



System Status

- [Audit Logs, on page 1](#)
- [System Logs, on page 3](#)

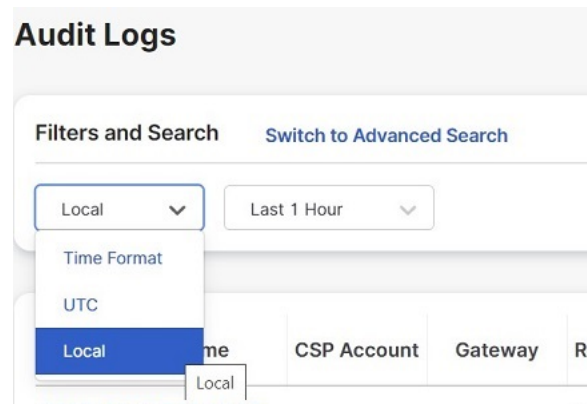
Audit Logs

Audit logs contain details of actions performed by Users. This includes, but not limited to, actions of login/logout activity, creating, deleting, updating, enabling, disabling etc. of Profiles, Rules, Gateways or any User activity that relates to the configuration and operation of the Multicloud Defense solution.

Time Format

Logs can be displayed in UTC (Coordinated Universal Time) or Local time format. Local means the time zone of the user as configured e.g. USA/Pacific. Date and Time of logs will be displayed in ISO 8601 format (Complete date plus hours, minutes, seconds and a decimal fraction of a second - YYYY-MM-DD T HH:MM:SS.S). Example: 2020-11-22T10:58:46.820

To select, or switch between, different Time Formats, click the radio button as shown:



Timeframe

Logs can be displayed in increment options from 15 minutes to 30 days, or Custom timeframes. To select, or switch between, timeframes, click the pulldown and select timeframe as shown:

Audit Logs

Filters and Search [Switch to Advanced Search](#)

Local

Select Time Frame

- Last 15 Mins
- Last 1 Hour
- Last 1 Day
- Last 7 Days
- Last 30 Days
- Custom

Date and Time	Resource N...	User	Role	Source
2023-07-26T14:43			ROLE_SU...	

For Custom timeframes, select **Custom**, the **Start** and the **End** date or time by clicking the calendar objects followed by **Save**.

Search Filter

Logs can be filtered using the Search function and audit log fields. The audit log fields are Action Type Source IP User Gateway CSP Account Role

To filter audit logs on one, or multiple, fields:

Step 1 Left mouse-click in the Search field to access the pull down menu.

Audit Logs

Filters and Search [Switch to Quick Filters](#)

Q

- Action
- Type
- Source IP
- User
- Gateway
- CSP Account
- Role

CSP Account	Gateway	I

Step 2 Select a field e.g. *Action*.

Step 3 Type a desired search string e.g. *DELETE*.

Step 4 Add additional fields to the search criteria as required.

Example: Filter for Actions = "**DELETE**" and performed by user with string containing "**steve**" would appear in the filter criteria and results.

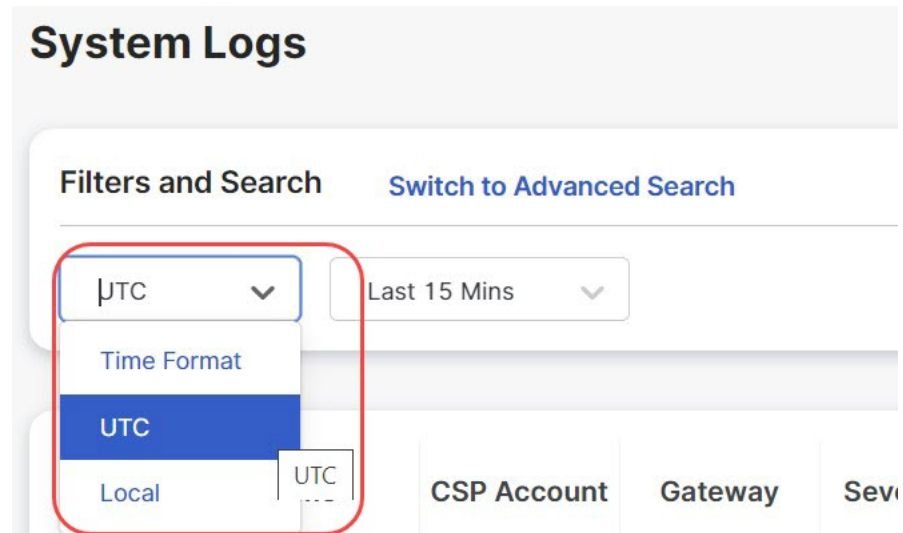
System Logs

System logs contain details of actions performed by the Multicloud Defense solution. This includes, but not limited to, system messages, gateway events, instance creation/deletion and other configuration and operation modifications of the Multicloud Defense solution (system).

Time Format

Logs can be displayed in UTC (Coordinated Universal Time) or Local time format. Local means the time zone of the user as configured e.g. USA/Pacific. Date and Time of logs will be displayed in ISO 8601 format (Complete date plus hours, minutes, seconds and a decimal fraction of a second - YYYY-MM-DD T HH:MM:SS.S). Example: 2020-11-22T10:58:46.820

To select, or switch between, different Time Formats, click the radio button as shown:



Timeframe

Logs can be displayed in increment options from 15 minutes to 30 days, or Custom timeframes.

To select, or switch between, timeframes, click the pulldown and select timeframe as shown:

System Logs

Filters and Search [Switch to Advanced Search](#)

UTC ▼

Last 15 Mins ▼

Select Time Frame

Last 15 Mins

Last 1 Hour

Last 1 Day

Last 7 Days

Last 30 Days

Custom

Date and Time

Severity

Sub Ty

No Logs Found

For Custom timeframes, select **Custom**, the **Start** and the **End** date or time by clicking the calendar objects followed by **Save**.

Search Filter

Logs can be filtered using the Search function and System log fields.

The System log fields are Gateway CSP Account Message

To filter System logs on one, or multiple, fields:

Step 1 Left mouse-click in the Search field to access the pull down menu.

System Logs

Filters and Search [Switch to Quick Filters](#)

Q

- Gateway
- CSP Account
- Message
- Severity
- Sub Type

CSP Account	Gateway	Severity	Sub Type
-------------	---------	----------	----------

Step 2 Select a field e.g. Gateway.

Step 3 Type a desired search string e.g. `ingress`.

Step 4 Add additional fields to the search criteria as required.

Example: Filter for a Gateway = **"ingress"** and Messages containing **"created"** would appear in the filter criteria and results.