings** before you can select any of the settings.
- 6 Fill in the fields. For more information, see [Section 3.4.4, “Application Explorer General Settings,” on page 38.](#)
- 7 Click **OK** to apply the changes.

3.4.3 Configuring Application Explorer Settings on the Device Level

- 1 In Endpoint Management Console, click the **Devices** tab.
- 2 Click **(Details)** against the **Servers** or **Workstations** folder.
- 3 Click the device for which you want to configure settings.
- 4 Click the **Settings** tab, click **Device Management**, and then click **Application Explorer Configuration**.
- 5 Click **Override Settings**.
If you are configuring the settings on a device folder or a device, you need to click **Override Settings** before you can select any of the settings.
- 6 Fill in the fields. For more information, see [Section 3.4.4, “Application Explorer General Settings,” on page 38.](#)
- 7 Click **OK** to apply the changes.

3.4.4 Application Explorer General Settings

You can use the Application Explorer General panel to configure Application Explorer to uninstall a bundle that is no longer assigned to the device, specify the number of days to wait before uninstalling the bundle, and specify the default folder that Application Explorer uses:

- ♦ **Unassigned Bundles:** 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.

If you choose to uninstall the bundle, select the number of days to wait before uninstalling the application. Specify 0 if you want the application to be uninstalled as soon as it is no longer assigned to the device or user.

- ♦ **Default Folder:** Application Explorer displays a default folder in Windows Explorer, on the Windows Start menu and in the Application Explorer Window. Bundles are placed in the default folder unless you override the default folder by specifying a folder on a bundle's Summary page. The default folder can be renamed to meet the needs of your organization. Click **Edit** to change the folder name.
- ♦ **Disable Icon Overlays:** Select this option to disable both the status indicator overlay and the red Agent Tray Icon overlay from a bundles icon.

NOTE: After choosing to disable the icon overlays, you must do the following on a Windows device for the bundle icon changes to be effective on the device:

- ♦ **For the Desktop, System Tray, Start Menu, and Quick Launch bundle icons:** Logout and log into the device again.
 - ♦ **For the Applications Portal Window bundle icons:** Close the Applications Portal Window and launch it again.
-

- ♦ **Enable the display of folders in the Start Menu:** Select this option to enable the display of folders in the Windows Start Menu.


In the Start Menu, bundles are displayed under the immediate parent folder, without including the folder hierarchy.

3.5 Configuring the Update Behavior of the Endpoint Agent

You can configure the update behavior on the Endpoint Agent that resides on managed devices. This includes if a dialog box displays on the managed devices prompting users to allow the system update or a required boot after a system update is applied. Users can either postpone the update or reboot. You can also provide custom text in the prompts that you choose to display.

For more information, see [“Configuring the Agent Update Behavior of the Endpoint Agent”](#) in the *Endpoint Management Agent Updates Reference*.

3.6 Customizing the Look and Feel of the Agent Tray Icon

The Agent Tray Icon  is located in the Windows notification area of the managed device. This is a default static icon. When the managed device is refreshed, the default static icon is replaced by the default animated icons.

Endpoint Management allows you to change the look and feel of the Agent Tray Icon. You can choose to replace the default icons with different icons, such as your company logo.

- ♦ [Section 3.6.1, “Replacing the Default Agent Tray Icons with the New Customized Icons,” on page 40](#)
- ♦ [Section 3.6.2, “Replacing the Customized Icons with the Default Agent Tray Icons,” on page 40](#)

3.6.1 Replacing the Default Agent Tray Icons with the New Customized Icons

To replace the following default Agent Tray Icons, you need 16x16-pixel PNG files:

- ♦ **Customized Static Icon:** The static icons named `loggedIn_zappTray.png` and `zenworks.png`.
- ♦ **Customized Animated Icons** One or more custom animated icons named `refresh_x.png`, where *x* represents a single and double-digit numeric value that can range from 1 to 12. These icons are displayed when the managed device is refreshed.

You must have at least one animated icon. If you choose to have more than one animated icon, the icons are displayed sequentially based on the value of *xx* in the filename. For example, if you have the `refresh_1.png` and `refresh_2.png` icons, `refresh_1.png` is displayed first followed by `refresh_2.png`.

Before changing the default icons with the customized icons, ensure that you rename or back up the default icons.

To replace the default icons on a managed device:

- 1 Copy the customized static and animated icons `loggedIn_zappTray.png`, `zenworks.png`, and `refresh_x.png` icons to the `Program Files\OpenText\Endpoint Agent\zapp\assets` directory.
- 2 Stop the **zapp.exe** process by using the Windows Task Manager.
- 3 Go to the `Program Files\OpenText\Endpoint Agent\bin` directory and double-click `zapp-launcher.exe` to restart the process.

3.6.2 Replacing the Customized Icons with the Default Agent Tray Icons

- 1 Delete the customized icons from the `Program Files\OpenText\Endpoint Agent\zapp\assets` directory.
- 2 Stop the **zapp.exe** process by using the Windows Task Manager.
- 3 Copy the default Agent Tray Icons to `Program Files\OpenText\Endpoint Agent\zapp\assets` directory.
- 4 Restart `Program Files\OpenText\Endpoint Agent\bin\zapp-launcher.exe`.

4 Applications Portal

4.1 Overview

Applications Portal leverages the capabilities of a unified endpoint management solution to provide an enhanced user experience. The features include:

- ♦ A brand new user interface that serves as a single place for all Endpoint Management user functionality on Windows.
- ♦ An integrated search to help you find the app of your choice. The search includes full and split pattern matching by name, description, and contact information.
- ♦ You can pin and unpin bundles to the Desktop, Taskbar, and Start menu tiles.

This document includes the following:

- ♦ [Section 4.1.1, “Launching Applications Portal,” on page 41](#)
- ♦ [Section 4.1.2, “Launching help,” on page 42](#)
- ♦ [Section 4.1.3, “About Endpoint Management,” on page 42](#)
- ♦ [Section 4.1.4, “Launching Applications Portal using the Command Line Switches,” on page 42](#)
- ♦ [Section 4.1.5, “Launching Technician Portal,” on page 43](#)
- ♦ [Section 4.1.6, “Refreshing the Agent,” on page 43](#)
- ♦ [Section 4.1.7, “Searching bundles and folders,” on page 44](#)
- ♦ [Section 4.1.8, “Viewing bundles and folders using the icons,” on page 44](#)
- ♦ [Section 4.1.9, “Viewing the bundle progress status,” on page 44](#)
- ♦ [Section 4.1.10, “Viewing and using the bundle actions,” on page 44](#)
- ♦ [Section 4.1.11, “Cleaning up the Bundle Shortcuts,” on page 45](#)
- ♦ [Section 4.1.12, “Accessing options through shortcuts,” on page 45](#)
- ♦ [Section 4.1.13, “Creating Applications Portal as Shell,” on page 45](#)
- ♦ [Section 4.1.14, “Managing Favorites,” on page 46](#)

4.1.1 Launching Applications Portal

You can launch Applications Portal by using any of the following options:

- ♦ Click the Agent Tray Icon from the system tray.
- ♦ Press the Windows logo key, and then type **Applications Portal**.

4.1.2 Launching help

You can launch Applications Portal help by using any of the following options:

- ♦ Select the **Hamburger** menu and click **Help**.
- ♦ On the system tray, right-click the **Agent Tray Icon** and click Help.

4.1.3 About Endpoint Management

You can view Endpoint Management details such as build version, agent version, configuration location, device name, and user name:

- ♦ Select the **Hamburger** menu and click **About**.

4.1.4 Launching Applications Portal using the Command Line Switches

Open the command prompt and execute the `zapp-launcher` command. By default, ZAPP-Launcher is started from the **Run** registry keys.

For example: To disable the **Close** option for Applications Portal, append the `/s` option to the following registry keys:

For 32-bit Operating Systems:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
```

```
ZAPP=C:\Program Files\OpenText\Endpoint Agent\bin\zapp-launcher.exe /runonce /s
```

Registry key Type: REG_EXPAND_SZ

For 64-bit Operating Systems:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run]
```

```
ZAPP=C:\Program Files\OpenText\Endpoint Agent\bin\zapp-launcher.exe /runonce /s
```

Registry key Type: REG_EXPAND_SZ

IMPORTANT: ♦ If Applications Portal is already running and you want to launch it again with other command line parameters, kill all instances of Applications Portal and then execute `zapp-launcher` with the new parameters.

- ♦ Command line parameters set before an agent update is retained after agent is updated.
-

The following command line switches can be used when starting the Applications Portal Window using `zapp-launcher`:

Switch	Description
/? Example: zapp-launcher /?	Displays Help. If Applications Portal is launched with invalid parameters, help is displayed.
/max Example: zapp-launcher /max	Displays the Applications Portal window maximized when first loaded, overriding the window state (size and position) that was saved when exiting the previous Applications Portal window session.
/min Example: zapp-launcher /min	Displays the Applications Portal window minimized when first loaded, overriding the window state (size and position) that was saved when exiting the previous Applications Portal window session.
/norm Example: zapp-launcher /norm	Displays the Applications Portal window in its original state when first loaded, and maintains the window state (size and position) that was saved when exiting the previous Applications Portal window session.
/runonce	This command is used for internal purposes and it is located at HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. Ensure that you do not delete it.
/s Example: zapp-launcher /s	Enables the Applications Portal window to behave like the Windows shell. For example, on the Hamburger menu, the standard Windows Power Options are displayed. The Close option is not available. This is not a true replacement for the Windows shell. If users minimize the Applications Portal window, they have access to the normal desktop.
/d Example: zapp-launcher /d	Displays the Applications Portal window without the Help option on the Hamburger menu and System Tray. So, you cannot view the help.

4.1.5 Launching Technician Portal

To launch Technician Portal: Right-click the **Agent Tray Icon** and click **Technician Portal**

4.1.6 Refreshing the Agent

You can refresh the agent by using any of the following options:




- Select the **Hamburger** menu and click **Refresh**.
- Click the **Refresh** icon in the status bar.
- Right-click the **Agent Tray** icon and click **Refresh**.

4.1.7 Searching bundles and folders

The Search option enables you to search the required bundles and folders with name, description, and contact information. Even if a particular folder is selected the search is performed across the application.

4.1.8 Viewing bundles and folders using the icons

The following views are available:

- ♦ : Icon View displays icons of bundles and folders.
- ♦ : Detailed View displays folders and bundle information such as name, version, and status. You can sort the bundle as required.
- ♦ : Toggle Tree View displays and hides the left pane folder view.

4.1.9 Viewing the bundle progress status

To view the bundle progress status:

- 1 Select the **Hamburger** menu and click **View Progress**.

In the **Progress Status** you can retry on bundle failure, pause and resume while downloading bundle content.

You can also clear the bundle progress by right-clicking the progress status and click **Clear**.

4.1.10 Viewing and using the bundle actions

To view and use the bundle actions:

- 1 Select a bundle and right-click.
 - ♦ **Open**: Performs install and launch actions. If any install action set is specified in a bundle, then it installs else it executes launch action set, if specified.
 - ♦ **Repair**: Re-runs the install action set. This option is enabled only if a bundle has the install action. This is same as **Verify** in NAL.
 - ♦ **Uninstall**: If this option is enabled for a bundle it will undo the install actions. This option is enabled only if administrator has configured the uninstall action.
 - ♦ **Send to Desktop**: Creates a shortcut of bundle on the Desktop.
 - ♦ **Set as Favorite**: Marks a bundle as a Favorite.
 - ♦ **Remove as Favorite**: Removes the Favorite tag from a bundle.
 - ♦ **Pin to Start**: Pins the bundle to the Start.
 - ♦ **Pin to Taskbar**: Pins the bundle to the Taskbar.
 - ♦ **Remove from Desktop**: Removes the bundle from the Desktop.
 - ♦ **Unpin from Start**: Unpins the bundle from the Start.
 - ♦ **Unpin from Taskbar**: Unpins the bundle from the Taskbar.

- ♦ **Properties:** Displays bundle details such as name, status, description, contacts, and failure messages in case of system requirements failure.

IMPORTANT: The **Pin** and **Unpin** options are not displayed for a location if the bundle is already assigned to the same location by the administrator. Start and taskbar options are not displayed if the administrator sets the **Allow the end user to pin bundles** option as **No** or **Unconfigured** in the Application Explorer Configuration Policy or if there are no Application Explorer Configuration Policies.

4.1.11 Cleaning up the Bundle Shortcuts

To clean up the bundle shortcuts that are created by an Endpoint Management user:

- 1 Select the **Hamburger** menu and click **Cleanup user settings**.
- 2 In the Warning window, select **Yes**.

4.1.12 Accessing options through shortcuts

You can use the following shortcuts:

- ♦ **Tab:** To navigate between panes (Toggle Tree View, Icon View, and Detailed View), folders, and bundles. After an element is highlighted, press **Enter** to perform the related operation.
- ♦ **Shift + Tab:** To navigate through the Hamburger menu, Toggle Tree View, Icon View, Detailed View, Properties, Progress status, and Status bar.

NOTE: The **Tab** and **Shift + Tab** keys enable you to navigate forward and back respectively.

- ♦ **Arrow Keys:** To navigate through folders and bundles.
- ♦ **Ctrl + Shift:** Use the following keys for different views:
 - ♦ `Ctrl + shift + 1` Toggle Tree View
 - ♦ `Ctrl + shift + 2` Icon View
 - ♦ `Ctrl + shift + 3` Detailed View
- ♦ **Ctrl + F:** Go to the **Search** window.

4.1.13 Creating Applications Portal as Shell

To create Applications Portal as Shell:


- 1 Open the Registry Editor.
- 2 Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell`
- 3 Change Shell to `Program Files\OpenText\Endpoint Agent\bin\zapp-launcher.exe`
- 4 Log off and log into Windows.

In the Shell mode, the following additional **Windows Power** options are displayed:

- ♦ Logout
- ♦ Restart
- ♦ Shutdown

NOTE: When Applications Portal is launched as Shell it will have both the minimize and maximize buttons. When you click the minimize button, the Applications Portal screen is resized and centered on the desktop screen.

4.1.14 Managing Favorites

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

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

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

5 Technician Portal

- ♦ [Section 5.1, “Agent,” on page 47](#)
- ♦ [Section 5.2, “Policies,” on page 49](#)
- ♦ [Section 5.3, “Windows Bundles,” on page 49](#)
- ♦ [Section 5.4, “Inventory,” on page 57](#)
- ♦ [Section 5.5, “Logging,” on page 58](#)


5.1 Agent

The Endpoint Agent provides information such as the last time it contacted a cloud server, whether or not the Agent Modules are running, and the Closest Servers configured by the administrator in Endpoint Management Console.

The following sections contain more information:

- ♦ [Section 5.1.1, “Viewing the Agent’s Status,” on page 47](#)
- ♦ [Section 5.1.2, “Registering with a Key,” on page 48](#)

5.1.1 Viewing the Agent’s Status

- 1 Right-click the Agent Tray Icon  in the notification area, and select **Technician Portal**.
- 2 In the left navigation pane, click **Agent**.


Status Field	Description
Device Address	The IP address of your device .
Device Name	The computer name for your device.
Device State	The device’s state: managed, unmanaged, retired, or unknown. Unknown displays only if there is an error.
Last Contact with Server	The last time the Endpoint Agent had contact with the cloud server listed in the Server DNS field.
Next Contact with Server	The next time the Endpoint Agent is scheduled to contact (or be contacted by) the cloud server.
HTTP Proxy	A proxy server lets a device connect indirectly to a cloud server through the proxy server.
Agent Version	The version of the Endpoint Agent.
Management Zone	The name of the Management Zone in which your device is located.

Status Field	Description
Server	The DNS name of the cloud server that your device's Endpoint Agent communicates with to send and receive Endpoint Management content and information.
Subscription	The subscription name to which the agent is associated.
Registration Keys	The alphanumeric strings supplied during registration of the device in the Management Zone. Registration keys, which are defined by your administrator, help determine bundle and policy assignments.
Agent Status	The status and versions of the Agent modules.

5.1.2 Registering with a Key

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

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

- 1 Right-click the Agent Tray Icon  in the notification area, and select **Technician Portal**.
- 2 In the left navigation pane, click **Agent**.
- 3 In the **Registration Keys** field, type the registration key, then click **Register**.

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

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

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

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

5.2 Policies


The Endpoint Agent applies policies that your administrator defines. Policies are rules that control a range of hardware and software configuration settings. For example, your administrator can create policies that control the Endpoint Agent features you can use, the bookmarks available in your browser, the printers you can access, and the security and system configuration settings for your device. You cannot change the policies applied by your administrator.

The following sections contain more information about policies.

- ♦ [Section 5.2.1, “Viewing Policies,” on page 49](#)

5.2.1 Viewing Policies

To view the policies assigned to you and your device:

- 1 Right-click the Agent Tray Icon  in the notification area.
- 2 Click **Technician Portal**.
- 3 In the left navigation pane, click **Policies**.

5.3 Windows Bundles

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

The following sections contain more information:

- ♦ [Section 5.3.1, “Bundles Versus Applications,” on page 49](#)
- ♦ [Section 5.3.2, “Accessing Bundles,” on page 50](#)
- ♦ [Section 5.3.3, “Understanding Bundle Icons,” on page 53](#)
- ♦ [Section 5.3.4, “Launching a Bundle,” on page 54](#)
- ♦ [Section 5.3.5, “Postponing a Bundle Download,” on page 55](#)
- ♦ [Section 5.3.6, “Repairing a Bundle,” on page 55](#)
- ♦ [Section 5.3.7, “Viewing a Bundle’s Properties,” on page 55](#)
- ♦ [Section 5.3.8, “Uninstalling a Bundle,” on page 56](#)
- ♦ [Section 5.3.9, “Managing Favorites,” on page 56](#)

5.3.1 Bundles Versus Applications

Bundles are different than standard applications, such as Windows Notepad, that already reside on your device. When you double-click a bundle to launch it, the Endpoint Agent might first complete a variety of distribution tasks before the application is launched, including installing the application

files, running scripts, and changing the device's registry specific INI files, or environment variables. These tasks are all configured by your administrator to ensure that the application runs correctly on your device.


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

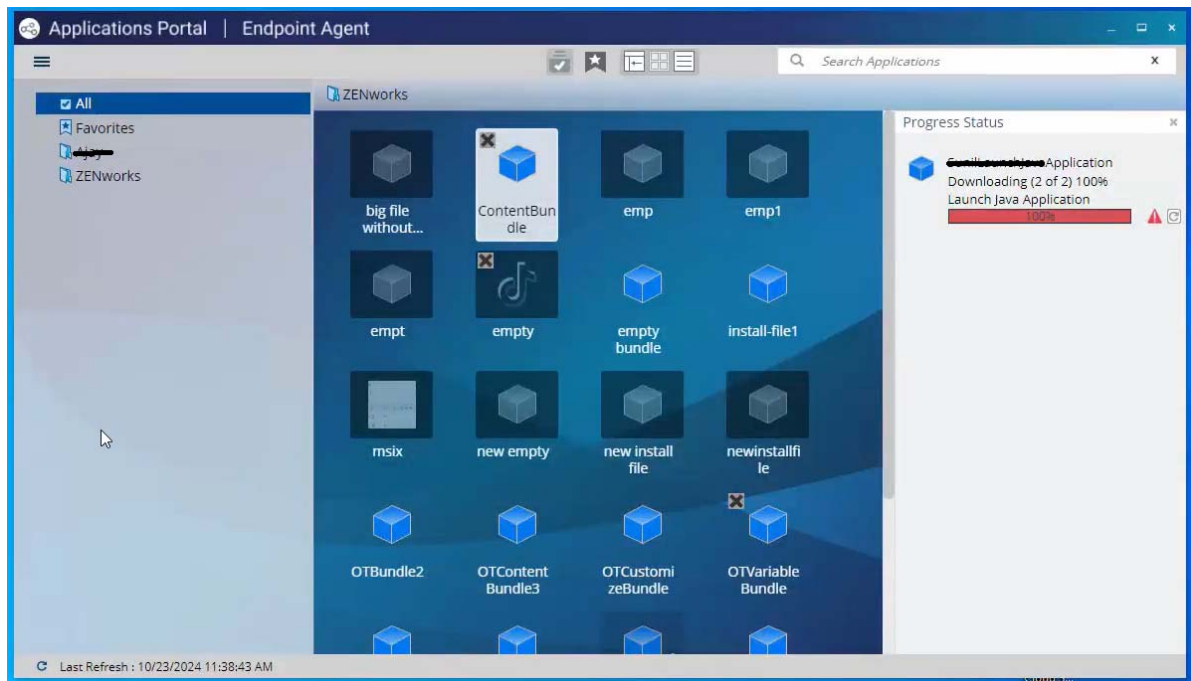
5.3.2 Accessing Bundles

There are three ways for accessing bundles on a managed device assigned to you:

- ♦ “Applications Portal” on page 50
- ♦ “Application Explorer” on page 51
- ♦ “Endpoint Agent” on page 52

Applications Portal

The Applications Portal is a standalone application that you can launch from the Start menu, or you can click the **Agent Tray** icon  from the system tray.



The Applications Portal left pane displays the following:

- ♦ **[All] folder:** Contains all bundles that have been distributed to you, regardless of the folder in which they are located.
- ♦ **Folder:** Contains all bundles that have not been assigned to a different folder. The folder is the default folder for bundles; however, your administrator can create additional folders in which to organize bundles, and can even rename the folder.

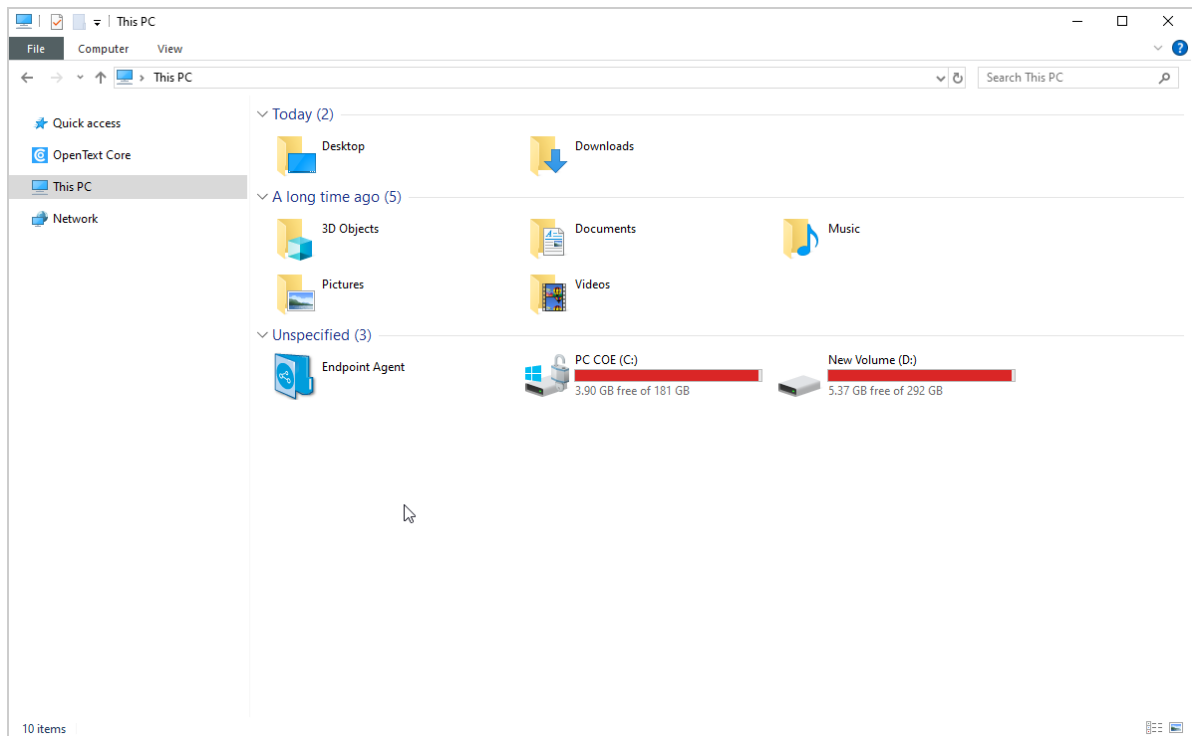
- ♦ **Favorites:** Contains all bundles that have been set a favorite. This folder will be displayed only if the setting **Enable Users to manage Favorites** is enabled in the Application Explorer Configuration Policy.

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

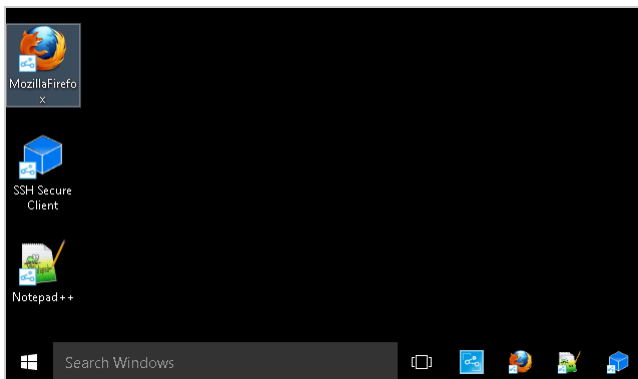
- ♦ Install a bundle or launch an application for an already installed bundle.
- ♦ View the properties of a bundle. The properties include a description of the bundle, information about people to contact for help with the bundle, the times when the bundle is available for use, and the system requirements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

Application Explorer

Application Explorer is an extension to Windows Explorer that enables bundles to be displayed in Windows Explorer, on the desktop, on the Start menu, on the Quick Launch toolbar, and in the notification area. The following graphic shows bundles displayed in Windows Explorer.



The following graphic shows bundles displayed on the desktop.

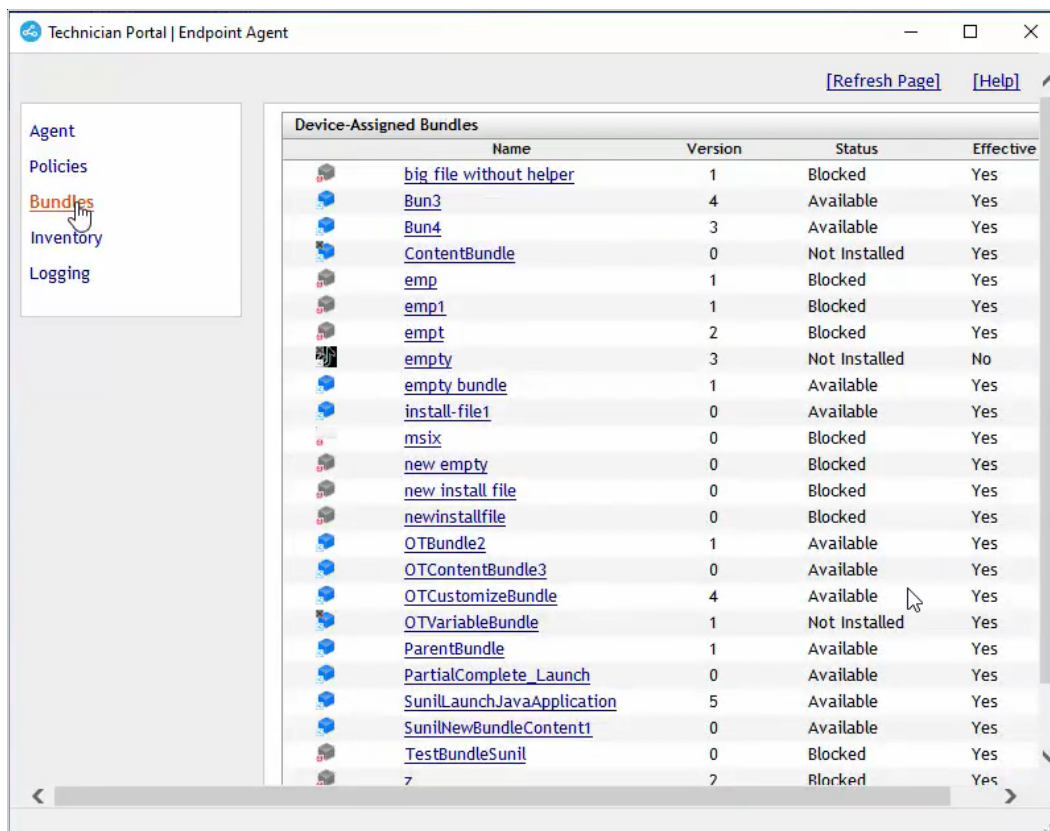


You can perform the same tasks on the bundles in the Application Explorer as you can in the Applications Portal. You can also view the Favorites folder in the Application Explorer window, which will be displayed only if the setting **Enable Users to manage Favorites** is enabled in the Application Explorer Configuration Policy.

Endpoint Agent

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


The **Bundles** link, located in the left navigation pane of the Endpoint Agent, lets you view the bundles that are assigned to your **device**.



The bundle list includes the following information:


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

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










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

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

5.3.3 Understanding Bundle Icons

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

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

Icon	Status
	Available. You can launch the bundle.
	Unavailable. You cannot launch the bundle. Either the device does not meet the system requirements established for the bundle.
	Installing. The bundle is installing to the device.
	Downloading. The bundle is downloading from the network location where it is stored.
	Uninstalling. The bundle is being removed from the device.
	Running. The bundle is currently running.
	Downloaded: Downloaded but not installed: The bundle has been downloaded on the device. However, it has not been installed as yet.
	Blocked. The bundle is blocked on the device. You cannot perform any of the actions on the bundle other than viewing its properties.
	Favorite: The bundle is set as a favorite.

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


5.3.4 Launching a Bundle

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

To launch a bundle:

- 1 Access the bundle in one of the following locations:

Applications Portal: Press the Windows logo key, and then type **Applications Portal**.

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

- 2 Double-click the bundle icon.

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


5.3.5 Postponing a Bundle Download

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

To postpone a bundle download:

- 1 Access the bundle in one of the following locations:

Applications Portal: Press Windows logo key, and then type **Applications Portal**.

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

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


5.3.6 Repairing a Bundle

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

To repair a bundle:

- 1 Access the bundle in one of the following locations:

Applications Portal: Press the Windows logo key, and then type **Applications Portal**.

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

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


5.3.7 Viewing a Bundle's Properties

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

To view a bundle's properties:

- 1 Access the bundle in one of the following locations:

Applications Portal: Press the Windows logo key, and then type **Applications Portal**.

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

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

5.3.8 Uninstalling a Bundle

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


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

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

To uninstall a bundle:


- 1 Access the bundle in one of the following locations:

Applications Portal: Press the Windows logo key, and then type **Applications Portal**.

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

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

5.3.9 Managing Favorites

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

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

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

5.4 Inventory

The Endpoint Agent scans your [device](#) for software and hardware information. This information is viewable by both you and your administrator.

The following sections contain more information:

- [Section 5.4.1, “What Is Inventory Information Used For?,” on page 57](#)
- [Section 5.4.2, “Scanning the Device,” on page 57](#)
- [Section 5.4.3, “Viewing Inventory Information,” on page 58](#)
- [Section 5.4.4, “Completing a Collection Data Form,” on page 58](#)

5.4.1 What Is Inventory Information Used For?

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


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

5.4.2 Scanning the Device

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

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

To initiate a scan:


- 1 Right-click the Agent Tray Icon  in the notification area.
- 2 Click **Technician Portal**.
- 3 From the left navigation pane, in the inventory menu, click **Scan Now**.

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

5.4.3 Viewing Inventory Information


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

To view inventory information:

- 1 Right-click the Agent Tray Icon  in the notification area.
- 2 Click **Technician Portal**.
- 3 From the left navigation pane, in the Inventory menu, click **View Inventory Details**.

5.4.4 Completing a Collection Data Form

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

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

5.5 Logging

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

The following sections contain more information:

- [Section 5.5.1, “Changing the Message Log Level,” on page 58](#)
- [Section 5.5.2, “Clearing the Message Log File,” on page 59](#)
- [Section 5.5.3, “Viewing the Message Log File,” on page 59](#)
- [Section 5.5.4, “Accessing the Backup Log Files,” on page 60](#)

5.5.1 Changing the Message Log Level

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

To change the log level:


- 1 Click the Agent Tray Icon  in the system tray.

- 2 In the left navigation pane, click **Logging**.
- 3 In the **Applied Log Level** field, select one of the following options:
 - ♦ **Use Global Setting:** Uses the message log level listed in the **Global Log Level** field.
 - ♦ **Error:** Logs error messages only. Error messages are generated whenever the Endpoint Agent is unable to perform a requested task.
 - ♦ **Errors, Warnings:** Logs error and warning messages. Warning messages are generated whenever the Endpoint Agent encounters a problem that might result in failure of a task.
 - ♦ **Errors, Warning, Info:** Logs error, warning, and informational messages. Informational messages are generated whenever the Endpoint Agent performs a task to show that the normal process is taking place.
 - ♦ **Errors, Warning, Info, Debug:** Logs all available messages to enable debug tracing of a problem. This level significantly increases the log file size and should be used only under the direction of your administrator.
- 4 Click **Apply** to apply the new severity level.

5.5.2 Clearing the Message Log File

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


To clear the log:

- 1 Click the Agent Tray Icon  in the system tray.
- 2 In the left navigation pane, click **Logging**.
- 3 Click **Clear Log**.

5.5.3 Viewing the Message Log File

The local log file, `EndpointAgent.log`, is stored in the `program files\OpenText\Endpoint Agent\logs\LocalStore\` directory on the root of the system drive (for example, `C:\Program Files\OpenText\Endpoint Agent\logs\LocalStore\EndpointAgent.log`).

To view the log file:

- 1 Click the Agent Tray Icon  in the system tray.
- 2 In the left navigation pane, click **Logging**.
- 3 Click **View Log**.


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

Field Number	Example	Description
1	ERROR	The severity level. Possible values are ERROR, WARNING, INFORMATION, and DEBUG.
2	3/14/2007 4:21:35 PM	The date and time the message was generated.

5.5.4 Accessing the Backup Log Files

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

To access the backup log file:

- 1 Click the Agent Tray Icon  in the system tray.
- 2 In the left navigation pane, click **Logging**.
- 3 Click **Open Log Folder**.

6 Uninstalling Endpoint Agent from Windows Devices

The following sections provide instructions for uninstalling Endpoint Agent from Windows devices.

- ♦ [Section 6.1, “Uninstalling Endpoint Agent from a Windows Device,” on page 61](#)

6.1 Uninstalling Endpoint Agent from a Windows Device

When uninstalling the Endpoint Agent from a managed device, please be aware of the following:

- ♦ If an uninstall password is required (the **Require an uninstall password for the Endpoint Agent** option is enabled), you must know the password and supply it during the uninstall process.

The agent uninstall password is set in Endpoint Management Console at either the zone level (**Configuration > Management Zone Settings > Device Management > Endpoint Agent > Agent Security**), folder level (**Devices > Managed > folder Details > Settings > Device Management > Endpoint Agent > Agent Security**), or device level (**Devices > device > Settings > Device Management > Endpoint Agent > Agent Security**).

To uninstall Endpoint Agent from a Windows managed device:

- 1 At a command prompt, run the following command to launch the uninstall program:

```
agent_installation_directory\OpenText\Endpoint  
Agent\bin\ZENworksUninstall.exe
```

To see the list of uninstall options, run `ZENworksUninstall.exe --help`

- 2 Click **Next**, then follow the prompts to uninstall the agent. Refer to the information in the following table if you have questions about any of the uninstall options.

Screen	Explanation
Administrator Information	<p>In order to unregister a device from the Zone during the uninstall process, you must provide the following information:</p> <p>You can perform a local uninstallation only if user uninstall is allowed for the device (the Allow users to uninstall the Endpoint Agent option is enabled).</p> <p>The agent user uninstall option is set in Endpoint Management Console at either the zone level (Configuration > Management Zone Settings > Device Management > Endpoint Agent > Agent Security), folder level (Devices > Managed > folder Details > Settings > Device Management > Endpoint Agent > Agent Security), or device level (Devices > device > Settings > Device Management > Endpoint Agent > Agent Security).</p>

- 3 If the Endpoint Agent requires an uninstall password, enter the password when prompted.

You must enter the password within 5 minutes of the prompt being displayed. Otherwise, the uninstall process times out and you must restart the process.

- 4 When the uninstall is finished, the Uninstallation Status dialog box is displayed. Review the status comments, make sure the **Restart Now** option is selected, then click **Finish**.

If desired, you can deselect the **Restart Now** option and reboot the device at a later time to complete uninstallation of the files and folders that were not able to be removed.

- 5 After the device reboots, perform the following tasks to ensure that Endpoint Agent is completely removed:
 - ♦ **Endpoint Agent Log Files:** Log files are purposely left here for your review. You can manually delete the *agent_installation_path*\OpenText\Endpoint Agent directory at any time.

7 Endpoint Management Terminology

The following terms are used throughout the Endpoint Agent documentation.

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

Device: A server or workstation.

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

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


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

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

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

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

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

Agent Tray Icon: The Agent Tray Icon  icon is located in the notification area of the Windows managed devices. Click the Agent Tray Icon to display the Endpoint Agent properties.

Applications Portal: A standalone window that you can launch from the Start Menu (Press the Windows logo key, and then type **Applications Portal**). The window displays all assigned bundles.

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

A Troubleshooting

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

- ♦ [“Endpoint Agent Explorer is not displayed in the Windows Explorer” on page 65](#)
- ♦ [“Desktop Icons are Rearranged after the Reboot” on page 65](#)
- ♦ [“The Endpoint Agent UI shows both English and the local language chosen for viewing” on page 66](#)
- ♦ [“Security vulnerabilities in .NET framework” on page 66](#)
- ♦ [“The Endpoint Agent Window Displays the Username with Random characters” on page 66](#)
- ♦ [“Desktop Icons are Rearranged after the Reboot” on page 66](#)
- ♦ [“The partial or the general refresh of a terminal server might cause high usage of system resources and take considerable time to refresh the server” on page 67](#)
- ♦ [“The quick-task execution fails when a policy is assigned to a device.” on page 67](#)
- ♦ [“Endpoint Agent service crashes” on page 67](#)

Endpoint Agent Explorer is not displayed in the Windows Explorer

Source: Endpoint Agent

Explanation: The Endpoint Agent Explorer might not be displayed in Windows Explorer by default after installing the agent.

Action: To enable the Endpoint Agent Explorer in Windows Explorer, follow these steps:

1. Open the Applications Portal:
 - a. Press the Windows logo key.
 - b. Type Applications Portal and select it from the search results.
2. Locate a bundle in the Applications Portal.
3. Right-click the bundle and select Send to Desktop.
4. After the bundle is pinned to the desktop, the Endpoint Agent Explorer will be displayed in Windows Explorer.

Desktop Icons are Rearranged after the Reboot

Source: Endpoint Agent

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

Action: None

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

Source: Endpoint Agent.

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

Action: Do one of the following:

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

Security vulnerabilities in .NET framework

Source: Endpoint Agent.

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

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

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

The Endpoint Agent Window Displays the Username with Random characters

Source: Endpoint Agent

Explanation: This issue is observed when you log into a device with the same username that is part of different tenants. If you log into the same device for the second time with the same username that is part of another tenant, then the username in the Endpoint Agent window is appended with random characters.

Action: none

Desktop Icons are Rearranged after the Reboot

Source: Endpoint Agent

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

Action: None

The partial or the general refresh of a terminal server might cause high usage of system resources and take considerable time to refresh the server

Source: Endpoint Agent.

Explanation: During a partial or general refresh of a terminal server, the Endpoint Agent on the server simultaneously refreshes the sessions of all the users logged into the terminal server. If too many users are logged in to the terminal server, the Endpoint Agent might take substantial time to refresh the terminal server and the usage of the system resources on the server might also be high.

Action: Perform the following steps to refresh the user sessions in batches:

- 1 Open the Registry Editor.
- 2 Go to `HKLM\Software\OpenText\EndpointAgent\`.
- 3 To enable batch refreshes, create a string called `EnableBatchRefresh` and set the value to 1.
By default, there are 5 sessions in a batch.
- 4 (Optional) To change the number of user sessions in a batch, create a string called `maxUserRefreshThreads` and set the desired value.

The quick-task execution fails when a policy is assigned to a device.

Source: Endpoint Agent.

Explanation: The quick-task execution fails when a policy is assigned to a device because the primary server is unable to communicate to the Agent on the Quick Task port.

Possible Causes: The possible causes for this issue could be:

- ♦ The Agent is switched off.
- ♦ The Firewall of the Agent or router prevents communication with the Quick Task port.
- ♦ Any security software, such as an antivirus, blocks the communication with the Quick Task port.

Endpoint Agent service crashes

Source: Endpoint Agent.

Explanation: Sometimes Endpoint Agent service crashes due to an internal error in the .NET Runtime with exit code 80131506 and unable to recover automatically.

Action: You must apply the hotfix (KB2640103) provided by Microsoft support. For more information, see [Microsoft support](#).

