

OpenText™ Endpoint Management Administration Quick Start

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
Part I System Configuration	7
1 Quick List	9
Management Tools	9
Zone Configuration	9
Agent Deployment	10
System Messages	11
2 Management Tools	13
Endpoint Management Console	13
Accessing Endpoint Management Console	13
Navigating Endpoint Management Console	15
zac Command Line Utility	16
Location	16
Syntax	16
Help with Commands	17
3 Management Zone Configuration	19
Organizing Devices: Folders and Groups	19
Folders	19
Groups	20
Assignment Inheritance for Folders and Groups	22
Creating Registration Keys and Rules	22
Registration Keys	22
Registration Rules	23
Device Naming Template	23
Where to Find More Information	24
Modifying Configuration Settings	24
Modifying Configuration Settings at the Zone	24
Modifying Configuration Settings on a Folder	25
Modifying Configuration Settings on a Device	25
Dashboard	25
4 Endpoint Agent Deployment	27
Protect the Endpoint Agent from Uninstallation	27
Downloading the Endpoint Agent	27
Installing the Endpoint Agent	28
Manual Installation on Windows	28
Using the Endpoint Agent	29
Navigating the Endpoint Agent Views	29

5	System Messages	33
	Viewing System Messages	33
	Viewing a Summary of Messages	33
	Acknowledging Messages	34
	Creating a Watch List	34
6	Audit Management	37
	Types of Audit Events	37
	Enabling an Event	37
	Viewing a Generated Event	38
	Part II Product Administration	41
7	Quick List	43
	Configuration Management	43
8	Configuration Management	45
	Distributing Software	45
	Creating a Bundle	45
	Assigning a Bundle	46
	Where to Find More Information	46
	Applying Policies	46
	Creating a Policy	46
	Assigning a Policy	47
	Where to Find More Information	47
	Collecting Software and Hardware Inventory	47
	Initiating a Device Scan	47
	Viewing a Device Inventory	48
	Generating an Inventory Report	48
	Where to Find More Information	48

About This Guide

This *OpenText™ Endpoint Management Administration Quick Start* helps you quickly master the basics of administering your Endpoint Management system.

The information in this guide is organized as follows:

- ♦ [System Configuration \(page 7\)](#): Provides instructions for configuring your Endpoint Management Zone prior to using Endpoint Management.
- ♦ [Product Administration \(page 41\)](#): Provides instructions for using Endpoint Management (Configuration Management).

Audience

This guide is intended for anyone who will configure the Endpoint Management system, monitor the Endpoint Management system, or perform any Endpoint Management tasks related to managing 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* link at the bottom of each page of the online documentation.

Additional Documentation

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

System Configuration

The following sections provide information to help you understand your Endpoint Management system.

- ♦ [Chapter 1, “Quick List,” on page 9](#)
- ♦ [Chapter 2, “Management Tools,” on page 13](#)
- ♦ [Chapter 3, “Management Zone Configuration,” on page 19](#)
- ♦ [Chapter 4, “Endpoint Agent Deployment,” on page 27](#)
- ♦ [Chapter 5, “System Messages,” on page 33](#)
- ♦ [Chapter 6, “Audit Management,” on page 37](#)



1 Quick List

Before you begin using Endpoint Management, you should review the concepts and tasks in the following sections. These sections are designed to quickly introduce you to what you need to know about your Management Zone:

- ♦ [“Management Tools” on page 9](#)
- ♦ [“Zone Configuration” on page 9](#)
- ♦ [“Agent Deployment” on page 10](#)
- ♦ [“System Messages” on page 11](#)




Management Tools

OpenText™ Endpoint Management provides a Web-based console (Endpoint Management Console) that you can use to manage your Endpoint Management system. You should become familiar with at least Endpoint Management Console.

Task	Details	
	Launch Endpoint Management Console	For instructions, see “Endpoint Management Console” on page 13 .
	Discover how to run the zac utility	<p>The zac utility is a command line interface for the Endpoint Agent.</p> <p>For instructions, see “zac Command Line Utility” on page 16.</p>


Zone Configuration


Before you start taking full advantage of the management capabilities provided by the Endpoint Management product, there are a few configuration tasks you need to complete to ensure that your Management Zone is configured correctly.

Task	Details	
	Create folders and groups for organizing devices	<p>Organize devices into folders and groups to ease the overhead involved in applying Endpoint Management configuration settings and performing tasks on similar devices. Rather than making assignments or performing tasks on individual devices, you can manage the folders and groups, with each device in a folder or group inheriting the assignment or task.</p> <p>For instructions, see “Organizing Devices: Folders and Groups” on page 19.</p>
	Create registration keys or rules	<p>Endpoint Agent must be deployed on each device that you want to manage. When you deploy the Endpoint Agent to a device, the device is registered in your Management Zone.</p> <p>You can use registration keys or rules to automatically assign devices to the appropriate folders and groups, enabling the devices to immediately inherit any assignments associated with the folders and groups.</p> <p>For instructions, see “Creating Registration Keys and Rules” on page 22.</p>
	Modify zone configuration settings	<p>The Management Zone settings are preset to provide the most common configuration. You don’t need to change any settings at this time, but you might want to browse the settings to become more familiar with them.</p> <p>For instructions, see “Modifying Configuration Settings” on page 24.</p>

Agent Deployment

The Endpoint Agent communicates with the cloud server to perform management tasks on a device. You must deploy the Endpoint Agent to all devices you want to manage. Deploying the Endpoint Agent installs the agent files and registers the device in your Management Zone.

Task	Details	
	Protect the Endpoint Agent from Uninstallation	<p>You can configure the Endpoint Agent install and uninstall.</p> <p>For instructions, see “Protect the Endpoint Agent from Uninstallation” on page 27.</p>

Task	Details
 Install the Endpoint Agent	<p>You can use Use Endpoint Management Console to install the agent from a cloud server to the device.</p> <p>For instructions, see “Installing the Endpoint Agent” on page 28.</p>

System Messages

As you perform management tasks in your zone, information is recorded so that you can view the status of your zone and the activities taking place within it.

Table 1-1

Task	Details
View system messages	<p>View system messages</p> <p>For instructions, see “Viewing System Messages” on page 33.</p>
Create a Watch List	<p>If you have devices, bundles, and policies whose activity you want to closely monitor, you can add them to the Watch List.</p> <p>For instructions, see “Creating a Watch List” on page 34.</p>

2 Management Tools

OpenText™ Endpoint Management provides a web-based console (Endpoint Management Console) that you can use to manage your Endpoint Management system. The following sections explain how to access and use the management tools:

- ♦ [“Endpoint Management Console” on page 13](#)
- ♦ [“zac Command Line Utility” on page 16](#)

Endpoint Management Console

- ♦ [“Accessing Endpoint Management Console” on page 13](#)
- ♦ [“Navigating Endpoint Management Console” on page 15](#)

Accessing Endpoint Management Console

- 1 Using a Web browser that meets the requirements listed in [“Administration Browser Requirements”](#), enter the following URL:

```
https://https://em.prod.ca.opentext.com/?subscription-  
name=<subscriptionname>
```

If you are accessing the Endpoint Management Console for the first time, then click the **Core Endpoint Management** link that you receive in the **Welcome** email from **OpenText Core Endpoint Management**.

The Sign in page is displayed.



NOTE: Signing in with otconnect is not allowed.

- 2 In the **Username** field, type the user name that you have entered for logging and accessing the Core Endpoint Management application.

You log in to the Endpoint Management Console as per the role assigned to you by the Tenant Administrator in the Admin Centre.

- 3 Click **Next**.

- 4 Enter the password in the **Password** field

- ♦ Specify the password for the administrator name that you created in Endpoint Management Console.

To prevent unauthorized users from gaining access to Endpoint Management Console, the administrator account is disabled after three unsuccessful login attempts, and a 60-second timeout is enforced before you can attempt another login.

- 5 Click **next** to access Endpoint Management Console.

To log in again as a different administrator/ user, click the **Logout** option in the upper right corner of the Endpoint Management Console, then when the login dialog box is displayed, log in as a different administrator/ user.

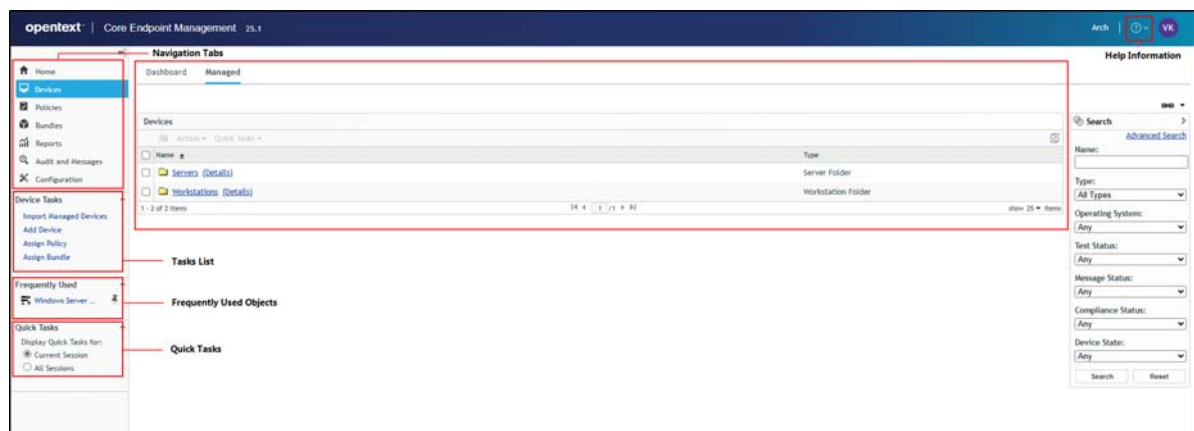
Performing concurrent operations in multiple sessions of Endpoint Management Console might result in an exception

If Endpoint Management Console is opened in multiple browsers and you choose to perform an operation on an object in one browser when the same object is being modified or accessed in the other browser, an exception might occur.

For example, an error might occur if you update an object in one session of Endpoint Management Console when the same object has been deleted in another session of Endpoint Management Console.

Navigating Endpoint Management Console

The following Workstations page represents a standard view in Endpoint Management Console.



Navigation Tabs: The tabs in the left pane let you navigate among the functional areas of Endpoint Management. For example, the Workstations page shown above lets you manage tasks associated with workstations.

Task List: The task list in the left pane provides quick access to the most commonly performed tasks for the current page. The task list changes for each page. For example, the task list on the Devices page displays device-related tasks and the task list on the Configuration page displays configuration-related tasks.

Frequently Used Objects: The Frequently Used list in the left pane displays the 10 objects that you have accessed most often, from most used to least used. Clicking an object takes you directly to the details page for the object.

Work Panel: The work panels are where you monitor and manage your Endpoint Management system. The panels change depending on the current page. In the above example, there are two work panels: **Devices** and **Search**. The **Devices** panel lists the workstations, workstation folders, workstation groups, and dynamic workstation groups that have been created; you use this panel to manage workstations. The **Search** panel lets you filter the Devices panel based on criteria such as a workstation's name, operating system, or status.

Help Information: The Help button links to Help topics that provide information about the current page. The Help button links change depending on the current page.

zac Command Line Utility

The zac utility provides a command line management interface that lets you perform tasks available in the Endpoint Agent.

- ♦ [“Location” on page 16](#)
- ♦ [“Syntax” on page 16](#)
- ♦ [“Help with Commands” on page 17](#)

Location

The utility is installed on all Windows managed devices in the following location:

%ENDPOINT_AGENT_HOME%

where %ENDPOINT_AGENT_HOME% represents the Endpoint Management installation path. The default path is C:\Program Files\OpenText\Endpoint Agent\bin on a 64-bit Windows device.

Syntax

The zac utility uses the following basic syntax:

zac command options

For example, to launch a bundle on a device, you use the following command:

```
zac bundle-launch "bundle 1"
```

where `bundle-launch` is the command and `bundle 1` is the command option. In this example, the option is the display name of the bundle to be launched. Enclosing quotation marks are required only if the bundle display name includes spaces.

For example, to initiate an inventory scan on a device, you use the following command:

```
zac inv scannow
```

where `inv` is the command and `scannow` is the command option.

Help with Commands

The best way to understand the commands is to use the online help or see “[zac for Windows\(1\)](#)” in the [Endpoint Management Command Line Utilities Reference](#).

To use the online help:

- 1 On the managed device, enter one of the following commands at a command prompt.

Command	Description
<code>zac --help</code>	Displays a complete list of commands.
<code>zac command --help</code>	Displays detailed help for a command.

3 Management Zone Configuration

OpenText™ Endpoint Management is designed to let you efficiently manage a large number of devices with as little effort as possible. The first step in easing this management burden is to ensure that you've configured your Management Zone so that you can take full advantage of the Endpoint Management capabilities.

The following sections introduce the basic concepts you need to set up a Management Zone that best supports the ongoing management tasks you perform. Each section explains a management concept and provides general steps to perform the tasks associated with the concept.

- ♦ [“Organizing Devices: Folders and Groups” on page 19](#)
- ♦ [“Creating Registration Keys and Rules” on page 22](#)
- ♦ [“Modifying Configuration Settings” on page 24](#)
- ♦ [“Dashboard” on page 25](#)

Organizing Devices: Folders and Groups

Using Endpoint Management Console, you can manage devices by performing tasks directly on individual device objects. However, this approach is not very efficient unless you have only a few devices to manage. To optimize management of a large number of devices, Endpoint Management lets you organize devices into folders and groups; you can then perform tasks on a folder or group to manage its devices.

You can create folders and groups at any time. However, the best practice is to create folders and groups before you register devices in your zone. This allows you to use registration keys and rules to automatically add devices to the appropriate folders and groups when they register (see [“Creating Registration Keys and Rules” on page 22](#)).

- ♦ [“Folders” on page 19](#)
- ♦ [“Groups” on page 20](#)
- ♦ [“Assignment Inheritance for Folders and Groups” on page 22](#)

Folders

Folders are a great tool to help you organize devices in order to simplify management of those devices. You can apply configuration settings, assign assignments, and perform tasks on any folder. When you do so, the folder's devices inherit those settings, assignments, and tasks.

For best results, you should place devices with similar configuration setting requirements in the same folder. If all devices in the folder require the same assignments or tasks, you can also make assignments or task assignments on the folder. However, all devices in the folder might not have the same assignments and task requirements. Therefore, you can organize the devices into groups and assign the appropriate assignments and tasks to each groups (see [“Groups” on page 20](#) below).

For example, assume that you have workstations at three different sites. You want to apply different configuration settings to the workstations at the three sites, so you create three folders (/Workstations/Site1, /Workstations/Site2, and /Workstations/Site3) and place the appropriate workstations in each folder. You decide that most of the configuration settings apply to all workstations, so you configure those settings at the Management Zone. However, you want to perform a weekly collection of software and hardware inventory at Site1 and Site2 and a monthly inventory collection at Site3. You configure a weekly inventory collection at the Management Zone and then override the setting on the Site3 folder to apply a monthly schedule. Site1 and Site2 collect inventory weekly, and Site3 collects inventory monthly.

Creating a Folder

- 1 In Endpoint Management Console, click the **Devices** tab.
- 2 Click the **Workstations**, or **Servers** folder.
- 3 Click **New > Folder** to display the New Folder dialog box.
- 4 In the **Name** field, type a name for the new folder.

When you name an object in the Endpoint Management Console (folders, groups, bundles, policies, and so forth), ensure that the name adheres to the following conventions:

- ♦ The name must be unique in the folder.
- ♦ Depending on the database software being used for the Endpoint Management database, uppercase and lowercase letters might not create uniqueness for the same name. The embedded database included with Endpoint Management is case insensitive, so Folder 1 and FOLDER 1 are the same name and cannot be used in the same folder. If you use an external database that is case-sensitive, Folder 1 and FOLDER 1 are unique.
- ♦ If you use spaces, you must enclose the name in quotes when entering it on the command line. .
- ♦ The following characters are invalid and cannot be used: / \ * ? : " ' < > | ` % ~

- 5 Click **OK** to create the folder.

Groups

As you can with folders, you can also assign content and perform tasks on device groups. When you do so, the group's devices inherit those assignments and tasks. Unlike with folders, you cannot apply configuration settings to groups.

Groups provide an additional layer of flexibility for content assignments and tasks. In some cases, you might not want to assign the same content to and perform the same task on all devices in a folder. Or, you might want to assign the same content to and perform tasks on one or more devices in different folders. To do so, you can add the devices to a group (regardless of which folders contain the devices) and then assign the content to and perform the tasks on the group.

For example, let's revisit the example of the workstations at three different sites (see [“Folders” on page 19](#)). Assume that some of the workstations at each site need the same accounting software. Because groups can be assigned software, you could create an Accounting group, add the target workstations to the group, and then assign the appropriate accounting software to the group. Likewise, you could use the groups to assign Windows configuration and policies.

The advantage to making an assignment to a group is that all devices contained in that group receive the assignment, but you only need to make the assignment one time. In addition, a device can belong to any number of unique groups, and the assignments from multiple groups are additive. For example, if you assign a device to group A and B, it inherits the software assigned to both groups.

Endpoint Management provides both groups and dynamic groups. From the perspective of content assignments or performing tasks, groups and dynamic groups function exactly the same. The only difference between the two types of groups is the way that devices are added to the group. With a group, you must manually add devices. With a dynamic group, you define criteria that a device must meet to be a member of the group, and then devices that meet the criteria are automatically added.

Endpoint Management include several predefined dynamic server groups.

Endpoint Management also includes dynamic workstation groups. Devices that have these operating systems are automatically added to the appropriate dynamic group.

Creating a Group

- 1 In Endpoint Management Console, click the **Devices** tab.
- 2 If you want to create a group for servers, click the **Servers** folder.
or
If you want to create a group for workstations, click the **Workstations** folder.
- 3 Click **New > Server Group** (**New > Workstation Group** for workstations) to launch the Create New Group Wizard.
- 4 On the Basic Information page, type a name for the new group in the **Group Name** field, then click **Next**.
The group name must follow the [naming conventions](#).
- 5 On the Summary page, click **Finish** to create the group without adding members.
or
Click **Next** if you want to add members to the group, then continue with [Step 6](#).
- 6 On the Add Group Members page, click **Add** to add devices to the group, then click **Next** when finished adding devices.
- 7 On the Summary page, click **Finish** to create the group.

Creating a Dynamic Group

- 1 In Endpoint Management Console, click the **Devices** tab.
- 2 If you want to create a group for servers, click the **Servers** folder.
or
If you want to create a group for workstations, click the **Workstations** folder.
- 3 Click **New > Dynamic Server Group** (**New > Dynamic Workstation Group** for workstations) to launch the Create New Group Wizard.
- 4 On the Basic Information page, type a name for the new group in the **Group Name** field, then click **Next**.
The group name must follow the [naming conventions](#).

- 5 On the Define Filter for Group Members page, define the criteria that a device must meet to become a member of the group, then click **Next**.
Click the **Help** button for details about creating the criteria.
- 6 On the Summary page, click **Finish** to create the group.

Assignment Inheritance for Folders and Groups

When you assign content to a folder, all objects (devices, subfolders) except groups that are located in the folder inherit the assignment. For example, if you assign BundleA and PolicyB to DeviceFolder1, all devices within the folder (including all devices in subfolders) inherit the two assignments. However, none of the device groups located in DeviceFolder1 inherit the assignments. Essentially, folder assignments do not flow down to groups located within the folder.

Creating Registration Keys and Rules

When you deploy the Endpoint Agent to a device, the device is registered in your Management Zone and becomes a managed device. As part of the registration, you can specify the device's Endpoint Management name and the folder and groups to which you want the device added.

By default, a device's hostname is used as its Endpoint Management name, it is added to the `/Servers` or `/Workstations` folder, and it is not given membership in any groups. You can manually move devices to other folders and add them to groups, but this can be a burdensome task 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 have them automatically added to the correct folders and groups during registration.

To add devices to folders and groups during registration, you can use registration keys, registration rules, or both. Both registration keys and registration rules let you assign folder and group memberships to a device. However, there are differences between keys and rules that you should be aware of before choosing whether you want to use one or both methods for registration.

- ♦ [“Registration Keys” on page 22](#)
- ♦ [“Registration Rules” on page 23](#)
- ♦ [“Device Naming Template” on page 23](#)
- ♦ [“Where to Find More Information” on page 24](#)

Registration Keys

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 can 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.

You can create one or more registration keys to ensure that devices are placed in the desired folders and groups. For example, you might want to ensure that all of the Sales department's workstations are added to the `/Workstations/Sales` folder but are divided into three different groups (SalesTeam1, SalesTeam2, SalesTeam3) depending on their team assignments. You could create

three different registration keys and configure each one to add the Sales workstations to the `/Workstations/Sales` folder and the appropriate team group. As long as each workstation uses the correct registration key, it is added to the appropriate folder and group.

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 Follow the prompts to create the key.

For information about what you need to supply at each step of the wizard, click the **Help** button.

Registration Rules

If you don't want to enter an enrollment token during deployment, or if you want devices to be automatically added to different folders and groups based on predefined criteria (for example, operating system type, CPU, or IP address), you can use registration rules.

Endpoint Management includes a default registration rule for servers and another one for workstations. If a device registers without a key and you haven't created registration rules, the default registration rules are applied to determine the folder assignments. The two default rules cause all servers to be added to the `/Servers` folder and all workstations to the `/Workstations` folder.

You can define additional rules that enable you to filter devices as they register and add them to different folders and groups. If, as recommended in [“Organizing Devices: Folders and Groups” on page 19](#), you've established folders for devices with similar configuration settings and groups for devices with similar assignments, then newly registered devices automatically receive the appropriate configuration settings and assignments.


To create 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 Follow the prompts to create the rule.

For information about what you need to supply at each step of the wizard, click the **Help** button.

Device Naming Template

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

- 1 In Endpoint Management Console, click the **Configuration** tab.
- 2 In the Management Zone Settings panel, click **Device Management**.
- 3 Click **Registration** to display the Registration page.
- 4 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}`

- 5 Click **OK** to save the changes.

Where to Find More Information

For more information about registering devices, see the [Registering Devices](#) in the *Endpoint Agent Guide*.

Modifying Configuration Settings

The Management Zone configuration settings enable you to control a wide range of functionality behavior for your zone. There are Device Management settings that let you control how often devices access a cloud server for refreshed information, how often dynamic groups are refreshed, and what levels of messages (informational, warning, or error) are logged by the Endpoint Agent. There are Event and Messaging settings, and much more.

Management Zone settings that apply to devices are inherited by all devices in the zone. As mentioned in “[Organizing Devices: Folders and Groups](#)” on page 19, you can override zone settings by configuring them on device folders or on individual devices. This allows you to establish zone settings that apply to the largest number of devices, and then override the settings on folders and devices, as required.

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

- ♦ “[Modifying Configuration Settings at the Zone](#)” on page 24
- ♦ “[Modifying Configuration Settings on a Folder](#)” on page 25
- ♦ “[Modifying Configuration Settings on a Device](#)” on page 25

Modifying Configuration Settings at the Zone

- 1 In Endpoint Management Console, click the **Configuration** tab.
- 2 In the Management Zone Settings panel, click the settings category (for example, **Device Management**, and **Event and Messaging**) whose settings you want to modify.
- 3 Click the setting to display its details page.
- 4 Modify the setting as required.

For information about the setting, see the [Endpoint Management Zone Settings Reference](#).

- 5 Click **OK** or **Apply**.

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

Modifying Configuration Settings on a Folder

- 1 In Endpoint Management Console, click the **Devices** tab.
- 2 In the Devices panel (on the **Managed** tab), browse for the folder whose settings you want to modify.
- 3 Click **Details** next to the folder name to display the details.
- 4 Click the **Settings** tab.
- 5 In the Settings panel, click the settings category (**Device Management**, **Infrastructure Management**, and so forth) of the settings that you want to modify.
- 6 Click the setting to display the details page.
- 7 Modify the setting as required.

For information about the setting, see the [Endpoint Management Zone Settings Reference](#).

- 8 Click **OK** or **Apply**.

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

Modifying Configuration Settings on a Device

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

For information about the setting, click the **Help** button in Endpoint Management Console.

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

Dashboard

The dashboard feature provides a comprehensive snapshot of key indicators, so you can quickly assess the overall health and compliance of devices in your zone. Using dashboards, you can drill down to further areas of interest.

The Endpoint Management dashboards enable you to view information related to the status of devices within the zone, and perform the required actions.

For more information, see [Endpoint Management Dashboard Reference](#).

4 Endpoint Agent Deployment

The Endpoint Agent must be deployed to the devices that you want to manage. The following sections provide instructions to help you understand the process of deploying the agent:

- ♦ [“Protect the Endpoint Agent from Uninstallation” on page 27](#)
- ♦ [“Downloading the Endpoint Agent” on page 27](#)
- ♦ [“Installing the Endpoint Agent” on page 28](#)
- ♦ [“Using the Endpoint Agent” on page 29](#)

Protect the Endpoint Agent from Uninstallation

To secure the Endpoint Agent on devices, you can configure install or uninstall for the agent.

- 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, configure the following settings:
 - ♦ **Allow Users to Uninstall the Endpoint Agent:** Select this option to uninstall the Endpoint Agent.
- 4 To save the changes, click **OK**.

Downloading the Endpoint Agent

To download the Endpoint Agent on any supported device, perform the following tasks:

In the Endpoint Management Home page, go to **Common Tasks**, click **Download Admin Tools** and then click the **Endpoint Agent** tab.

In the Endpoint Agent page, based on your requirements, you can download the required package.

For more information on the deployment packages, see [Manually Deploying the Agent on Windows](#) in the [Endpoint Agent Guide](#).

Installing the Endpoint Agent

The following sections provide instructions for manually installing the Endpoint Agent on devices.

- ♦ [“Manual Installation on Windows” on page 28](#)

Manual Installation 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.

For information about logging in and using the Endpoint Agent on a device, see [“Using the Endpoint Agent” on page 29](#).

Using the Endpoint Agent

The following sections provide information to help you log in and use the Endpoint Agent:

- ♦ [“Navigating the Endpoint Agent Views” on page 29](#)

Navigating the Endpoint Agent Views

The Endpoint Agent provides the following views:

- ♦ [“Application Portal” on page 29](#)
- ♦ [“Application Explorer” on page 29](#)
- ♦ [“Agent Tray Icon” on page 31](#)

Application Portal

The Application Portal is a standalone window that provides access to bundles. You can launch the window from the Start menu (**Start menu** > **Programs** > **Endpoint Agent** > **Application Portal**).

The Application left pane displays the following:

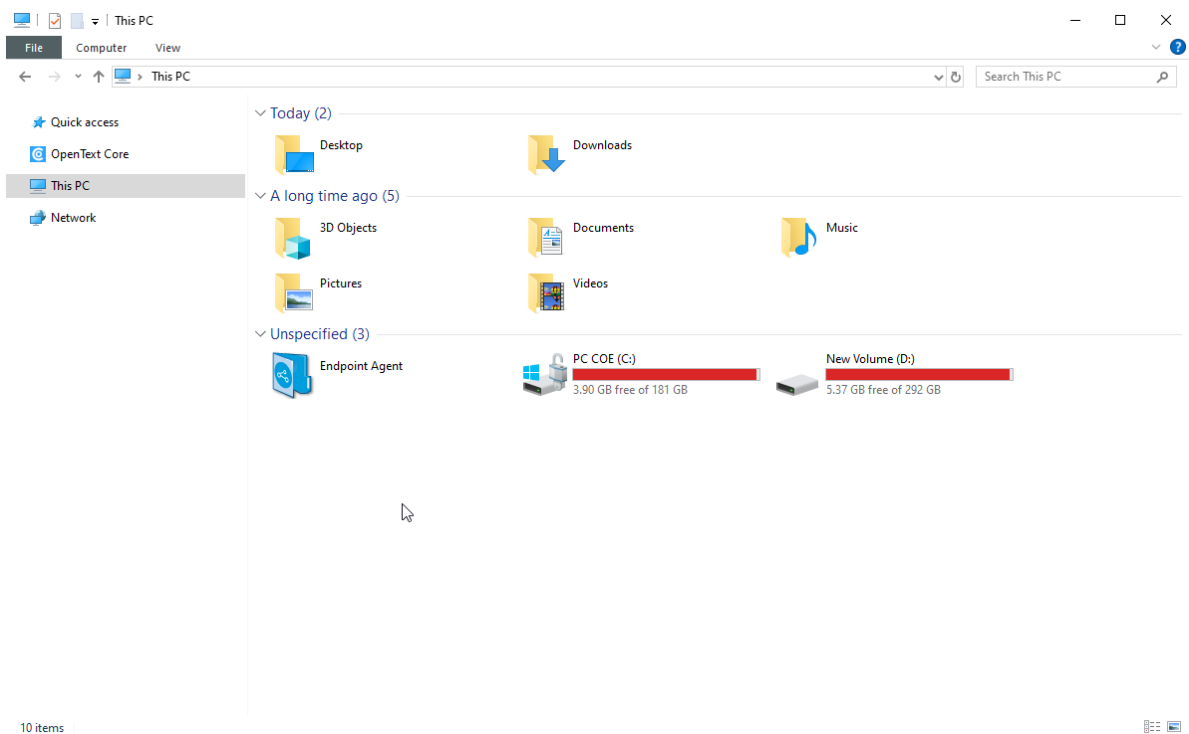
- ♦ **[All] folder:** Contains all bundles that have been distributed to you, regardless of the folder in which they are located.
- ♦ **Folder:** Contains all bundles that have not been assigned to a different folder. The folder is the default folder for bundles; however, your administrator can create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

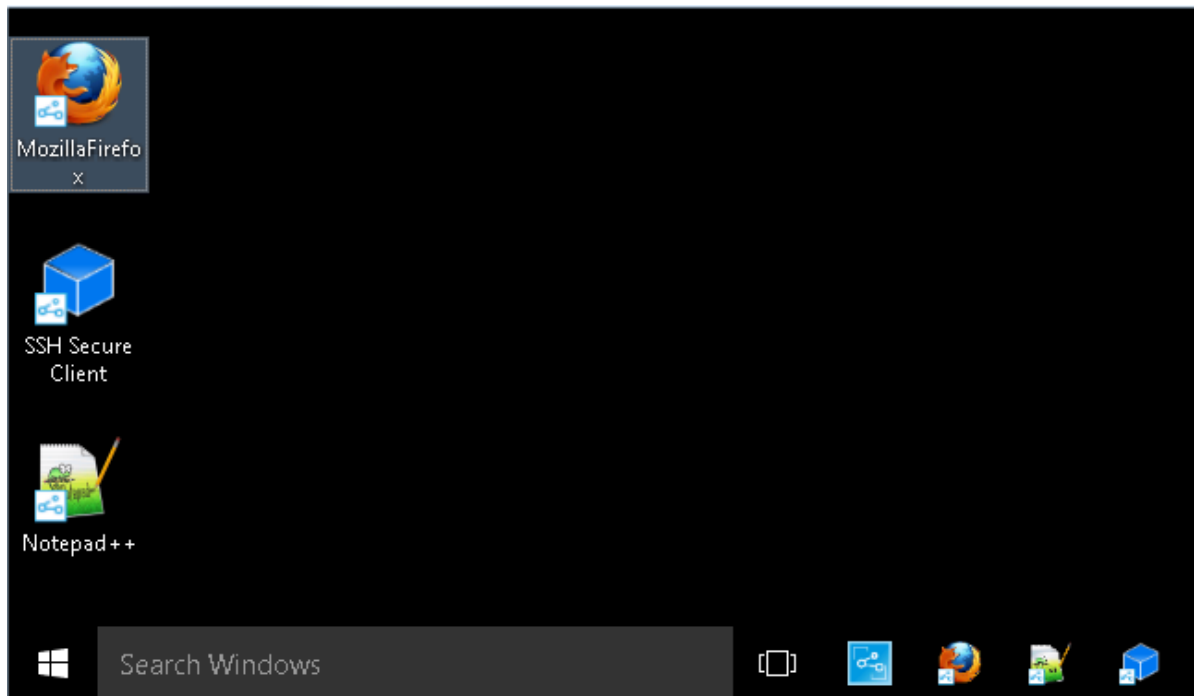
- ♦ Install a bundle or launch an application that is already installed.
- ♦ View the properties of a bundle. The properties include a description of the bundle, information about who to contact for help with the bundle, when the bundle is available for use, and the system requirements established for 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 (system tray). The following graphic shows bundles displayed in Windows Explorer.




The following graphic shows bundles displayed on the desktop.



The tasks performed on the bundles in the Application Window can also be performed in the Application Explorer.

Agent Tray Icon

The Agent Tray Icon  is located in the Windows notification area (system tray). You can click the icon to display the Endpoint Agent window.

To view the agent properties, right click the Agent Tray icon and select Technician Portal. The Endpoint Agent Properties window is displayed.

The left navigation pane of the properties window contains links for the Endpoint Agent status and its features:

- ♦ **Agent:** Displays information such as the last time the agent contacted a Cloud Server and whether the Agent features are running.
- ♦ **Policies:** Displays the policies assigned to the device, and also displays whether the policy is effective.
- ♦ **Bundles:** Displays the bundles assigned to the device. It also displays the current installation status of each bundle (available, downloading, installing, and so forth) and whether the bundle is effective (the device meets the requirements for distribution).
- ♦ **Inventory:** Displays inventory information for the device. 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 Windows hot fixes and patches, and the version numbers and locations of installed software products.
- ♦ **Logging:** Displays information about the Endpoint Agent's log file, such as the location of the log file, the Cloud Server to which the agent's log file will be uploaded, and the next time the log is scheduled to be uploaded. It also lets you determine the severity level for logged messages.

For more information on using the Endpoint Agent, see [Endpoint Agent Guide](#).

5 System Messages

OpenText™ Endpoint Management lets you monitor the activity within your Management Zone through system messages.

- ♦ [“Viewing System Messages” on page 33](#)
- ♦ [“Creating a Watch List” on page 34](#)

Viewing System Messages

The Endpoint Management system generates normal (informational), warning, and error messages to help you monitor activities such as the distribution of software and application of policies.




Each cloud server and Endpoint Agent creates a log of the activities associated with it. These messages are displayed in Endpoint Management Console in various areas:





- ♦ **Device Message Log:** A device message log, located on the Summary page for a server or workstation, displays messages generated by the Cloud Server or the Endpoint Agent. For example, the message log for Workstation1 includes all messages generated by the Endpoint Agent on Workstation1.
- ♦ **Message Log:** A message log, located on the Summary page for a bundle or policy, displays only the Server or Endpoint Agent messages associated with the bundle or policy.

Viewing a Summary of Messages

You can view a summary that shows the number of messages generated for the servers, workstations, bundles, and policies in the zone.

- 1 In Endpoint Management Console, click the **Home** tab.

The Message Summary panel displays the status of all servers, workstations, policies, and bundles in the Management Zone. For example, if two servers have unacknowledged critical messages (those messages that you or another administrator have not yet acknowledged), the  column displays the number 2. Or, if you have three bundles with warning messages and five bundles with only normal messages, the  column displays the number 3 and the  column displays the number 5. You can do the following with the summary:

- ♦ Click an object type to display its root folder. For example, click **Servers** to display the Servers root folder (/Servers).
- ♦ For any object type, click the number in one of its status columns (  ) to display a listing of all the objects that currently have that status. For example, to see the list of servers that have a normal status, click the number in the  column.
- ♦ For any object type, click the number in the **Total** column to display all the objects that have critical, warning, or normal messages. For example, click the **Total** count for **Servers** to display a list of all servers that have any type of messages.

Acknowledging Messages

A message remains in a message log until you acknowledge it. You can acknowledge individual messages or acknowledge all messages in the message log at one time.




- 1 In Endpoint Management Console, click the **Devices** tab.
- 2 Navigate the **Servers** folder until you locate a Cloud Server.
- 3 Click the server to display its details.
- 4 On the **Summary** tab, locate the Message Log panel.



The Message Log panel lists all messages (informational, warning, and error) generated by the Cloud Server. The following table explains the various ways you can acknowledge and delete messages.

Task	Steps	Additional Details
Acknowledge a message	<ol style="list-style-type: none">1. Click the message to display the Message Detail Information dialog box.2. Click Acknowledge.	If you do not want to acknowledge the message, click Finished to close the dialog box. This causes the message to remain in the Message Log list.
Acknowledge all messages	<ol style="list-style-type: none">1. In the Tasks list located in the left navigation pane, click Acknowledge All Messages.	
View all acknowledged or unacknowledged messages	<ol style="list-style-type: none">1. Click the Advanced button to display the Edit Message Log page.	<p>In addition to viewing all acknowledged and unacknowledged messages, you can also view only those messages with a specific status or date, view more details about messages, and acknowledge messages.</p> <p>Click the Help button on the Edit Message Log page for specific information about performing tasks on that page.</p>
Delete a message	<ol style="list-style-type: none">1. Click the message to display the Message Detail Log dialog box.2. Click Delete.	Deleting a message completely removes the message from your Endpoint system.

Creating a Watch List

If you have devices, bundles, or policies whose status you want to closely monitor, you can add them to the Watch List. The Watch List provides the following information:

- ♦ **Agent:** For servers and workstations, displays whether the device's Endpoint Agent is currently connected () or disconnected ().
- ♦ : Displays whether the object has any critical messages.

- ♦ **Type:** Displays an icon representing the object's type. For example, a bundle might have a  icon to show that it is a Windows bundle. Or a device might have a  icon to show that it is a server. You can mouse over the icon to see a description.
- ♦ **Name:** Displays the object's name. You can click the name to go to the object's message log.

To add a device, bundle, or policy to the Watch List:

- 1 In Endpoint Management Console, click the **Home** tab.
- 2 In the Watch List panel, click **Add**, then select the type of object (device, bundle, or policy) that you want to add to the list.
- 3 In the selection dialog box, select the desired object, then click **OK** to add it to the Watch List.
For example, if you are adding servers, browse and select a server.

Objects remain in the Watch List until you remove them.

6 Audit Management

OpenText™ Endpoint Management enables you to successfully record and view activities that take place in your Endpoint Management system, by using the Audit Management feature. The Audit Management feature enables you to capture various events that occur in your zone. The details of a captured event can be used for security and compliance purposes, enabling you to identify who did what and on which system, when an important event occurs in your environment. Using this feature, you can centrally monitor activities related to all devices.

- ♦ [“Types of Audit Events” on page 37](#)
- ♦ [“Enabling an Event” on page 37](#)
- ♦ [“Viewing a Generated Event” on page 38](#)

Types of Audit Events

- ♦ **Change Events:** These events capture configuration changes made to the zone through Endpoint Management Console. You can capture a variety of changes ranging from bundle changes to Endpoint Management system changes. For example, you can configure an audit event that records the activity of an administrator assigning a bundle to a device.

The change events can be enabled for all devices in the zone or for individual devices.

Enabling an Event

To audit an event, you must first enable the event in Endpoint Management Console. You can enable the event at the zone or device level. An event that is enabled at the zone level applies to all devices in the zone, and an event that is enabled at the device level applies to only the selected device.

- 1 Log in to Endpoint Management Console.
- 2 (Zone) To enable events at the zone, click **Configuration > Management Zone Settings > Audit Management**.
or
(Devices) To enable events at the device, click **Devices > Managed Devices**. Locate the device in the Servers or Workstations folders, click the device object to display its properties, then click **Settings > Audit Management**.
- 3 Click **Events Configuration** to display the Events Configuration dialog page.
- 4 In the **Change Events** tab, click **Add** to display the Add Change Events dialog box.
For information about the change event categories, see [Endpoint Management Audit Management Reference](#).
- 5 Expand the **Change Events** tree and select the required event.

- 6 Specify the following information for the **Event Settings**:
 - ♦ **Event Classification**: Based on the importance of the event, select **Critical**, **Major**, or **Informational**.
 - ♦ **Days to Keep**: Indicate the number of days to keep the event before purging it.
- 7 Click **OK** to add the event.

You can edit or delete an event by selecting the event in the Event Configuration page and clicking **Edit** or **Delete** from the menu bar. To select multiple events at a time, press **Ctrl** and click to select.

Viewing a Generated Event

When an enabled event has occurred, an audit event is generated.

After an audit event is generated, you can access the details of the event from the following locations:

- ♦ **Dashboard**: You can view the audit data through the Endpoint Management Console Dashboard. The Dashboard has the following tabs:
 - ♦ **Dashboard**: From this tab you can see a summary of the audit events that have occurred in the zone. You can see key indicators about top events and impacted objects, and can drill into the event log view in a filtered manner. By default, this dashboard shows you an overview of events in the last 4 hours. If you want to see more data, you can change the time period.
 - ♦ **Events (Audit Log)**: This tab enables you to view all of the events that have occurred in the zone. The information is displayed in a format similar to the Events Configuration page. A count is displayed against those categories for which an event has been generated. For example, if a **Bundle Assignment Management** event has been generated, **1** is displayed against the Bundle Assignment Management category in the tree structure. When you click the event, the details of the event are displayed in the right pane.
- ♦ **(Change Events) Object Folders**: The **Audit** tab in the object folders (**Devices**, **Bundles**, **Polices**) enables you to view the audit events that are generated for all objects within the selected folder. For example, you can view the events generated for all bundles within a bundles folder. Hence, all bundle-related events can be viewed in the Bundles folder. The information is categorized similar to the **Events Configuration** page. You can browse through events that have occurred, and if you need more information, you can click the event to view the event details.
- ♦ **(Change Events) Objects**: You can also view the audit events for an object within the object folder. For example, if you select a particular bundle within a bundles folder, you can view the events generated for that specific bundle.

To view the generated event details:

- 1 Log in to Endpoint Management Console.
- 2 (Dashboard) To view the events in the Dashboard, click **Dashboard > Events**.
or
(Object Folder) To view the events for all objects in a folder (for example, a device folder, bundles folder, or policy folder), click the folder's **Details** link, then click the **Audit** tab.
or

(Object) To view the events for a specific object (for example, a device, bundle, or policy), click the object, then click the **Audit** tab.

(Devices Folder) To view the events in the Devices folder, in the left pane, click **Devices**. If the event has been performed on a server in the zone, click the server **Details**, or if the event has been performed on a managed device, click the workstation **Details**. Then click the **Audit** tab to view the Events screen.


3 Click the **Change Events** tab.

4 Expand the tree structure and navigate to the relevant category.

Depending on the number of audit events configured, the relevant count is displayed against the category.

5 Click the event.

The details of the generated event are displayed in the right pane.

NOTE: To view the details of the event in a new window, click 



Product Administration

The following sections provide information to help you use the Endpoint Management. Before attempting any of the sections, you should have already completed the configuration tasks in [Part I, “System Configuration,”](#) on page 7.

- ♦ [Chapter 7, “Quick List,”](#) on page 43
- ♦ [Chapter 8, “Configuration Management,”](#) on page 45

7 Quick List

After you have configured settings in the Management Zone (see [Section I, System Configuration](#)), you should review the concepts and tasks in the following sections:

- ♦ [“Configuration Management” on page 43](#)

Configuration Management

OpenText Configuration Management lets you manage a device’s configuration, including distributing software to the device, and applying Windows configuration policies. In addition, you can collect device hardware and software inventory to inform your upgrade and buying decisions.

The following tasks can be done as needed and in any order.

Task	Details
Distribute software	<p>Distribute software through bundles. Bundles include the software files and instructions required to install, launch, and uninstall (when necessary) the software. You can create bundles to distribute Windows Installer applications (both MSI and MSP), non-Windows Installer applications, Web URLs, and thin-client applications.</p> <p>For instructions, see “Distributing Software” on page 45.</p>
Apply policies	<p>Control device behavior through the application of policies. Endpoint Management lets you create and apply various policy types.</p> <p>For instructions, see “Applying Policies” on page 46.</p>
Scan devices to collect software and hardware inventory	<p>Scan devices to collect software and hardware inventories for the devices. The inventory information can help you make decisions about software distribution and hardware upgrades.</p> <p>For instructions, see “Collecting Software and Hardware Inventory” on page 47.</p>

8

Configuration Management

The following sections provide explanations and instructions for the tasks you can perform with Configuration Management. Depending on your environment and the functionality you plan to use, you might not need to know how to perform all tasks. For the ones you decide to learn about, you can review them in any order.

- ♦ [“Distributing Software” on page 45](#)
- ♦ [“Applying Policies” on page 46](#)
- ♦ [“Collecting Software and Hardware Inventory” on page 47](#)

Distributing Software

OpenText Configuration Management provides great flexibility in distributing software. You can distribute applications and individual files; simply make modifications to existing files on a device; install, remove, and roll back applications on your devices.

Software is distributed through the use of bundles. A bundle consists of all the files, configuration settings, installation instructions, and so forth required to deploy and manage the application or files on a device. When you assign a bundle to a device, you can install and launch it on the device according to the schedules (distribution, launch, and availability) that you define.

You can also view the summary of the assignment, distribution, install and launch status of the bundle, using the Bundle dashboard. For more information, see [Endpoint Management Software Distribution Reference](#).

You can create the following bundle types:

- ♦ **Windows Bundle:** Allows you to configure and manage applications on Windows devices.

Creating a Bundle

To create a software bundle, you use the Create New Bundle Wizard. In addition to helping you create the bundle, the wizard also lets you assign it to devices and create distribution, launch, and availability schedules.

- 1 In Endpoint Management Console, click the **Bundles** tab.
- 2 In the Bundles panel, click **New > Bundle** to launch the Create New Bundle Wizard.
- 3 Follow the prompts to create the bundle.

Click the **Help** button on each wizard page for detailed information about the page.

When you complete the wizard, the bundle is added to the Bundles panel. You can click the bundle to view and modify the bundle’s details.

- 4 Continue with the next section, [Assigning a Bundle](#).

Assigning a Bundle

After you create a bundle, you need to assign it to the devices where you want it installed. You can make assignments to devices.

- 1 In the Bundles panel, select the bundle you want to assign by selecting the check box next to it.
- 2 Click **Action** > **Assign to Device**.
- 3 Follow the prompts to assign the bundle.

Click the **Help** button on each wizard page for detailed information about the page.

Where to Find More Information

For more information about distributing software, see the [Endpoint Management Software Distribution Reference](#).

Applying Policies

OpenText Configuration Management lets you use policies to create a set of configurations that can be assigned to any number of managed devices. It helps you to provide the devices with a uniform configuration, and it eliminates the need to configure each device separately.

The following section contains the list of Windows Configuration policies that can be created and assigned to a managed device.

- ♦ **Local File Rights Policy:** Configures rights for files or folders that exist on the NTFS file systems.

The policy can be used to configure basic and advanced permissions for both local and domain groups. It provides the ability for an administrator to create custom groups on managed devices.
- ♦ **Power Management Policy:** Configures Power Management settings on the managed devices.
- ♦ **Printer Policy:** Configures Local, SMB, HTTP, TCP/IP, CUPS, and iPrint printers for Windows devices
- ♦ **Endpoint Agent Configuration Policy:** Allows you to administer and centrally manage the behavior and features of Application Explorer.

Creating a Policy

To create a policy, you use the Create New Policy Wizard. In addition to helping you create the policy, the wizard also lets you assign it to devices and decide whether to enforce the policy immediately or wait until the device refreshes its information.

- 1 In Endpoint Management Console, click the **Policies** tab.
- 2 In the Policies panel, click **New** > **Policy** to display the Select Platform page.
- 3 Select the policy category, then click **Next** to display the Select Policy Category page.
- 4 Select the category of policy you want to create, then click **Next**.
- 5 Select a Policy Type from the list of policies provided. Follow the on-screen prompts to create the policy.

Click the **Help** button on each wizard page for detailed information about the page.

When you complete the wizard, the policy is added to the Policies panel. You can click the policy to view the policy's details and modify assignments.

Assigning a Policy

After you create a policy, you need to assign it to the devices where you want it applied. You can make assignments to devices.

- 1 In the Policies panel, select the policy you want to assign by selecting the check box next to it.
- 2 Click **Action > Assign to Device**.
- 3 Follow the prompts to assign the policy.

Click the **Help** button on each wizard page for detailed information about the page.

When you complete the wizard, the assigned devices are added to the policy's Relationships page. You can click the policy to view the assignments.

Where to Find More Information

For more information about applying policies, see the [Endpoint Management Configuration Policies Reference](#).

Collecting Software and Hardware Inventory

OpenText Configuration Management lets you collect software and hardware information from devices. You can view the inventory for an individual device and generate inventory based on specific criteria.

For example, you want to distribute a software application that has specific processor, memory, and disk space requirements. You create two, one that lists all devices that meet the requirements and one that lists the devices that don't meet the requirements. Based on the , you distribute the software to the compliant devices and create an upgrade plan for the non-compliant devices.

By default, devices are automatically scanned at 1:00 a.m. the first day of each month. You can modify the schedule, as well as many other **Inventory** configuration settings, on the **Configuration** tab in Endpoint Management Console.

- ♦ [“Initiating a Device Scan” on page 47](#)
- ♦ [“Viewing a Device Inventory” on page 48](#)
- ♦ [“Generating an Inventory Report” on page 48](#)
- ♦ [“Where to Find More Information” on page 48](#)

Initiating a Device Scan

You can initiate a scan of a device at any time.

- 1 In Endpoint Management Console, click the **Devices** tab.
- 2 Navigate the **Servers** or **Workstations** folder until you locate the device you want to scan.

- 3 Click the device to display its details.
- 4 In the task list located in the left navigation pane, click **Server Inventory Scan** or **Workstation Inventory Scan** to initiate the scan.

The QuickTask Status dialog box displays the status of the task. When the task is complete, you can click the **Inventory** tab to view the results of the scan.

Viewing a Device Inventory

- 1 In Endpoint Management Console, click the **Devices** tab.
- 2 Navigate the **Servers** or **Workstations** folder until you locate the device you want to scan.
- 3 Click the device to display its details.
- 4 Click the **Inventory** tab.

Generating an Inventory Report

OpenText Configuration Management includes several standard reports. In addition, you can create custom to provide different views of the inventory information.

- 1 In Endpoint Management Console, click the **Configuration > Inventory** tab.
- 2 In the Inventory Standard panel, click **Software Applications**.
- 3 Click the **Operating System** report to generate the report.

Using the options at the bottom of the report, you can save the generated report as a Microsoft Excel spreadsheet, CSV (comma-separated values) file, PDF file, or PDF Graph file.

Where to Find More Information

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