MX7000 Advance Filtering

Dell EMC Technical White Paper

Revisions

Date	Description
Jan 2019	Initial release

Acknowledgements

This paper was produced by the following members of the Dell EMC storage engineering team:

Author: Dahir Herzi and Gilberto Osuna Gonzalez

Table of contents

Introduction

The purpose of this whitepaper is to describe Audit logs and Alert logs in MX7000 chassis. Audit logging presents information about the operations/actions that have been invoked in the MX7000 environment. For audit logs it displays details in a categorized manner and informs about the time in which an action took place. Also it provides details on the user that invoked the operation, the source of the request, the message id and a brief description explaining the operation or action that was performed.

As per Alert logs, it provides information about notification events generated by devices or internal chassis components. The type of events can be SNMP Traps, REDFISH events or internal chassis events. The alert details surfaced are extracted from the incoming events and are rendered on the alerts page. The alert information contains valuable details about the nature of the issue, the severity of the event, and in most cases a recommended action to perform that could resolve the issue reported by a device. In addition, the events are categorized, also events provide other details such as reception time, source or originating device information, a message id and a detailed descriptive message.

Both alerts and audits can be filtered to find relevant information. This helps the user locate specific alerts or audit logs in an efficient manner. Locating an audit entry or an alert by filtering criteria helps reduce time spent on the audit logs or the alert pages.

More information will be provided to explain how we can filter entries of the audit logs or alerts and how the different filtering criteria can be utilized.

Audit Logs

The primary objective of this section is:

- Locating audit logs on the MX7000 chassis.
- The combination of filters that can be utilized.

Navigate to Audit Logs

Audit logs can be found in the following path: ***Monitor -> Audit Logs*** of the MX7000 UI.

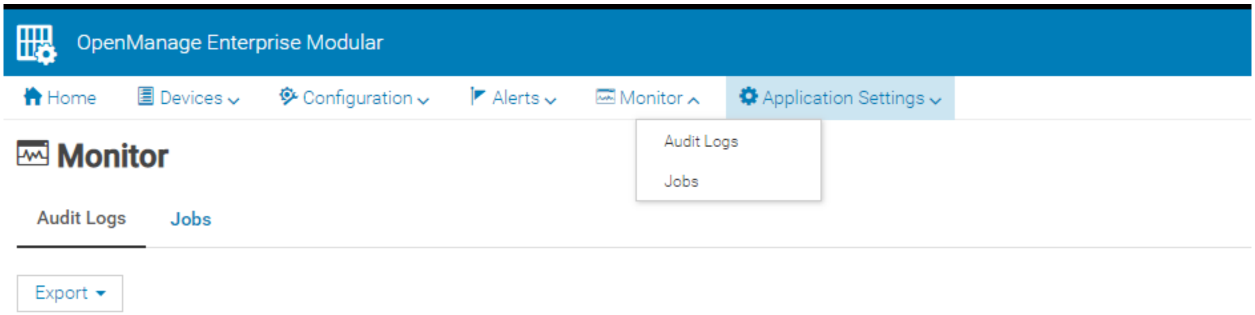


Figure 1 Audit Logs Location

Audit Log Page Sections

All the existing audit log entries will be rendered in that page. By default, all audit log records are not filtered and shown sorted based on time stamp. The advanced filters option will be at top along with export as shown in figure 2. Expanding the advanced filters will show all available filtering criteria for Audit Logs. There is also an option named '*Clear All Filters*' which will clear out any applied filters and show all audit log records without filtering.

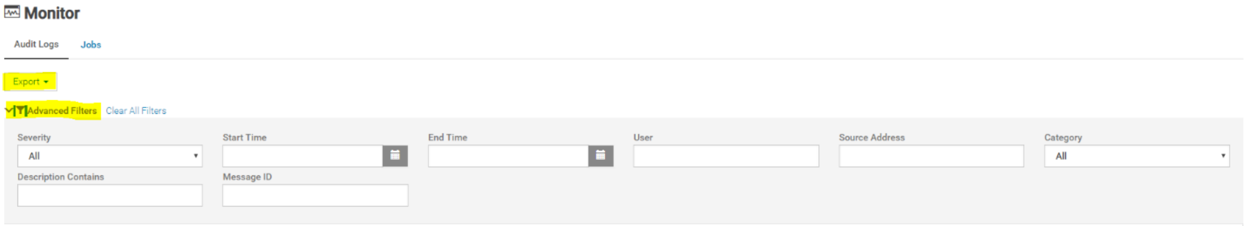


Figure 2 Audit Logs Top Section

At the bottom of this page there's a navigation bar and details about the amount of records and how many records are shown per page (by default it is 30 records per page). In the navigation it will show the current page and the total number of pages (1 of N). The total number of pages is determined by the total number of records that can be grouped in counts of 30 records per page.

Arrows indicates the navigation for last (⏭), next (⏩), (⏪) previous and first (⏮) pages. In addition, the page number can be typed to navigate to it.

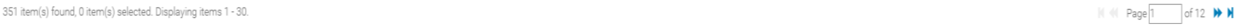

351 item(s) found, 0 item(s) selected. Displaying items 1 - 30.

Figure 3 – Audit Logs Bottom Section (Navigation Bar)

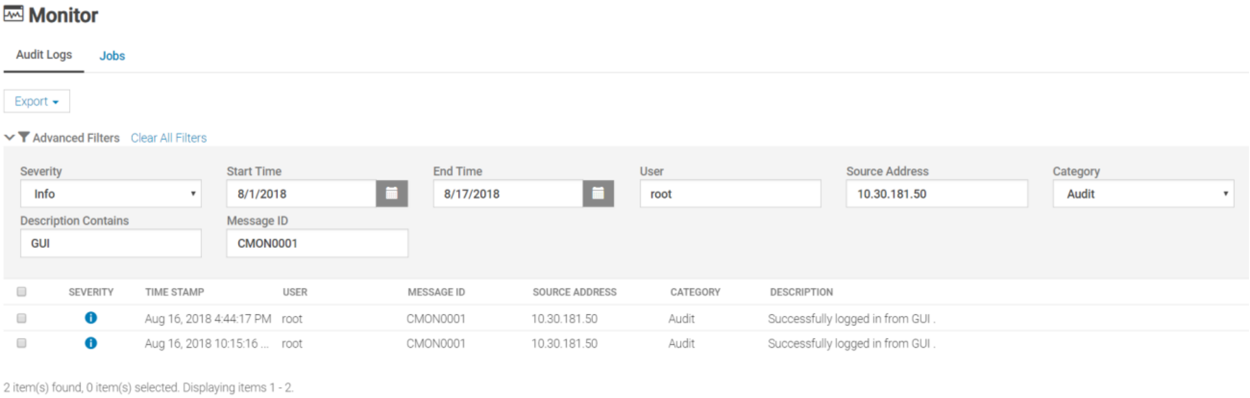
Audit Log Filters

Filter	Description
Severity	Severity to filter from the list of audit logs. Values can be: • All • Info • Warning • Critical
Start Time	Start time to be applied to filter audit log. This filter **MUST** be combined with End Time to filter data in a date/time range manner.
End Time	End time to be applied to filter audit log. This filter **MUST** be combined with Start Time to filter data in a date/time range manner.
User	User, name of the user that generate an audit log.
Source Address	IP address of the source attached to the creation of the audit log record.
Category	List of available categories to filter. Values can be: • All • Audit • Configuration

Description Contains	Filter applied to description. This is more like a LIKE and will audit logs based in this condition.
Message ID	Message ID to be filter out from audit logs.

Table 1 Audit Logs Filters

The following shows an example of how all filters can be combined to obtain a more specific list of audit logs.



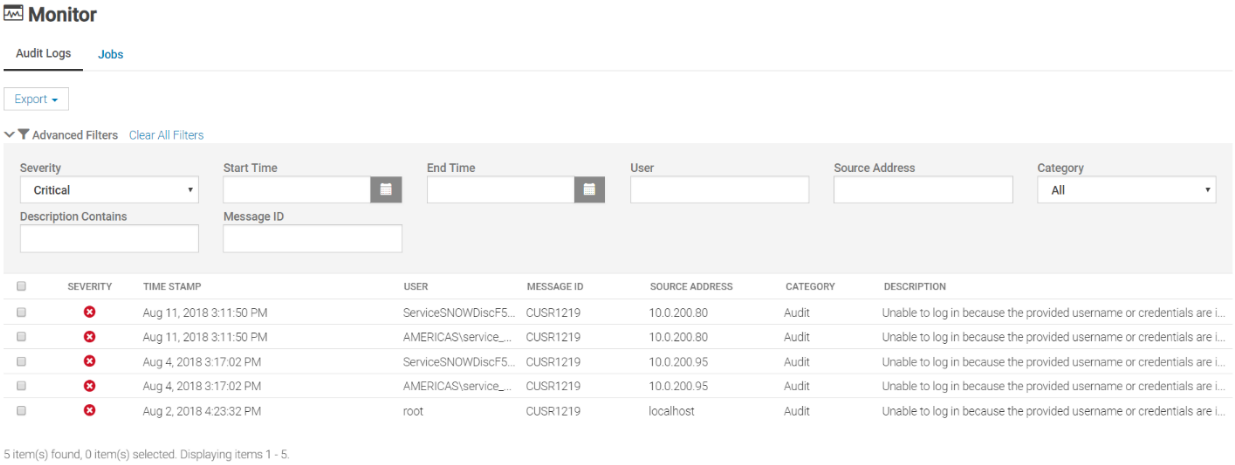
Severity: Info
Start Time: 8/1/2018
End Time: 8/17/2018
User: root
Source Address: 10.30.181.50
Category: Audit
Description Contains: GUI
Message ID: CMON0001

□	SEVERITY	TIME STAMP	USER	MESSAGE ID	SOURCE ADDRESS	CATEGORY	DESCRIPTION
□	ⓘ	Aug 16, 2018 4:44:17 PM	root	CMON0001	10.30.181.50	Audit	Successfully logged in from GUI .
□	ⓘ	Aug 16, 2018 10:15:16 ...	root	CMON0001	10.30.181.50	Audit	Successfully logged in from GUI .

2 item(s) found, 0 item(s) selected. Displaying items 1 - 2.

Figure 4 Audit Logs Filters (All filters Applied

Other examples of filters are as follows:

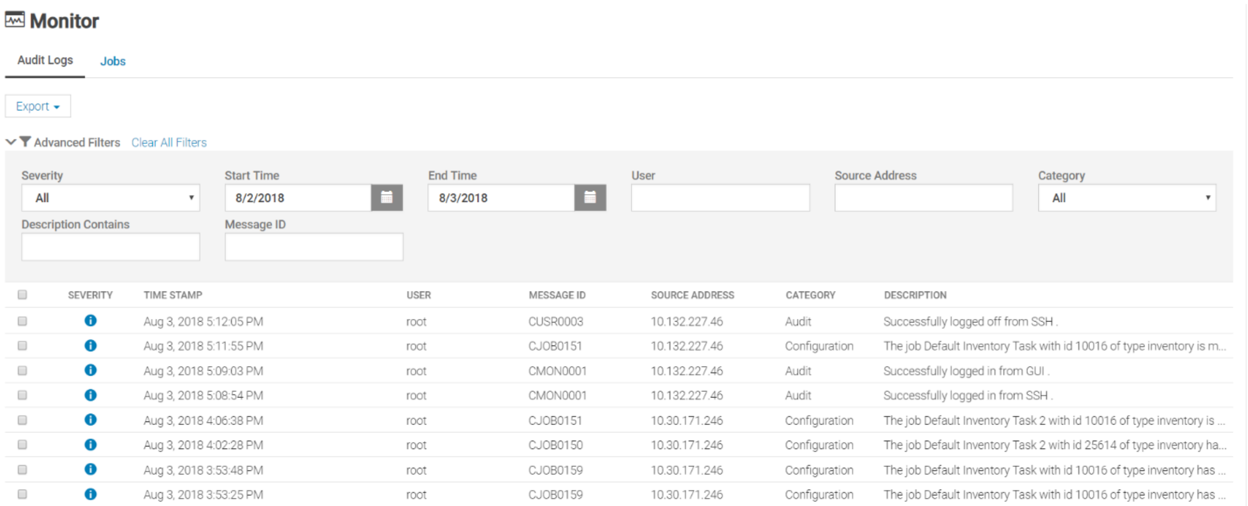


Severity: Critical
Start Time:
End Time:
User:
Source Address:
Category: All
Description Contains:
Message ID:

□	SEVERITY	TIME STAMP	USER	MESSAGE ID	SOURCE ADDRESS	CATEGORY	DESCRIPTION
□	⊗	Aug 11, 2018 3:11:50 PM	ServiceSNOWDiscF5...	CUSR1219	10.0.200.80	Audit	Unable to log in because the provided username or credentials are i...
□	⊗	Aug 11, 2018 3:11:50 PM	AMERICAS\service_...	CUSR1219	10.0.200.80	Audit	Unable to log in because the provided username or credentials are i...
□	⊗	Aug 4, 2018 3:17:02 PM	ServiceSNOWDiscF5...	CUSR1219	10.0.200.95	Audit	Unable to log in because the provided username or credentials are i...
□	⊗	Aug 4, 2018 3:17:02 PM	AMERICAS\service_...	CUSR1219	10.0.200.95	Audit	Unable to log in because the provided username or credentials are i...
□	⊗	Aug 2, 2018 4:23:32 PM	root	CUSR1219	localhost	Audit	Unable to log in because the provided username or credentials are i...

5 item(s) found, 0 item(s) selected. Displaying items 1 - 5.

Figure 5 Audit Logs Filters (Filter by Severity)



Monitor

Audit Logs | Jobs

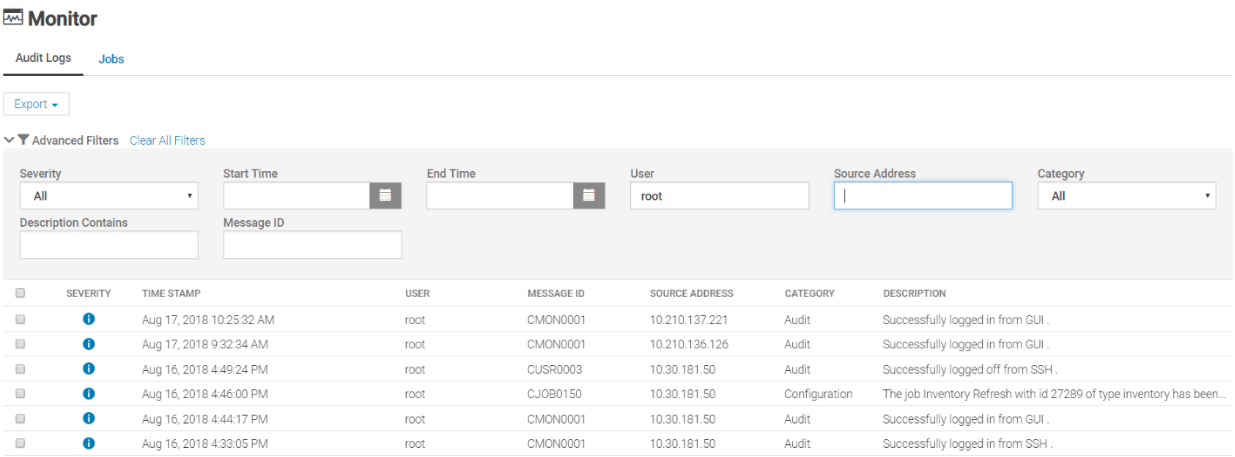
Export

Advanced Filters | Clear All Filters

Severity: All
Start Time: 8/2/2018
End Time: 8/3/2018
User:
Source Address:
Category: All
Description Contains:
Message ID:

□	SEVERITY	TIME STAMP	USER	MESSAGE ID	SOURCE ADDRESS	CATEGORY	DESCRIPTION
□	ℹ	Aug 3, 2018 5:12:05 PM	root	CUSR0003	10.132.227.46	Audit	Successfully logged off from SSH .
□	ℹ	Aug 3, 2018 5:11:55 PM	root	CJOB0151	10.132.227.46	Configuration	The job Default Inventory Task with id 10016 of type inventory is m...
□	ℹ	Aug 3, 2018 5:09:03 PM	root	CMON0001	10.132.227.46	Audit	Successfully logged in from GUI .
□	ℹ	Aug 3, 2018 5:08:54 PM	root	CMON0001	10.132.227.46	Audit	Successfully logged in from SSH .
□	ℹ	Aug 3, 2018 4:06:38 PM	root	CJOB0151	10.30.171.246	Configuration	The job Default Inventory Task 2 with id 10016 of type inventory is ...
□	ℹ	Aug 3, 2018 4:02:28 PM	root	CJOB0150	10.30.171.246	Configuration	The job Default Inventory Task 2 with id 25614 of type inventory ha...
□	ℹ	Aug 3, 2018 3:53:48 PM	root	CJOB0159	10.30.171.246	Configuration	The job Default Inventory Task with id 10016 of type inventory has ...
□	ℹ	Aug 3, 2018 3:53:25 PM	root	CJOB0159	10.30.171.246	Configuration	The job Default Inventory Task with id 10016 of type inventory has ...

Figure 6 Audit Logs Filters (Filter by Start and End Time)



Monitor

Audit Logs | Jobs

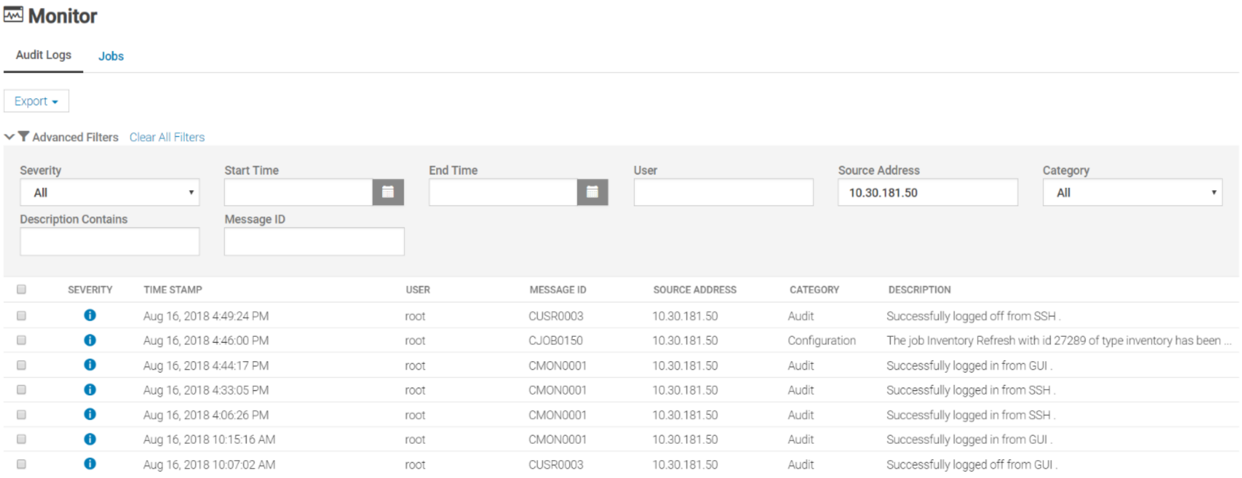
Export

Advanced Filters | Clear All Filters

Severity: All
Start Time:
End Time:
User: root
Source Address:
Category: All
Description Contains:
Message ID:

□	SEVERITY	TIME STAMP	USER	MESSAGE ID	SOURCE ADDRESS	CATEGORY	DESCRIPTION
□	ℹ	Aug 17, 2018 10:25:32 AM	root	CMON0001	10.210.137.221	Audit	Successfully logged in from GUI .
□	ℹ	Aug 17, 2018 9:32:34 AM	root	CMON0001	10.210.136.126	Audit	Successfully logged in from GUI .
□	ℹ	Aug 16, 2018 4:49:24 PM	root	CUSR0003	10.30.181.50	Audit	Successfully logged off from SSH .
□	ℹ	Aug 16, 2018 4:46:00 PM	root	CJOB0150	10.30.181.50	Configuration	The job Inventory Refresh with id 27289 of type inventory has been...
□	ℹ	Aug 16, 2018 4:44:17 PM	root	CMON0001	10.30.181.50	Audit	Successfully logged in from GUI .
□	ℹ	Aug 16, 2018 4:33:05 PM	root	CMON0001	10.30.181.50	Audit	Successfully logged in from SSH .

Figure 7 Audit Logs Filters (Filter by User)



Monitor

Audit Logs | Jobs

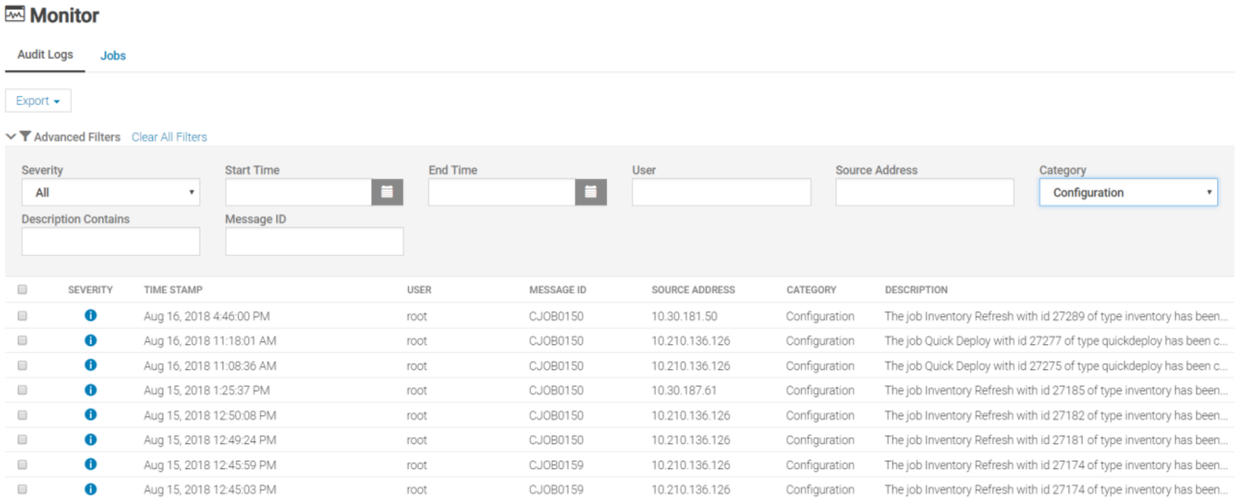
Export

Advanced Filters | Clear All Filters

Severity: All
Start Time:
End Time:
User:
Source Address: 10.30.181.50
Category: All
Description Contains:
Message ID:

□	SEVERITY	TIME STAMP	USER	MESSAGE ID	SOURCE ADDRESS	CATEGORY	DESCRIPTION
□	ℹ	Aug 16, 2018 4:49:24 PM	root	CUSR0003	10.30.181.50	Audit	Successfully logged off from SSH .
□	ℹ	Aug 16, 2018 4:46:00 PM	root	CJOB0150	10.30.181.50	Configuration	The job Inventory Refresh with id 27289 of type inventory has been ...
□	ℹ	Aug 16, 2018 4:44:17 PM	root	CMON0001	10.30.181.50	Audit	Successfully logged in from GUI .
□	ℹ	Aug 16, 2018 4:33:05 PM	root	CMON0001	10.30.181.50	Audit	Successfully logged in from SSH .
□	ℹ	Aug 16, 2018 4:06:26 PM	root	CMON0001	10.30.181.50	Audit	Successfully logged in from SSH .
□	ℹ	Aug 16, 2018 10:15:16 AM	root	CMON0001	10.30.181.50	Audit	Successfully logged in from GUI .
□	ℹ	Aug 16, 2018 10:07:02 AM	root	CUSR0003	10.30.181.50	Audit	Successfully logged off from GUI .

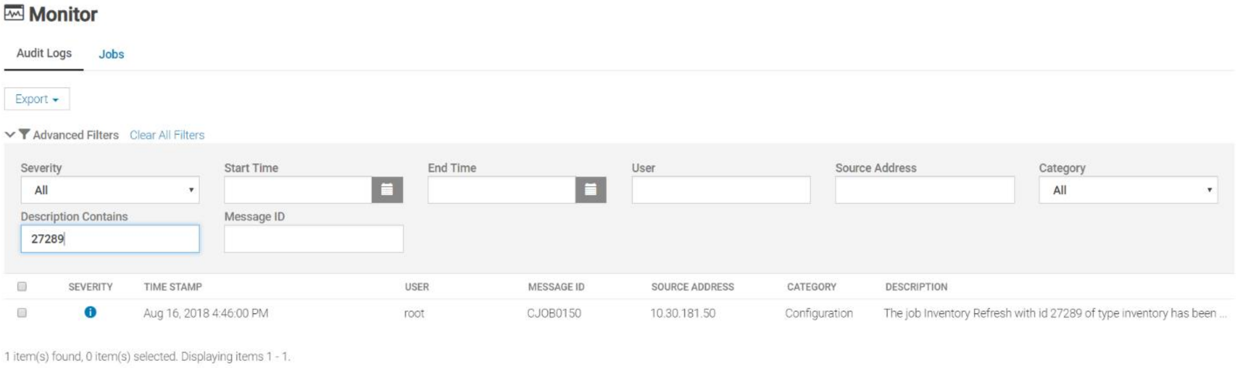
Figure 8 Audit Logs Filters (Filter by Source Address)



Severity: All
Start Time:
End Time:
User:
Source Address:
Category: Configuration
Description Contains:
Message ID:

□	SEVERITY	TIME STAMP	USER	MESSAGE ID	SOURCE ADDRESS	CATEGORY	DESCRIPTION
□	ⓘ	Aug 16, 2018 4:46:00 PM	root	CJOB0150	10.30.181.50	Configuration	The job Inventory Refresh with id 27289 of type inventory has been...
□	ⓘ	Aug 16, 2018 11:18:01 AM	root	CJOB0150	10.210.136.126	Configuration	The job Quick Deploy with id 27277 of type quickdeploy has been c...
□	ⓘ	Aug 16, 2018 11:08:36 AM	root	CJOB0150	10.210.136.126	Configuration	The job Quick Deploy with id 27275 of type quickdeploy has been c...
□	ⓘ	Aug 15, 2018 1:25:37 PM	root	CJOB0150	10.30.187.61	Configuration	The job Inventory Refresh with id 27185 of type inventory has been...
□	ⓘ	Aug 15, 2018 12:50:08 PM	root	CJOB0150	10.210.136.126	Configuration	The job Inventory Refresh with id 27182 of type inventory has been...
□	ⓘ	Aug 15, 2018 12:49:24 PM	root	CJOB0150	10.210.136.126	Configuration	The job Inventory Refresh with id 27181 of type inventory has been...
□	ⓘ	Aug 15, 2018 12:45:59 PM	root	CJOB0159	10.210.136.126	Configuration	The job Inventory Refresh with id 27174 of type inventory has been...
□	ⓘ	Aug 15, 2018 12:45:03 PM	root	CJOB0159	10.210.136.126	Configuration	The job Inventory Refresh with id 27174 of type inventory has been...

Figure 9 Audit Logs Filters (Filter by Category)

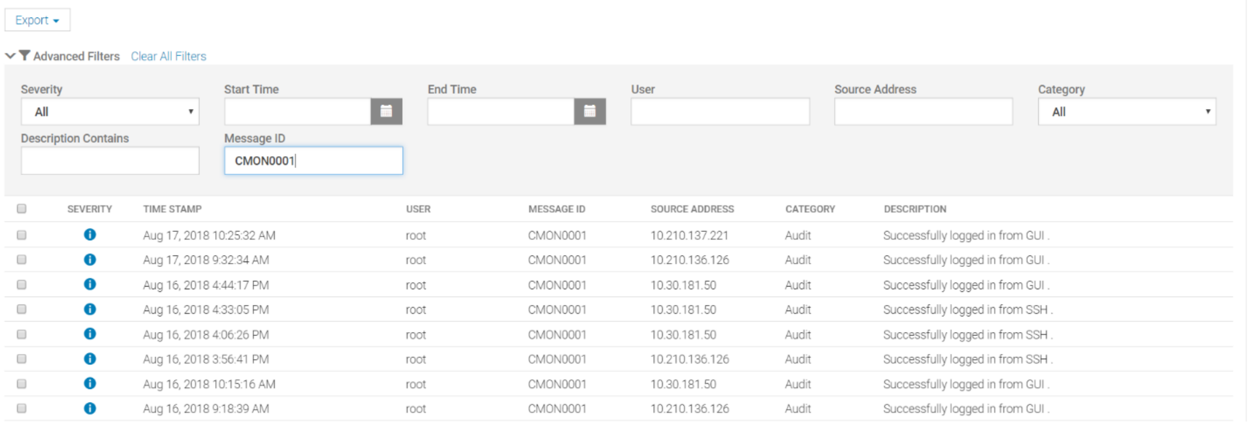


Severity: All
Start Time:
End Time:
User:
Source Address:
Category: All
Description Contains: 27289
Message ID:

□	SEVERITY	TIME STAMP	USER	MESSAGE ID	SOURCE ADDRESS	CATEGORY	DESCRIPTION
□	ⓘ	Aug 16, 2018 4:46:00 PM	root	CJOB0150	10.30.181.50	Configuration	The job Inventory Refresh with id 27289 of type inventory has been ...

1 item(s) found, 0 item(s) selected. Displaying items 1 - 1.

Figure 10 Audit Logs Filters (Filter by Description Contains)



Severity: All
Start Time:
End Time:
User:
Source Address:
Category: All
Description Contains:
Message ID: CMON0001

□	SEVERITY	TIME STAMP	USER	MESSAGE ID	SOURCE ADDRESS	CATEGORY	DESCRIPTION
□	ⓘ	Aug 17, 2018 10:25:32 AM	root	CMON0001	10.210.137.221	Audit	Successfully logged in from GUI .
□	ⓘ	Aug 17, 2018 9:32:34 AM	root	CMON0001	10.210.136.126	Audit	Successfully logged in from GUI .
□	ⓘ	Aug 16, 2018 4:44:17 PM	root	CMON0001	10.30.181.50	Audit	Successfully logged in from GUI .
□	ⓘ	Aug 16, 2018 4:33:05 PM	root	CMON0001	10.30.181.50	Audit	Successfully logged in from SSH .
□	ⓘ	Aug 16, 2018 4:06:26 PM	root	CMON0001	10.30.181.50	Audit	Successfully logged in from SSH .
□	ⓘ	Aug 16, 2018 3:56:41 PM	root	CMON0001	10.210.136.126	Audit	Successfully logged in from SSH .
□	ⓘ	Aug 16, 2018 10:15:16 AM	root	CMON0001	10.30.181.50	Audit	Successfully logged in from GUI .
□	ⓘ	Aug 16, 2018 9:18:39 AM	root	CMON0001	10.210.136.126	Audit	Successfully logged in from GUI .

Figure 11 Audit Logs Filters (Filter by Message ID)

Audit Log Export

Audit Logs entries can be export to a CSV file by clicking the Export button located in the top of the Audit Log Page, a sub menu will be shown and from there we select Export All.

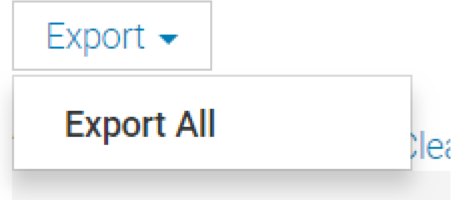
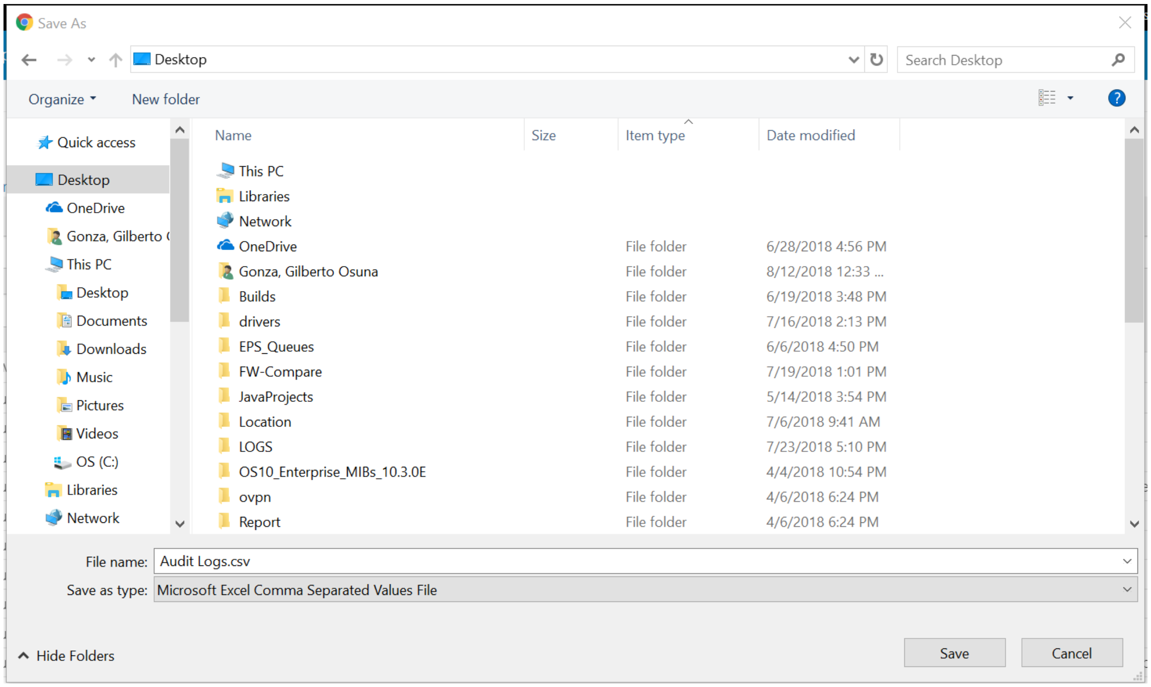


Figure 12 Audit Logs Filters (Export All)

Export all will show a ‘Save As’ window and from there we can navigate to the location where we want to save our current Audit Logs.



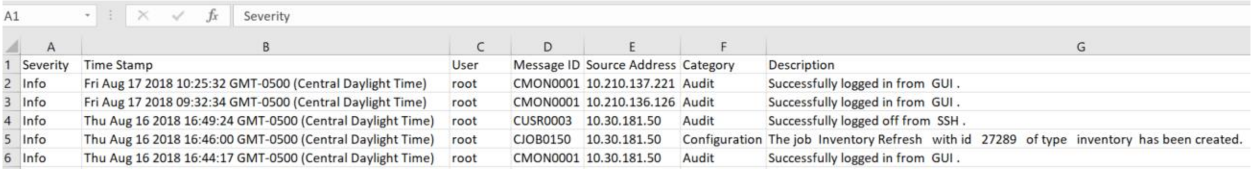
Name	Size	Item type	Date modified
This PC			
Libraries			
Network			
OneDrive		File folder	6/28/2018 4:56 PM
Gonza, Gilberto Osuna		File folder	8/12/2018 12:33 ...
Builds		File folder	6/19/2018 3:48 PM
drivers		File folder	7/16/2018 2:13 PM
EPS_Queues		File folder	6/6/2018 4:50 PM
FW-Compare		File folder	7/19/2018 1:01 PM
JavaProjects		File folder	5/14/2018 3:54 PM
Location		File folder	7/6/2018 9:41 AM
LOGS		File folder	7/23/2018 5:10 PM
OS10_Enterprise_MIBs_10.3.0E		File folder	4/4/2018 10:54 PM
ovpn		File folder	4/6/2018 6:24 PM
Report		File folder	4/6/2018 6:24 PM

File name: Audit Logs.csv

Save as type: Microsoft Excel Comma Separated Values File

Figure 13 Audit Logs Filters (Save As)

The generated audit log CSV file can be opened by using Excel or a text editor. It will show the details as indicated in below Figure 14.


A1 Severity

	A	B	C	D	E	F	G
1	Severity	Time Stamp	User	Message ID	Source Address	Category	Description
2	Info	Fri Aug 17 2018 10:25:32 GMT-0500 (Central Daylight Time)	root	CMON0001	10.210.137.221	Audit	Successfully logged in from GUI .
3	Info	Fri Aug 17 2018 09:32:34 GMT-0500 (Central Daylight Time)	root	CMON0001	10.210.136.126	Audit	Successfully logged in from GUI .
4	Info	Thu Aug 16 2018 16:49:24 GMT-0500 (Central Daylight Time)	root	CUSR0003	10.30.181.50	Audit	Successfully logged off from SSH .
5	Info	Thu Aug 16 2018 16:46:00 GMT-0500 (Central Daylight Time)	root	CJOB0150	10.30.181.50	Configuration	The job Inventory Refresh with id 27289 of type inventory has been created.
6	Info	Thu Aug 16 2018 16:44:17 GMT-0500 (Central Daylight Time)	root	CMON0001	10.30.181.50	Audit	Successfully logged in from GUI .

Figure 14 Audit Logs Filters (Generated Audit Log CSV File Contents)

Alert Logs

The following section describes:

- The alert logs section of MX7000.
- Locating the alert logs page. The combination of filters that can be utilized.

Alert log entries are the events generated by devices such as SLEDs, IOMs, chassis controller or internal events by MX7000 chassis. These events are recorded and presented in the UI through the Alert Log page. These events are generated, received and processed. The source of the event is a device (except for internal events) and the type can be SNMP or REDFISH events (in case of EC).

Navigate to Alert Logs

Alert logs can be found in the following path: **Alerts -> Alert Log** of the MX7000 UI.

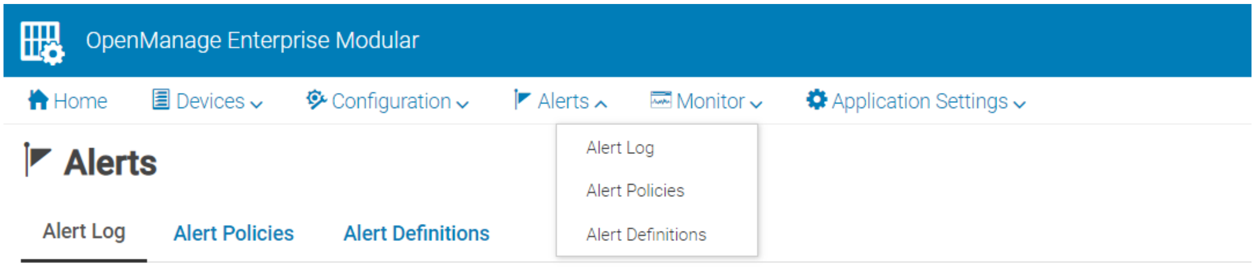
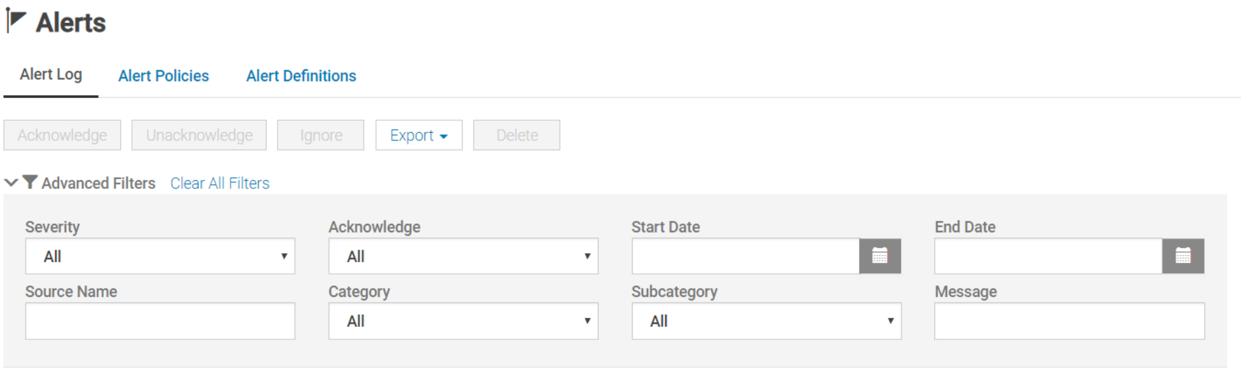


Figure 15 Alert Logs Location

Alert Log Page Sections

All alerts will be available on above mentioned page. By default the alerts are not filtered and they are render in a sorted order based on the time stamp. The advanced filters option will be at top along with export. Expanding the advanced filters will show all available filters for Alerts.

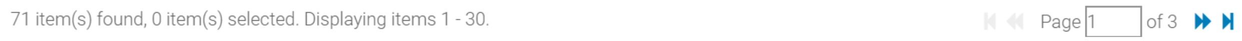


Severity: All
Acknowledge: All
Start Date:
End Date:
Source Name:
Category: All
Subcategory: All
Message:

Figure 16 Alert Log Top Section

At the bottom of this page there's a navigation bar and details about the amount of records and how many records are shown per page (by default it is 30 records per page). In the navigation it will show the current page and the total number of pages (1 of N). The total number of pages are determined by the total number of records that can be grouped in counts of 30 records per page.

Arrows indicates the navigation for last (⏭), next (⏩), (⏪) previous and first (⏮) pages. In addition, the page number can be typed to navigate to it.

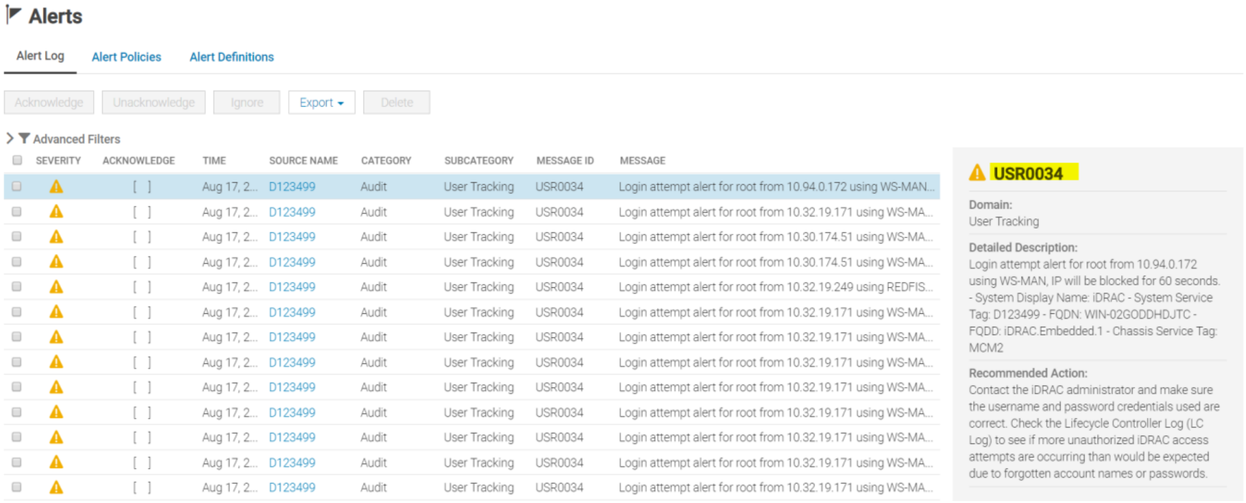


71 item(s) found, 0 item(s) selected. Displaying items 1 - 30.

Page 1 of 3

Figure 17 Alert Log Bottom Section (Navigation Bar)

At the right side of the page there's an information bock that shows relevant information from the event generated by the device. Like the domain corresponding to the event, detailed message of the event, recommended action to resolve the issue, and Message ID (EEMI Message ID).



□	SEVERITY	ACKNOWLEDGE	TIME	SOURCE NAME	CATEGORY	SUBCATEGORY	MESSAGE ID	MESSAGE
□	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.94.0.172 using WS-MAN...
□	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.171 using WS-MA...
□	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.30.174.51 using WS-MA...
□	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.30.174.51 using WS-MA...
□	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.249 using REDFIS...
□	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.171 using WS-MA...
□	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.171 using WS-MA...
□	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.171 using WS-MA...
□	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.171 using WS-MA...
□	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.171 using WS-MA...
□	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.171 using WS-MA...
□	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.171 using WS-MA...
□	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.171 using WS-MA...

⚠ USR0034

Domain:
User Tracking

Detailed Description:
Login attempt alert for root from 10.94.0.172 using WS-MAN, IP will be blocked for 60 seconds. - System Display Name: iDRAC - System Service Tag: D123499 - FQDN: WIN-02GODDHDJTC - FQDD: iDRAC.Embedded.1 - Chassis Service Tag: MCM2

Recommended Action:
Contact the iDRAC administrator and make sure the username and password credentials used are correct. Check the Lifecycle Controller Log (LC Log) to see if more unauthorized iDRAC access attempts are occurring than would be expected due to forgotten account names or passwords.

Figure 18 Audit Logs Bottom Section (Navigation Bar)

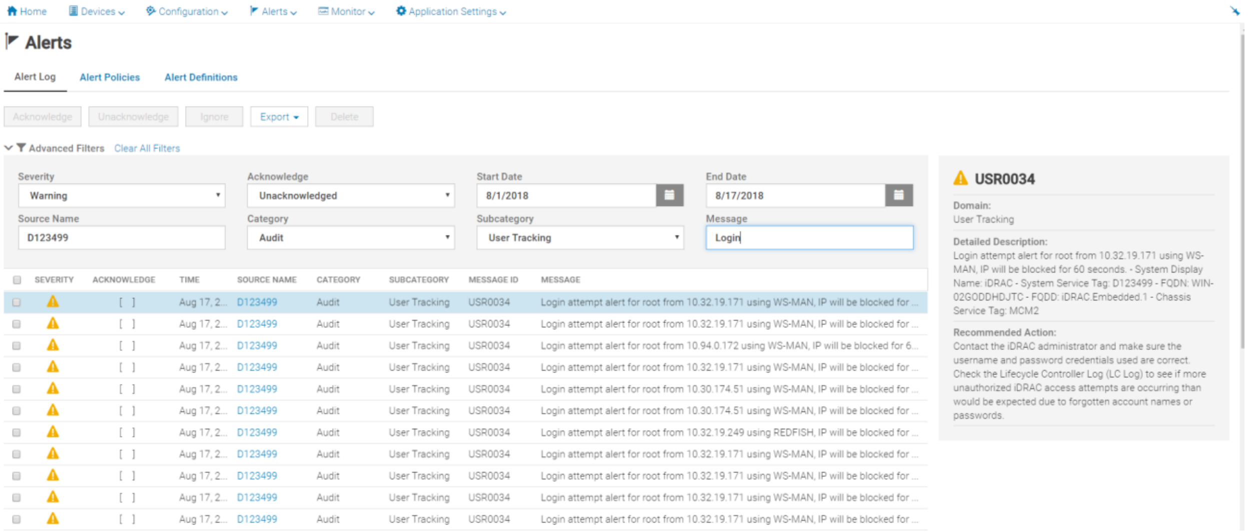
Alert Log Filters

Filter	Description
Severity	Severity to filter from the list of alert logs. Values can be: • All • Unknown • Info • Normal • Warning • Critical
Acknowledge	Indicate if the alert is acknowledged or unacknowledged.
Start Date	Start Date to be applied to filter audit log. This filter **MUST** be combined with End Date to filter data in a date/time range manner.
End Date	End Date to be applied to filter audit log. This filter **MUST** be combined with Start Date to filter data in a date/time range manner.
Source Name	Source name or identifier of the device that generates the aler.t
Category	To indicate which category, we need to filter out. This is combined with sub category. If we require a specific subcategory. Values can be: • All • Audit • Configuration • Miscellaneous • Storage • System Health • Updates

	• Work Notes
Subcategory	Indicates which subcategories of the selected category can be filter. This list is variable, and it can contain 1 to N subcategories per selected category. Is recommended to select a subcategory to filter more accurately.
Message	A message that can be filter out from the list of alerts. This will use a LIKE to filter out alerts.

Table 2 Alert Log Filters

following filters that can be applied to the existing view of recorded logs. Also, all of them can be combined to be stricter in the filter.



Severity: Warning
Acknowledge: Unacknowledged
Start Date: 8/1/2018
End Date: 8/17/2018
Source Name: D123499
Category: Audit
Subcategory: User Tracking
Message: Login

☐	SEVERITY	ACKNOWLEDGE	TIME	SOURCE NAME	CATEGORY	SUBCATEGORY	MESSAGE ID	MESSAGE
☐	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.171 using WS-MAN, IP will be blocked for ...
☐	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.171 using WS-MAN, IP will be blocked for ...
☐	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.94.0.172 using WS-MAN, IP will be blocked for 6...
☐	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.171 using WS-MAN, IP will be blocked for ...
☐	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.30.174.51 using WS-MAN, IP will be blocked for ...
☐	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.30.174.51 using WS-MAN, IP will be blocked for ...
☐	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.249 using REDFISH, IP will be blocked for ...
☐	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.171 using WS-MAN, IP will be blocked for ...
☐	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.171 using WS-MAN, IP will be blocked for ...
☐	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.171 using WS-MAN, IP will be blocked for ...
☐	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.171 using WS-MAN, IP will be blocked for ...

⚠ USR0034

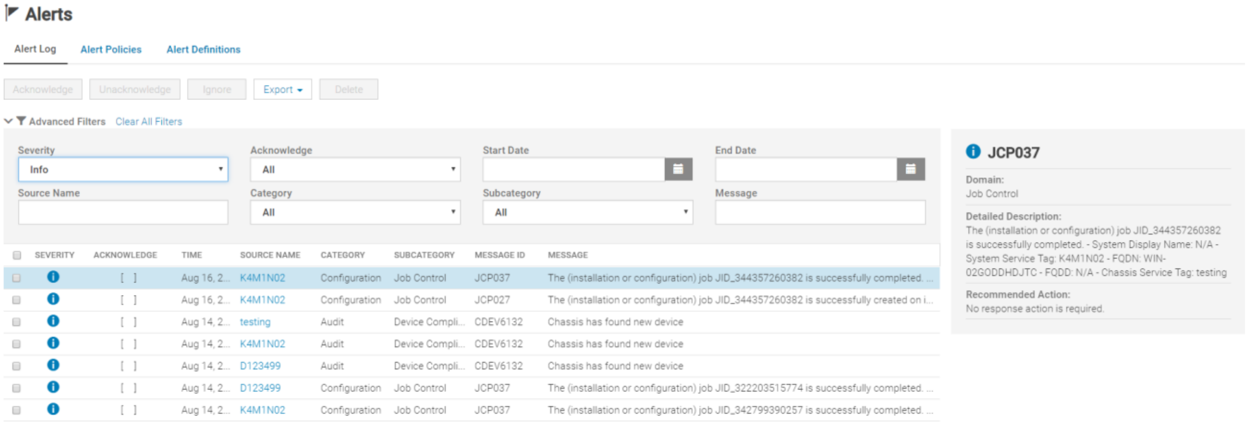
Domain:
User Tracking

Detailed Description:
Login attempt alert for root from 10.32.19.171 using WS-MAN, IP will be blocked for 60 seconds. - System Display Name: iDRAC - System Service Tag: D123499 - FQDN: WIN-02GODDHDJTC - FQDD: iDRAC.Embedded.1 - Chassis Service Tag: MCM2

Recommended Action:
Contact the iDRAC administrator and make sure the username and password credentials used are correct. Check the Lifecycle Controller Log (LC Log) to see if more unauthorized iDRAC access attempts are occurring than would be expected due to forgotten account names or passwords.

Figure 19 Alert Log Filters (All filters Applied)

Other examples of filters are as follows:



Severity: Info
Acknowledge: All
Start Date:
End Date:
Source Name:
Category: All
Subcategory: All
Message:

☐	SEVERITY	ACKNOWLEDGE	TIME	SOURCE NAME	CATEGORY	SUBCATEGORY	MESSAGE ID	MESSAGE
☐	ℹ	[ ]	Aug 16, 2...	K4M1N02	Configuration	Job Control	JCP037	The (installation or configuration) job JID_344357260382 is successfully completed. ...
☐	ℹ	[ ]	Aug 16, 2...	K4M1N02	Configuration	Job Control	JCP027	The (installation or configuration) job JID_344357260382 is successfully created on i...
☐	ℹ	[ ]	Aug 14, 2...	testing	Audit	Device Compli...	CDEV6132	Chassis has found new device
☐	ℹ	[ ]	Aug 14, 2...	K4M1N02	Audit	Device Compli...	CDEV6132	Chassis has found new device
☐	ℹ	[ ]	Aug 14, 2...	D123499	Audit	Device Compli...	CDEV6132	Chassis has found new device
☐	ℹ	[ ]	Aug 14, 2...	D123499	Configuration	Job Control	JCP037	The (installation or configuration) job JID_322203515774 is successfully completed. ...
☐	ℹ	[ ]	Aug 14, 2...	K4M1N02	Configuration	Job Control	JCP037	The (installation or configuration) job JID_342799390257 is successfully completed. ...

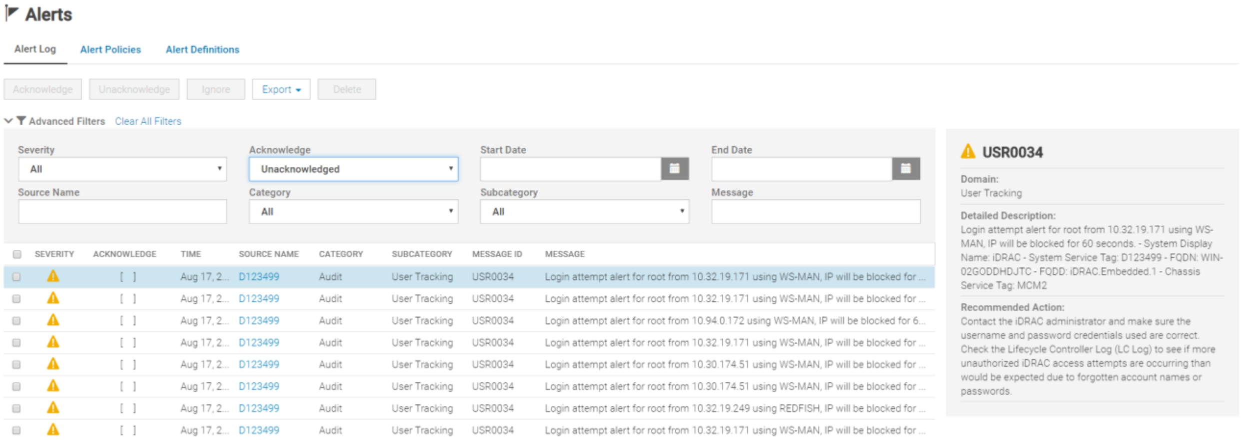
ℹ JCP037

Domain:
Job Control

Detailed Description:
The (installation or configuration) job JID_344357260382 is successfully completed. - System Display Name: N/A - System Service Tag: K4M1N02 - FQDN: WIN-02GODDHDJTC - FQDD: N/A - Chassis Service Tag: testing

Recommended Action:
No response action is required.

Figure 20 Alert Log Filters (Filter by Severity)



Severity: All	Acknowledge: Unacknowledged	Start Date:	End Date:
Source Name:	Category: All	Subcategory: All	Message:

□	SEVERITY	ACKNOWLEDGE	TIME	SOURCE NAME	CATEGORY	SUBCATEGORY	MESSAGE ID	MESSAGE
□	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.171 using WS-MAN, IP will be blocked for ...
□	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.171 using WS-MAN, IP will be blocked for ...
□	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.94.0.172 using WS-MAN, IP will be blocked for 6...
□	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.171 using WS-MAN, IP will be blocked for ...
□	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.30.174.51 using WS-MAN, IP will be blocked for ...
□	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.30.174.51 using WS-MAN, IP will be blocked for ...
□	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.249 using REDFISH, IP will be blocked for ...
□	⚠	[ ]	Aug 17, 2...	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19.171 using WS-MAN, IP will be blocked for ...

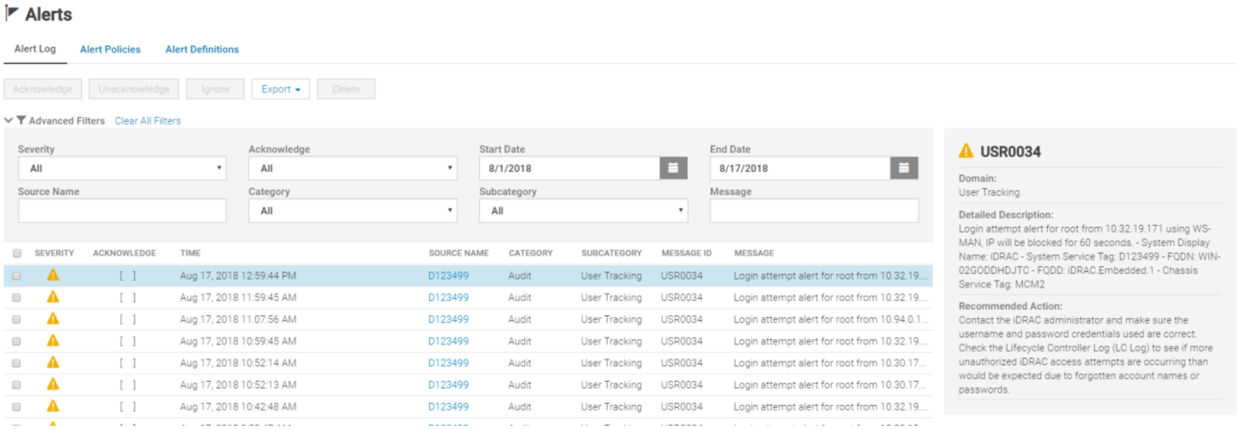
⚠ USR0034

Domain:
User Tracking

Detailed Description:
Login attempt alert for root from 10.32.19.171 using WS-MAN, IP will be blocked for 60 seconds. - System Display Name: iDRAC - System Service Tag: D123499 - FQDN: WIN-02GODDHDJTC - FQDD: iDRAC.Embedded.1 - Chassis Service Tag: MCM2

Recommended Action:
Contact the iDRAC administrator and make sure the username and password credentials used are correct. Check the Lifecycle Controller Log (LC Log) to see if more unauthorized iDRAC access attempts are occurring than would be expected due to forgotten account names or passwords.

Figure 21 Alert Log Filters (Filter by Acknowledge)



Severity: All	Acknowledge: All	Start Date: 8/1/2018	End Date: 8/17/2018
Source Name:	Category: All	Subcategory: All	Message:

□	SEVERITY	ACKNOWLEDGE	TIME	SOURCE NAME	CATEGORY	SUBCATEGORY	MESSAGE ID	MESSAGE
□	⚠	[ ]	Aug 17, 2018 12:59:44 PM	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19....
□	⚠	[ ]	Aug 17, 2018 11:59:45 AM	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19....
□	⚠	[ ]	Aug 17, 2018 11:07:56 AM	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.94.0.1...
□	⚠	[ ]	Aug 17, 2018 10:59:45 AM	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19....
□	⚠	[ ]	Aug 17, 2018 10:52:14 AM	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.30.17...
□	⚠	[ ]	Aug 17, 2018 10:52:13 AM	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.30.17...
□	⚠	[ ]	Aug 17, 2018 10:42:48 AM	D123499	Audit	User Tracking	USR0034	Login attempt alert for root from 10.32.19....

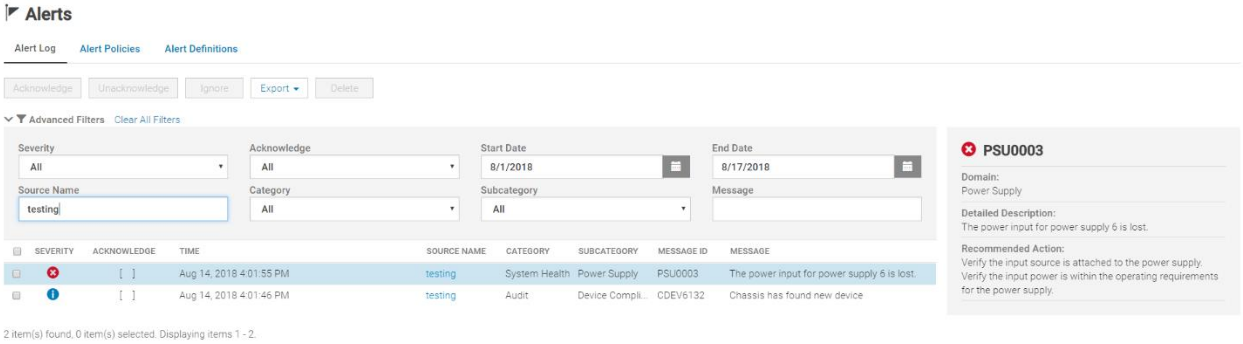
⚠ USR0034

Domain:
User Tracking

Detailed Description:
Login attempt alert for root from 10.32.19.171 using WS-MAN, IP will be blocked for 60 seconds. - System Display Name: iDRAC - System Service Tag: D123499 - FQDN: WIN-02GODDHDJTC - FQDD: iDRAC.Embedded.1 - Chassis Service Tag: MCM2

Recommended Action:
Contact the iDRAC administrator and make sure the username and password credentials used are correct. Check the Lifecycle Controller Log (LC Log) to see if more unauthorized iDRAC access attempts are occurring than would be expected due to forgotten account names or passwords.

Figure 22 Alert Log Filters (Filter by Start Date and End Date)



Severity: All	Acknowledge: All	Start Date: 8/1/2018	End Date: 8/17/2018
Source Name: testing	Category: All	Subcategory: All	Message:

□	SEVERITY	ACKNOWLEDGE	TIME	SOURCE NAME	CATEGORY	SUBCATEGORY	MESSAGE ID	MESSAGE
□	✖	[ ]	Aug 14, 2018 4:01:55 PM	testing	System Health	Power Supply	PSU0003	The power input for power supply 6 is lost.
□	ℹ	[ ]	Aug 14, 2018 4:01:46 PM	testing	Audit	Device Compli...	CDEV6132	Chassis has found new device

2 item(s) found, 0 item(s) selected. Displaying items 1 - 2.

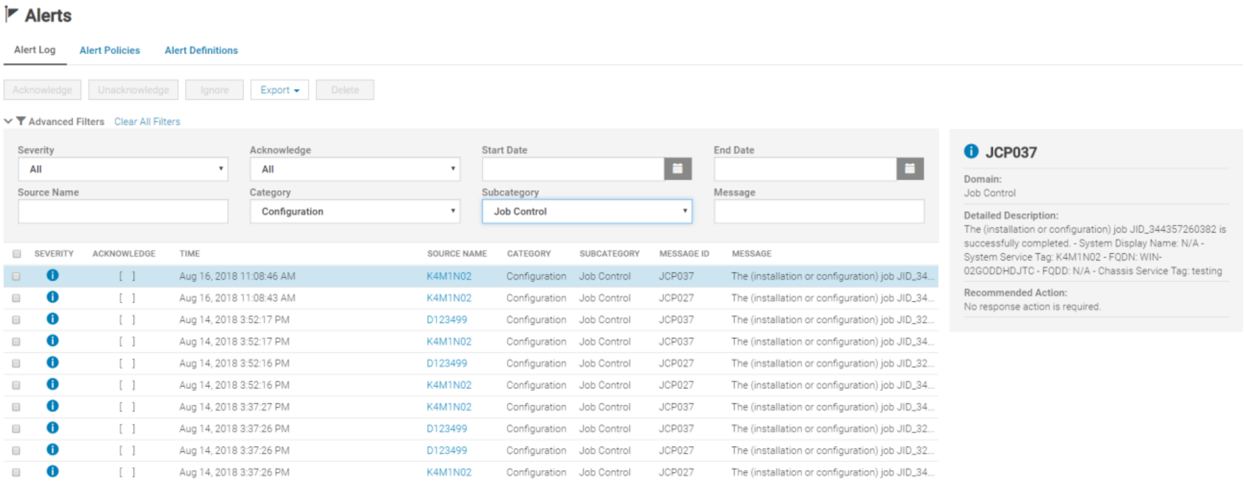
✖ PSU0003

Domain:
Power Supply

Detailed Description:
The power input for power supply 6 is lost.

Recommended Action:
Verify the input source is attached to the power supply. Verify the input power is within the operating requirements for the power supply.

Figure 23 Alert Log Filters (Filter by Source Name)



Severity: All
Acknowledge: All
Start Date:
End Date:
Source Name:
Category: Configuration
Subcategory: Job Control
Message:

□	SEVERITY	ACKNOWLEDGE	TIME	SOURCE NAME	CATEGORY	SUBCATEGORY	MESSAGE ID	MESSAGE
□	ⓘ	[ ]	Aug 16, 2018 11:08:46 AM	K4M1N02	Configuration	Job Control	JCP037	The (installation or configuration) job JID_34...
□	ⓘ	[ ]	Aug 16, 2018 11:08:43 AM	K4M1N02	Configuration	Job Control	JCP027	The (installation or configuration) job JID_34...
□	ⓘ	[ ]	Aug 14, 2018 3:52:17 PM	D123499	Configuration	Job Control	JCP037	The (installation or configuration) job JID_32...
□	ⓘ	[ ]	Aug 14, 2018 3:52:17 PM	K4M1N02	Configuration	Job Control	JCP037	The (installation or configuration) job JID_34...
□	ⓘ	[ ]	Aug 14, 2018 3:52:16 PM	D123499	Configuration	Job Control	JCP027	The (installation or configuration) job JID_32...
□	ⓘ	[ ]	Aug 14, 2018 3:52:16 PM	K4M1N02	Configuration	Job Control	JCP027	The (installation or configuration) job JID_34...
□	ⓘ	[ ]	Aug 14, 2018 3:37:27 PM	K4M1N02	Configuration	Job Control	JCP037	The (installation or configuration) job JID_34...
□	ⓘ	[ ]	Aug 14, 2018 3:37:26 PM	D123499	Configuration	Job Control	JCP037	The (installation or configuration) job JID_32...
□	ⓘ	[ ]	Aug 14, 2018 3:37:26 PM	D123499	Configuration	Job Control	JCP027	The (installation or configuration) job JID_32...
□	ⓘ	[ ]	Aug 14, 2018 3:37:26 PM	K4M1N02	Configuration	Job Control	JCP027	The (installation or configuration) job JID_34...

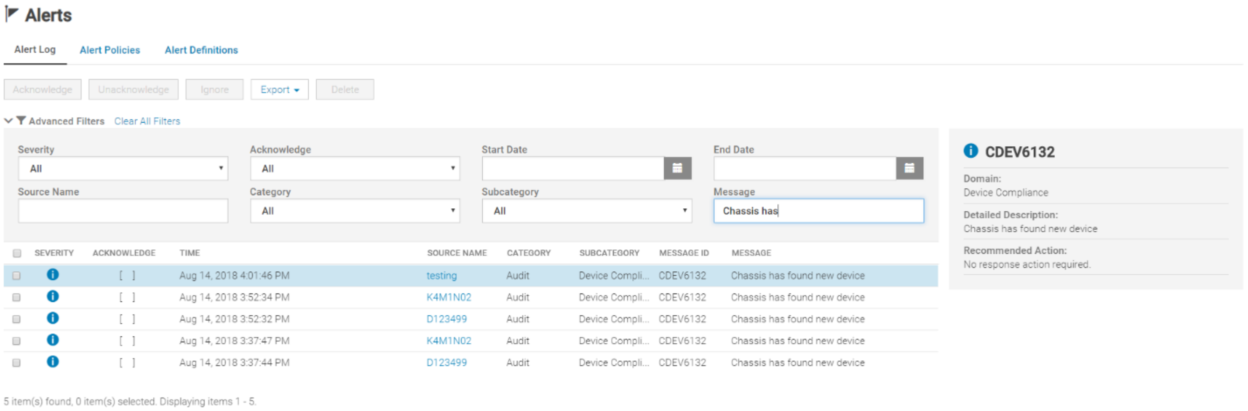
ⓘ JCP037

Domain:
Job Control

Detailed Description:
The (installation or configuration) job JID_344357260382 is successfully completed. - System Display Name: N/A - System Service Tag: K4M1N02 - FQDN: WIN-02GODDHDJTC - FQDD: N/A - Chassis Service Tag: testing

Recommended Action:
No response action is required.

Figure 24 Alert Log Filters (Filter by Category and Subcategory)



Severity: All
Acknowledge: All
Start Date:
End Date:
Source Name:
Category: All
Subcategory: All
Message: Chassis has

□	SEVERITY	ACKNOWLEDGE	TIME	SOURCE NAME	CATEGORY	SUBCATEGORY	MESSAGE ID	MESSAGE
□	ⓘ	[ ]	Aug 14, 2018 4:01:46 PM	testing	Audit	Device Compli...	CDEV6132	Chassis has found new device
□	ⓘ	[ ]	Aug 14, 2018 3:52:34 PM	K4M1N02	Audit	Device Compli...	CDEV6132	Chassis has found new device
□	ⓘ	[ ]	Aug 14, 2018 3:52:32 PM	D123499	Audit	Device Compli...	CDEV6132	Chassis has found new device
□	ⓘ	[ ]	Aug 14, 2018 3:37:47 PM	K4M1N02	Audit	Device Compli...	CDEV6132	Chassis has found new device
□	ⓘ	[ ]	Aug 14, 2018 3:37:44 PM	D123499	Audit	Device Compli...	CDEV6132	Chassis has found new device

5 item(s) found, 0 item(s) selected. Displaying items 1 - 5.

ⓘ CDEV6132

Domain:
Device Compliance

Detailed Description:
Chassis has found new device

Recommended Action:
No response action required.

Figure 25 Alert Log Filters (Filter by Message)

Appendix

REST calls can be performed to retrieve filtered audit and alert logs. Perform REST requests.

More details in how to install the and how to use it can be found in the Doc section of the tool: https://www.getpostman.com/docs/v6/.

Appendix I. Using REST to apply filters to Audit Logs

The following URIs can be used to access audit logs.

/api/ApplicationService/AuditLogs → To return a collection of audit logs.

/api/ApplicationService/AuditLogs(id) → Returns a single audit log entry.

Audit Logs Filters (REST)

The next table list the attributes that can be filter out by using a REST call.

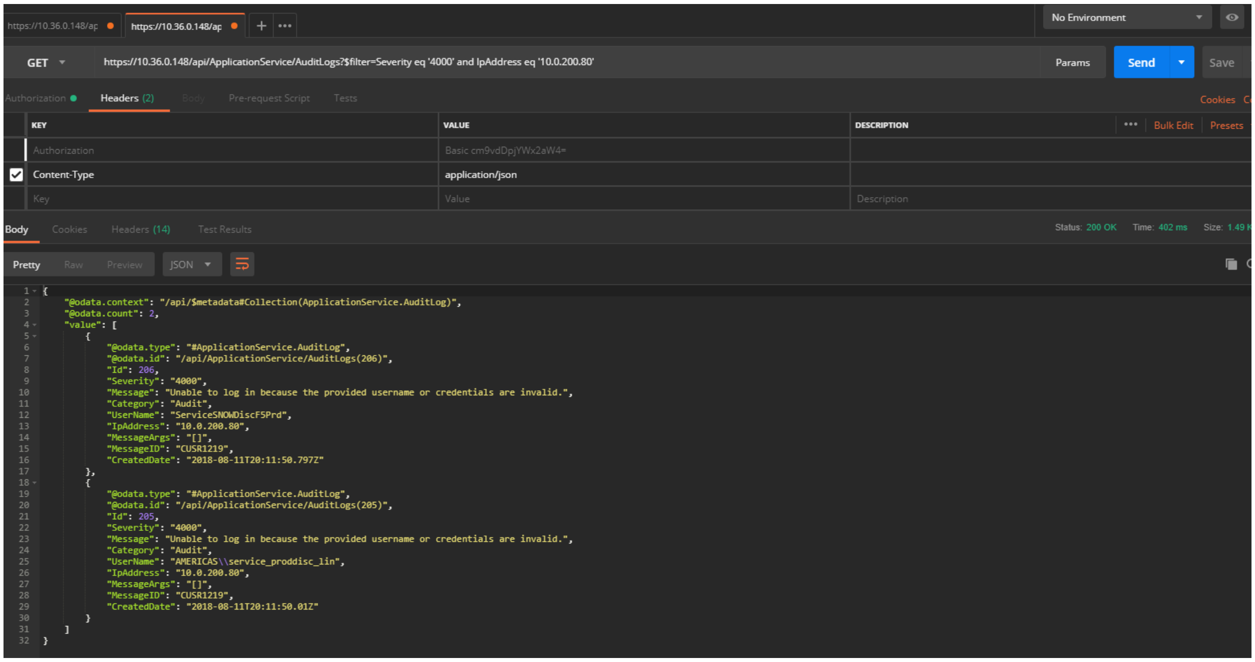
Filter Name	Description
Severity	Filter by the severity of the EEMI message. Critical, Warning and Informational.
Message	Filter by the EEMI message contents.
Category	Filter by the Category that the EEMI message comes under.
UserName	Filter by the Authenticated user who generated the EEMI message.
IpAddress	Filter by IP address of the authenticated user.
MessageID	Filter by the EEMI message identifier.
CreatedDateBegin	Filter by Created Date (start) of the EEMI message.
CreatedDateEnd	Filter by Created Date (end) of the EEMI message.

Table 3 Audit Log Filters

Above filters can be combined to have a more explicit list in response. The following is a sample of using filters in the REST request.

API request with all filters:

```
/api/ApplicationService/AuditLogs?$top=30&$skip=0&$filter=Severity eq '2000' and UserName eq 'root' and IpAddress eq '127.0.0.1' and Category eq 'Configuration' and Message eq 'EPS Event management plugin doc' and CreatedDate ge '2018-08-01 05:00:00.000' and CreatedDate le '2018-08-18 04:59:59.000'
```



GET https://10.36.0.148/api/ApplicationService/AuditLogs?$filter=Severity eq '4000' and IpAddress eq '10.0.200.80'

KEY	VALUE	DESCRIPTION
Authorization	Basic cm9vdDpjYWx2aW4=	
☑ Content-Type	application/json	
Key	Value	Description

Status: 200 OK Time: 402 ms Size: 1.49 K

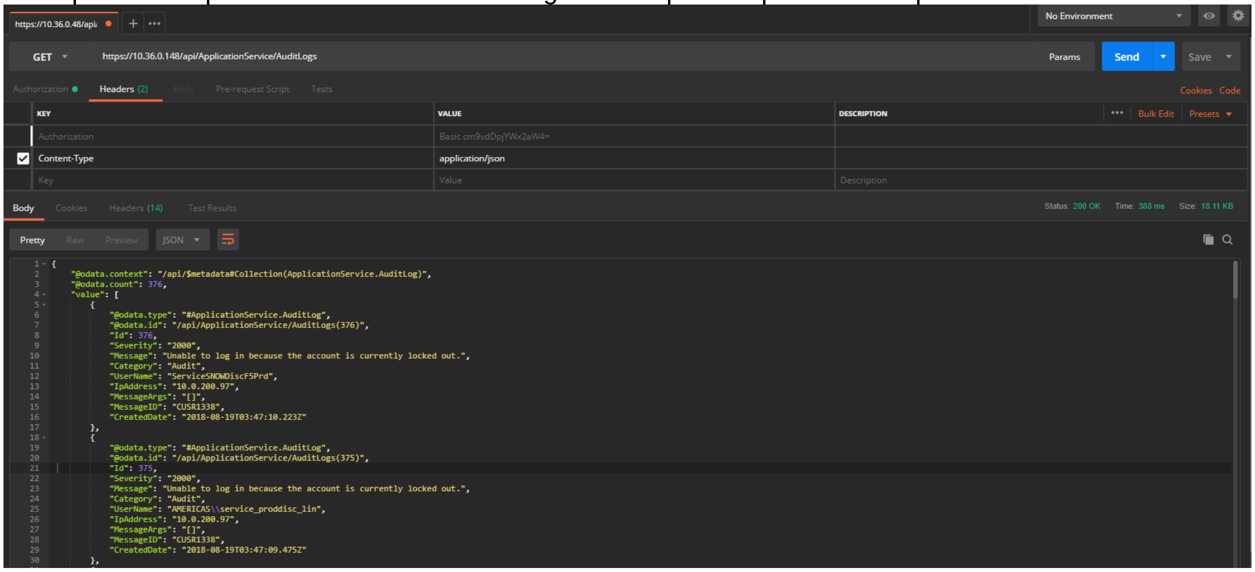
```
{
    "@odata.context": "/api/$metadata#Collection(ApplicationService.AuditLog)",
    "@odata.count": 2,
    "value": [
        {
            "@odata.type": "#ApplicationService.AuditLog",
            "@odata.id": "/api/ApplicationService/AuditLogs(206)",
            "Id": 206,
            "Severity": "4000",
            "Message": "Unable to log in because the provided username or credentials are invalid.",
            "Category": "Audit",
            "UserName": "ServiceSNOWDiscF5Prd",
            "IpAddress": "10.0.200.80",
            "MessageArgs": "[]",
            "MessageID": "CUSR1219",
            "CreatedDate": "2018-08-11T20:11:50.797Z"
        },
        {
            "@odata.type": "#ApplicationService.AuditLog",
            "@odata.id": "/api/ApplicationService/AuditLogs(205)",
            "Id": 205,
            "Severity": "4000",
            "Message": "Unable to log in because the provided username or credentials are invalid.",
            "Category": "Audit",
            "UserName": "AMERICAS\\service_proddisc_lin",
            "IpAddress": "10.0.200.80",
            "MessageArgs": "[]",
            "MessageID": "CUSR1219",
            "CreatedDate": "2018-08-11T20:11:50.01Z"
        }
    ]
}
```

Figure 26 Audit Logs REST Filters

Get all Audit Logs

URI	Description
/api/ApplicationService/AuditLogs	Returns a collection of audit logs.

The operation to perform is **GET**. The following is an output sample of the response:



	KEY	VALUE	DESCRIPTION
	Authorization	Basic cm9vdDpjYWx2aW4=	
☑	Content-Type	application/json	
	Key	Value	Description

Status: 200 OK Time: 388 ms Size: 18.11 KB

```
{
    "@odata.context": "/api/$metadata#Collection(ApplicationService.AuditLog)",
    "@odata.count": 376,
    "value": [
        {
            "@odata.type": "#ApplicationService.AuditLog",
            "@odata.id": "/api/ApplicationService/AuditLogs(376)",
            "Id": 376,
            "Severity": "2000",
            "Message": "Unable to log in because the account is currently locked out.",
            "Category": "Audit",
            "UserName": "ServiceSNOWDiscF5Prd",
            "IpAddress": "10.0.200.97",
            "MessageArgs": "[]",
            "MessageID": "CUSR1338",
            "CreatedDate": "2018-08-19T03:47:10.223Z"
        },
        {
            "@odata.type": "#ApplicationService.AuditLog",
            "@odata.id": "/api/ApplicationService/AuditLogs(375)",
            "Id": 375,
            "Severity": "2000",
            "Message": "Unable to log in because the account is currently locked out.",
            "Category": "Audit",
            "UserName": "AMERICAS\\service_proddisc_lin",
            "IpAddress": "10.0.200.97",
            "MessageArgs": "[]",
            "MessageID": "CUSR1338",
            "CreatedDate": "2018-08-19T03:47:09.475Z"
        },
```

Figure 27 All Audit Logs REST

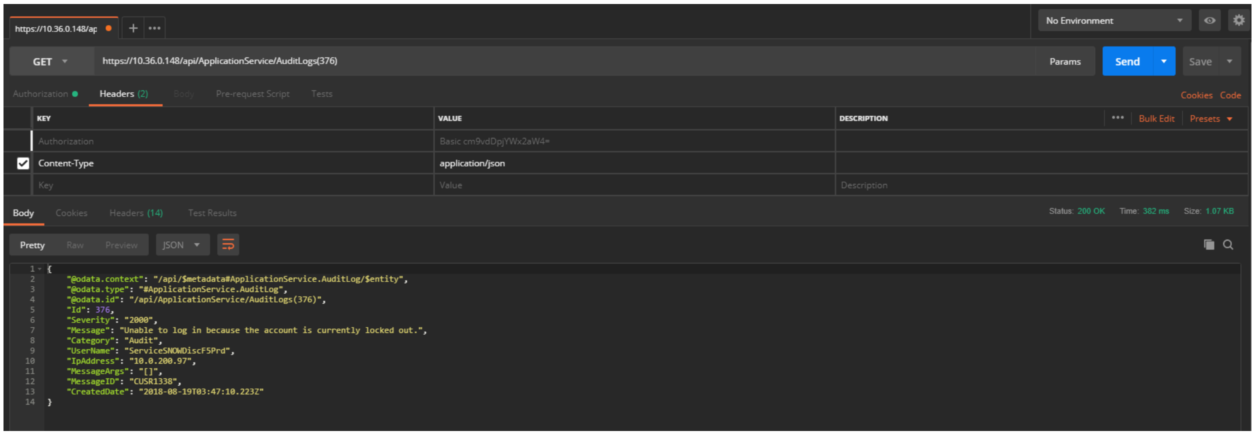
Payload Output Sample:

```
{
    "@odata.context": "/api/$metadata#Collection(ApplicationService.AuditLog)",
    "@odata.count": 6,
    "value": [
        {
            "@odata.type": "#ApplicationService.AuditLog",
            "@odata.id": "/api/ApplicationService/AuditLogs(387)",
            "Id": 387,
            "Severity": "1000",
            "Message": "Successfully logged off from  GUI .",
            "Category": "Audit",
            "UserName": "root",
            "IpAddress": "10.210.136.126",
            "MessageArgs": "GUI",
            "MessageID": "CUSR0003",
            "CreatedDate": "2018-08-21T16:47:23.554Z"
        },
        {
            "@odata.type": "#ApplicationService.AuditLog",
            "@odata.id": "/api/ApplicationService/AuditLogs(386)",
            "Id": 386,
            "Severity": "1000",
            "Message": "Successfully logged in from  GUI .",
            "Category": "Audit",
            "UserName": "root",
            "IpAddress": "10.210.136.126",
            "MessageArgs": "GUI",
            "MessageID": "CMON0001",
            "CreatedDate": "2018-08-21T15:42:07.185Z"
        },
        {
            "@odata.type": "#ApplicationService.AuditLog",
            "@odata.id": "/api/ApplicationService/AuditLogs(385)",
            "Id": 385,
            "Severity": "1000",
            "Message": "Successfully logged in from  GUI .",
            "Category": "Audit",
            "UserName": "root",
            "IpAddress": "10.210.136.126",
            "MessageArgs": "GUI",
            "MessageID": "CMON0001",
            "CreatedDate": "2018-08-21T14:41:08.004Z"
        },
        {
            "@odata.type": "#ApplicationService.AuditLog",
            "@odata.id": "/api/ApplicationService/AuditLogs(384)",
            "Id": 384,
            "Severity": "1000",
            "Message": "The job  Inventory Refresh   with id   27478   of type   inventory  has been scheduled
to run now.",
            "Category": "Configuration",
            "UserName": "root",
            "IpAddress": "10.210.136.126",
            "MessageArgs": "Inventory Refresh || 27478 || inventory",
            "MessageID": "CJOB0159",
            "CreatedDate": "2018-08-20T20:25:03.612Z"
        },
        {
            "@odata.type": "#ApplicationService.AuditLog",
            "@odata.id": "/api/ApplicationService/AuditLogs(383)",
            "Id": 383,
            "Severity": "1000",
            "Message": "The alert(s) with ID(s)  Multiple or All Event(s).  are deleted.",
            "Category": "Configuration",
            "UserName": "root",
            "IpAddress": "10.210.136.126",
            "MessageArgs": "Multiple or All Event(s).",
            "MessageID": "CMON0176",
            "CreatedDate": "2018-08-20T20:06:06.616Z"
        },
        {
            "@odata.type": "#ApplicationService.AuditLog",
            "@odata.id": "/api/ApplicationService/AuditLogs(382)",
            "Id": 382,
            "Severity": "1000",
            "Message": "Successfully logged off from  SSH .",
            "Category": "Audit",
            "UserName": "root",
            "IpAddress": "10.210.136.126",
            "MessageArgs": "SSH",
            "MessageID": "CUSR0003",
            "CreatedDate": "2018-08-20T20:00:20.682Z"
        }
    ],
    "@odata.nextLink": "/api/ApplicationService/AuditLogs?$skip=50&$top=50"
}
```

Get a Single Audit Log

URI	Description
/api/ApplicationService/AuditLogs(id)	Returns a single EEMI audit message.

The operation to perform is **GET**. The following is an output sample of the response:



GET https://10.36.0.148/api/ApplicationService/AuditLogs(376)

	KEY	VALUE	DESCRIPTION
	Authorization	Basic cm9vdDpjYWx2aW4=	
☑	Content-Type	application/json	
	Key	Value	Description

Status: 200 OK Time: 382 ms Size: 1.07 KB

```
{
    "@odata.context": "/api/$metadata#ApplicationService.AuditLog/$entity",
    "@odata.type": "#ApplicationService.AuditLog",
    "@odata.id": "/api/ApplicationService/AuditLogs(376)",
    "Id": 376,
    "Severity": "2000",
    "Message": "Unable to log in because the account is currently locked out.",
    "Category": "Audit",
    "UserName": "ServiceSNOWDiscF5Prd",
    "IpAddress": "10.0.200.97",
    "MessageArgs": "[]",
    "MessageID": "CUSR1338",
    "CreatedDate": "2018-08-19T03:47:10.223Z"
}
```

Figure 28 Single Audit Logs REST

Payload Sample Output:

```
{
    "@odata.context": "/api/$metadata#ApplicationService.AuditLog/$entity",
    "@odata.type": "#ApplicationService.AuditLog",
    "@odata.id": "/api/ApplicationService/AuditLogs(387)",
    "Id": 387,
    "Severity": "1000",
    "Message": "Successfully logged off from  GUI .",
    "Category": "Audit",
    "UserName": "root",
    "IpAddress": "10.210.136.126",
    "MessageArgs": "GUI",
    "MessageID": "CUSR0003",
    "CreatedDate": "2018-08-21T16:47:23.554Z"
}
```

Appendix II. Using REST to apply filters to Alert Logs

The following URIs can be used to access alert logs.

/api/AlertService/Alerts → Returns a collection of alert logs.

/api/AlertService/Alerts(id) → Returns a single alert log entry.

Alert Logs Filters (REST)

The next table list the attributes that can be filter out by using a REST call.

Filter Name	Description
AlertDeviceId	Filter by device id – default 0
AlertDeviceIdentifier	Filter by device identifier
AlertDeviceType	Filter by device type – default 0
SeverityType	Filter by severity type – default 0
StatusType	Filter by status type – default 0

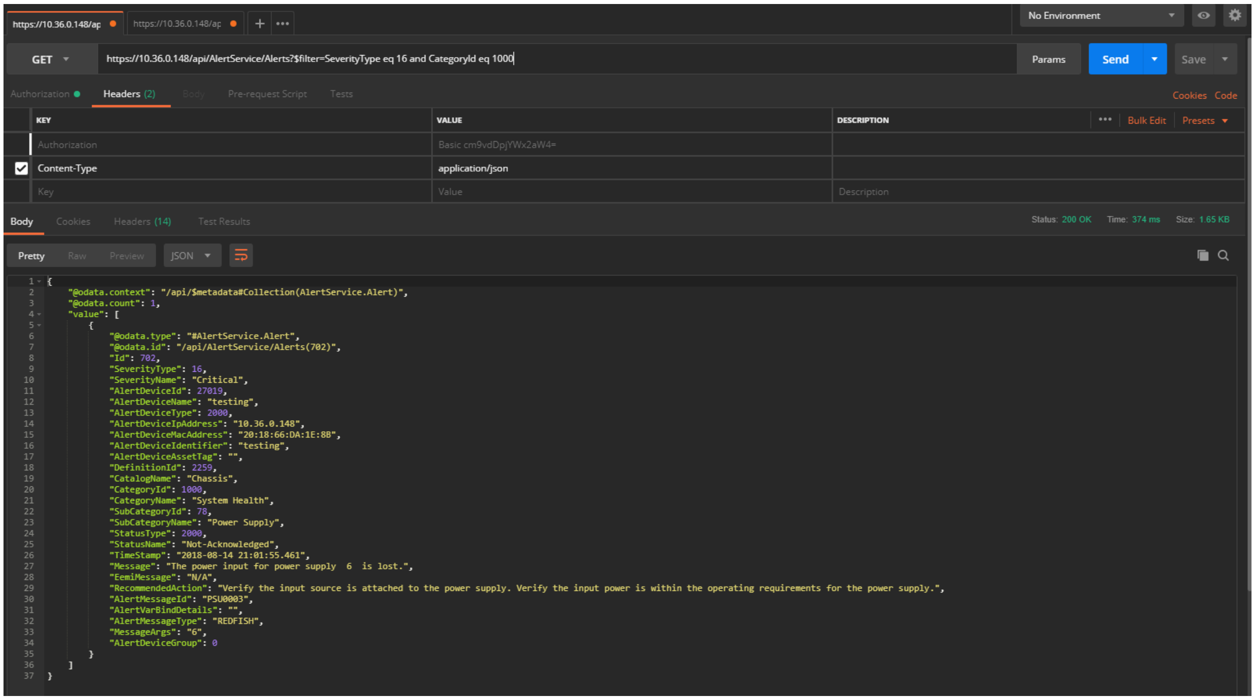
CategoryId	Filter by category id – default 0
SubCategoryId	Filter by sub category id – default 0
SubCategoryName	Filter by sub category name
Message	Filter by message
TimeStampBegin	Filter by alert time (begin)
TimeStampEnd	Filter by alert time (end)
AlertDeviceName	Filter by alert device name

Table 4 Alert Log Filters

Above filters can be combined to have a more explicit list in response. The following is a sample of using filters in the REST request.

API request with all filters:

/api/AlertService/Alerts?$filter=CategoryId eq 1004 and SeverityType eq 1 and StatusType eq 1000 and TimeStamp ge '2018-08-01 05:00:00.000' and TimeStamp le '2018-08-04 04:59:59.000' and AlertDeviceName eq 'test' and SubCategoryId eq 107 and Message eq 'test'&$top=30&$skip=0



GET https://10.36.0.148/api/AlertService/Alerts?$filter=SeverityType eq 16 and CategoryId eq 1000

KEY	VALUE	DESCRIPTION
Authorization	Basic cm9vdDpjYWx2aW4=	
☑ Content-Type	application/json	
Key	Value	Description

Status: 200 OK Time: 374 ms Size: 1.65 KB

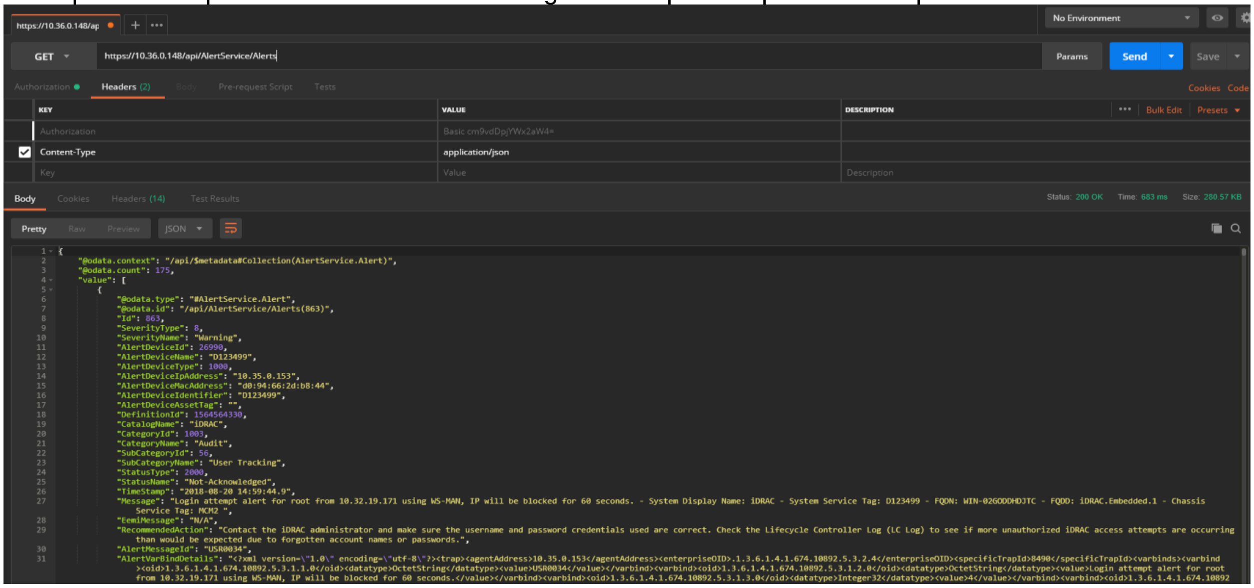
```
{
    "@odata.context": "/api/$metadata#Collection(AlertService.Alert)",
    "@odata.count": 1,
    "value": [
        {
            "@odata.type": "#AlertService.Alert",
            "@odata.id": "/api/AlertService/Alerts(702)",
            "Id": 702,
            "SeverityType": 16,
            "SeverityName": "Critical",
            "AlertDeviceId": 27019,
            "AlertDeviceName": "testing",
            "AlertDeviceType": 2000,
            "AlertDeviceIpAddress": "10.36.0.148",
            "AlertDeviceMacAddress": "20:18:66:DA:1E:8B",
            "AlertDeviceIdentifier": "testing",
            "AlertDeviceAssetTag": "",
            "DefinitionId": 2259,
            "CatalogName": "Chassis",
            "CategoryId": 1000,
            "CategoryName": "System Health",
            "SubCategoryId": 78,
            "SubCategoryName": "Power Supply",
            "StatusType": 2000,
            "StatusName": "Not-Acknowledged",
            "TimeStamp": "2018-08-14 21:01:55.461",
            "Message": "The power input for power supply  6  is lost.",
            "EemiMessage": "N/A",
            "RecommendedAction": "Verify the input source is attached to the power supply. Verify the input power is within the operating requirements for the power supply.",
            "AlertMessageId": "PSU0003",
            "AlertVarBindDetails": "",
            "AlertMessageType": "REDFISH",
            "MessageArgs": "6",
            "AlertDeviceGroup": 0
        }
    ]
}
```

Figure 29 Alert Logs REST Filters

Get all Alert Logs

URI	Description
/api/AlertService/Alerts	Returns a collection of alert logs.

The operation to perform is **GET**. The following is an output sample of the response:



GET https://10.36.0.148/api/AlertService/Alerts

KEY	VALUE	DESCRIPTION
Authorization	Basic cm9vdDpjYWx2aW4=	
☑ Content-Type	application/json	
Key	Value	Description

Status: 200 OK Time: 683 ms Size: 280.57 KB

```
{
    "@odata.context": "/api/$metadata#Collection(AlertService.Alert)",
    "@odata.count": 175,
    "value": [
        {
            "@odata.type": "#AlertService.Alert",
            "@odata.id": "/api/AlertService/Alerts(863)",
            "Id": 863,
            "SeverityType": 8,
            "SeverityName": "Warning",
            "AlertDeviceId": 26990,
            "AlertDeviceName": "D123499",
            "AlertDeviceType": 1000,
            "AlertDeviceIpAddress": "10.35.0.153",
            "AlertDeviceMacAddress": "d0:94:66:2d:b8:44",
            "AlertDeviceIdentifier": "D123499",
            "AlertDeviceAssetTag": "",
            "DefinitionId": 1564564330,
            "CatalogName": "iDRAC",
            "CategoryId": 1003,
            "CategoryName": "Audit",
            "SubCategoryId": 56,
            "SubCategoryName": "User Tracking",
            "StatusType": 2000,
            "StatusName": "Not-Acknowledged",
            "TimeStamp": "2018-08-20 14:59:44.9",
            "Message": "Login attempt alert for root from 10.32.19.171 using WS-MAN, IP will be blocked for 60 seconds. - System Display Name: iDRAC - System Service Tag: D123499 - FQDN: WIN-02GODDHDJTC - FQDD: iDRAC.Embedded.1 - Chassis
                Service Tag: MCM2 ",
            "EemiMessage": "N/A",
            "RecommendedAction": "Contact the iDRAC administrator and make sure the username and password credentials used are correct. Check the Lifecycle Controller Log (LC Log) to see if more unauthorized iDRAC access attempts are occurring
                than would be expected due to forgotten account names or passwords.",
            "AlertMessageId": "USR0034",
            "AlertVarBindDetails": "<?xml version=\"1.0\" encoding=\"utf-8\"?><trap><agentAddress>10.35.0.153</agentAddress><enterpriseOID>.1.3.6.1.4.1.674.10892.5.3.2.4</enterpriseOID><specificTrapId>8490</specificTrapId><varbinds><varbind
                ><oid>1.3.6.1.4.1.674.10892.5.3.1.1.0</oid><datatype>OctetString</datatype><value>USR0034</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.2.0</oid><datatype>OctetString</datatype><value>Login attempt alert for root
                from 10.32.19.171 using WS-MAN, IP will be blocked for 60 seconds.</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.3.0</oid><datatype>Integer32</datatype><value>4</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892
```

Figure 30 All Alert Logs REST

Payload Sample Output:

```
{
    "@odata.context": "/api/$metadata#Collection(AlertService.Alert)",
    "@odata.count": 44,
    "value": [
        {
            "@odata.type": "#AlertService.Alert",
            "@odata.id": "/api/AlertService/Alerts(919)",
            "Id": 919,
            "SeverityType": 8,
            "SeverityName": "Warning",
            "AlertDeviceId": 26990,
            "AlertDeviceName": "D123499",
            "AlertDeviceType": 1000,
            "AlertDeviceIpAddress": "10.35.0.153",
            "AlertDeviceMacAddress": "d0:94:66:2d:b8:44",
            "AlertDeviceIdentifier": "D123499",
            "AlertDeviceAssetTag": "",
            "DefinitionId": 1564564330,
            "CatalogName": "iDRAC",
            "CategoryId": 1003,
            "CategoryName": "Audit",
            "SubCategoryId": 56,
            "SubCategoryName": "User Tracking",
            "StatusType": 2000,
            "StatusName": "Not-Acknowledged",
            "TimeStamp": "2018-08-21 19:59:55.183",
            "Message": "Login attempt alert for root from 10.32.19.128 using WS-MAN, IP will be
blocked for 60 seconds. - System Display Name: iDRAC - System Service Tag: D123499 - FQDN: WIN-
02GODDHDJTC - FQDD: iDRAC.Embedded.1 - Chassis Service Tag: MCM2 ",
            "EemiMessage": "N/A",
            "RecommendedAction": "Contact the iDRAC administrator and make sure the username and
password credentials used are correct. Check the Lifecycle Controller Log (LC Log) to see if more
unauthorized iDRAC access attempts are occurring than would be expected due to forgotten account
names or passwords.",
            "AlertMessageId": "USR0034",
            "AlertVarBindDetails": "<?xml version=\"1.0\" encoding=\"utf-
8\"?><trap><agentAddress>10.35.0.153</agentAddress><enterpriseOID>.1.3.6.1.4.1.674.10892.5.3.2.4</ent
erpriseOID><specificTrapId>8490</specificTrapId><varbinds><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.1
.0</oid><datatype>OctetString</datatype><value>USR0034</value></varbind><varbind><oid>1.3.6.1.4.1.674
.10892.5.3.1.2.0</oid><datatype>OctetString</datatype><value>Login attempt alert for root from
10.32.19.128 using WS-MAN, IP will be blocked for 60
seconds.</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.3.0</oid><datatype>Integer32</dat
atype><value>4</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.4.0</oid><datatype>OctetStr
```

```
ing</datatype><value>D123499</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.5.0</oid><dat
atype>OctetString</datatype><value>WIN-
02GODDHDJTC</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.6.0</oid><datatype>OctetString
</datatype><value>iDRAC.Embedded.1</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.7.0</oi
d><datatype>OctetString</datatype><value>iDRAC</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5
.3.1.8.0</oid><datatype>OctetString</datatype><value>\"root\",\"10.32.19.128\",\"WS-
MAN\",\"60\"</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.9.0</oid><datatype>OctetStrin
g</datatype><value>MCM2</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.10.0</oid><datatyp
e>OctetString</datatype><value></value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.11.0</oid>
<datatype>OctetString</datatype><value>iDRAC-D123499</value></varbind></varbinds></trap>",
            "AlertMessageType": "SNMP",
            "MessageArgs": "",
            "AlertDeviceGroup": 0
        },
        {
            "@odata.type": "#AlertService.Alert",
            "@odata.id": "/api/AlertService/Alerts(918)",
            "Id": 918,
            "SeverityType": 8,
            "SeverityName": "Warning",
            "AlertDeviceId": 26990,
            "AlertDeviceName": "D123499",
            "AlertDeviceType": 1000,
            "AlertDeviceIpAddress": "10.35.0.153",
            "AlertDeviceMacAddress": "d0:94:66:2d:b8:44",
            "AlertDeviceIdentifier": "D123499",
            "AlertDeviceAssetTag": "",
            "DefinitionId": 1564564330,
            "CatalogName": "iDRAC",
            "CategoryId": 1003,
            "CategoryName": "Audit",
            "SubCategoryId": 56,
            "SubCategoryName": "User Tracking",
            "StatusType": 2000,
            "StatusName": "Not-Acknowledged",
            "TimeStamp": "2018-08-21 19:59:49.003",
            "Message": "Login attempt alert for root from 10.32.19.171 using WS-MAN, IP will be
blocked for 60 seconds. - System Display Name: iDRAC - System Service Tag: D123499 - FQDN: WIN-
02GODDHDJTC - FQDD: iDRAC.Embedded.1 - Chassis Service Tag: MCM2 ",
            "EemiMessage": "N/A",
            "RecommendedAction": "Contact the iDRAC administrator and make sure the username and
password credentials used are correct. Check the Lifecycle Controller Log (LC Log) to see if more
unauthorized iDRAC access attempts are occurring than would be expected due to forgotten account
names or passwords.",
            "AlertMessageId": "USR0034",
            "AlertVarBindDetails": "<?xml version=\"1.0\" encoding=\"utf-
8\"?><trap><agentAddress>10.35.0.153</agentAddress><enterpriseOID>.1.3.6.1.4.1.674.10892.5.3.2.4</ent
erpriseOID><specificTrapId>8490</specificTrapId><varbinds><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.1
.0</oid><datatype>OctetString</datatype><value>USR0034</value></varbind><varbind><oid>1.3.6.1.4.1.674
.10892.5.3.1.2.0</oid><datatype>OctetString</datatype><value>Login attempt alert for root from
10.32.19.171 using WS-MAN, IP will be blocked for 60
seconds.</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.3.0</oid><datatype>Integer32</dat
atype><value>4</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.4.0</oid><datatype>OctetStr
ing</datatype><value>D123499</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.5.0</oid><dat
atype>OctetString</datatype><value>WIN-
02GODDHDJTC</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.6.0</oid><datatype>OctetString
</datatype><value>iDRAC.Embedded.1</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.7.0</oi
d><datatype>OctetString</datatype><value>iDRAC</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5
.3.1.8.0</oid><datatype>OctetString</datatype><value>\"root\",\"10.32.19.171\",\"WS-
MAN\",\"60\"</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.9.0</oid><datatype>OctetStrin
g</datatype><value>MCM2</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.10.0</oid><datatyp
e>OctetString</datatype><value></value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.11.0</oid>
<datatype>OctetString</datatype><value>iDRAC-D123499</value></varbind></varbinds></trap>",
            "AlertMessageType": "SNMP",
            "MessageArgs": "",
            "AlertDeviceGroup": 0
        },
        {
            "@odata.type": "#AlertService.Alert",
            "@odata.id": "/api/AlertService/Alerts(917)",
            "Id": 917,
            "SeverityType": 8,
            "SeverityName": "Warning",
```

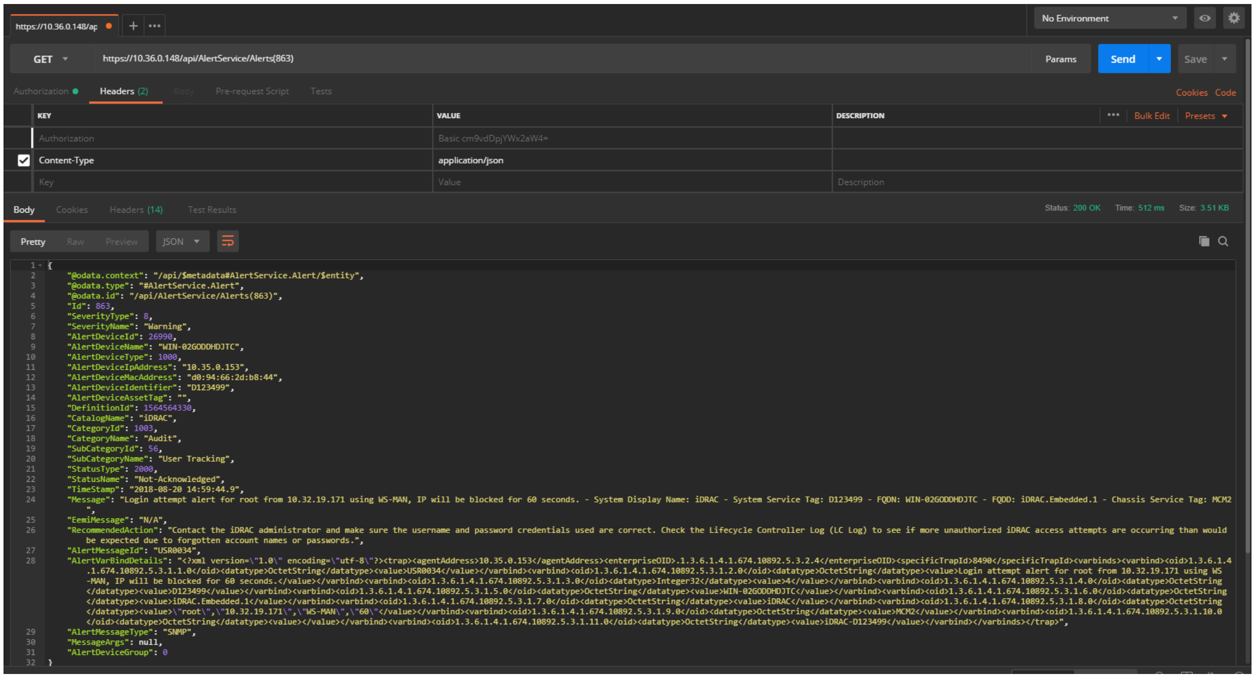
Get all Alert Logs

```
            "AlertDeviceId": 26990,
            "AlertDeviceName": "D123499",
            "AlertDeviceType": 1000,
            "AlertDeviceIpAddress": "10.35.0.153",
            "AlertDeviceMacAddress": "d0:94:66:2d:b8:44",
            "AlertDeviceIdentifier": "D123499",
            "AlertDeviceAssetTag": "",
            "DefinitionId": 1564564330,
            "CatalogName": "iDRAC",
            "CategoryId": 1003,
            "CategoryName": "Audit",
            "SubCategoryId": 56,
            "SubCategoryName": "User Tracking",
            "StatusType": 2000,
            "StatusName": "Not-Acknowledged",
            "TimeStamp": "2018-08-21 18:59:50.741",
            "Message": "Login attempt alert for root from 10.32.19.171 using WS-MAN, IP will be 
blocked for 60 seconds. - System Display Name: iDRAC - System Service Tag: D123499 - FQDN: WIN-
02GODDHDJTC - FQDD: iDRAC.Embedded.1 - Chassis Service Tag: MCM2 ",
            "EemiMessage": "N/A",
            "RecommendedAction": "Contact the iDRAC administrator and make sure the username and 
password credentials used are correct. Check the Lifecycle Controller Log (LC Log) to see if more 
unauthorized iDRAC access attempts are occurring than would be expected due to forgotten account 
names or passwords.",
            "AlertMessageId": "USR0034",
            "AlertVarBindDetails": "<?xml version=\"1.0\" encoding=\"utf-
8\"?><trap><agentAddress>10.35.0.153</agentAddress><enterpriseOID>.1.3.6.1.4.1.674.10892.5.3.2.4</ent
erpriseOID><specificTrapId>8490</specificTrapId><varbinds><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.1
.0</oid><datatype>OctetString</datatype><value>USR0034</value></varbind><varbind><oid>1.3.6.1.4.1.674
.10892.5.3.1.2.0</oid><datatype>OctetString</datatype><value>Login attempt alert for root from 
10.32.19.171 using WS-MAN, IP will be blocked for 60 
seconds.</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.3.0</oid><datatype>Integer32</dat
atype><value>4</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.4.0</oid><datatype>OctetStr
ing</datatype><value>D123499</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.5.0</oid><dat
atype>OctetString</datatype><value>WIN-
02GODDHDJTC</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.6.0</oid><datatype>OctetString
</datatype><value>iDRAC.Embedded.1</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.7.0</oi
d><datatype>OctetString</datatype><value>iDRAC</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5
.3.1.8.0</oid><datatype>OctetString</datatype><value>\"root\",\"10.32.19.171\",\"WS-
MAN\",\"60\"</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.9.0</oid><datatype>OctetStrin
g</datatype><value>MCM2</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.10.0</oid><datatyp
e>OctetString</datatype><value></value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.11.0</oid>
<datatype>OctetString</datatype><value>iDRAC-D123499</value></varbind></varbinds></trap>",
            "AlertMessageType": "SNMP",
            "MessageArgs": "",
            "AlertDeviceGroup": 0
        },
        {
            "@odata.type": "#AlertService.Alert",
            "@odata.id": "/api/AlertService/Alerts(916)",
            "Id": 916,
            "SeverityType": 8,
            "SeverityName": "Warning",
            "AlertDeviceId": 26990,
            "AlertDeviceName": "D123499",
            "AlertDeviceType": 1000,
            "AlertDeviceIpAddress": "10.35.0.153",
            "AlertDeviceMacAddress": "d0:94:66:2d:b8:44",
            "AlertDeviceIdentifier": "D123499",
            "AlertDeviceAssetTag": "",
            "DefinitionId": 1564564330,
            "CatalogName": "iDRAC",
            "CategoryId": 1003,
            "CategoryName": "Audit",
            "SubCategoryId": 56,
            "SubCategoryName": "User Tracking",
            "StatusType": 2000,
            "StatusName": "Not-Acknowledged",
            "TimeStamp": "2018-08-21 18:59:46.002",
            "Message": "Login attempt alert for root from 10.32.19.128 using WS-MAN, IP will be 
blocked for 60 seconds. - System Display Name: iDRAC - System Service Tag: D123499 - FQDN: WIN-
02GODDHDJTC - FQDD: iDRAC.Embedded.1 - Chassis Service Tag: MCM2 ",
            "EemiMessage": "N/A",
            "RecommendedAction": "Contact the iDRAC administrator and make sure the username and
password credentials used are correct. Check the Lifecycle Controller Log (LC Log) to see if more
unauthorized iDRAC access attempts are occurring than would be expected due to forgotten account
names or passwords.",
            "AlertMessageId": "USR0034",
            "AlertVarBindDetails": "<?xml version=\"1.0\" encoding=\"utf-
8\"?><trap><agentAddress>10.35.0.153</agentAddress><enterpriseOID>.1.3.6.1.4.1.674.10892.5.3.2.4</ent
erpriseOID><specificTrapId>8490</specificTrapId><varbinds><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.1
.0</oid><datatype>OctetString</datatype><value>USR0034</value></varbind><varbind><oid>1.3.6.1.4.1.674
.10892.5.3.1.2.0</oid><datatype>OctetString</datatype><value>Login attempt alert for root from
10.32.19.128 using WS-MAN, IP will be blocked for 60
seconds.</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.3.0</oid><datatype>Integer32</dat
atype><value>4</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.4.0</oid><datatype>OctetStr
ing</datatype><value>D123499</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.5.0</oid><dat
atype>OctetString</datatype><value>WIN-
02GODDHDJTC</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.6.0</oid><datatype>OctetString
</datatype><value>iDRAC.Embedded.1</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.7.0</oi
d><datatype>OctetString</datatype><value>iDRAC</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5
.3.1.8.0</oid><datatype>OctetString</datatype><value>\"root\",\"10.32.19.128\",\"WS-
MAN\",\"60\"</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.9.0</oid><datatype>OctetStrin
g</datatype><value>MCM2</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.10.0</oid><datatyp
e>OctetString</datatype><value></value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.11.0</oid>
<datatype>OctetString</datatype><value>iDRAC-D123499</value></varbind></varbinds></trap>",
            "AlertMessageType": "SNMP",
            "MessageArgs": "",
            "AlertDeviceGroup": 0
        }
    ]
}
```

Get a Single Alert Log

URI	Description
/api/AlertService/Alerts(id)	Returns a single alert log message.

The operation to perform is **GET**. The following is an output sample of the response:



GET https://10.36.0.148/api/AlertService/Alerts(863)

	KEY	VALUE	DESCRIPTION
	Authorization	Basic cm9vdDpjYWx2aW4=	
☑	Content-Type	application/json	

Status: 200 OK Time: 512 ms Size: 3.51 KB

```
{
    "@odata.context": "/api/$metadata#AlertService.Alert/$entity",
    "@odata.type": "#AlertService.Alert",
    "@odata.id": "/api/AlertService/Alerts(863)",
    "Id": 863,
    "SeverityType": 8,
    "SeverityName": "Warning",
    "AlertDeviceId": 26990,
    "AlertDeviceName": "WIN-02GODDHDJTC",
    "AlertDeviceType": 1000,
    "AlertDeviceIpAddress": "10.35.0.153",
    "AlertDeviceMacAddress": "d0:94:66:2d:b8:44",
    "AlertDeviceIdentifier": "D123499",
    "AlertDeviceAssetTag": "",
    "DefinitionId": 1564564330,
    "CatalogName": "iDRAC",
    "CategoryId": 1003,
    "CategoryName": "Audit",
    "SubCategoryId": 56,
    "SubCategoryName": "User Tracking",
    "StatusType": 2000,
    "StatusName": "Not-Acknowledged",
    "TimeStamp": "2018-08-20 14:59:44.9",
    "Message": "Login attempt alert for root from 10.32.19.171 using WS-MAN, IP will be blocked for 60 seconds. - System Display Name: iDRAC - System Service Tag: D123499 - FQDN: WIN-02GODDHDJTC - FQDD: iDRAC.Embedded.1 - Chassis Service Tag: MCM2
        ",
    "EemiMessage": "N/A",
    "RecommendedAction": "Contact the iDRAC administrator and make sure the username and password credentials used are correct. Check the Lifecycle Controller Log (LC Log) to see if more unauthorized iDRAC access attempts are occurring than would
        be expected due to forgotten account names or passwords.",
    "AlertMessageId": "USR0034",
    "AlertVarBindDetails": "<?xml version=\"1.0\" encoding=\"utf-8\"?><trap><agentAddress>10.35.0.153</agentAddress><enterpriseOID>.1.3.6.1.4.1.674.10892.5.3.2.4</enterpriseOID><specificTrapId>8490</specificTrapId><varbinds><varbind><oid>1.3.6.1.4
        .1.674.10892.5.3.1.1.0</oid><datatype>OctetString</datatype><value>USR0034</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.2.0</oid><datatype>OctetString</datatype><value>Login attempt alert for root from 10.32.19.171 using WS
        -MAN, IP will be blocked for 60 seconds.</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.3.0</oid><datatype>Integer32</datatype><value>4</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.4.0</oid><datatype>OctetString
        </datatype><value>D123499</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.5.0</oid><datatype>OctetString</datatype><value>WIN-02GODDHDJTC</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.6.0</oid><datatype>OctetString
        </datatype><value>iDRAC.Embedded.1</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.7.0</oid><datatype>OctetString</datatype><value>iDRAC</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.8.0</oid><datatype>OctetString
        </datatype><value>\"root\",\"10.32.19.171\",\"WS-MAN\",\"60\"</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.9.0</oid><datatype>OctetString</datatype><value>MCM2</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.10.0
        </oid><datatype>OctetString</datatype><value></value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.11.0</oid><datatype>OctetString</datatype><value>iDRAC-D123499</value></varbind></varbinds></trap>",
    "AlertMessageType": "SNMP",
    "MessageArgs": null,
    "AlertDeviceGroup": 0
}
```

Figure 31 Single Alert Logs REST

Get a Single Alert Log

Payload Sample Output:

```
{
    "@odata.context": "/api/$metadata#AlertService.Alert/$entity",
    "@odata.type": "#AlertService.Alert",
    "@odata.id": "/api/AlertService/Alerts(919)",
    "Id": 919,
    "SeverityType": 8,
    "SeverityName": "Warning",
    "AlertDeviceId": 26990,
    "AlertDeviceName": "WIN-02GODDHDJTC",
    "AlertDeviceType": 1000,
    "AlertDeviceIpAddress": "10.35.0.153",
    "AlertDeviceMacAddress": "d0:94:66:2d:b8:44",
    "AlertDeviceIdentifier": "D123499",
    "AlertDeviceAssetTag": "",
    "DefinitionId": 1564564330,
    "CatalogName": "iDRAC",
    "CategoryId": 1003,
    "CategoryName": "Audit",
    "SubCategoryId": 56,
    "SubCategoryName": "User Tracking",
    "StatusType": 2000,
    "StatusName": "Not-Acknowledged",
    "TimeStamp": "2018-08-21 19:59:55.183",
    "Message": "Login attempt alert for root from 10.32.19.128 using WS-MAN, IP will be blocked for 60 seconds.
- System Display Name: iDRAC - System Service Tag: D123499 - FQDN: WIN-02GODDHDJTC - FQDD: iDRAC.Embedded.1 -
Chassis Service Tag: MCM2 ",
    "EemiMessage": "N/A",
    "RecommendedAction": "Contact the iDRAC administrator and make sure the username and password credentials
used are correct. Check the Lifecycle Controller Log (LC Log) to see if more unauthorized iDRAC access attempts
are occurring than would be expected due to forgotten account names or passwords.",
    "AlertMessageId": "USR0034",
    "AlertVarBindDetails": "<?xml version=\"1.0\" encoding=\"utf-
8\"?><trap><agentAddress>10.35.0.153</agentAddress><enterpriseOID>.1.3.6.1.4.1.674.10892.5.3.2.4</enterpriseOID>
<specificTrapId>8490</specificTrapId><varbinds><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.1.0</oid><datatype>Octe
tString</datatype><value>USR0034</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.2.0</oid><datatype>O
ctetString</datatype><value>Login attempt alert for root from 10.32.19.128 using WS-MAN, IP will be blocked for
60
seconds.</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.3.0</oid><datatype>Integer32</datatype><valu
e>4</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.4.0</oid><datatype>OctetString</datatype><value>D
123499</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.5.0</oid><datatype>OctetString</datatype><valu
e>WIN-
02GODDHDJTC</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.6.0</oid><datatype>OctetString</datatype>
<value>iDRAC.Embedded.1</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.7.0</oid><datatype>OctetStrin
g</datatype><value>iDRAC</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.8.0</oid><datatype>OctetStri
ng</datatype><value>\"root\",\"10.32.19.128\",\"WS-
MAN\",\"60\"</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.9.0</oid><datatype>OctetString</datatype
><value>MCM2</value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.10.0</oid><datatype>OctetString</datatyp
e><value></value></varbind><varbind><oid>1.3.6.1.4.1.674.10892.5.3.1.11.0</oid><datatype>OctetString</datatype><
value>iDRAC-D123499</value></varbind></varbinds></trap>",
    "AlertMessageType": "SNMP",
    "MessageArgs": null,
    "AlertDeviceGroup": 0
}
```