



ArcSight Recon as a Service 1.3 User Guide

July 2021

Copyright Notice

© Copyright 2021 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

For additional information, such as certification-related notices and trademarks, see <https://www.microfocus.com/about/legal/>.

Contents

Chapter 1: Welcome to ArcSight Recon as a Service	10
I Investigating Events	11
Chapter 2: Searching for Events	12
Understanding the Search Feature	12
Creating and Saving Searches	13
Creating a Search	13
Saving a Search	14
Naming a Search	15
Finding a Saved Search	15
Initiating a Search from Enterprise Security Manager	15
Understanding the Search Progress Indicators	15
Chapter 3: Managing Your Searches	17
Viewing Search Results	17
Viewing the Events Timeline	17
Viewing the Events Table	18
Viewing and Using the Details of an Event	20
Identifying Fields without Data	21
Refreshing Search Results	21
Modifying the Search Settings	21
Exporting the Search Results	21
Scheduling Regular Runs of a Search	22
Creating a Scheduled Search	22
Viewing Scheduled Searches	24
Cloning a Scheduled Search	25
Editing a Scheduled Search	25
Deleting a Scheduled Search	26
Enabling and Disabling a Scheduled Search	26
Managing Completed Runs of a Scheduled Search	26
Viewing a Completed Run of a Scheduled Search	27
Deleting Completed Runs of a Scheduled Search	28
Exporting Completed Runs of a Scheduled Search	28
Chapter 4: Understanding the Search Parameters	30
Understanding the Types of Search Queries	30

FULL TEXT SEARCH	31
FIELD-BASED SEARCH	31
HASHTAG (predefined searches)	31
Using GlobalEventID in a Query	32
Understanding the Query Syntax, Operators, and Functions	33
Understanding the Query Syntax Requirements	33
Understanding the Search Query Functions and Operators	35
Understanding the Functions for Building Eval Expressions	37
Specifying a Group of Fields	45
Specifying an Alias for a Field	46
Specifying IP Addresses and Subnets	50
Understanding How Search Stores IP and MAC Addresses	50
Entering an IP or MAC Address	51
Including a Storage Group's Filter in the Search Query	52
Extending the Search with a Lookup List	53
Understanding Considerations for the Lookup List File	53
Creating a Lookup List	53
Replacing a Lookup List	54
Deleting a Lookup List	55
Using Specific Sets of Fields for Search Results	55
Viewing and Creating Fieldsets	56
Creating a Fieldset	56
Editing a Fieldset	57
Deleting a Fieldset	58
Cloning a Fieldset	59
Configuring the Time Range	59
Specifying a Dynamic Date Range	60
Understanding Search Timestamps for Events	61
Understanding How Time Zones Affect Search Results	62
Configuring Preferred Settings for Searches	62
Chapter 5: Checking the Integrity of Event Data	63
Understanding Event Integrity Check	63
Running an Event Integrity Check	64
Viewing Event Integrity Check Results	65
Viewing the Event Integrity Check Status	65
Viewing Last Event Integrity Check Results Table	66
Configuring Data Collection to Support Event Integrity Checks	68

II Hunting for Undetected Threats	69
Chapter 6: Viewing Dashboards and Reports	70
Viewing a Dashboard	70
Viewing a Report	71
Specifying Default Dashboards for the Reports Portal	71
Chapter 7: Understanding the MITRE ATT&CK	73
MITRE ATT&CK Dashboards	74
MITRE ATT&CK Overview	74
Evaluation Techniques and Tactics Summary	75
MITRE ATT&CK Reports	76
MITRE ATT&CK Destination Address Summary	76
MITRE ATT&CK Destination Host Summary	76
MITRE ATT&CK Destination Username Summary	77
MITRE ATT&CK Source Address Summary	77
MITRE ATT&CK Source Hostname Summary	78
MITRE ATT&CK Source Username Summary	78
MITRE ATT&CK Technique Summary	78
Chapter 8: Understanding the Cloud Security Dashboards and Reports	80
Abuse and Nefarious Use of Cloud Services – Dashboards	83
Account Hijacking – Dashboards and Reports	84
Advanced Persistent Threats – Dashboard	85
Data Breaches – Dashboards	85
Data Loss – Dashboard and Reports	86
Denial of Service – Dashboard	87
Insecure Interfaces and APIs – Report	87
Insufficient Due Diligence – Reports	88
Insufficient Identity Credential and Access Management – Reports	88
Malicious Insiders – Report	89
System Vulnerabilities – Dashboard and Reports	89
Vulnerabilities on Shared Technologies	91
Chapter 9: Understanding the Foundation Dashboards and Reports	92
Entity Monitoring – Dashboards and Reports	94
Events Overview – Dashboards	95
Hosts Monitoring - Reports	96
Malware Monitoring – Dashboard and Reports	97
Network Monitoring – Dashboards and Report	98
Perimeter Monitoring – Dashboards and Reports	100
Vulnerability Monitoring – Dashboard and Reports	101

Chapter 10: Understanding the OWASP Security Dashboards and Reports	103
Broken Access Control	104
Broken Authentication	104
Cross-site Scripting	105
Injections	105
Insecure Deserialization – Dashboards and Reports	106
Insufficient Logging and Monitoring – Dashboards and Reports	107
Security Misconfiguration	109
Sensitive Data Exposure	109
Using Components with Known Vulnerabilities – Dashboards and Reports	110
XML External Entities	111
III Analyzing Anomalous Data with Outlier Analytics	113
Chapter 11: Generating Models to View Anomalous Data	114
Considerations for Generating Models	114
Defining and Building a Model	115
Scoring a Model	116
Deleting a Model	117
Chapter 12: Viewing Anomalous Data in a Model	118
Understanding the Provided Analytics Charts	118
Investigating Anomalies Further	119
Viewing a Scored Model	119
IV Managing the Quality of Your Data	121
Chapter 13: Understanding the Data Quality Insights	122
Chapter 14: Understanding How Data Quality is Calculated	123
Chapter 15: Analyzing Data Quality	124
V Managing Your Stored Data	125
Chapter 16: Organizing Your Data	126
Using Storage Groups to Organize and Retain Data	126
Creating a Storage Group	127
Directing Events to the Correct Storage Group	127
Activating and Deactivating Storage Groups	128
Changing the Settings of a Storage Group	128
Modifying a Storage Group	128
Applying Your Changes to a Storage Group	129

Setting Retention Policies for the Data	129
Deleting Old Data	130
Using Storage Group Queries in a Search	130
VI Using Visuals and Reports to Analyze Data	131
Accessing Reports and Dashboards	131
Scheduling Report Generation	131
Designing Dashboards for Data Analysis	132
Designing Reports for Data Analysis	132
VII Managing User Access and Preferences	134
Chapter 17: Assigning Permissions for Recon	135
Chapter 18: Understanding Default Roles for Recon	136
Chapter 19: Configuring User Preferences	137
Configure Search Preferences	137
VIII Appendices	139
A Mapping Database Names to their Appropriate Search Fields	140
Agent Fields	140
Category Fields	141
Correlation Fields	141
Destination Fields	142
Device Fields	143
Device Custom Fields	144
Event Fields	145
Extension Fields	146
File Fields	146
Flex Fields	147
OldField Fields	147
Old File Fields	147
Request Fields	148
Source Fields	148

About This Book

This *User's Guide* provides concepts, use cases, and contextual help for ArcSight Recon.

- ["I Investigating Events" on page 11](#)
- ["II Hunting for Undetected Threats" on page 69](#)
- ["III Analyzing Anomalous Data with Outlier Analytics" on page 113](#)
- ["IV Managing the Quality of Your Data" on page 121](#)
- ["VI Using Visuals and Reports to Analyze Data" on page 131](#)
- ["V Managing Your Stored Data" on page 125](#)
- ["VII Managing User Access and Preferences" on page 134](#)

Intended Audience

This book provides information for individuals who investigate events and hunt for undetected threats. These individuals have experience in security operation centers or performing duties of a security analyst or operator.

Additional Documentation

The ArcSight Recon documentation library includes the following resources:

- [ArcSight as a Service](#), which provides information about features available in the current release
- [Administrator's Guide to ArcSight Platform](#), which provides information about deploying, configuring, and maintaining the products that you deploy in the containerized environment
- [Technical Requirements for ArcSight Platform](#), which provides information about the hardware and software requirements for installing Recon as well as the other containerized capabilities

For the most recent version of this guide and other ArcSight documentation resources, visit the [documentation for ArcSight Recon](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care at <https://www.microfocus.com/support-and-services/>.

Chapter 1: Welcome to ArcSight Recon as a Service

Recon provides a modern log search and hunt solution powered by a high-performance column oriented, clustered database. The [Search](#) feature helps you investigate security issues by viewing search results and identifying outlier events. The [Reports](#) feature, including MITRE ATT&CK content, enables you to [hunt](#) for undetected threats as well as create charts and dashboard to [visualize](#) filtered data with tables, charts, and gauges. With the [Outlier Analytics](#) feature you can identify anomalous behavior by comparing incoming event values to typical values for your environment.

Recon deploys within the **ArcSight Platform**, which provides common services such as the Dashboard and user management.

- [Investigate alerts and events](#)
- [Hunt for undetected threats](#)
- [Analyze anomalous data with outlier analytics](#)
- [Evaluate and manage the quality of your data](#)
- [Use visuals and reports to analyze your data](#)
- [Organize data into storage groups](#)
- [Manage user access](#)

I Investigating Events

The **Search** feature enables you to look for and investigate events that meet specified criteria so you can detect anomalies that point to security threats. You can view the results in tabular and timeline formats. Each search consists of [specifying query input](#), [search result fields](#), and the [time period](#) for which you want to search events.

Queries are case sensitive. The query input determines the [search type](#) (full text, natural language, or contextual). As you specify the criteria for a search query, Search suggests items and operators based on a schema data dictionary. You can also choose from [predefined search queries](#).

- ["Searching for Events" on page 12](#)
- ["Managing Your Searches" on page 17](#)
- ["Understanding the Search Parameters" on page 30](#)
- ["Checking the Integrity of Event Data" on page 63](#)

Chapter 2: Searching for Events

Search is contextual and has an auto-suggest capability to help you specify search criteria and improve productivity. You can retrieve events from an index; search for specific conditions within a rolling time window; create aggregate charts; and identify patterns in your data.

- ["Understanding the Search Feature" below](#)
- ["Creating and Saving Searches " on the next page](#)
- ["Initiating a Search from Enterprise Security Manager" on page 15](#)
- ["Understanding the Search Progress Indicators" on page 15](#)

Understanding the Search Feature

Recon ingests log data from ArcSight Logger and SmartConnectors routed through Transformation Hub and events from ArcSight Enterprise Security Manager. Each entry in a log is referred to as an **event**. Recon accepts events from Transformation Hub and organizes them to maximize search and storage efficiency.

The **Search** feature enables you to search events by entering a search command, a time window over which to search, and the fields from the Unified Event Schema. Search displays results in an [Events Timeline](#) chart, which a histogram shows the number of events returned over event occurrence time. The [Events table](#) below the Timeline shows events returned by search. When you select an event, Search displays the [Event Details](#) panel.

Search uses a database that serves as the main data store, as well as a cache. The search engine is a scalable server-side application that executes and caches large search queries in the database. In the backend, Recon saves your searches, user preferences, and proxy search requests to the search engine using a REST API. The database stores three [timestamps for each event](#) to provide more clarity in your search results. When [creating a search](#), you specify the timestamp to use for retrieving events.

For the query's time range, you can choose a fixed start and end date, where you cannot refresh data, or a predefined date range. For example, for the last **30 minutes** predefined search, you receive updates upon re-executing the search based on the most recent 30

minutes. Alternatively, you could specify [dynamic dates](#), such as **Midnight on the first day of the current month**.

After initiating a search, you can pause, restart, and cancel the process as needed. A [progress bar](#) shows you the percent of retrieved data.

Creating and Saving Searches


Recon supports up to 10 active searches and 40 saved searches per user.

- ["Creating a Search " below](#)
- ["Saving a Search" on the next page](#)
- ["Naming a Search" on page 15](#)
- ["Finding a Saved Search" on page 15](#)

Creating a Search

For every search, you must enter the query input, search result fields, and the time period for which you want to search events. Queries are case sensitive. The query input determines the search type (full text, natural language, or contextual). As you specify the criteria for a search query, Search suggests search items and operators based on a schema data dictionary. You can also choose from predefined queries.

If you tend to use the same settings for some search parameters, you might want to specify a [preferred default setting](#). For example, you can configure a default time range.

 **NOTE:** Recon treats a comma (,) between search items and values as an OR operator.

To create a search:

1. Select **Search > + New Search**. You can choose search data migrated from ArcSight Logger.
2. Specify the [query parameters](#).
For example:
Source Address = 192.10.11.12 and Destination Address less than 192.10.11.12
Enter # to view the predefined queries.
3. To search for a field without data, enter [field_name] = Null.

4. Specify the [fieldset](#) you want for the search results.

By default, Search displays the your [preferred default fieldset](#). If you have not specified one, Search display the Base Event Fields fieldset.

5. For the time range, perform **one** of the following actions:

- Accept the default time (**Last 30 minutes**)
- From the drop-down menu, select a pre-defined value under **Quick Ranges**
- From the drop-down menu, use the **Custom Range** fields to specify a time range
- From the drop-down menu, select **Dynamic**, and then enter a [dynamic date value](#)

You can also specify the timestamp you want to use for the retrieved events.

Search uses "[Normalized Event Time](#)" on page 61 by default.

6. Click **Search**.

Search begins populating the [Events Timeline](#) and [Events table](#). Depending on the number of events retrieved, the search might pause to indicate that the amount of data could impact the search performance. You might want to select a smaller time range. To resume a search, click the play button in the progress bar.

7. (Optional) To more easily find the search later, give the search a [name](#).
8. To [save](#) the search for future use, select **Save**.

Saving a Search

After you execute a search, Recon automatically saves the search if you navigate away from the search page to another Recon feature, the Dashboard, or the Admin pages. However, your search is not automatically saved if you close the browser or tab or when you log out. To permanently save your search, you can add it to the [Saved Searches](#) list.

You can delete the search from the saved list at any time. You can also [configure Search](#) to automatically delete searches after a specific time.


To permanently save your search:

1. (Optional) Give the search a name.
2. Select **Save**.
3. To view your search, select **Saved Searches**.

Naming a Search

By default, Recon gives each search the title *Search <N>*. You can apply a custom name to the search at any time.

To name a search:

1. In the top-left corner of your screen, hover over the search name and then click the **pencil** icon  .
2. Enter the custom name.
3. To save your changes, select the **Check** icon.

Finding a Saved Search

Select **Search > Saved Searches**.

Recon saves up to 40 searches. You can sort the table of saved searches by the search name, query, number of results, or date it was saved. To more easily find searches, you can give them [custom names](#).

Initiating a Search from Enterprise Security Manager

From Enterprise Security Manager (ESM), you can initiate a search in Recon for a maximum of five fields, based on the available columns on the active channel. Within Recon, you can filter ESM data for more specific results. ESM generates a URL, opens a browser, and creates the new search in Recon.

To perform this action, you must enable Recon in ESM. For more information, see the [ESM Installation Guide](#).

Understanding the Search Progress Indicators

As the **Search** feature retrieves data, it displays a **progress bar** to show its status, including the percent of data received. Rather than attempting to read all data at once, Search gathers data in chunks of time. The progress bar shows the time range from which the results are currently being retrieved.

You can **pause the search** and restart as needed.



NOTE: When performing a search with two or more identical queries the number of events returned for the second search will correspond to the next chunk of data. If you pause then resume the search, the first search will be moved to the next chunk as well, maintaining the same number of events retrieved. The identical queries can contain either one of the built-in queries or a custom query.

Chapter 3: Managing Your Searches

You can save, refresh, and edit your searches. To help you investigate events, Search displays the results as a [timeline](#), in a [table](#), and in a [detailed view](#). You can export the search results in the table to a CSV file. You can also schedule a search to run at specific intervals, then analyze the completed runs of that search over time.

- ["Viewing Search Results" below](#)
- ["Modifying the Search Settings" on page 21](#)
- ["Exporting the Search Results" on page 21](#)
- ["Scheduling Regular Runs of a Search" on page 22](#)
- ["Managing Completed Runs of a Scheduled Search" on page 26](#)

Viewing Search Results

Search displays results in an **Events Timeline**, **Events table**, and **Event Details panel**. If connectors are configured to send raw events, the table and details panel can include **raw event data**. Also, the maximum number of events that a search can return is 10 million. If your searches regularly stop at the maximum limit, consider splitting the query into separate searches.

- ["Viewing the Events Timeline" below](#)
- ["Viewing the Events Table" on the next page](#)
- ["Viewing and Using the Details of an Event" on page 20](#)
- ["Identifying Fields without Data" on page 21](#)
- ["Refreshing Search Results " on page 21](#)

Viewing the Events Timeline

The **Events Timeline** displays data points in a segmented timeline across the specified time range. The time range in the Timeline corresponds with the data listed in the [Events table](#).

If you have a large number of data points or a wide time range, you can see the big, overall picture, but you might not be able to clearly identify specific data points. To

narrow the scope of the displayed data, select **Enable Range Selector** then adjust the boundaries of the selector.

To view the **details of a data point** or moment in time, select **Disable Range Selector**, and then hover over the data point.

Viewing the Events Table

The **Events** table contains all the fields specified in the **fieldset**. You can choose to display the table in **Grid View** or **Raw View**. To **view details of a specific event**, select the event.

While viewing the table, you can perform the following actions:

View all details for an event

When you select an event in the table, Search opens the **Event Details panel**. Within the panel, you can further expand the fields for more information.

View raw event data

When you click the **Raw View** icon, the Events table replaces the fieldset columns with a Raw Data column, which displays the whole raw syslog event.

Although the **Raw Event** field is most applicable for syslog events, you can also display the raw event associated with CEF events.

To do so, make sure the connector that is sending events to the database populates the *rawEvent* field with the raw event.

View all event data for a field value

Right-click a value in a table row, then select **Search For**.

Search displays all of the event data based on the selected field value.

View the most and least common values for an event record field

Right-click a column heading, then select **Preview Top/Bottom**.

To help filter data for security threats, you can quickly display the most and least common values for a field. Search displays the count and percentage of hits for the value.

For example, the *Device Vendor* field might have a top value of “bluecoat” with a count of 3,000 hits, accounting for 30 percent of 10,000 results.

View authenticated users

*Applies only when the fieldset for the original search includes the **Device Receipt Time** field.*

Right-click an IP address or host name, then select **Get Authenticated Users**.

Search displays users who have successfully authenticated to the IP address or host name in the last 24 hours.

Copy a value from an event

To use a value from an event elsewhere, simply right-click and copy the value.

Search for an event value

To add a value from an event to your query, right-click the value.

Compare data in columns

Right-click a column heading, then select **Pin Column** or **Unpin Column**.

By pinning a column, you can compare the column’s values against those of other columns. Search moves the pinned column to the extreme left location in the table. You can pin multiple columns.

Remove or hide columns

If you do not want to view a column, right-click the column heading, then select **Hide Column**.

Alternatively, you can click the **Wrench** icon, and then select the column.

Reorder columns

To rearrange the order of the columns, drag each column to new position.

Sort the data in columns

Select the **up or down arrow** in the column heading to change the sort order.

Viewing and Using the Details of an Event

When you select an event in the [Events table](#), Search opens the **Event Details** panel. In this panel, you can scroll through the specific details of the event. Search groups the details by categories such as **Agent** and **Source**.

You can view the raw data details for the event, as well as instruct the panel to include fields with *null* data. For example, you could view details about the agent, category, device, source, or severity. Details displayed in blue text are part of the query filter.

- ["Exporting All or Some Event Details" below](#)
- ["Applying Event Details to Other Searches or Share with Colleagues" below](#)

Exporting All or Some Event Details

You might want to share the selected event's details with a colleague or use the details in a report or other media. You can export all content in the **Event Details** panel with or without empty values.

Apply Event Details to Other Searches or Share with Colleagues Search allows you to copy the URL of a detail to share with colleagues or open in a separate browser tab. You can also choose to use the detail in a new search query and in an nslookup or WhoIs search.

For example, you might select a domain name and use a nslookup to check whether the domain is valid.

Applying Event Details to Other Searches or Share with Colleagues

Search allows you to copy the URL of a detail to share with colleagues or open in a separate browser tab. You can also choose to use the detail in a new search query and in an nslookup or WhoIs search.

For example, you might select a domain name and use a nslookup to check whether the domain is valid.

Identifying Fields without Data

If an event does not have data for a schema field, Search represents the absence of data (*null*) in the results in the following ways:

Affected Field	Displayed Result
Search field	Null, NULL and null query formats
Events table	Empty cell
Empty field from ESM (for example, name="")	name = "", NULL
Event Details panel	--- in the cell

Refreshing Search Results

If the [time range](#) for your search is based on a predefined range, such as **Last 30 minutes**, you can refresh the search results as desired. However, refreshing the browser as you update a search does not save your changes. You must [save the refreshed results](#).

Modifying the Search Settings

When viewing a search, you can change the query, a fieldset, and the range selector.

To modify the settings:

1. In the saved search, change the query, [fieldset](#), or [time range](#).
2. To return to your original settings, select **Revert Changes**.
3. To update the search results with the modified settings, select **Search Now** or **Search**.

Exporting the Search Results

You can export the [Events table](#) to a CSV file. Search exports data based on the specified fieldset for the search. The export process limits the file to one million event records.

To export the results:

1. In the table's header, select the **CSV** icon.
2. Choose to save the file or open in a desired application.

Scheduling Regular Runs of a Search

You must have the Scheduled Search permission to schedule runs of a search.

Select **Search > Scheduled Searches > Schedule**.

A **scheduled search** is a search that runs on a regular interval. Whereas a [saved search](#) is saved, but does not run automatically.

Each time a scheduled search runs, search adds the results to the list of [Completed Searches](#) runs.

- ["Creating a Scheduled Search" below](#)
- ["Viewing Scheduled Searches" on page 24](#)
- ["Cloning a Scheduled Search" on page 25](#)
- ["Editing a Scheduled Search" on page 25](#)
- ["Deleting a Scheduled Search" on page 26](#)
- ["Enabling and Disabling a Scheduled Search" on page 26](#)

Creating a Scheduled Search

Before creating a [Scheduled Search](#), you must [create or save](#) at least one search. For every scheduled search, enter the [query](#), [fieldset](#), or [time range](#) for the search events or leave the defined values for the saved search.

Just as for a saved search, the following considerations apply to a scheduled search:

- The search is case sensitive.
- The query input determines the [search type](#) (full text, natural language, or contextual).
- The system treats a comma (,) between search items and values as an OR operator.

- As you specify the search criteria, the system suggests search items and operators based on a schema data dictionary. To view the [predefined queries](#), type # in the **query** field.
- To search for a field without data, enter [field_name] = *Null*.

To create a scheduled search:

1. (Conditional) To schedule a search that you are currently viewing, select **Schedule**.
2. (Conditional) To schedule a search without currently viewing one, complete the following steps:
 - a. Select **Search > Scheduled Searches**.
 - b. Select **+**.
3. Specify a **Name** that is 5 to 255 character long.
4. To enable the scheduled search, select **enable**. You can enable and disable scheduled searches at any time in the **Scheduled** tab.
5. To indicate how frequently you want the search to run, specify one of the following options:
 - **Hourly**
 - **Daily**
 - **Weekly**
 - **Monthly**
6. Depending on the frequency that you specified in [Step 5](#), configure the settings for the dates and times of each run.



NOTE: For **Starting from**, if you select end after, the maximum number of instances is 1000.

7. (Conditional) To schedule an existing search, select one from the pull-down menu under **Search Query and Metadata**.
8. (Conditional) To create a query, specify the [query parameters](#), [fieldset](#), or [time range](#).
For example:
Source Address = 192.10.11.12 and Destination Address less than 192.10.11.12
9. Under **Result Retention and Limitations**, configure how long you want to keep each completed run of the scheduled search.

- Your choice of values for each setting might be confined to limits set by your product administrator.
 - For **Delete results after**, you can specify a value that overrides how you configured **Search Expires In** for your search preferences. For example, your prefer that searches expire within five days. But you want the results for this scheduled search to expire after 10 days.
 - If you select **Keep only the most recent run**, then, when a run completes successfully, Search deletes the results of the previous run.
10. For **Retrieve up to**, specify the number of results you want to receive.
 11. Select **Schedule**.

Viewing Scheduled Searches

The **Scheduled** tab displays information for created scheduled searches.

You can perform the following actions:

View and edit all details for a schedule search

To view specific scheduled search details, in the Name column, locate the search name and select it. Click **Edit** at the top of the table.

Sort the data in columns

To change the sort order, click the column heading to toggle between ascending and descending order.

Reorder columns

To rearrange the order of the columns, drag each column header to a new position.

Search for a search keyword

To find a keyword, click the field next to the **Magnifying Glass** icon (Search Keyword), enter a value, and the system displays your results automatically.

Hide and display columns

To hide and display a column, in the far right-corner of the window, click the **Wrench** icon (Manage Columns), and then select and clear the column name checkboxes.

Filter the data in columns

You can filter scheduled searches based on Status, Timestamp, and Fieldset. To filter the data for more specific results, in the far-right corner of the window, click the **Funnel** icon (Filters), and then select and clear the filter options.

Cloning a Scheduled Search

After creating a scheduled search, you can clone it at any time.

To clone a search:

1. Select **Search > Scheduled Searches**.
2. Select the scheduled searches that you want to clone.
3. Click the **clone** icon.

Editing a Scheduled Search

After creating a scheduled search, you can edit it at any time. After you modify a schedule, the first completed run will have a flag to indicate that the modification occurred.

If you change the **Pattern** values, please be aware that Search counts any and all completed runs before you made the change. For example, your scheduled search uses the **repeat forever** option and Search has performed three runs. If you update the **ending option** to end after eight occurrences, Search counts the three previous completed runs; therefore, you would only have five occurrences of the eight occurrences left to run. Should you want eight occurrences, you would need to change your **ending option** to 11 occurrences.

To edit a search:

1. Select **Search > Scheduled Searches**.
2. Select the scheduled searches that you want to edit.
3. Click the **edit** icon.

Deleting a Scheduled Search

You can delete a scheduled search at any time. After selecting **Delete**, the system prompts you to keep or delete the [completed runs](#) associated with the scheduled search.



NOTE: To cancel the deletion process, select the **X** that closes the dialog box, instead of selecting **Yes** or **No**.

Enabling and Disabling a Scheduled Search

After creating a scheduled search, you can enable and disable it at any time.

1. Select **Search > Scheduled Searches**.
2. Select the searches that you want to enable or disable.
3. Select **Enable** or **Disable**.
The **Status** column, if selected in the **Manage Columns** option, displays the status of either **Enabled** (green) or **Disabled** (red).

Managing Completed Runs of a Scheduled Search

You must have the Scheduled Search permission to schedule searches.

Select **Search > Scheduled Searches > Completed**.

After creating a [scheduled search](#), you can view, delete, export, and filter the **completed runs** of that search. The results of a completed run are immutable. That is, if you edit the settings or query of a completed run, your changes do not affect the original results stored in the Completed list of scheduled searches.

- ["Viewing a Completed Run of a Scheduled Search" below](#)
- ["Deleting Completed Runs of a Scheduled Search" on the next page](#)
- ["Exporting Completed Runs of a Scheduled Search" on the next page](#)

Viewing a Completed Run of a Scheduled Search

You must have the Scheduled Search permission to schedule searches.

Select **Search** > **Scheduled Searches** > **Completed**.

The name of a completed run represents the name of the scheduled search name plus its start date and time.

When a run is in progress, Search displays the number of events received thus far and when the last chunk of data was received. Also, a flag beside the name of a completed run indicates that the settings for that scheduled search were changed before this run.

In the **Completed** tab, you can perform the following actions:

View all details for a completed schedule search

To view completed search results, click the **Eye** icon beside the search name.

Sort the data in columns

To change the sort order, click the **column heading**.

Reorder columns

To rearrange the order of the columns, drag each column to new position.

Search for a search keyword

To find a keyword, click in the field next to the **Magnifying Glass** icon (Search Keyword), enter a value, and the system displays your results automatically.

Hide and display columns

To hide and display a column, in the far right-corner of the window, click the **Wrench** icon (Manage Columns), and then select and clear the column name checkboxes.

Filter the data in columns

To filter scheduled searches based on *Status* and *Fieldset*, select the corresponding filter parameter. You can also filter completed scheduled searches based on a time range (custom and preset).

To filter the data for more specific results, in the far right-corner of the window, click the **Funnel** icon (Filters), and then select and clear the filter options. To filter the results based on execution time, set the date picker filter in the far right corner.

Create a report based on the run results

Each completed run has a unique [Search Results ID](#), which allows you to create a report based on the search results.

To copy the ID, [view](#) the search results. Then either copy the ID from the URL or select the **Copy** icon above the Events table. To complete the process, follow the steps in [Build a Report Using Search Results](#).

Deleting Completed Runs of a Scheduled Search

You can delete a completed run of a scheduled search at any time.

To delete a search:

1. Select **Search > Scheduled Searches > Completed**.
2. Select the completed runs that you want to delete.
3. Click the **delete** icon.

Exporting Completed Runs of a Scheduled Search

You can export the completed run of a scheduled search to CSV format.

To export a search:

1. Select **Search > Scheduled Searches > Completed**.
2. Click the **CSV** icon next to the name of the scheduled search that you want to export.
3. Alternatively, view the search, then select the **CSV** icon to export the results.

Chapter 4: Understanding the Search Parameters

To search for events or alerts, you specify the [query input](#), the [search result fields](#), and the [time period](#). The query input determines the search type (full text, natural language, or contextual). As you specify the criteria for a search query, Search suggests search items and operators based on a schema data dictionary. You can also choose from predefined queries and specify default settings.

In the search query, you can enter the alias, or abbreviated term, for a field name rather than entering the full name. For the fields shown in the following table, you can also use the **presentable field names**, such as Agent Address. Search suggests presentable names.

- ["Understanding the Types of Search Queries" below](#)
- ["Using GlobalEventID in a Query" on page 32](#)
- ["Understanding the Query Syntax, Operators, and Functions" on page 33](#)
- ["Specifying a Group of Fields" on page 45](#)
- ["Specifying an Alias for a Field" on page 46](#)
- ["Specifying IP Addresses and Subnets" on page 50](#)
- ["Including a Storage Group's Filter in the Search Query" on page 52](#)
- ["Extending the Search with a Lookup List" on page 53](#)
- ["Using Specific Sets of Fields for Search Results" on page 55](#)
- Use the Search Functions
- ["Configuring the Time Range" on page 59](#)
- ["Configuring Preferred Settings for Searches " on page 62](#)

Understanding the Types of Search Queries

Search supports the following types of search queries:

- ["FULL TEXT SEARCH" on the next page](#)
- ["FIELD-BASED SEARCH" on the next page](#)
- ["HASHTAG \(predefined searches\)" on the next page](#)

FULL TEXT SEARCH

Searches across all columns using a 'contains' operation to determine if the value is found.

Syntax	Example
<value>	ssh

FIELD-BASED SEARCH

Searches based on the field and operator designation to determine if the value is found in the specified field.

Your search can reference fields with the Unified Schema to either retrieve the field in results, apply a filter criteria or create a user defined expression. The **Unified Schema** defines a consistent event model that can be used across all of ArcSight family of products.

Syntax	Example
<key> <operator> <value>	sourceAddress = 10.0.111.5

HASHTAG (predefined searches)

The Search feature includes several predefined queries out-of-the-box. In the query field, enter a hashtag, and then select the criteria to use. In addition to these predefined searches, you can use the session searches and save searches in the input field using a hashtag prefix.

This predefined query...	Uses this search criteria...
#Configuration Changes	categoryBehavior = /Modify/Configuration AND categoryOutcome = /Success
#DGA Events	deviceCustomNumber1 >= 1 AND deviceCustomNumber1Label contains DNS
#DNS Events	deviceEventCategory = PACKET
#DoS Events	#Category Technique = /DoS
#ESM Correlation Events	Type=Correlation

#Failed Logins	Category Behavior = /Authentication/Verify AND categoryOutcome != /Success
#Failed Logins For User \$Username	Category Behavior = /Authentication/Verify AND categoryOutcome != /Success for user <username>
#Firewall Events	categoryDeviceGroup = /Firewall
#Firewall Drop	categoryDeviceGroup = /Firewall AND categoryObject starts with /Host/Application/Service AND (categoryBehavior starts with /Access OR categoryBehavior = /Communicate/Query) AND categoryOutcome = /Failure
#Firewall Drop For \$Ip	categoryDeviceGroup = /Firewall AND categoryObject starts with /Host/Application/Service AND (categoryBehavior starts with /Access OR categoryBehavior = /Communicate/Query) AND categoryOutcome = /Failure for <IP_address>
#Malicious Code Activity	categoryObject STARTS WITH /Vector, /Host/Infection, /Host/Application/Malware OR categoryObject = /Host/Application/DoS Client, /Host/Application/Backdoor OR categoryTechnique STARTS WITH /Code
#MITRE ATT&CK Events	Device Custom String1 Label ='MITRE ID'
#Proxy Events	Category Technique=/Proxy
#SSH Authentication	categoryBehavior = /Authentication/Verify AND destinationUserName != Null and contains ssh
#VPN Connections	categoryDeviceGroup = /VPN AND Category Behavior = /Authentication/Verify AND categoryOutcome = /Success AND destinationUserName != Null
#Vulnerabilities Events	Category Technique= /scanner/device/vulnerability
#Windows Account Creation	deviceVendor = Microsoft AND deviceEventClassId = Microsoft-Windows-Security-Auditing:4720, Security:624
#Windows New Service Created	(deviceEventClassId='Microsoft-Windows-Security-Auditing:4697' or deviceEventClassId=' Service Control Manager:7045') and deviceProduct='Microsoft Windows'

Using GlobalEventID in a Query

To help you identify an event that might be seen by multiple ArcSight components, the connectors assign the event a unique 64-bit ID. To include a GEID in your search query, enter globalEventID. You can view the GEID of the event in the Event Details.

Syntax	Example
<geid> <value>	global event id= 2864991913017849867

For events to have a GEID, use ArcSight Management Center to configure connectors to include the ID. For more information, see the [Administrator's Guide to ArcSight Platform](#) or the guide for the connector.

Understanding the Query Syntax, Operators, and Functions

Search supports a variety of search operators and functions. The search query bar automatically displays related fields and operators as you enter your query.

For example, type the word “domain” to see all available fields that might contain that string or name.

Type an integer like “22”, and Search displays a list of fields to choose from, such as Destination Port, Source Port or “any port.”

You can also specify a storage group in the query.

- ["Understanding the Query Syntax Requirements" below](#)
- ["Understanding the Search Query Functions and Operators" on page 35](#)
- ["Understanding the Functions for Building Eval Expressions" on page 37](#)

Understanding the Query Syntax Requirements

Depending on the [type of search](#) you create, the query must meet the requirements listed in the following table. Also, Search treats a comma (,) between search items and values as an **OR** operator.

By default, Search is case-sensitive to support faster performance. However, you can instruct the database to support case-insensitive searches. For more information, see the [Administrator's Guide to ArcSight Platform](#).

Type	Full-text	Field-based	Hashtag (predefined)
Case sensitivity	Case-sensitive	Case-sensitive	Case-insensitive

Exact Match	<p>Keyword treated as keyword*.</p> <p>Example: /Execute matches: /Execute, /Execute/Start, /Execute/Response,/Execute/Query</p>	<p>Enclose value in double quotes.</p> <p>Example: Category Behavior ="/Execute"</p>	n/a
Nesting, including parenthetical clauses, such as (a OR b) AND c	<p>Allowed</p> <p>Use Boolean operators to connect and nest keywords.</p>	<p>Allowed</p> <p>Use Boolean operators to connect and nest keywords.</p>	<p>Allowed</p> <p>Use Boolean operators to connect and nest keywords.</p>
Implicit Operators	<p>When you enter two values separated by a space, this is treated as an implicit AND condition.</p> <p>Example: ssh fail</p>	<p>The AND/OR treatment depends on the operator used in the search.</p> <p>For example, destinationAddress = 1.1.1.1, 2.2.2.2 is equivalent to destinationAddress = 1.1.1.1 or destinationAddress = 2.2.2.2 ,</p> <p>while the query destinationAddress != 1.1.1.1, 2.2.2.2 is equivalent to destinationAddress != 1.1.1.1 and destinationAddress != 2.2.2.2</p>	n/a
List Operations	n/a	<p>Performs an inner join or a left join against a custom list.</p> <p><i>Syntax for an Inner Join:</i> source address in list CustomListName_CustomColumnName</p> <p><i>Syntax for a Left Join:</i> source address not in list CustomListName_ CustomColumnName</p>	n/a

Time Format (when searching for events that occurred at a particular time)	No specific format The query needs to contain the exact timestamp string. Example: "10:34:35"	YYYY-MM-DD YYYY-MM-DD HH:mm YYYY-MM-DD HH:mm:ss.fff To narrow the time range, use the following operators: <ul style="list-style-type: none"> • in between (><) • greater than (>) • less than (<) 	n/a
Special Characters: \ * ' "	Use the backslash (\) as an escape character.	Use the backslash (\) as an escape character.	n/a
Wildcard	Can appear anywhere in the value. Examples: *log log* lo*g* Searches for ablog, blog, long, etc.	Can appear anywhere in the field. Examples: name=*log Searches for ablog, blog, etc. in name field name="*log" name=*log Both search for *log	n/a
Escape a Wildcard Character	Can search for * by escaping the character. Example: log*	Can search for * by escaping the character. Example: log*	n/a

Understanding the Search Query Functions and Operators

You can specify the following search operators in the query:

Operator	Alternative Operator	Examples
AND		#Firewall drop and sourceAddress equals 10.0.112.9 sourceAddress equals 10.0.112.9 and destinationAddress = 10.0.116.148
OR		fail OR ssh destinationAddress = 10.0.111.5 OR destinationAddress=10.0.116.148 destinationAddress =10.0.111.5, 10.0.116.48
not equal	<> !=	destinationPort not equal 21
equals	= == is equal to equal	name equals INVALID password device vendor equals CISCO
greater than	> is greater	bytes In greater than 100
less than	< is less is lower less	bytes out less than 1000
greater equal than	>= gte greater equal	End Time greater equal than 2017-07-25 End Time greater equal than 2017-07-25 09:07 End Time greater equal than 2017-07-25 09:07:43 End Time greater equal than 2017-07-25 09:31:22.685
less equal than	<= lte less equal	Base Event Count less equal than or equal 50
starts with	startswith	message starts with FIN
does not start with		name does not start with FIN
ends with	endswith	message ends with out
does not end with		message does not end with out
contains	contain like has substring	name contains TCP

does not contain	does not have	name does not contain TCP
in list	match in list of	device vendor equals CISCO and source address in list customListName_ customColumnName device vendor equals CISCO and source address in list badGuyIpList_ badGuyIp
not in list	not match not in list of	source address not in list customListName_ customColumnName source address not in list badGuyIpList_ badGuyIp
in subnet	n/a	source address in subnet 10.0.0.0/8
not in subnet	n/a	source address not in subnet 10.0.0.0/8
 (Pipeline operator)	n/a	Combine various search functions separated by the operator: ssh eval test1 = abs (40) ssh eval test1 = sin (Bytes In)
eval <expression> name	n/a	eval URL_Length = length (Request URL)
rename	n/a	rename source address as NewSourceAddress
where	n/a	where Bytes In >= 3000 where Category Outcome = /Success

Understanding the Functions for Building Eval Expressions

The Eval function allows you to define and name an expression that is returned in the search. To build an eval expression, you can use the following functions:

- ["Comparison and Conditional Functions" on the next page](#)
- ["Cryptographic Function" on the next page](#)
- ["Informational Function" on the next page](#)
- ["Mathematical Functions" on page 39](#)
- ["Statistical Functions" on page 41](#)

- ["Text Functions " on page 42](#)
- ["Trigonometry Functions" on page 44](#)

Comparison and Conditional Functions

Function	Description	Example
coalesce(X [, Y, Z,N, ...])	<p>Returns the value of the first non-null expression in the list. If all expressions evaluate to null, then COALESCE returns null. The list is up to 20 elements long.</p> <p>In the list of expressions, all elements must be of same type.</p> <p>The only supported types are numeric and string. X can be a number, field or expression.</p>	<p>... eval username = coalesce (Source Username, Destination Username)</p> <p><i>Returns: 2</i></p>
nullif(X,Y)	<p>Compares two expressions. If the expressions are not equal, the function returns the first expression (expression1). If the expressions are equal, the function returns null.</p> <p>X and Y can be a number, field or expression. Y must have same data type that X.</p>	<p>... eval newField = nullif(2, 3)</p> <p><i>Returns: 2</i></p> <p>... eval newField = nullif(2, 2)</p> <p><i>Returns: null</i></p>

Cryptographic Function

Function	Description	Example
md5(X)	<p>Calculates the MD5 hash of string, returning the result as a string in hexadecimal.</p> <p>X must be a string.</p>	<p>... eval usermd5 = md5 (Destination Username)</p> <p><i>Returns:</i> 202cb962ac59075b964b07152d234b70</p>

Informational Function

Function	Description	Example
isnull(X)	Returns true if the X is null otherwise returns false.	<p>... eval newField = isnull(2)</p> <p><i>Returns: false</i></p>

Mathematical Functions

Function	Description	Example
abs(X)	Takes a number, X, and returns its absolute value. X can be a number, field or expression.	The function assigns the evaluated value to the new field. If the value of X is 3 or -3, the function assigns the evaluated value of 3 to the field absnum: ... eval absnum=abs(number) ... eval absnum = abs(bytesIn) ... eval absnum = abs(1 - bytesIn)
cbrt(X)	Takes one numeric argument, X, and returns its cube root.	... eval n=cbrt(2) <i>Returns: 8</i>
ceiling(X)	Rounds a number, X, up to the next highest integer. X can be a number, field or expression.	... eval n=ceil(1.9) ... eval n=ceiling(1.9) <i>Returns: n=2</i>
exp(X)	Takes a number, X, and returns eX. X can be a number, field or expression.	... eval y=exp(3) <i>Returns: y=20.0855369231877</i>
floor(X)	Rounds a number, X, down to the nearest whole integer. X can be a number, field or expression.	... eval n=floor(1.9) <i>Returns: 1</i>
mod(X, Y)	Returns the modulo of X and Y. (X%Y; the remainder of X divided by Y.)	... eval newField = mod(25,10) <i>Returns: 5</i>
ln(X)	Takes a number, X, and returns its natural log. X can be a number, field or expression.	... eval lnBytes=ln(bytesIn) <i>Returns: the natural log of the value of "bytesIn". If "bytesIn" contains 100, returns 4.605170186.</i>

Function	Description	Example
log(X, Y)	Returns the logarithm to the specified base of the argument. X is the base and Y can be a number, field or expression. X is optional. If not specified, it will take 10 as the default value.	... eval test1= log (10,2) <i>Returns:</i> 0.301 ... eval test1 = log (2) <i>Returns:</i> 0.301 as it takes the default base as 10
log10(X)	(Evaluates the log of number X with base 10. X can be a number, field or expression.	... eval num=log10(10000) <i>Returns:</i> 4
power (X,Y)	Returns a value representing one number raised to the power of another number. X is the base and Y the exponent. X and Y can be a number, field or expression.	... eval newField = power(2, 3) <i>Returns:</i> 8
round(X, Y)	Rounds X to the nearest integer. Y is the precision to use, if omitted the default precision is zero. X can be a number, field or expression. Y is a numeric value to indicate the precision.	... eval n=round(1.4) <i>Returns:</i> 1 ... eval n=round(1.5) <i>Returns:</i> 2
sign(X)	Returns a value of -1, 0, or 1 representing the arithmetic sign of the argument.	... eval newField = sign(-8.4) <i>Returns:</i> -1 ... eval newField = sign(4) <i>Returns:</i> 1 ... eval newField = sign(0) <i>Returns:</i> 0
sqrt(X)	Takes one numeric argument, X, and returns its square root. X can be a number, field or expression.	... eval n=sqrt(9) <i>Returns:</i> 3
trunc(X,Y)	Returns the expression value truncated (toward zero). X can be a number, field or expression. Y is a numeric value to indicate the precision.	... eval newField = trunc(1.9) <i>Returns:</i> 1 ... eval newField = trunc(2.89999, 2) <i>Returns:</i> 2.89

Statistical Functions

Function	Description	Example
greatest(X,Y [,Z,N, ...])	<p>Returns the largest value in a list of expressions. The list is up to 20 elements long.</p> <p>In the list of expressions all elements must be of same type.</p> <p>The only supported types are numeric and string. X can be a number, field or expression.</p>	<p>... eval newField = greatest(7, 5, 9)</p> <p><i>Returns: 9</i></p> <p>... eval newField = greatest ('sit', 'site', 'sight')</p> <p><i>Returns: site</i></p> <p>... eval newField = greatest (bytesIn, 100)</p> <p><i>Returns: 100, when bytesIn is less than 100</i></p>
least(X,Y[,Z,N, ...])	<p>Returns the smallest value in a list of expressions. The list is up to 20 elements long.</p> <p>In the list of expressions all elements must be of same type.</p> <p>The only supported types are numeric and string. X can be a number, field or expression.</p>	<p>... eval newField = least (bytesIn, bytesOut)</p> <p><i>Returns: 5</i></p> <p>... eval newField = least('sit', 'site', 'sight')</p> <p><i>Returns: sight</i></p> <p>... eval newField = least (bytesIn, 100)</p> <p><i>Returns: 100, when bytesIn is greater than 100</i></p>
randomint(X)	<p>Returns a random number between 0 and X-1.</p> <p>X can be any positive integer between the values 1 and 9,223,372,036,854,775,807.</p>	<p>... eval newField = randomint (10)</p> <p><i>Returns: a random number between 0 and 9</i></p>

Text Functions

Function	Description	Example
length(X)	Returns the character length of a string, X.	<pre>... eval n=length(field)</pre> <p><i>Returns:</i> the length of (field). If the field is 256 characters long, it returns n=256.</p> <pre>... eval n=length("abc")</pre> <p><i>Returns:</i> n=3 (abc is a literal string, surrounded by double quotes)</p>
lower(X)	Takes a string argument, X, and returns the lowercase version.	<pre>... eval name=lower("USERNAME")</pre> <pre>... eval name=tolower("USERNAME")</pre> <p><i>Returns:</i> the value of the field username in lowercase. If the username field contains FRED BROWN, it returns name=fredbrown.</p>

Function	Description	Example
substr (X,Y,Z)	<p>This function returns a new string that is a substring of string X.</p> <p>The substring begins with the character at index Y and extends up to the character at index Z-1.</p> <p>The index is a number that indicates the location of the characters in string X, from left to right, starting with zero.</p> <p>Y can be negative.</p> <p>Z cannot be negative.</p>	<p>... eval n=substr("ArcSight", 5, 6) <i>Returns: "g"</i></p> <p>... eval n=substr("ArcSight", 2, 6) <i>Returns: "cSig"</i></p> <p>... eval n=substr("ArcSight", 0, 3) <i>Returns: "Arc"</i></p>
trim(X) ltrim(X) rtrim(X)	<p>trim(X) removes all spaces from both sides of the string X.</p> <p>ltrim(X) removes all spaces from the left side of the string X.</p> <p>rtrim(X) removes all spaces from the right side of the string X.</p>	<p>For the sake of these examples, assume that X is a literal string and _ represents any number of space characters.</p> <p>... eval trimmed=ltrim("_string_") <i>Returns: trimmed="string_"</i></p> <p>... eval trimmed=rtrim("_string_") <i>Returns: trimmed="_string"</i></p> <p>... eval trimmed=trim("_string_") <i>Returns: "string"</i></p>
upper(X)	<p>Takes one string argument and returns the uppercase version.</p>	<p>... eval name=upper("username")</p> <p>... eval name=toupper("username")</p> <p><i>Returns: the value of the field username in uppercase. If username contains fred brown, it returns name=FRED BROWN.</i></p>

Trigonometry Functions

Function	Description	Example
$\text{acos}(X)$	Takes one numeric argument, X , and returns its trigonometric inverse cosine.	... eval newField = acos(0.3) <i>Returns:</i> 1.2661036727795
$\text{asin}(X)$	Takes one numeric argument, X , and returns its trigonometric inverse sine.	... eval newField = asin(3) <i>Returns:</i> 0.304692654015398
$\text{atan}(X)$	Takes one numeric argument, X , and returns its trigonometric inverse tangent.	... eval newField = atan(3) <i>Returns:</i> 0.291456794477867
$\text{atan2}(X,Y)$	Returns a value representing the trigonometric inverse tangent of the arithmetic dividend of the arguments.	... eval newField = atan2(2,1) <i>Returns:</i> 1.10714871
$\text{cos}(X)$	Takes one numeric argument, X , and returns its trigonometric cosine.	... eval newField = cos(3) <i>Returns:</i> 2435538
$\text{cosh}(X)$	Takes one numeric argument, X , and returns its hyperbolic cosine.	... eval newField = cosh(3) <i>Returns:</i> 10.0676619957778
$\text{cot}(X)$	Takes one numeric argument, X , and returns its trigonometric cotangent.	... eval newField = cot(3) <i>Returns:</i> - 7.01525255143453
$\text{sin}(X)$	Takes one numeric argument, X , and returns its trigonometric sine.	... eval newField = sin(3) <i>Returns:</i> 0.141120008059867

Function	Description	Example
<code>sinh(X)</code>	Takes one numeric argument, X, and returns its hyperbolic sine.	<pre>... eval newField = sinh(3)</pre> <p><i>Returns:</i> 10.0178749274099</p>
<code>tan(X)</code>	Takes one numeric argument, X, and returns its trigonometric tangent.	<pre>... eval newField = tan(3)</pre> <p><i>Returns:</i> - 0.142546543074278</p>
<code>tanh(X)</code>	Takes one numeric argument, X, and returns its hyperbolic tangent.	<pre>... eval newField = tanh(3)</pre> <p><i>Returns:</i> 0.99505475368673</p>

Specifying a Group of Fields

Search enables you to quickly select fields that have common groupings. In the query, you can specify a **group alias** that displays all fields or columns associated with the group. The following table provides some common group aliases.

Group Alias	Includes a list of these fields or columns...
<code>category</code>	All category fields
<code>custom float</code>	All custom float fields
<code>domain</code>	All domain fields
<code>hostname</code>	All hostname columns
<code>id</code>	All ID columns
<code>ip</code>	All IP address columns
<code>ip6</code>	All IPv6 address columns
<code>label</code>	All label columns
<code>mac</code>	All MAC address columns
<code>path</code>	All path columns
<code>port</code>	All port columns
<code>timestamp or time</code>	All time columns (device receipt time, agent receipt time)

Group Alias	Includes a list of these fields or columns...
uri	All URI columns
url	All URL columns
username or user	All user columns

Specifying an Alias for a Field

In the search query, you can enter the alias, or abbreviated term, for a field name rather than entering the full name. For the fields shown in the following table, you can also use the **presentable field names**, such as Agent Address. Search suggests presentable names.

Field	Aliases
agentAddress	agt agent ip
agentHostName	ahost
agentId	aid
agentMacAddress	amac agent mac
agentReceiptTime	art
agentTimeZone	atz
agentTranslatedAddress	agent translated ip
agentType	at
agentVersion	av
applicatonProtocol	app protocol
baseEventCount	cnt
bytesIn	in
bytesOut	out
categoryBehavior	behavior
categoryDeviceGroup	device group
categoryObject	object

Field	Aliases
categorySignificance	significance
categoryTechnique	technique
destinationAddress	dst destination ip destinationip dst ip dest ip target ip targetip target
destinationHostName	dhost destination name
destinationMacAddress	dmac destination mac
destinationNtDomain	dntdom
destinationPort	dpt destination port dstport dest port targetport target port
destinationProcessId	dpid
destinationProcessName	dproc
destinationTranslatedAddress	destination translated ip
destinationuserId	duid

Field	Aliases
destinationUserName	duser dst user dest user destination user dst usr
destinationUserPrivileges	dpriv
deviceAction	act
deviceAddress	dvc deviceaddr deviceip device ip
deviceCustomFloatingPoint <i>n</i> Valid values for <i>n</i> are integers between 1 and 4 For example: deviceCustomFloatingPoint1	cfp <i>n</i> For example: cfp1
deviceCustomFloatingPoint <i>n</i> Label Valid values for <i>n</i> are integers between 1 and 4 For example: deviceCustomFloatingPoint1Label	cfp <i>n</i> Label For example: cfp1Label
deviceCustomIPv6Address <i>n</i> Valid values for <i>n</i> are integers between 1 and 4 For example: deviceCustomIPv6Address2	c6a <i>n</i> device custom ipv6 <i>n</i> For example: c6a2
deviceCustomIPv6Address <i>n</i> Label Valid values for <i>n</i> are integers between 1 and 4 For example: deviceCustomIPv6Address2Label	c6a <i>n</i> Label For example: c6a2Label
deviceCustomNumber <i>n</i> Valid values for <i>n</i> are integers between 1 and 3 For example, deviceCustomNumber3	cn <i>n</i> For example: cn3

ArcSight Recon as a Service 1.3 User Guide
 Chapter 4: Understanding the Search Parameters

Field	Aliases
deviceCustomNumber <i>n</i> Label Valid values for <i>n</i> are integers between 1 and 6 For example: deviceCustomNumber6Label	cn <i>n</i> Label For example: cn6Label
deviceCustomString <i>n</i> Valid values for <i>n</i> are integers between 1 and 6 For example: deviceCustomString5	C <i>n</i> For example: Cs5
deviceEventCategory	cat
deviceHostName	dvchost
deviceMacAddress	dvcmac device mac
deviceProcessId	dvcpid
deviceReceiptTime	rt
deviceTimeZone	dtz
deviceTranslatedAddress	device translated ip
endTime	end
eventOutcome	outcome
fileNme	fname
fileSize	fsize
message	msg
requestUrl	request URL
sourceAddress	src source ip sourceip src ip
sourceHostName	shost
sourceMacAddress	smac source mac

Field	Aliases
sourceNtDomain	sntdomain
sourcePort	spt srcport src port
sourceProcessId	spid
sourceProcessName	sproc
sourceTranslatedAddress	source translated ip
sourceUserId	suid
sourceuserName	suser src user source user src usr
sourceUserPrivileges	spriv
startTime	start
transportProtocol	proto

Specifying IP Addresses and Subnets

Your query can include IPv4, IPv6, and MAC addresses.

- ["Understanding How Search Stores IP and MAC Addresses" below](#)
- ["Entering an IP or MAC Address" on the next page](#)

Understanding How Search Stores IP and MAC Addresses

Search stores IPv4, IPv6, and MAC addresses in a format that provides search flexibility and enables you to perform the following actions:

Compare IP addresses for optimum performance

For example, Agent Address > 192.10.11.12.

Specify a range of IP addresses

For example, you can enter the following types of queries:

- Agent Address in between 192.2.13.1 and 192.2.13.11
- Source Address greater equal than 192.10.11.12
- Destination Address less than 192.112.98.33

Use abbreviated input search notation

You can enter the following types of queries:

- To specify IP addresses in the subnet starting with a particular value:
Agent Address in subnet 192.*
- To specify an IPv4 address in a subnet that uses CIDR notation. The first eight bits are the network part of the address, leaving the last 24 bits for specific host addresses.
Agent Address in subnet 192.0.0.0/8
- To specify an agent address in a subnet that uses CIDR notation. The first 24 bits are the network part of the address, leaving the last 40 bits for specific host addresses.
Agent Address in subnet 2001:0db8:0000:0000:0000:ff00:0042:8329/24

Search stores MAC addresses in their original format.

Entering an IP or MAC Address

You can enter IP addresses in the following formats:


- aa:aa:aa:aa:aa:aa
- aa-aa-aa-aa-aa-aa

The following table lists the query format and examples for the type of IP address.

Type of address	Format in a query...	Examples
IPv4	a.b.c.d	a.* a.b.* a.b.c.* a.b.c.d/8
IPv6	Full form	2001:0db8:0000:0000:0000:ff00:0042:8329
	Canonical form without leading zeroes in each group	2001:db8:0:0:0:ff00:42:8329
	Canonical form without consecutive sections of zeroes	2001:db8::ff00:42:8329
IPv6 in a subnet	Include CIDR notation	2001:0db8:0000:0000:0000:ff00:0042:8329 2001:0db8:0000:0000:0000:ff00:0042:8329/24 2001:db8::/32
		NOTE: For the 2001:db8::/32 format, you can omit part of the IPv6 address, depending on the subnet that you are querying.
MAC	a:b:c:d:e:f	94:18:82:6D:63:74
	a-b-c-d-e-f	94-18-82-6D-63-74

Including a Storage Group’s Filter in the Search Query

Search allows you to include a [storage group](#) in a query. For example, you have a storage group called *Firewall Events* that has the following query: `categoryDeviceGroup='/Firewall'` or `categoryDeviceGroup='/IDS'`. Rather than entering that query again in Search, specify the following for your Search query: `storageGroup=Firewall Events`.



IMPORTANT: For best results, specify the storage group at the beginning of the Search query.

Extending the Search with a Lookup List

Select **Configuration** > **Lookup Lists**.

You can create CSV files, or **lookup lists**, that enables the **Search feature** to create additional tables with different fields and store them in the database. You can add lookup list fields to [fieldsets](#) and use them in search queries.

- ["Understanding Considerations for the Lookup List File" below](#)
- ["Creating a Lookup List " below](#)
- ["Replacing a Lookup List " on the next page](#)
- ["Deleting a Lookup List " on page 55](#)

Understanding Considerations for the Lookup List File

The CSV file for your lookup list must meet the following requirements:

- The first row must be a comma-separated list of field names.
- The field names cannot exceed 40 characters. The names can only contain alphanumeric characters and underscores. They must start with an alpha character.
- The remaining rows must be comma-separated values for the fields in the first row.
- All rows must contain the same number of values.
- You must select one of the columns as the key field, and the values of the key field must be unique.
- The **key field** is the field that you can use with the `in list` operator in queries.
- The file cannot exceed 25 fields and 2 million rows.
- The file cannot exceed 150 MB.

Creating a Lookup List

1. Select **Configuration** > **Lookup Lists**.
2. Select **Add**.
3. Drag-and-drop your [CSV file](#) to the **Lookup Lists** page or select **Browse** to navigate to the file.

- Specify a name for the lookup list.
Once created, you cannot change the name of the lookup list. The name must meet the following requirements:
 - Does not exceed 20 characters
 - Contains only alphanumeric characters and underscores
 - Starts with an alpha character
- Specify the [key field](#), then either accept the recommended value type or specify a different one. The following are possible values:

Value type	Specifies
domain	The name of the lookup list.
float	A number whose radix point can be placed anywhere relative to the significant digits of the number
hostname	Fully qualified domain name
int	Integer value
ipv4	IPv4 address
ipv6	Ipv6 address
mac	MAC address
short text	Text that cannot exceed 1K of space
long text	Text that cannot exceed 4K of space
time	Time stamp
url	A URL address that cannot exceed 4K
username	A string type

- To upload the file as a table in the database, select **Upload**.

Replacing a Lookup List

Replacing the contents of a lookup list does not affect queries that use the original lookup list. You cannot change the name of a lookup list. The field names in the replacement file must match the field names in the original file.

To replace the list:

1. Select **Configuration > Lookup Lists**.
2. Select the list you want to replace.
3. Click the **eye** icon on the left side of the selected lookup list.
4. Select **Replace**.
5. Select the CSV file you want to use to replace the contents of the existing lookup list.

Deleting a Lookup List

1. Select **Configuration > Lookup Lists**.
2. Select the list you want to delete.
3. Select the **Trash can** icon.

Using Specific Sets of Fields for Search Results

*You must have the **Create Fieldsets** permission.*

You can specify a **fieldset** that determines a group of search result fields the system displays in the [Events table](#). In the table, each field can provide the ten most and less common values. Multiple searches can share a fieldset, and new searches display a default fieldset that contains the most common event fields. Use the fieldsets window to view and add the customize and system fieldsets, including [lookup lists](#).

- **System:** Predefined fieldsets provided by the system.
- **Custom:** Customize the default fieldsets and lookup list fields for individual purposes.

New searches display the user's default fieldset. These will remain selected in the fieldsets drop-down even when moving to other search tabs. If you select another fieldset, the popup window closes, displaying the new option. A message will display allowing you to revert the change to the previously selected fieldset.



NOTE: Whenever you replace or update the fieldset, your search becomes out of sync, since the fields shown might differ from the new selection. Rerun the search with the new selection to correct this.

- ["Viewing and Creating Fieldsets" below](#)
- ["Creating a Fieldset " below](#)
- ["Editing a Fieldset " on the next page](#)
- ["Deleting a Fieldset" on page 58](#)
- ["Cloning a Fieldset" on page 59](#)

Viewing and Creating Fieldsets

To access the fieldsets window, from the **Search** page, click the fieldset located at the left of the time range selector. By default, the system displays the name of the last used fieldset. You can also perform the following actions:

- Filter fieldsets by lists
- Search fieldsets by name or specific field

You can designate a fieldset as your [preferred default](#). The fieldset will only be used for your search results and will not affect other users connecting to the same system.

1. From the **Search** page, click the fieldset shown to the left of the time range selector.
2. Click **Manage Fieldsets**.
The Manage Fieldsets window displays.
3. Click **+**.
The Create Fieldset window displays.
4. To view the complete list of available fieldsets, click the **filter** icon.
 - Recently Created Fieldsets
 - My Fieldsets
 - Recently Updated Fieldsets
 - All Fieldsets

Creating a Fieldset

1. From the **Search** page, click the fieldset name (at the left of the time range selector).
2. From the fieldsets window, click **Create Fieldsets**.
3. Click **+** to add a new fieldset.

4. Select or deselect the options, including lookup fields.
 - a. Drag and drop any field to the **Selected Fields** column. Otherwise, select **Text Editor** to enter the fields that you need.
 - b. To locate a specific field, use the search field.



NOTE: The fieldset editor displays the coding-style name for search fields. For more information about which fields to choose or type, see "[A Mapping Database Names to their Appropriate Search Fields](#)" on page 140.

5. Specify a name for the new fieldset.
 - a. Each fieldset should have a unique name.
 - b. Fieldset names are not case sensitive.
6. To save the fieldset as default, select the checkbox at the bottom left corner. The fieldset is used only for your search results and does not affect other users connecting to the same system.
7. Click **Save**.
8. (Optional) Select **Apply** to this search to customize the original fieldset without overwriting or saving it.

This new option displays in the custom category as Custom. The temporary fieldset will not be visible to other users, and it will only remain available on that session. After you log out, the system removes the temporary fieldset. You can have one temporal custom fieldset at a time.
9. To execute the query again, click **Search**.

Editing a Fieldset

You can edit custom fieldsets only. You cannot modify system fieldsets, and you can only edit one fieldset at the time.

- "[Editing the Selected Fieldset](#)" below
- "[Editing a Different Fieldset](#)" on the next page

Editing the Selected Fieldset

1. From the **Search** page, click the fieldset shown to the left of the time range selector.
2. From the fieldsets window, select **Edit Fieldset**.

The **Edit Fieldset** window displays.

3. Drag and drop any field to the **Selected Fields** column. Otherwise, select **Text Editor** to write the fields you need.
4. To locate a specific field, use the **Search** field.
5. In the **Fieldset Name** field, update the fieldset name as needed.
6. Click **Save**.
7. (Optional) Select **Apply To This Search** to customize the existing fieldset without overwriting or saving it.
This option displays in the custom category as **Custom**. The temporary fieldset will not be visible to other users, and it will only remain available on that session. After you log out, the system removes the temporary fieldset. You can have one temporal custom fieldset at a time.

Editing a Different Fieldset

1. From the **Search** page, click the fieldset shown to the left of the time range selector.
2. Click **Manage Fieldsets**.
3. Select the fieldset checkbox.
4. Click the **edit** icon.
The Edit Fieldset window displays.
5. Drag and drop any field to the **Selected Fields** column. Otherwise, select **Text Editor** to write the fields you need.
6. To locate a specific field, use the **Search** field.
7. In the **Fieldset Name** field, update the fieldset name as needed.
8. Click **Save**.
9. (Optional) Select **Apply To This Search** to customize the existing fieldset without overwriting or saving it.
This option displays in the custom category as **Custom**. The temporary fieldset will not be visible to other users, and it will only remain available on that session. After you log out, the system removes the temporary fieldset. You can have one temporal custom fieldset at a time.

Deleting a Fieldset

You can delete a fieldset that you have [created](#). If you delete a fieldset that's used in an active search, Search changes the fieldset name to **Custom** for that search. You cannot

delete a system fieldset.

To delete a fieldset:

1. From the **Search** page, click the fieldset shown to the left of the time range selector.
2. Click **Manage Fieldsets**.
3. Select the fieldset checkbox.
4. Click the **delete** icon.
A confirmation pop-up window displays.
5. Click **Yes** to proceed.

Cloning a Fieldset

When you clone a fieldset, Search creates a copy of the existing fieldset under the shared fieldsets category. You can update the cloned fieldset and give it a different name.

To clone a fieldset:

1. From the **Search** page, click the fieldset shown to the left of the time range selector.
2. Click **Manage Fieldsets**.
3. Select the fieldset checkbox.
4. Click the **clone** icon.
The system adds the fieldset to the list.
5. To edit the fieldset, see "[Editing a Fieldset](#) " on page 57.

Configuring the Time Range

A search query can either have a fixed start and end date, where you cannot [refresh](#) data, or a time range that captures the most recent data. For example, if you choose the predefined **Last 30 minutes** setting, Recon updates data upon re-executing the search based on the most recent 30 minutes. Alternatively, you can create a [dynamic date range](#).

The time range that you specify in the time range selector is inclusive. Search includes the whole second as the end time. For example, if you specify a time range between *2018-01-01 12:00:00* and *2018-01-01 12:59:59*, Search includes all data from 2018-01-01 12:00:00.000 to 2018-01-01 12:59:59.999, inclusive.

- ["Specifying a Dynamic Date Range " below](#)
- ["Understanding Search Timestamps for Events" on the next page](#)
- ["Understanding How Time Zones Affect Search Results" on page 62](#)

Specifying a Dynamic Date Range

Search offers a flexible, dynamic setting for the time range where you can enter the desired time stamp without using the calendar to specify days, hours, and minutes. The dynamic date range uses the following syntax:

`<dynamic_time>`

or

`<dynamic_time> [+/- <units>]`

For example, to search for events that have occurred in the last two hours, you can specify `$Now - 2h` for **Start time** and `$Now` for **End time**. To find events that have occurred this week, you can enter `$CurrentWeek` for **Start time** and `$Now` for **End time**.

To enter a dynamic date range:

When viewing a search or starting a query, select the currently specified time range.

For the start or end time under **Custom Range**, select **Dynamic**.

To specify the **dynamic_time**, enter one of the following values:


Value	Represents
<code>\$Now</code>	The current minute
<code>\$Today</code>	Midnight of the current day
<code>\$CurrentWeek</code>	Midnight of the previous Monday (or same as <code>\$Today</code> if today is Monday)
<code>\$CurrentMonth</code>	Midnight on the first day of the current month
<code>\$CurrentYear</code>	Midnight on the first day of the current year

To specify the **units**, enter one of the following values:

Value	Represents
m (lowercase)	Minutes
h	Hours
d	Days
w	Weeks
M (uppercase)	Months

Understanding Search Timestamps for Events

Search can display results based on the timestamp associated with each event. The database stores three different timestamps for each event. For peak performance, Search automatically uses the Normalized Event Time setting. However, you can specify any timestamp setting for a search. You can also choose to make the timestamp the [default setting](#).

 **NOTE:** The Date Picker displays this Timestamp setting on when searching for events.

Type	Description
Database Receipt Time	Database Receipt Time (dBRT) represents the time when the database received the event. The database considers this timestamp as the <i>persisted time</i> of the event.
Device Receipt Time	Device Receipt Time (DRT) represents the time when the connected device claims the event occurred. This timestamp preserves the original time recorded by the device. However, this timestamp might not be credible in all cases. For example, it is possible that the time settings for the connected device are not configured correctly or the clock on the server that hosts the connected device might gain or lose time, which causes the timestamp to be out of sync with the actual time the event occurred.
Normalized Event Time	Normalized Event Time (NET) represents the best known time for an event. Ideally NET is the time when the connected device reported the event occurred (the DRT) because the device is the most direct known observer of the event occurrence. However, when the DRT for an event is not within a credible time range compared to the database’s time, NET represents the time when the database received the event (the dBRT). For example, the time on a connected device was configured incorrectly such that DRT for an event is May 29 1975 when the current date in the database when the database received the event is June 29 2020. The database recognizes that the event’s May 29 1975 timestamp for DRT is outside the credible time range. Based on the discrepancy with DRT, the database sets NET to June 29 2020 (same as the dBRT). By default, the DRT value must be within a boundary of -7 days in the past and +1 days in the future from the dBRT. To configure the boundary criteria, see the Administrator’s Guide to ArcSight Platform .

Understanding How Time Zones Affect Search Results

Searches for events in a time range are based on the [timestamps](#) of matching events and use the time zone of the local browser by default. You might need to account for the time zone offset from UTC and from other time zones, including Daylight Savings Time.

You can configure Search results to adjust the time for events to a [specific time zone](#). For example, it's possible that you might create a search while in a one time zone, then view the search from a different computer set to a different time zone. When this occurs, the [Events Timeline](#) converts the time segments to the specified time zone. If the [Events table](#) includes a time attribute, Search converts the time. However, the aggregation reflects the original time zone. For example, if the Events Timeline has seven bars in the original time zone, the number of bars could increase or decrease to reflect the currently specified time zone.

Configuring Preferred Settings for Searches

You can [specify the default settings](#) that you want to apply for new searches. For example, you might want all of your searches to return results from the last 24 hours.

Chapter 5: Checking the Integrity of Event Data

You must have the Perform Event Integrity Check permission to run a check.

Select **Admin** > **Event Integrity**.

When investigating an event or hunting for threats, users expect that the search results provide valid and accurate data. However, the data that you rely on could be compromised by users who want to hide their activities or maliciously change content. Data also is vulnerable to human errors, transfer errors, or loss and corruption caused by hardware or software issues.



NOTE: This feature searches Recon events only and does not include events migrated from Logger at this time.

To validate that the event information in your database matches the content sent from SmartConnectors, run an **Event Integrity Check**. When you run the check, Recon searches the database for [verification events](#) received within the specified date range, then runs a series of checks to compare content in the database with information supplied by the verification event. The results of an the Event Integrity Check help you identify whether event data might be compromised.

- ["Understanding Event Integrity Check" below](#)
- ["Running an Event Integrity Check" on the next page](#)
- ["Viewing Event Integrity Check Results" on page 65](#)
- ["Configuring Data Collection to Support Event Integrity Checks" on page 68](#)

Understanding Event Integrity Check

Event Integrity Check looks for base events referenced by verification events in the database. To have a **batch event**, you must [configure a SmartConnector](#) to generate the events, which will accompany each batch of base events sent to the database.

The base event includes a list of globally unique event IDs that match base events reference in the verification event to identify all base events with the batch. Each **base event** has its individual hash.

The crypto signature field in the verification event is a hash that represents the base events' hashes that the SmartConnector created for the verification event. The number of events in a batch depends on how you configure the batch size setting for each connector.

For each verification event, the Event Integrity Check performs the following actions:

- Looks for the [globally unique event ID \(GEID\)](#) of each base event referenced with the verification event.
Depending on the [Storage Group](#) configuration, some base events could have been intentionally deleted to comply with [data retention policies](#). When performing an event integrity check, the system will report these as missing base events.
- Generates hashes for the base events.
- Generates a hash to represent the base events' hashes in the sequence provided by the verification event. You might call this generated hash a hash of hashes.
- Compares the generated hash of hashes to the hash of hashes in the crypto signature field that the SmartConnector created for the verification event.

Running an Event Integrity Check

The **Event Integrity Check** feature looks for [verification events](#) received within the specified date range. To reduce the chance of false-negative results, Event Integrity Check searches for base events outside of the specified date range.

For example, you specify a date range of 29 May to 5 June. The check finds several verification events within the date range; however, Verification Event A was created on 29 May and includes base events that occurred on 28 May. To prevent the verification event from failing, Recon will expand the search for base events beyond the specified dates.



NOTE: The check process can take a long time if it includes large amounts of data. Therefore you should run the check during off-peak hours, and limit the date range to include only the data that you are interested in.

To run a check:

1. Select **Admin > Event Integrity**.
2. Specify the **Start Date** and **End Date**. The start time for the check corresponds to the time when you select Run. For example, 5:29 pm.
3. Select the [timestamp type](#).
4. Click **Run**. If the Run button is disabled, a check is running currently. You can run one check at a time only.

The **Status** updates and a spinner with the started on date and time and the date range for the check displays.
5. (Optional) To cancel the check, click **Cancel**. Run as needed.
6. [View the results](#).

Viewing Event Integrity Check Results

The **Event Integrity Check** feature provides the following status and results:

- ["Viewing the Event Integrity Check Status" below](#)
- ["Viewing Last Event Integrity Check Results Table" on the next page](#)

To view the results, select **Admin > Event Integrity**.



Event Integrity Check may display the last result from another user. The last result may also display after logging out.

Viewing the Event Integrity Check Status

The **Event Integrity Check status** displays the date range from which the results are currently being checked, as well as the current status, including:

New

Displays when you have never performed an Event Integrity check; therefore, no results display.

In Progress

Displays while the Event Integrity check is running. If the Run button is disabled, a check is running currently. You can run one check at a time only.

Canceling

Displays after you click Cancel when the Event Integrity check was in progress. Canceling might take time. While the status displays Canceling, you cannot run another Event Integrity check. The system displays Canceled when the system has finished canceling.

Canceled

Displays when you cancel an Event Integrity check and the system has completed the cancel task.

Completed

Displays after the Event Integrity check has completed successfully. The results display in the [results table](#).

Failed

Displays after the Event Integrity check did not complete due to an error.



NOTE: If there are no verification events in the selected date range, the Event Integrity check will be failed. Be sure Event Integrity is turned on in the SmartConnector.

Viewing Last Event Integrity Check Results Table



NOTE: Event Integrity Check may display the last result from another user. Log out to clear the last result.

The Last Event Integrity Check Results table displays the date range from the last check as well as the details of the last check, including:

Base events checked

Represents the number of [base events referenced by verification events](#) found in the specified date range.

Intact events

Represents the number of base events referenced by verification events that passed the Event Integrity [check](#).

Missing events

Represents the number of base events referenced by verification events where missing base events exist.

Tampering detected has been detected

Represents the number of base events referenced by verification events where the Event Integrity check failed to match the information provided by the verification events, such as due to a change in the data in the base event.

Missing hashes, incorrect hashes, or base events being out of sequence usually indicates that the data has been deliberately changed in an attempt to hide a user's activities.

Duplicate base event IDs

Represents the number of base events referenced by verification events where the Event Integrity check failed because more than one base event has a globally unique event ID. This situation results in the Event Integrity check of the referenced base events to fail.

Duplicate verification events IDs

Represents the number of base events referenced by verification events where the Event Integrity check failed because more than one verification event has a globally unique event ID.

Configuring Data Collection to Support Event Integrity Checks

The Event Integrity Check requires that you configure the SmartConnectors to include a verification event for each batch of events. This configuration ensures that the connector generates a verification event for the Raw Event field in the event.

The SmartConnector can create verification events for the Raw Event field in an event at the moment that your environment captures the event.

For the SmartConnector to support event integrity checks, configure the following settings:

For this setting	Enter
Preserve Raw Event	Yes NOTE:When you enable this setting, the size of each event increases, which will require more storage space in your database.
Event Integrity Algorithm	SHA-256
Check Event Integrity Method	Recon

For more information about configuring SmartConnectors, see the following documentation:

- [“Configuring Processing”](#) in the *Installation Guide for ArcSight SmartConnectors*
- [“Destination Runtime Parameters”](#) in the *Administrator Guide to ArcSight Platform*

II Hunting for Undetected Threats

To help you hunt for undetected threats, the **Reports Portal** includes a set of built-in dashboards and reports. You can view this content based on the tactics and standards established by MITRE, the Cloud Security Alliance, and OWASP. Additional report and dashboards focus on fundamental security issues, such as monitoring firewalls and malware. For rapid access to your regular dashboards, you can configure the Reports Portal to display those dashboards by default.

- ["Viewing Dashboards and Reports " on page 70](#)
- ["Understanding the MITRE ATT&CK" on page 73](#)
- ["Understanding the Cloud Security Dashboards and Reports" on page 80](#)
- ["Understanding the Foundation Dashboards and Reports" on page 92](#)
- ["Understanding the OWASP Security Dashboards and Reports" on page 103](#)

Chapter 6: Viewing Dashboards and Reports

Select **Reports > Portal**.

When you view the dashboards and reports, be aware that they are not persistent. Once you leave a report or dashboard, you must regenerate the view when you return to the page. If you choose to open a report in a new browser tab, you can leave that tab open to keep the dashboard or report active while you look at other dashboards or reports.

Many reports and dashboards contain pre-built queries. When you run a report or view a dashboard, it might prompt you to provide values for the run-time parameters. Reports also prompt for the start and end time of the data search.

You access the dashboards and reports from the [Reports Portal](#). In the portal, you can print or export the reports; schedule regular notifications of dashboard results; share reports on social media; and email the dashboard or report to others. You can also [configure](#) the Reports Portal to display specific dashboards by default.

- ["Viewing a Dashboard" below](#)
- ["Viewing a Report" on the next page](#)
- ["Specifying Default Dashboards for the Reports Portal" on the next page](#)

Viewing a Dashboard

When you open a dashboard, it automatically retrieves data from the last two hours. However, you can modify the time range as needed.

To view a dashboard:

1. Select **Reports > Portal > Repository > Standard Content**.
2. Expand the desired category, then select the [dashboard](#) that you want to view.
3. (Optional) To change the time range for the report, modify the start or end time parameters.

When you change the time range, the dashboard refreshes the data.

Viewing a Report

When you open a report, you must define the time range for the data you want to view.

To view a report:

1. Select **Reports > Portal > Repository > Standard Content**.
2. Expand the desired category, then select the [report](#) that you want to view.
3. To change the time range, complete the following steps:
 - a. To activate the Calendar, point your cursor at the position of the **Calendar** icon to the right of the time selection box.
 - b. Select the **Calendar** icon.
 - c. Enter the **Start Time** for the report.
 - d. Enter the **End Time** for the report.
4. Select **Submit**.
The report will execute and display when it is complete.
5. (Optional) To email the report when it completes, select **Schedule**, then define the delivery options.

Specifying Default Dashboards for the Reports Portal

The Reports feature allows you to specify the default dashboards that display when you enter the [Reports Portal](#). You can choose from any of the content available within the Reports Repository. Alternatively, if you have the *Design Reports* permission, you can create dashboards that you or others might want to include in their default dashboard.

For example, in the Reports Portal, you might want a ready access to dashboards that you use regularly. So you add the [MITRE ATT&CK Overview](#), the [OWASP Attacks and Suspicious Activity](#), and Denial of Service Activity dashboards.

To specify default dashboards:

1. Select **Reports > Portal > Portal Dashboards**.
2. Specify a name for your default dashboard.
3. (Optional) Enter a description for your dashboard portal.
4. Select one of the available dashboards.

You can specify only one dashboard at this time. However, once you are in the Reports Portal, you can add more dashboards. Each dashboard appears as a tab in the page.

5. (Conditional) To create a dashboard, select **Compose Dashboard**.
6. Click **OK**.
7. (Conditional) If you chose to create a dashboard, continue adding the items that you want to include. For additional instructions, select **(?)**.

Chapter 7: Understanding the MITRE ATT&CK

Select Reports > Portal > Repository > Standard Content > MITRE.

The MITRE ATT&CK dashboards and reports provide you with an immediately recognizable frame of reference, allowing you to view the activity based on content from Enterprise Security Manager for the MITRE ATT&CK matrix and identify possible security gaps. The dashboards and reports also provide you with valuable resources to aid you in your hunt for undetected threats in your enterprise by helping you recognize patterns and trends in the MITRE ATT&CK events.

The dashboards display a visualization based on tactics. In addition to the high-level dashboards, the MITRE ATT&CK reports provide you with detailed information to help you identify security threats.

MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. Many companies use MITRE as the go-to source for classifying various types of adversary behaviors. MITRE's periodic table and radial chart enable you to show the linkage between a specific adversary behavior and the subsystem. You can access more detailed information on MITRE tactics and techniques (MITRE IDs) on the [MITRE ATT&CK website](#).

Dashboards	Reports
MITRE ATT&CK Overview	MITRE ATT&CK Destination Address Summary
Evaluation Techniques and Tactics Summary	MITRE ATT&CK Destination Host Summary
	MITRE ATT&CK Destination Username Summary
	MITRE ATT&CK Source Address Summary
	MITRE ATT&CK Source Hostname Summary
	MITRE ATT&CK Source Username Summary
	MITRE ATT&CK Technique Summary

MITRE ATT&CK Dashboards

Content in a MITRE dashboard depends on the widgets that it displays, as well as the dashboard's specified time range.

- ["MITRE ATT&CK Overview" below](#)
- ["Evaluation Techniques and Tactics Summary" on the next page](#)

MITRE ATT&CK Overview

The **MITRE ATT&CK Overview** dashboard provides a view of MITRE ATT&CK events forwarded to Recon from ArcSight ESM. This dashboard includes the following charts:

Top 10 Destination Hostnames

Provides a list of the Top 10 destination host names of MITRE ATT&CK events.

Top 10 Source Hostnames

Provides a list of the Top 10 source host names of MITRE ATT&CK events.

MITRE IDs by Destination Hosts

Indicates whether a destination host is involved in one to three MITRE IDs. The size of the solid ovals in the chart are an approximate graphical representation of the count of the MITRE IDs. To get the actual count, move your cursor over the oval.

Source Hosts by MITRE IDs

Indicates whether the same MITRE ID is involved in one to three source host names. The color of the solid ovals in the chart indicate the count for the host name shown in the oval when compared to the legend. To get the actual count, move your cursor over the oval.

Top Destination IPs

Provides the Top 10 destination IP addresses related to a MITRE ID. The donut chart represents the number of times an IP address was the destination of a MITRE ID: the larger the area, the higher the count. The legend is not sorted by count.

Top Source IPs

Provides the Top 10 Source IP addresses related to a MITRE ID. The pie chart is evenly distributed by size among the IP addresses. The count is indicated by the color of the pie piece.

Destination Usernames by MITRE ID

Shows whether one or two destination user names are involved in the same MITRE ID.

MITRE IDs by Source Username

Shows the usernames involved with a MITRE ID (up to 10).

Evaluation Techniques and Tactics Summary

The **Summations of the Evaluation Techniques and Tactics** dashboard shows the total detection count by techniques and tactics. This dashboard includes the following bar charts:

Total Technique by Tactic

Displays the top tactics.

Total Techniques by ID

Displays the top technique IDs (up to 30).

Total Technique IDs by MITRE Name

Displays the top MITRE names (up to 20).

Total Techniques IDs by Event Name

Displays the top technique event names (up to 20).

MITRE ATT&CK Reports

Each MITRE ATT&CK report provides a Top 10 summary of different MITRE ATT&CK events. By reviewing these summaries, you might identify a host or user that is the source or target of an attack.

- ["MITRE ATT&CK Destination Address Summary" below](#)
- ["MITRE ATT&CK Destination Host Summary" below](#)
- ["MITRE ATT&CK Destination Username Summary" on the next page](#)
- ["MITRE ATT&CK Source Address Summary" on the next page](#)
- ["MITRE ATT&CK Source Hostname Summary" on page 78](#)
- ["MITRE ATT&CK Source Username Summary" on page 78](#)
- ["MITRE ATT&CK Technique Summary" on page 78](#)

MITRE ATT&CK Destination Address Summary

The **MITRE ATT&CK Destination Address Summary** report provides a bar graph of the MITRE ATT&CK events by the Top 10 destination addresses. In addition to the graph, the report includes a second page that provides the following information about the addresses:

- Destination Address
- Destination Username
- MITRE ID
- Event Name
- Count

MITRE ATT&CK Destination Host Summary

The **MITRE ATT&CK Destination Host Summary** report provides a bar graph of the MITRE ATT&CK events by the Top 10 destination host names. In addition to the graph, the report

includes a second page that provides the following information about the host names:

- Destination Host Name
- Destination Username
- MITRE ID
- Event Name
- Count

MITRE ATT&CK Destination Username Summary

The **MITRE ATT&CK Destination Username Summary** report provides a bar graph of the MITRE ATT&CK events by the Top 10 destination usernames. In addition to the graph, the report includes a second page that provides the following information about the usernames:

- Destination Username
- Destination Host Name
- MITRE ID
- Event Name
- Count

MITRE ATT&CK Source Address Summary

The **MITRE ATT&CK Source Address Summary** report provides a bar graph of the MITRE ATT&CK events by the Top 10 source addresses. In addition to the graph, the report includes a second page that provides the following information about the addresses:

- Source Address
- Source Username
- MITRE ID
- Event Name
- Count

MITRE ATT&CK Source Hostname Summary

The **MITRE ATT&CK Source Hostname Summary** report provides a bar graph of the MITRE ATT&CK events by the Top 10 source host names. In addition to the graph, the report includes a second page that provides the following information about the host names:

- Source Hostname
- Source Username
- MITRE ID
- Event Name
- Count

MITRE ATT&CK Source Username Summary

The **MITRE ATT&CK Source Username Summary** report provides a bar graph of the MITRE ATT&CK events by the Top 10 source usernames. In addition to the graph, the report includes a second page that provides the following information about the usernames:

- Source Username
- Source Hostname
- MITRE ID
- Event Name
- Count

MITRE ATT&CK Technique Summary

The **MITRE ATT&CK Technique Summary** report provides a bar graph of the MITRE ATT&CK events by the Top 10 technique summaries. In addition to the graph, the report includes a second page that provides the following information about the technique summaries:

- MITRE ID
- Event Name
- Destination Username

- Source Username
- Count

Chapter 8: Understanding the Cloud Security Dashboards and Reports

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **Cloud**.

Cloud services providers are highly accessible, and the vast amount of data that they host makes them an attractive target for malicious users. To help you assess the security of services in the cloud, we provide dashboards and reports based on the industry-wide standards set by the [Cloud Security Alliance \(CSA\)](#). This alliance has identified the most significant security threats to the shared, on-demand nature of cloud computing. CSA refers to these issues as the **Treacherous 12**.

Reporting includes the following dashboards and reports, organized by the Treacherous 12 categories:

Category	Dashboards	Reports
"Abuse and Nefarious Use of Cloud Services – Dashboards" on page 83	DoS Originated from EC2 Instances EC2 Instances Communicating with Cryptocurrency Entity EC2 Instances Querying Domains Involved in Phishing Attacks EC2 Machines Involved in Suspicious Communication Email Spam Originated from EC2 Instances Nefarious Activity by an Unauthorized Individual from EC2 Suspicious Activity Reported by Microsoft Azure Trojans or Backdoors Installed on EC2 Instances	n/a
"Account Hijacking – Dashboards and Reports" on page 84	Account Hijacking Vulnerabilities Man in the Middle Attacks Phishing Attacks Principal Invoked an API Commonly used to Discover Information Associated with AWS account	Broken Authentication and Session Management
"Advanced Persistent Threats – Dashboard" on page 85	Trojans or Backdoors Installed on EC2 Instances	n/a
"Data Breaches – Dashboards" on page 85	All Information Leakage Events Information Disclosure Vulnerabilities Organizational Information Leakage Personal Information Leakage	n/a
"Data Loss – Dashboard and Reports" on page 86	Amazon AWS Deletion Events	Amazon S3 Bucket Deletion Events Amazon VPC Deletion Events

Category	Dashboards	Reports
"Denial of Service – Dashboard" on page 87	DoS Activity	n/a
"Insecure Interfaces and APIs – Report" on page 87	n/a	Vulnerabilities on Interfaces and API
"Insufficient Due Diligence – Reports" on page 88	n/a	EC2 Machines Behavior Deviates from the Established Baseline Failed Technical Compliance Events
"Insufficient Identity Credential and Access Management – Reports" on page 88	n/a	AWS Account Password Policy Was Weakened Invalid or Expired Certificate Unsecured Password Events
"Malicious Insiders – Report" on page 89	n/a	Nefarious Activity by an Unauthorized Individual
"System Vulnerabilities – Dashboard and Reports" on page 89	Vulnerability Overview	Cloud Related Vulnerabilities Critical Vulnerabilities Heartbleed Vulnerabilities Kernel Vulnerabilities Overflow Vulnerabilities Security Patch Missing Shellshock Vulnerabilities Spectre and Meltdown Vulnerabilities Vulnerabilities by Host
"Vulnerabilities on Shared Technologies" on page 91	n/a	"Vulnerabilities on Shared Technologies" on page 91

The cloud-based security dashboards and reports provide a view of events occurring in Amazon Web Service (AWS) and Azure, forwarded to Recon from ArcSight ESM. Content in a dashboard depends on the widgets that it displays, as well as the dashboard's

specified time range. For example, some widgets summarize events by resource names and profile IDs, as well as by the event's severity.

Abuse and Nefarious Use of Cloud Services – Dashboards

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [Cloud](#) > [CSA](#) > [The Treacherous 12](#).

Malicious users can exploit poorly secured cloud service deployments, free cloud service trials, and fraudulent account sign-ups, which expose cloud computing models such as IaaS, PaaS, and SaaS. You might experience denial of service attacks, email spam and phishing campaigns, and brute-force computing attacks, or malicious individuals spoofing identities.

Some charts display data reported by Amazon GuardDuty, which is a threat detection service that continuously watches for malicious activity and unauthorized behavior.

To search for potential threats, use the following dashboards:

DoS Originated from EC2 Instances

Helps you identify denial of services activities that arise from EC2 (AWS Elastic Compute Cloud service) instances. The charts and table show events summarized by their Amazon resource name, severity, and GuardDuty.

EC2 Instances Communicating with Cryptocurrency Entity

Displays EC2 instances that communicates with cryptocurrency IP addresses or domains.

EC2 Instances Querying Domains Involved in Phishing Attacks

Lists the EC2 instances in which querying domains are involved in phishing attacks.

EC2 Machines Involved in Suspicious Communication

Lists the EC2 machines that are involved in suspicious communication.

Email Spam Originated from EC2 Instances

Identifies email spam that originates from EC2 instances.

Nefarious Activity by an Unauthorized Individual from EC2

Displays events that Amazon GuardDuty reports as nefarious activity by an unauthorized individual from EC2 machines. Amazon GuardDuty a threat detection service that continuously watches for malicious activity and unauthorized behavior.

Suspicious Activity Reported by Microsoft Azure

Lists suspicious activity reported by Microsoft Azure.

Trojans or Backdoors Installed on EC2 Instances

Lists backdoors or trojans discovered on EC2 machines.

Account Hijacking – Dashboards and Reports

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [Cloud](#) > [CSA](#) > [The Treacherous 12](#).

CSA identifies the hijacking of accounts and services as an ongoing, top threat. Malicious users might hijack accounts by phishing, fraud, and exploiting software vulnerabilities. In the cloud, the hijackers can eavesdrop on organizational activities, manipulate data, and redirect your clients.

To search for potential threats, use the following dashboards and report:

Account Hijacking Vulnerabilities

Provides charts of the top 10 vulnerabilities and the number of vulnerabilities over time. This dashboard also includes a table of the vulnerabilities, so you can review the reporting vendor or device, agent severity, asset, and the asset's zone.

Man in the Middle Attacks

Provides charts that show man in the middle events by time, source address, destination address, source MAC address, and destination MAC address.

Phishing Attacks

Provides charts that show the phishing attacks against the organizations.

Principal Invoked an API Commonly used to Discover Information Associated with AWS account

Provides charts that show the principals invoked by an API commonly used to discover information associated with AWS accounts.

Broken Authentication and Session Management

Lists the events that might be associated with broken authentication (possibly hijacked credentials) and session management issues reported by vulnerability scanners in the organization.

Advanced Persistent Threats – Dashboard

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **Cloud** > **CSA** > **The Treacherous 12**.

Advanced Persistent Threats (APTs) are a parasitical form of cyberattack that infiltrates systems to establish a foothold in the computing infrastructure of target companies from which they smuggle data and intellectual property. This category provides the **Trojans or Backdoors Installed on EC2 Instances** dashboard, which provides charts showing backdoors or trojans discovered on EC2 (AWS Elastic Compute Cloud service) machines. This dashboard also is available within the "[Abuse and Nefarious Use of Cloud Services – Dashboards](#)" on page 83 category.

Data Breaches – Dashboards

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **Cloud** > **CSA** > **The Treacherous 12**.

While the risk of a data breach is not unique to the cloud, the CSA ranks it as a top concern for cloud customers. Sometimes the breach is the prime motivation of malicious users. However, breaches also result from mistakes made by individuals within the organization or poor security practices and software vulnerabilities.

To search for potential threats, use the following dashboards:

All Information Leakage Events

Provides charts and a table that show the leakage events in the organization, including the top reported events, destination users, and assets.

Information Disclosure Vulnerabilities

Provides charts and a table that show the disclosure vulnerabilities reported in the organization over time and by agent severity. You can also see the top 20 hosts, IP addresses, and signature ID events.

Organizational Information Leakage

Provides charts and a table that show the leakage of organizational information. You can view the top 20 leakage events and signature IDs, as well as leakage over time and agent severity.

Personal Information Leakage

Provides charts and a table that show the leakage of personal information. You can view the top reported, top 10 destination and source users, and leakage over time.

Data Loss – Dashboard and Reports

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **Cloud** > **CSA** > The Treacherous 12.

No organization wants to lose data, particularly to malicious individuals who might use the information in an adverse manner. Unfortunately, data stored in the cloud can also be deleted accidentally or as a result of a catastrophe.

To assess the potential for data loss, use the following reports:

Amazon S3 Bucket Deletion Events

Lists the deletion events that occur in Amazon S3 Buckets.

Amazon VPC Deletion Events

Lists the deletion events that occur in Amazon VPC.

This category includes the **Amazon AWS Deletion Events** dashboard, which provides charts and a table listing the number of deletion events by operations, day, source address, and source user.

Denial of Service – Dashboard

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **Cloud** > **CSA** > **The Treacherous 12**.

Denial-of-service (DoS) attacks deliberately attempt to prevent users from accessing services, data, and applications. Use the **DoS Activity** dashboard to watch for potential service interruptions. You can view the top source and destination addresses, as well as events by day.

This dashboard also is available in the **Network Monitoring** category of the **Foundation** reports.

Insecure Interfaces and APIs – Report

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **Cloud** > **CSA** > **The Treacherous 12**.

Users interact with cloud computing services through user interfaces (UIs) and application program interfaces (APIs), and the value-added services built on these services. APIs and UIs are generally the most exposed part of a system, perhaps the only asset with an IP address available outside the trusted organizational boundary. These assets will be the target of heavy attack. Use the **Vulnerabilities on Interfaces and API** report to identify the vulnerabilities found in your cloud-based interfaces and APIs.

Insufficient Due Diligence – Reports

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [Cloud](#) > [CSA](#) > [The Treacherous 12](#).

The CSA states that it is essential to develop a good roadmap and checklist for due diligence when evaluating technologies and CSPs. Organizations should perform due diligence to mitigate the myriad risks associated with providing cloud services. To identify areas with insufficient due diligence, use the following reports:

EC2 Machines Behavior Deviates from the Established Baseline

Details how the behavior of EC2 (AWS Elastic Compute Cloud) machines deviates from the established baseline.

Failed Technical Compliance Events

Lists the failed technical compliance events.

0 Comment(s)

Insufficient Identity Credential and Access Management – Reports

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [Cloud](#) > [CSA](#) > [The Treacherous 12](#).

Malicious users can infiltrate and cause data breaches based on poor authentication methods and weak password policies. Use the following reports to watch for threats due to insufficient identity credentials and access management:

AWS Account Password Policy Was Weakened

Lists events associated with weakened AWS account password policy.

Invalid or Expired Certificate

Lists events associated with invalid or expired certificates.

Unsecured Password Events

Lists events associated with unsecured passwords.

Malicious Insiders – Report

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **Cloud** > **CSA** > **The Treacherous 12**.

Individuals within an organization, such as system administrators or disgruntled colleagues, might access sensitive information for malicious intent. Most organizations use controls to limit risk from malicious insiders, such as controlling encryption keys and monitoring or auditing the activities of specific users.

The **Nefarious Activity by an Unauthorized Individual** report lists events that Amazon GuardDuty reports as nefarious activity by an unauthorized individual from EC2 (AWS Elastic Compute Cloud) machines. Amazon GuardDuty is a threat detection service that continuously watches for malicious activity and unauthorized behavior.

System Vulnerabilities – Dashboard and Reports

Select > **Reports** > **Portal** > **Repository** > **Standard Content** > **Cloud** > **System Vulnerabilities**.

Most computer systems have programs, services, and operating systems that are vulnerable to exploitation. According to the CSA, vulnerabilities within the components of the operating system – kernel, system libraries and application tools – put the security of all services and data at significant risk.

To mitigate the risk to your systems, use the following reports and dashboard:

Cloud Related Vulnerabilities

Lists all events associated with vulnerabilities known to affect AWS and Azure.

Critical Vulnerabilities

Lists all events that have a High or Very High severity, based on CVE and CVSS data.

Heartbleed Vulnerabilities

Lists all events associated with the heartbleed bug, which is a system vulnerability in the OpenSSL cryptographic software library. This weakness allows malicious users to steal the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. A Heartbleed attack works by tricking servers into leaking information stored in their memory. Attackers can also get access to a server's private encryption key, allowing the attacker to unscramble any private messages sent to the server and even impersonate the server.

Kernel Vulnerabilities

Lists all events associated with kernel vulnerabilities. For example, the vulnerability in the Linux Kernel netfilter/xt_TCPMSS, which could allow remote hackers to carry out a denial of service attack.

Overflow Vulnerabilities

Lists all events associated with buffer overflows. When a buffer receives more data than it can handle, the data can overflow to other storage locations. Overflows can cause system crashes or create an exploitable vulnerability.

Security Patch Missing

Reports the hosts that do not have the security patches needed to resolve known vulnerabilities.

Shellshock Vulnerabilities

Reports the hosts vulnerable to a ShellShock attack. In a Shellshock attack, the Unix shell Bash could execute arbitrary commands and allow unauthorized access to services, such as web servers, that use Bash to process requests.

Spectre and Meltdown Vulnerabilities

Reports the hosts vulnerable to Meltdown and Spectre attacks, which exploit critical vulnerabilities in modern processors. Meltdown breaks the fundamental isolation between user applications and the operating system, allowing a program to access the memory and data of other programs and the operating system. Spectre attacks break

the isolation between applications, allowing programs to leak information to each other. These exploitations do not leave any traces in traditional log files.

Vulnerability Overview

Provides a dashboard view of the vulnerabilities found in the organization.

Vulnerabilities by Host

Lists all vulnerabilities detected on the specified hosts.

Vulnerabilities on Shared Technologies

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **Cloud** > **Vulnerabilities on Shared Technologies**.

Some technologies that form the infrastructure for the cloud-based services started as on-premises capabilities, and thus might not have been designed to share its resources in multi-tenancy or multi-customer environments.

For example, an application might not have initially been expected to support multi-factor authentication or a its database designed to partition data by tenant.

The **Vulnerabilities on Shared Technologies** report provides you insight into the vulnerable technologies that a malicious user might exploit.

Chapter 9: Understanding the Foundation Dashboards and Reports

Select **Reports > Portal > Repository > Standard Content > Foundation**.

Reporting includes the following dashboards and reports, organized by the following foundational categories:

Category	Dashboards	Reports
"Entity Monitoring – Dashboards and Reports" on page 94	Account Management Overview Failed Logins Overview Successful Login Overview	All Logins by Hostname Failed Logins Summary Login Activity by User
"Events Overview – Dashboards" on page 95	Least Common Events Most Common Events Most Common Events by Severity Reporting Devices	n/a
"Hosts Monitoring - Reports" on page 96	n/a	Anti-Virus Activity Anti-Virus Stopped or Paused Audit Log Cleared Failed Anti-Virus Updates Summary Operating Systems Errors and Warnings Services Shutdown Services Started

Category	Dashboards	Reports
"Malware Monitoring – Dashboard and Reports" on page 97	Malware Overview	Reported Malware by Host Worm Infected Systems
"Network Monitoring – Dashboards and Report" on page 98	Attacks and Suspicious Activity Overview DGA Overview DoS Activity Email Attacks IDS Events Man in the Middle Attacks Reconnaissance Activity Traffic Anomaly Overview VPN Activities Overview	Exploit Attempts Detected by IDS Network Device Configuration Changes
"Perimeter Monitoring – Dashboards and Reports" on page 100	Firewall Blocked Events Firewall Traffic Overview	Firewall Configuration Changes Firewall Blocked Traffic by Destination Address
"Vulnerability Monitoring – Dashboard and Reports" on page 101	n/a	High Risk Vulnerabilities by Host SSL Vulnerabilities Vulnerability Overview Vulnerabilities by Host XSRF Vulnerabilities XSS Vulnerabilities

Entity Monitoring – Dashboards and Reports

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **Foundation**.

To prevent brute force attacks or denial-of-service attacks, you could track login activities in your environment. A malicious user might attempt to guess another user's password by repeatedly attempting to log in to the same account. You can track this behavior by observing failed login attempts. You might also watch for users who attempt to log in to multiple devices and hosts. Malicious users might also create, modify, and delete accounts to gain unauthorized access or let them execute harmful code.

To monitor account activity, use the following dashboards and reports:

Account Management Overview

Provides charts and a table to help you identify users who are creating and deleting the most accounts. You also can track which hosts have had the largest number of accounts modified or deleted.

All Logins by Hostname

Reports the number of login attempts over time, including the outcome, for the specified hosts.

You must specify one IP address.

Failed Logins Overview

Provides an overview, in charts and a table, of the hosts and users with the highest number of failed logins. You can also view the number of failed logins over time, by reporting device, or source address.

Failed Logins Summary

Reports the number of failed logins over time. The table includes the user, source address, target host, and number of failed attempts.

Login Activity by User

Reports the number of times that the specified users have attempted to log in to a host. The table indicates whether the attempt is successful.

You must specify one user by Destination UserName.

Successful Login Overview

Provides an overview, in charts and a table, of users with the highest number of successful logins. You can review the relationship between the users and the hosts to which they successfully log in.

Events Overview – Dashboards

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [Foundation](#).

To identify threats in your environment, you might want to have an overview of the events that occur the most often or affect the most devices and hosts. You could also watch for events that rarely occur to check for unusual activity.

To monitor event activity, use the following dashboards:

Least Common Events

Provides charts and a table to help you identify the events that have the fewest reported occurrences. You can view the results by vendor, such as Amazon, or product, such as Microsoft Windows.

Most Common Events

Provides charts and a table to help you identify the common events that affect your environment by vendor, such as Amazon, or product, such as Microsoft Windows.

Most Common Events by Severity

Provides a table to help you track the events by count and severity.

Reporting Devices

Provides charts and a table to help you identify the hosts and devices with the most reported security events. You can view charts summarizing the most common severity of the events; top 20 events by vendor such as Microsoft or McAfee; top 20 events types of events, such as stopped services, and the top 20 events by class ID, such as a CVE.

Hosts Monitoring - Reports

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **Foundation**.

In general, you should consistently monitor host-based events that indicate unauthorized activities. For example, a malicious user or program might start and stop host services and anti-virus programs. Additionally, they might clear the audit log to hide their actions on a host.

To monitor unusual activity that affects hosts, use the following reports:

Anti-Virus Activity

Reports the volume of activity by reporting anti-virus service. The table provides results by event name, count, affected host, and outcome.

Anti-Virus Stopped or Paused

Reports the top IP addresses where an anti-virus service has been stopped or paused. The table provides results by host, service name, and number of events.

Audit Log Cleared

Reports the number of times that the audit log has been cleared by user, host, and date.

Failed Anti-Virus Updates Summary

Reports the number of failures in updating anti-virus software by date and host.

Operating Systems Errors and Warnings

Reports the top system errors and warnings by host. You could identify issues associated with specific errors or warnings, such as privileged objects and users, password changes, and login failures. Alternatively, you could sort the table by the reported hosts to review the types of issues affecting each host.

Services Shutdown

Reports the top 10 services that have been shut down in your environment. The table provides a summary of all services, including the associated hosts.

Services Started

Reports the top 10 services that have been started in your environment. The table provides a summary of all services started, including the associated hosts.

Malware Monitoring – Dashboard and Reports

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [Foundation](#).

Malware, or malicious software, represents all the variations of programs designed to damage computers, servers, clients, devices, applications, and networks. To monitor malware activity, use the following dashboard and reports:

Malware Overview

Provides charts and a table to help you identify the malware affecting your enterprise and the top 10 infected hosts. You can also view the malware events reported over time.

Reported Malware by Host

Lists the malware found on the specified hosts.

You must specify one host.

Worm Infected Systems

Lists the hosts infected by worms, and provides a chart that shows the malware by count found in your enterprise.

Network Monitoring – Dashboards and Report

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [Foundation](#).

The traffic exchanged between devices and servers tells you a lot about your network. By monitoring network traffic, you can identify cyber attacks and network events that could affect your enterprise. For example, malicious users might find a way to intercept communications to generate a man-in-the-middle attack or change the configuration of devices to gain unauthorized access. In both cases, the attack is the beginning of further intrusions. Also, a system infected by malware can be instructed generate a large volume of domains, thus causing increased traffic.

To monitor network activity, use the following dashboards and reports:

Attacks and Suspicious Activity Overview

Provides charts and a table to help you identify the top attackers, targets, and events over time.

This dashboard also is available in the [Insufficient Logging and Monitoring](#) category of the OWASP reports.

DGA Overview

Provides charts and a table to help you watch for domain generation algorithms (DGAs). You can identify the IP addresses generating the most DGA domains or the unique domains that the largest number of hosts attempt to connect with. You can also check for the hosts that are transmitting the largest amount of data.

DoS Activity

Provides charts and a table for you to identify denial-of-service events. You can view the number of events per day, as well as the top source and destination addresses.

This dashboard also is available in the Denial of Service category of the Cloud reports.

Email Attacks

Provides charts and a table that describe the email attacks detected in your enterprise. You can view the top events or target users, as well as the destination and source addresses.

Exploit Attempts Detected by IDS

Shows the top 10 exploit attempts reported by the intrusion detection systems (IDS) in your enterprise. In the table, you can sort the events by count or severity.

IDS Events

Provides a chart and table showing all events reported by the IDSs in your enterprise.

Man in the Middle Attacks

Provides charts and a table to help you catch potential man-in-the-middle (MitM) attacks. You can view events over time, by source and destination address including MAC addresses, and the top MitM events.

During a MitM attack, the malicious user intercepts communications between two parties either to secretly eavesdrop or modify traffic traveling between the two.

Network Device Configuration Changes

Reports the top 10 devices whose configurations have changed, as well as the top 10 events causing configuration changes.

Reconnaissance Activity

Provides charts and a table to help you watch for active reconnaissance attacks. You can view identify the top sources of recon activity, as well as the primary destinations for these attacks. Review the pie charts to identify the main types of events and affected zones.

Active reconnaissance is a type of computer attack in which an intruder engages with the targeted system to gather information about vulnerabilities. Malicious users might

use tools like ping or traceroute to perform recon through automated scanning or manual testing.

Traffic Anomaly Overview

Provides charts to help you identify anomalies in network traffic. You can view the top source and destination address, events, and activity over time.

VPN Activities Overview

Provides charts and a table for you to monitor VPN activity, such as the top users who access the VPN. You can view the VPN activities per day, as well as review the top source and destination addresses.

Perimeter Monitoring – Dashboards and Reports

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [Foundation](#).

The perimeters of an enterprise's network handle a great deal of traffic, causing system administrators to face an ever-increasing need to allow fast, efficient flow of traffic while also keeping the network secure. If you pro-actively monitor the firewalls in your enterprise, you can identify problems at an early stage and prevent network attacks. Malicious users often exploit loopholes in your firewall rules, particularly any old or unused rules. Network traffic also can be vulnerable to unencrypted data.

To monitor your network's perimeter, use the following dashboards and reports:

Firewall Blocked Events

Provides charts and a table for you to monitor the events that your firewalls have blocked, such as the bytes in and out for all blocked events. You can view the top events blocked per device, application protocol, source address, or destination address.

Firewall Blocked Traffic by Destination Address

Lists the top 10 firewall traffic events that have been blocked from reaching the specified hosts.

You must specify one IP address.

Firewall Configuration Changes

Lists the top 10 changes to the firewall configuration by host.

Firewall Traffic Overview

Provides charts and a table for you to monitor traffic through your firewalls, such as the bytes in and out by accepted and denied traffic. You can view the top reporting devices and destination addresses, as well as the outcomes of port usage over time. The table lists the Port, transport protocol, application protocol, and number of events reported by firewalls.

Vulnerability Monitoring – Dashboard and Reports

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **Foundation**.

Many of the components within a web application, such as the libraries and modules, run with the same privileges as the application itself. Applications and APIs using components with known vulnerabilities can undermine application defenses and enable various attacks and impacts. For example, malicious users can exploit a known in SSL with the [Heartbleed Bug](#). Web site and web applications can be vulnerable to cross-site scripting (XSS) and cross-site request forgery (XSRF) attacks. In an XSRF attack, also known as a one-click attack or session riding, a malicious user submits unauthorized commands to a web application from a user account that the application trusts.

High-risk vulnerabilities represent those that are relatively easy for attackers to exploit and gain control over system components. Many high-risk vulnerabilities can temporarily or permanently disrupt enterprise operations.

To check whether your enterprise has vulnerabilities, use the following dashboard and reports:

High Risk Vulnerabilities by Host

Lists all high-risk vulnerabilities found on the specified hosts.

You must specify one host by **Destination Host**.

SSL Vulnerabilities

Lists the hosts reported to have the most SSL vulnerabilities.

This report also is available in the [Using Components with Known Vulnerabilities](#) category of the **OWASP** reports.

Vulnerability Overview

Provides charts and a table to help you track the vulnerabilities reported in your enterprise.

Vulnerabilities by Host

Lists all vulnerabilities found on the specified hosts.

You must specify one IP address.

XSRF Vulnerabilities

Lists the top 10 hosts that are vulnerable to a cross-site request forgery (XSRF or CSRF) attack.

XSS Vulnerabilities

Lists the top 10 hosts that are vulnerable to [cross-site scripting \(XSS\)](#) attacks.

Chapter 10: Understanding the OWASP Security Dashboards and Reports

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP**.

We provide dashboards and reports based on the industry-wide standards set by the [Open Web Application Security Project®](#). OWASP is a nonprofit foundation that works to improve the security of software. The organization has established a list of the Top 10 security risks to web applications, focusing on the most critical threats to the shared, on-demand nature of webbased applications.

Reporting includes the following dashboards and reports, organized according to **OWASP's Top 10** risk categories:

Category	Dashboards	Reports
"Broken Access Control" on the next page	n/a	"Broken Access Control" on the next page
"Broken Authentication" on the next page	n/a	"Broken Authentication" on the next page
"Cross-site Scripting" on page 105	Cross Site Scripting	XSS Vulnerabilities
"Injections" on page 105	Injection Vulnerabilities Overview	Command Injections on HTTP Request Injection Vulnerabilities SQL Injection
"Insecure Deserialization – Dashboards and Reports" on page 106	Deserialization Flaws Overview	Deserialization Flaws
"Insufficient Logging and Monitoring – Dashboards and Reports" on page 107	Attacks and Suspicious Activities Overview Failed Logins Overview Login Activity Overview Operating System Errors and Warnings Security Log is Full	All Logins by Hostname Failed Logins Summary Audit Log Cleared

Category	Dashboards	Reports
"Security Misconfiguration" on page 109	Misconfiguration Events Overview Missing Security Patches Overview	Security Patch Missing
"Sensitive Data Exposure" on page 109	Information Leaks Overview	Organizational Records Information Leaks Personal Information Leaks
"Using Components with Known Vulnerabilities – Dashboards and Reports" on page 110	SSH Vulnerabilities Overview Vulnerability Overview	SSH Vulnerabilities Summary SSL Vulnerabilities
"XML External Entities" on page 111	XML Vulnerabilities Overview	XML Vulnerabilities

Broken Access Control

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 5 - Broken Access Control**.

Some enterprises fail to enforce access controls that restrict what authenticated users are allowed to do. By exploiting vulnerabilities in access controls, a malicious user might retrieve sensitive files, gain access other user's accounts, change access rights, and misuse data.

The **Broken Access Control** report lists vulnerable hosts by severity over time.

Broken Authentication

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 2 - Broken Authentication**.

Some enterprises fail to enable or mis-configure the authentication and session management functions of applications and web sites. When this occurs, a malicious user could compromise passwords, keys, and session tokens.

Use the **Broken Authentication and Session Management** report to identify hosts vulnerable to malicious users. This report also is available in the Account Hijacking category of the Cloud reports.

Cross-site Scripting

Select > **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 7 - Cross-Site Scripting**.

Vulnerabilities associated with **cross-site scripting (XSS)** enable malicious users to inject code in legitimate web pages or applications that executes harmful scripts in the user's web browser when the browser parses data. The scripts might hijack user sessions, deface web sites, or redirect users to harmful sites. A web application or web page becomes vulnerable when it includes untrusted data; data without proper validation or escaping; or data supplied by users through an API that can create HTML or Java-script. XSS attacks tend to occur in forums, message boards, and web pages that allow comments. Malicious users can execute XSS attacks in VPScript, ActiveX, Flash, and CSS. However, this type of injection attack most commonly occurs in Java Script.

To identify XSS vulnerabilities in your environment, use the following report and dashboard:

Cross Site Scripting

Lists events associated with XSS vulnerabilities.

XSS Vulnerabilities

Provides charts and a table so you can review potential XSS vulnerabilities in your environment by vulnerability type or the top vulnerable hosts.

To get a list of the top 10 hosts vulnerable to cross-site scripting attacks, run the **XSS Vulnerabilities** report.

Injections

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 1 - Injections**.

Injection vulnerabilities, or flaws, allow malicious users to inject code in other systems, especially interpreters, by using vulnerable applications. For example, in a SQL, NoSQL, OS

or LDAP injection attack, someone sends untrusted data to an interpreter as part of a command or query to trick the interpreter into executing hostile commands or accessing data without appropriate authorization. Usually, these flaws result from insufficient validation of data input or the failure to filter or sanitize the input.

To check for injection vulnerabilities, use the following reports and dashboard:

Command Injections on HTTP Request

Lists the highest number of events associated with command injections in an HTTP request, by the requested URL. This report includes a chart to help you identify the relationship between the IP addresses of the attacker and the target.

In a command injection attack that exploits an HTTP request, malicious users execute arbitrary commands on the host operating system via a vulnerable application. For example, the web application passes unsafe data supplied by the user to a system shell.

Injection Vulnerabilities

Lists the hosts with the most injection vulnerabilities over time.

Injection Vulnerabilities Overview

Provides charts and a table to help you identify the systems affected by injection vulnerabilities, as well as view the top reported vulnerabilities by agent severity, risk, and over time.

SQL Injection

Lists the systems with the highest number of SQL injection vulnerabilities.

In a SQL injection attack, a malicious user can interfere with the queries that an application makes to its database. The user could view delete, or modify data not usually available for retrieval. A malicious user could also use SQL injections to start a denial-of-service attack or compromise other services, servers, or infrastructure.

Insecure Deserialization – Dashboards and Reports

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [OWASP](#) > [A 8 - Insecure Deserialization](#).

Untrusted, or insecure, deserialization allows malicious users to use untrusted data to abuse the logic of an application, initiate a denial-of-service or injection attacks, or execute harmful code when the data is deserialized. The user could even replace a serialized object with objects of a different class. Deserialization is a common process where the web site or application takes data from a file, stream, or network and rebuilds it into an object. The serialized objects might be used in JSON, XML, or YAML.

To check for deserialization vulnerabilities, use the following report and dashboard:

Deserialization Flaws

Lists the hosts with most deserialization flaws.

Deserialization Flaws Overview

Provides charts and a table to help you identify the top hosts, deserialization flaws, and flaws found over time. You can view the flaws by agent severity and risk indicator.

Insufficient Logging and Monitoring – Dashboards and Reports

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [OWASP](#) > [A 10 - Insufficient Logging and Monitoring](#).

According to OWASP, insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows malicious users to further attack systems; maintain persistence; pivot to more systems; and tamper, extract, or destroy data. Most major incidents start with an exploitation of the vulnerabilities in logging and monitoring. Yet, most organizations fail to discover the breach until several months have passed.

To help you detect potential breaches as soon as possible, use the following reports and dashboards:

All Logins by Hostname

Lists all logins that have occurred on the specified host.

Attacks and Suspicious Activities Overview

Provides charts and a table to help you identify the top attackers, targets, and events over time.

This dashboard also is available in the **Network Monitoring** category of the Foundation reports.

Audit Log Cleared

Lists all the Audit Clear events that have occurred in the organization.

Failed Logins Overview

Provides charts and a table showing failed logins by time, users, hosts, reporting devices, and attacker address.

Failed Logins Summary

Lists the failed login events that have occurred in your environment.

Login Activity Overview

Provides charts and a table showing the outcome of login activity, including successful logins. You can view activity by machine or user, as well as a chart showing the relationship between users and systems to which they log in.

Operating System Errors and Warnings

Provides charts and a table that report the operating systems errors and warnings in the organization.

Security Log is Full

Provides charts and a table to help you identify the hosts where the security log is full.

Security Misconfiguration

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 6 - Security Misconfiguration**.

In general, the most common vulnerability in your environment is mis-configured operating systems, frameworks, libraries, and applications. Mis-configurations include missing security patches or updates, incomplete or ad hoc configurations, use of insecure default configurations, poorly configured HTTP headers, and error messages that contain sensitive information.

To identify systems that need reconfiguration, use the following dashboards and report:

Misconfiguration Events Overview

Provides an overview of the mis-configured events reported in your environment. The charts show the top mis-configured systems, the top misconfiguration events, an indicator of the risk associated with the reported misconfiguration events, events by agent severity, and misconfiguration events over time. The table provides additional information, such as the associated vulnerability.

Missing Security Patches Overview

Provides charts and a table to help you identify the top machines that fail to have all relevant security patches, as well as the security patches most reported as not having been applied. You can review the missing patch reports over time, by agent severity, and by risk indicator.

Security Patch Missing

Lists the security patches that have not been applied, as reported by vulnerability scanners in your environment.

Sensitive Data Exposure

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 3 - Sensitive Data Exposure**.

Most enterprises store sensitive data that needs to be protected, such as personal information, customer and organizational financial data, healthcare records, or intellectual property. Web applications and APIs might inadvertently expose sensitive data by not having enough protections such as encryption at rest or in transit, or when exchanging data with the browser. Malicious users could use the data for credit card fraud, identity theft, and other crimes.

To identify potential exposure of sensitive data, use the following dashboard and reports:

Information Leaks Overview

Provides charts and a table to help you identify the most reported systems, types of leaks, and leakage events that occur over time. You can identify the top reported users and view leaks by category.

Organizational Records Information Leaks

Lists the top leakage events that affect organizational records.

Personal Information Leaks

Lists the top leakage events that affect personal records by Destination UserName.

Using Components with Known Vulnerabilities – Dashboards and Reports

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [OWASP](#) > [A 9 - Using Components with Known Vulnerabilities](#).

Many of the components within a web application, such as the libraries and modules, run with the same privileges as the application itself. Applications and APIs using components with known vulnerabilities can undermine application defenses and enable various attacks and impacts. Malicious users can exploit vulnerabilities in SSH and SSL. For example, the **Heartbleed Bug** is a known SSL vulnerability. Your enterprise might have large numbers of SSH keys because end users can create new SSH keys (credentials) or even duplicate them without oversight, unlike certificates or passwords. A malicious user can gain long-term access to your resources by taking advantage of SSH keys that have been left unaccounted for.

To check whether components can be exploited, use the following dashboards and reports:

SSH Vulnerabilities Overview

Provides charts and a table that show hosts with the most SSH vulnerabilities and the most reported vulnerabilities. You can review these vulnerabilities over time, by agent severity, and by risk indicator.

SSH Vulnerabilities Summary

Lists the hosts reported to have the most SSH vulnerabilities.

SSL Vulnerabilities

Lists the hosts reported to have the most SSL vulnerabilities.

This report also is available in the **Vulnerability Monitoring** category of the Foundation reports.

Vulnerability Overview

Provides charts and a table that show the top signature IDs for the anti-virus programs that have failed to update, as well as the hosts most likely to be vulnerable. You can review these vulnerabilities over time and by agent severity.

XML External Entities

Select **Reports > Portal > Repository > Standard Content > OWASP > A 4 - XML External Entities**.

Older or mis-configured XML processors use XML documents to evaluate external entity references, and can inadvertently process harmful XML input. Malicious users use the XML processor's to reveal internal content such as files, file shares, and port scans, as well as execute remote code and denial-of-service attacks.

To watch for XML external entity attacks, use the following report and dashboard.

XML Vulnerabilities

Lists the hosts with the most XML vulnerabilities.

XML Vulnerabilities Overview

Provides charts and a table to help you identify the systems with the most XML vulnerabilities as well as the most reported vulnerabilities. You can review the vulnerabilities by severity and risk indicator.

III Analyzing Anomalous Data with Outlier Analytics

Select **Insights** > **Outliers**.

To help you identify anomalous behavior, the **Outlier Analytics** feature allows you to compare incoming *EventCount*, *BytesIn*, and *BytesOut* values to typical values for your environment. The *EventCount*, *BytesIn* and *BytesOut* values are aggregations over certain time periods for each host/IP address. Outlier Analytics can create and persist a baseline of host behavior. To derive outliers, you compare this baseline with aggregations over new time periods. Basically, the lower the anomaly score, the more likely the event is anomalous.

The analytics process allows you to [define and build a model](#) that identifies typical behavior for your environment, and then start a [scoring process](#) that evaluates incoming events against the model. The scoring process assigns a score that indicates the degree to which the incoming data varies from the typical behavior. Outlier Analytics [displays the results](#) of the scoring process in a table that shows the top anomalous hosts. From the table, you can generate charts that provide additional information about the anomaly.

The model specifies a subset of data from the [Events table](#) that represents typical behavior on your network. When you define the model, you can specify criteria that identify which device behaviors you want to model. For example, you might want to look for anomalous values in events that you receive from a specific device vendor or in systems on a specific subnet.

- ["Generating Models to View Anomalous Data " on page 114](#)
- ["Viewing Anomalous Data in a Model" on page 118](#)

Chapter 11: Generating Models to View Anomalous Data

You must have the Manage Outlier Models and Scoring permissions to define and build models.

The model for Outlier Analytics defines typical *EventCount*, *BytesIn*, and *BytesOut* behavior for a set of IP addresses over a specified date range. You can define the criteria that identify which device behaviors you want to model. If you want a different model, you must define and build a new one.

- ["Considerations for Generating Models" below](#)
- ["Defining and Building a Model" on the next page](#)
- ["Scoring a Model" on page 116](#)
- ["Deleting a Model" on page 117](#)

Considerations for Generating Models

Before defining and building a model, review the following considerations:

- You can create and delete models, but you cannot modify them.
- You can define as many models as you want, but you can only build one model at a time.
- When you define the model, you should set the date range wide enough (more than 168 hours) so that the model includes a variety of device behaviors, including cyclical patterns.
- Because the scoring algorithm is based on peer group analysis, Micro Focus recommends that you include similar devices in a model, based on activity. For example, you might want to create separate models for scoring endpoints, scoring DNS servers, and scoring databases.
- Each model definition applies a filter where `Source Address != NULL`.
- When you build a model, Outlier Analytics adds a [lookup list](#) of the same name to **Configuration > Lookup Lists**. You cannot view or edit this list. When you delete the model, the lookup list also gets deleted.
- The auto-complete functionality is temporarily unavailable in search input. The following columns are available for outliers filtering in the Search feature:

- Source Address of *<Model_Name>*
 - Base Event Count Score of *<Model_Name>*
 - Bytes Out of *<Model_Name>*
 - Bytes In of *<Model_Name>*
- <Model_Name>* corresponds to the model name being scored.

Defining and Building a Model

When you build the model, the feature aggregates events from the Events table by IP address, day of week, and hour of day for each five-minute time increment.

The feature then calculates a sum for:

- *EventCount*
- *BytesIn*
- *BytesOut*

Outlier Analytics then creates conditional probability tables for sum of *EventCount*, sum of *BytesIn*, and sum of *BytesOut*.

To build a model:

1. Review the considerations for building a model.
2. Select **Configuration** > **Outlier**.
3. From the **Create Model Configuration** section, specify the criteria that you want to use for building the model.

For example:

- To define a specific subnet that represents a specific class of equipment (like server or data center), specify criteria similar to the following:
`sourceAddress in subnet 10.1.1.0/24.`
- To model outbound HTTP/HTTPS traffic, specify criteria similar to the following:
`destinationPort = 80,443`

4. To more easily find the model later, give the model a name by typing over the **Model Name**.

The model name can contain letters, numbers, and underscores only. The name must start with an alpha character and cannot exceed 19 characters.

5. For the [time range](#), perform **one** of the following actions:
 - Accept the default time (**Last 14 days**)
 - From the drop-down menu, select a pre-defined value under **Quick Ranges**
 - From the drop-down menu, use the **Custom Range** fields to specify a [time range](#)
 - From the drop-down menu, select **Dynamic**, and then enter a [dynamic date value](#)

Because of assumptions about the hours and days that comprise a model, do not specify a range that includes a shift in Daylight Savings Time. Also, the timestamp for events always represents the [Normalized Event Time](#).

6. Click **Create**.

The created model displays in the **Available Models** table with a status of **Created**.
7. From the **Available Models** table, select the model that you want to build.

You can build only one model at a time.
8. Click **Build**.
9. To evaluate incoming events against the model, you must [start the scoring process](#).

Scoring a Model

You must have Administrative permissions to score a model.

Select **Insights > Outliers**.

After you build a model, you can start a **scoring process** that evaluates incoming events against the model. The process assigns a score that indicates the degree to which the incoming data varies from typical behavior. By default, Outlier Analytics selects the current date as the scoring start date. You can only score one model at a time, but you can build another model while a different model is being scored.

To start the scoring process:

1. Select **Configuration > Outlier**.
2. From the **Available Models** table, select the model that you want to score.

The model must be in **Build Complete** status before you can score it.

3. Select **Score**.
4. Select the date for which you want to start the scoring process, then click **Start**.
Because of assumptions about the hours and days that comprise a model, do not use a model that you built with Daylight Savings Time data to score non-Daylight Savings Time data. Conversely, do not use a model that you built with non-Daylight Savings Time data to score Daylight Savings Time data.
5. (Conditional) To pause scoring because of performance or ingestion issues, select **Pause**.
If you selected a date in the past to start the scoring process, the scoring job runs frequently to catch up to the current date.
To allow any running scoring jobs to complete, wait 15 minutes before performing any other action such as deleting a model or resetting scoring.
6. (Conditional) To resume the scoring process from the point at which you paused it, select **Resume**. Alternatively, to restart the scoring process, select **Reset**.
7. To [view the scored data](#) when scoring completes, select **Insights > Outliers**.

Deleting a Model

You must have the Administrative permissions to delete a model.

When you delete a model, Outlier Analytics deletes the model definition and all scores that are based on that model.

To delete a model:

1. Select **Configuration > Outlier**.
2. From the **Available Models** table, select the model that you want to delete.
3. Click **Delete**.

Chapter 12: Viewing Anomalous Data in a Model

Select **Insights > Outliers**.

After you specify search criteria for the data that you want to view in the model, Outlier Analytics displays the top anomalous hosts that meet the criteria. When you select a host from the **Top Anomalous Hosts** table, the feature generates charts that provide more information about the anomaly scores.

The scores are calculated for five-minute chunks, so each source address can have multiple outlier scores each hour. When listing the top anomalous hosts, Outlier Analytics shows the maximum scores for each source address for each hour. If the specified search criteria included a filter, the scores represent results after being filtered.

- ["Understanding the Provided Analytics Charts" below](#)
- ["Investigating Anomalies Further" on the next page](#)
- ["Viewing a Scored Model" on the next page](#)

Understanding the Provided Analytics Charts

Each Outlier Analytics model includes the following charts:

Outlier Scores History

Compares anomaly scores of the top anomalous hosts for one week from the specified **End time**.

Use this chart if you suspect a lateral attack. To view details about the score for a specific date and hour, hover over the corresponding area in the chart.

Selected Anomalous IP

Shows the anomaly score for the host that you selected for two weeks from the specified **End time**.

If you suspect that a host is under attack (for example, from ex-filtration malware), use this chart to study the behavior of the IP address over time and identify anomalous patterns. To view details about a data point, hover over it.

Selected Anomaly Hour

Compares the anomaly score for the host that you selected to the top 30 hosts for the anomaly hour.

If you suspect that a network is under attack (for example, a denial of service attack), use this chart to study the behavior of other top 30 hosts during the anomaly hour. To view more details, hover over a bar in the chart, click and drag to move within the chart, and double-click to reset it to its default view.

Investigating Anomalies Further

After you view the outlier data, you can use the action available from the grid rows in the **Top Anomalous Hosts** table to further investigate anomalies:

Search for <IP_Address>

Searches events for the host and time range for which you selected to view scoring data and displays the results on the **Search** page.

Viewing a Scored Model

1. Select **Insights > Outliers**.
2. Specify the outlier metric that you want to view: **EventCount**, **BytesIn**, or **BytesOut**.
3. For the search query, specify any of the following criteria that you want to apply to the data:
 - Base Event Count Score of
 - Bytes In Score of <Model_Name>
 - Bytes Out Score of <Model_Name>
 - Source Address of <Model_Name>
 - Start Time of <Model_Name>
4. Click **Detect**.

5. Specify a valid time range to view the scored data.

Time range selector displays the valid date range in the date selection area to ensure that you specify a valid date range. Scoring data is performed hourly so the time range for detection is in an hourly format (YYYY-MM-DD HH). End time hour is inclusive. If the end time is 2019-05-21 05, the scoring data from 2019-05-21 05:00-06:00 will be included. To help you select time range for detection, the time range selector displays **Score Available Range**.

6. Wait while Outlier Analytics processes the request and generates the **Top Anomalous Hosts** table and the **Outlier Scores History** table.



CAUTION: If Outlier Analytics retrieves a large amount of data, the search might pause. You must allow the feature to populate the **Top Anomalous Hosts** table before you click **Play** to resume the search. Otherwise, the table will not be displayed.

7. (Optional) To generate the remaining charts, select a row in the **Top Anomalous Hosts** table.
8. (Optional) To use the filter action in your investigation, complete the following steps:
 - a. Right-click a row in the grid.
 - b. Select **Search for <IP_Address>**.

IV Managing the Quality of Your Data

Select **Insights** > **Data Quality**.

Data Quality Dashboard provides detailed information about the gap between [Device Receipt Time](#) from the raw event itself versus the Normalized Event Time. Data Quality Dashboard identifies the sources that cause issues with the data. Based on the information analyzed through the Data Quality Dashboard, you can accurately mitigate the problem. This feature also provides history of your data over time.

- ["Understanding the Data Quality Insights" on page 122](#)
- ["Understanding How Data Quality is Calculated" on page 123](#)
- ["Analyzing Data Quality" on page 124](#)

Chapter 13: Understanding the Data Quality Insights

Content in the [Data Quality Dashboard](#) is divided into categories that represent how big the gaps are between Device Receipt Time and Normalized EventTime:

Future Events

Indicates that events have a future timestamp in them. This category uses the following formula:

$$\text{Normalized Event Time (NET)} - \text{Device Receipt Time (DRT)} < 0$$

Past Events

Indicates that events have a past timestamp in them. This category uses the following formula:

$$\text{Normalized Event Time (NET)} - \text{Device Receipt Time (DRT)} > 0$$

Active Events

Indicates that your events have a timestamp within the database's active time-frame. This category uses the following formula:

$$\text{Normalized Event Time (NET)} - \text{Device Receipt Time (DRT)} = 0$$

Chapter 14: Understanding How Data Quality is Calculated

Data Quality is calculated and aggregated every one hour, including all events that arrive in the database within the same hour. For example, the aggregated information at 10:00 AM includes all data from 10:00:00.000 to 10:59:59.999, inclusively. The time of the aggregation process depends on when the product was installed or upgraded:

- During a fresh installation, the process creates a new table to store Data Quality overtime with source information. The feature schedules the aggregation process at the tenth minute of every hour. For example, if a fresh install was performed at 9:15:00 AM, the aggregation would be scheduled to execute at 10:10:00 AM and every one hour after that.
- After an upgrade, previous data will be dropped because they are no longer relevant to new categories. For example, if an upgrade was performed at 9:15:00 AM, the aggregation would be scheduled to execute at 10:10:00 AM to aggregate all events from 9:00:00.000 to 9:59:59.999 AM, inclusive. Then it will run every one hour after that.

If you switch to a different database, you would need to wait for a few minutes before accessing the Data Quality page again.

Chapter 15: Analyzing Data Quality

Select **Insights > Data Quality**.

The Dashboard provides the following visualizations to help you gain insight into quality of your data.

Date Picker Filter

Provides options to filter the time range for the entire Data Quality Dashboard page, including built-in Custom Range and Quick Ranges. By default, the Dashboard displays data per the **Last 7 days** setting. If the Cron Job has not been run yet, the charts would display no data.

Data Timeseries

Represents, in a stacked area chart, how data is distributed among the Categories by percentage over time.

Source Agents

This visualization group consists of the following components:

1. Top 10 Agents from Future Events

Represents the percentages of up to 10 top agents with the greatest amount of events under the selected Data Categories. To see the IP address, hostname, and number of events of each source, hover over each donut piece. If you click a donut piece, Outlier Analytics displays additional details in the Data Timeseries side chart.

2. Hourly Event Volume

Shows, in a bar chart, the number of events from a source that contributed to the selected Data Categories. If available, the source with the highest number of events will be displayed by default.

V Managing Your Stored Data

You must have the Manage Storage Groups permission to use this feature.

Search performance can be affected by your environment's set up and the way that your data is organized. To enable faster search times, you can configure Recon to organize data into [storage groups](#), which represent partitions in the ArcSight database.

These storage groups can support compliance requirements for data retention policies, such as those for the Payment Card Industry Data Security Standard (PCI DSS). For example, you might be required to retain certain data for 12 to 24 months. You can instruct Recon to [purge](#) data that is older than a certain number of months. By deleting data, you reduce the amount of content within the database and improve search performance.

- ["Organizing Your Data" on page 126](#)

Chapter 16: Organizing Your Data

You must have the Manage Storage Groups permission to use this feature.

Select **Configuration > Storage**.

The **Storage Information** list provides an overview of all available [storage groups](#). You can have up to 10 storage groups, each with specific retention periods and query filters. To find a storage group, use the **Search** field.

- ["Using Storage Groups to Organize and Retain Data" below](#)
- ["Activating and Deactivating Storage Groups" on page 128](#)
- ["Changing the Settings of a Storage Group" on page 128](#)
- ["Setting Retention Policies for the Data" on page 129](#)
- ["Using Storage Group Queries in a Search" on page 130](#)

Using Storage Groups to Organize and Retain Data

Recon can divide data into **storage groups**, which allows you to partition the incoming events data and provide different retention periods, based on the query filter. Because you can set [data retention policies](#) per storage group, you can retain certain high volume events for a short time period and other important events for longer time period.

The **query filter** enables you to associate a storage group with specific compliance requirements, business needs, or search activities. Recon uses the specified query filters to direct events to the correct storage group. For example, one group might have a filter for `categoryDeviceGroup =/ Firewall` and another for `severity >= 7`. If an event does not match any of the active filters, Recon sends the event to the *Default Storage Group*. You cannot change the name, query, or rank of this built-in group.

Recon displays a **Apply Changes to System** option at the top of the Storage Groups page to let you know that one or more groups have been modified but the [changes need to be applied](#) yet.


- ["Creating a Storage Group" on the next page](#)
- ["Directing Events to the Correct Storage Group" on the next page](#)

Creating a Storage Group

Recon allows you to have up to **10 storage groups**, including the provided *Default Storage Group*.

To create a storage group:

1. Select **Configuration > Storage**.
2. Click **+**.
3. Enter a name for the storage group.

 You cannot change the name after you create the group. Also, the name cannot include special characters.

4. Enter a query with which to filter the incoming events into this storage group.
For example, `categoryDeviceGroup='/Firewall'` or `categoryDeviceGroup='/IDS'`.
The query can include parentheses, quotes, and single quotes.
5. For the storage group's status, indicate whether to [activate the group](#).
6. (Optional) For **Delete Data Older than**, enter the age of data, in months, that you want to [purge](#) from the storage group in the database.
7. Click **Save**.
8. [Apply your changes](#).

Directing Events to the Correct Storage Group

For efficient data retrieval, Recon matches each incoming event with the query filter for single, active storage group. However, an event could be associated with the rules of more than one group. When an event matches with multiple storage groups, Recon **assigns the event to the highest ranked group**.

For example, *if Event_29* matches the query filter for the storage groups ranked 3, 5, and 6, then Recon assigns the event to the group that is ranked 3. If an event does not match any of the active filters, Recon sends the event to the *Default Storage Group*.

You can change the ranking of storage groups to ensure that Recon places events in the best location.


To change the ranking:

1. Select **Configuration > Storage**.
2. From the **Storage Information** table, drag each storage group up or down to the preferred priority position.
Recon always places the *Default Storage Group* in the lowest ranked position.

Activating and Deactivating Storage Groups

Recon allows you to have up to 10 **storage groups**, including the provided *Default Storage Group*. To inactive to prevent new events from being sent to the group, change a storage group's status. For example, you might no longer need a particular storage group or find that you have changed the filters and functionality of that group from its original purpose. Rather than continuing to modify an existing group, you can deactivate it. Alternatively, you might want to activate a storage group only during certain periods of time.

Although you deactivate a group, the [deletion](#) settings for that group remain in effect.

1. Select **Configuration > Storage**.
2. Select the storage group that you want to activate or deactivate.
3. Select .
4. For **Group Status**, slide the indicator left or right.
Activated groups will display a status of **Active**.
5. Select **SAVE**.


Changing the Settings of a Storage Group

After creating or modifying storage groups, you must apply the changes. You can modify multiple groups before applying your changes.

- ["Modifying a Storage Group" below](#)
- ["Applying Your Changes to a Storage Group" on the next page](#)

Modifying a Storage Group

You can modify a storage group at any time.

1. Select **Configuration > Storage**.
2. Select the storage group that you want to modify.
3. Select .
4. For **Group Status**, slide the indicator left or right.
5. Activated groups will display a status of **Active**.
6. Select **SAVE**.
7. "[Applying Your Changes to a Storage Group](#)" below.

Applying Your Changes to a Storage Group

Select **Configuration > Storage > Apply Changes to System**.

When you change the query filter, [status](#), or rank of a storage group, your changes do not go into effect until you apply the changes. The following considerations affect how your changes are applied:

- If you modify the query filter, Recon will begin adding events that match the updated filter. However, the storage group retains all currently stored events associated with the previous filter. The retention policies continue to apply to all events within the group.

If you do not want the storage group to have both sets of events, you can create a new storage group for the updated query filter, then [deactivate](#) the older storage group.

- On the first day of the month, Recon deletes events matching the [retention policies](#) of the storage groups. For example, on March 15, you change the deletion time to three months from four months. On April 1, Recon begins deleting all data older than three months.
- While changes are being applied, you cannot create or modify a storage group.

Setting Retention Policies for the Data

The Watchdog service in the database monitors system storage capacity. If the capacity exceeds a certain threshold then Watchdog tells the database to start deleting the oldest partitions until disk usage drops below the threshold. By default, the Watchdog threshold is 95% of capacity. To prevent the purging of needed data, you can use storage groups to set retention policies for [deleting](#) specific data.

When setting the policies for storage group retention and disk space utilization, do not allow your storage group utilization to increase above 90%. As storage groups near 99% utilization, they start running out of disk space, which reduces the performance of searches due to increasing fragmentation.

- ["Deleting Old Data" below](#)

For more information about Watchdog, see the [Administrator's Guide to ArcSight Platform](#) on the ArcSight documentation site.

Deleting Old Data

Events are stored in their assigned storage groups either in the ArcSight database. Over time, the storage system can retain unneeded or outdated data. To preserve space in the database and improve data retrieval from storage groups, you can configure the database to remove events older than a certain number of months. For example, your data retention policy might expect data older than 24 months to be purged. This process **deletes data from the database**.

Search automatically applies all deletion settings on the first day of the month at 2:10 a.m.

1. [Create](#) or [modify](#) a storage group.
2. For **Delete Data Older Than**, enter the age of data, in months, that you want to be deleted.

Ensure that your retention policy takes into consideration the maximum size of your storage groups and database. If a storage group fills up, the oldest events could be purged automatically to make room for incoming events, even if the older events are within the retention period.

3. Click **Save**.
4. [Apply your changes](#).

Using Storage Group Queries in a Search

Search allows you to include a storage group in a query. Rather than entering the query filter of a storage group again in Search, [specify](#) the following for your Search query: `Storage Group = Firewall Events`. By specifying the storage group, you limit the search to that storage group's partitions only, thus improving search performance.

VI Using Visuals and Reports to Analyze Data

The **Reports** feature allows you to browse and filter your dataset and to visualize results in a dashboard. Rapidly discover meaningful trends and associations that yield actionable intelligence. Leverage the included MITRE ATT&CK, cloud-based, system, and foundational reports and dashboards to quickly launch [threat-hunting](#) exercises.

Depending on your [assigned permissions](#), you can view, schedule, design, or manage reports and dashboards.

- ["Accessing Reports and Dashboards" below](#)
- ["Scheduling Report Generation" below](#)
- ["Designing Dashboards for Data Analysis" on the next page](#)
- ["Designing Reports for Data Analysis" on the next page](#)

Accessing Reports and Dashboards

You must have one of the [Reports permissions](#) to use this feature.

Select **Reports** > **Portal**.

The Reports **Portal** provides a repository of built-in reports and dashboards for data analysis, including MITRE ATT&CK content for use in threat hunting. You add custom reports and dashboards by collecting and filtering data from your connected sources. The Reports feature supports the ability to drill down into specific elements for thorough data reviews.

The built-in admin reports enable a report administrator track use of the Portal.

Scheduling Report Generation

*You must have the **Report Admin** or **Schedule Reports** permission to use this feature.*

Select **Reports** > **Scheduler**.

The Reports **Scheduler** enables you to schedule and manage batch report generation. You can create one or more scheduled tasks for which you specify a time condition, reports to be generated, and delivery mechanism of the generated output.

The Reports feature can output the reports in formats such as PDF and Excel. The Scheduler can send the reports in email them.

Designing Dashboards for Data Analysis

*You must have the **Report Admin** or **Design Reports** permission to use this feature.*

Select **Reports** > **Dashboard Designer**.

Dashboard Designer provides a wizard that allows you to create new dashboards using the bundled Standard Content data worksheets. . You can dynamically filter a dataset and visualize the output on tables, charts, and gauges. The Designer saves all attributes and related information in a template file in XML format.

The Designer offers you the same functionality as an API, but makes most tasks, such as report layout, much simpler. You can also use the Designer to attach scripts to embed business logic into the report.

Designing Reports for Data Analysis

*You must have the **Report Admin** or **Design Reports** permission to use this feature.*

Select **Reports** > **Report Designer**.

Report Designer provides a wizard that allows you to create new reports using the bundled Standard Content data worksheets. You can design elements, change their attributes, and control all aspects of element presentation and layout. The Designer saves all attributes and related information in a template file in XML format.



NOTE: When you create a query in a report, Report Design displays the coding-style name for search fields. For more information, see [Mapping Database Names to their Appropriate Search Fields](#).

The Designer offers you the same functionality as an API, but makes most tasks, such as report layout, much simpler. You can also use the Designer to attach scripts to embed business logic into the report.

VII Managing User Access and Preferences

The Fusion capability in the ArcSight Platform supports user management, where you can add users, create roles, and assign roles. Recon adds a role and several permissions to the common set of roles and permissions available with Fusion. As a user, you can specify the settings that you prefer to use for all searches.

- ["Assigning Permissions for Recon" on page 135](#)
- ["Understanding Default Roles for Recon" on page 136](#)
- ["Configuring User Preferences" on page 137](#)

Chapter 17: Assigning Permissions for Recon

To view your permissions, select **your_ID > My Profile > Permissions**.

To assign permissions to a role, select **ADMIN > Roles**.

Recon includes specific permissions for accessing or managing the following activities:

- Using [Search](#)
- Running and developing [reports](#)
- Managing [storage groups](#)
- Monitoring the database with widgets in the Dashboard

For more information about these permissions or assigning them to a role, select **ADMIN > Help** or see the [User Guide for Fusion in the ArcSight Platform](#).

Chapter 18: Understanding Default Roles for Recon

Select **ADMIN** > Roles.

When you deploy Recon, Fusion adds Recon's [permissions](#) to the default roles:

- System Admin
- Admin
- Analyst L1
- Guest
- User
- Report User (default role to support the Reports portal)

Fusion also adds a default role to support the [Reports](#) portal: the Report User role.

For more information about assigning these roles, select **ADMIN** > **Help** or see the [User Guide for Fusion in the ArcSight Platform](#).

Chapter 19: Configuring User Preferences

Select `[your_ID]` > **My Profile** > **Preferences**.

Some deployed capabilities enable you to configure preferences for commonly used settings. For example, in Recon, if you regularly use the same fieldset for a Search, you can specify that set as your preferred default.

- ["Configure Search Preferences" below](#)

Configure Search Preferences

Available only when ArcSight Recon is deployed in your environment

To reduce the time required to create and manage searches, configure Search to use your preferred settings. You can always override your preferences as needed when you create a search. When you modify your Search preferences, the changes apply to new searches. Existing searches are not affected unless you re-run the search.

Default Fieldset

Specifies the [fieldset](#) you regularly use for a search. The default value is *Base Event Fields*.

Default View

Specifies if the [Events Table](#) displays results in the Grid View or Raw View. The default value is *Grid View*.

Time Zone

Instructs Search to adjust the timestamp for events to the chosen [time zone](#).

Date/Time Format

Specifies the format of dates and times you want Search to use. The default is *MM/DD/YY*.

Default Time Setting

Specifies the time range you want Search to find events. The default is *Last 30 minutes*.

Base Searches On

Specifies the [timestamp](#) Recon associates with the event you want to find. The default value is Normalized Event Time.

Search Expires In

Specifies how often you want searches to expire, and thus Recon to remove them from the system. Alternatively, you can choose to never remove a search.

Also, the expiration date resets whenever you access the search. Resetting the date includes resuming or re-running the search, as well as saving the search. The default value is 7 days.

Maximum Search Results

Specifies the maximum number of events Search returns. Search considers a search complete when the results reach the maximum limit. The default value is 10,000,000.

Highlight Query Syntax

Specifies whether Search uses color to differentiate the syntax terms from the operators and functions within the query. The default value is Yes per default.

VIII Appendices

The appendices in this guide provide additional information or guidance for using the features and functions for this product.

- ["A Mapping Database Names to their Appropriate Search Fields" on the next page](#)

A Mapping Database Names to their Appropriate Search Fields

When creating a fieldset, Search displays the coding-style name for the fields instead of the human-readable names that you see when creating a query. For example, in a query you can enter or select Agent Address. However, in the fieldsets selection, this same field appears as agentAddressBin. This issue also occurs when you're adding queries to a Report.

The following tables provide the coding-style names that appear in the fieldset and report configurations, so that you can easily map them to their human-readable names.

- ["Agent Fields" below](#)
- ["Category Fields" on the next page](#)
- ["Correlation Fields" on the next page](#)
- ["Destination Fields" on page 142](#)
- ["Device Fields" on page 143](#)
- ["Device Custom Fields" on page 144](#)
- ["Event Fields" on page 145](#)
- ["Extension Fields" on page 146](#)
- ["File Fields" on page 146](#)
- ["Flex Fields" on page 147](#)
- ["OldField Fields" on page 147](#)
- ["Old File Fields" on page 147](#)
- ["Request Fields" on page 148](#)
- ["Source Fields" on page 148](#)

Agent Fields

Substitute the following labels in the agent category:

For the field that you want to add...	You should choose...
Agent Address	agentAddressBin
Agent DNS Domain	agentDnsDomain
Agent Hostname	agentHostName

Agent ID	agentId
Agent Mac Address	agentMacAddressBin
Agent NT Domain	agentNtDomain
Agent Receipt Time	agentReceiptTime
Agent Severity	agentSeverity
Agent Timezone	agentTimeZone
Agent Translated Address	agentTranslatedAddressBin
Agent Translated Zone External ID	agentTranslatedZoneExternalID
Agent Translated Zone URI	agentTranslatedZoneURI
Agent Type	agentType
Agent Version	agentVersion
Agent Zone External ID	agentZoneExternalID
Agent Zone URI	agentZoneURI

Category Fields

Substitute the following labels in the category:

Category Behavior	categoryBehavior
Category Device Group	categoryDeviceGroup
Category Device Type	categoryDeviceType
Category Object	categoryObject
Category Outcome	categoryOutcome
Category Significance	categorySignificance
Category Technique	categoryTechnique
Version	version

Correlation Fields

Substitute the following labels in the correlation category:

Substitute the following labels in the correlation category:	You should choose...
Base Event Ids	correlated_event_id

Correlated Event Id	generatorURI
Generator External ID	generatorExternalID
Generator URI	base_event_ids
Priority	priority

Destination Fields

Substitute the following labels in the destination category:

For the field that you want to add...	You should choose...
Destination Address	destinationAddressBin
Destination DNS Domain	destinationDnsDomain
Destination Geo Country Code	destinationGeoCountryCod
Destination Geo Latitude	destinationGeoLatitude
Destination Geo Longitude	destinationGeoLongitude
Destination Geo Postal Code	destinationGeoPostalCode
Destination Geo Region Code	destinationGeoRegionCode
Destination Geolocation Info	destinationGeoLocationInfo
Destination Hostname	destinationHostName
Destination Mac Address	destinationMacAddressBin
Destination NT Domain	destinationNtDomain
Destination Port	destinationPort
Destination Process ID	destinationProcessId
Destination Process Name	destinationProcessName
Destination Service Name	destinationServiceName
Destination Translated Address	destinationTranslatedAddressBin
Destination Translated Port	destinationTranslatedPort
Destination Translated Zone External ID	destinationTranslatedZoneExternalID
Destination Translated Zone URI	destinationTranslatedZoneURI
Destination User ID	destinationUserId
Destination User Privileges	destinationUser Privileges

Destination Username	destinationUserName
Destination Zone External ID	destinationZoneExternalID
Destination Zone URI	destinationZoneURI

Device Fields

Substitute the following labels in the device category:

For the field that you want to add...	You should choose...
Device Action Device Event Class ID deviceEventClassId	deviceAction
Device Address	deviceAddressBin
Device Asset ID	deviceAssetID
Device Direction	deviceDirection
Device DNS Domain	deviceDnsDomain
Device Domain	deviceDomain
Device Event Category	deviceEventCategory
Device Inbound Interface	deviceInboundInterface
Device Event Class ID	deviceEventClassId
Device External ID	deviceExternalId
Device Facility Hostname	deviceFacility
Device Hostname	deviceHostName
Device Mac Address	deviceMacAddressBin
Device NT Domain	deviceNtDomain
Device Outbound Interface	deviceOutboundInterface
Device Process ID	deviceProcessId
Device Process Name	deviceProcessName
Device Product	deviceProduct
Device Receipt Time	deviceReceiptTime
Device Severity	deviceSeverity
Device Timezone	deviceTimeZone
Device Translated Address	deviceTranslatedAddressBin
Device Translated Zone External ID	deviceTranslatedZoneExternalID

Device Translated Zone URI	deviceTranslatedZoneURI
Device Version	deviceVendor
Device Version	deviceVersion
Device Zone External ID	deviceZoneExternalID
Device Zone URI	deviceZoneURI
Normalized Event Time	normalizedEventTime

Device Custom Fields

Substitute the following labels in the device custom category:

For the field that you want to add...	You should choose...
Device Custom Date 1	deviceCustomDate1
Device Custom Date 1 Label	deviceCustomDate1Label
Device Custom Date 2	deviceCustomDate2
Device Custom Date 2 Label	deviceCustomDate2Label
Device Custom Descriptor ID	deviceCustomDescriptorId
Device Custom Floating Point 1	deviceCustomFloatingPoint1
Device Custom Floating Point 1 Label	deviceCustomFloatingPoint1Label
Device Custom Floating Point 2	deviceCustomFloatingPoint2
Device Custom Floating Point 2 Label	deviceCustomFloatingPoint2Label
Device Custom Floating Point 3	deviceCustomFloatingPoint3
Device Custom Floating Point 3 Label	deviceCustomFloatingPoint3Label
Device Custom Floating Point 4	deviceCustomFloatingPoint4
Device Custom Floating Point 4 Label	deviceCustomFloatingPoint4Label
Device Custom Number 1	deviceCustomNumber1
Device Custom Number 1 Label	deviceCustomNumber1Label
Device Custom Number 2	deviceCustomNumber2
Device Custom Number 2 Label	deviceCustomNumber2Label
Device Custom Number 3	deviceCustomNumber3
Device Custom Number 3 Label	deviceCustomNumber3Label
Device Custom String 1	deviceCustomString1

For the field that you want to add...	You should choose...
Device Custom String 1 Label	deviceCustomString1Label
Device Custom String 2	deviceCustomString2
Device Custom String 2 Label	deviceCustomString2Label
Device Custom String 3	deviceCustomString3
Device Custom String 3 Label	deviceCustomString3Label
Device Custom String 4	deviceCustomString4
Device Custom String 4 Label	deviceCustomString4Label
Device Custom String 5	deviceCustomString5
Device Custom String 5 Label	deviceCustomString5Label
Device Custom String 6	deviceCustomString6
Device Custom String 16 Label	deviceCustomString6Label
Device CustomIPv6 Address 1	deviceCustomIPv6Address1Bin
Device CustomIPv6 Address 1 Label	deviceCustomIPv6Address1Label
Device CustomIPv6 Address 2	deviceCustomIPv6Address2Bin
Device CustomIPv6 Address 2 Label	deviceCustomIPv6Address2Label
Device CustomIPv6 Address 3	deviceCustomIPv6Address3Bin
Device CustomIPv6 Address 3 Label	deviceCustomIPv6Address3Label
Device CustomIPv6 Address 4	deviceCustomIPv6Address4Bin
Device CustomIPv6 Address 4 Label	deviceCustomIPv6Address4Label

Event Fields

Substitute the following labels in the event category:

For the field that you want to add...	You should choose...
Application Protocol	applicationProtocol
Base Event Count	baseEventCount
Bytes In	bytesIn
Bytes Out	bytesOut
Crypto Signature	cryptoSignature
Customer External ID	customeExternalID

For the field that you want to add...	You should choose...
Customer URI	customerURI
End Time	endTime
Event ID	eventId
Event Outcome	eventOutcome
External Id	externalID
Locality	locality
Message	message
Name	name
Originator	originator
Reason	reason
Start Time	startTime
Transport Protocol	transportProtocol
Type	type

Extension Fields

Substitute the following labels in the extension category:

For the field that you want to add...	You should choose...
Extra Fields	extraFields
Storage Group	storageGroup

File Fields

Substitute the following labels in the file category:

For the field that you want to add...	You should choose...
File Create Time	fileCreateTime
File Hash	fileHash
File ID	fileId
File Modification Time	fileModificationTime
File Name	fileName

For the field that you want to add...	You should choose...
File Path	filePath
File Permission	filePermission
File Size	fileSize
File Type	fileType

Flex Fields

Substitute the following labels in the flex category:

For the field that you want to add...	You should choose...
Flex Date 1	flexDate1
Flex Date 1 Label	flexDate1Label
Flex Number 1	flexNumber1
Flex Number 1 Label	flexNumber1Label
Flex Number 2	flexNumber2
Flex Number 2 Label	flexNumber2Label
Flex String 1	flexString1
Flex String 1 Label	flexString1Label
Flex String 2	flexString2
Flex String 2 Label	flexString2Label

OldField Fields

Substitute the following labels in the oldfield category:

For the field that you want to add...	You should choose...
Old File Create Time	oldFileCreateTime

Old File Fields

Substitute the following labels in the old file category:

For the field that you want to add...	You should choose...
Old File Hash	oldFileHash
Old File ID	oldFileId
Old File Modification Time	oldFileModificationTime
Old File Name	oldFileName
Old File Path	oldFilePath
Old File Permission	oldFilePermission
Old File Size	oldFileSize
Old File Type	oldFileType

Request Fields

Substitute the following labels in the request category:

For the field that you want to add...	You should choose...
Request Client Application	requestClientApplication
Request Context	requestContext
Request Cookies	requestCookies
Request Method	requestMethod
Request URL	requestUrl
Request URL FileName	requestUrlFileName
Request URL Query	requestUrlQuery

Source Fields

Substitute the following labels in the source category:

For the field that you want to add...	You should choose...
Source Address	sourceAddressBin
Source DNS Domain	sourceDnsDomain
Source Geo Country Code	sourceGeoCountryCode
Source Geo Latitude	sourceGeoLatitude
Source Geo Longitude	sourceGeoLongitude

For the field that you want to add...	You should choose...
Source Geo Postal Code	sourceGeoPostalCode
Source Geo Region Code	sourceGeoRegionCode
Source Geolocation Info	sourceGeoLocationinfo
Source Hostname	sourceHostName
Source Mac Address	sourceMacAddressBin
Source NT Domain	sourceNtDomain
Source Port	sourcePort
Source Process ID	sourceProcessId
Source Process Name	sourceProcessName
Source Service Name	sourceServiceName
Source Translated Address	sourceTranslatedAddressBin
Source Translated Port	sourceTranslatedPort
Source Translated Zone External ID	sourceTranslatedZoneExternalID
Source Translated Zone URI	sourceTranslatedZoneURI
Source User ID	sourceUserId
Source User Privileges	sourceUser Privileges
Source Username	sourceUserName
Source Zone External ID	sourceZoneExternalID
Source Zone URI	sourceZoneURI