

OpenText™ Endpoint Management Configuration Policies Reference

Legal Notice

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

© Copyright 2008 – 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
1.1 What Is a Policy?	7
1.2 What Is a Policy Group?	7
1.3 Understanding the Policy Types	8
1.4 Understanding the Features of a Policy	8
2 Creating Windows Configuration Policies	11
2.1 Local File Rights Policy	11
2.2 Power Management Policy	13
2.3 Printer Policy	16
2.4 Endpoint Agent Configuration Policy	21
3 Managing Policies	25
3.1 Creating Policies	25
3.2 Viewing the Policy's Summary	26
3.2.1 General	26
3.2.2 Policy Status	27
3.2.3 Message Log	28
3.3 Policy Groups	29
3.4 Editing Policies	30
3.5 Deleting Policies	31
3.6 Adding Policies to Groups	31
3.7 Assigning a Policy to Devices	32
3.8 Assigning the Local File Rights Policy to Devices Running Different Languages	33
3.9 Unassigning a Policy from Devices	34
3.10 Adding System Requirements for a Policy	34
3.10.1 Filter Conditions	34
3.10.2 Filter Logic	38
3.11 Disabling Policies	39
3.12 Enabling the Disabled Policies	40
3.13 Publish a Policy	40
3.13.1 Publish as New Version	40
3.13.2 Publish as New Policy	40
3.14 Reviewing the Status of the Policies at the Managed Device	41
3.15 Understanding Policy Versions	41
3.16 Managing Policy Versions	42
3.17 Older Policy Versions Retain Setting	43
3.18 Publishing a Sandbox	44
3.18.1 Publishing a Sandbox as a New Version	44
3.18.2 Publishing a Sandbox as a New Policy	44
3.18.3 Publishing Multiple Sandbox as New Versions	45

4	Managing Policy Groups	47
4.1	Creating Policy Groups	47
4.2	Renaming or Moving Policy Groups	48
4.3	Deleting a Policy Group	48
4.4	Assigning a Policy Group to Devices	49
4.5	Adding a Policy to a Group	49
5	Managing Folders	51
5.1	Creating Folders	51
5.2	Renaming or Moving Folders	51
5.3	Deleting a Folder	52
A	Troubleshooting Policy Management	53
A.1	General Policy Troubleshooting	53
A.2	Local File Rights Policy Errors	53
A.3	Printer Policy Errors	54
A.4	Printer Policy Troubleshooting	57
B	Best Practices	61
B.1	Local File Rights Policy	61
B.2	Windows Group Policy	61
B.3	Printer Policy	61

About This Guide

This *OpenText Configuration Management Policy Management Reference* includes information about Policy Management features and procedures to help you configure and maintain your Configuration Management system.

The information in this guide is organized as follows:

- ♦ [Chapter 1, “Overview,” on page 7](#)
- ♦ [Chapter 2, “Creating Windows Configuration Policies,” on page 11](#)
- ♦ [Chapter 3, “Managing Policies,” on page 25](#)
- ♦ [Chapter 4, “Managing Policy Groups,” on page 47](#)
- ♦ [Chapter 5, “Managing Folders,” on page 51](#)
- ♦ [Appendix A, “Troubleshooting Policy Management,” on page 53](#)
- ♦ [Appendix B, “Best Practices,” on page 61](#)

Audience

This guide is intended for OpenText™ Endpoint Management administrators.

Feedback

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

Additional Documentation

OpenText Configuration 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](#).

1 Overview

OpenText Configuration Management provides policies to configure operating system settings and select application settings. By applying a policy to multiple devices, you can ensure that all of the devices have the same configuration.

The following sections contain additional information:

- ♦ [Section 1.1, “What Is a Policy?,” on page 7](#)
- ♦ [Section 1.2, “What Is a Policy Group?,” on page 7](#)
- ♦ [Section 1.3, “Understanding the Policy Types,” on page 8](#)
- ♦ [Section 1.4, “Understanding the Features of a Policy,” on page 8](#)

1.1 What Is a Policy?

A policy is a rule that controls a range of hardware and software configuration settings on the managed devices. For example, an administrator can create policies to control browser bookmarks available in the browser, printers to access, and security and system configuration settings on the managed devices.

You can use the 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.

You can assign a policy directly to a device. You can also assign the policy to a folder or group where the device is a member. Assigning a policy to device groups rather than device folders is the preferred way, because a device can be a member of multiple device groups, but it can be a member of only one device folder.

On managed devices, each policy type is enforced by a Policy Handler or Enforcer, which makes all the configuration changes necessary to enforce or unenforce the settings in a given policy.

1.2 What Is a Policy Group?

A policy group is a collection of one or more policies. Creating policy groups eases the administration efforts in managing policies. You can create policy groups and assign them to managed devices the same way you would assign individual policies.

Because the policy inherits the group’s assignments, managing a policy group is easier than managing individual policies. For example, if multiple policies are included in a policy group and the policy group is assigned to a device or a device group, then all the policies included in the policy group are automatically assigned to the device or device group at the same time. You need not individually assign each policy to a device or a device group.

1.3 Understanding the Policy Types

OpenText™ Endpoint Management lets you create the following policy types:

- ♦ **Windows Configuration Policies:** Lets you configure policies supplied by OpenText Configuration Management that are used to manage configuration settings for Windows devices. The following policies are located in this category:
 - ♦ Endpoint Agent Configuration policy
 - ♦ Local File Rights policy
 - ♦ Power Management policy
 - ♦ Printer policy

1.4 Understanding the Features of a Policy

- ♦ A policy is applied to a device only if the policy is directly or indirectly associated to that device.

The Endpoint Agent Configuration policy, Local File Rights, Power Management policy, and Printer policy can be applied to a device.

- ♦ A policy can be associated to groups.

In Endpoint Management Console, devices can be organized by using groups. A device can be a member of multiple groups. If a policy is associated to a group of devices, it applies to all devices in that group.

- ♦ A policy can be associated to query groups.

In Endpoint Management Console, the devices can also be members of query groups. Query groups are similar to ordinary groups except that the membership is determined by a query defined by the administrator. All devices that satisfy the query become members of that device group. The query is evaluated periodically and the membership is updated with the results. An administrator can configure the periodicity of the evaluation. An administrator can also force an immediate refresh of a query group. Query groups act just like other groups where policies are concerned.

- ♦ Policies are chronologically ordered by default.

When multiple policies are associated to a device, group, or container, the associations are chronologically ordered by default. The administrator can change the ordering.

If a device belongs to multiple groups, the groups are ordered. Consequently, the policies associated to those groups are also ordered. The administrator can change the ordering of groups for a device at any time.

In addition, the policies in a policy group are ordered.

- ♦ Policies have a precedence configured to determine the policy that is effective for a device.

Many policies of the same type can be applied to a device through direct association and inheritance.

- ♦ Policies support system requirements.

You can specify the system requirements of a device in a policy. The policy is applied to a device only if the device meets the system requirements.

- ♦ OpenText Configuration Management supports singular and plural policies.

Singular Policy: If multiple policies of the same policy type are assigned to a device and the policy type is a Singular policy, then only the nearest associated policy meeting the system requirements is applied. If the policy type is associated to device, then two different policies can be assigned to device.

The Power Management policy and Endpoint Agent Configuration policy are singular policies.

Plural Policy: If multiple policies of the same policy type are assigned to a device and the policy type is a Plural type, then all policies meeting the associated system requirement are applied.

The Local File Rights policy and Printer policy are plural policies.

- ♦ Policies can be disabled.

When you create a policy in OpenText Configuration Management, the policy is enabled by default. You can disable it if you do not want to apply it on a device.

- ♦ OpenText Configuration Management allows you to resolve policy conflicts.

The set of effective policies is a subset of the set of assigned policies. The set of effective policies for a device is calculated by applying precedence rules, multiplicity rules, and system requirements filters on the set of assigned policies. Effective policies are calculated separately for devices. The Policy Conflict Resolution setting determines how device policies interact for a specific device combination.

Effective policies are calculated separately for devices. When a user logs in to a device, policies associated to the device must be applied. Policy Conflict Resolution settings are used only when policies of the same type are associated to both the device. This setting determines the precedence order among the policies associated to the device. The Policy Conflict Resolution settings are applied after the effective policies are calculated.

Policy Conflict Resolution settings are defined when associating a policy to a device. For each policy type, the Policy Conflict Resolution setting defined in the closest effective policy of that type is applied for all policies of that type.

A Policy Resolution Conflict setting can have one of the following values:

- ♦ **Device Precedence:** Select this option to apply policies that are associated to the devices.
- ♦ **Device Only:** Applies only the policies associated to the device.

NOTE: The Policy Conflict Resolution setting is taken from the device-associated policy with the highest precedence.

2 Creating Windows Configuration Policies

OpenText Configuration Management lets you create policies by using Endpoint Management Console.

The following sections contain step-by-step instructions about creating the Windows Configuration policies by using Endpoint Management Console:

- ♦ [Section 2.1, “Local File Rights Policy,” on page 11](#)
- ♦ [Section 2.2, “Power Management Policy,” on page 13](#)
- ♦ [Section 2.3, “Printer Policy,” on page 16](#)
- ♦ [Section 2.4, “Endpoint Agent Configuration Policy,” on page 21](#)

2.1 Local File Rights Policy

The Local File Rights policy allows you to configure 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.

- 1 In Endpoint Management Console, click the **Policies** tab.
- 2 In the **Policies** list, click **New**, then click **Policy**.

or

In the **Policy Tasks**, click **New Policy**.

The **Select Platform** page is displayed.

- 3 Select **Windows**, then click **Next**.
The **Select Policy Category** page is displayed.
- 4 Select **Windows Configuration Policies**, then click **Next**.
- 5 Select **Local File Rights Policy** as the **Policy Type**, then click **Next**
- 6 In the **Define Details** page fill in the following fields:

Policy Name: Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in Endpoint Management Console.

Folder: Type the name or browse to and select the Endpoint Management Console folder where you want the policy to reside. The default is `/policies`, but you can create additional folders to organize your policies.

Administrator Notes: Provide a short description of the policy’s content. This description displays in Endpoint Management Console.

- 7 Click **Next** to display the Configure Basic Properties page, then use the options on the page to configure the attributes.

The following table contains information about configuring a file or folder and the attributes associated with it:

Field	Details
File / Folder Path	<p>Allows you to specify the complete path of a file or folder on the managed device. You can use the Endpoint Management system variables or environment variables to specify the path.</p> <p>To configure system variables in Endpoint Management Console, click the Configuration tab > the Device Management setting in the Management Zone Settings panel > System Variables. Click the Help button for details about configuring system variables.</p>
Notify if the file or folder does not exist	<p>When you select this option, a message is sent to the Cloud Server. If a folder entered by the user is not present on the Endpoint Agent, then the policy fails to enforce on the managed device.</p> <p>If you de-select this option, even if a folder is not present on the Endpoint Agent, a message will not be sent to the Cloud Server and the policy will be enforced successfully on the managed device.</p>
Attributes	<p>Allows you to specify the attributes of a file or folder, such as Read only and Hidden.</p>

This page allows you to configure permissions for only one file or folder. If you want to assign permissions to multiple files or folders, then configure them in the Details page after creating the policy.

- 8 Click **Next** to display the Configure Permissions page, then use the options on the page to configure permissions for selected groups.

The following table contains information about configuring permissions:

Field	Details
Permission for Groups	<p>Allows you to configure permissions for groups.</p> <ol style="list-style-type: none">1. Click Add, then Click Group to select a group from the appropriate drop-down list. <p>NOTE: The domain group name should be specified as domaingroupname and not as domainname/domaingroupname.</p> <ol style="list-style-type: none">2. Select the type of permission you want to configure as Simple NTFS Permissions or All NTFS Permissions. Depending on the type of permission you select, a list of permissions are displayed. Configure the permissions as applicable to the selected group.3. By default, when a permission is set on a folder, all the subfolders and the files also inherit the permissions. If you want to restrict the inheritance of the rights to only the immediate child file or folder, select Restrict inheritance to immediate child files/folders only.4. Click OK.

Field	Details
Create Groups on the Managed Device if they Do not Exist	Creates a group for which permissions are configured; however the group does not exist on the managed device. With this option, you can create only local groups.
Remove Access Control Rules not Configured by Endpoint Management	Removes all access control entries for groups not configured by the Endpoint Management Local File Rights policy. Also, updates the existing access control entries for groups configured in the policy. After the policy is applied, any manual changes made to the permissions for group configured by the policy are lost when the policy is re-applied.
Inherit Applicable Access Rights Configured on Parent Folders	Select Yes if you want a file or folder to inherit applicable access control rules from its parent object. If you select No , inherited rules are removed. If you do not want to make any changes, select not configured on the managed device. At least one attribute, permission, or inheritance setting must be configured to create a policy. Without configuring any settings, you cannot create a policy.

NOTE: If the **Full Control** access right is denied for the Administrators or Authenticated Users group, the policy is successful only during the first enforcement. However, if the **Full Control** access right is denied for the Administrators or Authenticated Users group and the **Remove access control rules not configured by Endpoint Management** option is selected, the policy fails.

The unenforcement of the Local File Rights policy from a device fails if the Full Control access right is denied for the Administrators or Authenticated Users group in the policy.

- 9 Click **Next** to display the Summary page. Review the information and, if necessary, use the **Back** button to make changes to the information on the Summary page.
- 10 (Conditional) Select **Create as Sandbox**, if you want to create the sandbox version of the policy.
- 11 Click **Finish** to create the policy now, or select **Define Additional Properties** to specify additional information, such as policy assignment, **system requirements**, enforcement, status, and which group the policy is a member of.

2.2 Power Management Policy

The Power Management policy allows you to configure the Power Management settings on the managed devices by creating a power scheme. It lets you configure the plugged in and battery power management settings and assign them to a device .

- 1 In Endpoint Management Console, click the **Policies** tab.
- 2 In the **Policies** list, click **New**, then click **Policy**.
or
In the **Policy Tasks**, click **New Policy**.
The **Select Platform** page is displayed.
- 3 Select **Windows**, then click **Next**.
The **Select Policy Category** page is displayed.
- 4 Select **Windows Configuration Policies**, then click **Next**.
- 5 Select **Power Management Policy** as the **Policy Type**, then click **Next**.

6 In the **Define Details** page fill in the following fields:

Policy Name: Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in Endpoint Management Console.

Folder: Type the name or browse to and select the Endpoint Management Console folder where you want the policy to reside. The default is `/policies`, but you can create additional folders to organize your policies.

Administrator Notes: Provide a short description of the policy's content. This description displays in Endpoint Management Console.

7 Click **Next** to configure the power settings for a managed device.

8 In the Add Power Scheme Settings page fill in the following fields:

Scheme Name: The policy name specified on the Define Details page is automatically displayed. You can either retain the policy name for the scheme or specify a new scheme name. Endpoint Management creates a scheme with the specified name on the managed device.

Scheme Description: Provide a description for the power scheme. The description is displayed as a tooltip for the power scheme on the managed device.

Power Settings: To add power scheme settings to a device, refer to the following table:

Task	Description
Turn off hard disk after	How long your hard disk is inactive before the disk turns off.
Slide show	The duration for which you want the desktop background slide show to be active.
Power saving mode	The power saving mode for a wireless adapter.
Sleep after	How long your computer will be inactive before switching to sleep mode.
Allow hybrid sleep	If your system needs to save work it can, enter a low power state and resume work immediately.
Enable System Hibernation	If system hibernation is enabled or not.
Hibernate after	How long your system will be inactive before switching to hibernate mode.
Allow wake timer	If timed events should change the state of the computer from sleep mode to active mode.
USB selective suspend setting	If the USB selective suspend feature is turned Off or On.
Lid close action	The action that the computer takes when you close the lid of your mobile-PC.
Power button action	The action to be taken when you press the Power button.
Sleep button action	The action to be taken when you press the Sleep button.
Link state	The Active State Power Management mode to be used for PCI Express-based serial links when the links are idle or less active.
Minimum processor state	The minimum performance state of your processor.

Task	Description
System cooling policy	The cooling mode for your system.
Maximum processor state	The maximum performance state of your processor.
Dim display after	How long your system is inactive before the display dims.
Turn off display after	How long your system is inactive before the display turns off.
Display brightness	The normal brightness level of your system.
Dimmed display brightness	The display brightness when your monitor display is dimmed.
Enable adaptive brightness	If your monitor supports adaptive brightness.
When sharing media	What your computer does when sharing media files.
When playing video	The power optimization mode used by your computer's video playback pipeline.
JavaScript timer frequency	The power optimization mode used by your computer for Internet Explorer 9 and Internet Explorer 10 browsers.
Critical battery action	The action that your computer takes when the battery reaches the critical level.
Low battery level	The percentage of battery capacity remaining that initiates the low battery action.
Critical battery level	The percentage of battery capacity remaining that initiates the critical battery action.
Low battery notification	Whether a notification is shown when the battery capacity reaches the low level.
Low battery action	The action that your computer takes when battery capacity reaches the low level.
Reserve battery level	The percentage of battery capacity remaining that initiates reserve power action.

NOTE:

- ◆ We recommend that you configure the power scheme duration in the following descending order: System Hibernation > System Standby > Hard Disks > Monitor.
 - ◆ The values of System Standby and System Hibernation are interdependent. If you choose to set the state of these settings to **Not Configured**, in such a case, the other setting can only be set to either **Never** or **Not Configured**. This is to ensure that the 'Standby Timeout' is always lesser than the 'Hibernate Timeout'.
- For example, if you set a duration for the System Standby value and then set the System Hibernation value to **Not Configured**, the System Standby value automatically changes to **Not Configured**.
- ◆ When you apply power management settings on a Windows 10 managed device, the scheme name is displayed in the settings panel of the Windows Power Options console only for a system user.
-

2.3 Printer Policy

The Printer policy allows you to configure Local, SMB, HTTP, TCP/IP, CUPS, and iPrint printers on a Windows device.

1 In Endpoint Management Console, click the **Policies** tab.

2 In the **Policies** list, click **New**, then click **Policy**.

or

In the **Policy Tasks**, click **New Policy**.

The **Select Platform** page is displayed.

3 Select **Windows**, then click **Next**.

The **Select Policy Category** page is displayed.

4 Select **Windows Configuration Policies**, then click **Next**.

5 Select **Printer Policy** as the **Policy Type**, then click **Next**.

6 In the **Define Details** page fill in the following fields:

Policy Name: Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in Endpoint Management Console.

Folder: Type the name or browse to and select the Endpoint Management Console folder where you want the policy to reside. The default is `/policies`, but you can create additional folders to organize your policies.

Administrator Notes: Provide a short description of the policy's content. This description displays in Endpoint Management Console.

7 Click **Next** to display the Printer Identification page, then select the type of printer to be installed on the managed device.

8 Click **Next**, then skip to the appropriate step, depending on which printer type you chose in [Step 7](#):

- ♦ **Local Printer:** Continue with [Step 9](#).
- ♦ **Network Printer:** Skip to [Step 10](#).
- ♦ **iPrint Printer:** Skip to [Step 11](#).

NOTE: Create and assign separate policies for different platforms for a printer.

9 (Conditional) If you are configuring a local printer, refer to the following table for more information:

Field	Details
Name	Specify the name of the local printer that you want to configure on the target device.
Driver	Browse to and select a suitable driver for the printer. If the driver is not contained in the browser list, type in the correct model name. The driver must either be installed on the target device or specified in the enforced policies. The driver must be digitally signed by Microsoft.

Field	Details
Port	<p>Select the physical port to which the printer is added, such as LPT1, COM1 or Standard TCP/IP.</p> <p>NOTE: If you assign a TCP/IP Printer policy to a 11 SP1 or older version of the agent, the policy gets applied and then fails and sends errors to the server at every refresh, as it is not supported.</p> <p>Remove the association with the lower version of the agents from the TCP/IP printer policy, to prevent it from being applied at every refresh.</p>
IP Address	Specify the IP address of the local printer. This field appears only if you select Standard TCP/IP as the port.
Protocol	Specify the protocol of the local printer. You can select either RAW or LPR from the drop-down options. This field appears only if you select Standard TCP/IP as the port.
Port Number	Specify the port number for the protocol. Typically the port number is 9100. This field appears only if you select the RAW protocol on the Standard TCP/IP settings page.
Queue Name	Specify the queue name to be used by this port, if a name is required by your printer. This field appears only if you select the LPR protocol on the Standard TCP/IP settings page.
LPR Byte Counting Enabled	Choose this option if you encounter problems such as missing or incomplete documents when printing. When LPR byte counting is enabled, the system counts the number of bytes in a document before processing the print request. Most printers do not need byte counting enabled because it can be very time consuming. This field appears only if you select the LPR protocol on the Standard TCP/IP settings page.
SNMP Status Enabled	<p>Select this option if the printer attached to this port supports RFC1759. This field appears only if you select Standard TCP/IP as the port.</p> <p>Community Name: Specify a community name, for example: <i>public</i>.</p> <p>SNMP Device Index: Specify the device index, for example: <i>1</i>.</p>
Install a Driver	Select this option to install a driver on the target device. The driver installation must be non-interactive and silent. The supported driver installation types are .inf and .exe. For the .inf type, the driver files can be bundled in .zip or .tar formats. The .inf file can be specified directly if it is already available on the target device
Model Name	Browse to select the model name of the driver.
Driver File Path	<p>Specify the driver files either from a particular device where the browser is running or from a path on the managed device, such as C:\temp\nipp.zip.</p> <p>NOTE: While configuring the policy, if you are using a UNC path to access the Driver file, make sure the file you access must be on an anonymous share.</p>
Supported Platforms	Specify a platform for the driver. The platform information helps to select a suitable driver from the available drivers list, which is based on the installation platform.

Field	Details
Language of Installation	Select the installation language. Your choices are English (United States), French, German, Portuguese, Spanish, Italian, Chinese (Traditional), Chinese (Simplified), or Japanese.
Install Forcefully Even if the Driver is Already Installed	Select this option to force installation of the driver, even though it is already installed on the target device.

- 10 (Conditional) If you are configuring a Network printer, refer to the following table for more information:

Field	Details
Name / Location	Specify the UNC path or URL name of the HTTP, SMB or CUPS printer. For example, it is \\server-name\printer-name for an SMB printer, http://server:631/printers/myprinter for a CUPS printer, or http://server/printers/.myprinter/.printer for a HTTP printer. NOTE: Support for network printer that prompts for user credentials is not provided.
Driver	Browse to add and select a suitable driver for the Windows HTTP printer. You can ignore this for SMB printers. The driver must be digitally signed by Microsoft. However, if you choose to use a driver that is not digitally signed, see the Troubleshooting Scenario
Install a Driver	Use this option to install a driver on the target device. The driver installation is non-interactive and silent. The supported driver installation types is .inf and the .inf driver files can be bundled in .zip or .tar formats. The .inf file can be specified directly if it is already available on the target device. Ensure that the .inf file supports the installation of the driver.
Model Name	Browse to select the model name of the driver.
Driver File Path	Specify the driver files either from a particular device where the browser is running or from a path in the managed device, such as c:\temp\nip.zip. NOTE: While configuring the policy, if you are using a UNC path to access the Driver file, make sure the file you access must be on an anonymous share.
Supported Platforms	Specify a platform for the driver. The platform information helps to select a suitable driver from the available drivers list, which is based on the installation platform.
Language of Installation	Select the installation language. Your choices are English (United States), French, German, Portuguese, Spanish, Italian, Chinese (Traditional), Chinese (Simplified), or Japanese.
Install Forcefully Even if the Driver is Already Installed	Select this option to force the installation of the driver on the device every time the policy is applied on the device, even if the driver is already installed on the device.

- 11** (Conditional) If you are configuring an iPrint printer, refer to the following table for more information:

Field	Details
Name / Location	Specify the URI name of the iPrint printer. For example, <code>ipp://acme.com/ipp/servername</code> .
Update iPrint Printer while Installing the Driver	Select this option to update the printer driver and to reinstall the printer driver from the iPrint server while installing the iPrint printer.
Install iPrint Client	<p>Select this option to install the iPrint client on a target machine.</p> <p>The installation file can be either <code>nipp.zip</code> or <code>nipp-s.exe</code>, both of which are capable of carrying out non-interactive silent installation. These files can be uploaded from the machine where the browser is running.</p> <p>To install the iPrint client, you cannot use a <code>.exe</code> file that does not support a silent installation. For example, you cannot use a <code>nipp.exe</code> file to install iPrint client.</p>
iPrint Client Installer File Path	<p>Allows to specify the path to the iPrint Client Installer (which installs the iPrint client on the managed device).</p> <ul style="list-style-type: none">♦ On the Managed Device: Select this option to specify the path to the iPrint client installer on the managed device.♦ Select from this Device: Select this option to add the iPrint client installer as content with the policy. You can also distribute the iPrint client installer along with the policy. <p>If the installer file path is a UNC path, the iPrint Client dialog box is displayed until the installation process completes. This process can be performed only by users with administrative rights.</p>
Install Forcefully Even if the Driver is Already Installed	Select this option to force installation of the driver, even though it is already installed on the target device.
Configure iPrint Client	<p>Select this option to configure the iPrint proxy server.</p> <p>If the workstations are located outside the physical firewall, you can use this option to specify the proxy address followed by a <code>(:)</code> and the port number.</p>
Proxy Server	Specify the iPrint proxy server name. For example, <code>http://proxy.companyx.com:8080</code>

- 12** Click **Next** to display the Printing Preferences page, then use the options to specify the preferences. Refer to the following table for more information:

Field	Details
Orientation	Select this option to specify the paper layout for the printer, such as landscape or portrait.
Duplex Printing	Specify whether or not to print on both sides of the paper, if the printer has that capability.

Field	Details
Collate	Specify whether or not the printer should organize multiple copies of a document, if the printer has that capability.
Print Quality	Select the print quality. Select High quality, for the best possible resolution, or select Low quality for lower resolution and lower quality.
Paper Source	Specify the paper source for the printer. A source that is not listed in the standard available list can also be specified, but it must be supported by the printer. Information on supported paper sources is available in the printer documentation or in the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\printer-name\DsDriver\printBinNames on a Windows machine.
Paper Size	Specify the paper size for the printer. You can specify any paper size supported by the printer, in addition to the options listed in the menu. Information on supported sizes is available in the printer documentation or in the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\printer-name\DsDriver\printMediaSupported on a Windows machine, where a printer is locally installed.

- 13** Click **Next** to display the Additional Printer Policy settings, then use the options to specify the settings. Refer to the following table for more information:

Field	Details
Set as Default Printer	Select this option to specify a printer as the default printer to which the print requests are sent if no other printer is specified by the user. On a Windows 7 managed device, the assigned printer might be set as a default printer on the device even if the Set as Default Printer option is not selected in the policy.
Remove all Printers not Specified by Printer Policies	Select this option to remove all printers that are not specified through the Printer policy.

- 14** Click **Next** to display the Summary page. Review the information and, if necessary, use the Back button to make changes to the information on the Summary page.
This wizard allows you to configure only one printer. If you want to configure additional printers, then configure them in the Details page after creating the policy.
- 15** (Conditional) Select **Create as Sandbox**, if you want to create the sandbox version of the policy.
- 16** Click **Finish** to create the policy now, or select **Define Additional Properties** to specify additional information, such as policy assignment, **system requirements**, enforcement, status, and which group the policy is a member of.
Only the preferences that are supported by the printer are configured on that printer.

2.4 Endpoint Agent Configuration Policy

The Endpoint Agent Configuration Policy allows you to administer and centrally manage the behavior and features of Application Explorer.

1 In Endpoint Management Console, click the **Policies** tab.

2 In the **Policies** list, click **New**, then click **Policy**.

or

In the **Policy Tasks**, click **New Policy**.

The **Select Platform** page is displayed.

3 Select **Windows**, then click **Next**.

The **Select Policy Category** page is displayed.

4 Select **Windows Configuration Policies**, then click **Next**.

5 Select **Endpoint Agent Configuration Policy** as the **Policy Type**, then click **Next**.

6 In the **Define Details** page fill in the following fields:

Policy Name: Provide a name for the policy. The policy name must be different than the name of any other item (group, folder, and so forth) that resides in the same folder. The name you provide displays in Endpoint Management Console.

Folder: Type the name or browse to and select the Endpoint Management Console folder where you want the policy to reside. The default is `/policies`, but you can create additional folders to organize your policies.

Administrator Notes: Provide a short description of the policy's content. This description displays in Endpoint Management Console.

7 Click **Next** to display the Application Explorer Configuration Settings page, then use the options to specify the settings. Refer to the following table for more information:

Field	Details
Allow the end user to pin bundles	Use this option to enable users to pin bundles to the Start menu and Taskbar. The values are Yes , No , and Unconfigured . If you select the value as Unconfigured , the default value No is set on the managed device.
Allow the end user to pin bundles	Enables user to pin bundles to Start and Taskbar. If you select the value as Unconfigured , the default value No is set on the managed device.
Show the All Folder in Application Explorer and Applications Portal	Specifies whether All folder should be displayed when you start the Application Explorer and Applications Portal. If you select the value as Unconfigured , the default value Yes is set on the managed device.
Enables users to manage favorites	Use this option to allow the user to set one or more applications as favorites. If you select the value as Unconfigured , the default value Yes is set on the managed device. Hence, this setting should be applied to restrict the user from managing favorites

Field	Details
Enable Folder View	<p>Use this option to display a folder list in the application window.</p> <p>The values are Yes, No, and Unconfigured. If you select the value as Unconfigured, the default value Yes is set on the managed device.</p>
Expand the Entire Folder Tree	<p>Use this option to expand the entire folder tree when the application window is opened.</p> <p>The values are Yes, No, and Unconfigured. If you select the value as Unconfigured, the default value No is set on the managed device.</p>
Display as the default folder	<p>Use this option to set the selected folder as the default folder when the application window is opened.</p> <p>The values are All, Favorites, or the Last viewed folder as the default folder. If you select the value as Unconfigured, the last viewed folder is set as the default folder</p>
Display Applications in Windows Explorer	<p>Use this option to display the application list in Windows Explorer.</p> <p>The values are Yes, No, and Unconfigured. If you select the value as Unconfigured, the default value Yes is set on the managed device.</p>
Name of Root Folder	<p>Use this option to change the name of the root folder.</p>
Hide the Agent Tray Icon	<p>Use this option to hide the Agent icon in the taskbar.</p> <p>The values are Yes, No, and Unconfigured. If you select the value as Unconfigured, the default value No is set on the managed device.</p>
Show Default Notifications	<p>Use this option to specify whether the default notification should be displayed. The notification is displayed when the content associated with a policy or a bundle is downloaded on the device. For example, during the enforcement of the Printer policy on a device, the following message is displayed in the notification area of the device:</p> <p>Downloading Files for Printer Policy</p> <p>The values are Yes, No, and Unconfigured. If you select the value as Unconfigured, the default value Yes is set on the managed device.</p>
Show Technician Portal Help	<p>Specifies whether the technician portal should be displayed.</p> <p>If you select the value as Unconfigured, the default value Yes is set on the managed device.</p>
Enable Manual Refresh	<p>Use this option to specify whether manual refresh of applications is enabled after starting Application Explorer.</p> <p>The values are Yes, No, and Unconfigured. If you select the value as Unconfigured, the default value Yes is set on the managed device.</p>
View Progress	<p>Use this option to specify whether the progress of the bundle operations should be displayed.</p> <p>The values are Yes, No, and Unconfigured. If you select the value as Unconfigured, the default value Yes is set on the managed device.</p>

- 8 Click **Next** to display the Summary page. Review the information and, if necessary, use the Back button to make changes to the information on the Summary page.
- 9 (Conditional) Select **Create as Sandbox**, if you want to create the sandbox version of the policy.
- 10 Click **Finish** to create the policy now, or select **Define Additional Properties** to specify additional information, such as policy assignment, [system requirements](#), enforcement, status, and which group the policy is a member of.

3 Managing Policies

OpenText Configuration Management lets you use effectively manage software and content in your system. In addition to editing and deleting existing objects, you can create new objects and perform various tasks on the objects.

You can use Endpoint Management Console to manage policies. This section explains how to perform this task by using Endpoint Management Console.

- ♦ [Section 3.1, “Creating Policies,” on page 25](#)
- ♦ [Section 3.2, “Viewing the Policy’s Summary,” on page 26](#)
- ♦ [Section 3.3, “Policy Groups,” on page 29](#)
- ♦ [Section 3.4, “Editing Policies,” on page 30](#)
- ♦ [Section 3.5, “Deleting Policies,” on page 31](#)
- ♦ [Section 3.6, “Adding Policies to Groups,” on page 31](#)
- ♦ [Section 3.7, “Assigning a Policy to Devices,” on page 32](#)
- ♦ [Section 3.8, “Assigning the Local File Rights Policy to Devices Running Different Languages,” on page 33](#)
- ♦ [Section 3.9, “Unassigning a Policy from Devices,” on page 34](#)
- ♦ [Section 3.10, “Adding System Requirements for a Policy,” on page 34](#)
- ♦ [Section 3.11, “Disabling Policies,” on page 39](#)
- ♦ [Section 3.12, “Enabling the Disabled Policies,” on page 40](#)
- ♦ [Section 3.13, “Publish a Policy,” on page 40](#)
- ♦ [Section 3.14, “Reviewing the Status of the Policies at the Managed Device,” on page 41](#)
- ♦ [Section 3.15, “Understanding Policy Versions,” on page 41](#)
- ♦ [Section 3.16, “Managing Policy Versions,” on page 42](#)
- ♦ [Section 3.17, “Older Policy Versions Retain Setting,” on page 43](#)
- ♦ [Section 3.18, “Publishing a Sandbox,” on page 44](#)

3.1 Creating Policies

For step-by-step instructions on creating Windows policies, see [Chapter 2, “Creating Windows Configuration Policies,” on page 11](#).

3.2 Viewing the Policy's Summary

The Summary page of a policy displays the following panels:

- ♦ [Section 3.2.1, "General," on page 26](#)
- ♦ [Section 3.2.2, "Policy Status," on page 27](#)
- ♦ [Section 3.2.3, "Message Log," on page 28](#)

3.2.1 General

The General panel provides a summary of the policy's general settings. Click the headings below for descriptions of the settings.

Policy Type

Displays the type of policy.

Size

Click **Compute** to display the size of the content associated with the policy.

Version

Displays the policy's version number.

Enabled

Displays whether or not the policy can be deployed to managed devices.

If a policy is enabled, it can be deployed to managed.

If you disable a policy that has already been deployed to some managed devices, the policy is removed from those devices. Also, it cannot be deployed to new devices .

Number of Errors Not Acknowledged

An error is anything that causes the deployment or installation of the policy to fail. The number displayed indicates the number of unacknowledged errors, which are any errors that you have not specifically marked as acknowledged. Unacknowledged errors are displayed in the Message Log section.

Number of Warnings Not Acknowledged

A warning is anything that does not cause the deployment or installation of the policy to fail, but indicates minor problems with the policy. The number displayed indicates the number of unacknowledged warnings, which are any warnings that you have not specifically marked as acknowledged. Unacknowledged warnings are displayed in the Message Log section.

GUID

Lists the policy's GUID (global unique identifier), a randomly generated string that provides a unique identifier for the policy. You cannot edit the GUID.

Original Created Date

Displays the timestamp (Month, date, year and time) when the policy was created and saved for the first time. The author of the policy will also be displayed in this field.

Version Created Date

Displays the timestamp (Month, date, year and time) when the current version of the policy was created. The version created date will be updated only when the policy version is changed.

Modified Date

Displays the timestamp (Month, date, year and time) when the policy was modified. The modifier name is also displayed in this field.

Administrator Notes

Displays the policy's description, if one was provided when the policy was created. The description appears in Endpoint Management Console and the Endpoint Agent (on managed devices). Click [Edit](#) to change the description.

Content Status

The Content Status field displays the current status of the content on a bundle or policy. The following are statuses:

- ♦ Available: The content is physically present on a bundle or policy and available for distribution.
- ♦ Not Applicable: The content is not uploaded to a bundle or policy.
- ♦ Not Applicable: The content is not uploaded to a bundle or policy.
- ♦ In-progress: The content is not yet physically present on a bundle or policy but is currently being uploaded.
- ♦ Failed: The content set to be hosted on a bundle or policy has failed.

3.2.2 Policy Status

The Policy Status panel displays a summary of the policy's assignment and enforcement status. The **Device** row displays the status of the policy through assignment to devices. A policy can be directly assigned or assigned through membership in a folder or group. You can click an underlined link in any column to view the status of the individual devices to which the policy is assigned, retry a failed policy, or export the data to a CSV file.

A policy's status is calculated using the status of many events. The numbers in the various columns represent an overall view of the policy's status.

NOTE: The Policy Status panel on the policy's sandbox or the older versions page does not display the status. However, the Policy Status panel on the policy's published version page displays the status of the policy's published version, sandbox, and the older versions.

The policy status information is separated into the following groups, which are independent of each other. For example, it is possible for an installation to be successful, but the launch to be unsuccessful.

Assignment Status

The following status information is available:

Targeted: Displays the number of devices on which the policy is enforced.

Devices Effective: Displays the number of devices on which the policy is effective through a device assignment. A policy is effective for a device if the device meets the system requirements of the policy. The number of devices in the **Devices Effective** column might be less than the number in the **Targeted** column because the policy might be enforced on a device that does not meet the policy's system requirements. For example, you might have a Windows policy enforced on a Linux device, but the policy is not effective for that device.

Devices Not Effective: Displays the number of devices on which the policy is not effective through a device assignment. If a policy is not effective for the device, it means that the device does not meet the policy's system requirements.

Pending: The pending status for the device displays the number of devices on which the policy is not yet enforced, such as devices that are switched off. Click the underlined link to display the list of such devices.

Enforcement Status

The following status information is available:




Devices Pending: Displays the number of devices on which the policy is pending. A policy's status is pending if the policy has met the device's system requirements, but the policy has not been enforced on the device.

Devices Succeeded: Displays the number of devices on which the policy was successfully enforced.

Devices Failed: Displays the number of devices on which the policy's enforcement failed.

3.2.3 Message Log

The Message Log panel displays all unacknowledged messages generated for the object. An unacknowledged message is one that you have not yet reviewed and marked as acknowledged.

- ♦ **Status:** Displays an icon indicating the type of message:  critical,  warning, and  normal.
- ♦ **Message:** Displays a brief description of the event that occurred.
- ♦ **Date:** Displays the date and time the event occurred.

NOTE: The Message Log panel on the policy's sandbox or the older versions page does not display any messages. However, the Message Log panel on the policy's published version page displays the messages of the policy's published version, sandbox, and the older versions.

A message remains in the Message Log list until you acknowledge it. You can acknowledge individual messages, acknowledge all messages at one time, or view more information about both acknowledged and unacknowledged messages. The following table explains how to do these tasks:

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 decide that you do not want to acknowledge the message, click Finished to dismiss 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 Management system.

3.3 Policy Groups

A policy group consists of two or more policies. Creating policy groups eases administration efforts by letting you assign the group, rather than each individual policy, to devices. You can create a policy group with a single policy and then add policies to the group as and when required.

- 1 In Endpoint Management Console, click the **Policies** tab.
- 2 In the **Policies** list, click **New**, click **Policy Group** to display the Basic Information page, then fill in the fields:
Group Name: Provide a unique name for your policy group. The name you provide displays in the Endpoint Management Console interface.
Folder: Type the name or browse to and select the folder that contains this policy group
Description: Provide a short description of the policy group's content. This description displays in Endpoint Management Console.
- 3 Click **Next** to display the Add Group Members page. You can add any number of policies to the group. You cannot add other policy groups to the group.

To add a policy:

3a Click **Add** to display the Select Members dialog box.

Because you are adding policies to the group, the Select Members dialog box opens with the **Policies** folder displayed.

3b Browse for and select the policies you want to add to the group. To do so:

3b1 Click **⚡** next to a folder to navigate the folders until you find the policy you want to select.

If you know the name of the policy you are looking for, you can also use the **Item name** box to search for the policy.

3b2 Click the underlined link in the **Name** column to select the policy and display its name in the **Selected** list.

3b3 (Optional) Repeat **Step 3b1** and **Step 3b2** to add additional policies to the **Selected** list.

3b4 Click **OK** to add the selected policies to the group.

4 Click **Next** to display the Summary page. Review the information and, if necessary, use the **Back** button to make changes to the information on the Summary page.

5 (Conditional) Select **Create as Sandbox**, if you want to create the sandbox version of the policy.

6 Click **Finish** to create the policy group now, or select **Define Additional Properties** to specify additional information, such as device assignment, and which members the policy group is a member of.

3.4 Editing Policies

The following table lists the tasks you can perform for a policy:

Task	Steps	Additional Details
Edit the content of a policy	<ol style="list-style-type: none">1. Click the policy whose content you want to edit.2. Click the Details tab, then edit the settings according to your requirements.3. Click Apply.4. Click the Summary page.5. Increment the version of the policy to enforce the changes made to the policy on the managed device.	
Rename a policy	<ol style="list-style-type: none">1. Select the check box next to the policy.2. Click Edit > Rename, then specify the new name.3. (Conditional) Select Publish changed display name immediately.4. Click OK.	<p>If more than one check box is selected, the Rename option is not available in the Edit menu.</p> <p>If a sandbox exists, the policy is updated to a sandbox.</p> <p>If a sandbox does not exist, you can choose to publish the policy as a new version or update to a sandbox.</p>

Task	Steps	Additional Details
Create a copy of the policy	<ol style="list-style-type: none"> 1. Select the check box next to the policy. 2. Click Edit > Copy, then specify a new name. 	<p>If more than one check box is selected, the Copy option is not available in the Edit menu.</p> <p>The copy option is useful to create a new policy that is similar to an existing policy. You can copy a policy and then edit the new policy's settings.</p>
Move a policy to a different folder	<ol style="list-style-type: none"> 1. Select the check box next to the policy (or policies). 2. Click Edit > Move, then select the target folder. 	
Copy the system requirements of one policy to another policy	<ol style="list-style-type: none"> 1. Select the check box next to the policy. 2. Click Edit > Copy System Requirements. 3. Select Policies, then click Add to select the policies to which you want to copy the selected policy's system requirements. 	<p>If more than one check box is selected, the Copy System Requirements option is not available in the Edit menu.</p>

3.5 Deleting Policies


- 1 In Endpoint Management Console, click the **Policies** tab.
- 2 Select the check box next to the policy (or policies) that you want to delete.
- 3 Click **Delete**.

3.6 Adding Policies to Groups

- 1 In Endpoint Management Console, click the **Policies** tab.
- 2 Select the check box next to the policy (or policies) that you want to add to the group.
- 3 Click **Action > Add to Group** to display the Existing Group or a New Group page.
- 4 You can add the selected objects (devices, bundles, policies) to an existing group or a new group.
 - ♦ If the group to which you want to add the objects already exists, select **Add selected items to an existing group**, then click **Next** to continue with [Step 5](#).
 - ♦ If you need to create a new group for the selected objects, select **Create a new group to contain the selected items**, then click **Next** to skip to [Step 6](#).
- 5 (Conditional) If you are adding selected items to an existing group, the Targets page is displayed. Select the groups to which you want to add the objects (devices, bundles, policies).
You can add any number of policies to the group. You cannot add other policy groups to the group.
 - 5a Click **Add** to display the Select Groups dialog box.

Because you are adding policies to the group, the Select Members dialog box opens with the **Policies** folder displayed.

5b Browse for and select the policies you want to add to the group. To do so:

5b1 Click  next to a folder to navigate the folders until you find the policy you want to select.

If you know the name of the policy you are looking for, you can also use the **Item name** box to search for the policy.

5b2 Click the underlined link in the **Name** column to select the policy and display its name in the **Selected** list.

5b3 (Optional) Repeat [Step 5a](#) and [Step 5b](#) to add additional policies to the **Selected** list.

5b4 Click **OK** to add the selected policies to the group.

5c Click **Next** to skip to [Step 7](#).

6 (Conditional) If you are creating a new group to contain the selected items, the Basic Information page is displayed. Fill in the following fields, then click **Next** to continue with [Step 7](#).

Group Name: Provide a unique name for your policy group. The name you provide displays in the Endpoint Management Console interface.

Folder: Type the name or browse to and select the folder that contains this policy group

Description: Provide a short description of the policy group's content. This description displays in Endpoint Management Console.

7 On the Finish page, review the information and, if necessary, use the **Back** button to make changes to the information.

8 Click **Finish**.

3.7 Assigning a Policy to Devices

Certain key points that you must be aware of before you assign a policy to a device are as follows:

- ♦ If you are assigning a Local File Rights policy to a network made up of devices running different languages, see [Section 3.8, "Assigning the Local File Rights Policy to Devices Running Different Languages,"](#) on page 33.


Perform the following steps to assign a policy to a device:

1 In Endpoint Management Console, click the **Policies** tab.

2 In the **Policies** list, select the check box next to the objects such as policies or policy groups.

3 Click **Action > Assign to Device**.

4 Browse for and select the devices, device groups, and device folders to which you want to assign the group. To do so:

4a Click  next to a folder (for example, the **Workstations** folder or **Servers** folder) to navigate through the folders until you find the device, group, or folder you want to select.

If you are looking for a specific item, such as a Workstation or a Workstation Group, you can use the **Items of type** list to limit the types of items that are displayed. If you know the name of the item you are looking for, you can use the **Item name** box to search for the item.

- 4b Click the underlined link in the **Name** column to select the device, group, or folder and display its name in the **Selected** list box.
- 4c Click **OK** to add the selected devices, folders, and groups to the **Devices** list.
- 5 Click **Next** to display the Policy Conflict Resolution page.
- 6 Set the priority for device-associated policies for resolving conflicts that arise when policies of the same type are associated to both devices.
 - ♦ **User Last:** Select this option to apply policies that are associated to devices first and then the users.
 - ♦ **Device Last:** Select this option to apply policies that are associated to users first and then the devices.
 - ♦ **Device Only:** Select this option to apply policies that are associated only to devices.
 - ♦ **User Only:** Select this option to apply policies that are associated only to users.
- 7 Click **Next** to display the Finish page, review the information and, if necessary, use the **Back** button to make changes to the information.

If you want the policies to be immediately enforced on all the assigned devices, select **Enforce Policies Immediately on all Assigned Devices**.

Policies might not be enforced immediately if the server is loaded, the duration for policies to be enforced on the managed devices depends upon the server load.
- 8 Click **Finish**.

The following points are applicable when you assign a policy to a device:

- ♦ If device-associated policies is effective for a device, only the policy that takes precedence according to the Policy Conflict Resolution settings is applied on the device. However, the **Effective** status for both policies is displayed as **Success** in the Endpoint Agent icon
- ♦ On a managed device, if you launch a published application that is installed on a Citrix server having iPrint policy configured, it might take considerable time for the policy to be enforced on the server. During this period, the iPrint functionality is not available for the application.

3.8 Assigning the Local File Rights Policy to Devices Running Different Languages

- 1 Create a separate Local File Rights policy for each language. For more information on creating the policy, see [Section 2.1, “Local File Rights Policy,” on page 11](#).
- 2 Add a filter for each policy:
 - 2a Click the policy, then click **Requirements**.
 - 2b Click **Add Filter**, select the **Registry Key Value** condition, then specify the following:

Key:

```
\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\WOW
\boot.description
```

Value: language.dll

Comparator: = (String Type)

Value Data: *language*

For example, on a device with the English language, **language** is **English (American)**. You can use the registry editor to determine the value data of the language.

2c Click **Apply**.

- 3 Assign the policy to the device. For more information on assigning a policy to a device, see [Section 3.7, “Assigning a Policy to Devices,” on page 32](#).

3.9 Unassigning a Policy from Devices

- 1 In Endpoint Management Console, click the **Policies** tab.
- 2 In the **Policies** list, click the policy you want to unassign.
- 3 Click **Relationships**.
- 4 In the Device Assignments panel, select the devices from which you want to unassign the policy.
- 5 Click **Remove**.

3.10 Adding System Requirements for a Policy

The System Requirements panel lets you define specific requirements that a device must meet for the specified version of the policy to be assigned to it. You can choose to edit the requirement.

You define requirements through the use of filters. A filter is a condition that must be met by a device in order for the policy to be applied. For example, you can add a filter to specify that the device must have exactly 512 MB of RAM in order for the policy to be applied, and you can add another filter to specify that the hard drive be at least 20 GB in size.

To create system requirements for a policy:

- 1 In Endpoint Management Console, click the **Policies** tab.
- 2 Click the underlined link for the desired policy to display the policy’s Summary page.
- 3 Click the **Requirements** tab.
- 4 Click **Add Filter**, select a filter condition from the drop-down list, then fill in the fields.

As you construct filters, you need to know the conditions you can use and how to organize the filters to achieve the desired results. For more information, see [Section 3.10.1, “Filter Conditions,” on page 34](#) and [Section 3.10.2, “Filter Logic,” on page 38](#).

- 5 (Conditional) Add additional filters and filter sets.
- 6 Click **Apply** to save the settings.

3.10.1 Filter Conditions

You can choose from any of the following conditions when creating a filter:

Bundle Installed: Determines if a specific policy is installed. After specifying the bundle, the two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the specified bundle must already be installed to meet the requirement. If you select **No**, the bundle must not be installed.

Connected: Determines if the device is connected to a network. The two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the device must be connected to the network to meet the requirement. If you select **No**, it must not be connected.

Connection Speed: Determines the speed of the device's connection to the network. The condition you use to set the requirement includes an operator and a value. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible values are bits per second (**bps**), kilobits per second (**Kbps**), megabits per second (**Mbps**), and gigabits per second (**Gbps**). For example, if you set the condition to >= 100 Mbps, the connection speed must be greater than or equal to 100 megabits per second to meet the requirement.

Disk Space Free: Determines the amount of free disk space on the device. The condition you use to set the requirement includes a disk designation, an operator, and a value. The disk designation must be a local drive map (for example, c: or d:). The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible values are bytes (**Bytes**), kilobytes (**KB**), megabytes (**MB**), and gigabytes (**GB**). For example, if you set the condition to c: >= 80 MB, the free disk space must be greater than or equal to 80 megabytes to meet the requirement.

Disk Space Total: Determines the amount of total disk space on the device. The condition you use to set the requirement includes a disk designation, an operator, and a value. The disk designation must be a local drive map (for example, c: or d:). The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible values are bytes (**Bytes**), kilobytes (**KB**), megabytes (**MB**), and gigabytes (**GB**). For example, if you set the condition to c: >= 40 GB, the total disk space must be greater than or equal to 40 gigabytes to meet the requirement.

Disk Space Used: Determines the amount of used disk space on the device. The condition you use to set the requirement includes a disk designation, an operator, and a value. The disk designation must be a local drive map (for example, c: or d:). The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible values are bytes (**Bytes**), kilobytes (**KB**), megabytes (**MB**), and gigabytes (**GB**). For example, if you set the condition to c: <= 10 GB, the used disk space must be less than or equal to 10 gigabytes to meet the requirement.

Environment Variable Exists: Determines if a specific environment variable exists on the device. After specifying the environment variable, the two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the environment variable must exist on the device to meet the requirement. If you select **No**, it must not exist.

Environment Variable Value: Determines if an environment variable value exists on the device. The condition you use to set the requirement includes the environment variable, an operator, and a variable value. The environment variable can be any operating system supported environment variable. The possible operators are **equal to**, **not equal to**, **contains**, and **does not contain**. The possible variable values are determined by the environment variable. For example, if you set the condition to Path contains c:\windows\system32, the Path environment variable must contain the c:\windows\system32 path to meet the requirement.

File Date: Determines the date of a file. The condition you use to set the requirement includes the filename, an operator, and a date. The filename can be any filename supported by the operating system. The possible operators are **on**, **after**, **on or after**, **before**, and **on or before**. The possible dates are any valid dates. For example, if you set the condition to appl.msi on or after 6/15/07, the appl.msi file must be dated 6/15/2007 or later to meet the requirement.

File Exists: Determines if a file exists. After specifying the filename, the two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the specified file must exist to meet the requirement. If you select **No**, the file must not exist.

File Size: Determines the size of a file. The condition you use to set the requirement includes the filename, an operator, and a size. The filename can be any file name supported by the operating system. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible sizes are designated in bytes (**Bytes**), kilobytes (**KB**), megabytes (**MB**), and gigabytes (**GB**). For example, if you set the condition to `doc1.pdf <= 3 MB`, the `doc1.pdf` file must be less than or equal to 3 megabytes to meet the requirement.

File Version: Determines the version of a file. The condition you use to set the requirement includes the filename, an operator, and a version. The filename can be any file name supported by the operating system. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=).

Be aware that file version numbers contain four components: Major, Minor, Revision, and Build. For example, the file version for `calc.exe` might be 5.1.2600.0. Each component is treated independently. For this reason, the system requirements that you set might not provide your expected results. If you do not specify all four components, wildcards are assumed.

For example, if you set the condition to `calc.exe <= 5`, you are specifying only the first component of the version number (Major). As a result, versions 5.0.5, 5.1, and 5.1.1.1 also meet the condition.

However, because each component is independent, if you set the condition to `calc.exe <= 5.1`, the `calc.exe` file must be less than or equal to version 5.1 to meet the requirement.

IP Segment: Determines the device's IP address. After specifying the IP segment name, the two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the device's IP address must match the IP segment. If you select **No**, the IP address must not match the IP segment.

Memory: Determines the amount of memory on the device. The condition you use to set the requirement includes an operator and a memory amount. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The memory amounts are designated in megabytes (**MB**) and gigabytes (**GB**). For example, if you set the condition to `>= 2 GB`, the device must have at least 2 gigabytes of memory to meet the requirement.

Operating System - Windows: Determines the service pack level, server type, and version of Windows running on the device. The condition you use to set the requirement includes a property, an operator, and a property value. The possible properties are **service pack**, **server type**, and **version**. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The property values vary depending on the property. For example, if you set the condition to `version = Windows XP Versions`, the device's Windows version must be XP to meet the requirement.

NOTE: Be aware that operating system version numbers contain four components: Major, Minor, Revision, and Build. For example, the Windows 2000 SP4 release's number might be 5.0.2159.262144. Each component is treated independently. For this reason, the system requirements that you set might not provide your expected results.

For example, if you specify **Operating System - Windows** in the first field, **Version** in the second field, **>** in the third field, and **5.0 -Windows 2000 Versions** in the last field, you are specifying only the first two components of the version number: Major (Windows) and Minor (5.0). As a result, for the requirement evaluated to true, the OS will have to be at least 5.1 (Windows XP). Windows 2003 is version 5.2, so specifying **> 5.2** will also evaluate to true.

However, because each component is independent, if you specify the version **> 5.0**, Windows 2000 SP4 evaluates to false because the actual version number might be 5.0.2159.262144. You can type **5.0.0** to make the requirement evaluate as true because the actual revision component is greater than 0.

When you select the OS version from the drop-down, the Major and Minor components are populated. The Revision and Build components must be typed in manually.

Process Running: Determines if a process is running. After specifying the process name, the two conditions you can use to set the requirement are Yes and No. If you select Yes, the specified process must be running to meet the requirement. If you select No, the process must not be running.

Processor Family: Determines the device's processor type. The condition you use to set the requirement includes an operator and a processor family. The possible operators are equals (=) and does not equal (<>). The possible processor families are **Pentium**, **Pentium Pro**, **Pentium II**, **Pentium III**, **Pentium 4**, **Pentium M**, **WinChip**, **Duron**, **BrandID**, **Celeron**, and **Celeron M**. For example, if you set the condition to **<> Celeron**, the device's processor can be any processor family other than Celeron to meet the requirement.

Processor Speed: Determines the device's processor speed. The condition you use to set the requirement includes an operator and a processor speed. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), and is less than or equal to (<=). The possible processor speeds are hertz (**Hz**), kilohertz (**KHz**), megahertz (**MHz**), and gigahertz (**GHz**). For example, if you set the condition to **>= 2 GHz**, the device's speed must be at least 2 gigahertz to meet the requirement.

Registry Key Exists: Determines if a registry key exists. After specifying the key name, the two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the specified key must exist to meet the requirement. If you select **No**, the key must not exist.

Registry Key Value: Determines if a registry key value exists on the device. The condition you use to set the requirement includes the key name, the value name, an operator, a value type, and a value data. The key and value names must identify the key value you want to check. The possible operators are equals (=), does not equal (<>), is greater than (>), is greater than or equal to (>=), is less than (<), is less than or equal to (<=). The possible value data is determined by the key, value name, and value type.

If the value type is **String Type**, Endpoint Management compares only those values in the registry if the actual type in the registry is REG_STRING or REG_EXPANDED_STRING.

If the value type is **Integer**, Endpoint Management compares only those values in the registry if the actual type in the registry is REG_DWORD.

Leave the key value field blank to use the default value. The default value of a registry key has no name and is displayed in regedit as (Default).

For example, if you specify `HKEY_LOCAL_MACHINE\SOFTWARE\OpenText\Messenger\Login` as the key name, `Port` as the value name, select `=` as the operator, select **Integer Type** as the value type, and specify `443` as the value data, the port specified as the value data must match with the port specified in the registry key to meet the requirement.

If the value type is **IP Address**, Endpoint Management compares only those values in the registry if the actual type in the registry is `REG_STRING`.

If you have set the condition to **Registry Key Value** and selected **IP Address** as the value type, then the two conditions that you can use to set the requirements are **Is in Subnet** and **Is not in Subnet**. If you select **Is in Subnet**, then the thin-client IP address of the device must be within a specific subnet. If you select **Is not in Subnet**, then the thin-client IP address of the device must be outside the subnet.

Specify the following in the text fields:

- ♦ Path of the registry key that should be compared
- ♦ Name of the registry value, for example: `ViewClient_IP_Address`
- ♦ IP Address of the network and a subnet mask to compare in order to determine if the device is within the segment (Example: `10.0.0.0/24`)

Registry Key and Value Exists: Determines if a registry key and value exists. After specifying the key name and value, the two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the specified key and value must exist to meet the requirement. If you select **No**, the key and value must not exist.

Service Exists: Determines if a service exists. After specifying the service name, the two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the service must exist to meet the requirement. If you select **No**, the service must not exist.

Service Running: Determines if a service is running. After specifying the service name, the two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the specified service must be running to meet the requirement. If you select **No**, the service must not be running.

Specified Devices: Determines if the device is one of the specified devices. After specifying the devices, the two conditions you can use to set the requirement are **Yes** and **No**. If you select **Yes**, the device must be included in the specified devices list to meet the requirement (an inclusion list). If you select **No**, the device must not be included in the list (an exclusion list).

3.10.2 Filter Logic

You can use one or more filters to determine whether the policy should be applied to a device. A device must match the entire filter list (as determined by the logical operators that are explained below) for the policy to be applied to the device.

There is no technical limit to the number of filters you can use, but there are practical limits, such as:

- ♦ Designing a filter structure that is easy to understand
- ♦ Organizing the filters so that you do not create conflicting filters

Filters, Filter Sets, and Logical Operators

You can add filters individually or in sets. Logical operators, either **AND** or **OR**, are used to combine each filter and filter set. By default, filters are combined using **OR** (as determined by the **Combine Filters Using** field) and filter sets are combined using **AND**. You can change the default and use **AND** to combined filters, in which case filter sets are automatically combined using **OR**. In other words, the logical operator that is to combine individual filters (within in a set) must be the opposite of the operator that is used between filter sets.

You can easily view how these logical operators work. Click both the **Add Filter** and **Add Filter Set** options a few times each to create a few filter sets, then switch between **AND** and **OR** in the **Combine Filters Using** field and observe how the operators change.

As you construct filters and filter sets, you can think in terms of algebraic notation parenthesis, 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 parenthesis.

For example, “(u AND v AND w) OR (x AND y AND z)” means “match either uvw or xyz.” In the filter list, this looks like:

```
u AND
v AND
w
OR
x AND
y AND
z
```

Nested Filters and Filter Sets

Filters and filter sets cannot be nested. You can only enter them in series, and the first filter or filter set to match the device is used. Therefore, the order in which they are listed does not matter. You are simply looking for a match to cause the policy to be applied to the device.

3.11 Disabling Policies

When you create a policy in OpenText Configuration Management, the policy is enabled by default. Policies can be disabled by an administrator. If a policy is disabled, it is not considered for enforcement on any of the devices that it applies to.

To disable a policy:

- 1 In Endpoint Management Console, click the **Policies** tab.
- 2 Select the check box next to the policy (or policies) that you want to disable.
- 3 Click **Action > Disable Policies**.

In the Policies list, the status of **Enabled** for the policy (or policies) is changed to **No**.

When you disable a policy that has already been enforced for some managed devices , the policy is removed from those devices and it is not enforced for new devices.

3.12 Enabling the Disabled Policies

- 1 In Endpoint Management Console, click the **Policies** tab.
- 2 Select the check box next to the policy (or policies) that you want to enable.
- 3 Click **Action > Enable Policies**.

In the Policies list, the status of the **Enabled** column for the policy (or policies) is changed to **Yes**.

3.13 Publish a Policy

The Publish Policy(s) option allows you to publish the sandbox as a new version of the policy or as a different policy.

3.13.1 Publish as New Version

Lets you create a new version of the policy that has the version number incremented by one from the latest available version of the policy.

Select the **Include policies from subfolders** option to enable all the policies that are within the subfolders of the selected folders to be published.

- 1 In Endpoint Management Console, click the **Policies** tab.
- 2 Select the check box next to the policy (or policies) that has a sandbox.
- 3 Click **Action > Publish Policy(s)**.
- 4 Follow the on-screen prompts. Click the **Help** button if you need additional information.

3.13.2 Publish as New Policy

Lets you create a new policy.

Name

Provide a name for the policy. The policy name must be different from the names of any other items (policy, group, folder, and so forth) that reside in the same folder. The name you provide displays in Endpoint Management Console and the Endpoint Agent (on managed devices).

Folder

Specify the name or browse to the Endpoint Management Console folder where you want the policy to reside. The default is `/Policies`, but you can create additional folders to organize your policies.

Create as Sandbox

Select the **Create as Sandbox** check box to enforce the policy as a sandbox version. A sandbox version of a policy enables you to try it in a test environment before actually implementing it on your device.

Select Groups

Lists all the available policy groups. Select the policy groups that the new policy should be a member of.


3.14 Reviewing the Status of the Policies at the Managed Device

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 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.

You cannot change the policies applied by your administrator. Policies are assigned to your device.

The Agent always enforces the device-assigned policies regardless of whether or not you are logged in. Therefore, device-assigned policies are enforced for all users of the device.

To view the policies assigned to your device:

- 1 Double-click the Endpoint Management icon  in the notification area.
- 2 In the left navigation pane, click **Policies**.

3.15 Understanding Policy Versions

Policy Change Management allows you to create either a sandbox-only policy or a Published version of the policy. If you edit a published version of the policy, a sandbox is created. You can choose to publish the sandbox either as a new version of the policy or a new policy.

For more information on publishing the sandbox, see [Section 3.18, “Publishing a Sandbox,” on page 44](#).

For more information on the policy versions, see [Section 3.16, “Managing Policy Versions,” on page 42](#).

The **Displayed Version** option on the policy’s page lists all the existing versions of the policy, and the latest version of the policy is selected by default. However, if a sandbox exists, the sandbox is selected by default.

Scenario:

- 1 Consider a policy named sos1 that is created as a sandbox. The **Displayed Version** option on the policy page lists **sandbox** and it is selected by default.
- 2 Click **Publish** to publish the sandbox to a new version. The **Displayed Version** option on the policy page now lists **0(Published)** and it is selected by default.
- 3 Edit the policy’s description to create a sandbox. The **Displayed Version** option on the policy page now lists **0(Published)** and **sandbox**. **sandbox** is selected by default.
- 4 Click **Publish** to publish the sandbox to a new version. The **Displayed Version** option on the policy page now lists **0(Published)**, and **1(Published)**. The policy’s latest version, **1(Published)**, is selected by default.

0(Published) is the older version of the policy.

- 5 Edit the policy's description again to create a sandbox. The **Displayed Version** option on the policy page now lists **0(Published)**, **1(Published)**, and **sandbox**. **sandbox** is selected by default.

0(Published) is the older version of the policy and **1(Published)** is the latest version of the policy.

- 6 Click **Publish** to publish the sandbox to a new version. The **Displayed Version** option on the policy page now lists **0(Published)**, **1(Published)**, **2(Published)**. The policy's latest version, **2(Published)**, is selected by default.

0(Published) and **1(Published)** are the older versions of the policy; and **2(Published)** is the latest version of the policy.

3.16 Managing Policy Versions

The **Displayed Version** option on the policy's page lists all existing versions of the policy, and the latest version of the policy is selected by default. However, if a sandbox exists, the sandbox is selected by default.

For more information on the policy versions, see [Section 3.15, "Understanding Policy Versions," on page 41](#).

Select the version of the policy whose details you want to view or edit.

Task	Steps	Additional Details
Create a sandbox from the published version of the policy	<ol style="list-style-type: none">1. Select the published version of the policy.2. Edit the policy.	<p>A single modification made to the policy creates a sandbox. The created sandbox is a copy of the policy and also includes the additional edit. However, the change is not made to the published version of the policy.</p> <p>Changes can now be made to the sandbox.</p> <p>You can revert a sandbox to the original version of the policy or publish a sandbox to create a new version or a new policy.</p>
Create a sandbox from an older version of the policy	<ol style="list-style-type: none">1. Select an older version of the policy.2. Click Create sandbox.	<p>The created sandbox is an exact copy of the policy.</p> <p>Changes can now be made to the sandbox.</p>
Publish a sandbox	<ol style="list-style-type: none">1. Select sandbox.2. Click Publish to display the Publish Option page.	<p>The sandbox must be published for the changes to be effective on the devices to whom the policy is assigned.</p>

Task	Steps	Additional Details
Revert a sandbox	<ol style="list-style-type: none"> 1. Select sandbox. 2. Click Revert to delete the sandbox. 	<p>All the changes made are discarded. The sandbox no longer exists.</p> <p>The published version of the policy is displayed in the Displayed Version option.</p>
Delete an older version of the policy	<ol style="list-style-type: none"> 1. Select an older version of the policy. 2. Click Delete Selected Version. 	<p>To delete all older versions of a policy or delete all versions older than a particular version, click Delete Older Versions under the Policy Tasks list located in the Endpoint Management Console left navigation pane.</p>

3.17 Older Policy Versions Retain Setting

Using the Policy Version Retain setting, you can configure the number of older policy versions that should be retained. This setting can be configured at the zone, folder and policy levels. The order of precedence is policy, folder and then zone.

To configure the policy version retain settings, perform the following steps:

In Endpoint Management Console, go to **Configuration > Management Zone Settings > Bundle, Policy and Content > Older Policy Version Retain Setting**.

Following are the available options to retain the version:

- ♦ **Retain all versions:** Select this option to retain all versions of the policy. This includes the published and sandbox versions.
- ♦ **Retain the specified number of older versions:** Select this option to specify the number of older versions of the policy to be retained.

The number that you specify should be a positive integer and it should not include the Published and Sandbox versions as they are retained by default. For example: If a policy has 5 versions and if you specify 2, then only the 2 versions prior to the currently published version will be retained along with Published and Sandbox versions. The remaining versions will be deleted.

- ♦ **Do not retain any older versions:** Select this option if you do not want to retain any older versions of policies in Endpoint Management. This option retains only the Published and Sandbox versions.

3.18 Publishing a Sandbox

The sandbox must be published for the changes to be effective on the devices to whom the policy is assigned. You can choose to publish the sandbox either as a new version or as a new policy. Review the following sections:

- ♦ [Section 3.18.1, “Publishing a Sandbox as a New Version,” on page 44](#)
- ♦ [Section 3.18.2, “Publishing a Sandbox as a New Policy,” on page 44](#)
- ♦ [Section 3.18.3, “Publishing Multiple Sandbox as New Versions,” on page 45](#)

3.18.1 Publishing a Sandbox as a New Version

Publishing a sandbox as a new version lets you create a new version of the policy that has a version number incremented by one from the latest available version of the policy.

To publish the sandbox as a new version:

- 1 In the **Displayed Version** option on the policy page, select **sandbox**.
- 2 Click **Publish** to display the Publish Option page.
- 3 Click **Publish as New Version**.
- 4 Click **Finish** to create a new published version.

For example, if the **Displayed Version** option on the policy page lists **0(Published)**, **1(Published)**, and **sandbox**, publishing the sandbox as a new version creates a version 2. The **Displayed Version** option on the policy page now lists **0(Published)**, **1(Published)**, and **2(Published)**.

3.18.2 Publishing a Sandbox as a New Policy

Publishing a sandbox as a new policy creates a new policy.

- 1 In the **Displayed Version** option on the policy page, select **sandbox**.
- 2 Click **Publish** to display the Publish Option page.
- 3 Click **Publish as New Policy**.
- 4 Specify a name for the policy.

The policy name must be different from the name of any other item (policy, group, folder, and so forth) that resides in the same folder. The name you provide displays in Endpoint Management Console and the Endpoint Agent (on managed devices).

For more information, see [“Naming Conventions in Endpoint Management Console”](#) in the [Endpoint Management Console Reference](#).

- 5 Specify the folder name or browse to the Endpoint Management Console folder where you want the policy to reside. The default is `/Policies`, but you can create additional folders to organize your policies.
- 6 Select the **Create as Sandbox** option to enforce the policy as a sandbox version. A sandbox version of a policy enables you to try it in a test environment before actually implementing it on your device.
- 7 Select the policy groups that the new policy should be a member of.
- 8 Click **Next** to display the **Select Assignments** page.

- 9 Select the device assignments that you want to apply to the new policy.
- 10 Click **Next**.
- 11 On the Summary Page, review the information and, if necessary, use the **Back** button to make changes to the information.
- 12 Click **Finish** to create the policy.

3.18.3 Publishing Multiple Sandbox as New Versions

Perform the following steps in the Endpoint Management Console:

- 1 Select a few policy folders, policy groups, and policies.
- 2 Click **Action > Publish Policy(s)** to display the Publish Options page.
- 3 (Conditional) Select the **Include policys from subfolders also** option to publish all the policies within the selected folders as new versions of the policies.
This option is displayed only if you have selected a policy folder in [Step 1](#).
- 4 Click **Next**. On the Select Policys page, select the policy you want to publish to next version, then click **Next**.
- 5 Click **Finish** to create a new published version.
For example, if the **Displayed Version** option on the policy page lists **0(Published)**, **1(Published)**, and **Sandbox**, publishing the sandbox as a new version creates a version 2. The **Displayed Version** option on the policy page now lists **0(Published)**, **1(Published)**, and **2(Published)**.

4 Managing Policy Groups

A policy group lets you group policies to ease administration and to provide easier assigning and scheduling of the policies in the policy group.

You can use Endpoint Management Console. This section explains how to perform this task using the Endpoint Management Console.

- ♦ [Section 4.1, “Creating Policy Groups,” on page 47](#)
- ♦ [Section 4.2, “Renaming or Moving Policy Groups,” on page 48](#)
- ♦ [Section 4.3, “Deleting a Policy Group,” on page 48](#)
- ♦ [Section 4.4, “Assigning a Policy Group to Devices,” on page 49](#)
- ♦ [Section 4.5, “Adding a Policy to a Group,” on page 49](#)

4.1 Creating Policy Groups

1 In Endpoint Management Console, click the **Policies** tab.

2 Click **New > Policy Group**.

3 Fill in the fields:

Group Name: Provide a name for the policy group. The name must be different than the name of any other item (policy, group, folder, and so forth) that resides in the same folder. The name you provide displays in Endpoint Management Console.

For more information, see [“Naming Conventions in Endpoint Management Console”](#) in the [Endpoint Management Console Reference](#).

Folder: Type the name or browse to and select the Endpoint Management Console folder where you want the policy to reside. The default is `/policies`, but you can create additional folders to organize your policies.

If you want to create the group in another folder, browse to and select the folder. By default, the group is created in the current folder.


Description: Provide a short description of the policy group's contents. This description displays in Endpoint Management Console.

4 Click **Next** to display the Add Group Members page, then specify policies to be members for the group.

You can add any number of policies to the group. You cannot add other policy groups to the group.

4a Click **Add** to display the Select Members dialog box.

Because you are adding policies to the group, the Select Members dialog box opens with the `Policies` folder displayed.

- 4b** Browse for and select the policies you want to add to the group. To do so:
- 4b1** Click  next to a folder to navigate the folders until you find the policy you want to select.
If you know the name of the policy you are looking for, you can also use the **Item name** box to search for the policy.
 - 4b2** Click the underlined link in the **Name** column to select the policy and display its name in the **Selected** list.
 - 4b3** (Optional) Repeat [Step 4a](#) and [Step 4b](#) to add additional policies to the **Selected** list.
 - 4b4** Click **OK** to add the selected policies to the group.
- 5** Click **Next** to display the Summary page. Review the information and, if necessary, use the **Back** button to make changes to the information.
- 6** (Conditional) Select **Create as Sandbox**, if you want to create the sandbox version of the policy.
- 7** (Optional) Select the **Define Additional Properties** option to display the group's properties page after the group is created. You can then configure additional policy properties.
- 8** Click **Finish** to create the group.

Before the policy group's contents are distributed to devices, you must continue with [Section 3.7, "Assigning a Policy to Devices,"](#) on page 32.

4.2 Renaming or Moving Policy Groups

Use the **Edit** drop-down list on the Policies page to edit an existing object. To access the **Edit** drop-down list, you must select an object by clicking the check box next to the object's name in the list.

Depending on the type of object you select, you can rename, copy, or move the selected object. For example, if you select a policy object, you can rename, copy, and move the policy. If you select a Policy Group object, you can rename or move the policy group object, but not copy it. If the option is dimmed, that option is not available for the selected object type.

Some actions cannot be performed on multiple objects. For example, if more than one check box is selected, the **Rename** option is not available from the **Edit** menu.

- 1** In Endpoint Management Console, click the **Policies** tab.
- 2** In the **Policies** list, select the box next to the policy group's name, click **Edit**, then click an option:
 - Rename:** Click **Rename**, provide a new name for the policy group, then click **OK**.
 - Move:** Click **Move**, select a destination folder for the selected objects, then click **OK**.

4.3 Deleting a Policy Group


Deleting a policy group does not delete its policies. It also does not unenforce the policies from devices where they have already been enforced. To unenforce the policy from devices, remove the assignment of each policy from the devices before deleting the policy group.

For information on unassigning policy from a device, see [Section 3.9, "Unassigning a Policy from Devices,"](#) on page 34.

To delete the policy group:

- 1 In Endpoint Management Console, click the **Policies** tab.
- 2 In the **Policies** list, select the check box next to the policy group (or policy groups).
- 3 Click **Delete**.

4.4 Assigning a Policy Group to Devices

- 1 In Endpoint Management Console, click the **Policies** tab.
- 2 In the **Policies** list, select the check box next to the policy group (or policy groups).
- 3 Click **Action > Assign to Device**.
- 4 Browse for and select the devices, device groups, and device folders to which you want to assign the group. To do so:
 - 4a Click  next to a folder (for example, the **Workstations** folder or **Servers** folder) to navigate through the folders until you find the device, group, or folder you want to select.
If you are looking for a specific item, such as a Workstation or a Workstation Group, you can use the **Items of type** list to limit the types of items that are displayed. If you know the name of the item you are looking for, you can use the **Item name** box to search for the item.
 - 4b Click the underlined link in the **Name** column to select the device, group, or folder and display its name in the **Selected** list box.
 - 4c Click **OK** to add the selected devices, folders, and groups to the **Devices** list.
- 5 Click **Next** to display the Finish page, review the information and, if necessary, use the **Back** button to make changes to the information.
- 6 Click **Finish**.

4.5 Adding a Policy to a Group

For more information, see [Section 3.6, “Adding Policies to Groups,” on page 31](#).

5 Managing Folders

A folder is an organizational object. You can use folders to structure your policies and policy groups into a manageable hierarchy for your Endpoint Management system. For example, you might want a folder for each type of policy, or, if applications are department-specific, you might want a folder for each department (Accounting Department folder, Payroll Department folder, and so forth).

The following sections contain additional information:

- ♦ [Section 5.1, “Creating Folders,” on page 51](#)
- ♦ [Section 5.2, “Renaming or Moving Folders,” on page 51](#)
- ♦ [Section 5.3, “Deleting a Folder,” on page 52](#)

5.1 Creating Folders

- 1 In Endpoint Management Console, click the **Policies** tab.
- 2 Click **New** > **Folder**.
- 3 Provide a unique name for your folder. This is a required field.

When you name an object in Endpoint Management Console (folders, policies, policy groups, and so forth), ensure that the name adheres to the naming conventions; not all characters are supported. For more information, see [“Naming Conventions in Endpoint Management Console”](#) in the *Endpoint Management Console Reference*.

- 4 Type the name or browse to and select the folder that will contain this folder in the Endpoint Management Console interface. This is a required field.
- 5 Provide a short description of the folder's contents.
- 6 Click **OK**.

5.2 Renaming or Moving Folders

Use the **Edit** drop-down list on the Policies page to edit an existing object. To access the **Edit** drop-down list, you must select an object by clicking the check box next to the object's name in the list.

Depending on the type of object you select, you can rename, copy, or move the selected object. For example, if you select a Policy object, you can rename, copy, and move the policy. If you select a Folder object, you can rename or move the Folder object, but not copy it. If the option is dimmed, that option is not available for the selected object type.

Some actions cannot be performed on multiple objects. For example, if more than one check box is selected, the **Rename** option is not available from the **Edit** menu.

- 1 In Endpoint Management Console, click the **Policies** tab.
- 2 In the **Policies** list, select the box next to the folder's name, then click **Edit**.

3 Select an option:

- ♦ **Rename:** Click **Rename**, provide a new name for the folder, then click **OK**.
- ♦ **Move:** Click **Move**, choose a destination folder for the selected objects, then click **OK**.

5.3 Deleting a Folder

Deleting a folder also deletes all of its contents (policies, policy groups, and subfolders).

- 1 In Endpoint Management Console, click the **Policies** tab.
- 2 In the **Policies** list, select the check box next to the folder (or folders).
- 3 Click **Delete**.

A

Troubleshooting Policy Management

The following sections contain detailed explanations of the error messages or problems you might encounter when using the OpenText Configuration Management policies.

- ♦ [Section A.1, “General Policy Troubleshooting,” on page 53](#)
- ♦ [Section A.2, “Local File Rights Policy Errors,” on page 53](#)
- ♦ [Section A.3, “Printer Policy Errors,” on page 54](#)
- ♦ [Section A.4, “Printer Policy Troubleshooting,” on page 57](#)

A.1 General Policy Troubleshooting

- ♦ [“Some of the policy settings might not get enforced on a Terminal Server session” on page 53](#)

Some of the policy settings might not get enforced on a Terminal Server session

Source: OpenText Configuration Management; Policy Management; Windows Configuration Policy.

Explanation: Some policies might not be applied when a user logs into a Terminal Server session. The policy would get automatically enforced during the next device refresh schedule. For example, iPrint policy maintenance settings that are configured in the Group policy are not applied to the device.

Possible Cause: Endpoint Management user daemon might not have started when the policies were getting enforced on the device.

Action: If you want to enforce the policy immediately on the device, you must manually refresh the Endpoint Agent in one of the following ways:

- ♦ Right-click the Endpoint Agent Tray icon, then select **Refresh**.
- ♦ In the command prompt, run the `zac ref` command.

A.2 Local File Rights Policy Errors

- ♦ [“The file or folder was not found while enforcing the policy” on page 53](#)

The file or folder was not found while enforcing the policy

Source: Endpoint Configuration Management; Policy Management; Windows Configuration Policy.

Possible Cause: This occurs when a file or folder configured in the policy is not found on the managed device.

Action: On the managed device, do the following:

- ♦ Verify whether the file or folder exists and the name and path are correct.
- ♦ Ensure that Windows Explorer is configured to display extensions for a file of a known type. In Windows Explorer, click **Tools > Folder Options** to display the Folder Options dialog box. Click the **View** tab, then ensure that the **Hide Extension for known file types** option is not selected.

A.3 Printer Policy Errors

- ♦ *“Printer driver installation failed for `printer_name`. The provided driver install file type is not supported” on page 54*
- ♦ *“Printer driver installation failed for `printer_name`. File extraction failed for `filename`” on page 54*
- ♦ *“Printer driver installation failed for `printer_name`. Check if provided drivers inf file is in proper format” on page 55*
- ♦ *“Unable to get iprint install file from the specified location in managed device, please check if file is there in specified location” on page 55*
- ♦ *“Unable to extract iprint client installer from the content” on page 55*
- ♦ *“Bad iprint install file. Unable to extract setupipp.exe file. Expectation is for a zip file which extracts setupipp.exe on the root. check the file mentioned for install” on page 55*
- ♦ *“iPrint client install failed. Check if the provided iprint client supports silent install” on page 56*
- ♦ *“Failed to add smb printer `printer_name`” on page 56*
- ♦ *“Failed to add iprint printer `printer_name`” on page 56*
- ♦ *“An incorrect error message that the iPrint policy could not be enforced is displayed on the managed device” on page 56*

Printer driver installation failed for `printer_name`. The provided driver install file type is not supported

Source: Endpoint Configuration Management; Policy Management; Windows Configuration Policy.

Possible Cause: The Printer policy supports only `.inf` drivers.

Action: A `.inf` type driver along with all the dependent files can be zipped or tarred and uploaded using the policy. If you have a self-extracting `exe`, extract it to a temporary location, compress it into a `.zip` file, then distribute it through the policy.

Printer driver installation failed for `printer_name`. File extraction failed for `filename`

Source: Endpoint Configuration Management; Policy Management; Windows Configuration Policy.

Possible Cause: The policy cannot extract the zipped or tarred files for the driver because the file might be corrupted.

Action: Ensure that the files are not corrupted by manually extracting the .tar or .zip file, then include the .tar or .zip file in the policy.

Printer driver installation failed for *printer_name*. Check if provided drivers inf file is in proper format

Source: Endpoint Configuration Management; Policy Management; Windows Configuration Policy.

Possible Cause: This error message can occur if the driver .inf file is not in proper format, or the .inf file does not contain installation instructions for the driver's model name.

Action: Extract the driver files and verify whether the driver's model name provided in the Printer policy is contained in the .inf file. The model name must exactly match the name contained in the file.

Unable to get iprint install file from the specified location in managed device, please check if file is there in specified location

Source: Endpoint Configuration Management; Policy Management; Windows Configuration Policy.

Possible Cause: The iPrint installer is not found on the managed device. This error message can occur if the location of the file is not correctly specified in the Printer policy, or the file resides in a shared network location and is not available to the Printer policy handler module.

Action: Ensure that the file exists on the managed device or it is directly associated to the Printer policy.

Unable to extract iprint client installer from the content

Source: Endpoint Configuration Management; Policy Management; Windows Configuration Policy.

Possible Cause: The iPrint client attached with the Printer policy is not available on the managed device. This error message can occur if the policy is enforced immediately after it's created.

Action: After creating the policy, wait for five to ten minutes before enforcing the policy, then try to log into the managed device.

Bad iprint install file. Unable to extract setupipp.exe file. Expectation is for a zip file which extracts setupipp.exe on the root. check the file mentioned for install

Source: Endpoint Configuration Management; Policy Management; Windows Configuration Policy.

Possible Cause: The Printer policy supports iPrint installation only in silent mode and does not require user intervention. Hence, `nipp-s.exe` or `nipp.zip` can be used, but not `nipp.exe`.

Action: If `nipp.zip` is used for installation, extract it to verify whether the installation file is correct and the extracted files contain `setupipp.exe`.

iPrint client install failed. Check if the provided iprint client supports silent install

Source: Endpoint Configuration Management; Policy Management; Windows Configuration Policy.

Possible Cause: The Printer policy supports iPrint installation only in silent mode and does not require a user intervention. Hence, `nipp-s.exe` or `nipp.zip` can be used, but not `nipp.exe`.

Action: If `nipp.zip` is used for installation, extract it to verify whether the installation file is correct and the extracted files contain `setupipp.exe`.

Failed to add smb printer *printer_name*

Source: Endpoint Configuration Management; Policy Management; Windows Configuration Policy.

Possible Cause: The SMB printer connection is not valid.

Action: Ensure that there is no problem in the network by using the UNC path to add the printer through the Windows Add Wizard.

Failed to add iprint printer *printer_name*

Source: Endpoint Configuration Management; Policy Management; Windows Configuration Policy.

Action: Verify whether the iPrint URL is correct. The iPrint URL must be specified in the format `ipp://server-address/ipp/printer name`.

Also, check if the iPrint client is installed on the target device. If the client is not installed, attach it through the Printer policy.

An incorrect error message that the iPrint policy could not be enforced is displayed on the managed device

Source: Endpoint Configuration Management; Policy Management; Windows Configuration Policy.

Explanation: The iPrint policy might take some time to install an iPrint printer on a device, depending on the size of the iPrint printer driver and the network connectivity. In such a scenario, even if the iPrint printer is successfully installed on the device, an incorrect message that the iPrint policy could not be enforced is displayed on the managed device.

Action: Ignore the error message and refresh the device.

The correct message indicating that the policy has been successfully enforced is displayed on the device after a manual or automatic refresh.

A.4 Printer Policy Troubleshooting

- ♦ [“Unable to install or update the printer drivers on re-enforcing the policy” on page 57](#)
- ♦ [“Installation of the iPrint printer fails on a device if the printer does not have the supported drivers” on page 57](#)
- ♦ [“Unable to enforce a printer policy on a managed device if the printer driver that is installed on the device is unsigned” on page 58](#)
- ♦ [“The Printer policy might fail to install an iPrint printer on a managed device if iPrint printer drivers are configured in the policy” on page 58](#)
- ♦ [“The Printer policy with a Samba or network printer installation does not complete as timeout for the Printer Driver installation command is not effective” on page 58](#)
- ♦ [“The iPrint policy fails when the iPrint client is uninstalled manually” on page 59](#)

Unable to install or update the printer drivers on re-enforcing the policy

Source: Endpoint Configuration Management; Policy Management; Windows Configuration Policy.

Explanation: The Printer policy installs the printer driver during the first enforcement of the policy. If the driver is changed after the first enforcement of the policy, the new drivers are not installed or updated on the subsequent enforcement of the policy.

Action: Create a new printer policy with the new driver and assign it to the same device or user.

Installation of the iPrint printer fails on a device if the printer does not have the supported drivers

Source: Endpoint Configuration Management; Policy Management; Windows Configuration Policy.

Explanation: If a printer configured in the iPrint policy has assigned drivers that are not supported by the operating system on the managed device, then the Installation of the printer fails.

Action: Before assigning a iPrint policy to a device, ensure that the drivers assigned to the printer configured in the policy are supported by the operating system on the device.

Unable to enforce a printer policy on a managed device if the printer driver that is installed on the device is unsigned

Source: Endpoint Configuration Management; Policy Management; Windows Configuration Policy.

Explanation: The printer driver that is installed on the device has not been digitally signed by Microsoft.

Action: Enable using unsigned drivers in the printer policy:

- 1 On the device, right-click **My Computers > Properties**.
- 2 In the System Properties window, click **Hardware > Driver Signing**.
- 3 Select **Ignore - Install the software anyway and don't ask for my approval**.

The Printer policy might fail to install an iPrint printer on a managed device if iPrint printer drivers are configured in the policy

Source: Endpoint Configuration Management; Policy Management; Windows Configuration Policy.

Explanation: The iPrint policy might fail to install the iPrint printer on a device if iPrint printer drivers are configured in the policy. You must not add iPrint printer drivers in the Printer Driver Installation panel of a printer policy details page because the iPrint drivers are automatically downloaded from the iPrint servers when the iPrint printer is installed on the device.

Action: Edit the policy to remove the iPrint printers from the Driver List in the Printer Driver Installation panel of the printer policy details page.

The Printer policy with a Samba or network printer installation does not complete as timeout for the Printer Driver installation command is not effective

Source: Endpoint Configuration Management; Policy Management; Windows Configuration Policy.

Explanation: If you are planning to install a Samba or a network printer by using a Printer policy, the Printer driver installation command that is invoked might need to wait more than the default timeout of 40 sec before terminating.

This can be controlled by setting the appropriate timeout value for the printer driver install command to complete.

Action: To change the default wait time value for the installation or configuration of a network or Samba printer, perform the following:

- 1 On a Windows managed device, open the Registry Editor.
- 2 Go to `HKLM\Software\OpenText\EndpointAgent\PrinterPolicy`.
- 3 Change the value for the `PrintWaitTime` parameter from the default value of 40 seconds to 200 seconds or higher.

The iPrint policy fails when the iPrint client is uninstalled manually

Source: Endpoint Configuration Management; Policy Management; Windows Configuration Policy.

Explanation: When the iPrint client is uninstalled manually and you apply the iPrint policy again, it fails.

Action: Reboot the system after uninstalling the iprint client.

B Best Practices

The following sections contain information on the best practices to follow when using the OpenText Configuration Management policies:

- ♦ [Section B.1, “Local File Rights Policy,” on page 61](#)
- ♦ [Section B.2, “Windows Group Policy,” on page 61](#)
- ♦ [Section B.3, “Printer Policy,” on page 61](#)

B.1 Local File Rights Policy

- ♦ For information on managing access control to files and folders, see [Microsoft’s Access Control Best Practices Web site](#).

B.2 Windows Group Policy

- ♦ Do not apply the Windows Group policy to a Windows managed device that is a part of the Microsoft domain and has a group policy from the Windows domain controller applied. The Endpoint Management Windows Group policy must be applied only if the group policy from the Windows domain controller is not applied.
- ♦ If you want the Windows Group policy settings to be applied to all users of a device, the settings must be configured as a part of a device-assigned policy. The user-assigned policies must contain only the configuration settings specific to the user to whom the policy is assigned.
- ♦ If you apply Local Group policies on a managed device that has Endpoint Management Group policies already applied, some of the settings might not work correctly.
- ♦ If you want to configure the security settings for a Endpoint Management Group Policy on a newly installed 64-bit Windows device, launch and close the Group Policy editor, `gpedit.msc`, before running the Group Policy Helper tool.

B.3 Printer Policy

You must not edit the Printer policy to add iPrint printer drivers in the Printer Driver Installation panel of a printer policy details page. This is because the iPrint drivers are automatically downloaded from the iPrint servers when the iPrint printer is installed on a device. However, you can add local or network printer drivers to the drivers list if the policy has local or network printers configured.

