

Click 'Dashboard' > Audit Logs'

- Endpoint Manager logs all actions taken on managed devices by admins and staff. These logs can be useful when troubleshooting issues.
- Example logged actions include:
 - Add or remove devices
 - Apply a security profile
 - Create or edit a profile
 - Package installations
 - Remote take-over sessions
 - Changes to containment settings
 - Remote file transfers
 - Auto-removal of old / duplicate devices
- Each log entry is accompanied with details such as the staff member who applied the action, the affected device, the action taken, and more.
- Audit logs are maintained for up to a year for PCI-DSS compliance.

STAFF	EVENT NAME	AFFECTED OBJECT	OLD VALUE	NEW VALUE	EXTRA INFO	SESSION ID	LOG CREATION DATE
herculespopular22@...	File Transfer Favorites	TECHMONSTER	Application Packages	Application Packages	Type: Folder Session ID: 1049A802-3FE0-41FD-AEBF-B5177A4FFDDC Source Name: Application Packages Destination Name: Application Packages Local Path: D:/ Status: Changed	94c07fdc53ea4b44abff3786bdc2bed9	2019/11/22 03:54:25 PM
herculespopular22@...	File Transfer Favorites	TECHMONSTER		Application Packages	Type: Folder Session ID: 1049A802-3FE0-41FD-AEBF-B5177A4FFDDC Destination Name: Application Packages Local Path: D:/ Status: Added	94c07fdc53ea4b44abff3786bdc2bed9	2019/11/22 03:54:12 PM
herculespopular22@...	File Transfer session status	TECHMONSTER	Connecting	Connected	Session ID: 1049A802-3FE0-41FD-AEBF-B5177A4FFDDC	94c07fdc53ea4b44abff3786bdc2bed9	2019/11/22 03:09:35 PM
herculespopular22@...	File Transfer session status	TECHMONSTER	Starting	Connecting	Session ID: 1049A802-3FE0-41FD-AEBF-B5177A4FFDDC	94c07fdc53ea4b44abff3786bdc2bed9	2019/11/22 03:09:02 PM

The logs screen shows activities in chronological order.

- **Staff** - Username of the admin or staff member who executed the action.

- **Event Name** - The action executed on the device. Examples include device enrollment, remote installation of packages, remote take-overs and device removals.
- **Affected Object** - The device, device group, profile, procedure or file group on which the action was executed.
 - Click the name to view more details about the item.
- **Old Value** - The setting or value before the action was implemented.

For example, if a Comodo package is remotely updated, the old version number of the package is shown here.

- **New Value** - The setting or value after the action was implemented.

For example, if a Comodo package is remotely updated, the version number of the new package is shown here.

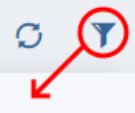
- **Extra Info** - Additional details about the action. These include devices on which the procedure was run, installation parameters, profiles applied/removed, malware quarantined, scans run and so on.

Script or patch procedures - Click 'Selected Devices' to view the devices on which the procedure was run.

- **Session ID** - String that identifies the connection session between the device and the EM server during the action.
- **Log Creation Date** - Date and time of the event.

Use the filters to view events of a specific type, events that affected a specific object, and more:

- Click the funnel icon at the top right.



OLD VALUE NEW VALUE EXTRA INFO SESSION ID

Type: Folder
Session ID:
1049A802-3FE0-41FD-
AEBF-B5177A4FFDDC
Source Name:

Log creation date

Start End

Staff

Component name

Endpoint Manager

Remote Control

Source

Device

Common

RBAC

Procedure

Profile

Device group

Antivirus

Patch Management

Global Software Inventory

System templates

Network discovery

Network device

License Management

Windows Client Settings

Network Profiles

Network Monitors

Two-Factor Authentication

Event name

Affected object

Old value

New value

Extra info

Session ID

You can filter items by various criteria or search for specific events.

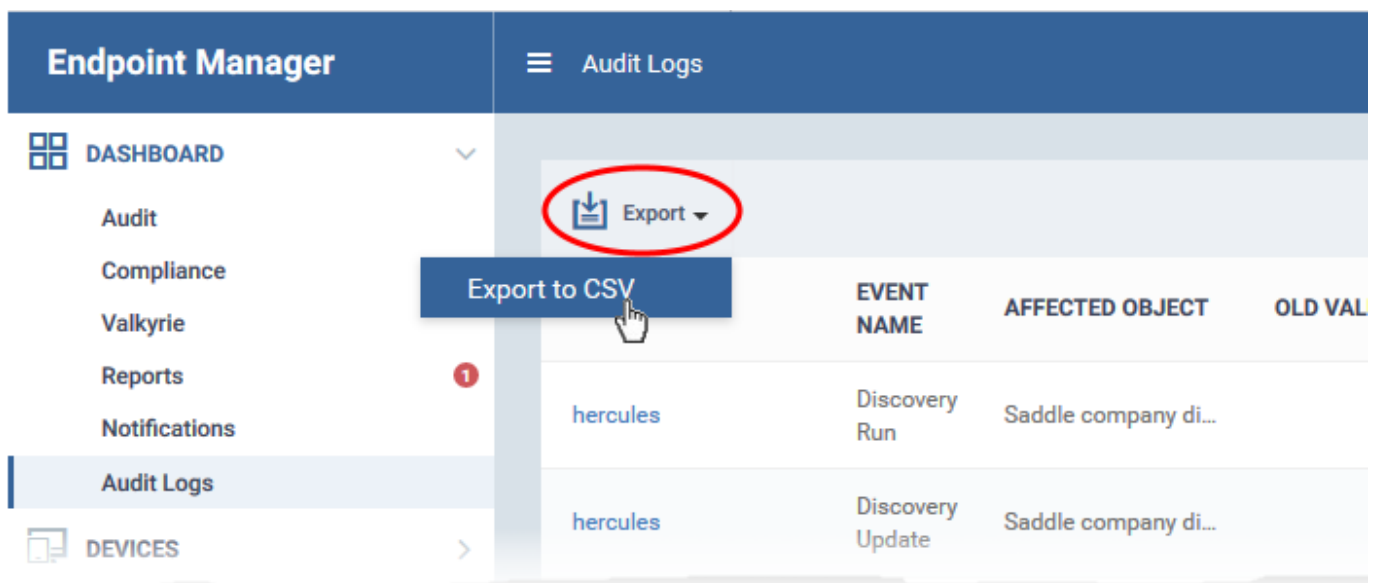
- **Component name** – Select whether you want to view the events from the EM portal or from the Remote Control sessions handled by admins and staff.
- **Source** – Select the category of objects affected by the actions for which you want to see the logs
- **Event name** - Select the type of action
- **Affected object** – Enter the label of the device, device group, profile, procedure or file group affected by the events
- **Old Value** – Enter a setting or value to filter the actions involving change of that item
- **New Value** - Enter a setting or value to filter the actions involving implementation of that setting or value
- **Extra info** – Enter additional details about the actions for which you want to see the logs.
- **Session ID** – Enter the connection session identification string of a device to view only the actions executed during that session

Select your filter criteria and click 'Apply'.

Generate Log Reports

You can generate a log report for up to the past 90 days.

- Click 'Dashboard' > 'Audit Logs'.
- Click the funnel icon to filter which records are included in the report.
- Click 'Export' above the table then choose 'Export to CSV'.



The screenshot shows the 'Endpoint Manager' interface. The top navigation bar includes 'Endpoint Manager' and 'Audit Logs'. A sidebar on the left contains a 'DASHBOARD' menu with options: Audit, Compliance, Valkyrie, Reports (with a red notification badge), Notifications, and Audit Logs (highlighted). Below the sidebar is a 'DEVICES' section. The main content area displays an 'Export' button circled in red, with a dropdown menu open showing 'Export to CSV'. Below the menu is a table with columns: EVENT NAME, AFFECTED OBJECT, and OLD VAL. The table contains two rows of data:

EVENT NAME	AFFECTED OBJECT	OLD VAL
Discovery Run	Saddle company di...	
Discovery Update	Saddle company di...	

- Go to 'Dashboard' > 'Reports' to download the report.
- See [this page](#) for more advice on reports.