

Device Collection Audit

In this post, I will show you how to audit device collection for addition/deletion/modification done by users who have access to sccm console.

Device collection message id. With this ID we can audit device collection.

Message ID	Message ID Description
30015	Find who created SCCM collection
30016	Find who modified SCCM collection
30017	Find who deleted SCCM collection

Run this report

The screenshot shows the SCCM Reporting console. The breadcrumb path is 'Reporting > Reports'. Below the breadcrumb, it says 'Reports 630 items'. There is a search bar with the text 'Search'. Below the search bar is a table with columns 'Icon', 'Name', and 'Category'. The table contains two rows: 'All inventoried products for a specific software company' (Software - Companies and Produ.) and 'All messages for a specific message ID' (Status Messages). An orange arrow points to the 'All messages for a specific message ID' row. Below the table is a 'Run' button with a green play icon.

Now enter value ID which is our message ID and click view report

The screenshot shows the 'Parameter Value' dialog box. It has a title bar 'Parameter Value'. Below the title bar is a grey box with the text 'Select a value to use for this parameter when running the report.' Below this is a text input field containing '30015'. Below the input field is a list box with the text 'Message ID' and '30015'.

The screenshot shows the report viewer window titled 'All messages for a specific message ID'. It has a title bar with standard window controls. Below the title bar is a grey box with the text 'To view the report, provide values for the parameters below, then click View Report.' Below this is a list of report details: 'Report Category: Status Messages', 'Report Name: All messages for a specific message ID', and 'Report Description: Displays a list of messages with a single message ID.' Below the list is a text input field labeled 'Message ID:' containing '30015' and a 'Values...' button. To the right of the input field is a 'View Report' button. Below the input field is a '< Back' button. At the bottom of the window is a navigation bar with icons for back, forward, search, and other functions, along with a '100%' zoom level and 'Find | Next' text.

The report will give you the result which is less than 6 months old. The audit cannot be done, if the device collection is older than 6 months.

The screenshot shows a web-based report viewer. At the top, there is a title bar with the text 'All messages for a specific message ID' and window control buttons. Below the title bar, there is a section with instructions: 'To view the report, provide values for the parameters below, then click View Report.' This section lists the report's category as 'Status Messages', its name as 'All messages for a specific message ID', and its description as 'Displays a list of messages with a single message ID.' Below this, there is a form with a 'Message ID' field containing the value '30015' and a 'View Report' button. A '< Back' link is also visible. The main content area shows a table with the following data:

Status Message	Record ID	Severity	Message ID	Component
User "RAMLAN\Administrator" created a collection named "Win10 20H2 Upgrade" (TOR00038).	72057594041543730	Informational	30015	Microsoft Configuration Manager
User "RAMLAN\Administrator" created a collection named "TEN20H2" (TOR00037).	72057594041542550	Informational	30015	Microsoft Configuration Manager

Repeat the same for rest of the message ID. I hope this helps you how to audit device collection.

Thanks

Ram Lan
26th Mar 2021