ArcSight Recon 1.0

User Guide

July 2020

Legal Notice

Contents

About This Book

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

- Investigating Events
- Hunting for Undetected Threats
- Analyzing Anomalous Data with Outlier Analytics
- Managing the Quality of Your Data
- Using Visuals and Reports to Analyze Data
- Managing User Access

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 Recon documentation library includes the following resources:

- *Release Notes for ArcSight Platform*, which provides an overview of the products deployed in this suite and their latest features or updates
- *Administrator Guide for ArcSight Recon*, which provides information about deploying, configuring, and maintaining this product
- *Release Notes for ArcSight Recon*, which provides information about updates or new features available in the current release
- *Technical Requirements for ArcSight Recon*, which provides information about the hardware and software requirements for installing Recon

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/.

1 Welcome to ArcSight Recon

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
- Manage user access

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.

- Chapter 2, “Searching for Events,” on page 13
- Chapter 3, “Understanding the Search Parameters,” on page 19

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.

You can save, refresh, and edit your searches. To help you investigate events, Search displays the results as both a timeline and in a table. You can export the search results in the table to a CSV file.

Understanding the Search Feature

Recon ingests log data from SmartConnectors routed through ArcSight Transformation Hub. 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 that shows the number of events returned over event occurrence time. The Events table below the Timeline shows events returned by search.

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 the REST API.

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.

Understand 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.

Creating and Saving Searches

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

- “Create a Search” on page 14
- “Save a Search” on page 15
- “Name a Search” on page 15
- “Find a Saved Search” on page 15

Create 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, Recon suggests search items and operators based on a schema data dictionary. You can also choose from predefined queries.

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

1. Select Search > New Search.
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 that you want for the search results.

   By default, Recon displays the name of the last used 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** then enter a dynamic date value

6 Select **Search**.

   Recon 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**.

Save 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.

To permanently save your search:

1 (Optional) Give the search a name.

2 Select **Save**.

3 To view your search, select **Saved Searches**.

Name a Search

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

1 When viewing the search, select ✎ beside the search’s name.

2 Enter the custom name.

3 To save your changes, select the **Check** icon.

Find 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*.

Viewing Search Results

Search displays results in an **Events Timeline** and **Events** table. If connectors are configured to send raw events, the table can include **raw event data**.

- "View the Events Timeline" on page 16
- "View the Events Table" on page 16
- "Identify Fields without Data" on page 17
- "Refresh Search Results" on page 18

View 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**, then hover over the data point.

View 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. For example, you could view details about the agent, category, device, source, or severity. You can also view the raw data in the details.

View raw event data

When you select 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 that is 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.

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 select the **Wrench** icon, then deselect 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.

Identify 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

Refresh 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.

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.

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

Search exports data based on the specified fieldset for the search. The export process limits the file to one million event records.

3 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.

Understanding the Types of Search Queries

Search supports the following types of search queries:

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 then select the criteria that you want 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
#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 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*>
#Firewall Events	categoryDeviceGroup = /Firewall
#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
#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
#Windows Account Creation	deviceVendor = Microsoft AND deviceEventClassId = Microsoft-Windows-Security-Auditing:4720, Security:624

Creating the Search Query

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."

- "Understand the Query Syntax Requirements" on page 21
- "Understand the Search Query Functions and Operators" on page 23
- "Understand the Functions for Building Eval Expressions" on page 25
- "Specify a Group of Fields" on page 31
- "Specify an Alias for a Field" on page 31

Understand 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.

Type	**Full-text**	**Field-based**	**Hashtag (predefined)**
Case sensitivity	Case-sensitive	Case-sensitive	Case-insensitive
Exact Match	Keyword treated as keyword*. Example: /Execute matches: /Execute, /Execute/Start, /Execute/Response,/Execute/Query	Enclose value in double quotes. Example: `Category Behavior ="/Execute"`	n/a
Nesting, including parenthetical clauses, such as (a OR b) AND c	Allowed Use Boolean operators to connect and nest keywords.	Allowed Use Boolean operators to connect and nest keywords.	Allowed Use Boolean operators to connect and nest keywords

Type	Full-text	Field-based	Hashtag (predefined)
Implicit Operators	When you enter two values separated by a space, this is treated as an implicit AND condition. Example: `ssh fail`	The AND/OR treatment depends on the operator used in the search. 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,` 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`	n/a
List Operations	n/a	Performs an inner join or a left join against a custom list. *Syntax for an Inner Join:* `source address in list CustomListName_CustomColumn Name` *Syntax for a Left Join:* `source address not in list CustomListName_CustomColumnName`	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: ◆ in between (><) ◆ greater than (>) ◆ less than (<)	n/a

Type	Full-text	Field-based	Hashtag (predefined)
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: name=log*	n/a

Understand 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

Operator	Alternative Operator	Examples
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 src
where	n/a	| where Bytes In >= 3000 | where Category Outcome = /Success

Understand 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 page 25
- "Cryptographic Function" on page 25
- "Informational Function" on page 26
- "Mathematical Functions" on page 26
- "Statistical Functions" on page 27
- "Text Functions" on page 28
- "Trigonometry Functions" on page 29

Comparison and Conditional Functions

Function	Description	Example
coalesce(*X*[, *Y*, *Z*,*N*, ...])	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. In the list of expressions all elements must be of same type. The only supported types are numeric and string. *X* can be a number, field or expression.	... | eval newField = coalesce(null, null,2,3) *Returns*: 2
nullif(*X*,Y)	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. *X* and *Y* can be a number, field or expression. *Y* must have same data type that *X*.	... | eval newField = nullif(2, 3) *Returns*: 2 ... | eval newField = nullif(2, 2) *Returns*: null

Cryptographic Function

Function	Description	Example
md5(*X*)	Calculates the MD5 hash of string, returning the result as a VARCHAR string in hexadecimal. *X* must be a string.	... | eval newField = md5('123') *Returns*: 202cb962ac59075b964b07152d234b70

Informational Function

Function	Description	Example
isnull(*X*)	Returns true if the *X* is null otherwise returns false.	... | eval newField = isnull(2) *Returns*: false

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) *Returns*: 8
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) *Returns*: n=2
exp(*X*)	Takes a number, *X*, and returns e*X*. *X* can be a number, field or expression.	... | eval y=exp(3) *Returns*: y=20.0855369231877
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) *Returns*: 1
mod(*X*, *Y*)	Returns the modulo of *X* and *Y*. (*X*%*Y*; the remainder of *X* divided by *Y*.)	... | eval newField = mod(25,10) *Returns*: 5
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) *Returns*: 8

Function	Description	Example
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) *Returns*: 1 ... | eval n=round(1.5) *Returns*: 2
sign(*X*)	Returns a value of -1, 0, or 1 representing the arithmetic sign of the argument.	... | eval newField = sign(-8.4) *Returns*: -1 ... | eval newField = sign(4) *Returns*: 1 ... | eval newField = sign(0) *Returns*: 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) *Returns*: 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) *Returns*: 1 ... | eval newField = trunc(2.89999, 2) *Returns*: 2.89

Statistical Functions

Function	Description	Example
greatest(*X*,*Y*[,*Z*,*N*, ...])	Returns the largest value in a list of expressions. The list is up to 20 elements long. In the list of expressions all elements must be of same type. The only supported types are numeric and string. *X* can be a number, field or expression.	... | eval newField = greatest(7, 5, 9) *Returns*: 9 ... | eval newField = greatest('sit', 'site', 'sight') *Returns*: site ... | eval newField = greatest(bytesIn, 100) *Returns*: 100, when bytesIn is less than 100

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

Text Functions

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

Function	Description	Example
substr(*X*,*Y*,*Z*)	This function returns a new string that is a substring of string *X*. The substring begins with the character at index *Y* and extends up to the character at index *Z*-1. The index is a number that indicates the location of the characters in string *X*, from left to right, starting with zero. *Y* can be negative. *Z* cannot be negative.	...| eval n=substr("ArcSight", 5, 6) *Returns*: "g" ...| eval n=substr("ArcSight", 2, 6) *Returns*: "cSig" ...| eval n=substr("ArcSight", 0, 3) *Returns*: "Arc"

trim(*X*)
ltrim(*X*)
rtrim(*X*)
	trim(*X*) removes all spaces from both sides of the string *X*.
	ltrim(*X*) removes all spaces from the left side of the string *X*.
	rtrim(*X*) removes all spaces from the right side of the string *X*.
		For the sake of these examples, assume that *X* is a literal string and _ represents any number of space characters.
		... | eval trimmed=ltrim("_string_")
		Returns: trimmed="string_"
		... | eval trimmed=rtrim("_string_")
		Returns: trimmed="_string"
		... | eval trimmed=trim("_string_")
		Returns: "string"

upper(*X*)	Takes one string argument and returns the uppercase version.	... | eval name=upper("username") ... | eval name=toupper("username") *Returns*: the value of the field username in uppercase. If username contains fred brown, it returns name=FRED BROWN.

Trigonometry Functions

Function	Description	Example
acos(*X*)	Takes one numeric argument, *X*, and returns its trigonometric inverse cosine.	...| eval newField = acos(0.3) *Returns*: 1.2661036727795

Function	Description	Example
asin(*X*)	Takes one numeric argument, *X*, and returns its trigonometric inverse sine.	...| eval newField = asin(3) *Returns*: 0.304692654015398
atan(*X*)	Takes one numeric argument, *X*, and returns its trigonometric inverse tangent.	...| eval newField = atan(3) *Returns*: 0.291456794477867
atan2(*X*,*Y*)	Returns a value representing the trigonometric inverse tangent of the arithmetic dividend of the arguments.	...| eval newField = atan2(2,1) *Returns*: 1.10714871
cos(*X*)	Takes one numeric argument, *X*, and returns its trigonometric cosine.	...| eval newField = cos(3) *Returns*: 2435538
cosh(*X*)	Takes one numeric argument, *X*, and returns its hyperbolic cosine.	...| eval newField = cosh(3) *Returns*: 10.0676619957778
cot(*X*)	Takes one numeric argument, *X*, and returns its trigonometric cotangent.	...| eval newField = cot(3) *Returns*: -7.01525255143453
ln(*X*)	Takes a number, *X*, and returns its natural log. *X* can be a number, field or expression.	... | eval lnBytes=ln(bytesIn) *Returns*: the natural log of the value of " bytesIn". If "bytesIn" contains 100, returns 4.605170186.
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) *Returns*: 0.301 ... | eval test1 = log (2) *Returns*: 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) *Returns*: 4
sin(*X*)	Takes one numeric argument, *X*, and returns its trigonometric sine.	...| eval newField = sin(3) *Returns*: 0.141120008059867
sinh(*X*)	Takes one numeric argument, *X*, and returns its hyperbolic sine.	...| eval newField = sinh(3) *Returns*: 10.0178749274099
tan(*X*)	Takes one numeric argument, *X*, and returns its trigonometric tangent.	...| eval newField = tan(3) *Returns*: -0.142546543074278
tanh(*X*)	Takes one numeric argument, *X*, and returns its hyperbolic tangent.	...| eval newField = tanh(3) *Returns*: 0.99505475368673

Specify 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...
category	All category fields
custom float	All custom float fields
domain	All domain fields
hostname	All hostname columns
id	All ID columns
ip	All IP address columns
ip6	All IPv6 address columns
label	All label columns
mac	All MAC address columns
path	All path columns
port	All port columns
timestamp or time	All time columns (device receipt time, agent receipt time)
uri	All URI columns
url	All URL columns
username or user	All user columns

Specify 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

Field	Aliases
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
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

Field	Aliases
destinationuserId	duid
destinationUserName	duser dst user dest user destination user dst usr
destinationUserPrivileges	dpriv
deviceAction	act
deviceAddress	dvc deviceaddr deviceip device ip
deviceCustomFloatingPoint*n*	cfp*n*
Valid values for *n* are integers between 1 and 4 For example: deviceCustomFloatingPoint1	For example: cfp1
deviceCustomFloatingPoint*n*Label	cfp*n*Label
Valid values for *n* are integers between 1 and 4 For example: deviceCustomFloatingPoint1Label	For example: cfp1Label
deviceCustomIPv6Address*n*	c6a*n* device custom ipv6 *n*
Valid values for *n* are integers between 1 and 4 For example: deviceCustomIPv6Address2	For example: c6a2
deviceCustomIPv6Address*n*Label	c6a*n*Label
Valid values for *n* are integers between 1 and 4 For example: deviceCustomIPv6Address2Label	For example: c6a2Label
deviceCustomNumber*n*	cn*n*
Valid values for *n* are integers between 1 and 3 For example, deviceCustomNumber3	For example: cn3
deviceCustomNumber*n*Label	cn*n*Label
Valid values for *n* are integers between 1 and 6 For example: deviceCustomNumber6Label	For example: cn6Label
deviceCustomString*n*	Cs*n*
Valid values for *n* are integers between 1 and 6 For example: deviceCustomString5	For example: Cs5
deviceEventCategory	cat
deviceHostName	dvchost

Field	Aliases
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
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.

- "How Search Stores IP and MAC Addresses" on page 35
- "Enter an IP or MAC Address" on page 35

How Search Stores IP and MAC Addresses

Search stores IPv4, IPv6, and MAC adresses 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.

Enter 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 a-b-c-d-e-f	94:18:82:6D:63:74 94-18-82-6D-63-74

Creating and Applying Sets of Fields to Include in Searches

You can specify a **fieldset** that determines a group of search result fields to be displayed in the Events table. In the table, each field in the set can provide the 10 most and least common values. Multiple searches can share a fieldset. Search provides a default fieldset that contains the most common event fields. You can customize the default fieldset for individual searches, and you can add lookup list fields to a fieldset.

- "Create a Fieldset" on page 36
- "Modify a Fieldset" on page 37
- "Specify a Default Fieldset" on page 37
- "Delete a Fieldset" on page 38

Create a Fieldset

1 Select Search.

2 Select the name of the current fieldset (shown to the left of the time range selector).

By default, Search displays the name of the last used fieldset.

3 In the **Fieldset Lists** window, select **Create New**.

4 Select and/or deselect the desired fields.

5 To view the complete list of available fields, click **View all**.

6 To locate a specific field, use the search field.

7 To add fields from a lookup list, complete the following steps:

  7a Select **Lookup Lists**.

  7b Under the name of the desired lookup list, select the fields that you want to include.

8 Specify a name for the new fieldset.

9 Select **Save**.

Modify a Fieldset

1 Select **Search**.

2 Select the name of the current fieldset (shown to the left of the time range selector).

By default, Search displays the name of the last used fieldset.

3 If the last used fieldset is not the fieldset that you want to edit, select another fieldset from the drop-down menu.

4 Select **Edit**.

5 Select and/or deselect the desired fields.

When you remove a field from a fieldset, Search removes all filters and charts that use that field.

6 Change the name of the fieldset as needed.

7 Add lookup list fields as needed.

8 Select **Save**.

Specify a Default Fieldset

You must have Administrator permissions to perform this action.

You can create a default fieldset to provide a limited number of returned fields and thus improve the search response and performance. Minimizing the number of fields in the default fieldset will not compromise the required fields. When creating a default fieldset, review the following considerations:

- Select a new fieldset other than the default *Base Event Fields* provided with the Search feature.
- Only one fieldset can be designated as the default fieldset. There must be a default fieldset.
- Saved fieldsets are the only ones that can be set as default.
- Each fieldset should have a unique name.
- Fieldset names are not case sensitive.
- A default fieldset cannot be edited and saved under the original name.

Delete a Fieldset

You can delete a fieldset that you have created or that has not been designated as a default fieldset. If you delete a fieldset that's used in an active search, Search changes the fieldset name to **Custom** for that search.

1. Select **Search**.
2. Select the name of the current fieldset (shown to the left of the time range selector).

   By default, Search displays the name of the last used fieldset.
3. If the last used fieldset is not the fieldset that you want to delete, select another fieldset from the drop-down menu.
4. Select **Edit this set**.
5. Select **Delete**.

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.

- "Considerations for the Lookup List File" on page 38
- "Create a Lookup List" on page 39
- "Replace a Lookup List" on page 39
- "Delete a Lookup List" on page 40

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.

Create 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.
4. 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
5. 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	
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
6. To upload the file as a table in the database, select **Upload**.

Replace 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.

1. Select **Configuration** > **Lookup Lists**.
2. Select the list that you want to replace.

3. Select **Replace**.
4. Select the CSV file that you want to use to replace the contents of the existing lookup list.

Delete a Lookup List

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

Configuring the Time Range for a Search

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 reexecuting the search based on the most recent 30 minutes. Alternatively, you can create a dynamic date range.

- "Specify a Dynamic Date Range" on page 40
- "Understand How Timezones Affect Search Results" on page 41

Specify 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:

1. When viewing a search or starting a query, select the currently specified time range.
2. For the start or end time under **Custom Range**, select **Dynamic**.

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

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

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

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

Understand How Timezones 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. The time range criteria applies to the *Normalized Event Time* (NET) rather than the *Event Time*. NET replaces illogical Event Time values with *Persisted Time* to correct the incorrect Event Times. You might need to account for the time zone offset from UTC and from other time zones, including Daylight Savings Time. 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.

For searches that you create in a different time zone, the Events Timeline converts the time segments to local times. If the Events table includes a time attribute, Search converts the time to local 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 current time zone.

II Hunting for Undetected Threats

To help you hunt for undetected threats, the **Reports** feature includes a set of MITRE ATT&CK™ dashboards and reports. 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.

4 Understanding the MITRE ATT&CK Dashboards and Reports

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.

While you are working with the MITRE ATT&CK dashboards and reports, you can access more detailed information on MITRE tactics and techniques (**MITRE ID**s) on the MITRE ATT&CK website (https://attack.mitre.org/)

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

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 indicted 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" on page 47
- "MITRE ATT&CK Destination Host Summary" on page 47
- "MITRE ATT&CK Destination Username Summary" on page 47
- "MITRE ATT&CK Source Address Summary" on page 48
- "MITRE ATT&CK Source Hostname Summary" on page 48

- “MITRE ATT&CK Source Username Summary” on page 48
- “MITRE ATT&CK Technique Summary” on page 48

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 infomration 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

5 Viewing the MITRE ATT&CK Dashboards and Reports

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

When you view the MITRE 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 tab, you can leave that tab open to keep the dashboard or report active while you look at other dashboards or reports.

You access the MITRE 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.

- "View a MITRE Dashboard" on page 51
- "View a MITRE Report" on page 52

View a MITRE Dashboard

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

1. Select **Reports** > **Portal** > **Repository** > **Standard Content** > **MITRE ATT&CK Dashboards**.
2. 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.

View a MITRE Report

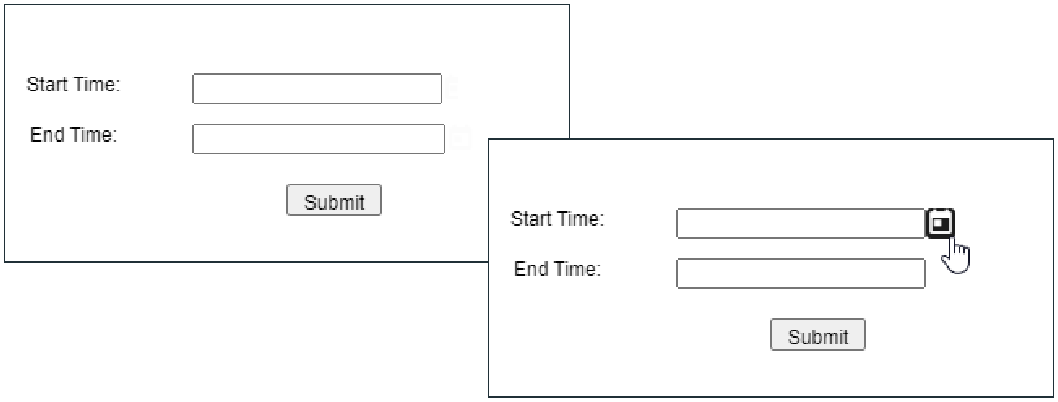
When you open a report, you must define the time range for the data you want to view.

1 Select **Reports** > **Portal** > **Repository** > **Standard Content** > **MITRE ATT&CK Reports**.

2 Select the report that you want to view.

3 To change the time range, complete the following steps:

3a To activate the Calendar, point your cursor at the position of the **Calendar** icon to the right of the time selection box.



3b Select the **Calendar** icon.

3c Enter the **Start Time** for the report.

3d 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 **Add to Queue**, then define the delivery options.

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.

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.

6 Generating Models to View Anamalous Data

You must have the Administrative 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" on page 55
- "Defining and Building a Model" on page 56
- "Scoring a Model" on page 56
- "Deleting a Model" on page 57

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

1. Review the considerations for building a model.
2. Select **Configuration** > **Outlier**.
3. For **Create Model Configuration**, 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 name the model, type over **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. Specify a time range for the model.

   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.

6. Select **Create**.

   The created model appears 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. Select **Build**.
9. To evaluate incoming events against the model, you must start the scoring process.

Scoring a Model

You must have the 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.

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

7 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.

Understand 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 exfiltration 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.

Further Investigate Anomalies

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.

View 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. Select **Detect**.
5. Specify a valid time range for which 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**.

   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 select the **Play** button 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:

   8a Right-click a row in the grid.

   8b 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. **Device Receipt Time** represents the moment when the connector received the event, typically close to the time that the event occurred. **Normalized Event Time** represents the time that the database receives the event. Usually Normalized Event Time is set to the Device Receipt Time, except when the receipt time is not within the boundary of +/-7 days of Recon persistence time. When the Device Receipt Time is not within the boundary, the Normalized Event Time gets assigned to the event. The normalized time removes bad time values from the event data.

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 overtime.

8 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 Event Time*:

Future Events

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

```
Normalized Event Time (NET) - Device Receipt Time (DRT) < 0
```

Past Events

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

```
Normalized Event Time (NET) - Device Receipt Time (DRT) > 0
```

Active Events

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

```
Normalized Event Time (NET) - Device Receipt Time (DRT) = 0
```

9 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 data sources 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.

10 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 Quick Ranges and a Custom Range. 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.

Data Sources

This visualization group consists of the following components:

Category Selector

Displays data sources in each of the three Data Categories.

Top Sources

Represents the percentages of up to 10 top data sources with the most 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 Source Timeseries side chart.

Source Timeseries

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

V 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 reports and dashboards to quickly launch threat-hunting exercises.

Depending on your assigned permissions, you can view, schedule, design, or manage reports and dashboards.

11 Accessing Reports and Dashboards

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.

12 Scheduling Report Generation

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, save to disk or an archive, or print them.

13 Designing Reports for Data Analysis

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

Report **Designer** provides a wizard that allows you to create new reports and dashboards from your data sources. 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. The Designer also supports visually building queries against multiple types of data sources and specifying data grouping, summarization and element data binding.

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.

VI Managing User Access

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 in Fusion.

- Chapter 14, “Assigning Permissions for Recon,” on page 79
- Chapter 15, “Default Roles for Recon,” on page 81

14 Assigning Permissions for Recon

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

- "Default Permissions for Searches" on page 79
- "Default Permissions for Reports" on page 79

Default Permissions for Searches

The Search feature provides the following default permissions:

Permission	Allows users to...
Execute Search	Execute searches using fieldsets, custom ranges dates, and search operators
Export Search Results	Export the search results in csv format
Manage Outlier Models and Scoring	Create and delete Outliers models Build and pause the scoring processes
Manage Lookup Lists	Add, configure, view, and delete lookup lists

Default Permissions for Reports

The Reports feature provides the following permissions:

Permission	Allows users to...
Report Admin	◆ View dashboards and reports ◆ Create subfolders ◆ Account logout ◆ Schedule reports ◆ Create data worksheets, dashboards, and reports ◆ View Admin reports ◆ Manage the data source
Design Reports	◆ View dashboards and reports ◆ Create subfolders ◆ Account logout ◆ Schedule reports ◆ Create data worksheets, dashboards, and reports

Permission	Allows users to...
Schedule Reports	◆ View dashboards and reports ◆ Create subfolders ◆ Account logout ◆ Schedule reports
View Reports	◆ View dashboards and reports ◆ Create subfolders ◆ Account logout

15 Default Roles for Recon

When you deploy Recon, the default roles provided for the common services in Fusion adapt to include appropriate Recon permissions. Common services include the Dashboard.

Default Role	Permissions
System Admin	- All **Admin** and both **Dashboard** permissions - All **Recon** permissions
Admin	- All **Admin** and both **Dashboard** permissions - All **Recon** permissions
Analyst L1	- Both **Dashboard** permissions - Execute Search permission
Guest	- Both **Dashboard** permissions - Execute Search permission
Report User	Report **Admin** permission
User	- Both **Dashboard** permissions - Execute Search permission

You can create new roles that reflect your organization's needs. You cannot change the permissions of the System Admin role.