



ArcSight Command Center

Software Version: 8.1

User's Guide

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2001-2023 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.

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

Contents

Chapter 1: Welcome to the Real-time Threat Detection Command Center	6
Starting the Real-time Threat Detection Command Center	6
Configuring Your Browser	6
Launching Real-time Threat Detection Command Center	6
Logging in to Real-time Threat Detection Command Center	7
Basic Navigation	8
Using the Site Map	8
Monitoring Usage Metrics (Stats)	9
Chapter 2: Viewing System Information	12
Managing Dashlets in the Dashboard Home Page	12
Adding a Data Monitor Dashlet to the Dashboards Page	13
Adding My Dashboards to the Dashboard Home Page	14
Rearrange Real-time Threat Detection Command Center Dashboard If Charts and Tables Overlap	15
Adding My Notifications to the Dashboards Home Page	15
Adding a Query Viewer to the Dashboards Home Page	16
Changing the Dashboards Layout	17
Managing Dashboards in the Dashboard Navigator Page	17
Viewing Dashboards in the Dashboard Navigator	17
Navigate from a Dashboard to a Channel in a Data Monitor	19
Specifying a Dashlet Chart Type	20
Downloading a Dashlet to a CSV File	23
Viewing Details for Events in a Last N Events Data Monitor	24
Using the Cluster View Dashboard	25
Distributed Correlation Stats	25
Cluster	26
Details and Metrics for Individual Services	27
Audit Event Lists	28
Using the MITRE Dashboard	29
MITRE Activity	30
MITRE Coverage	30
Chapter 3: Monitoring Events Through Active Channels	31
Viewing Events On an Active Channel	32

Viewing a Channel Condition Summary	34
Viewing the Event Priority for a Channel	35
Evaluate the Network Route of an Event in a Channel	36
Accessing Integration Commands from an Event List	39
Accessing Recon or Recon Search from an Event List	40
About the Active Channel Header	41
Using the Active Channel Radar	43
Annotating an Event	44
Viewing Event Information	45
Managing Channels	46
Creating an Event Channel	47
Specifying Columns For the Active Channel Event List	49
Specifying Filter Conditions for an Active Channel	50
Creating a Channel Based on an Event Attribute	55
Editing an Event Channel	57
Deleting an Event Channel	60
Copying an Event Channel	60
Marking an Event as Reviewed	61
Visualizing an Event Graphically	61
 Chapter 4: Understanding Active Lists	 63
Deleting an Entry from an Active List	63
Exporting an Active List to a CSV File	64
Filtering an Active List	64
 Chapter 4: Understanding Session Lists	 66
Deleting an Entry from a Session List	66
Exporting a Session List to a CSV File	67
Filtering a Session List	67
 Chapter 5: Understanding Field Sets	 69
 Chapter 6: Applications	 70

Appendix 7: Frequently Asked Questions	71
What happens if I'm investigating a channel that has event fields that are not supported in Command Center?	71
Can I change the default start time and end time for an event channel?	71
What do I do if a channel is taking long to load?	72
How many channels can I have open at one time?	72
What fields are supported in Command Center channels?	72
Does Command Center support non-ASCII payload data?	73
How do I get my <code>[[[Undefined variable _ARSTc_Variables.NewDownloadCenter]]]</code> credentials?	73
Why are channels not current in a new Real-time Threat Detection session?	73
Does the change to or from Daylight Savings Time effect an open active channel?	74
Why does the right end of the top menu bar appear overlapped?	74
Send Documentation Feedback	75

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Chapter 1: Welcome to the Real-time Threat Detection Command Center

The Real-time Threat Detection Command Center is a web-based user interface that enables you to perform many of the functions found in the ArcSight Console. Real-time Threat Detection Command Center provides dashboards, several kinds of searches, notifications, and administrative functions for managing active channels and system logs.

Starting the Real-time Threat Detection Command Center

Configuring Your Browser

For best results, specify the same language for the browser as you did for the Manager. If the browser allows you to select a priority language, select the same language defined by Manager.

Most browsers will give you a certificate error if you have not imported the Manager's certificate into the browser. You can ignore the error and choose to continue. Exporting a certificate is covered in the [Administrator's Guide for Real-time Threat Detection](#). In the Edge browser in Windows 10, you do not import the certificate from the browser. From the Start icon, search for "internet options" and select **Content > Certificates > Import** and follow the wizard. (You cannot open the Edge browser as user *administrator*, but you may log in as a user other than *administrator* with administrative privileges.)

To view this user interface properly, configure your browser to at least 1920 by 1080 pixels. The Real-time Threat Detection Command Center top menu bar appears to have the right-most Top menu bar options overlapped if the browser window dimensions are smaller than 1920 by 1080 pixels.

Launching Real-time Threat Detection Command Center

From a supported browser, go to `https://<IP address>:443/`

Where **<IP address>** is the host name or IP address that you specified when you first configured Command Center.



Note: Host names with underscores do not work on Microsoft Internet Explorer, so use the IP address.

Logging in to Real-time Threat Detection Command Center

After you have logged in, there is a logout link in the lower left corner of the window, under the <user name> menu.

General Prerequisites

- If the Manager is using FIPS, then configure your browser to use TLS.
- If you are using FIPS and SSL, use the `keytool` command to export a client certificate for the browser machine.
- If you are not using FIPS, export certificates with the `keytoolgui` command. For more information, see the [Administrator's Guide for Real-time Threat Detection](#).

Logging in with Password Authentication

Log in with your User ID and password. Your user type controls your resource access.

Logging in with SSL Authentication

Make sure you have exported a client certificate from an ArcSight Console. Specify the certificate to use and click **OK**. When you get to the Command Center user ID and Password screen, click **Login** without specifying anything.

Logging in with Password Authentication or SSL

To log in with an SSL certificate, make sure you have exported a client certificate from an ArcSight Console machine. Specify the certificate to use, and click **OK**. When you get to the Command Center User ID and Password screen, leave the fields blank and click **Login**.

To log in with a user ID and password, click **Cancel** on the certificate dialog, then provide your user ID and password on the User ID and Password screen.



Note: If you are using Microsoft Internet Explorer, and you import a certificate, you must always use SSL (cancelling fails to load the page). If you do not import a certificate, you can only use password authentication.

Logging in with Password Authentication and SSL

Make sure you have exported a client certificate from an ArcSight Console machine. Specify the certificate to use and click **OK**. When you get to the User ID and Password screen, specify your User ID and password.



Note: While logging into a Manager that has been configured to use Password-based or SSL Client Based authentication, if you try to log in using a certificate and the login fails, all subsequent attempts to use the username/password login will also fail during the same session. To work around this, restart the browser and clear its cache.

Basic Navigation

Use the Dashboards, Channels, Resources, Administration, License, and User links at the left of the display to go to those features. Click each one to display a menu of available options.

The links in the upper right corner provide these features:

- **Dark Theme:** Changes the display from the default light to dark theme. The dark theme reduces glare from the screen, providing visual comfort in dark room environments.
- **Notifications:** Displays pending notifications.
- **Help**

Click **Help** to get context-sensitive help for the page you are viewing.

The help for those applications is accessible from the **Help** link when you view the integrated application from the **Applications** tab. Such help has its own appearance and navigation.

Hover over the **Help** link to see a list of options:

- **What's New:** Displays the online help system, open to a list of new features in this release.
- **Documentation:** Displays the main online documentation page, with a description of each book and a table of contents in the left panel.
- **Online Support:** Takes you to the online support web site in a separate window.
- **About:** Displays the current Real-time Threat Detection product version number.
- **Site Map:** Provides a mechanism to access Command Center primary landing pages using keyboard-navigation only.

Using the Site Map

The Site Map link provides a mechanism to access Real-time Threat Detection Command Center pages using keyboard-navigation only. The Site Map link opens the Site Map page which displays a list of links to the primary landing pages in the Command Center.

Monitoring Usage Metrics (Stats)

Real-time Threat Detection monitors the event data that flows through the ArcSight Manager and generates a 45-day moving median EPS (MMEPS) report that tracks the history of average EPS, average EPS per day, MMEPS, and the entitled EPS limit so that you can identify whether you are in danger of being out of compliance with the license agreement.



Note: You must be an administrator to view usage metrics.

You are considered to be in compliance with the license agreement as long as the MMEPS values remain at or below the purchased licensed capacity. You are considered to be in violation of the license agreement if three or more consecutive MMEPS values exceed the purchased license capacity.

To view the usage metrics, click **License > License Usage** in the menu bar.

The usage metrics that Real-time Threat Detection displays are a result of the following calculations:

- Events per day (EPD)

EPD is the total number of events that are generated in a 24-hour period. The 24-hour period is based on UTC time. It starts at 00:00:00 and ends at 23:59:59, regardless of local time.

EPD calculations vary according to the version of SmartConnectors in use. If the SmartConnector version is greater than 7.13.0, Real-time Threat Detection counts post-filter and pre-aggregation events from connectors. If the SmartConnector version is 7.13.0 or lower, Real-time Threat Detection counts post-filter and post-aggregation events from connectors.

- Sustained events per second (SEPS)

SEPS is the constant events per second that the system sustained within the 24-hour period. The calculation normalizes peaks and valleys and provides a better indication of usage. Real-time Threat Detection uses the following formula to calculate SEPS:

$$(EPD / ((60 * 60) * 24))$$

- 45-day moving median (MMEPS)

Real-time Threat Detection uses the SEPS calculations per day to identify the MMEPS value. Real-time Threat Detection uses a 45-day data set to calculate the median value and shifts the calculation window one day every 24 hours after the first 45 days. The 24-hour period is based on UTC time. It starts at 00:00:00 and ends at 23:59:59, regardless of local time.

Because Real-time Threat Detection does not yet have enough SEPS calculations to calculate MMEPS for the first 45 days of usage, it displays approximate MMEPS values. As the number of days increases, the approximate MMEPS becomes a more accurate indication of the actual MMEPS.

For example:

- On day 2, the MMEPS value is the SEPS value for day 1.
- On day 3, the MMEPS value is the average of the SEPS values for days 1 and 2.
- On day 4, the MMEPS value is the average of the SEPS values for days 1, 2, and 3.
- The pattern continues until day 46, when Real-time Threat Detection has 45 SEPS values for calculating the actual MMEPS.

Real-time Threat Detection displays approximate values in gray to distinguish them from actual values.

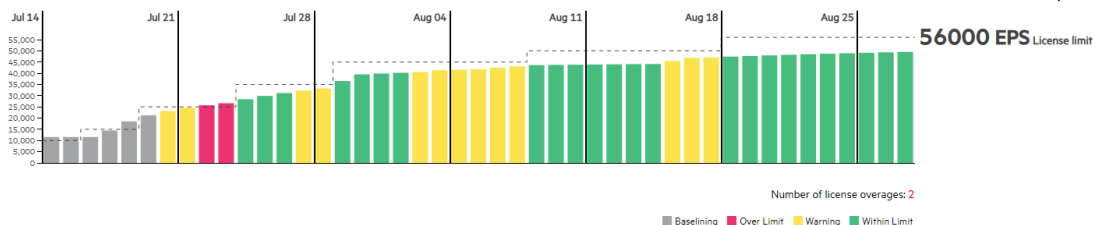
Real-time Threat Detection must be running for at least one day before it displays usage metrics. If you click **Stats** on day 0, Real-time Threat Detection generates a message that it did not receive any results from the server.

After Real-time Threat Detection begins collecting data, when you click **License Usage**, Real-time Threat Detection displays the usage metrics in a bar chart and in a table. For example:

EPS/day License Usage for Last 45 Days



Your usage exceeds its license limits. Please contact your license administrator



Date	Events Received	License Usage (MMEPS)	License Limit
Jul 01, 2019	1,000,000,000	11,574	15,000
Jul 02, 2019	1,000,000,000	11,574	15,000
Jul 03, 2019	1,000,000,000	11,574	15,000
Jul 04, 2019	2,000,000,000	14,467	15,000
Jul 05, 2019	3,000,000,000	18,518	15,000
Jul 06, 2019	3,000,000,000	21,219	25,000
Jul 07, 2019	3,000,000,000	23,148	25,000
Jul 08, 2019	3,000,000,000	24,594	25,000
Jul 09, 2019	3,000,000,000	25,720	25,000
Jul 10, 2019	3,000,000,000	26,620	25,000
Jul 11, 2019	4,000,000,000	28,408	35,000
Jul 12, 2019	4,000,000,000	29,899	35,000
Jul 13, 2019	4,000,000,000	31,160	35,000
Jul 14, 2019	4,000,000,000	32,241	35,000
Jul 15, 2019	4,000,000,000	33,178	35,000
Jul 16, 2019	7,500,000,000	36,530	45,000
Jul 17, 2019	7,500,000,000	39,487	45,000
Jul 18, 2019	4,000,000,000	39,866	45,000
Jul 19, 2019	4,000,000,000	40,204	45,000
Jul 20, 2019	4,000,000,000	40,509	45,000
Jul 21, 2019	5,000,000,000	41,335	45,000
Jul 22, 2019	4,000,000,000	41,561	45,000
Jul 23, 2019	4,000,000,000	41,767	45,000

Date	Events Received	License Usage (MMEPS)	License Limit
Jul 24, 2019	5,000,000,000	42,438	45,000
Jul 25, 2019	5,000,000,000	43,055	45,000
Jul 26, 2019	5,000,000,000	43,625	50,000
Jul 27, 2019	4,000,000,000	43,724	50,000
Jul 28, 2019	4,000,000,000	43,815	50,000
Jul 29, 2019	4,000,000,000	43,901	50,000
Jul 30, 2019	4,000,000,000	43,981	50,000
Jul 31, 2019	4,000,000,000	44,055	50,000
Aug 01, 2019	4,000,000,000	44,125	50,000
Aug 02, 2019	7,500,000,000	45,419	50,000
Aug 03, 2019	8,000,000,000	46,806	50,000
Aug 04, 2019	5,000,000,000	47,122	50,000
Aug 05, 2019	5,000,000,000	47,421	56,000
Aug 06, 2019	5,000,000,000	47,703	56,000
Aug 07, 2019	5,000,000,000	47,971	56,000
Aug 08, 2019	5,000,000,000	48,225	56,000
Aug 09, 2019	5,000,000,000	48,466	56,000
Aug 10, 2019	5,000,000,000	48,695	56,000
Aug 11, 2019	5,000,000,000	48,913	56,000
Aug 12, 2019	5,000,000,000	49,122	56,000
Aug 13, 2019	5,000,000,000	49,321	56,000
Aug 14, 2019	5,000,000,000	49,511	56,000

Because MMEPS calculations are approximate values for the first 45 days, Real-time Threat Detection does not calculate license violations during this time.

If Real-time Threat Detection calculates a license violation on a particular day and you then increase the licensed capacity, the increase does not affect the previous license violation.

Chapter 2: Viewing System Information

Real-time Threat Detection Command Center provides the Dashboard Home page and Dashboard Navigator page to allow you to view system information. Information appears in these two pages in the form of *dashlets*.

From the Dashboard Home page, you can add any available dashlets while from the Dashboard Navigator page you can view dashboards comprised of data monitor and query viewer dashlets. Unlike the Dashboard Home page, dashboards in the Dashboard Navigator page cannot be modified since they originate in the ArcSight Console.

Command Center opens in the Dashboard Home page. You can return to this page any time by clicking **Dashboards > Home**.

Managing Dashlets in the Dashboard Home Page

The Dashboard Home page is where you monitor your workflow. You can customize the Dashboard Home page by adding or removing any available system-monitoring and workflow-based dashlets.

The dashlets provide the following types of information:

- Workflow information:
 - My Dashboards
 - My Notifications
- System information:
 - Data Monitor
 - Query Viewer
- MITRE ATT&CK information:
 - Last MITRE ATT&CK Events
 - MITRE by Tactic
 - Top 10 Attackers
 - Top 10 Targets
 - Last 10 Attacks and Suspicious Activity Events
 - Top Indicator Type in Suspicious Address

By default, a new installation displays the following dashlets;

- Last MITRE ATT&CK Events
- MITRE by Tactic
- Top 10 Attackers

- Top 10 Targets
- Last 10 Attacks and Suspicious Activity Events
- Top Indicator Type in Suspicious Address

Adding a Data Monitor Dashlet to the Dashboards Page

About:

A data monitor dashlet can display information for events, rules, and other types of information.



Note: You can customize the look of a data monitor and query viewer dashlets in the Dashboard Navigator page (see "[Managing Dashboards in the Dashboard Navigator Page](#)" on page 17).

Prerequisite:

- Create one or more data monitors in ArcSight Console.

Procedure:

Location: Dashboards > Home

1. Click **Add Content**.
2. From the Add Content to Home popup, select **Data Monitors**.
3. Navigate to the data monitor folder containing the desired data monitor.
4. Select the desired data monitor in the Name column and then click **Add Content**.
5. Add any additional data monitors and then close the popup.
6. To change a data monitor view, make a selection from the available drop-down in the data monitor title bar.



Note: Not all chart options that are supported in the ArcSight Console are available in the Command Center.

More:

- Available data monitor views vary based on the data monitor type.

See Also:

[ArcSight Console User's Guide](#)

Adding My Dashboards to the Dashboard Home Page

About:

Dashboards display data gathered from data monitors or query viewers. Dashboards can display data in a number of formats, including pie charts, bar charts, line charts, and tables, and you can rearrange and save the dashboard element display. You can edit the existing dashboards and create new ones from the ArcSight Console.

Procedure:

Location: Dashboards > Home

1. Click **Add Content**.
2. From the Add Content to Home popup, select **Dashboards** and then click **Add Content**.
Command Center displays the list of dashboards that are in your personal folder.

More:

- You can also see the list of dashboards under **Dashboards > Navigator**, along with all the other dashboards.
- Use the ArcSight Console to create dashboards under your personal folder.
- The link in the My Dashboards widget title bar opens the Dashboard Navigator where you can see the list of dashboards created in the ArcSight Console. This is the same as selecting **Dashboards > Navigator**.
- If you would like to add another dashboard to your personal folder, go to the ArcSight Console and drag it into your folder.
- Access Recon from a dashboard by clicking on a field name and selecting **Recon**. The fields that enable this access must be supported Recon fields. Not all Real-time Threat Detection fields are supported for search in Recon. These unsupported fields are disabled for selection in a Recon search.



Note: The Target Address and Attacker Address fields have no Recon option.

If the field you are searching is empty, the Recon popup automatically uses "=", 'None' as the search condition. For example, for an empty deviceVendor field, the search statement in Recon is

```
deviceVendor "=", 'None'
```

See Also:

- [Viewing System Information](#)
- [ArcSight Console User's Guide](#)

Rearrange Real-time Threat Detection Command Center Dashboard If Charts and Tables Overlap

In some cases, data monitors and query viewers on the dashboard will overlap. When this happens, switch to tab view. You can also edit the dashboard in the ArcSight Console as follows:

1. Log in to the ArcSight Console and display the dashboard.
2. Click the blue arrow at the bottom right corner of the dashboard and select **Tile Best Fit**.
3. Save the dashboard and exit the Console.

Adding My Notifications to the Dashboards Home Page

About:

Notifications and their content are created using rules configured with the Send Notification rule action. Notifications come in the form of pending, undelivered, acknowledged, not acknowledged, resolved, and informational.

Procedure:

Location: Dashboards > Home

1. Click **Add Content**.
2. From the Add Content to Home popup, select **My Notifications** and then click **Add Content**.

Command Center displays the list of notifications that are in your personal folder.

More:

- The link in the My Notifications dashlet title bar opens the Notifications page where all the notifications are listed.
- You can also click the Notifications button in the upper right corner to open the Notifications page. The number of pending notifications are indicated within a red circle.

- By default, the My Notifications dashlet is filtered by the Pending, Acknowledged and Resolved statuses of the Notifications page.
- From the Notifications page you can:
 - Adjust the filter that controls which notifications appear
 - Acknowledge notifications
 - Mark notifications as resolved
 - Delete notifications
- Notifications are configured in the ArcSight Console. For more information, see the [ArcSight Console User's Guide](#).

Adding a Query Viewer to the Dashboards Home Page

About:

A query viewer is a resource for defining and running SQL queries on other resources, such as assets, connectors, and events. Each query viewer contains a SQL query along with other logic for establishing and comparing baseline results, analyzing historical data to find patterns in network activity, and performing drill-down investigations on a particular aspect of the results. Query viewers are defined in the ArcSight Console.

Procedure:

Location: Dashboards > Home

1. Click **Add Content**.
2. From the Add Content to Home popup, select **Query Viewers**.
3. Navigate to the query viewer folder containing the desired query viewer.
4. Select the desired query viewer in the Name column and then click **Add Content**.
5. Add any additional query viewers and then close the popup.

More:

Query viewers use specific types of queries, and some are not supported. Depending on the query used, not all query viewers are displayed.

Query viewers are available in the Command Center in tabular and chart formats. For charts, the x and y axes display only aggregated fields (such as count).

Query viewers displaying bar charts support only aggregated fields in the bar chart's y-axis and z-axis.

See Also:

[ArcSight Console User's Guide](#)

Changing the Dashboards Layout

About:

Dashlets can appear in either one, two, or three columns.

Procedure:

Location: Dashboards > Home

- Click **Change Layout** and specify the number of columns to display.

More:

- You can reposition widgets using drag and drop.

Managing Dashboards in the Dashboard Navigator Page

About:

The Dashboard Navigator page is where you can access ArcSight Console dashboards and view the data monitor and query viewer dashlets for each dashboard. It displays the information view that is shown in the ArcSight Console. This information is in view-only mode.

See Also:

[ArcSight Console User's Guide](#)

Viewing Dashboards in the Dashboard Navigator

About:

From the Dashboard Navigator, you can view dashboard information based on that in the ArcSight Console. The Dashboard Navigator displays the ArcSight Console view as much as

possible. You will be prompted to refresh your Dashboard Navigator view if there are changes to resources on the ArcSight Console.



Note: If a resource changes on the ArcSight Console that you are displaying in the Command Center Dashboard Navigator page, you will have to refresh your view of the Dashboard Navigator to be able to see the changes.

Prerequisite:

- Create one or more data monitors or query viewers in ArcSight Console in a dashboard.
For more information, see the [ArcSight Console User's Guide](#).

Procedure:

Location: Dashboard menu > Navigator > Dashboard - list screen > resource tree

1. Click **Dashboard > Navigator**.
2. Expand the dashboard folder in the resource tree and then click the desired folder.

Dashboards associated with the folder appear in a table in the center of the screen, as seen in the following example of dashboards listed in the navigator. Click

[Configure Columns...](#)

to change the columns in the table listing the dashboards. Click



Refresh

to update the dashboard data.

Dashboards

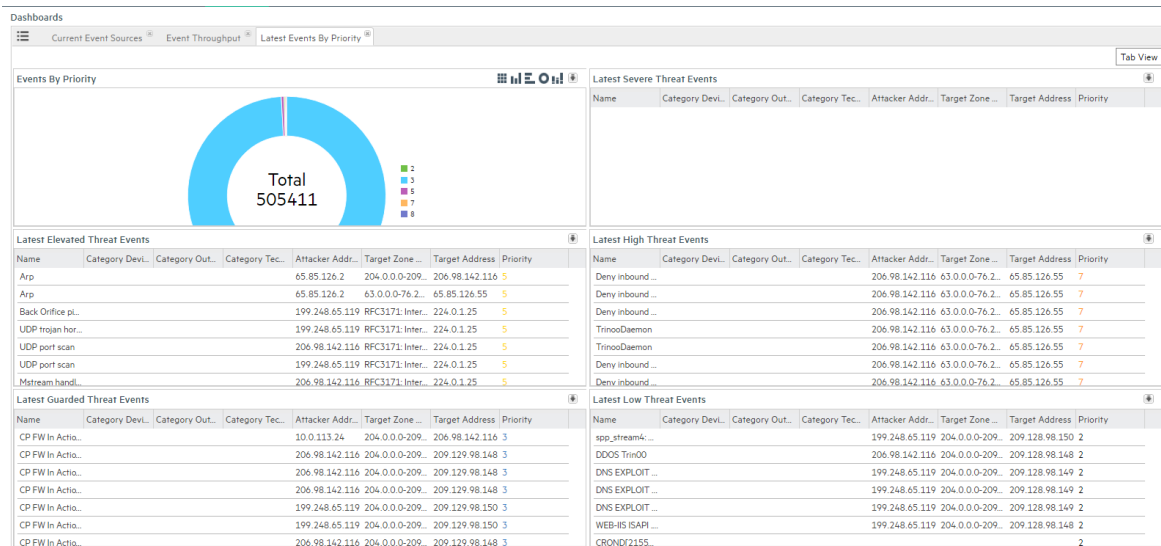
Display Name ▲	Last Update Time
Connector Connection and Cac...	2016 August 9, Tuesday 22:28:57 UTC-7
Current Event Sources	2016 August 9, Tuesday 22:28:57 UTC-7

3. Click the **Display Name** link for the desired dashboard.

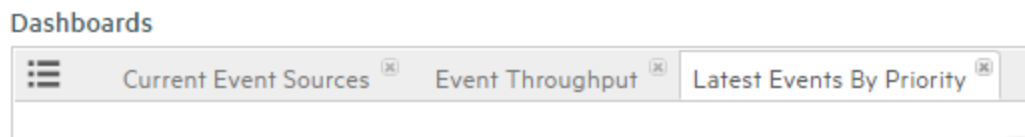
The dashboard screen for the selected dashboard opens, displaying dashlets the events for the dashboard. For example:

User's Guide

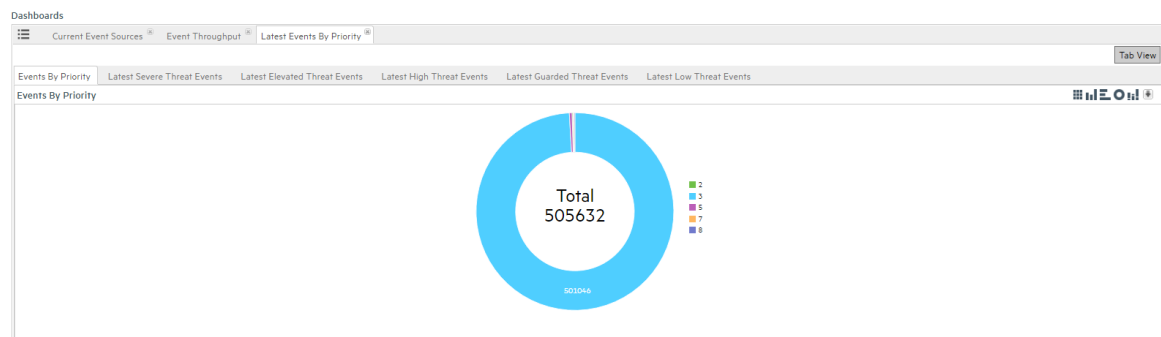
Chapter 2: Viewing System Information



4. If you have multiple dashboards open, these will appear in tabs, as seen in the following example.



Click **Tab View** to change the dashboard view to show dashlets in individual tabs, as shown in the following example. You can click the various tabs to view each tab.



Click **Tab View** to change back to the tiled view of the dashboards.

Navigate from a Dashboard to a Channel in a Data Monitor

Procedure:

1. Add a data monitor, per steps in ["Adding a Data Monitor Dashlet to the Dashboards Page" on page 13](#)

2. In a dashboard data monitor dashlet, right-click in a data display (for example, right-click in a segment of a pie chart).
3. Select **Create Channel**, and enter a name for the channel. This will create and display a temporary channel.
4. Click **Save As** to save the channel as a resource that you can access again.

Note: Some data monitors do not support navigation directly to a channel. These are:

- Asset Category Count
- Event Correlation
- System Monitor
- System Monitor Attribute
- Rules Partial Match

Also, some of fields are not supported for drilldown. These include:

- Data Viewer fields
- Aggregated fields

Specifying a Dashlet Chart Type

About:

Command Center enables you to specify the dashlet chart type.

Procedure:

Location: Dashboards > Navigator

1. In the upper right corner of the dashboard page dashlet, select a chart type from the icon choices. The chart type currently displayed is highlighted in green.
2. Click the icon again to change the chart type, or return to the original view of a chart.

More:

The available view options vary based on the dashlet type, and other selections made when it was created in the ArcSight Console. They might show different kinds of charts, if the data monitor can be displayed in those formats. Below are the possible data presentation formats.

Dashlet Types

Display Format	Description
Bar Chart	<p>Shows data as a series of proportional bar elements and may include bar segmentation to subdivide the data.</p> <p>Applies to data monitors and query viewers.</p>
Horizontal Bar Chart	<p>Shows data as a series of proportional bar elements and may include bar segmentation to subdivide the data. This format forces the bars to run left-to-right rather than up-and-down.</p> <p>Applies to data monitors and query viewers.</p>
Pie Chart or Donut Chart	<p>Shows data as a circle with proportional wedges for elements and a hole in the middle.</p> <p>Applies to data monitors and query viewers.</p>
Statistics Chart	<p>Overlays Moving Average data graphs on a data monitor, when multiple graphs are present. Compare this display format to the Tiles format, which arranges individual-graph monitors into fixed arrays.</p> <p>Applies to data monitors.</p>
Table	<p>Displays data as a grid.</p> <p>Applies to data monitors and query viewers.</p>
Stacking Bar Chart	<p>Shows data from a query viewer as a series of proportional bar elements and may include bar segmentation to subdivide the data.</p>
Geographical Event Map	<p>Shows a map of the world with lines connecting the origin and destination of each event. You can zoom in and hover over individual events for details.</p> <p>Applies to geographical event graphs.</p>
Event Graph	<p>Displays the event endpoints like nodes on a spider web. You can hover over individual events endpoints for details.</p>
Topology Graph	<p>A variation of the Event Graph that displays event endpoints in relation to each other, in terms of Source Nodes, Event Nodes, and Target Nodes. This graph allows you to explore the relationships and connections among the nodes. Hover over a node to highlight that node's connections. Click individual nodes to drill down and explore the relationships among the nodes.</p> <p>You can pause auto-refresh so that data will stop updating and remain stable during an investigation. Click play to restart data update.</p> <p>Right-click on any individual node to copy node information to the clipboard; you can use this data later in filter, or for another purpose.</p> <p>Note: You can configure a display limit for Event Graphs in the ArcSight Console. Depending on your monitor size, you might have to adjust this value to yield usable data in the Topology Graph view.</p>

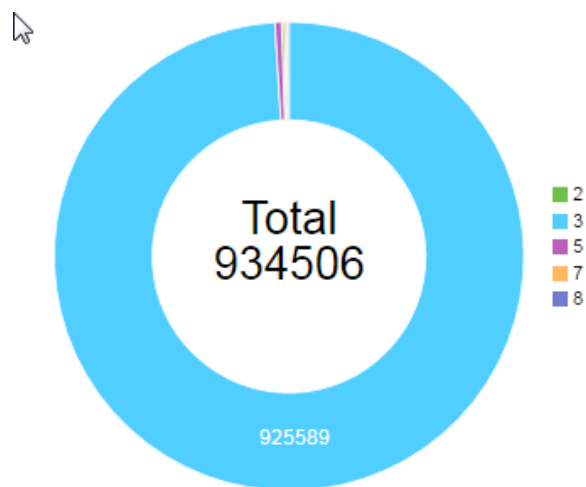
Points to consider:

- Charts may appear differently in the Command Center than they do in the ArcSight Console. The default chart view in the Command Center is the bar chart.

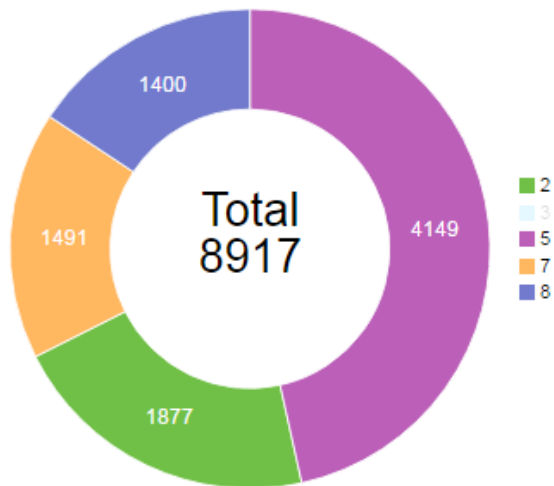
- Not all chart options are available in the Command Center that are supported in the ArcSight Console. For example, the 3D bar chart is not available in the Command Center, and a regular bar chart will display instead.
- In the Command Center, the display limit for all charts is 20 entries. The grid view limit is 1000.
- Charts in the Command Center Dashboard navigator provide a view of charts, but do not allow drilldown into the data; this is provided in the ArcSight Console.
- If you refresh the Dashboard Navigator view when displaying several dashboards, the refreshed view will subsequently display the last dashboard viewed.
- You can use your browser's bookmark capability to bookmark a dashboard view. Use the bookmark to log in and the bookmarked view will display.
- Right-click and copy is not available in Topology Graphs.
- For Topology Graphs, if the source node and attacker node are the same node, the source and attacker nodes in this case are shown as separate nodes in the graph (are not depicted as one node).

Tip: You can click an entry in a chart to filter data.

For example, in this chart:



If you click on the entry labeled 3, this is the result:



The data you choose is filtered out. Click again to turn the filter off and the filtered data is again considered in the chart. This filtering persists only for the current session.

See Also:

ArcSight Console User's Guide: [Using Dashboards](#)


Downloading a Dashlet to a CSV File

About:

From a data monitor or query viewer dashlet, Command Center enables you to save dashlet data to a CSV file.

Procedure:

Location: Dashboards > Navigator

1. In the data monitor or query viewer dashlet, click the  icon.
2. Follow any further prompts to save the data to a CSV file.



Note: The Safari browser blocks popups by default, and does not give notification that it does so. You must enable popups in Safari for them to function.

Viewing Details for Events in a Last N Events Data Monitor

About:

View event details for an event listed in a Last N Events data monitor.

Procedure:

1. Open the desired dashboard that includes a Last N Events data monitor.
2. Click an event row in the table.
3. Click the view details icon (magnifying glass).
4. View details in the **Event Details** popup.

From the **Event Tree**, select the desired event if multiple are present.

The **Details** tab of the Event Details popup shows attribute details related to the selected event. You can also access **Annotation History** and **Payload**.

5. To filter event information based on fields, use the **Show Fields Containing** field.
6. To filter event information by field set, specify the desired field-set field.
 - a. Click the **Field Set** drop-down.
 - b. From the Please Select a Field Set popup, select the desired field set and then the desired field.

The field set appears in the Selected Resource list.

You can select only one field set.

- c. Click **OK**.

To clear the field-set filter, open the field set selector popup again and click the left arrow button. The selected field returns to the Name list.

7. To hide and show empty attribute rows, click **Hide Empty Rows**.

Using the Cluster View Dashboard

About:

This dashboard provides a visual map of your cluster configuration, EPS, available node services, connections, and cluster audit events. The cluster is made up of nodes that represent systems on which the cluster services run. This dashboard applies only to systems running Real-time Threat Detection in distributed mode.

Procedure:

Location: Dashboards > Cluster View

The screen displays these sections: **Distributed Correlation Stats**, **Cluster**, and a list of audit events, either **Live View of Audit Events** (default view) or **Backpressure History**.

Users in the Analyzer Administrators group can access all the widgets on the dashboard by default. All other users in non-administrator groups need read access to the following resource groups

- /All Data Monitors/ArcSight Foundation/ArcSight ClusterView
- /All Filters/ArcSight Administration/Detect/Distributed Correlation Monitoring
- /All Fields/ArcSight Administration/Detect/Distributed Correlation Monitoring

Distributed Correlation Stats

Distributed Correlation Stats shows a representation of the cluster nodes that are part of the distributed correlation cluster and the various services (persistor, aggregator, correlator, message bus data, message bus control, information repository, or distributed cache) that are running on each node. The diagram shows the instance ID for each service instance.

The node representation starts with **Cluster**, and branches to nodes (represented by system hostname or IP address), and finally to individual instances of services (such as *aggregator2* or *repo3*). Double-click on the node to contract it and hide the associated services and change your view; double-click again to expand the node.

Click on each service to see details. Details vary depending on the service.

The status of the services is color-coded. Turn on the **Legend** for color code and icon definitions.

The service statuses are:

- Initializing
- Available
- Shutting down
- Unavailable
- Warning
- Unresponsive
- Unknown
- Host
- Host with Persistor



Tip: The Legend button is in the far upper right corner of the window. You might have to scroll all the way down and to the right to see it.



Note: The Persistor node has the instance ID *manager*.

Cluster

Cluster shows **Metrics**, **Services Configured** , and **Backpressure**.

Metrics displayed are:

- **EPS** – incoming EPS to the Manager.
- **Lag Aggregator** – Messages remaining in the message bus for the aggregator to consume.
- **Lag Correlator** – Events remaining in the message bus for the correlator to consume.
- **GB/Day** – incoming GB/day.



Note: Lag is shown as a metric on this dashboard. Lag indicates items waiting to be processed. The lag numbers shown for correlators are for events per second (EPS). Those shown for aggregators are messages per second.

View Audit Events shows the Live View of Audit Events, described below under "[Audit Event Lists](#)" on page 28.

Services Configured is a summary of the total correlator and aggregator services configured for the cluster. The count should match those on the cluster topology graph. It also indicates if the services are running (**Active**) or (**Stopped**)

Backpressure enables you to control lag by throttling the EPS, based on acceptable lag, to regulate event flow. It allows you to control the flow of events when there are more events

than the system can process. While backpressure is on, excess events are cached on the connector. When backpressure is off, event flow resumes.

- **Backpressure Mode:**

- **Auto:** (automatic backpressure) is based on the value of Acceptable Lag. Backpressure is turned on and off automatically to limit Estimated Lag to be less than Acceptable Lag. Given the dynamic nature of message consumption and message publishing rates, and also latency in lag monitoring, the system cannot guarantee that Estimated Lag is never more than the given value of Acceptable Lag. The system can only make a best effort.

Auto is the default setting for the backpressure mode, and is recommended. Auto is overridden by **On** or **Off**, which you can use to toggle user backpressure:

- **On:** Stops all events. Events already accepted are processed and internal queues are cleared. Use rarely if lag becomes too high and you need to temporarily stop event flow to allow Real-time Threat Detection to catch up.
- **Off:** Admits all events regardless of the specified Acceptable Lag. This option is no longer available to select.

- **Event Flow:** **ON** indicates that events are flowing. **OFF** indicates events are stopped.

- **Acceptable Lag:** Use this value to provide a threshold for enabling backpressure. Values for Acceptable Lag can be a number between 30 and 86400 (in seconds). Default is 180.

To modify the Acceptable Lag value, click the edit icon (pencil). Enter the value and click **OK**.

- **Estimated Lag:** Calculated estimate based on EPS.

Click **View History** to show **Backpressure History**, described below under "[Audit Event Lists](#)" on the next page.

Details and Metrics for Individual Services

Click on the representation of an individual instance of a service in the Distributed Correlation Stats to view details and metrics for that service instance. Hover the mouse over the detail or metric for a tool tip definition.

Details for each service include:

- Hostname:Port
- ID
- CPU percentage
- Heap memory usage percentage

The manager service includes **Health Check** information on connections to message bus and distributed cache.

Metrics available, by service instance:

Service Instance	Metrics
manager (persistor)	<ul style="list-style-type: none">• EPS In• EPS Out• ca-to-p-events Topic Lag
aggregator	<ul style="list-style-type: none">• MPS In• MPS Out• c-to-a-dm Topic Lag• c-to-a-rule Topic Lag
correlator	<ul style="list-style-type: none">• EPS In• MPS Out• p-to-c-events Topic Lag
message bus data (mbus_data)	Not applicable
message bus control (mbus_control)	Latency
distributed cache (dcache)	<ul style="list-style-type: none">• Uptime• Collected at
information repository (repo)	Latency

Audit Event Lists

Live View of Audit Events is updated every 15 minutes. This is the default view of audit events. The changing status of the cluster nodes and services generate audit events, which are displayed in the bottom right of the dashboard. For details about audit events, see the [ArcSight Console User's Guide](#). This data displays for the entire cluster, or for individual instances of aggregators and correlators, or for the persistor (manager).

Backpressure History lists the **Date**, **Status**, and **Reason** for a change in backpressure. When the status is **Off**, this indicates that the condition that triggered backpressure no longer exists and that backpressure is disabled. A status of **On** indicates that conditions have triggered backpressure. **Reason** entries allow you to see why the status changed, and the entries listed are linked to message bus topics (ca-to-p, p-to-c, or c-to-a).

Using the MITRE Dashboard

MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

Many companies are starting to use MITRE as the go-to source of classifying various types of adversary behaviors. MITRE have developed both a periodic table and a radial chart to show the linkage between a specific adversary behavior and the subsystem.

Command Center has developed the same view to show:

- How ArcSight content relates to the MITRE ATT&CK table and chart.
- The actual findings as they occur in the field, as Real-time Threat Detection identifies vulnerabilities from systems.

The MITRE Dashboard provides you with an immediately recognizable frame of reference, allowing you to view the activity based on Real-time Threat Detection content for the MITRE ATT&CK matrix and identify security gaps.

During the installation process, the administrator determines the type of information the MITRE Dashboard displays by choosing one or both of the following feeds:

- **Security Threat Monitoring** - default security content across the Defense in Depth (DiD) layer.
- **Threat Intelligence Platform** - content which works with the MISP Threat Intelligence feed.

The installation also add the following active lists to the MITRE Dashboard:

- **MITRE ATT&CK List** - contains MITRE ATT&CK information which includes MITRE Technique ID, MITRE Technique Name and Tactic.
- **Rules Triggered with MITRE ID** - stores MITRE ATT&CK information from correlation rules, populated with correlation events which captured by the "Track Rules with Mitre ID" rule.

To view the MITRE Dashboard, go to **Dashboards > MITRE**.

For more information about active lists, see the [ArcSight Console User's Guide](#).

The MITRE Dashboard provides the following views:

- MITRE Activity
- MITRE Coverage

MITRE Activity

The MITRE Activity view displays a visualization based on how many tactics and techniques the “Rules Triggered with MITRE ID” list has observed over the last two days.

To see more information about an attack, click a technique. Each technique links to the MITRE website, and displays the following information:

- Details for that technique, including the associated Tactic ID
- The rule that observed the attack
- The day the rule observed the attack

You can inspect a rule by clicking it, which opens a filtered channel specifically for that rule.

MITRE Coverage

The MITRE Coverage view is a customizable matrix that allows you to view one or more of the following:

- Attacks identified in the last 2 days
- Technique actively monitored
- Coverage installed but not enabled
- No coverage installed

By default, the MITRE Coverage view displays all available information. Use the checkboxes to display specific information.

Chapter 3: Monitoring Events Through Active Channels

Real-time Threat Detection Command Center recognizes event channels. You can create, edit, or delete active channels (event channels).

Also, you can copy a channel (create a new channel with the same properties as a selected channel), and refresh the channel view to get the latest data.

- Command Center provides the following channel and event functionality:

Channel creation, editing, deleting: Event channels can be newly created with empty attributes or created from an existing active channel. Channel attributes can be edited. You can change the name, start time, end time, timestamp displayed, time evaluation type, the configured filter, and the configured field set. You can also delete channels.

Channel filtering: Event channels can be filtered using conditions based on fields, assets, and vulnerabilities.

Condition Summary: Performs like a channel filter, where a raw string represents the conditions for the channel. This summary displays the filter conditions defined for a channel.

Header: Each active channel has a header section containing several features you can use to understand the channel and manipulate associated event information.

Radar display: The radar consists of a bar chart overview of events on the active channel. It is divided into time segments sorted by event end time, each segment representing groups of events with the same end time.

- To use event channels

Priority statistics: Rating events of a channel based on their priority.

Annotation: Annotating an event and viewing event annotation history

Payload summary: An event payload is the information carried in the body of the event's network packet.

Reviewed flag: Mark an event as reviewed, which can be helpful in the investigation process.

Graphical visualization: Through the use of widgets, you can view field information for events. You can choose the type of field information to display and the range of events for which this information should appear.

Event search: Search for events from the **Events** menu. See [Searching for Events in the Real-time Threat Detection Command Center](#).

Viewing Events On an Active Channel

About:

Viewing events on an active channel is done from the active channel screen. From this screen, you can also view related event information and perform functions using events.



Note:

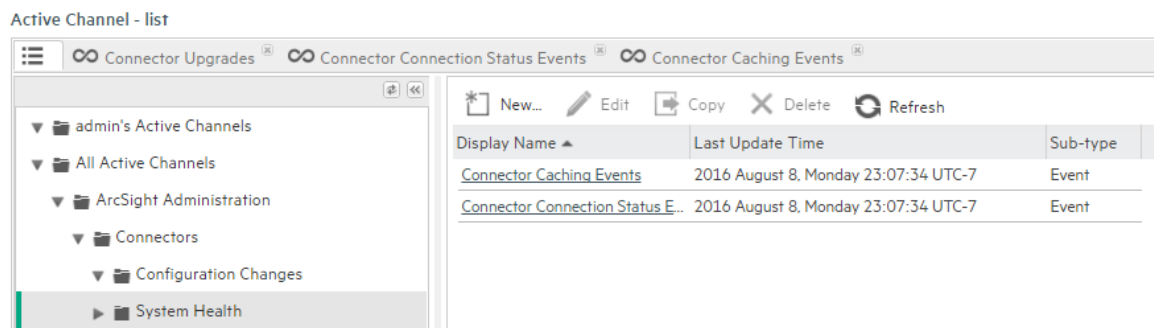
- Some channels in Command Center may not be current when accessed in a new Real-time Threat Detection session. To ensure current event information, refresh the channel by clicking the stop and play buttons.
- If an active channel is open when Daylight Savings Time goes into or out of effect, the active channel will not reflect the correct start and end times until the channel is closed and re-opened.
- The Country Flag URL is not displayed in active channel information for the Geo Active Channel in the Command Center, but is displayed in the ArcSight Console.

Procedure:

Location: Channels > Active Channels > Active Channel - list screen > resource tree

1. Click **Channels > Active Channels**.
2. Expand the appropriate active channel folder in the resource tree and then click the desired folder.

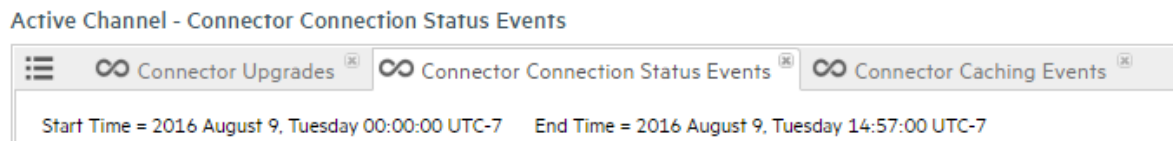
Channels associated with the folder appear in a table in the center of the screen, as seen in the following example of active channels.



3. Click the **Display Name** link for the desired channel.

The Active Channel screen for the selected channel opens, displaying all the events for the channel in the **Event List** tab. This is commonly known as the channel grid view.

If you have multiple channels open, these will appear in tabs, as seen in the following typical view open channel tabs.



4. To add a specific field to the channel grid view, choose **Customize > Fields**.
 - From the Select popup, select the desired field from the appropriate field set.

The Selected Fields list contains the fields that comprise the columns in the channel grid view. You can click the left arrow button (←) to remove any of these fields.

Use the up and down arrows in the Selected Fields list to sort the columns and control the order in which the columns are displayed in the grid.
 - Click **OK**.

The selected field appears as a column in the channel grid view, after the original columns.
5. To add the fields of a field set to the channel grid view, choose **Customize > Field Set**.
 - From the Select popup, select the desired field set.

The Selected Fields list contains the fields that comprise the columns in the channel grid view. You can click the left arrow button (←) to remove any of these fields.
 - Click **OK**.

The fields appear as columns in the channel grid view, after the original columns.

Columns for the channel grid view are originally specified during the creation or edit of a channel (see ["Specifying Columns For the Active Channel Event List" on page 49](#)).

**Note:**

- Some channels can be resource intensive, such as those with a time range of an hour or so. If a channel takes long to load in a high-traffic environment, open this channels in the ArcSight Console. To view a resource- intensive channel in Real- time Threat Detection Command Center, narrow the time range to 5 - 10 minutes to reduce the event volume.
- For optimum performance, limit open channels to 3 per browser, though Real-time Threat Detection Command Center can support up to 10 moderate-traffic channels or up to 15 light-traffic channels per browser. Between Real-time Threat Detection Command Center and ArcSight Console, Real-time Threat Detection can support up to 25 open channels.
- Real-time Threat Detection Command Center does not support custom columns in the Event List (Channels > Active Channels > Active Channel - list). If the channel has Custom Columns configured in Console, these will not appear in Command Center.

Viewing a Channel Condition Summary

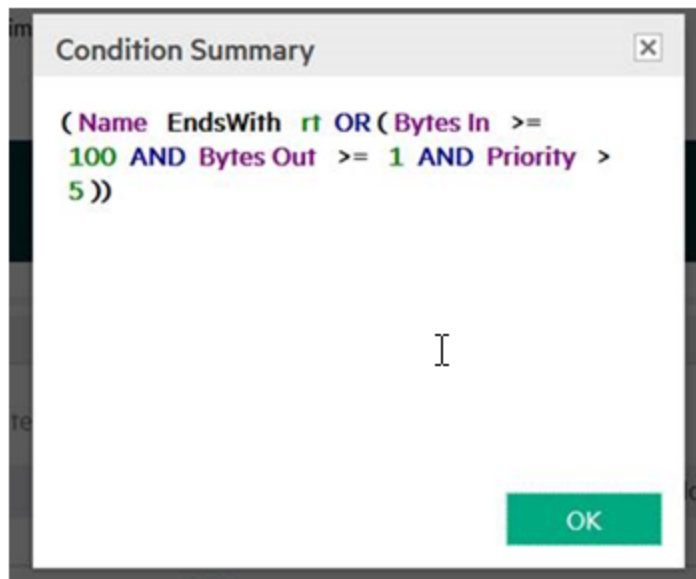
About:

A channel condition summary displays in a raw string represents the filter conditions for the channel. The syntax is slightly different than that displayed in **Configure Filter > Operations > Summary** when editing a channel or creating a new channel. However, the attributes and logic are the same.

Procedure:

1. Open the desired channel.
See ["Viewing Events On an Active Channel" on page 32](#).
2. From the Active Channel screen, click **Condition Summary**.
3. From the Condition Summary popup, view the condition statements of the active channel.

Example of an active channel condition summary



The Condition Summary provides a read-only view of the channel condition so that you can verify the syntax of the operators and their operands. For more information, see the [ArcSight Console User's Guide](#).

Access ArcSight Console to change any filter conditions.

Viewing the Event Priority for a Channel

During the normalization process, the SmartConnector collects data about the level of danger associated with a particular event, as interpreted by the data source that reported the event to the connector.

Command Center normalizes the various event-rating scales into the default scale of *Very Low*, *Low*, *Medium*, *High*, and *Very High*. An event can also be classified as *Unknown* if the data source does not provide a priority rating.

For additional details, see the [ArcSight Console User's Guide](#).

1. Open the desired channel.

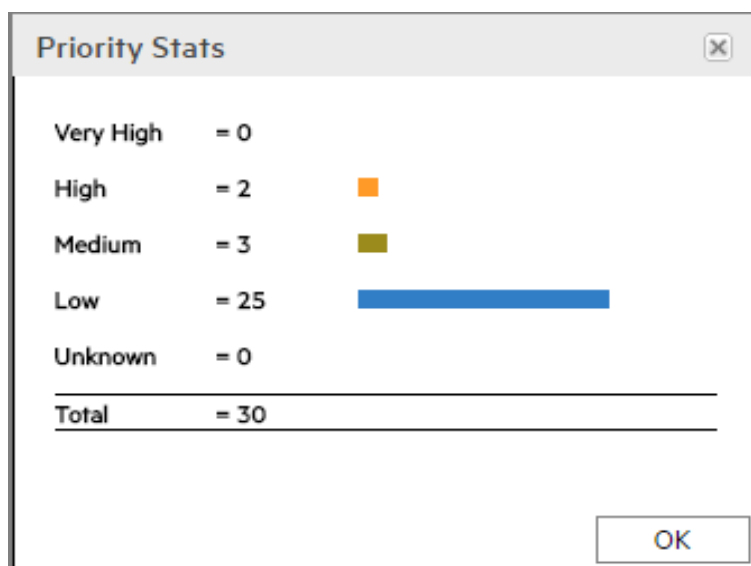
See "[Viewing Events On an Active Channel](#)" on page 32.

2. Click **Priority Stats**.

The Priority Stats popup opens, displaying the total number of events that are in each priority scale.

The bar colors in the popup match the corresponding bars of the event rows and radar display.

Example of a view of the Priority Stats popup



Evaluate the Network Route of an Event in a Channel

About:

Command Center Tool Commands enable you to evaluate the connections on the network used by a event in a channel.

Tool Commands are in a zip file included in the installation package. Unzip this file in a folder on the product server or some other server. The Tool Commands utilities are supported on the same platforms that ArcSight Console is supported. For supported platforms, see "Understanding the Technical Requirements" in the [Quick Start for Administrators Guide](#).

Traceroute: Shows the path from Command Center to the IP address of the selected channel event, reporting the IP addresses of all routers in between.

Ping: Determines whether the IP address of a channel event is active. Tests and debugs a network by sending a packet and waiting for a response.

Nmap (Network Mapper): This security scanner discovers hosts and services on a network, thus creating a "map" of the network. To accomplish its goal, Nmap sends special packets to the target host and then analyzes the responses.

Prerequisite:

Check to see that the nmap utility is installed on the client. Open a terminal or command window and type:
`nmap --version.`

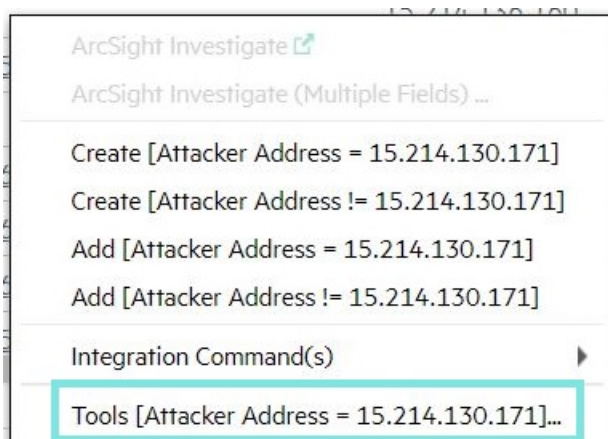
If nmap is installed, the version will be returned. If you get an error indicating that the command is not recognized, download and install the nmap binary from <http://nmap.org>.

Procedure:

1. Open the desired channel and view the associated events.
See ["Viewing Events On an Active Channel" on page 32](#).
2. From the Active Channel screen > Event List tab, click the desired event link.
For easier selection, click the pause button to freeze the Event List.



3. Identify an event, click on any field that contains an IP Address (such as Target Address, Destination Address), and then select **Tools** from the extended menu. A popup displays the **Tools** option.



4. Click **Tools**. From the Tools popup, click **Download Tools Command Webapp**.
You will be taken to `[[[Undefined variable _ARSTc_Variables.NewDownloadCenter]]]`.
5. Enter your `[[[Undefined variable _ARSTc_Variables.NewDownloadCenter]]]` login credentials.
If you do not have these credentials, contact Support.
If the download page does not display, go to <https://marketplace.microfocus.com/argsight/content/tool-commands-web-app> and locate the ArcSight Tools Command Web App download link for your specific operating system, and download the file to your local system. Unpack the file (either unzip or untar).
6. Change these default property values of the self-signed certificate in the `config.properties` file:
`ping.app.hostname=localhost`
`ping.app.port=3000`
The authentication certificate is valid for ten years.
7. If you are on a Linux and Mac system, give root user execute permissions on the node directory.
`chmod +x node`

On MAC OS steps to enable root user account:

```
% dsenableroot
username = Paul
user password:
root password:
verify root password:
dsenableroot:: ***Successfully enabled root user.
```

On MAC OS steps to disable root user account:

```
% dsenableroot -d
username = Paul
user password:
dsenableroot:: ***Successfully disabled root user.
```

8. Start the Web App by running the command:

```
<download directory>/node app.js
```

9. If using Internet Explorer Microsoft Edge, see the following **Note** section for browser configuration details.

Otherwise, to test the Webapp, you must run the Webapp on the web browser. Enter the URL from the configure.properties file (<https://localhost:3000>) in a web browser, ensure to reach the Tools Command page. You might need to rerun `node app.js` and start a new browser session afterward.

10. Specify the URL of the Tools Command panel and then click **Set**.

The URL is the one you specified in the config.properties file (<https://localhost:3000>).

11. Select the desired tool command or commands and then click **Run**.

The panel contains the results of the tool command. The panel displays within a tab by the same name as the tool command.




Note: If your operating system does not provide Nmap, then download the utility.

12. To change the URL of the tool command panel, click the gear icon, re-enter the URL, and then click **Set**.
13. To copy the contents of the tool command panel, click **Select All** in the tool command tab (or select the text manually), and then copy and paste the content into the destination.

Note:

If you are using the Tool Commands utility with Internet Explorer or Microsoft Edge and get the error "Content was blocked because it was not signed by a valid security certificate", perform

these steps to clear the error:

1. In Internet Explorer, go to Internet options > Security Tab > Trusted Sites > Sites button.
2. In the Trusted Sites dialog, add the Tool Commands URL to the list Websites (Add button), then click **Close**.
3. Click **OK** to close the Internet Options dialog.
4. Open the Tool Commands URL in a separate tab. When prompted, click "Continue to this website".
5. Click on the Certificate Error icon in the browser address bar, then select View Certificates.
A screenshot of a browser address bar showing a red 'X' icon with the text 'Certificate ...' next to it.
6. In the Certificate dialog > General tab, click the Install Certificate button.
7. In Certificate Import Wizard, navigate to Next > Place all certificates in the following store > Trusted Root Certification Authorities folder, and then click **OK**.
8. In the Security Warning dialog, click **Yes**. Close any open dialogs and return to Internet Explorer by clicking **OK**.
9. In Internet Explorer, click Tools > Internet options. The Internet Options dialog opens.
10. Go to Advanced Tab and scroll to the end of the Settings list.
11. Uncheck the "Warn about certificate address mismatch*" setting, then click **OK**.
12. In Internet Explorer, reload the page to check the result. You should see the Tool Commands Utility.

Accessing Integration Commands from an Event List

You can access Integration Commands from event links in the Event List. Integration Commands are defined in the ArcSight Console.

Procedure:

1. Open the desired channel and view the associated events.
See ["Viewing Events On an Active Channel" on page 32](#).
2. From the Active Channel screen > Event List tab, click the desired event link.
3. Select **Integration Command > <command>**.

Note these limitations:

- Only Integration Commands of type URL are supported; when executed, the command URL is launched in tab or new window based on browser preferences.

- The ability to save parameters to a user or a target is not supported in the context of the Integration Commands.

Accessing Recon or Recon Search from an Event List

You can access Recon event links in the Event List. See the Recon documentation for details.



Note: Be sure to have pop ups enabled for your browser. Recon opens in a separate browser window.

Accessing Recon

The fields that enable Recon access must be supported Recon fields.

Procedure:

1. Open an active channel.
See "[Viewing Events On an Active Channel](#)" on page 32.
2. Right-click an event, select Integration Commands, and select Recon Search.
3. Click Recon Search (Single Field.)

The Recon browser window opens for single field search.

Or

1. Click Recon (Multiple Fields.)
The Recon pane opens and displays a list of supported fields for the search.
The list is based on the columns available in the channel.



Tip: Users may enter the field name in Search Fields, instead of scrolling through the list. Enter the first few characters until the full name is displayed.

2. Drag and drop the fields from the Available Fields pane to the Selected Fields pane.
3. Select up to five fields.
4. Click Recon.

The Recon browser window opens for multiple fields search.



Note: Users might need to click 'allow the blocked pop-up' in order to open a browser for Recon Search Login page.

Accessing Integration Command(s) from Recon Search

Note that not all Real-time Threat Detection fields are supported for search in Recon. These unsupported fields are disabled for selection in a Recon search. For Recon searches on active channels, instead of Attacker Address, search Source Address instead. Instead of Target Address, search Destination Address instead.

Procedure:

1. Open the desired channel and view the associated events.
See ["Viewing Events On an Active Channel" on page 32](#).
2. From the Active Channel screen Event List tab, click the desired event Name.
3. Click **Integration Command(s) > Recon Search....**
4. The Integration Commands popup displays. Select a command to determine your search, such as **By Source and Destination**, or **By Vendor and Product**.
5. Select a target implementation of Recon. For example, **Recon 1**.
6. Click **OK**. The Recon browser window opens.

If the previous steps are not performed in Configure target with target parameters, then, you are prompted in another pop-up to enter the IP address for the Recon host. The pop-up also shows the option to save the IP address parameter to the target. For more information, see the [ArcSight Console User's Guide](#).



Note: Users might need to click 'allow the blocked pop-up' in order to open a browser for Recon Search Login page.

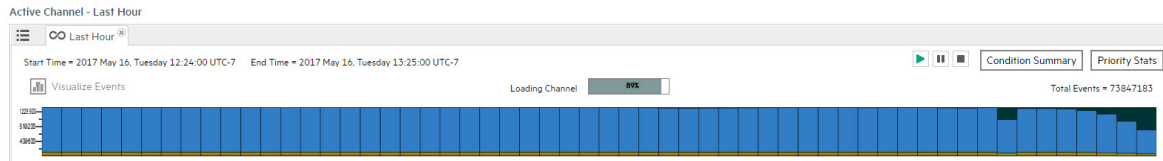


Note: On the Recon page, the time range for the search is the last 30 minutes by default, which may not yield any search results. If necessary, edit the active channel by changing the **Start Time** and **End Time** values for your search. See ["Creating an Event Channel" on page 47](#) for details on setting those values.

About the Active Channel Header

Each active channel has a header section with features you can use to understand and manipulate what the channel displays.

Elements on the active channel header



Active Channel Header Features

Feature	Usage
Name	Indicates the resource type (active channel) and active channel name.
Time Span	The Start Time and End Time show the chronological range of the channel.
Play, pause, and stop buttons	Controls updates to the channel with live events. Play: Events are continuously sent to update the channel. Pause: Temporarily stops updates to the channel. Click the play button to restore the update process. Stop: Stops updating the channel and removes all events from the grid. Click the play button to reload the channel.
Condition Summary	Displays the filter conditions defined for the channel. Filter conditions determine the amount of information to be displayed for events. Filters are in-line filters for the exclusive use of the active channel. For details about filter resources, see the ArcSight Console User's Guide .
Priority Stats	Displays event priority statistic indicators and their corresponding event count. For details about event priority scoring, see the ArcSight Console User's Guide .
Visualize Events button	Allows selection of up to four event fields (columns) on the channel to display in the graphical format of widgets. The results are displayed in the "Visualize Events tab" on the next page . In the Select Fields to Visualize Events popup, drag and drop to move field names from Available Fields to Selected Fields. Then click Visualize Events .
Channel status	Indicates status, for example, Channel Loaded.
Total Events	The total number of events received in the timeframe. Note: The event count function on active channels only reports live events, not replay events. If you prefer to see a count of all events coming through during a particular period, you should create a query viewer. If you want a count of only replay events, the event count in a replay channel will provide an accurate count of all replay events within a specific time window. For more information, see the ArcSight Console User's Guide .
Selected Events	The events within a time segment selected on the radar. If a segment is not selected, the value equals Total Events. See "Using the Active Channel Radar" on the next page for details.

Active Channel Header Features, continued

Feature	Usage
Radar display operation	A bar chart overview of events in the active channel. See "Using the Active Channel Radar" below for details.
Event Grid tab	Displays a grid view of incoming events.
Visualize Events tab	<p>Created after you click Visualize Events and select the event fields (columns) to be rendered in the graphical format of these widgets:</p> <ul style="list-style-type: none">• Event Count• Top 10 Row Chart for each selected event fields (up to four)• Pie chart for the Priority event field <p>Note: You can access Recon from the Visualize Events tab by clicking supported Recon fields and selecting Recon. Not all Real-time Threat Detection fields are supported for search in Recon. These unsupported fields are disabled for selection in a Recon search.</p> <p>The Target Address and Attacker Address fields have no Recon option.</p>

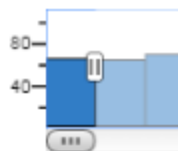
Using the Active Channel Radar

The radar consists of a bar chart overview of events on the active channel. It is divided into time segments sorted by event end time, each segment representing groups of events with the same end time.

The radar indicates the activity taking place in the entire channel, not just the current page. Its graphics represent units of time horizontally, and numbers of events vertically representing Priority attribute-value counts. The time and quantity scales in the graphic automatically adjust to accommodate the scope of the channel. The broader the scope, the smaller the graphical units.

Use the radar to focus events on selected time segments.

- To focus the grid on the event of one segment, click its corresponding bar on the radar as

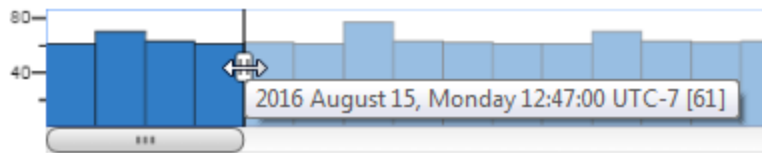


shown:

The selected time segment displays a handler widget. Depending on the location of the selected segment, handler widgets for both left and right boundaries are displayed.

- To select multiple segments, contiguous or not, press **Ctrl-click** on the desired segments.

- To focus the grid on multiple contiguous segments, drag the right or left handler to select more segments:



- To move a block of selected segments to a different area on the radar, drag the slider under the selected radar segments to the left or right along the radar:



The grid adjusts to display only the events within that segment. The Selected Events total also adjusts to display only the count of events within that same segment.

- To restore the radar to display all events, press **Ctrl-a**.

The grid adjusts to display all events matching the count in Total Events (the default view).

Annotating an Event

About:

When annotating an event, you can change the stage, add comments, specify a user, and mark the event as reviewed (see ["Marking an Event as Reviewed" on page 61](#)). You can only annotate events to which you have permission.

Procedure:

1. Open the desired channel.

See ["Viewing Events On an Active Channel" on page 32](#).

2. From the Active Channel screen > Event List tab, select the desired event and then click **Annotate**.

For easier selection, click the pause button to freeze the Event List.



Use the **Ctrl** or **Shift** key to select multiple events.



Note: If you scroll a selected event out of view in the Event List, the event becomes deselected.

3. Add annotation information as necessary.
 - a. If you applied the Code text tag to Queued, when do the same for the other stages. By default, the event stage is Queued. Other stages are Initial, Follow-Up, Final, and Closed. Your organization may have customized stages to suite your business requirements.

Default Collaboration Stages	Description
Queued	The event has not yet been inspected.
Initial	The event has been inspected.
Follow-up	The event is under investigation.
Final	The investigation has concluded.
Closed	The investigation is closed.

- b. Assign the event to a user as required.

Viewing Event Information

You can view event details, annotation history, and payload information for each event.

Event annotation is a workflow style of recording multiple users' analysis of an event. For more information, see [Annotating an Event](#).

An event payload is the information carried in the body of the event's network packet, separate from the packet's header data. For more information, see the [ArcSight Console User's Guide](#).



Tip: When viewing event information, click the pushpin icon to dock the Event Details dialog in the channel viewer grid.

To view event information:

1. Open the desired channel.
2. On the **Event List** tab, either double-click the desired event or select the event and then click **View Details**.

For easier selection, click the pause button to freeze the event list.

To select multiple events, use the **Ctrl** or **Shift** key.



Note: If you scroll a selected event out of view in the event list, the event is deselected.

3. If you selected multiple events, select the desired event from the event tree.
4. When viewing event details:
 - To filter event information based on fields, use the **Show Fields Containing** field.
 - To filter event information by field set, select the desired field-set from the **Field Set** drop-down list.
To clear the field set filter, open the field set selector and click the left arrow button.
 - To access Recon, click a field name and select **Recon** or **Recon (Multiple Fields)**.
Recon must support the fields that you select.
5. When viewing event annotation history:
 - The “Hidden” flag indicates that you specified “Flagged as Similar” for the event stage name. This event is hidden from all but the assigned users.
 - The “Is Reviewed” flag indicates that you marked an event as reviewed.
6. When viewing payload information:
 - A preserved payload remains attached to the event.
 - When you download a preserved payload, the payload still remains attached to the event.
Command Center might not display non-ASCII payload data. If the **Download Payload** button is enabled but no data appears, click **Download Payload** to download the data to a text editor.

Managing Channels

You can create two types of event channels: one based on the attributes of an existing channel and one created new.



NOTE: If a channel has not been locked, it is possible for multiple users to edit a Channel's attributes in both at the same time. If another user saves changes to a channel while you are editing it, you will be prompted that the channel has changed. If you are actively editing the channel, the page may return to the Channel resource list (for example, if the user changed the Channel name).

Creating an Event Channel

About:

Create an event channel to monitor events on a network.

Procedure:

Location: Channels > Active Channels > Active Channel - list screen > resource tree

1. Select the desired active channel folder.
2. Click **New**.

The New Channel popup opens.

3. Specify the channel name.
4. To specify the channel time attributes, refer to the following information:

Time Attribute	Usage
Start Time	<p>The relative or absolute time reference that begins the period to track events in the channel. To specify the time expression, make a selection from the Start Time drop-down menu.</p> <p>Note: If a channel is open when Daylight Savings Time starts or ends, it does not show the correct start time until you restart it.</p> <p>For a list of possible time values see the Start Time: field pull-down menu.</p>
End Time	<p>The relative or absolute time that ends the period to actively track the events in the channel. To specify the time expression, make a selection from the End Time drop-down menu.</p> <p>Note:</p> <p>If a channel is open when Daylight Savings Time starts or ends, the live channel does not show the correct start time until you restart it.</p>
Use as Timestamp	<p>Choose the event-timing phase that best supports your analysis. End Time represents the time the event ended, as reported by the device. Manager Receipt Time is the recorded arrival time of an event at the ArcSight Manager.</p>
Time Evaluation	<p>Choose whether the channel will Continuously Evaluate (like \$Now) to show events that are qualified by Start and End times which are re-evaluated constantly while the channel is running, or Snapshot to show only the events that qualify when the channel is first run.</p> <p>A channel set to Continuously evaluate is also known as a <i>sliding channel</i>, and typically has its End Time option set to \$Now.</p>

Start Time Attributes

Start Time Period	Description
\$Now - 30m	The current minute minus 30 minutes
\$Now	The current minute
\$Now - 1h	The current minute minus one hour
\$Now - 1d	The current minute minus one day
\$Today	Midnight (the beginning of the first minute) of the current day
\$Today - 1d	Midnight (the beginning of the first minute) of the current day minus one day
\$Today - 1w	Midnight (the beginning of the first minute) of the current day minus one week
Custom	The day and time for the start time.

Start Time Units

Start Time Unit	Description
m (lowercase)	Minutes (Do not confuse with M, meaning months.)
h	Hours
d	Days
w	Weeks
M (uppercase)	Months (Do not confuse with m, meaning minutes.)

- To specify columns for the active channel grid view, click **Configure Field Set**.
See ["Specifying Columns For the Active Channel Event List" on the next page.](#)
- To add a filter to the channel, click **Configure Filter** to add filter conditions in the Common Conditions Editor (CCE).
See [" Specifying Filter Conditions for an Active Channel" on page 50.](#)
- To validate the filter, choose **Operations > Validate**.
interactively checks condition statements as you add them. The validate option checks the condition statements collectively to ensure operators are used correctly.
The Validate Filter popup appears with the status of the filter. If there is a violation, edit the filter conditions.
- To edit filter conditions, choose either **Operations > Summary** and make changes directly in the SQL code, or right click the desired condition statement and make a selection from the extended menu.
Specifying **New Condition** from the extension menu creates a condition, at the specified location, that is in agreement with the selected condition.

9. Click **Update Filter Configuration** and then **Save** in the top half of the dialog box.

See Also:

["Creating a Channel Based on an Event Attribute" on page 55](#)

Specifying Columns For the Active Channel Event List

About:

The columns in the active channel Event List are based on the fields in a configured field set.

Prerequisite:

Create an event channel.

See ["Creating a Channel Based on an Event Attribute" on page 55](#) or ["Creating an Event Channel" on page 47](#).

Procedure:

Location: Channels > Active Channels > Active Channel - list screen > resource tree

1. Select the desired active channel folder.



Note: By default, Command Center stores active channels in the folder of the user who created the channels.

2. Do one of the following:
 - Click **New**.
The New Channel popup opens.
 - From the channel table, select the desired channel without clicking the **Display Name** link, and then click **Edit**.
The Edit Channel popup opens.
3. Click **Configure Field Set**.
4. From the navigation folders on the bottom left, select the desired field set folder and then select the desired field set from the Display Name column.
5. Click **Update Field Set** and then **Save Channel**.

Specifying Filter Conditions for an Active Channel

About:

You can specify filter conditions at channel creation or during a channel edit.

Prerequisite:

Create an event channel in order to edit filter conditions.

See ["Creating an Event Channel" on page 47](#) or ["Creating a Channel Based on an Event Attribute" on page 55](#).

Procedure:

Location: Channels > Active Channels > Active Channel - list screen > resource tree

1. Select the desired active channel folder.



Note: For a channel based on the attribute of an existing channel, Command Center stores the channel in the [user]'s Active Channel folder, by default, where [user] is the currently logged in username.

2. (Conditional) If you want to create a new filter, click **New**.
3. (Conditional) If you want to edit an existing filter, from the channel table, select the desired channel (without clicking the **Display Name** link), and then click **Edit**.
4. Click **Configure Filter**.

Use the Common Conditions Editor (CCE) in the lower half of the window to refine your view of the channel to show only the events you want to see. For example, if you have an active channel that includes both system and non-system events, you can filter out the system events to see only the non-system events.

The CCE presents Boolean logic in a user-friendly manner, allowing you to easily create conditions.



Note: Since the filter is created within the channel, the filter works only for the channel.

To edit a condition in the filter, double-click on the condition and use the statement editor on the right side of the window.


5. (Conditional) If you want to configure the filter using on-screen elements, complete the following:

- a. (Conditional) If your filter requires two or more condition statements, add a logical operator from the **Operators** area.

Logical Operator	Name	Use
&	AND	The new condition has to match in addition to existing conditions.
	OR	Either the new condition or any existing conditions have to occur.
!=	NOT	All but the new condition has to occur.

- b. From the the **Conditions** area, specify a condition.

Filter Condition	Description
Fields	You can specify fields with particular values as part of condition statements.
Filters	<p>A filter limits what events a channel displays. If the criteria of the condition are met, the evaluation returns true or false. Events that do not meet the condition or conditions are not evaluated further, but they are preserved in the data store.</p> <p>If there are existing filter conditions, you can tie them to the added filter condition with a logical operator.</p>
Assets	<p>After assets are added to your network model, you can select them in order to write conditions that help you analyze their role in the event traffic they process.</p> <p>Asset conditions state whether your enterprise assets are targets or sources of events. An asset condition states “if an event occurs and the selected asset is the source or target, generate a correlation event.”</p> <p>If there are existing filter conditions, you can tie them to the asset condition with a logical operator. If AND is used, all the existing conditions and the asset condition must occur in the event. If OR is used, either the existing conditions or the asset condition must occur. If NOT is used, all but the asset condition must occur.</p>
Vulnerabilities	<p>Specify the conditions of any hardware, firmware, or software state that leaves an asset open for potential exploitation.</p> <p>If there are existing filter conditions, you can tie them to the vulnerability condition with a logical operator. If AND is used, all the existing conditions and the vulnerability condition must occur in the event. If OR is used, either the existing conditions or the vulnerability condition must occur. If NOT is used, all but the vulnerability condition must occur.</p>

- i. To specify a Field Condition, complete the following steps:
- A. Select the Current Filter node or position the cursor in the desired location in the condition statements, click the **Fields** condition button , and then select the desired field from the area at the bottom right.
- You can use the **Show Fields Containing** field to locate a field. Start typing the name of the field, and the list will be actively filtered based on the text entered. Select a field from the list by double-clicking it in the field table.



Note: Field types of BitSet and Enumeration are not supported in Command Center. In addition, the Customer ID, Domain, Event Annotation Flags, and Generator fields are not supported. None of these appear in the field table. You cannot edit them in the Edit Channel popup. Certain fields, such as Event ID, have a limited set of operators provided. You will see a reduced set of operators in the Operator drop-down, compared to the Console.

- B. Specify the field value in the **Value** field.


To change the field or operator, use the **Field** and **Operator** fields, respectively.

- C. Click **Apply Condition**.


Starting with the addition of a logical operator, use the above steps to add any other field conditions.

- D. Click **Update Filter Configuration**.

- ii. To specify a Filter Condition, complete the following steps:

- A. Select a location in the condition statements list, and then click the **Filters** condition button . Select the desired filter from the area at the bottom right.
- B. Click **Apply Condition** to add the condition to the filter.
- C. Click **Update Filter Configuration**.

- iii. To specify an Asset Condition, complete the following steps:

- A. Select a location in the condition statements list, and then click the **Asset** condition button . Select the desired asset from the area at the bottom right. This list of Assets is larger than in the ArcSight Console.

The value selected from the **<xxx> Asset ID** drop-down menu, the checkbox, the value selected in the **NULL/NOT NULL** drop-down menu, and the Selected Resource group (under the Asset Category, Asset, or Zones tab) work together to define the Asset Condition statement. Selecting the checkbox enables the **is NULL** qualifier of the statement. When enabled, the statement evaluates whether the attribute does not exist in the Selected Resource group. When the checkbox is not selected, the statement evaluates whether the attribute value does exist.

Asset Condition filters select Events where the attribute you specified contains a value that is also found in the:

- Asset Category (if you selected an item under the Asset Categories tab)
- Asset Group (if you selected an item under the Assets tab)


- Zone Group (if you selected an item under the Zones tab)

To create a condition that selects an individual Asset by its unique ID or name, use the Field Condition and then specify the value directly.

B. Select an asset or group and then click **Apply Condition**.

C. Click **Update Filter Configuration**.

iv. To specify a Vulnerability Condition, complete the following steps:

A. Select a location in the condition statements list, and then click the **Vulnerability** condition button .

B. Select the desired vulnerability from the area at the bottom right.

C. To include any assets in the filter that could be impacted by the selected vulnerability, select the a value from the **<xxx> Asset ID** drop-down list (for example, *Agent Asset ID*).

D. Click **Apply Condition**.

E. Click **Update Filter Configuration**.

Repeat this step for each condition statement you want to include in the channel filter.

6. (Conditional) If you want to configure the filter using plain text, complete the following:

a. Choose **More Operations > Plain Text**.



Note: Using plain text overwrites any existing filter conditions. The Plain Text window also allows you to launch a third-party website that can convert SIGMA format to plain text, which you can then copy into the filter. Click **SIGMA Converter** and follow the instructions on the website.

b. In the text area, specify the filter, using the following.

- Field types:
 - String
 - Long
 - Int
 - Double
 - IP Address
 - Resource Ref
 - Bitset
 - Date Time



Note: The plain text filter does not support matchesfilter, Assets, hasvulnerability, or inActivelist field types.

- Joins:
 - AND
 - OR
 - NOT

Formatting considerations:

- For field names, use the database name in camel case, such as `targetAddress` or `bytesIn`.
- The String, Int, Date Time, and Resource Ref field values must be in double quotes, such as `"abc"`.
- All fields support the standard operators, except String fields, which do not support `<` or `>`.

Some examples:

```
((name Contains "abc" And targetAddress EQ "2.2.2.2") Or (bytesIn EQ 34 And bytesOut EQ 45))
```

```
vulnerability = "JliIuzwQBABCD+OSTHY1U5Q==:/All Vulnerabilities/CVE/CVE - CAN-2003-0605:CVE|CAN-2003-0605::"
```

```
endTime Between ("01/28/2020 16:21:51.000 -0600", "01/29/2020 16:21:51.000 -0600")
```

7. To validate the filter, choose **More Options: Operations > Validate**.

interactively checks condition statements as you add them. The validate option checks the condition statements collectively to ensure operators are used correctly.

The Validate Filter popup appears with the status of the filter. If there is a violation, edit the filter conditions.

8. To edit filter conditions, right click the desired condition statement and then choose either **Edit** or **Remove**.

This choice displays the appropriate work area at the bottom right.

9. To view the logic of the filter conditions, choose **More Options: Operations > Summary**.
10. Click **Update Filter Configuration** and then **Save Channel** in the top portion of the dialog box.



Note: When creating an Asset Filter, Command Center will not display Assets (under the Assets tab) that have the Asset Disabled flag set. You access this list in the New (or Edit) Channel pop up > Configure Filter > Asset Filter Condition statement options.

You can create a Field condition statement for any field that stores an IP Address and then use the InSubnet operator to match IP addresses in an address range. See the following topic for valid IP address ranges.

IP Address Ranges

The `insubnet` operator uses a range of IP addresses. Use the following guidelines to input IP address ranges in a single string.



Caution: The IP address range must be in the same family, for example, a range of IPv4 addresses or a range of IPv6 addresses.

Two-address range	<p>A two-address range is in the format <code>firstAddress - lastAddress</code>, meaning any address between an arbitrary range of any two addresses, inclusive.</p> <p>IPv4 range: <code>192.168.0.0 - 192.168.255.255</code></p> <p>IPv6 range: <code>2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff</code></p>
CIDR notation	<p>The CIDR notation is in the format <code>address/prefix-length</code>. This format is more restrictive than the two-address range format where the range starts and ends.</p> <p>IPv4 range: <code>192.168.0.0/24</code></p> <p>IPv6 range: <code>2001:db8:fd0c::/64</code></p>
Wildcard expressions	<p>Fields on the right end of an address may be replaced with an asterisk, with no numeric data to the right of the first asterisk. The wildcard represents the range of all values for the field, from all-zero bits to all-one bits. This format is more restrictive than the two-address range format in where the range starts and ends.</p> <p>IPv4 range: <code>192.168.*.*</code></p> <p>IPv6 range: <code>2001:db8:fd0c:*:*:*:*:*</code></p>

See Also:

["Editing an Event Channel" on page 57](#)

Creating a Channel Based on an Event Attribute

About:

You can further investigate a channel event attribute by creating a new channel based on that attribute. In addition to all the attributes of the originating channel, the new channel now collects greater detail on the specified attribute.

Because Command Center only supports basic event fields, such as name, attacker address, target address, target port, and priority, channel creation is limited to the attributes provided by these fields.



Note: If the channel that you are investigating originated in the ArcSight Console and contains event fields not supported in Command Center, these unsupported event fields will not be lost and can be viewed in the ArcSight Console.

Procedure:

1. Open the desired channel.
See "[Viewing Events On an Active Channel](#)" on page 32.
2. From the Active Channel screen > Event List tab, click the desired event link.
For easier selection, click the pause button to freeze the Event List.



3. Select the desired command from the extended menu.

Active Channel - System Events Last Hour

Start Time = 2017 May 16, Tuesday 07:39:00 UTC-7 End Time = 2017 May 16, Tuesday 08:40:00 UTC-7

Visualize Events Loading Channel 0%

Event List

View Details Add to Case Annotate Mark As Reviewed

Manager Receipt Time	Name	File Name	Target User Name	Priority
2017 May 16, Tuesday 08:37:4...	ActiveList entry upd...			3
2017 May 16, Tuesday 08:39:3...	ActiveList entry upd...			3
2017 May 16, Tuesday 08:39:3...	ActiveList entry upd...			3
2017 May 16, Tuesday 08:39:4...	Connector Device St...			3
2017 May 16, Tuesday 08:38:2...	ActiveList entry upd...			3
2017 May 16, Tuesday 08:36:0...	AL_GUID_Tracking			7
2017 May 16, Tuesday 08:37:3...	AddToList: Success			3
2017 May 16, Tuesday 08:39:4...	AddToList: Success			3
2017 May 16, Tuesday 08:39:5...	Channel [System Events Last H...	System Events Last Hour	admin	3
2017 May 16, Tuesday 08:39:5...	Connector Device Status			3
2017 May 16, Tuesday 08:35:1...	AddToList: Success	AL_GUID_Tracking		3

Context menu options:

- ArcSight Investigate
- ArcSight Investigate (Multiple Fields) ...
- Create [Name = ActiveList...dated]
- Create [Name != ActiveList...dated]
- Add [Name = ActiveList...dated]
- Add [Name != ActiveList...dated]
- Integration Command(s)
- Tools [Name = ActiveList entry updated]...

A new view that is a subset of the main active channel is created. Note that the total events count is less than the parent channel's total.

Option	Use
Create Channel [attribute=value]	Show only those events in which the selected attribute <i>matches</i> the value in the selected event.
Create Channel [attribute!=value]	Show only those events in which the selected attribute <i>does not match</i> the value in the selected event.

Option	Use
Add [attribute=value] to Channel	Show only those events that <i>match</i> both the prior and new filter elements.
Add [attribute!=value] to Channel	Show only those events that <i>do not match</i> both the prior and new filter elements.

4. To save the new channel, click **Save As** and do one the following in the Save Channel As dialog:

- Accept the default channel location - Specify the channel name and accept “[user’s] Active Channels” in the **Location** drop-down.
- Specify an alternate channel location - Specify the channel name, click the **Location** drop-down and then make the appropriate selection from the Select popup.



Note: If you choose a folder that has a parent, you must first select the parent folder from the left folder navigation and then select the child folder from the "Display Name" column. Direct selection of a child folder is not supported. This design helps to simplify the selection of a child folder that is multiple levels deep in a folder structure.

5. Click **OK**.

6. To view the new channel in the default folder, or alternative folder that you may have specified, click the resource tree tab.



See Also:

["Editing an Event Channel" below](#)

["Creating an Event Channel" on page 47](#)

Editing an Event Channel

About:

You can edit an event channel either created from an attribute of an existing channel or one created afresh.

Procedure:

Location: Channels > Active Channels > Active Channel - list screen > resource tree



Note: For a channel based on the attribute of an existing channel, Command Center stores the channel in the "[user's] Active Channel" folder, by default.

1. Select the desired active channel folder.
2. From the channel table, select the desired channel without clicking the **Display Name** link, and then click **Edit**.

The Edit Channel popup opens.

3. To change the channel name and or time attributes, refer to the following information:

Time Attribute	Usage
Start Time	<p>The relative or absolute time reference that begins the period to track events in the channel. To specify the time expression, make a selection from the Start Time drop-down menu.</p> <p>Note: If a channel is open when Daylight Savings Time starts or ends, it does not show the correct start time until you restart it.</p> <p>For a list of possible time values see the Start Time: field pull-down menu.</p>
End Time	<p>The relative or absolute time that ends the period to actively track the events in the channel. To specify the time expression, make a selection from the End Time drop-down menu.</p> <p>Notes:</p> <ul style="list-style-type: none">• If a channel is open when Daylight Savings Time starts or ends, the live channel does not show the correct start time until you restart it.• If setting the End Time results in the message "Invalid end date for sliding channel," the channel is set to Continuous evaluation instead of Evaluate once. Either re-set the End Time or change the Time Parameters option for the channel to Continuous evaluation.• Avoid creating an active channel that queries more than once per day.
Use as Timestamp	<p>Choose the event-timing phase that best supports your analysis. End Time represents the time the event ended, as reported by the device. Manager Receipt Time is the recorded arrival time of an event at the ArcSight Manager.</p>
Time Evaluation	<p>Choose whether the channel will be Continuously Evaluate (like \$Now) to show events that are qualified by Start and End times which are re-evaluated constantly while the channel is running, or Snapshot to show only the events that qualify when the channel is first run.</p> <p>A channel set to Continuously evaluate is also known as a <i>sliding channel</i>, and typically has its End Time option set to \$Now.</p>

Current Period

Period	Description
\$Now	The current minute
\$Today	Midnight (the beginning of the first minute) of the current day

Current Period, continued

Period	Description
\$CurrentWeek	Midnight of the previous Monday (or same as \$Today if today is Monday)
\$CurrentMonth	Midnight on the first day of the current month
\$CurrentYear	Midnight on the first day of the current year

Units

Unit	Description
m (lowercase)	Minutes (Do not confuse with M, meaning months.)
h	Hours
d	Days
w	Weeks
M (uppercase)	Months (Do not confuse with m, meaning minutes.)

4. To specify columns for the active channel grid view, click **Configure Field Set**.
See ["Specifying Columns For the Active Channel Event List" on page 49](#).
5. To add a filter to the channel, click **Configure Filter** to add filter conditions in the Common Conditions Editor (CCE).
See [" Specifying Filter Conditions for an Active Channel" on page 50](#).
6. To validate the filter, choose **Operations > Validate**.
interactively checks condition statements as you add them. The validate option checks the condition statements collectively to ensure operators are used correctly.
The Validate Filter popup appears with the status of the filter. If there is a violation, edit the filter conditions.
7. To edit filter conditions, right click the desired condition statement and make a selection from the extended menu.
Selecting a New **Condition** button creates a condition, at the specified location, that is in agreement with the selected condition.
8. Click **Update Filter Configuration** and then **Save Channel** in the top half of the dialog box.

See Also:

- ["Creating an Event Channel" on page 47](#)
- ["Creating a Channel Based on an Event Attribute" on page 55](#)

Deleting an Event Channel

About:

You can delete an event channel either created from an attribute of an existing channel or one created afresh.

Procedure:

Location: Channels > Active Channels > Active Channel - list screen > resource tree

1. Click **Channels > Active Channels**.
2. Expand the appropriate active channel folder in the resource tree and then click the desired folder.

Channels associated with the folder appear in a table in the center of the screen, as seen in the following typical view of active channels.

3. Click in the row of the desired channel, without clicking on the **Display Name** link.
4. With the channel row highlighted, click **Delete**.

Copying an Event Channel

About:

You can create a new channel by copying an existing event channel. The Copy feature is disabled if the channel or the folder storing the channel have been locked.

Procedure:

Location: Channels > Active Channels > Active Channel - list screen > resource tree

1. Click **Channels > Active Channels**.
2. Expand the appropriate active channel folder in the resource tree and then click the desired folder.

Channels associated with the selected folder appear in a table in the center of the screen.

3. Select the row of the desired channel, without clicking on the **Display Name** link.
4. With the channel row highlighted, click **Copy**. A new channel will be created in that folder with the same specifications as the original channel.

Marking an Event as Reviewed

Procedure:

1. Open the desired channel.
See ["Viewing Events On an Active Channel" on page 32.](#)
2. From the Active Channel screen > Event List tab, select the desired event and then click **Mark as Reviewed**.

Click the pause button to freeze the Event List for easier selection.



Use the **Ctrl** or **Shift** key to select multiple events.



Note: If you scroll a selected event out of view in the Event List, the event becomes deselected.


The Is Reviewed flag appears in the **Annotation History** tab of the Events Details popup.

Visualizing an Event Graphically

Through the use of widgets, you can view field information for events. You can choose the type of field information to display and the range of events for which this information should appear.



Note: can support only one visualization view per browser window session.

1. Open the desired channel.
See ["Viewing Events On an Active Channel" on page 32.](#)
2. From the Active Channel screen, click the pause button.
Pausing the channel event flow helps to ensure the proper selection of time intervals (buckets).

3. To select events over a specific period of time, make a selection from the Active Channel Radar.
See ["Using the Active Channel Radar" on page 43.](#)



Note: Command Center can accept a maximum of 100,000 events for visualization. Any events in excess of this limit will cause event visualization to be disabled. In this case, reduce the range of events on the Active Channel Radar. If a channel has too many events, using the correct filter can reduce the amount of events and make visualization possible.

4. Click the **Visualize Events** panel heading.
5. From the Select Fields to Visualize Events popup, specify the desired event field(s) by dragging and dropping. Click **Visualize Events**. The Field list is displayed is that same as the columns in the Event List.

A new tab appears. The selected event fields are represented graphically in the **Visualize Events** tab of the Active Channel panel. The graphs presented are "Top 10" values chart for the selected fields.

6. To limited the number of events, double click on the selected time bucket in the Event Count histogram.

The selected range appears between handles. Use these handles to change the event range.



Note: If the specified time range is very narrow and the number of events in this range is low, the Event Count widget will be empty.

Click **Reset All Filters** to restore all open widgets to reflect the full range of events.

You can create an Active Channel using the chart data in the Visualize Events tab.

1. Under the Visualize Events tab, right-click on a histogram bar in any chart.
2. In the context menu that appears, select one of the options to add filtering to the existing channel filter.



NOTE: When accessing Command Center using Firefox 38 from a Linux client, this context menu does not persist sufficiently to enable a selection. The work around is to access this capability using a browser on a non-Linux platform.

Chapter 4: Understanding Active Lists

Active lists allow you to track traffic with IP addresses of interest. Active lists are maintained in the ArcSight Console, but the Real-time Threat Detection Command Center allows you to view their contents.

To view an active list in the Real-time Threat Detection Command Center:

1. Go to Resources > Active Lists.
2. In the left pane, drill down to the folder that contains the active lists you want to view.
The right pane displays the active lists in the selected folder.
3. In the right pane, click the Display Name of the active list you want to view.

When you open an active list, you can perform the following actions on the generated content:

- Refresh.
- Delete one or more entries. For more information, see ["Deleting an Entry from an Active List" below](#).
- Export to CSV. For more information, see ["Exporting an Active List to a CSV File" on the next page](#).
- Filter. For more information about filters, see ["Filtering an Active List" on the next page](#).

Deleting an Entry from an Active List

When viewing the generated contents of an active list, you can delete one or more of the entries

To delete one or more entries:

1. (Conditional) If you want to delete one entry, click the entry in the active list.
2. (Conditional) If you want to delete multiple entries, Ctrl+click each entry.
3. In the toolbar, click **Delete**.
4. Click **OK** to confirm.

To delete all entries:

1. In the toolbar, click **Delete All Entries**.
2. Click **OK** to confirm.

Exporting an Active List to a CSV File

To export an active list:

If you want to manage active list data outside of the Real-time Threat Detection Command Center, you can export selected entries from an active list to a CSV file.

1. In the active list, Ctrl-click one or more entries.
2. In the toolbar, click **Export to CSV**.
3. Follow the download instructions for your browser.

Filtering an Active List

If an active list has a large number of entries, you can filter the list to show only the records that are most important to you. The filter can be a simple filter with a single condition, such as a field with a specific value, or a more complex filter with restrictive operators and multiple fields.

To filter an active list:

1. In the toolbar, click **Filter**.
2. (Conditional) If you want to add operators, Under Operators, add one or more of the following:
 - AND
 - OR
 - NOT



Note: By default, the Filter Editor places the operator under the selected item in the filter tree. After you add an operator to the tree, you can click and drag it to a different location.

3. To add a condition, complete the following steps:
 - a. Under Conditions, click the **Field** icon.



Note: By default, the Filter Editor places the condition under the selected item in the filter tree. After you add a condition to the tree, you can click and drag it to a different location.

- b. Select the Field you want to use in the condition.
 - c. Set the Operator and Value, and then click **Apply Condition**.
4. Under More Options, select **Validate**.
5. (Conditional) If the filter is invalid, correct the errors and try again.
6. (Conditional) If you need to edit a condition, right-click the condition in the tree and select **Edit**.
7. (Conditional) If the filter is valid, click **Update Filter Configuration**.

Chapter 4: Understanding Session Lists

Session lists allow you to track traffic with IP addresses of interest, similar to active lists. Session lists, however, are optimized for time-based queries and monitoring of rule-driven combinations of event attributes or custom fields.

Session lists are maintained in the ArcSight Console, but the Real-time Threat Detection Command Center allows you to view their contents.

To view a session list in the Real-time Threat Detection Command Center:

1. Go to Resources > Session Lists.
2. In the left pane, drill down to the folder that contains the session lists you want to view.
The right pane displays the active lists in the selected folder.
3. In the right pane, click the Display Name of the session list you want to view.

When you open a session list, you can perform the following actions on the generated content:

- Refresh.
- Delete one or more entries. For more information, see ["Deleting an Entry from a Session List" below](#).
- Export to CSV. For more information, see ["Exporting a Session List to a CSV File" on the next page](#).
- Filter. For more information about filters, see ["Filtering a Session List" on the next page](#).

Deleting an Entry from a Session List

When viewing the generated contents of a session list, you can delete one or more of the entries

To delete one or more entries:

1. (Conditional) If you want to delete one entry, click the entry in the session list.
2. (Conditional) If you want to delete multiple entries, Ctrl+click each entry.
3. In the toolbar, click **Delete**.
4. Click **OK** to confirm.

To delete all entries:

1. In the toolbar, click **Delete All Entries**.
2. Click **OK** to confirm.

Exporting a Session List to a CSV File

To export a session list:

If you want to manage session list data outside of the Real-time Threat Detection Command Center, you can export selected entries from a session list to a CSV file.

1. In the session list, Ctrl-click one or more entries.
2. In the toolbar, click **Export to CSV**.
3. Follow the download instructions for your browser.

Filtering a Session List

If a session list has a large number of entries, you can filter the list to show only the records that are most important to you. The filter can be a simple filter with a single condition, such as a field with a specific value, or a more complex filter with restrictive operators and multiple fields.

To filter a session list:

1. In the toolbar, click **Filter**.
2. (Conditional) If you want to add operators, Under Operators, add one or more of the following:
 - AND
 - OR
 - NOT



Note: By default, the Filter Editor places the operator under the selected item in the filter tree. After you add an operator to the tree, you can click and drag it to a different location.

3. To add a condition, complete the following steps:
 - a. Under Conditions, click the **Field** icon.



Note: By default, the Filter Editor places the condition under the selected item in the filter tree. After you add a condition to the tree, you can click and drag it to a different location.

- b. Select the Field you want to use in the condition.
 - c. Set the Operator and Value, and then click **Apply Condition**.
4. Under More Options, select **Validate**.
5. (Conditional) If the filter is invalid, correct the errors and try again.
6. (Conditional) If you need to edit a condition, right-click the condition in the tree and select **Edit**.
7. (Conditional) If the filter is valid, click **Update Filter Configuration**.

Chapter 5: Understanding Field Sets

Field sets are named subsets of available data fields. Field sets can help you focus a grid view, Event Inspector, or other field array on a particular context, such as customer accounts or vulnerability. Field sets are maintained in the ArcSight Console, but the Real-time Threat Detection Command Center allows you to view them.

To view a field set in the Real-time Threat Detection Command Center:

1. Go to Resources > Field Sets.
2. In the left pane, drill down to the folder that contains the field set you want to view.
The right pane displays the field sets in the selected folder.
3. To see all fields in the field set, in the right pane, expand the **Fields** column.



Note: If necessary, and you have the appropriate permissions, you can delete a field set in the Real-time Threat Detection Command Center.

Chapter 6: Applications

If you have licensed another application to integrate with Real-time Threat Detection, its user interface appears on the **Applications** tab.

When viewing an application on the **Applications** tab, you can access the application's online help by clicking the help link in the upper right corner of the Real-time Threat Detection Command Center window. Such documentation is separate from the Command Center online documentation.

For information on licensing an application contact your OpenText representative.

Appendix 7: Frequently Asked Questions

What happens if I'm investigating a channel that has event fields that are not supported in Command Center?

If the channel that you are investigating originated in the ArcSight Console and contains event fields not supported in Command Center, these unsupported fields are not lost and can be viewed in the ArcSight Console.

Related Topic:

["Creating an Event Channel" on page 47](#)

Can I change the default start time and end time for an event channel?

The default start and end times cannot be changed in Command Center. These changes have to be made in the ArcSight Console. Command Center recognizes any changes you make to the default times.

To change the default start time for new channels, edit the `console.properties` file in the `<ArcSight_Console_HOME>/current/config` directory. For example, add the this line...

```
console.channel.newChannel.defaultSubtractTime="$Now - 2h"
```

... to change the start time to two hours ago. For a list of possible time values see the **Start Time:** field pull-down menu.

If setting the End Time results in the message "Invalid end date for sliding channel," the channel is set to `Continuously evaluate` instead of `Evaluate once at attach time`. Either re-set the End Time or change the Time Parameters option for the channel to `Continuously evaluate`.

Avoid creating an active channel that queries more than once per day. For active channels that query more than once per day, use `Evaluate time parameters once at attach time` instead of `Continuously evaluate`.

Related Topic:

["Creating an Event Channel" on page 47](#)

What do I do if a channel is taking long to load?

Some channels can be resource intensive, such as those with a time range of an hour or so. If a channel takes long to load in a high-traffic environment, open this channels in the ArcSight Console. To view a resource-intensive channel in Command Center, narrow the time range to 5 - 10 minutes to reduce the event volume.

Related Topic:

["Viewing Events On an Active Channel" on page 32](#)

How many channels can I have open at one time?

For optimum performance, limit open channels to 3 per browser, though Command Center can support up to 10 moderate-traffic channels or up to 15 light-traffic channels per browser. Between Command Center and ArcSight Console, Real-time Threat Detection can support up to 25 open channels.

Related Topic:

["Viewing Events On an Active Channel" on page 32](#)

What fields are supported in Command Center channels?

The Real-time Threat Detection Command Center does not support global and local variables. The Real-time Threat Detection Command Center supports only standard event fields for viewing. Variables (global or local) are not supported. Use the ArcSight Console instead. See the following table:

Fields

User Interface	Standard Event Fields	Local Variables	Global Variables
Real-time Threat Detection Command Center	Yes	No	No
ArcSight Console	Yes	Yes	Yes

Related Topic:

["Viewing Events On an Active Channel" on page 32](#)

Does Command Center support non-ASCII payload data?

Command Center might not display non-ASCII payload data. If the **Download Payload** button is enabled but no data appears in the Event Details window, click **Download Payload** to download the data to a text editor.

How do I get my `[[[Undefined variable _ARSTc_Variables.NewDownloadCenter]]]` credentials?

Access to `[[[Undefined variable _ARSTc_Variables.NewDownloadCenter]]]` is necessary in order to download an app which enables you use Tool Commands. To receive your `[[[Undefined variable _ARSTc_Variables.NewDownloadCenter]]]` credentials (user name and password), contact ArcSight Support or your reseller.

Related Topic:

["Evaluate the Network Route of an Event in a Channel" on page 36](#)

Why are channels not current in a new Real-time Threat Detection session?

Some channels in Command Center may not be current when accessed in a new Real-time Threat Detection session. To ensure current event information, refresh the channel by clicking the stop and play buttons.

Related Topic:

["Viewing Events On an Active Channel" on page 32](#)

Does the change to or from Daylight Savings Time effect an open active channel?

If an active channel is open when Daylight Savings Time goes into or out of effect, the active channel will not reflect the correct start and end times until the channel is closed and reopened.

Related Topic:

["Viewing Events On an Active Channel" on page 32](#)

Why does the right end of the top menu bar appear overlapped?

To view this user interface properly, configure your browser to at least 1920 by 1080 pixels. The Real-time Threat Detection Command Center top menu bar appears to have the right-most Top menu bar options overlapped if the browser window dimensions are smaller than 1920 by 1080 pixels.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on User's Guide (Command Center 8.1)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!