

OpenText™ Endpoint Management Audit Management 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.novell.com/company/legal/>.

Copyright © 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 Audit Management Workflow	7
2 Audit Management Overview	9
2.1 Products That Include Auditing	9
2.2 Types of Audit Events	9
2.3 Audit Event Information	9
3 Working with Change Events	11
3.1 Change Event Categories.....	11
3.2 Enabling a Change Event.....	11
3.3 Viewing a Generated Change Event.....	12
3.4 Searching for Events	13
4 Common Tasks	15
4.1 Searching for Events	15
4.1.1 Search for Events	15
4.1.2 Perform an Advanced Search.....	15
4.2 Dashboard Details	16
A Troubleshooting	19

About This Guide

This *OpenText™ Endpoint Management Audit Management Reference* includes information to help you successfully record and view activities that take place in your Endpoint Management system.

The information in this guide is organized as follows:

- ♦ [Chapter 1, “Audit Management Workflow,” on page 7](#)
- ♦ [Chapter 2, “Audit Management Overview,” on page 9](#)
- ♦ [Chapter 3, “Working with Change Events,” on page 11](#)
- ♦ [Chapter 4, “Common Tasks,” on page 15](#)
- ♦ [Appendix A, “Troubleshooting,” on page 19](#)

Audience

This document is intended for administrators or individuals who are concerned with the auditing and monitoring of all actions performed in the zone. To understand and perform the procedures described in this document, you should have a working knowledge of Endpoint Management and its various features.

Feedback

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

Additional Documentation

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

1 Audit Management Workflow

To audit changes that occur in the zone, complete the following tasks in the order listed:

Task	Details
<input type="checkbox"/> Review concepts important to the successful auditing of changes that occur in the zone.	For information, see “Audit Management Overview” on page 9 .
<input type="checkbox"/> Understand the type of changes for which change events can be generated.	Change events capture any configuration changes made to the zone through Endpoint Management Console. For information about change events, see “Change Event Categories” on page 11 .
<input type="checkbox"/> Enable the change events you want to audit.	For information, see “Enabling a Change Event” on page 11
<input type="checkbox"/> View the generated event details in Endpoint Management Console.	For information about how to view a change event, see “Viewing a Generated Change Event” on page 12 .

2 Audit Management Overview

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

The following sections provide information to help you understand Endpoint Management Audit Management:

- ♦ [Section 2.1, “Products That Include Auditing,” on page 9](#)
- ♦ [Section 2.2, “Types of Audit Events,” on page 9](#)
- ♦ [Section 2.3, “Audit Event Information,” on page 9](#)

2.1 Products That Include Auditing

Auditing is provided for the following products: Endpoint Management.

2.2 Types of Audit Events

Audit events are of the following type:

- ♦ **Change Events:** These events capture configuration changes made to the zone through Endpoint Management Console. You can capture a variety of changes ranging from bundle changes to Endpoint Management system changes. For example, you can configure an audit event that records the activity of an administrator assigning a bundle to a device. For information about the various change events, see [Section 3.1, “Change Event Categories,” on page 11](#).

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

2.3 Audit Event Information

Each audit event captures the following information:

- ♦ **Message:** The configuration changes made in the zone.
- ♦ **Category:** The category of the event generated.
- ♦ **Date and Time:** The date and time at which the action was performed.
- ♦ **Initiator:** The email ID of the event initiator.
- ♦ **Targets:** The name of the target object. For example, Bundles, Policies, and Devices.
- ♦ **Classification:** The classification type of the event (Critical, Major, or Informational).
- ♦ **IP Address:** The IP address of the machine from where Endpoint Management is launched.

- ♦ **Session ID:** The session ID of the current session generated by the server.

You can view details of the generated Endpoint Management audit events in the Endpoint Management Console Dashboard. For information about the Dashboard, see [Section 4.2, “Dashboard Details,”](#) on page 16.

3 Working with Change Events

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

The following sections provide information to help you configure and monitor change events:

- ♦ [Section 3.1, “Change Event Categories,” on page 11](#)
- ♦ [Section 3.2, “Enabling a Change Event,” on page 11](#)
- ♦ [Section 3.3, “Viewing a Generated Change Event,” on page 12](#)
- ♦ [Section 3.4, “Searching for Events,” on page 13](#)

3.1 Change Event Categories

You can configure the following types of change events:

- ♦ **System:** When changes are made to the following objects:
 - ♦ **Settings:** When a zone setting or object setting is changed.
 - ♦ **Administration:** For all actions related to Endpoint Management Console login, administrator and enrollment token.
 - ♦ **Agent Update:** For the various stages of agent update deployment.
 - ♦ **Devices:** For all changes made to devices, device folders, and device groups.
 - ♦ **Bundles:** For all actions performed on bundles and bundle groups.
 - ♦ **Policies:** For all actions performed on policies, policy folders, and policy groups.

For information about how to configure change events, see [Enabling a Change Event](#).

3.2 Enabling a Change Event

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

- 1 Log in to Endpoint Management Console.
- 2 (Zone) To enable events at the zone, click **Configuration > Management Zone Settings > Audit Management**.
or

(Devices) To enable events at the device, click **Devices > Managed Devices**. Locate the device in the Servers or Workstations folders, click the device object to display its properties, then click **Settings > Audit Management**.

3 Click **Events Configuration** to display the Events Configuration dialog page.

4 In the **Change Events** tab, click **Add** to display the Add Change Events dialog box.

For information about the change event categories, see [Section 3.1, “Change Event Categories,” on page 11](#).

For this example, we are using the **Bundle Assignment Modified** event. However, depending on which event you want to enable, you can select the appropriate event category.

5 To select the **Bundle Assignment Modified** event, click **Change Events > System > Bundles**.

6 Select the **Bundle Assignment Modified** check box.

7 Specify the following information for the **Event Settings**:

- ♦ **Event Classification:** Based on the importance of the event, select **Critical**, **Major**, or **Informational**.
- ♦ **Days to Keep:** Indicate the number of days to keep the event before purging it.

8 Click **OK** to add the event.

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

You can also search for events that have been enabled by using the Search field in the **Events Configuration** page. For more information about how to search for events, see [Section 4.1, “Searching for Events,” on page 15](#).

3.3 Viewing a Generated Change Event

When an enabled change event has occurred, an audit event is generated. Hence, for the **Bundle Assignment Management** event used in this workflow, an audit event is generated when a bundle is assigned to a device. For information about how to assign a bundle to a device, see [“Managing Bundle Assignments” in the *Endpoint Management Software Distribution Reference*](#).

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


- ♦ **Dashboard:** You can view the audit data through the Endpoint Management Console Dashboard. The Dashboard has the following tabs:
 - ♦ **Dashboard:** From this tab, you can see a summary of the audit events that have occurred in the zone. You can see key indicators about top events and impacted objects, and you can drill into the event log view in a filtered manner. By default, this dashboard shows you an overview of events in the last 4 hours. If you want to see more data, you can change the time period. For more information about the event details listed in the Dashboard, see [Section 4.2, “Dashboard Details,” on page 16](#).
 - ♦ **Events (Audit Log):** This tab enables you to view all of the events that have occurred in the zone. The information is displayed in a format similar to the Events Configuration page. A count is displayed against those categories for which an event has been generated. For

example, if a **Bundle Assignment Management** event has been generated, **1** is displayed against the Bundle Assignment Management category in the tree structure. When you click the event, the details of the event are displayed in the right pane.

- ♦ **Object Folders:** The **Audit** tab in the object folders (**Devices**, **Bundles**, **Policies**) enables you to view the audit events that are generated for all objects within the selected folder. For example, you can view the events generated for all bundles within a bundles folder. Hence, all bundle-related events can be viewed in the Bundles folder. The information is categorized similar to the **Events Configuration** page. You can browse through events that have occurred, and if you need more information, you can click the event to view the event details.
- ♦ **Objects:** You can also view the audit events for an object within the object folder. For example, if you select a particular bundle within a bundles folder, you can view the events generated for that specific bundle.

To view the generated event details (Example: **Bundle Assignment Management** event):

- 1 Log in to Endpoint Management Console.
- 2 (Dashboard) To view the events in the Dashboard, click **Dashboard > Events**.
or
(Object Folder) To view the events for all objects in a folder (for example, a device folder, bundles folder, or policy folder), click the folder's **Details** link, then click the **Audit** tab.
or
(Object) To view the events for a specific object (for example, a device, bundle, or policy), click the object, then click the **Audit** tab.
- 3 Click the **Change Events** tab.
- 4 In the tree structure, click **Change Events** and expand the **System** category.
Depending on the number of audit change events configured, the relevant count is displayed against the change event category.
- 5 Click **Bundles > Bundle Assignment Modified**.
The details of the generated event are displayed in the right pane.

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

3.4 Searching for Events

You can search for specific events after they are generated. For information about how to search for an event, see [Section 4.1, “Searching for Events,” on page 15](#).

4 Common Tasks

The following sections provide information about change event tasks:

- ♦ [Section 4.1, “Searching for Events,” on page 15](#)
- ♦ [Section 4.2, “Dashboard Details,” on page 16](#)

4.1 Searching for Events

You can search for a specific event, or filter events based on category (**Critical**, **Major**, and **Informational**). You can also perform advanced searches and create, edit, and delete saved searches.

NOTE: Simple search results will include only event names that match the specified search entry. However, Advanced search results will include event names and categories that match the specified search entry.

Using the Search feature, you can perform the following tasks:

- ♦ [Section 4.1.1, “Search for Events,” on page 15](#)
- ♦ [Section 4.1.2, “Perform an Advanced Search,” on page 15](#)

4.1.1 Search for Events

To search for events at the zone, device, or object level:

- 1 In Endpoint Management Console, select the **Events** tab in the **Dashboard**, or the **Audit** tab in the required object folder (example, **Bundles** or **Policies**) or **Devices** folder (servers or workstations).
- 2 In the **Events** page, select the event category from the **Change Events** tab.
The search field is displayed.
- 3 Specify the name of the event in the search field (for example, **Bundle Assignment Management** or **File Transfer**), then press Enter.
Events that match your search criteria are displayed.

Whenever you perform a search, the name of the selected search is displayed next to the Search field. To clear the search, click x next to the search name.

4.1.2 Perform an Advanced Search

You can use the Advanced Search feature to search for events at the Zone or Device level.

- 1 In the Event Configuration screen, click the down-arrow next to the Search field.
A menu is displayed with various search-related options.

- 2 Click **Advanced Search** to display the Advanced Search screen.
- 3 Specify the following details:
 - ♦ **Search for:** Specify the name of the audit event.
 - ♦ **Event Class:** Select the classification type of the event.
 - ♦ **Initiator:** Specify the user name of the event initiator.
 - ♦ **Targets:** Specify the name of the target object. For example, Bundles, Policies, and Devices.
 - ♦ **IP Address:** Specify the IP address of the machine from where Endpoint Management is launched.
 - ♦ **Session ID:** Specify the session ID of the current session generated by the server.
- 4 To save the selected search criteria, select the Save search as check box, specify a search name, then click **Search**.

NOTE: If you have created saved searches, the search names will be displayed in the drop-down list. When you select a saved search name from the drop-down list, the relevant search results are displayed.

4.2 Dashboard Details

Audit data can be viewed through the Endpoint Management Console Dashboard. To access this page, click the Dashboard link in the left pane of Endpoint Management Console. From this page you can see a zone-wide view of the audit events that have been logged into the system. You can see key indicators about top events and impacted objects, and drill into the Events (Audit Log) view in a filtered manner. By default, the Dashboard displays an overview of events in the last 4 hours. If you want to view more data, you can choose alternative schedules.

When you log in to Endpoint Management Console and click Dashboard, the following information is displayed:

- ♦ **Top 5 Events:** The top 5 events generated by Endpoint Management Console administrators or managed devices, based on the event count. This list is not based on the classification type. Click the event name hyperlink to view the event details.
- ♦ **Top 5 Critical Events:** The top 5 events generated by Endpoint Management Console administrators or managed devices. This list is based on the maximum count for a particular event, with the classification type as **Critical**. Click the event name hyperlink to view the event details.
- ♦ **Top 5 Major Events:** The top 5 events generated by Endpoint Management Console administrators or managed devices. This list is based on the maximum count for a particular event, with the classification type as **Major**. Click the event name hyperlink to view the event details.
- ♦ **Top 5 Change Events by Administrator:** The top 5 events generated by a Endpoint Management administrator. This list is based on the maximum number of events generated by an administrator. Click the event name hyperlink to view the event details.
- ♦ **Top 5 Critical Events by User:** The top 5 events generated by users who have logged in to managed devices. This list is based on the maximum count for a particular event, generated by a managed device. Click the event name hyperlink to view the event details.

- ♦ **Top 10 Informational Events:** The top 10 events generated by Endpoint Management administrators, or managed devices. This list is based on the maximum count for a particular event, with the classification type as **Informational**. Click the event name hyperlink to view the event details.
- ♦ **Top 10 Devices:** The top 10 devices in the zone that are generating the maximum number of events. Click the device name hyperlink to view device details in the Audit Log panel.
- ♦ **Top 10 Referred Devices:** The top 10 devices in the zone on which the maximum events have occurred. The device might or might not be a target, but the actual target objects reside on this device. For example, a Primary Server on which a large number of bundles have been created can be a referred device. This is because although the target of change is the bundles, the events have occurred on the Primary Server.

A Troubleshooting

The following sections provide solutions to the problems you might encounter while using the Audit Management feature.

- ♦ [“Agent Event Advanced Search containing special characters does not return results” on page 19](#)
- ♦ [“Some audit event details are not localized based on the locale” on page 19](#)

Agent Event Advanced Search containing special characters does not return results

Source: Endpoint Management; Audit Management.

Explanation: Search containing special characters such as "\" does not return results.

Action: If the special characters search does not return results, you need to explicitly escape them in the search input. For example, if you want to search for a string such as `Workgroup\Win8`, you should specify `Workgroup\\Win8` in the search field.

Some audit event details are not localized based on the locale

Source: Endpoint Management; Audit Management.

Explanation: When an audit event is created in one locale, and the generated event details are viewed from another locale, some of the event details are not localized. For example, if you create a bundle by logging in to Endpoint Management Console using the **German** language, and then view details of the generated **Bundle Created** event by logging into Endpoint Management Console using the **English** language, the audit bundle name is displayed in German, as it is based on the user input. However, the type of bundle, for example Windows bundle, which should appear in English, appears in German.

Action: None.

