Micro Focus ArcSight Log Management and Compliance

User's Guide to ArcSight Log Management and Compliance

Contents

Intended Audience ... 8
Additional Documentation ... 8
Contact Information ... 8
Legal Notice ... 9
Welcome to Log Management and Compliance ... 10
Searching for Events ... 10
Understanding Search ... 11
Understand Session versus Saved Searches ... 11
Understand the Search Progress Indicators ... 12
Understand the System Searches ... 13
Understand Search Queries ... 14
General Search Operator Use Cases ... 29
Operator Chaining Use Cases ... 30
Syntax Recommendations ... 32
Syntax ... 34
Aggregation Functions ... 35
The Span Function ... 35
How Do I Use This? ... 36
Syntax ... 38
How Do I Use This? ... 39
top ... 39
bottom ... 40
Syntax ... 40
Parameters ... 40
How Do I Use This? ... 41
Syntax ... 42
How Do I Use This? ... 42
Syntax ... 43
Parameters ... 43

How Do I Use This? 43
Syntax Recommendations 44

General Syntax for Eval 46
Considerations for Using Eval Functions 46
Examples 46
Restrictions 47

Understand Eval Functions 49
Comparison and Conditional Functions 49
Boolean Functions 50
Cryptographic Function 50
Informational Function 50
Statistical Functions 51
Text Functions 52

concat 54
Syntax 54
Parameters 54
How Do I Use This? 55

if and case 56
Syntax 56
How Do I Use This? 56

replace 59
Syntax 59
Parameters 59
How Do I Use This? 60

tonumber 61
Syntax 61

Parameters 61
How Do I Use This? 61

tostring 63
Syntax 63
Parameters 63
How Do I Use This? 63
Understand the Search Criteria 64
Editing the Selected Fieldset 65
Editing a Different Fieldset 66
Cloning a Fieldset 67
Creating and Saving Searches 72
Create a Search 73
Load a Saved Search 75
Run a Search 75
Initiate a Search from Enterprise Security Manager 76
Modify the Search Query or Criteria 76
Name a Search 76
Search Event Data from Logger 77
Save the Search 78
Viewing and Managing Your Searches 78
Get an Overview of Your Searches 79
View the Results of a Search 79
View and Use the Details of an Event 83
Identify Fields without Data 86
Refresh Search Results 86
Export Completed Runs of a Scheduled Search 86
Configure Preferred Settings for Searches 86
Manage Searches 88
Scheduling Regular Runs of a Search 90
Manage Scheduled Searches 90
Manage Completed Runs of a Scheduled Search 93
Analyzing Anomalous Data with Outlier Analytics 97
Generating Models to View Anomalous Data 97
Considerations for Generating Models 98

Define and Build a Model 98
Score a Model 99
Delete a Model 100
Viewing Anomalous Data in a Model 101
Understand the Provided Analytics Charts 101
Investigate Anomalies Further 102
View a Scored Model 102
Managing the Quality of Your Data 104
Understanding the Data Quality Insights 104
Active Events 104
Future Events 105
Past Events 105
Understanding How Data Quality is Calculated 105
Analyzing Data Quality 106
Managing and Importing Stored Data 108
Managing Your Stored Data 108
Use Storage Groups to Organize and Retain Data 108
Activate and Deactivate Storage Groups 110
Change the Settings of a Storage Group 110
Use Storage Group Queries in a Search 111
Configure Retention Policies for Your Data 111
Importing Event Data From Logger 113
Importing Logger Data in a non-SaaS environment (requires ArcSight Database 11.1 or greater) 113
Ensuring Data Compliance 127
Ensuring Compliance with GDPR Standards 127
Access Activity 132
Admin Activity 136
Attack Surface Analysis 137
Corporate Governance 140
Regulatory Exposure 142
Threat Analysis 144
Ensuring Compliance with IT Governance 149
IT Governance – Executive Overview 153
6 – Organization of Information Security 154
8 – Asset Management 154
9 – Access Control 155

10 – Cryptography 157
12 – Operations Security 158
13 – Communications Security 167
14 – System Acquisition, Development, and Maintenance 169
16 – Information Security Incident Management 170
17 – Information Security Aspects of Business Continuity Management 172
Ensuring Compliance with PCI DSS 172
1 – Maintain Firewalls to Protect Cardholder Data 180
2 – Do Not Use Default Security Parameters 186
3 – Protect Stored Cardholder Data 188
4 – Encrypt Transmission of Cardholder Data 188
5 – Use and Regularly Update Antivirus Software or Programs 190
6 – Maintain Secure Systems and Applications 192
7 – Restrict Access to Cardholder Data 196
8 – Assign a Unique ID to Each User 197
9 – Restrict Physical Access to Cardholder Data 199
10 – Track and Monitor Access to Cardholder Data 200
11 – Test Security Systems and Processes Regularly 204
12 – Maintain a Policy that Addresses Information Security 209
Ensuring Compliance with SOX Standards 210
Sarbanes-Oxley Executive Summary 213
5 – Information Security Policies 214
6 – Organization of Information Security 214
7 – Human Resource Security 216
8 – Asset Management 216
9 – Access Control 216
10 – Cryptography 218
11 – Physical and Environmental Security 219
12 – Operations Security 220
13 – Communications Security 225
16 – Information Security Incident Management 226
17 – Information Security Aspects of Business Continuity Management 228
18 – Compliance 228
Legal Notice 229

About This Book

This *User's Guide* provides concepts, user cases, and contextual help for ArcSight Log Management and Compliance.

- Search for alerts and events
- Analyze anomalous data with outlier analytics
- Evaluate and manage the quality of your data
- Organize data into storage groups
- Comply with legal and governmental regulations

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 Log Management and Compliance documentation library includes the following resources:

- *Quick Start Guide for Administrators*, which provides an overview of the products deployed in this suite and their latest features or updates
- User Guides for the capabilities that deployed in your ArcSight SaaS environment and *Release Notes for ArcSight Platform*

For the most recent version of this guide and other ArcSight documentation resources, visit the documentation for ArcSight SIEM as a Service.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. 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/.

Legal Notice

Welcome to Log Management and Compliance

Log Management and Compliance 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 Portal**, which includes OWASP 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.

Log Management and Compliance deploys within the **ArcSight Platform**, which provides common services such as the Dashboard, the Reports Portal, and user management.
The **ArcSight Database** stores all collected events to support searches and analysis capabilities. The database enforces the immutability of events once they are stored, ensuring that not even the most privileged database administrator can modify or delete an event. Combined with the existing **Event Integrity Check**, the database's ability to resist tampering provides an end-to-end, long-term solution for safeguarding events to ensure they are exactly as reported by the device where the activity was observed.

- Search for alerts and events
- Analyze anomalous data with outlier analytics
- Evaluate and manage the quality of your data
- Organize data into storage groups
- Comply with legal and governmental regulations

Searching for 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, as well as view the raw event data. Each search consists of specifying query input, search result fields, and the criteria 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.

Understanding Search

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

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 enter a search query, the criteria (such as a time window) over which to search, and the fields from the Unified Event Schema. You can use one of the three timestamps the database stores for each event for your time window.

Search displays results in an Events timeline as a histogram chart, which shows the number of events returned over event occurrence time. The Events table shows events returned by search. When you select an event, Search displays the Event Inspector panel. For ongoing or regular searches, you can save queries, queries plus specific criteria, and search results. You can also schedule searches to run on a regular basis.

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, resume, and cancel the process as needed. A progress bar shows you the percent of retrieved data.

Because search results consume space, the system maintains a threshold for the total number of executed searches that it can store. Stored content includes saved search results, completed runs of session searches, and completed runs of scheduled searches. The system displays a notification when the threshold is passed. If this occurs, you cannot run a search and scheduled searches cannot run until some previously executed searches have been deleted.

Understand Session versus Saved Searches

Select **Search**.

As you initiate searches, Search automatically preserves your activity in case you must navigate to another search or to a different feature in the ArcSight Platform. Search temporarily maintains these **session searches** in tabs until you close the search tabs, exit your browser, or

log out. The Home tab lists all your current session searches. Therefore, if you close the search tabs or lose the search tabs by logging out, you can open them again from the Home tab.

- "Saved Searches" below
- "Expired Searches" below

Saved Searches

For long-term use of a search, you must save the query, criteria, or results. You can review and manage your **saved searches** at any time:

- Saved queries
- Saved criteria
- Saved search results

Expired Searches

Session and saved searches usually **expire** after a specified amount of time. When they expire, the system deletes all information about the search. If this occurs when you have the search open in a tab, you will receive a notification that the search has expired and be instructed to close the tab.

Because session searches are considered short-term or temporary searches, the default expiration time is after 24 hours of inactivity. Saved searches expire after seven days by default. You can reset the expiration time by running the search again or by modifying the query or criteria. However, if the search has already expired, you cannot reset the expiration clock.

You can also override the default expiration time by changing the **Search expires in** setting for a particular session or saved search.

Understand the Search Progress Indicators

As **Search** 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.

Understand the System Searches

Search includes the following out-of-the-box **system searches** that contain a query plus specific criteria. All of these system searches are set in Normalized Event Time. For more information about how to use these queries and criteria, see "Load a Saved Search" on page 75.

Note: You can also search queries by using # and the query name. For example, #Configuration changes or #DGA Events. Additionally, you can run criteria searches as queries using the same method. Additionally, there is a list of reserved words that must be enclosed in quotes (" ") to ensure the system correctly parses the query.

Category	Name	Use as	Description
Application Monitoring	Windows New Service Created	Query	Lists events indicating new windows services were created from the following event sources: • Microsoft-Windows-Security-Auditing:4697 • Service Control Manager: 7045
Configuration Monitoring	Configuration changes	Query	Lists configuration changes based on ArcSight categorization.
Entity Monitoring	Failed logins	Query	Lists events indicating failed login activity based on ArcSight categorization.
	Failed Login Events	Criteria	Lists failed login activity events based on ArcSight categorization for the last 30 minutes by default.
	Failed logins for $username	Query	Lists events indicating failed login activity based on ArcSight categorization for a specific user. The user should be specified before running the search.
	Windows account creation	Query	Lists events indicating new windows accounts created based on the following event sources: • Microsoft-Windows-Security-Auditing:4720 • Security:624
Event Monitoring	ESM Correlation Events	Query	Lists ESM correlation events.
Malware Monitoring	Malicious code activity	Query	Lists events indicating malicious code activity based on ArcSight categorization.

Category	Name	Use as	Description
MITRE Monitoring	MITRE ATT&CK Events	Criteria	Lists correlation events reported from Arcsight ESM content package: https://marketplace.microfocus.com/cyberres/content/esm-default-content. These events are forwarded to Log Management and Compliance using ArcSight Forwarding connector, or any other flex connector which reports this information, using the following mapping: deviceCustomString6Label='MITRE ID' Where deviceCustomString6 contains the actual MITRE ATT&CK technique.
Network Monitoring	DGA Events	Criteria	Lists DGA-related events based on Microsoft Trace Log.
	DNS Events	Query	Lists DNS-related events.
	DoS Events	Criteria	Lists events indicating denial of service based on ArcSight categorization.
	Firewall drop	Query	Lists Drop Firewall events based on Arcsight categorization for a specific IP address. The IP address should be provided at runtime.
	Firewall drop for $ip		Lists Drop Firewall events based on Arcsight categorization.
	Firewall Events	Criteria	Lists Firewall events based on ArcSight categorization.
	Proxy Events	Criteria	Lists Proxy events based on ArcSight categorization.
	SSH authentication	Query	Lists events indicating SSH Authentication events based on ArcSight categorization.
	VPN connections	Query	Lists events indicating VPN connections based on ArcSight Categorization.
Vulnerability Monitoring	Vulnerabilities Events	Criteria	Lists events indicating vulnerabilities based on ArcSight categorization and Vulnerability Scanner events.

Understand Search Queries

You must have the **Manage Search Queries** *permission.*

A **search query** is a set of conditions used to select events when you run a search. For example, you can enter a very simple term to match such as "login" or an IP address. Alternatively, you can specify a complex query to match events that include multiple IP addresses and reference a lookup list. In the search query, you can enter the alias, or abbreviated term, for a field name

rather than entering the full name. You can also use the **presentable field names**, such as Agent Address.

Your query input determines the search type: full text, natural language, or contextual. As you specify the fields and values for the query, Search suggests search items and operators based on a schema data dictionary.

Search provides default queries, labeled as *system*. However, you can save your own queries, which you can load into another search. You have the option to clone, modify, or remove a saved query at any time.

Understand the Query Syntax

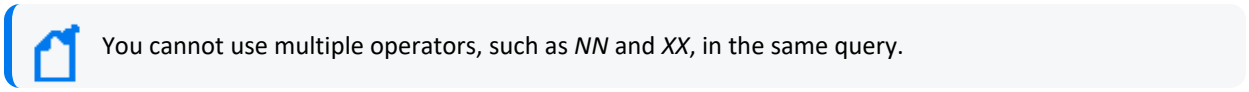
Depending on the type of search you create, the query must meet the requirements listed in the following table. Search treats a comma (,) between search items and values as an **OR** operator. Additionally, there is a list of reserved words that must be enclosed in quotes (" ") to ensure the system correctly parses the query.

If you do not get the search results you expect, you might need to restate the query. For example:

- If the query is written with spaces, only the first word is shown in the results. A better way to write the query statement is to use explicit phrasing without any spaces.
- Queries that filter specific "id" field values (for example, id = "123456789" or id != "123456789") will not return correct results. Create the query without using "id" fields.

By default, search operations are case-sensitive to support faster performance. However, you can instruct the database to support case-insensitive searches. For SaaS deployments, talk to your SaaS Admin about changing the database.

When you construct a query, you can include operators, such as eval and lookup, for more robust searches.



- "General Syntax Rules" on the next page
- "Implicit Operators" on page 17

General Syntax Rules

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.
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
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

Implicit Operators

Implicit operators form the basic building blocks for query construction. Use them along with other operators and functions to create robust search queries.

To build queries, use the following general operators:

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	startwith	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

Understand the Types of Search Queries

Search supports the following types of search queries:

- "Full Text Search" below
- "Field-based Search" below
- "Hashtag (predefined searches)" below

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.

To ensure the system correctly parses your query, if your search entity name includes one of the reserved words listed before, you should surround the query name with quotes (" ") in order to avoid ambiguity in the query statement.

This predefined query...	Description
#Configuration Changes	Lists configuration changes based on ArcSight categorization.
#DGA Events	Lists DGA-related events based on Microsoft Trace Log.
#DNS Events	Lists DNS-related events.
#DoS Events	Lists events indicating denial of service based on ArcSight categorization.
#ESM Correlation Events	Lists ESM correlation events.
#Failed Logins	Lists events indicating failed login activity based on ArcSight categorization.
#Failed Logins For User $Username	Lists events indicating failed login activity based on ArcSight categorization for a specific user. The user should be specified before running the search.
#Firewall Drop	Lists Drop Firewall events based on Arcsight categorization for a specific IP address. The IP address should be provided at runtime.
#Firewall Drop For $Ip	Lists Drop Firewall events based on Arcsight categorization.
#Firewall Events	Lists Firewall events based on ArcSight categorization.
#Malicious Code Activity	Lists events indicating malicious code activity based on ArcSight categorization.
#MITRE ATT&CK Events	Lists correlation events reported from Arcsight ESM content package: https://marketplace.microfocus.com/cyberres/content/esm-default-content. These events are forwarded to Log Management and Compliance using ArcSight Forwarding connector, or any other flex connector which reports this information, using the following mapping: deviceCustomString6Label='MITRE ID' Where deviceCustomString6 contains the actual MITRE ATT&CK technique.
#Proxy Events	Lists Proxy events based on ArcSight categorization.
#SSH Authentication	Lists events indicating SSH Authentication events based on ArcSight categorization.
#VPN Connections	Lists events indicating VPN connections based on ArcSight Categorization.
#Vulnerabilities Events	Lists events indicating vulnerabilities based on ArcSight categorization and Vulnerability Scanner events.
#Windows Account Creation	Lists events indicating new windows accounts created based on the following event sources: • Microsoft-Windows-Security-Auditing:4720 • Security:624
#Windows New Service Created	Lists events indicating new windows services were created from the following event sources: • Microsoft-Windows-Security-Auditing:4697 • Service Control Manager: 7045

Use Reserved Words in a Query

To ensure the system correctly parses your query, if your search entity name includes one of the reserved words listed before, you should surround the query name with quotes (" ") in order to avoid ambiguity in the query statement.

For example, if your query name is: "System warnings and errors" use the following notation: #"System warnings and errors."

Reserved Words for Queries		
and	as	between
by	category	connecting to
contain	contains	custom float
distinct	does not contain	does not end with
does not start and end with	domain	ends with
endswith	equal	equals
filter	for	greater
greater equal	greater equal than	greater than
gte	has	has substring
hostname	ibt	id
in between	in cidr block	in list
in list of	in subnet	is
is between	is equal	is equal to
is greater	is greater or equal than	is greater than
is greater than or equal to	is larger	is larger than
is less	is less equal	is less or equal than
is less than	is less than or equal to	is lower
is lower than	is not	is not between
is not equal	is not equal to	ip
ip6	label	less
less equal	less equal than	less than
like	lte	mac
match	nibt	not

Reserved Words for Queries		
not between	not equal	not equals
not in between	not in cidr block	not in list
not in subnet	not match	not within subnet
or	path	pipe
port	span	starts and ends with
starts with	startswith	timestamp
username	uri	url
where	wheresql	within subnet
withinsubnet		

Include 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.

Use 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
global event id=<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.

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
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

Field	Aliases
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
destinationUserName	duser dst user dest user destination user dst usr
destinationUserPrivileges	dpriv
deviceAction	act
deviceAddress	dvc deviceaddr deviceip device ip
deviceCustomFloatingPoint*n* Valid values for *n* are integers between 1 and 4 For example: deviceCustomFloatingPoint1	cfp*n* For example: cfp1
deviceCustomFloatingPoint*n*Label Valid values for *n* are integers between 1 and 4 For example: deviceCustomFloatingPoint1Label	cfp*n*Label For example: cfp1Label

Field	Aliases
deviceCustomIPv6Address*n* Valid values for *n* are integers between 1 and 4 For example: deviceCustomIPv6Address2	c6a*n* device custom ipv6 *n* For example: c6a2
deviceCustomIPv6Address*n*Label Valid values for *n* are integers between 1 and 4 For example: deviceCustomIPv6Address2Label	c6a*n*Label For example: c6a2Label
deviceCustomNumber*n* Valid values for *n* are integers between 1 and 3 For example, deviceCustomNumber3	cn*n* For example: cn3
deviceCustomNumber*n*Label Valid values for *n* are integers between 1 and 6 For example: deviceCustomNumber6Label	cn*n*Label For example: cn6Label
deviceCustomString*n* Valid values for *n* are integers between 1 and 6 For example: deviceCustomString5	Cs*n* 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

Field	Aliases
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

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

Group Alias	Includes a list of these fields or columns...
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 IP Addresses and Subnets

Your query can include IPv4, IPv6, 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`

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.

To enter an IP or MAC address in a search query:

Enter the MAC 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

Use an Operator in the Query

Create powerful queries with search operators and functions. You can also select several out-of-the-box system searches that contain a query plus specific criteria. Operators, such as eval, can be chained together to create complex queries.

Search operators and functions must be entered in all lower case letters when they are used in queries.

Do not use a raw event field as part of a query.

Use Cases for Search Operators

The following are just a few examples of the flexibility and power of search operators.

- "General Search Operator Use Cases" below
- "Operator Chaining Use Cases" on the next page

You may need to adjust a query to work with your own fieldsets.

For more information about working with operator chaining see "Create powerful queries with search operators and functions. You can also select several out-of-the-box system searches that contain a query plus specific criteria. Operators, such as eval, can be chained together to create complex queries." above and "Syntax Recommendations" on page 32.

General Search Operator Use Cases

I want to see where possible brute force password guessing is happening.

Additional Information: To determine this, I want to see the top 10 devices that are responsible for the most number of failed logins.
Operator used: top

```
#FailedLogin | top 10 deviceEventClassId
```

I want to know the hourly amount of data transfer on MyWebserver.

Operators used: chart, sum, by, span

```
sourcehostname = MyWebserver.com | chart sum(bytesIn), sum(bytesOut) by
deviceVendor, deviceProduct span 1h
```

I want to see a sum of events, grouped by hostname and day.

Operator used: chart
Aggregate function: sum (This summarizes the values passed as an input, grouped by the "by" clause.)
Time bucket: 1h (Events are grouped in time increments of one hour.)

```
| chart sum(baseEvents) by hostName span 1h
```

I want to determine all account lockouts, grouped by user name.

Operators used: wheresql, top

```
(deviceVendor="Microsoft" and deviceProduct="Microsoft Windows") or
deviceProduct="Unix" | wheresql  deviceEventClassId in
["Security:539","Security:644","arcsight:66:0","Microsoft-Windows-
Security-Auditing:4740","Microsoft-Windows-Security-Auditing:6279"] and
destinationUserName is not null |top destinationUserName
```

Operator Chaining Use Cases

I want to identify the rare occurrences of Firewall events.

Additional Information: I want to determine this from 3 specific fields' data (device vendor, category device group, and name).
Operators used: rename, rare (bottom)

```
#Firewall Events | rename deviceVendor as DV | rename category device
group as CDG | rare DV , name , CDG
```

I want to isolate vulnerabilities.

Additional Information: I will base this on data from 3 significant fields (device vendor, category technique, and device group), then determine the most common occurrences found in those categories.
Operators used: rename, rare (bottom)

```
#Vulnerabilities | rename deviceVendor as DV | rename category technique
as CT | rename category device group as CDG | rare DV , name , CDG , CT
```

I want to apply filters to a set of fields and then to extract the top-50 most common occurrences of those events.

Operators used: where, top

```
source address is not null | where Bytes In >= 3000 | where Category
Outcome = /Success | top 50 source address , Category Outcome
```

I want to determine the top insecure processes on devices in my company.

Operators used: top, rename

```
destinationProcessName in ["telnetd", "ftpd", "pop3", "rsh" ,
"imapd","rexec"] | top destinationProcessName  | rename
destinationProcessName as  "Process"
```

```
deviceVendor = ArcSight | rename sourceUserName USER | top USER
```

Show me all configuration changes by product.

Operators used: top, rename

```
categoryBehavior = "/Modify/Configuration" and categoryOutcome =
"/Success" | top deviceProduct | rename deviceProduct_count_2 as "Changes"
| rename deviceProduct as "Product"
```

I want to apply filters to a set of fields and then to extract the top-50 most common occurrences of those events.

Operators used: where, top

```
source address is not null | where Bytes In >= 3000 | where Category
Outcome = /Success | top 50 source address , Category Outcome
```

Chaining Search Operators

Construct a complex query statement by chaining together multiple search operators into a single query instead of implementing separate queries. This powerful capability lets you

perform robust, real-world searches while providing the flexibility to customize searches for specific scenarios. You can save these searches to reuse them in future updates.

Operator chaining is a process by which the search takes a set of results from one operation and uses these results as input for the next operation. Chaining a series of operations equips you with the options needed to "slice and dice" data to extract and analyze it on a highly granular level.

Operator chaining works with all the pipeline operators (rename, eval, where/filter, wheresql, top, bottom/rare and chart/stats).

During operator chaining, fieldsets become more restricted as more operators are added to the query, especially with eval and aggregation operators. For example:

```
severity!=null | top severity | stats avg (Count_1) by severity
```

For information about operator chaining workflows, see "General Search Operator Use Cases" on page 29.

Syntax Recommendations

Use the following syntax recommendations to ensure operator chained searches succeed.

- To use the fields from a **lookup list** table with the search operators, make a **join** with one of the lookup fields using the **"in list"** operator. You also should add the lookup list fields to the current fieldset. For example:

  Add a lookup list with name as **Customer** then add its field, which will be used with search operator (e.g. **Customer_Vendor**) to the current fieldset.

  ```
  Source Address in list Customer_Address | wheresql Customer_Vendor =
  'Microsoft'
  ```

- **Alias/New** column name cannot be an existing column name or a synonym of an existing column name. Also, an alias column name cannot be an existing group name or reserved word.

  In this example, "destination hostname" and its synonyms "dhost" and "destination name" cannot be used as aliases.

- **Alias/New** column name should not have spaces (like test 1), otherwise it will cause conflicts. These are examples for acceptable alias/new column names:

  ```
  name is not null| eval test1 = concat(name, "_test") | eval test_2 =
  upper(test1)
  ```

```
name is not null | where name not equals ARCSIGHT | chart count (distinct
name) as Dcount by name
```

- The following is an example of how to use a generated field with **eval** in another operator:

```
| eval test = upper ( name ) | where test != "ARCSIGHT"
```

- **Count_<number>** cannot be used as an alias for a field name.
- The **wheresql** operator is case sensitive. Just like all other operators, the wheresql name must be stated in all lower case letters.
- Do not create new column with spaces if these new columns will be used later with the **wheresql** operator. The where condition of wheresql operator will not recognize new column with spaces that were created by previous operators. In addition to wheresql, this is also applicable for the **eval** and **chart and stats** operators. Here are two **invalid** examples:

```
| rename name as new name | wheresql new name = 'TCP'
```

```
destination port is not null | eval convert name = upper ( Name ) |
wheresql convert name = 'MSTYPE'
```

- You can use the **where** operator to filter dynamic fields, for example:

```
| top 5 Name | where Count_1 > 1000
```

- More filters can be added to a search through the Fields Summary feature. Click on **Fields Summary** and select a field and a value for that field. The new filter will be appended at the end of the query in use as a |**where** clause.
- Multiple **aggregate functions** can drastically modify drastically the fieldset that is available for the next pipe operator. for example:

```
name is not null | char count (Name) by Device Vendor span 1h | chart
count (Name) by Name
```

The second chart pipe cannot access to span operations because the NET, DRT, dBRT are not available for this chaining level.

Same scenario applies to the **top** operator:

```
name is not null | top Name | char count(count_Name_1) by Name span 1h
```

chart/stats

The **chart/stats** operators display search results for specified fields as columns.

- "Syntax" on the next page

- "Aggregation Functions" on the next page
- "The Span Function" on the next page
- "How Do I Use This?" on page 36

Syntax

```
...| chart count by <field1>,<field2>,<field3> ... [span [<time_
field>]=<time_bucket>]
...| chart {{sum | avg | min | max | } (<field>)}+ by
<field1>,<field2>,<field3> ...[span [<time_field>]= <time_bucket>]
...| chart {<function> (<field>)} as <new_column_name> by <field> [span
[<time_field>]
```

where:

- <*field*>,<*field1*>,<*field2*> are the names of event fields used in system queries.
- <*time_bucket*> is the bucket size (in any combination) used for grouping events. Use **d** for day, **h** for hour, **m** for minute, and **s** for seconds. For example, *2h*, *5d*, *1m*.
- <*function*> is one of the following: **count**, **sum**, **avg** , **min**, **max**, **latest** or **earliest**..
- <*new_column_name*> is the name you want to assign to the column in which the function's results are displayed. For example, <*Total*>.

Query input within [ ] (straight brackets) is optional for the query syntax.

Input within < > (angle brackets) indicates users may enter their own input: ... | rename <*source_name*> as <*NewSourceName*>

- All chart/stats commands accept only one field in the input. For example, | stats count (device vendor) by...
- The input field must contain a column that exists in the database.
- If multiple fields are specified, separate the field names using commas without any spaces.
- The function input field must contain numeric values for chart/stats sub-operators that are mathematical operations (sum, avg, min, max).
- The mathematical operators **avg** and **mean** are equivalent.

"by" Statements

- The chart/stats operators and eval, require a "by" statement. For example: eval | chart sum(AgentSeverity) by Destination HostName

- Specify a field name after the "by" statement. For example: "by deviceVendor"
- Columns in a by statement should be separated by comma: For example: ... | chart count (Name) by deviceEventCategory , name

Aggregation Functions

Note: Aggregation functions only work on numeric fields. The specified fields must contain numeric values. If a field you specify is of the wrong data type, you will receive an error message like the following: "java.lang.NumberFormatException".

- You can include multiple functions in the same chart/stats command. When doing so, separate each function with a comma, as shown:

```
...| chart count(Name) by Destination Hostname, sum(deviceCustomNumber3)
by deviceEventClassId
```

- When you include multiple functions, the search results table displays one column per function.
- You can use the "**as new_column_name**" clause to name any column resulting from the aggregation functions, as shown:

```
...| chart sum(deviceCustomNumber3) as TotalStorage, avg
(deviceCustomNumber3) as AverageStorage by deviceCustomNumber3
```

- Instances of "**<new_column_name>**" should be changed by the alias name of the aggregation result.

The Span Function

In addition to grouping events defined by **eval** operators, the **span** function groups events by a time field (such as EventTime or deviceReceiptTime) and a time bucket.

- The span function can only accept three columns (Normalized Event Time, Device Receipt Time, and Database Receipt Time) before the equals sign, for example:
  - |chart sum(Agent Severity) by Destination hostName span Normalized Receipt Time = 1h
  - |chart sum(Agent Severity) by Destination hostName span = 1h
  - |chart sum(Agent Severity) by Destination hostName span 1h
- The span operator is not allowed after an aggregation operator.

- The span operator must use an equal sign or a supported field name. For example: span Normalized Event Time = 1h
- The span operator only accepts timestamp fields. For example: span Normalized Event Time = 1h.
- A span's time bucket must use one of the following types of values: <*number*>d, <*number*>h, <*number*>m, and <*number*>s
- By default, the chart/stats command displays the first 10 unique values. If the span function creates more than 10 unique groups, not all of them will be displayed.
- When span is included in a query, search results are grouped by the specified time bucket. For example, if span=5m, the search results will contain one row for each 5-minute span. If there are no events within a specific 5-minute span, that row will be empty.
- The span function assumes a **24-hour day, all year long**. If span=1d or 24h, on the day of the daylight savings time change, the event time indicated by the span_eventTime field in the search results will be different from the previous day by one hour. On the day when there are 23 hours in a day (in March), the span bucket will still include events from the last 24 hours. Similarly, on the day when there are 25 hours in the day (in November), the span bucket will include events from the last 24 hours.

How Do I Use This?

Aggregation Function Examples

- Use the default chart setting (Column Chart) to specify multiple fields. In this example, a count of unique groups of deviceEventCategory and name fields is displayed and plotted.

```
... | chart count(Name) by deviceEventCategory name
```

- Simple query using 1 (min) aggregation function and one group by field (min)

```
... | [chart | stats] <aggregation_function> (<field_name>) [as <alias_
name>] by <field_name>
```

```
 chart count (Name) by Destination Hostname
```

- Query using 1 to N aggregation functions, the result and 1 to N group by field (min)

```
... | [chart | stats] [<aggregation_function> (<field_name>), ...
<aggregation_function> (<field_name>)] [as <alias_name>] by <field_name>
```

```
chart count (Name), sum(Agent severity) by Destination Hostname
```

- Query using 1 to N aggregation functions, the result and 1 to N group by field (min)

```
... | [chart | stats] [ <aggregation_function> (<field_name>), ...
<aggregation_function> (<field_name>)] [as <alias_name>] by <field_name>
[, ...<field_name>]
```

```
chart count (Name), sum(Agent severity) by Destination Hostname, Name
```

- Adding alias in every aggregation function

```
... | [chart | stats] [ <aggregation_function> (<field_name>), ...
<aggregation_function> (<field_name>)] [as <alias_name>] by <field_name>
[, ...<field_name> ]
```

```
chart count (Name) as <alias_name1>, sum(Agent severity) as <alias_name2>
by Destination Hostname, Name
```

Span Function Examples

- If time stamp is specified for span input, it does not use parenthesis: The correct query would be:

```
...| chart count(Name) by deviceEventCategory span deviceReceiptTime = 5m
```

- Destination Hostname is the time field and one hour is the time bucket:

```
 chart count (Name), sum(Agent severity) by Destination Hostname, Name
span 1h
```

- <*deviceReceiptTime*> is the time field and <*5m*> (5 minutes) is the time bucket:

```
...| chart count(Name) by deviceEventCategory span (deviceReceiptTime) =
5m
```

- Span is used to organize events by time frame:

```
... | [chart | stats] [ <aggregation_function> (<field_name>), ...
<aggregation_function> (<field_name>)] [as <alias_name>] by <field_name>
[, ...<field_name> ] span = n[s|m|h|d]|m|h|d]
```

- If a time field is not specified for the span function ,<*EventTime*> is used as the default. For example, the following query uses EventTime by default:

```
...| chart count(Name) by deviceEventCategory span = 5m
```

Grouping with span is useful in situations when you want to find out the number of occurrences in a specific time span.

- If you want to find out the total number of incoming bytes every 5 minutes on a device, you can specify a span of 5m. This example assumes that deviceCustomNumber1 field provides the incoming bytes information for these events.

```
...| chart sum(deviceCustomNumber1) by hostName span 5m
```

- You want to see a sum of events by hostName in one week of events, listed by day. When a **span** field is specified in conjunction with an **event** field, the unique sets of all those fields are used for grouping.

```
...| chart sum (baseEvents) by hostName span = 1d
```

- The following example uses <*deviceCustomNumber3*> and <*deviceAddress*> in conjunction with span to find out the number of events (using <*deviceCustomNumber3*>) from a specific source (using <*deviceAddress*>) in one (1) hour:

```
...| chart sum(deviceCustomNumber3) by deviceAddress span=1h
```

- When span is included in a query, search results are grouped by the specified time bucket. For example, if span=5m, the search results will contain one row for each 5-minute span. If there are no events within a specific 5-minute span, that row will be empty.
- The span function assumes a **24-hour day, all year long**. If span=1d or 24h, on the day of the daylight savings time change, the event time indicated by the span_eventTime field in the search results will be different from the previous day by one hour. On the day when there are 23 hours in a day (in March), the span bucket will still include events from the last 24 hours. Similarly, on the day when there are 25 hours in the day (in November), the span bucket will include events from the last 24 hours.

For information about other operators, functions, and syntax requirements, see "Create powerful queries with search operators and functions. You can also select several out-of-the-box system searches that contain a query plus specific criteria. Operators, such as eval, can be chained together to create complex queries." on page 29.

rename

Use the pipeline operator **rename** to assign a new name to a portion of the search query.

- "Syntax" below
- "How Do I Use This?" on the next page

Syntax

```
... | rename <source_name> as <NewSourceName>
```

Query input within [ ] (straight brackets) is optional for the query syntax.

Input within < > (angle brackets) indicates users may enter their own input: ... | rename *<source_name>* as *<NewSourceName>*

How Do I Use This?

- Assign a new address name to an existing source address.

```
... | rename <source_address> as <NewSourceAddress>
```

For information about other operators, functions, and syntax requirements, see "Create powerful queries with search operators and functions. You can also select several out-of-the-box system searches that contain a query plus specific criteria. Operators, such as eval, can be chained together to create complex queries." on page 29.

top and bottom

The **top** and **bottom** operators list the search results of the most common values for the specified field. The resulting values are listed in tabular format from the highest count value to the lowest.

The fields can be event fields, available in the application menu. If multiple fields are specified, you need to separate the field names with white space or a comma.

- "top" below
- "bottom" on the next page
- "Syntax" on the next page
- "Parameters" on the next page
- "How Do I Use This?" on page 41

top

The **top** operator provides the most common values for the specified field(s). The values are listed from the highest count value to the lowest.

bottom

The **bottom** operator provides the least common values for the specified field(s). The values are listed from the lowest count value to the highest. The **rare** operator can be used as an alias to **bottom**.

Syntax

```
…| top [<N>] <field1>[,<field2>,<field3>]
```

where:

- [ ] indicate optional input you can enter.
- < > indicates a user can enter *custom* information.
- Only <*N*> is optional. <*N*> limits the matches to the top *n* values for the specified fields. One (1) field is required, but you can specify a maximum of five (5) integers, separated by commands.
- If you do not specify <*N*>, the default value is 500.
- If included, <*N*> should be between one (1) and the search results limit.
- The operator performs a standard count (*) to retrieve the number of events.
- No search operator other than "where" can be used in a query after the top/bottom operator is used.

Query input within [ ] (straight brackets) is optional for the query syntax.

Input within < > (angle brackets), indicates users may enter their own input: … | rename <*source_name*> as <*NewSourceName*>

Parameters

The parameters are <*N*> and a list of comma-separated fields.

For the **top** operator, when multiple fields are specified, the count of unique sets for all of the fields is listed from the highest to lowest count. For the **bottom** operator, the fields are listed from the lowest to the highest count.

How Do I Use This?

The top operator is used to limit the matches to the top <*N*> values for the specified fields. Likewise, the bottom operator is used to limit the matches to the bottom <*N*> values for the specified fields. The default count number is 500 unless you specify a value for <*N*>. Here are a few examples:

- You want to limit your results to the 1,000 most common event categories.

  ```
  …| top 1000 deviceEventCategory
  ```

- You want to limit your search for the top 5 event categories.

  ```
  …| top 5 categories
  ```

- You want to see all products from a specific vendor that are sending the least number of events.

  ```
  deviceVendor = Vendor| bottom 10 deviceProduct
  ```

- See the rare user action in the organization happening using the HTTPS protocol.

  ```
  protocol=https | rare requestuseragent
  ```

For information about other operators, functions, and syntax requirements, see "Create powerful queries with search operators and functions. You can also select several out-of-the-box system searches that contain a query plus specific criteria. Operators, such as eval, can be chained together to create complex queries." on page 29.

where

The **where** operator displays events that match criteria specified in a "where" expression. Where expressions act as filters to return only those results that fulfill a particular condition. In fact, **filter** is a synonym of the operator **where**.

- "Syntax" on the next page
- "How Do I Use This?" on the next page

Syntax

```
... | where <expression>
```

- *<expression>* can only be a valid field-based query expression. Arithmetic expressions or functions are not supported.
- For **where any <…> contains** queries, all fields are executed, but only results for alpha (letter) IDs are displayed. For example, results for the ID "HostName" display, but results for the ID CEID-3631 will not display, even though the field is executed.
- You can specify multiple field conditions in one query expression by using the listed operators between them. The conditions can be nested. For example:

  `(name="John Doe" OR name="Jane Smith")AND message!="success"`

Query input within [ ] (straight brackets) is optional for the query syntax.

Input within < > (angle brackets) indicates users may enter their own input: ... | rename *<source_name>* as *<NewSourceName>*

How Do I Use This?

```
... | where eventId is NULL
```

```
... | where eventId=10006093313 OR deviceVersion CONTAINS "4.0.6.4924.1"
```

```
... | where eventId >=10005985569 OR categories= "/Agent/Started"
```

For information about other operators, functions, and syntax requirements, see "Create powerful queries with search operators and functions. You can also select several out-of-the-box system searches that contain a query plus specific criteria. Operators, such as eval, can be chained together to create complex queries." on page 29.

wheresql

The **wheresql** operator supports all of the ArcSight Database functions. Nested queries are allowed, but you may use only one dataset for the search.

- "Syntax" below
- "Parameters" below
- "How Do I Use This?" below

Syntax

```
…|wheresql <boolean_expression>
```

You must construct your queries with syntax supported by the ArcSight database.

Query input within [ ] (straight brackets) is optional for the query syntax.

Input within < > (angle brackets) indicates users may enter their own input: … | rename *<source_name>* as *<NewSourceName>*

Parameters

You can include the following parameters in the boolean expression:

- AND
- OR
- LIKE

How Do I Use This?

- You want to construct filter your search results to display numerical data between 10 and 50.

  ```
  …|wheresql bytesOut between 10 and 50
  ```

- Match the company name of a device vendor.

  ```
  … | wheresql regexp_ilike(deviceVendor, 'Company_Name')
  ```

- Further refine the search to select a device vendor from a specified table used in another search.

  ```
  … | wheresql deviceVendor in (select deviceVendor from tableX)
  ```

Syntax Recommendations

Use the following syntax to ensure searches and schedule searches that use the "wheresql" condition succeed:

- As with all search operators, the operator name must be in all lower case letters.
- The result of a wheresql expression should be boolean.
- Enclose **string** values in single quotes. For example, use `name = 'TCP'` instead of `name = TCP`. (Columns should be named exactly as in the DB when using wheresql. In this case, Name with uppercase would cause an error.)
- If **mathematical operators** such as square root or pi **contain a pipe**, the wheresql condition must be enclosed in double quotes. For example:

  `|wheresql "bytesin > (|/ 25.0)"`
- Fields must have valid names from columns in the ArcSight database.
- The "wheresql" condition field must exist in the current fieldset or be generated by a previous operator. For example, the field `agentHostName` must be contained in the *Base Events Field* fieldset. (Besides fields in a fieldset you can also use dynamic fields generated by previous operators. For example: | eval test1 = upper(name) | wheresql name != 'ArcSight')
- The "wheresql" condition cannot contain a limit. For example, the following statement is invalid: `| wheresql Name = 'TCP' limit 1000`
- Do not use the word "wheresql" for the name of a search, a search criteria, or a search query. The "wheresql" is a reserved word for the name of the search operator only.
- Do not use a semicolon at the end of the condition.

For information about other operators, functions, and syntax requirements, see "Create powerful queries with search operators and functions. You can also select several out-of-the-box system searches that contain a query plus specific criteria. Operators, such as eval, can be chained together to create complex queries." on page 29.

eval

The **eval** operator displays events after evaluating the results of a specified function. This can be a mathematical, string, or boolean operation and is evaluated when the query is run.

The resulting value is assigned to a field name. Once a new field has been defined by the eval operator, it can be used in the query to further refine the search results.

For information about other operators, functions, and syntax requirements, see "Create powerful queries with search operators and functions. You can also select several out-of-the-box system searches that contain a query plus specific criteria. Operators, such as eval, can be chained together to create complex queries." on page 29.

General Syntax for Eval

The **eval** operator displays events after evaluating the result of the specified function.

Eval operators use the following syntax formats:

```
| eval newField = <expression>
```

```
<EXPRESSION> Evaluation of values(fields) or constants with operators
```

Functions that can be used with the eval operator include:

concat, tonumber, tostring, replace(X,Y,Z), abs(X), case(X,"Y",...), ceil(X), ceiling(X), exp(X), floor (X), if(X,Y,Z), isfalse(X), istrue(X), len(X), ln(X), log(X), lower(X), tolower(X), mod(x,y), rand(), round(X), sqrt(X), substr(X,Y,Z), sum(x,y,z,...), trim(X), ltrim(X), rtrim(X), upper(X)toupper(X), urldecode(X).

For more information about eval functions, see "Understand Eval Functions" on page 49.

Considerations for Using Eval Functions

Please be aware of the following considerations when using the eval functions:

- You might encounter a search error if you run a query that uses both an "All Fields" fieldset and more than five pipeline operations. To avoid this, either reduce the number of fields in the fieldset or reduce the number of pipeline operators in your query.
- The md5(X) function is not supported in a FIPS environment.

Examples

- Could be a simple constant value: "Hello world", 5.

  ```
  ... | eval test0 = 5
  ```

- Could be a simple column: Name, Destination Hostname from the current selected fieldset.

  ```
  ... | eval test1 = Name
  ```

Pipeline operators, such as eval, can use operator chaining to allow output from one pipe operator to be used as input to a subsequent one.

- Find the longest URLs from the vendor ArcSight.

```
deviceVendor = ArcSight |eval urllength=length(requestUrl) |sort
urllength
```

- There is no limit to using arithmetic and boolean operators along with data (in fields or as constants).

```
... | eval test3 = Agent Severity + 1
```

```
... | eval test4 = Name and Device Vendor
```

```
... | eval test5 = (Name and Device Vendor) / 2
```

  If the boolean operator is the last operation applied, the overall result will be {0,1}.

- Examples of expressions that use arithmetic and boolean operators:

```
... | eval test6 = upper(Agent Severity ) + 1
```

```
... | eval test6 = upper(Agent Severity ) and Name
```

  If the boolean operator is the last operation applied the overall result will be {0,1}.

- Example using "if" and "case" statements:

```
... | eval test = if ( deviceCustomNumber1 = 200, Success, Failure)
… | eval test = case ( deviceCustomNumber1 = 200, Success,
deviceCustomNumber1 = 400, Failure, Unknown)
```

- "Case" requires a final parameter that serves as the else condition. For example:

```
case(name = 'Mandy', 'analyst', name = 'Oskar', 'operator', unknown')
where 'unknown' is the else condition.
```

- Functions can receive other expressions as input:

```
...  | eval test6 = upper(Agent Severity and 1 ) and Name
```

Restrictions

Some functions have restrictions based on the data type:

The expression below is not allowed because two different data types (Name and 1) are not allowed in an arithmetic operation.

```
... | eval test1 = Name + 1
```

The expression below is not allowed because **replace** expects string data types for parameters.

```
... | eval test1 = Name and replace ( 1 , Name , Name )
```

For more information about syntax requirements that the query must meet, see "Depending on the type of search you create, the query must meet the requirements listed in the following table. Search treats a comma (,) between search items and values as an OR operator. Additionally, there is a list of reserved words that must be enclosed in quotes (" ") to ensure the system correctly parses the query. " on page 15.

Understand Eval Functions

Eval allows you to define and name an expression that is returned in the search. Use the following functions to build an eval expression:

- "Comparison and Conditional Functions" below
- "Boolean Functions" on the next page
- "Cryptographic Function" on the next page
- "Informational Function" on the next page
- "Statistical Functions" on page 51
- "Text Functions " on page 52

For more information about other operators, functions, and syntax requirements, see "The eval operator displays events after evaluating the results of a specified function. This can be a mathematical, string, or boolean operation and is evaluated when the query is run. " on page 44.

Comparison and Conditional Functions

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.
- Parameters are the values used in the test.
- The only supported types are numeric and string. X can be a number, field or expression.

```
... | eval username = coalesce (Source Username, Destination Username)
Returns: Username
```

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
```

Boolean Functions

and (&&), **or (||)**, and **not (!)**

- connect and nest keywords. For example, (boolean_check_a) **and** (boolean_check_b).
- Use parentheses to group boolean operations.
- Each parenthesis should only do one binary "and/or" operation.
- Do not use more two boolean operators to connect keyword clauses. Instead, use parentheses to nest clauses. For example:

  Not allowed: (boolean_check_a) **and** (boolean_check_b) **and** (boolean_check_c)

  Allowed: ((boolean_check_a) **and** (boolean_check_b)) **and** (boolean_check_c)

```
| eval test_auto = (Agent Severity equals 4) and (Agent Severity equals
0)
```

```
| eval test_auto = (( Agent Severity equals 4 ) and ( Agent Severity
equals 0 )) and ( Agent Severity equals 2 )
```

Cryptographic Function

md5(*X*)

- Calculates the MD5 hash of string, returning the result as a string in hexadecimal.
- *X* must be a string.

```
... | eval usermd5 = md5 (Destination Username)
Returns: 202cb962ac59075b964b07152d234b70
```

The md5(X) function is not supported in a FIPS environment.

Informational Function

isnull(*X*)

- Returns true if the *X* is null otherwise returns false.

```
... | eval newField = isnull(2)
Returns: false
```

Statistical Functions

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
```

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(bytesIn, bytesOut)
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

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.
```

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*)

- trim(*X*) removes all spaces from both sides of the string *X*.

ltrim(*X*)

- ltrim(*X*) removes all spaces from the left side of the string *X*.

rtrim(*X*)

- rtrim(*X*) removes all spaces from the right side of the string *X*.

  For the sake of these following 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.
```

For more information about syntax requirements that the query must meet, see "Depending on the type of search you create, the query must meet the requirements listed in the following table. Search treats a comma (,) between search items and values as an OR operator. Additionally, there is a list of reserved words that must be enclosed in quotes (" ") to ensure the system correctly parses the query. " on page 15.

concat

The **concat** function creates a new string field that concatenates (or links together) strings from fields. It concatenates any user-defined strings that are separated by a comma (",").

IP and MAC binary fields are converted into a more user-friendly string format and then concatenated. Date fields are converted to the user format that is configured in your user preferences.

NULL values will be converted to empty string fields. The maximum limit for concat results is 6,000 characters. Anything longer than this will be truncated.

- "Syntax" below
- "Parameters" below
- "How Do I Use This?" on the next page

Syntax

Syntax for concat should look like this:

```
... | eval <newField> = concat([<field>|<value>]*)
```

Query input within [ ] (straight brackets) is optional for the query syntax.

Input within < > (angle brackets) indicates users may enter their own input: ... | rename *<source_name>* as *<NewSourceName>*

Parameters

The concat function can receive from 1 to 20 parameters, which can be expressions, user defined strings, or fields from the fieldset.

```
| eval test0 = concat('Event Name: ',  'Name')
```

```
| eval test1 = concat ( 'Event Name: ' , upper ( Name ) )
```

```
| eval test0 = concat ( 'Event Name: ' , ceil ( 2 ) )
```

```
| eval test0 = concat ( 'Event Name: ' , ceil ( 2 ) , replace ( Name , 'HTTP'
, 'MQTT' ) )
```

How Do I Use This?

- Create an eval search that concatenates fields related to a Host:

  ```
  | eval Host = concat(destinationHostName, ':' ,destinationPort)  - sample
  output - mf.com:9000
  ```

- Create an eval search that concatenates fields related to the identity of an employee:

  ```
  | eval Employee = concat(FirstName,' - ', LastName,  ' - ', DeptName,'(',
  srcUserName, ')')
  ```

For information about other operators, functions, and syntax requirements, see "Create powerful queries with search operators and functions. You can also select several out-of-the-box system searches that contain a query plus specific criteria. Operators, such as eval, can be chained together to create complex queries." on page 29.

if and case

If() and **case()** are both eval operators that expect specified conditions be met (are True).

An **if statement** returns a value when the given condition is met (is True), or returns another value when the given condition is not met (is False).

A **case expression** runs through a set of given conditions and returns a value when the first condition is met (is True). Once the condition is met, the application stops any further searching for that condition. If no conditions are met (is False), then the software returns NULL.

When if() and case() are used together and the case expression is met (is True), the if statement returns that condition's values accordingly. If the case expression is not met (is False), then the application searches for the next condition given for the case expression.

- "Syntax" below
- "How Do I Use This?" below

Syntax

if

```
| eval test = if ( deviceCustomNumber1 = 200, Success, Failure)
```

case

```
| eval test = case ( deviceCustomNumber1 = 200, Success,
deviceCustomNumber1 = 400, Failure, Unknown)
```

The operators support conditional expressions, such as >, >=, <, <=, =, etc.

How Do I Use This?

Less than

if

- I want to determine if incoming bytes are less than 5000 and to identify the lowest and highest values of incoming bytes.

  ```
  bytes in != null | eval test = if ( bytes in < 5000 , Low , High )
  ```

case

- I want to identify instances where incoming or outgoing bytes are below 3000 and return the lowest and highest values for each categogy.

```
bytes in != null AND bytes out is not null | eval test = case ( bytes in
< 3000 , Low , Bytes out < 3000, Low, High )
```

Equals

if

- I want to know all instances with an agent severity of 3.

```
agent severity != null | eval test = if ( agent severity = 3 , Success ,
Failure )
```

case

- Show me the device with the identification number 170011; otherwise show me the device with the identification number 3.

```
deviceCustomNumber1 is not null | eval test = case ( deviceCustomNumber1
= 170011 , Success , deviceCustomNumber1 = 3 , Failure , Unknown )
```

Contains numbers

if

- I want to identify all instances with a severity rating of zero (0) or one (1).

```
agent severity is not null  | eval test = if ( agent severity = 1 , 1 , 0
)
```

case

- Show me which devices have encountered a severity level of four (4); otherwise show me the highest and lowest severity levels.

```
agent severity is not null AND priority is not null | eval test = case (
agent severity = 4 , SHigh , priority > 5 , PHigh , other )
```

Three conditions

case

- I want to test three conditions (username, category outcome, and category technique) to identify Arcsight user names, any failed category outcomes, and any category techniques that might be exploited or represent vulnerabilities.

```
source username != null AND category outcome != null AND category
technique is not null | eval test = case ( source username = Arcsight ,
Arcsight , category outcome = '/Failure' , Failure , Category Technique =
'/Exploit/Vulnerability' , Vulnerability , other )
```

For information about other operators, functions, and syntax requirements, see "General Syntax for Eval" on page 46, "Understand Eval Functions" on page 49, and "Create powerful queries with search operators and functions. You can also select several out-of-the-box system searches that contain a query plus specific criteria. Operators, such as eval, can be chained together to create complex queries." on page 29.

replace

The **replace** is a function of the eval operator that provides a mechanism to replace the content (expressed as string) of a column and to return the value in a new column.

Before using replace, create a query that contains string values in its columns. When using replace, the process transforms the data into temporary tables so that the transformation occurs after the main query is executed.

- "Syntax" below
- "Parameters" below
- "How Do I Use This?" on the next page

Syntax

```
Name is not null | eval test = replace(Name, "Response", "Returned Value")
```

The replace function is case sensitive. For example, "This," "THIS," and "this" are considered three different words. Match the exact string in order to replace it.

Query input within [ ] (straight brackets) is optional for the query syntax.

Input within < > (angle brackets) indicates users may enter their own input: ... | rename *<source_name>* as *<NewSourceName>*

Parameters

Replace has three parameters:

- **Name**, the source string value
- **Response**, the match value that will be substituted with the returned value in the results
- **Returned Value**, the replacement value

How Do I Use This?

Use replace when you want to obfuscate data, improve the context of a column, or make reading the text more intuitive.

You can also use the replace function to replace an entire string.

- In this example, use replace to substitute a device's vendor name with Micro Focus.

```
| eval newDeviceVendor = replace ( deviceVendor, "HPE", "Micro Focus")
```

  where:

- `DeviceVendor` is the source name for the string value.
- `HPE` is the response value.
- `Micro Focus` is the returned value.

For information about other operators, functions, and syntax requirements, see "Create powerful queries with search operators and functions. You can also select several out-of-the-box system searches that contain a query plus specific criteria. Operators, such as eval, can be chained together to create complex queries." on page 29.

tonumber

The **tonumber** eval function converts string columns into floating point numbers so that the data can be applied to additional calculations. If a result cannot be expressed as a number, the column is left empty.

- "Syntax" below
- "Parameters" below
- "How Do I Use This?" below

Syntax

```
suboperator : tonumber
```

```
<search_criteria> | eval <alias_name> = tonumber (<one_column>)
```

where:

- <*search_criteria*> a non-pipe operator query statement, such as "deviceVendor IS NOT NULL"
- <*alias_name*> a valid column alias
- <*one_column*> a valid column (or field) as a parameter for "tonumber"

Query input within [ ] (straight brackets) is optional for the query syntax.

Input within < > (angle brackets) indicates users may enter their own input: ... | rename <*source_name*> as <*NewSourceName*>

Parameters

There can be only one <*columnName*> such as a device vendor or a version.

How Do I Use This?

Use tonumber to convert string values to numbers.

- Create a search query that converts log messages to numbers:

```
| eval messagesAsNumber = tonumber ( message )
```

- Create a search query that converts vendor devices to numbers:

```
| eval x = tonumber ( deviceVendor )
```

- Create a search query that checks for vendor device data that is not NULL and convert the data from version fields to numbers:

```
deviceVendor IS NOT NULL | eval test = abs ( 10 ) + 10 | eval
toNumberAlias = tonumber(version) | eval test2 = abs (13)
```

- Filter the data for those entries where ArcSight is the device vendor. Transform the version to a number and the device's custom number to a string value:

```
Device Vendor = "ArcSight" | eval toNumberAlias = tonumber(version) |
eval numberToString = tostring (deviceCustomNumber1)
```

For information about other operators, functions, and syntax requirements, see "Create powerful queries with search operators and functions. You can also select several out-of-the-box system searches that contain a query plus specific criteria. Operators, such as eval, can be chained together to create complex queries." on page 29.

tostring

The **tostring** function is used in an eval operation to convert columns into string values. The input for tostring can be string values, numbers, integers, double point, float, IP/MAC address, and dates. All of these inputs must come from a column in the database.

- "Syntax" below
- "Parameters" below
- "How Do I Use This?" below

Syntax

```
<search_criteria> [<pipe_operator>]* eval <alias_name> = tostring (<one_column>) [<pipe_operator>]*]*
```

Query input within [ ] (straight brackets) is optional for the query syntax.

Input within < > (angle brackets) indicates users may enter their own input: ... | rename *<source_name>* as *<NewSourceName>*

Parameters

The function only accepts one parameter. More than that will cause an error. The parameter can be a column that represents a string, number, IP address, MAC address, and date. If the parameter is null, it returns a null input.

How Do I Use This?

Here are examples of queries using tostring:

```
... | eval testString = tostring(Name)
```

```
Name not equal null | eval testNumber = tostring(AgentSeverity)
```

```
... | eval testmac = tostring(Agent Mac Address)
```

```
... | eval testData = tostring(Device Receipt Time)
```

```
Agent Address not equal null | eval testIp = tostring(Agent Address)
```

For information about other operators, functions, and syntax requirements, see "Create powerful queries with search operators and functions. You can also select several out-of-the-box system searches that contain a query plus specific criteria. Operators, such as eval, can be chained together to create complex queries." on page 29.

Understand the Search Criteria

You must have the **Manage Search Criteria** *permission.*

The **search criteria** defines the settings for your search, the time range in which to find data and the fieldsets that you want to use for displaying the results. Search provides "Understand the System Searches" on page 13 that you can view and load, such as DoS Events, MITRE ATT&CK Events, and Failed Login Event.

You can also save your search criteria for future use, such as loading the criteria into another search. You have the option to clone, modify, or remove a saved criteria at any time.

Manage the Fieldsets Displayed in 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 in the Fields column 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 Fieldsets**: Predefined fieldsets provided by the system.
- **My Fieldsets**: 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 list box even when moving to other search tabs. If you select another fieldset, the pop-up window closes to display the new option. You can revert the change to the previously selected fieldset.

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.

Create a Fieldset

1. From the **Search** page, click the icon to the left of the search name.
2. From the selected search's tab, click the menu and select a fieldset from the list in the **My Fieldsets**panel.
3. Click **Manage**.
4. Click **+** to add a new fieldset.
5. Enter a **Fieldset Name**.
   - Each fieldset should have a unique name.
   - Fieldset names are not case sensitive.
   - The fieldset is used only for your search results and does not affect other users connecting to the same system.
6. Select a **Category** and drag and drop any of the **Fields** to the to the **Selected Fields** column.
7. Click **Save**.
8. (Optional) Select **Apply to This Search** to customize the original fieldset without overwriting or saving it.
9. To execute the query again, click **Search**.

Edit 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
- "Cloning a Fieldset" on page 67

Editing the Selected Fieldset

1. From the **Search** page, click the icon to the left of the fieldset name.
2. From the fieldsets window, click the fieldset menu and select a fieldset from the list in the My Fieldsets panel.
3. From the fieldsets window, select **Edit**.

   The **Edit Fieldset** window displays.

4. Drag and drop any field to the **Selected Fields** column OR select **Text Editor** to write the fields you need.
5. To locate a specific field, use the **Search** field.
6. In the **Fieldset Name** field, update the fieldset name as needed. 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 existing fieldset without overwriting or saving it.

   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 temporary custom fieldset at a time.

Editing a Different Fieldset

1. From the **Search** page, click the icon to the left of the fieldset name.
2. From the fieldsets window, click the fieldset menu and select a fieldset from the list in the My Fieldsets panel.
3. Click **Manage**.
4. Select the fieldset checkbox.
5. Click the **Edit fieldset(s)** icon.

   The Edit Fieldset window displays.
6. Drag and drop any field to the **Selected Fields** column OR select **Text Editor** to write the fields you need.
7. To locate a specific field, use the **Search** field.
8. In the **Fieldset Name** field, update the fieldset name as needed. The fieldset is used only for your search results and does not affect other users connecting to the same system.
9. Click **Save**.
10. (Optional) Select **Apply to This Search** to customize the existing fieldset without overwriting or saving it.

    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 temporary custom fieldset at a time.

Cloning a Fieldset

You can make a copy of a fieldset you have created. Edit this copy to save you from creating a completely new fieldset.

1. From the **Search** page, click the icon to the left of the fieldset name.
2. From the fieldsets window, click the fieldset menu and select a fieldset from the list in the My Fieldsets panel.
3. Click **Manage**.
4. Select the fieldset checkbox.
5. Click the **Clone fieldset(s)** icon to make a copy of the selected fieldset.

Delete 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. If you delete a fieldset used in a saved search query or saved search criteria, Search will use the default fieldset saved in your user preferences.You cannot delete a system fieldset.

1. From the **Search** page, click the icon to the left of the fieldset name.
2. From the fieldsets window, click the fieldset menu and select a fieldset from the list in the My Fieldsets panel.
3. Click **Manage**.
4. Select the fieldset checkbox.
5. Click the **Remove fieldset(s)** icon.
6. Click **Yes** to proceed.

Configure 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, Log Management and Compliance 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.

- "Specify a Dynamic Date Range " below
- "Understand the Search Timestamps for Events" on the next page
- "Understand How Time Zones Affect Search Results" on the next page

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:

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
$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

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 the 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 when searching for events.

Database Receipt Time (dBRT)

Represents the time when the database received the event. The database considers this timestamp as the *persisted time* of the event.

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 (NET)

Represents the best known time for an event. Ideally NET is the time when the connected device reported that 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*

Understand 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 Histogram converts the time segments to the specified time zone. If the Results 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.

Extend the Search with a Lookup List

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

You can make CSV files, or **lookup lists**, that enable 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.

- "Understand the Considerations for the Lookup List File" below
- "Create a Lookup List " on the next page
- "Append a Lookup List " on the next page
- "Replace a Lookup List " on page 72
- "Delete a Lookup List " on page 72

Understand the 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.
- For search operations, the corresponding data types for lookup lists with variable characters (or varchars) are short text (VarShort) and long text (VarLong).
- The remaining rows must be comma-separated values for the fields in the first row.
- Do not include spaces before, after, or within a field name.
- 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. Click **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	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

6. To upload the file as a table in the database, click **Upload**.

Append a Lookup List

Use the **Append** feature to add more rows to a current lookup list.

- The file you need to append needs to have the same structure as the one you uploaded. For example, the same amount of columns.
- The file you need to append should not have an empty value in any of its rows.

1. Select **Configuration** > **Lookup Lists**.
2. Click the **eye** icon on the left side of the selected lookup list.
3. Click **Append**.
4. Select the list you want to append.
5. Click **Upload**. The original lookup list will be updated with the new rows added.

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 you want to replace.
3. Click the **eye** icon on the left side of the selected lookup list.
4. Click **Replace**.
5. Select the CSV file 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 you want to delete.
3. Select the **trash can** icon.

Creating and Saving Searches

To execute a search, you must enter the query input, a fieldset that you want for the search results, 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 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 configure your preferred default setting. For example, you can configure a default time range. To use the same search query or query plus criteria for multiple searches, you should **save** the query or

criteria. You can also save the results of an executed search and configure a default expiration time for searches. By default, session searches expire after 24 hours of inactivity and saved searches after seven days. Search truncates long queries, displaying **…** to indicate additional content. To see the entire query, you can **pin** the input field.

NOTE: Log Management and Compliance supports up to 10 active searches and 40 saved searches per user.

Create a Search

Select **Search** > **+**.

To execute a search, you must specify the query. You can use the default values for the fieldset, time range of data to search, and some additional settings or specify your preferred settings. Alternatively, you can load a saved query, criteria, or dataset.

If you tend to use the same settings for some search parameters, you might want to configure your preferred default setting. For example, you can configure a default time range. To use the same search query or query plus criteria for multiple searches, you should **save** the query or criteria. You can also save the results of an executed search and configure a default expiration time for searches. By default, session searches expire after 24 hours of inactivity and saved searches after seven days. Search truncates long queries, displaying **…** to indicate additional content. To see the entire query, you can **pin** the input field.

If you exceed the search limit, the following error message will display when creating a new search: "An error occurred while creating search. Exceeding the limit of 1000 searches." You cannot create anymore searches if this error displays. Contact your Administrator to increase the search limit or delete some existing searches. If you are a SaaS customer, reach out to Support to increase the search limit. For more information about increasing the search limit, see Configuring the Deployed Capabilities in the *Administrator's Guide to ArcSight Platform.*

1. Select **Search** > **+**.
2. Enter the query in one of following ways:
   - To use a predefined System search, type **#**.

     The predefined searches might provide only a query expression or include search criteria such as a specific time range.
   - To use a search operator, such as eval and wheresql, begin typing the operator's syntax.

     For example, type:

     ```
     ... | where <expression>
     ```

- To manually enter the query, begin typing the expression.

  For example, type :

  ```
  Source Address = 192.10.11.12 and Destination Address= 192.10.11.12 or Destination Address in Subnet 192.10.*.*
  ```

- To use a saved query, criteria, or search results, select .
- To search data migrated from ArcSight Logger, select **Logger** from the list box next to the **Search** button.
- To search for a field without data, enter `[field_name] = Null`.

> In the query, Search treats a comma (,) between the search fields and values as an OR operator.

3. (Optional) To view all content in a very large query, select the **Pin** icon in the query input field.

   Otherwise, Search truncates long queries, displaying … to indicate additional content.
4. Specify the fieldset that you want for displaying the search results.

   By default, Search displays 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 menu, select a pre-defined value under **Quick Ranges**.
   - From the menu, use the **Custom Range** fields to specify a time range.
   - From the menu, select **Dynamic**, and then enter a dynamic date value.

   You can also specify the timestamp that you want to use for the retrieved events. Search uses "Normalized Event Time (NET)" on page 69 by default.
6. (Optional) To limit the number of results received from the search, complete the following steps:
   a. Select ⚙ to the right of the query input field.
   b. For **Maximum search results**, specify the maximum number of results that you want to receive in the dataset.

   > If you enter a value outside of the predefined max search results preference, you will receive an error message.
7. (Optional) If you do not want this search to expire in the default time, complete the following steps:

a. Select ⚙ to the right of the query input field.

b. For **Search expires in**, specify the number of hours that Search will store the session.

> If you enter a value outside of your predefined search expiration preference, you will receive an error message.

8. (Optional) To more easily find this session search later, give the search a name.
9. (Optional) To run the search, click **Search**.

   Alternatively, you can press **Enter** when editing the query input field.
10. (Optional) To save the query, criteria, or search results for future use, select the **Save** icon.

Load a Saved Search

If you have saved a query, criteria, or search results, you can load that saved item in a Search tab. You can also load the predefined search queries and criteria.

1. Select **Search** > **+**.
2. Select 📁 above the query input field.
3. Select the tab relevant to the saved search that you want to load:
   - Search Query
   - Search Criteria
   - Search Results
4. Select the saved search that you want to load.
5. Select **Load**.
6. (Optional) Modify the search settings as needed, then run the search.
7. (Optional) To more easily find this session search later, give the search a name.
8. (Optional) To save your changes as a new search, select 💾.

Run a Search

When you run a search, Search begins populating the Events histogram 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.

1. Create or load the search that you want to run.
2. Click **Search**.
3. (Optional) To more easily find this search later, give the search a name.
4. (Optional) To save the query, criteria, or search results for future use, select the **Save** icon.
5. Click the **pause** or **stop** icons if you need to interrupt the search. Click the **resume** icon to continue the search.

Initiate a Search from Enterprise Security Manager

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

To perform this action, you must enable Log Management and Compliance in ESM. For more information, see the *ESM Installation Guide*.

Modify the Search Query or Criteria

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

1. In the Search tab, 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**.

Name a Search

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

1. Right-click the name of the tab.
2. Select **Rename**.
3. Type the custom name.
4. Press **Enter**.
5. (Optional) To save the search, click the **Save** icon.

Search Event Data from Logger

Logger archive data can be viewed and consumed using the same parameters as in regular searches. From the **Search** page, hunt for ArcSight Logger events by selecting the **Logger** option from the list box next to the **Search** button.

Before searching Logger events, the data must be imported to the ArcSight Database. The import process might require several imports from several Loggers. Otherwise, the **Logger** option will not be displayed in the **Search** page.

Before running a search on the Logger data, review the following considerations:

- Search supports only Log Management and Compliance's specific set of operators.
- Your searches can include data from Logger's storage groups even if the Logger storage groups do not display as part of Log Management and Compliance's configuration.

1. Select **Search** > **+**.
2. From the list box next to the **Search** button, select **Logger**.
3. Add the required query details.
   You must use the search operators supported in ArcSight Platform.
4. Click **Search**.

Handling Logger imported data timestamps

The timestamps of the data imported from Logger are in UTC format. Since Log Management and Compliance uses browser time or a user-selected time zone for searches, the time period entered to search through imported Logger data must be adapted to those original UTC timestamps.

To obtain the data contained during the correct time stamps, you can either:

- **For already imported Logger data:** convert the archive UTC timestamp shown in the **Import Logger Data** tab to your browser time/selected time zone, and enter that value as search time
- **For non-imported Logger data:** convert the time period you wish to search through from browser time/selected time zone to UTC, and enter the UTC values in the **Import Logger Data** tab before importing the data. Once the data is imported, you can search through it using the original browser time/selected time zone.

Save the Search

In any Search tab, select **Save** or in the saved list, click **+**.

You can save a search at any time. To save just the query or the query and criteria, you do not need to execute the search. After entering a query or criteria, or executing a search, complete the following steps:

1. In the Search tab, select the **Save** icon.

   Alternatively, when viewing a list of saved queries, criteria, or results, click **+**.
2. Select which part of the search you want to save:
   - Search Query
   - Search Criteria
   - Search Results (Dataset)
3. Specify a name for the saved search.
   - Each saved search must have a unique name.
   - We do not recommend using the same names for saved search queries, criteria, and results.
4. (Conditional) When saving the search results, specify how long you want to store the dataset.

   For example, if you have a Log Management and Compliance license and the *Never Expire Search Results* permission, you can configure a search to never expire.
5. Select **Save**.

Viewing and Managing Your Searches

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.

Get an Overview of Your Searches

Search Queries
Shows the number of system, private, and public saved search queries that you can access.

Search Criteria
Shows the number of system, private, and public saved search criteria that you can access.

Search Results
Indicates whether any of your saved search results have completed, are running, or have been paused.

Fieldsets
Shows the number of system and private fieldsets that you can use when running a search.

Lists
Shows the number of lookup lists that you can include in a search.

View the Results of a Search

Search results are displayed in an Events Histogram, Search Results table, and Event Inspector panel. If connectors are configured to send raw events, the table and inspector panel can include raw event data. Also, the maximum number of events that a search can return is 10 million, but you can specify a preferred limit. If your searches regularly stop at the maximum limit, consider splitting the query into separate searches.

You can export the search results to a CSV file.

- View the Event Histogram
- View the Search Results Table
- View the Event Inspector

View the Event Histogram

The Histogram displays data in a segmented graph where the y-axis presents the number of events per bars of time segments in the x-axis. The time range on the x-axis might not match the time range specified in the search query because the start and end times on the x-axis are determined by the event times of the first and last matching events of the search query.

Click the menu to the right of the histogram and select either Linear Scale or Log Scale to display the data in your preferred format. As you hover your pointer over the histogram, the bar color directly below the pointer changes and displays a tooltip of the day/date/time of that event range. Click a bar to view event information for a specific time range. Click again to deselect the bar.

Note that some search activities do not require the histogram, and thus it will not be displayed. For example, if you perform an aggregation operation, such as "top" or "bottom," Search will not display the histogram because the Search Results table contains the aggregation of results, not events in a timeline.

How Search builds the histogram

Search progressively builds the histogram as it receives events that match the search settings. If the search needs to scan a large amount of data or a large time period, the histogram displayed initially might refresh multiple times while the search is running. To view the complete histogram of a search, wait until the search has finished running.

Search plots the first one million matching events on the histogram. If a search results exceed one million events, Search displays an informational message. If you need to use the histogram view for event analysis of a search that matches more than one million events, we suggest that you adjust the time range to retrieve fewer than one million events. This will allow you to obtain a complete and meaningful histogram. You can also use a pipeline operator to further refine search results so that the total number of hits is under one million events.

Narrow the scope of the search

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, adjust the boundaries of the displayed bars. As you adjust the time range within the Histogram, the Results table displays corresponding events.

Drill down to events

You can drill down to events in a specific time period by clicking the bar on the histogram that represents that time period. The bar you drilled down to is highlighted and the events matching that time period are listed below the histogram. To deselect the time period, click the bar again. When you **hover over a histogram bar**, the matching events listed below the histogram do not change, and the histogram continues to display all matching events.

View the Search Results Table

The **Search Results** table contains all the fields specified in the fieldset. You can choose to display the table in **Grid View** or **Raw View**.

The following actions can be performed while viewing the table:

View all details for an event

To view details of a specific event, right-click the event and select **Open In Event Inspector**. This action opens the Event Inspector in a panel on the right where you can view additional details on the event.

View raw event data

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

Export the search results

To export the results to a CSV file, select  .

Export a single event

To export a single event, right-click the event. Then, select either **Export to PDF** or **Export to CSV**.

Copy a value from an event

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

Compare data in columns

Hover over a column heading, then click the **Pin** icon to pin or unpin a 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.

Reorder columns

To rearrange the order of the columns, drag each column to new position by clicking and dragging the column header.

Sort the data in columns

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

View the Event Inspector

The Event Inspector displays additional details on any event you select from the Event table. This panel allows you to scroll through the specific details of the event and groups the details by categories such as **Agent** and **Source**. To open the Event Inspector, right-click any event in the Search Results table. Then, select **Open in Event Inspector** from the pop-up menu.

To view events migrated from Logger, select **Logger** before creating a search.

You can perform the following functions with the Event Inspector:

Search for fields and values

To search for fields and values in the details of an event, enter a string in the search box at the top of the Event Inspector. The Event Inspector will filter the fields and values to match your search criteria.

Add fields and values to current or new search

You can add event fields and values to your current search or a new search.

Hover over a field (for example, Agent Hostname) to display a check box next to the field. Then, select the check box to select the field and its value. Then, either click the magnifying glass icon at the top of the Event Inspector or right-click your selected field. Both actions display a pop-up menu with the following options:

- **Create New Search:** Selecting this option allows you to create a new search query with the selected event fields and their values. For example, if you selected the field "Name" and its value equals "failed login", then it would display as follows in the new search query: Name = failed login. The new search will open in a new tab on your web browser.
- **Add to Active Search:** Selecting this option adds your selected event fields and their values to the current search query in the search input field. For example, if you selected the field "Name" and its value equals "failed login", the field and value would display as follows in the current search query: <current search query> | where Name = failed login.

Copy and share event detail URL

To share event details with another Analyst, click the **Copy URL** icon at the top of the Event Inspector. This action copies the URL to your clipboard so you can share it as needed.

Export event details to PDF or CSV

To export event details to a PDF or CSV format, click the **Export** icon at the top of the Event Inspector. A pop-up menu opens with the options **Export to PDF** and **Export to CSV**. Select the option that best meets your needs. You can include or exclude null fields in the exported file.

Expand/collapse and show/hide data fields

The top of the Event Inspector contains an arrow icon that expands and collapses the event details. There is also an eye icon that can show or hide null fields. If you select to display null fields and export the event details to PDF or CSV, the exported file will contain the null fields.

View and Use the Details of an Event

Right-click an event in the Search Results Table > click **Open In Event Inspector**.

The Event Inspector opens in a panel that allows you to scroll through the details of an event and groups them by categories such as **Agent** and **Source**. Use this panel when you want to research specific details on an event.

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. You can only open one event in the Event Inspector at a time.

To view events migrated from Logger, select **Logger** before creating a search.

- Search for Event Details
- Copy and Share Event Detail URL
- Export Event Details to PDF or CSV
- Apply Event Details to Current or New Search
- View Null Data Fields
- Expand or Collapse All Data Fields

Search for Event Details

The top of the Event Inspector contains a search box that allows you to search through the fields in the event details. Use this feature to quickly locate specific details on an event without the need to scroll through the entire Event Inspector.

To search for fields and values in the details of an event, enter a string in the search box at the top of the Event Inspector. The Event Inspector will filter the fields and values to match your

search criteria. For example, if you searched the term "device" the panel will display all fields with the name "device" and any fields containing the value "device".

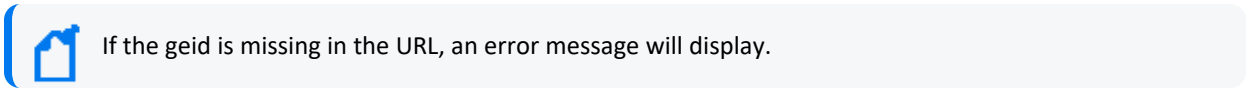
Copy and Share Event Detail URL

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

Click the **Copy URL** icon at the top of the Event Inspector to copy the Event Inspector URL to your clipboard. Then, you can share the URL as needed. When an Analyst loads the URL, the Event Inspector will open in their browser with the event details related to the URL.

This action is helpful in situations where you need an Analyst to research an event further or for reporting purposes.

Note: The Event Inspector URL contains the event's ID (id field in the Search Results table) and global event ID (geid field in the Search Results table). See the table below for an example and variations of the Event Inspector URL format. Use these formats to create the URL.



Event Inspector URL	Example
Full Event Inspector URL	/rec/fusionSearch/eventsInspector/?eventsTable=Recon&id=5139791690&geid=3009625190352082178
geid and id only	/rec/fusionSearch/eventsInspector/?id=5139791690&geid=3009625190352082178
geid only	/rec/fusionSearch/eventsInspector/?geid=3009625190352082178

Export Event Details to PDF or CSV

There may be situations where you need to use event details for reporting purposes. Or, you may need to share the event details with an Analyst who does not have access to the Event Inspector. You can do so by exporting the event details to PDF or CSV. Follow these steps:

1. At the top of the Event Inspector, click the **Export** icon.
2. A pop-up menu appears. Click either **Export to PDF** or **Export to CSV**.
3. Both selections will start a download of the event details to your selected format.
4. Share or use the PDF or CSV as needed.

If the option to show null values is selected, those null values are included in the exported CSV or PDF file. If null values are excluded, they will not appear in the exported file.

NOTE: You can also export an event to PDF or CSV from the **Search Results Table**. Right-click an event in the Search Results table to open a pop-up menu with the options **Export to PDF** and **Export to CSV**. If you use this method to export the event details, null values will be included in the exported file.

Apply Event Details to Current or New Search

You can add the field and value pairs in the event details to your current search or a new search. This action is helpful in situations where you need to research more data on a specific event. After adding a field and value pair to a current search or new search, you might need to add the respective field to the search fieldset if that field is not already part of the fieldset.

Hover over a field in the Event Inspector (for example, Agent Hostname) to display a check box next to the field. Then, select the check box to select the field and its value. From here, do one of the following actions:

- Right-click the selected event field
- Click the magnifying glass icon at the top of the Event Inspector

Both actions display a pop-up menu with the following options:

- **Create New Search:** Selecting this option allows you to create a new search query with your selected event fields and their values. For example, if you selected the field "Name" and its value equals "failed login", then it would display as follows in the new search query: | where Name = failed login.
- **Add to Active Search:** Selecting this option adds your selected event fields and their values to the current search query in the search input field. For example, if you selected the field "Name" and its value equals "failed login", the field and value would display as follows in the current search query: <current search query> | where Name = failed login.

Once you've performed a new search with the selected field and value pairs, the Event Timeline and Search Results table will filter to display data related to your new search.

View or Hide Null Data Fields

To show or hide fields with null data, click the eye icon at the top of the Event Inspector. Hiding the null fields filters your view of the event details to show only fields with data. Use this feature if you want to see only fields with data in the event details.

Expand or Collapse All Data Fields

Next to the eye icon at the top of the Event Inspector is an **Expand All/Collapse All** icon. Click this icon to expand the fields in the Event Inspector to show all values related to the fields. Or click it to hide the values related to the fields and display only the field names.

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
Event Details panel	--- in the cell

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.

Export Completed Runs of a Scheduled Search

*You must have the **Manage Scheduled Searches** permission to schedule runs of a search.*

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

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

1. Click the **CSV** icon next to the name of the scheduled search that you want to export.
2. Alternatively, view the search, then select the **CSV** icon to export the results.

Configure Preferred Settings for Searches

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

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. Or, if you regularly use the same fieldset for a Search, you can specify that fieldset as your preferred default. 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.

If you change your search preferences and you also have Scheduled Searches open in a separate browser tab, you must refresh the Scheduled Searches tab to ensure that the content in the tab reflects your changes.

Default Fieldset

Specifies the fieldset that you regularly use for a search. The default value is *Base Event Fields*.

Default View

Specifies whether 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 hh:mm:ss:ms`.

Default Time Setting

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

Base Searches On

Specifies the timestamp Search associates with the event you want to find. The default value is Normalized Event Time.

Search expires in

Specifies how often you want saved searches to expire, and thus for the system to remove them from the system. You can specify a value between 1 and 365. The default value is 7 days. Alternatively, if you have a Log Management and Compliance license, you can choose for a search to never expire.

The expiration date resets whenever you access the search. Resetting the expiration date includes resuming or re-running the search, as well as saving the search and changing its settings.

When you create or edit a search, you can override this default setting.

Session Search expires in

Specifies how often you want session searches to expire. The default is 24 hours. You can specify up to 120 hours.

The expiration time resets whenever you change or run the search. When you create or edit a search, you can override this default setting.

Maximum search results

Specifies the maximum number of events that Search returns. Search considers a search complete when the results reach the maximum limit. The default value is 10,000,000. The lowest value that you can specify is 1,000.

When you create a search, you can choose to override this default setting.

A **system-level setting** also controls the maximum number of searches (with a limit of 10 million) for all instances of Fusion. If you enter a value outside of the system-level setting, you will receive an error message indicating that your preferred default cannot exceed the system setting. For information about setting a global search limit, see Upgrading Deployed Capabilities in the *Administrator's Guide to ArcSight Platform*.

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 set as Yes.

Manage Searches

Select **Search** > **Search <*saved_search_type*>**.

If you have saved a search query, criteria, or dataset, you can manage the saved items individually or in bulk, import and export them in a CSV file, or delete them.

Manage Your Search Queries

Select **Search** > **Search Query**.

The saved search queries contain only the specified query expression, ready for you to load into a new search at any time. The list of saved queries includes both the queries that you have saved and the built-in System queries. You can **modify** or **delete** your queries at any time. However, you cannot delete or edit a System query. Rather, to change a System query, you should clone it, then make and save your changes.

Import a search query (as a gzipped JSON file) by clicking the `Import` icon, selecting the desired file, and clicking `Import`.

An imported file cannot exceed 100 MB, must contain only search queries with valid information.

You can also **export** one or more queries to a gzipped JSON file.

You must have *Import and Export Search Queries* permission to either import or export queries.

Manage Your Search Criteria

Select **Search** > **Search Criteria**.

Saved search criteria combine a query expression and other Search elements such as fieldsets and the time range of the data you want to retrieve. The list of saved criteria includes both the criteria that you have saved and the built-in System criteria. You can **modify** or **delete** your criteria at any time. However, you cannot delete or edit a System criteria. Rather, to change a System criteria, you should clone it, then make and save your changes.

By default, search criteria are sorted alphabetically by name. Date columns are displayed according to your user preferences.

If you have the *Import and Export Search Criteria* permission, you can **import** or **export** one or more criteria to a JSON file.

Import

1. Select **Search** > **Search Criteria**.
2. Click the **Import** icon.
3. Select the gzipped JSON file (or files) you want to import.
4. Click the **Import** icon.

   The selected criteria (and any associated fieldsets not already in the system) are imported.

Export

1. Select **Search** > **Search Criteria**.
2. Select the entries that you want to export.

3. Click the **Export** icon.

   The selected entries download into a gzipped JSON file.

Manage Your Search Results

Select **Search** > **Search Results**.

When you save search results, Search stores the dataset until the search expires or you delete it from the saved list. You can sort the list by the search's name, query, event time stamp, or date of the search.

If you load the saved dataset in a Search tab, you can update the query and criteria as needed, then save those changes as a new search query, criteria, or results. To share the results with colleagues, export the results to a CSV file.

Scheduling Regular Runs of a Search

*You must have the **Manage Scheduled Searches** 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.

Manage Scheduled Searches

*You must have the **Manage Scheduled Searches** permission to schedule runs of a search.*

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

- "Create a Scheduled Search" on the next page
- "Manage Scheduled Searches" above
- "Clone a Scheduled Search" on page 92
- "Edit a Scheduled Search" on page 92
- "Delete a Scheduled Search" on page 93
- "Enable and Disable a Scheduled Search" on page 93

For your 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.

Create a Scheduled Search

*You must have the **Manage Scheduled Searches** permission to schedule runs of a 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. Select **Search** > **Scheduled Searches**.
2. Select **+**.

3. Specify a **Name** that is 5 to 255 character long.
4. To enable the scheduled search, select **enable**.

   You also 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. Configure the settings for the dates and times of each run, based on how frequently they will run.

   NOTE: If you choose the **End after** option, the maximum number of instances is 1000.
7. For **Search Query and Metadata**, complete one of the following actions:
   - To use an existing search, type # then select from the list of available saved searches.
   - To create a new search, specify the query, fieldset, and time range.
8. Select **Schedule**.

Clone a Scheduled Search

*You must have the **Manage Scheduled Searches** permission to schedule runs of a search.*

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

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

1. Select the scheduled searches that you want to clone.
2. Click the **clone** icon.

Edit a Scheduled Search

*You must have the **Manage Scheduled Searches** permission to schedule runs of a 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.

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

Enable and Disable a Scheduled Search

*You must have the **Manage Scheduled Searches** permission to schedule runs of a search.*

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

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

1. Select the searches that you want to enable or disable.
2. Select **Enable** or **Disable**.

   The **Status** column, which you can add with the *Manage Columns* option, displays the status of either **Enabled** (green) or **Disabled** (red).

Delete a Scheduled Search

*You must have the **Manage Scheduled Searches** permission to schedule runs of a search.*

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

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.

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

Manage Completed Runs of a Scheduled Search

*You must have the **Manage Scheduled Searches** permission to schedule runs of a search.*

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.

- "View a Completed Run of a Scheduled Search" below
- "Save the Results of a Completed Run" on the next page
- "Delete Completed Runs of a Scheduled Search" on page 96
- "Export Completed Runs of a Scheduled Search" on page 96

View a Completed Run of a Scheduled Search

*You must have the **Manage Scheduled Searches** permission to schedule runs of a search.*

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.

A completed run can fail if the global search limit is exceeded. To verify if the global search limit was reached, create a new search. If the error message: "An error occurred while creating search. Exceeding the limit of 1000 global searches." displays, then the limit was reached. Contact your Administrator to increase the search limit or delete some existing searches. If you are a SaaS customer, reach out to Support to increase the search limit. For more information about increasing search limits, see Configuring the Deployed Capabilities in the *Administrator's Guide to ArcSight Platform.*

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.

Save the Results of a Completed Run

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

You can save the dataset from the completed run of a scheduled search, similar to saving other searches. When you save the run results, Search renames the selected run to the name that you specify. You also can choose how long to retain the dataset in the database.

1. When viewing a completed run, select the **Save** icon.
2. Specify a name for the saved dataset.
3. 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 files after**, you can specify a value that overrides how you configured **Search Expires In** for your search preferences.

     For example, you prefer that searches expire within five days. But you want the dataset for this completed run to expire after 10 days.
   - (Conditional) If you have the *Never Expire Search Results* permission, you can choose **Never Expire** to retain the dataset indefinitely.
4. Select **Save**.

Upgrading to the New Search Capability

After you upgrade to the new Search capability, you might encounter minor issues with saved scheduled searches. The general workaround to prevent these issues is to save your previous results **before** the upgrade and recreate them for new search runs. Issues you might see include:

- For completed scheduled searches before and after an upgrade, the "number of results" column may not match actual search results or equal zero. But, you can still view the actual results by opening the completed scheduled searches.
- The results of scheduled searches that contain the **eval** operator may not load properly if you are loading them in a search results tab that is already open.

Delete Completed Runs of a Scheduled Search

*You must have the **Manage Scheduled Searches** permission to schedule runs of a search.*

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

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

1. Select the completed runs that you want to delete.
2. Click the **delete** icon.

Export Completed Runs of a Scheduled Search

*You must have the **Manage Scheduled Searches** permission to schedule runs of a search.*

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

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

1. Click the **CSV** icon next to the name of the scheduled search that you want to export.
2. Alternatively, view the search, then select the **CSV** icon to export the results.

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

*You must have the **Manage Outlier Models and Scoring** permission 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 the next page
- "Define and Build a Model" on the next page
- "Score a Model" on page 99
- "Delete a Model" on page 100

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.

Define and Build 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 menu, select a pre-defined value under **Quick Ranges**
   - From the menu, use the **Custom Range** fields to specify a time range
   - From the 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.

Score a Model

*You must have the **Manage Outlier Models and Scoring** permission 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**.

Delete a Model

*You must have the **Manage Outlier Models and Scoring** permission 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. From the **Available Models** table, select the model that you want to delete.
3. Click **Delete**.

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, point to 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, point to 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.

Investigate 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.

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

   The 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**.
5. Click **Detect**.

If the scored model does not return data, the global search limit may have been reached. To verify, create a new search. If the following error message displays: "An error occurred while creating search. Exceeding the limit of 1000 global searches." displays, then the limit was reached. Contact your Administrator to increase the search limit or delete some existing searches. If you are a SaaS customer, reach out to Support to increase the search limit. For more information about increasing the search limit, see Configuring the Deployed Capabilities in the *Administrator's Guide to ArcSight Platform.*

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>**.

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 and Database Receipt 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" below
- "Understanding How Data Quality is Calculated" on the next page
- "Analyzing Data Quality" on page 106

Understanding the Data Quality Insights

Content in the Data Quality Dashboard is divided into the following categories that represent how big the gaps are among Database Receipt Time (dBRT), Device Receipt Time (DRT), and Normalized Event Time (NET):

- Active Events
- Future Events
- Past Events

Active Events

Indicates that your events have a timestamp within the database's active time frame where `NET - DRT = 0`. The Data Quality Dashboard presents active events in sub-categories based on the following time gaps between DRT and dBRT:

Sub-category	Description	Formula
Within 1 Minute	Data received in the ArcSight database with less than a one-minute gap	`dBRT- DRT = values between -60000 and 60000` milliseconds
Hour Ahead	Data received between one minute and an hour before DRT	`dBRT- DRT = a value between -3600000 and -60001` milliseconds
Hour Behind	Data received between one minute and an hour after DRT	`dBRT- DRT = a value between 60001 and 3600000` milliseconds

Sub-category	Description	Formula
Day Ahead	Data received between one and 24 hours before DRT	`dBRT- DRT = a value between -86400000 and -3600001` milliseconds
Day Behind	Data received between one and 24 hours after DRT	`dBRT - DRT = a value between 3600001 and 86400000` milliseconds
Week Behind	Data received between one day and one week after DRT	`dBRT - DRT = a value between 86400001 and 604800000` milliseconds

Future Events

Indicates that your events have a future timestamp where `NET - DRT < 0`. The Data Quality Dashboard presents future events in sub-categories based on the following time gaps between DRT and dBRT:

Sub-category	Description	Formula
Week Ahead	Data received between one and seven days before DRT	`dBRT - DRT = a value between -604800000 and -86400001` milliseconds
Far Future	Data received more than a week before DRT	`dBRT - DRT < -604800001` milliseconds

The **Far Future** critical category helps identify events that fall well outside the most accepted variance range.

Past Events

Indicates that events have a past timestamp where `NET - DRT > 0`. The Data Quality Dashboard presents past events in a sub-category based on the following time gap between DRT and dBRT:

Sub-category	Description	Formula
Distant Past	Data received more than a week after DRT	`dBRT - DRT > -604800001` milliseconds

The **Distant Past** critical category helps identify events that fall well outside the most accepted variance range.

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 ArcSight Database was installed or upgraded.

During a fresh installation, the process creates a new table to store Data Quality over time, with source information. The feature schedules the aggregation process at the tenth minute of every hour. For example, if a fresh install or upgrade was completed at 9:15:00 AM, the aggregation would be scheduled to execute at 10:10:00 AM and 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.

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 week** setting. If the Cron Job has not been run yet, the charts would display no data.

Data-Time series

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:

- **Category Selector**

  Displays data sources in each of the 12 Data Categories. *Far Future* is the default selection.
- **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, host name, and number of events of each source, hover over each donut piece. If you click a donut piece, the Hourly Event Volume chart displays more values.
- **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.

Managing and Importing 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 the system 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 the system 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.

Managing Your Stored 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.

Use Storage Groups to Organize and Retain Data

You 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. Your specified query filters 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, the event gets sent to the *Default Storage Group*. You cannot change the name, query, or rank of this built-in group.

By default, the maximum value for retaining events in the *Default Storage Group* is 12 months. However, the license for your deployed product might require a lower maximum value, such as 30 days.

The **Apply Changes to System** option at the top of the Storage Groups page indicates that one or more groups have been modified but the changes need to be applied.

- "Create a Storage Group" below
- "Direct Events to the Correct Storage Group" below

Create a Storage Group

You can have up to **10 storage groups**, including the provided *Default Storage Group*.

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

   You cannot change the name after you create the group.

   The name cannot include special characters other than a hyphen (-).
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.

Direct Events to the Correct Storage Group

For efficient data retrieval, the system matches each incoming event with the query filter for a 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, the system **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 the system assigns the event to the group that is ranked 3. If an event does not match any of the active filters, the system sends the event to the *Default Storage Group*.

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

1. Select **Configuration** > **Storage**.
2. From the **Storage Information** table, drag each storage group up or down to the preferred priority position.

   The system always places the *Default Storage Group* in the lowest ranked position.

Activate and Deactivate Storage Groups

You can have up to **10 storage groups**, including the provided *Default Storage Group*. To deactivate 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. To edit the group's settings, click the icon.
4. For **Group Status**, slide the indicator left or right.

   Activated groups display a status of **Active**.
5. Click **Save**.

Change 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.

- "Modify a Storage Group" below
- "Apply Your Changes to a Storage Group" on the next page

Modify 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. Click the **pencil** icon .
4. For **Group Status**, slide the indicator left or right.
5. Activated groups will display a status of **Active**.
6. Click **Save**.
7. "Apply Your Changes to a Storage Group" below.

Apply 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, the system 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, the system 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, the system begins deleting all data older than three months.
- While changes are being applied, you cannot create or modify a storage group.

Use 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.

Configure Retention Policies for Your Data

Events are stored in their assigned storage groups 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 your system to purge certain data, such as DNS logs that are older than 24 months.

When setting the policies for storage group retention and disk space utilization, do not allow your disk space utilization to increase above 90%. Running out of disk space can reduce the performance of searches due to increasing fragmentation. If such a situation continues to where there is no space left, then the database cannot ingest new data.

Delete Old Data from Storage Groups

Events are stored in their assigned storage groups 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, the data retention policy for your organization might expect data older than 24 months to be purged. This process **deletes data from the database**.

The system 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, when you want old events to be deleted.

   By default, the maximum value for retaining events in the Default Storage Group is 12 months. However, the license for your deployed product might require a lower maximum value, such as one month. Some licenses allow you to choose **Never Expire** for a long-term storage option.

   Ensure that your retention policy takes into consideration the maximum size of your storage groups and database. Also, consider that, in deleting events, the policy might affect results of an Event Integrity Check.
3. Click **Save**.
4. Apply your changes.

Retention Policies for Imported Logger Data

Applies only to a non-SaaS environment.

You can have up to 10 storage groups overall (including groups both created in the ArcSight Database and those migrated from Logger). Exceeding this quantity will likely affect the performance.

To manage the storage and expiration of the data recently imported from Logger to the ArcSight Database (see here for a non-SaaS environment or here for a SaaS environment), the retention policy will be automatically enabled for the Logger event data. You will not need to manually direct events to a certain storage group and implement additional retention policies, but rather take advantage of the same storage rules already set in Logger. You can update and review the retention policy strictly from the Logger interface. Likewise, the system will reflect the information added prior to the import.

For a non-SaaS environment

As part of the metadata migration, the tool brings in the Storage Groups and their retention information. Because in Logger the retention settings are based on days, the tool converts them to months and rounds it up as to comply with the format used by the ArcSight Database. If the **Maximum Archives Age** value was set to `-1` for a Storage Group in Logger (meaning a disabled retention policy), the retention process for it will also be disabled in the system.

Importing Event Data From Logger

If you have both ArcSight Logger and the Fusion capability deployed in your network infrastructure, you can search Logger event data collected over time. To do so, you must import the events stored in Logger archives. The process requires you to first import the event metadata, then the event data. Before you begin searching through Logger data, ensure that the data migrations have completed.

Choose your type of deployment and follow the instructions to set up the data migration:

For a non-SaaS deployment see "Importing Logger Data in a non-SaaS environment (requires ArcSight Database 11.1 or greater)" below.

For a SaaS deployment see Importing Logger Data in a SaaS Environment.

Importing Logger Data in a non-SaaS environment (requires ArcSight Database 11.1 or greater)

Does not apply in a SaaS environment

If you have installed the Platform using arcsight-platform-installer-22.1.0.16.zip or previous, the version of ArcSight Database you have is earlier than 11.1. Since importing Logger data requires version 11.1 or greater, please perform the database upgrade before attempting to conduct any Logger data importing.

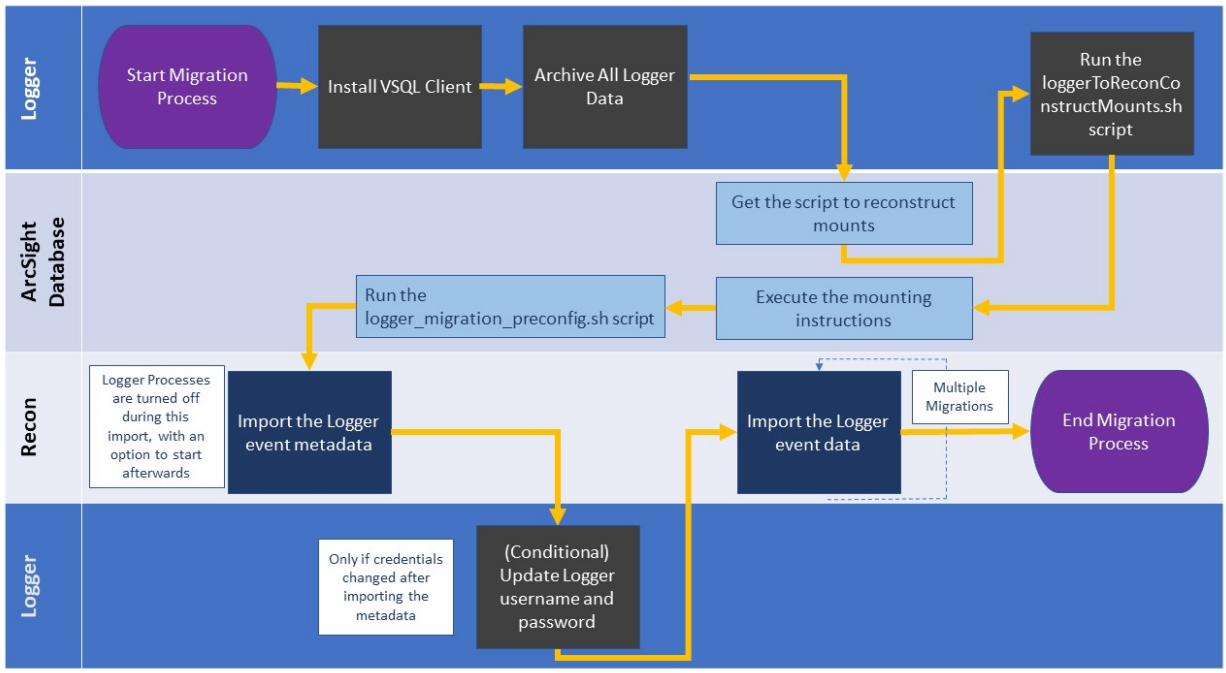
In a non-SaaS environment, you first import the event metadata, then the event data. Before you begin searching events imported from Logger, ensure that the data migrations have been completed. To start the procedure, please follow this checklist.

Logger event ingestion can continue during this procedure, up to the moment when the system advises you to stop ingestion.

Only one migration at a time can be done. If you plan to run migrations from different Loggers, run the migrations sequentially.

Only archive events from the current Logger instance are migrated to the ArcSight Database.The process does not migrate content, configuration, and data from Logger peers.

The following diagram shows the full process for importing event data from Logger to be used in the Fusion capability:



Checklist: Migrating Logger Data

Does not apply in a SaaS environment

Use the following checklist to migrate event data from Logger to be used in Search. You must perform the tasks in the listed order.

	Task	See
❑	1. Make sure that you comply with the prerequisites for importing Logger data	"Since this process involves different ArcSight products interacting with each other, ensure that you have the correct credentials and requirements for all of them before you proceed." on the next page
❑	2. Install VSQL Client Driver in Logger	"The Logger host requires the VSQL client to perform the data migration procedure. If the client is not present, follow these steps to install the VSQL Client driver." on page 117
❑	3. Archive all live data in Logger	"Archive Live Logger Data" on page 118
❑	4. Get the `loggerToReconConstructMounts.sh` script from ArcSight Database	"The following steps will allow you to obtain the instructions for mounting the archives in the ArcSight Database." on page 120
❑	5. Run the script to get archives mounting instructions	"The following steps will generate instructions for the mounting of the data." on page 120
❑	6. Run the mounting instructions and the `logger_migration_preconfig.sh` script in the ArcSight Database	"The following steps executed at ArcSight Database will set it up to receive the Logger migrated data." on page 121

❑	7. Import the Logger event metadata	"The Logger metadata represents the detailed references to events that can be:" on page 121
❑	8. (Conditional) If credentials were changed after importing metadata, update the username and password information, and then update the Logger registration	"(Conditional) Update the Logger Registration" on page 123
❑	9. Import the Logger event data that you want to search	"This option will allow you to bring events from a Logger instance to the ArcSight Databse and perform searches over the migrated data. Since this is process consumes both time and resources, consider migrating only data in necessary time ranges." on page 123

Prerequisites for Importing Logger Data

Does not apply in a SaaS environment

Since this process involves different ArcSight products interacting with each other, ensure that you have the correct credentials and requirements for all of them before you proceed.

- "Prerequisites for Logger" below
- "Prerequisites for the ArcSight Platform" on the next page
- "Prerequisites for the ArcSight Database" on the next page

Prerequisites for Logger

- Admin user with SSH credentials.
- The username and password that you use to import Logger data must match the OS credentials set in Logger.
- The system directory must have enough space. For more information, see the *Release Notes for ArcSight Logger*.
- Whether the Logger host is installed in the same machine or a different one, it will need to have the **VSQL Client Driver** installed (this will be explained in Step 1 of the procedure).

Prerequisites for the ArcSight Platform

- Admin user with ArcSight Database credentials.
- The system directory must have enough space. For more information, see the *Technical Requirements for the Arcsight Platform*.
- If the ArcSight Platform capabilities are deployed on the same machine as Logger, make sure that the RHEL/CentOS version used in Logger is supported by Fusion. For more information, see the *Release Notes for ArcSight Logger* and the *Technical Requirements for the Arcsight platform*.
- The ArcSight Platform capabilities must be reachable from the Logger instance (on port 5433).

Prerequisites for the ArcSight Database

- For the migration process, the user must have the *Logger Data Migration* permission assigned in Fusion. This is assigned by default to the *System Admin* role, but the user could have a custom role that includes the permission.
- For search execution after the data has been imported, users must have either the *Default Role* or a role with appropriate Search permissions.

Install VSQL Client Driver

Does not apply in a SaaS environment

The Logger host requires the VSQL client to perform the data migration procedure. If the client is not present, follow these steps to install the VSQL Client driver.

1. Download the TAR version of the driver.

   Tip: Micro Focus recommends to use the same version for database server and TAR driver. Refer to the Technical Requirements for Arcsight Platform for details on the supported version.

2. To extract the TAR from the directory, run the following command:

   ```
   tar xvfz vertica-client-[version] [OS].tar.gz -C /
   ```

3. From your home directory, add the PATH:

   ```
   cd ~
   ```

4. Open the file:

   ```
   vi .bashrc
   ```

5. On the PATH variable located by default in the **/opt/vertica/bin** file, add the vsql path:

```
export PATH-$ANT_HOME/bin:$JAVA_HOME/bin:$PATH:$P4_HOME/bin:/opt/vertica/bin
```

If the PATH variable is not found, create it:

```
PATH=$PATH:/opt/vertica/bin
```

6. Save the changes:

   `:wq` and press **ENTER**.

7. Refresh the .bashrc file:

```
source .bashrc
```

8. To verify VSQL has been installed, run the following command:

```
vsql --version
```

Archive Live Logger Data

Does not apply in a SaaS environment

You must archive all live data in Logger before you attempt the migration process.

- "Configure the Archive Storage Setting" below
- "Add an Event Archive" on the next page

Configure the Archive Storage Setting

Required only if you have not previously configured this setting

If you are using the Logger Appliance, create the NFS or CIFS mount point. For more information, see the Storage and Remote File System sections on Chapter 6 of the *Administrator's Guide to ArcSight Logger*. If you are using Software Logger and intend to use an NFS or CIFS mount point, ensure that the external storage point is mounted on the machine on which Logger is installed. For more information, see your system's operating system documentation.

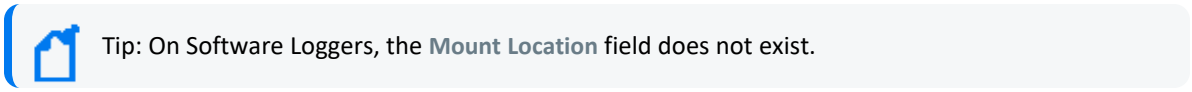
1. Go to **Configuration > Storage > Archive Storage Settings**.
2. Specify a mount location and an archive path for each storage group. You can specify a different path for each storage group, thus enabling Logger to archive events to a different location for each storage group.

   You can configure settings for all storage groups on the **Archive Storage Settings** page even if you do not intend to archive all of them. Logger enables you to only save the storage group paths that have a mount configured and ignore the empty fields.

- *On Logger Appliances:* Select (from the list box) a path in the Archive Path field appended to the path specified in the mount location. This location can be an NFS mount, CIFS mount, which is configured using the Logger user interface.

  For example, if the mount location you selected refers to the path `/opt/ARCHIVES`, and the archive directory in that location is `archivedir`, then specify `archivedir` in the **Archive Path** field.

- *On Logger Software:* Enter a complete path where the archive file will be written in the **Archive Path** field. This path could be a local directory or a mount point already established on the Logger host.



3. Click **Save**.

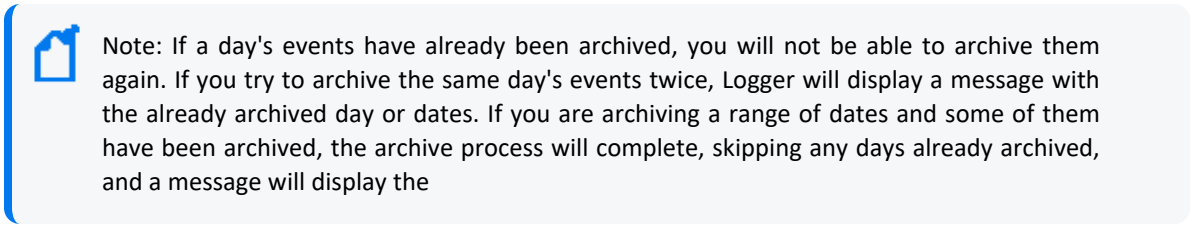
If all fields are blank or without any changes, Logger will display the message *No changes have been made* message. Otherwise, Logger will acknowledge the configuration with the message *Archive Storage Settings saved successfully*.

Add an Event Archive

1. Open the **Configuration > Storage** > **Event Archives**.
2. Click **Add** in the Event Archives page.
3. For **Name**, enter a meaningful name for the new **Event Archive**.
4. Specify the **Start** and **End** dates in the `mm/dd/yy` format.

   When the **Start** and **End** dates are different, the system creates one archive file per storage group, for each specified day. For example, that will be the case when you specify the following **Start** and **End** dates:

   ```
   Start Date: 8/12/19
   End Date: 8/13/19
   ```



   And, if you configure both storage groups—**Internal Event Storage Group** and **Default Storage Group**, four archive files will be created as a result of this archive operation—two files per storage group for the specified two days.

The **Event Archives table** in the **Event Archives** page lists the archives by an alias in the following format:

`<archive_name> [<yyyy-m-dd>] [<storage_group_name>]`

5. Select the names of the storage groups that need to be included in the archive.
6. Click **Save** to start archiving events, or **Cancel** to quit.

Note: You can cancel an in-progress archive operation at any time using the Cancel link that displays on top of the Event Archives page.

If corruption cases have been detected before, please check how To sanitize an Event Archive in chapter 5 of the *Administrator's Guide for ArcSight Logger*.

Obtain the Reconstruct Mounts Script

Does not apply in a SaaS environment

The following steps will allow you to obtain the instructions for mounting the archives in the ArcSight Database.

1. Navigate to the scripts folder in the ArcSight Database server, by default `/opt/arcsight-db-tools/scripts/`.

   This is where the loggerToReconConstructMounts.sh script is located.
2. To move the script to the Logger server from which you want to import event data, execute the following command:

```
scp /opt/arcsight-db-tools/scripts/loggerToReconConstructMounts.sh root@<LOGGER IP>/opt/
```

Execute the Reconstruct Mounts Script

Does not apply in a SaaS environment

The following steps will generate instructions for the mounting of the data.

These instructions are meant to be exact for use in Logger appliances. With Software Logger, which can save data locally or externally, you must make sure that the path contained in the instructions corresponds to the NFS mount you created when configuring archive storage. See "Archive Live Logger Data" on page 118

1. Give the execute right to the script that you just copied on Logger server:

```
chmod +x ./loggerToReconConstructMounts.sh
```

2. Execute the script:

```
./loggerToReconConstructMounts.sh $<INSTALL LOGGER PATH>
```

3. The instructions generated will consist of the `mkdir` command to create a directory, and the `mount` command to perform the actual mounting, for example:

```
Getting the instructions for /opt/mnt/ARCH-141-203
mkdir -p /opt/LOGGER_15214141203/opt/mnt/ARCH-141-203
mount -t nfs 15.214.129.238:/opt/shared|nfs4 /opt/LOGGER_15214141203/opt/mnt/ARCH-141-203
```

   These instructions will be generated for each of the mounts to be migrated.

Copy these instructions to execute them in ArcSight Database.

If the process fails to find archives that can be migrated, no instructions will be generated, and you will be notified by a UI message.

Execute the Instructions in ArcSight Database

Does not apply in a SaaS environment

The following steps executed at ArcSight Database will set it up to receive the Logger migrated data.

1. From your Linux command line, execute the two commands you copied during the procedure in "The following steps will generate instructions for the mounting of the data." on the previous page.
2. Run the `logger_migration_preconfig.sh` script located by default in the `/opt/arcsight-db-tools/scripts/` directory.

Import Metadata for Logger Events

Does not apply in a SaaS environment

This topic applies only to Logger processes soon-to-be shut down

The Logger metadata represents the detailed references to events that can be:

- Correctly scanned
- Allocated to the storage group of your selection
- Consumed in Search

You import the metadata once for each Loggerwhose processes are soon to be shutdown. Complete the following actions:

- "Register a Logger " below
- "Import the Metadata" below
- "(Conditional) Update the Logger Registration" on the next page

Register a Logger

Applies only if you have not previously registered the Logger from which you will import data

Before importing the metadata, make sure to add the Logger details for the import process.

1. Select **Configuration > Import Logger Data > Logger Metadata Import**.
2. Click the **+** icon.
3. Add the Logger details such as:
   a. **Host**: Logger IP address or host name
   For example, `12.345.67.890` or `logger6.extremelyfocused.com`
   b. **Host Username**: OS username
   c. **Host Password**: OS password
4. Click **Save**. Otherwise, click **Cancel**.

Note: You can remove Logger registration if no data has been imported. To delete the Logger registration, click the delete icon (trash can).

Import the Metadata

While importing the metadata, the Logger server must be accessible at all times.

The metadata contains all the information related to accessing the events of a particularLogger. You can migrate the Logger metadata to the ArcSight Database directly from the **Logger Metadata Import** page.

Make sure to import the metadata before importing the Logger data as this is the first step to view and consume logger events.

1. Go to **Configuration > Import Logger Data > Logger Metadata Import**
2. Check the box next to the Logger whose metadata will be migrated and click the **import** icon.

   A pop-up window will notify you that the Logger metadata import procedure is about to begin, making sure you have already mounted the appropriate archives on all database nodes.

Here you must also decide what you want done after the import of metadata is done. During the process itself, the associated Logger processes will be shut down. After the import ends, if you choose:

- **Yes** on the pop-up window, the Logger processes will resume after the import is finished. The system proceeds to import and store the metadata in Search.
- **No** on the pop-up window, the Logger processes will remain shut down. The system proceeds to import and store the metadata in Search.
- **Cancel** on the pop-up window, the metadata migration process will not be initiated.

(Conditional) Update the Logger Registration

If credentials have been changed after importing metadata, make sure to update the username and password information before importing data. Otherwise, an error message will be displayed. You will also need to update the Logger registration.

The Logger processes status, host username, and password can be updated after the Logger registration or metadata import. However, these values cannot be updated while an import is in progress.

1. Select **Configuration > Import Logger Data > Logger Data Import**
2. Check the box next to the Logger host and click the pencil icon.
3. Update the values accordingly.

   Ensure that the username and password that you use match the OS credentials set in Loggers.
4. Click **Save**. Otherwise, click **Cancel**.

Import Logger Data

Does not apply in a SaaS environment

This option will allow you to bring events from a Logger instance to the ArcSight Databse and perform searches over the migrated data. Since this is process consumes both time and resources, consider migrating only data in necessary time ranges.

Before you can migrate Logger data, you must import the metadata that defines it.

Select a data-time range different than the one already imported. To confirm the host's start and end dates already available in Search, see how to verify the migration table in "Review Migration Details" on the next page

- "Import Data" below
- "Review Migration Details" below
- "Resume an Incomplete Migration" on the next page
- "Delete Incomplete or Failed Migrations" on page 126

Import Data

Before importing data, review "Since this process involves different ArcSight products interacting with each other, ensure that you have the correct credentials and requirements for all of them before you proceed." on page 116.

1. Select **Configuration** > **Import Logger Data** > **Logger Data Import**.
2. Click **+**.
3. Select the Logger host of your preference.

   You can choose only one host at a time.
4. Specify the time range that you want to import.
   - The time range is based on receipt time.
   - The migration only allows you to migrate a minimum time range of 1 day.
   - Specify a date in the past. You cannot import data for future dates as it will import no events and will cause issues when you try to import new data again.
   - Overlapping dates will cause an error message. If this is not the first import of this Logger instance, ensure to select a time range different than the one already imported.
5. Click **Import**.
6. To check the import progress, view the **Import Status** column.

   The import will take a considerable amount of time, based on the quantity of events that are present in the time range selected.
7. (Optional) If the import is interrupted, you can attempt to resume the process.

   Alternatively, you can delete an incomplete migration.

Review Migration Details

The migrations table will display the most relevant information of all the imports executed. For each migration, the system registers the following details:

Logger Host
Represents the Logger IP address or host name. For example, `12.345.67.890` or `logger6.extremelyfocused.com`.

Data Start Date
Indicates the absolute date of the earliest possible event.

Data End Date
Indicates the absolute date of the latest possible event.

Import Date
Indicates the migration date and time displayed in the ArcSight Database timezone.

Import Status
Indicates the status of the import process:

- **Start Migration**: Confirms the Logger is reachable and can properly communicate with the system.
- **In progress**: Import is still in progress. PostgreSQL is downloaded to allow data to be extracted, read, and sent to the ArcSight Database.
- **Complete**: Successful import execution.
- **Failed**: Unavailable connections due to an unreachable Logger. Ensure that you review the prerequisites before importing data.

Event Count
Indicates the number of events migrated. This number increases automatically as the process continues.

Logger Host User Name
Indicates the OS username associated with the Logger host.

Data Import ID
Represents the unique identifier for the event migration. You must have this value to delete a migration.

To review details about the executed migration, see the logs in the `opt/vertica/udfs/datamigration/logs/` directory.

After events have been imported, the retention policy will be managed by Logger or the Fusion capability, depending on the state of the Logger processes.

Resume an Incomplete Migration

A migration might be interrupted if access to the mount or data file is affected in any way during the process: an unresponsive mount, a network connectivity issue, a user who doesn't

have the correct access permissions, data that couldn't be uncompressed, etc.

An **Incomplete** migration can be resumed. The process starts from the last point of migration so you do not lose the data previously migrated.

1. Select the migrations that you want to resume.
2. Click .

A migration that continues to appear as **incomplete** after it has been resumed at least once, might indicate the data cannot be migrated because of corruption issues.

Check the logs for any related messages, and contact support to help finish the migration.

Delete Incomplete or Failed Migrations

It's possible that a migration might fail to complete. For example, the status is **Failed** or indicates that the migration is **Complete** but it contains no events. In these types of scenarios, you can delete the migration, then try again.

1. Select the migrations that you want to delete.
2. Click .

Ensuring Data Compliance

We provide **Compliance Packs** that contain reports and dashboards to help you comply with a broad set of legal and governmental regulations that require your enterprise to organize and manage sensitive data and institute a strong IT governance program. Designed around industry best practices, these packages provide a comprehensive method for assessing and monitoring internal controls, such as access control changes, administrative activity, log-in monitoring, and change and risk management. The packages automatically map these technical checks to the relevant standard using policy and risk-relevant operational context so you can focus on key services and business processes and address critical audit points.

You must purchase, then import each Compliance Pack to the Reports Portal repository. For more information about the packs, see the ArcSight Solutions and Compliance Insight Package documentation site.

- "Ensuring Compliance with GDPR Standards" below
- "Ensuring Compliance with IT Governance" on page 149
- "Ensuring Compliance with PCI DSS" on page 172
- "Ensuring Compliance with SOX Standards" on page 210

Ensuring Compliance with GDPR Standards

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

The European Union (EU) adopted the General Data Protection Regulation (GDPR) to ensure that businesses and organizations protect individuals' data privacy and security. If your enterprise processes the personal data of EU citizens or residents or offers goods and services to such individuals, then you must comply with the GDPR. The regulation sets out standards for any action, automatic or manual, that processes a person's data. These standards include requiring that data controllers and data processors – the individuals in your enterprise or third-party organizations who control, manage, or make decisions about data processing – must be able to demonstrate that they are GDPR compliant.

To help you comply or prove compliance with GDPR, we provide the **Compliance Pack for GDPR**. For more information about adding the pack to the Reports repository, see the *Solutions Guide for ArcSight Compliance Pack for GDPR*. The guide includes information about identifying assets that must comply with GDPR.

This package includes the following dashboards and reports, organized by GDPR objectives:

Category	Dashboards	Reports
Access Activity - Access Activity	After Hours Access Activity on GDPR Systems Overview Authorization Changes on GDPR Systems Overview Failed Access Activity on GDPR Systems Overview Failed Access Relationship on GDPR Systems Overview Failed Access Activity by GDPR Asset Failed Access Activity on GDPR Systems by User	After Hours Access Activity on GDPR Systems Summary Authorization Changes Summary on GDPR Systems Failed Access Activity by GDPR Assets Failed Access Activity on GDPR Systems Summary Failed Access Activity on GDPR Systems by Users
Access Activity - Regulatory Exposure	n/a	Potential Regulatory Exposure on GDPR Systems
Access Activity - Threat User Analysis	n/a	Admin Activity from Compromised GDPR System Anti-Virus Disabled on GDPR Systems Summary Audit Log Cleared on GDPR Systems Summary Threats Executed against GDPR Systems Summary
Admin Activity	n/a	User Creations on GDPR Environment User Deletions on GDPR Environment Users Added to a Group on GDPR Environment Users Removed from a Group on GDPR Environment

Category	Dashboards	Reports
Attack Surface Analysis - Attack Surface Identification	High Risk Vulnerabilities on GDPR Systems Information Leakage Vulnerabilities on GDPR Systems Password and Authentication Weaknesses on GDPR Systems SQL Injection Vulnerabilities on GDPR Systems SSL or TLS Vulnerabilities on GDPR Systems Vulnerabilities on GDPR Systems Overview Vulnerable GDPR Assets by Vulnerability Type XSS Vulnerabilities on GDPR Systems	High Risk Vulnerabilities on GDPR Systems Information Leakage Vulnerabilities on GDPR Systems Password and Authentication Weaknesses on GDPR Systems SQL Injection Vulnerabilities on GDPR Systems SSL or TLS Vulnerabilities on GDPR Systems Unpatched GDPR Systems Vulnerability Summary by CVE ID Vulnerability Summary by GDPR Asset Vulnerability Summary on GDPR Systems XSS Vulnerabilities on GDPR Systems
Attack Surface Analysis - Security Controls Risk Identification	DoS Attacks Against GDPR Systems	DoS Attacks Against GDPR Systems
Corporate Governance	Access Activity on GDPR Systems Overview Geo Access Activity on GDPR Systems Overview Physical Access Activity on GDPR Systems Overview	Access Activity on GDPR Systems Summary After Work Hours Physical Access Activity on GDPR Systems Summary Physical Access Activity on GDPR Systems Summary

Category	Dashboards	Reports
Regulatory Exposure	Data Flow to GDPR Systems Data Flow from GDPR Systems Data Flow from GDPR Systems to non EU Data Flow from non EU to GDPR Systems GDPR Systems Communication with non EU Countries GDPR Systems Communication Overview High Risk Events on GDPR Systems Overview Policy Violations on GDPR Systems Overview Threat Relationship on GDPR Systems Overview Threats on GDPR Systems Overview	Data Flow from GDPR Systems Summary Data Flow from GDPR Systems to non EU Summary Data Flow from non EU to GDPR Systems Summary Data Flow to GDPR Systems Summary High Risk Events on GDPR Systems Summary Policy Violations on GDPR Systems Summary Threats on GDPR Systems Summary

Category	Dashboards	Reports
Threat Analysis - Data Store Risk	n/a	Attacks Against Databases on GDPR Systems Cassandra Vulnerabilities on GDPR Systems CRM and ERP Vulnerabilities on GDPR Systems Database Configuration Changes on GDPR Systems Database Weaknesses on GDPR Systems Elasticsearch Vulnerabilities on GDPR Systems IBM Db2 Vulnerabilities on GDPR Systems MariaDB Vulnerabilities on GDPR Systems Microsoft SQL Server Vulnerabilities on GDPR Systems MongoDB Vulnerabilities on GDPR Systems MySQL Vulnerabilities on GDPR Systems Oracle Vulnerabilities on GDPR Systems PostgreSQL Vulnerabilities on GDPR Systems Redis Vulnerabilities on GDPR Systems
Threat Analysis - Internet	Malware Found on GDPR Systems MITRE ATT&CK on GDPR Systems by GDPR Asset MITRE ATT&CK on GDPR Systems by MITRE ID MITRE ATT&CK on GDPR Systems Overview MITRE ATT&CK Relationship on GDPR Systems Overview	Firewall Blocked Events in GDPR Environment Information Leaks from GDPR Systems Malware Found on GDPR Systems

Access Activity

Select **Reports** > **Portal > Repository** > **Standard Content** > **GDPR** > *Reports* or *Dashboards* > **GDPR Access Activity**.

As a data controller or data processor, you need to track access to GDPR systems, which collect, store, transfer, use, and organize data related to EU citizens or residents.

Category	Dashboards	Reports
Access Activity	After Hours Access Activity on GDPR Systems Overview Authorization Changes on GDPR Systems Overview Failed Access Activity on GDPR Systems Overview Failed Access Relationship on GDPR Systems Overview Failed Access Activity by GDPR Asset Failed Access Activity on GDPR Systems by User	After Hours Access Activity on GDPR Systems Summary Authorization Changes Summary on GDPR Systems Failed Access Activity by GDPR Assets Failed Access Activity on GDPR Systems Summary Failed Access Activity on GDPR Systems by Users
Regulatory Exposure	n/a	Potential Regulatory Exposure on GDPR Systems
Threat User Analysis	n/a	Admin Activity from Compromised GDPR System Anti-Virus Disabled on GDPR Systems Summary Audit Log Cleared on GDPR Systems Summary Threats Executed against GDPR Systems Summary

Access Activity

Select **Reports** > **Portal > Repository** > **Standard Content** > **GDPR** > *Reports* or *Dashboards* > **GDPR Access Activity** > **Access Activity**.

To comply with GDPR, you might want to track accounts that have been accessing systems that store or process users' personal data. A high number of failed access attempts can indicate malicious activity. Also, to prevent a malicious user from accessing sensitive data, you should know when and what type of authorization changes occur on those systems.

After Hours Access Activity on GDPR Systems Summary

Reports the number of times and the accounts that accessed GDPR systems outside of regular hours, such as accessing a server on the weekend. The table provides results by the account and its associated server, and the target server accessed. This report relates to GDPR Articles 5 and 25 and Recital 49.

By default, the report uses the following time ranges to check for "after hours" access:

- 12 a.m. to 7 a.m. Monday through Friday
- 18 p.m. (6 p.m.) to 12 a.m. Monday through Friday
- All day on Saturday and Sunday

However, you can modify the time ranges by editing the filters for the report. The time range uses 24-hour values.

Authorization Changes Summary on GDPR Systems

Reports the number and type of authorization change events that occur on GDPR systems over time. The table provides results by the number of times each account made a change, the type of change, the affected GDPR system, and the outcome of the change such as 'success.' This report relates to GDPR Articles 5, 18, 24, 29, and 32 and Recital 39.

Authorization Changes Summary on GDPR Systems

Reports the number and type of authorization change events that occur on GDPR systems over time. The table provides results by the number of times each account made a change, the type of change, the affected GDPR system, and the outcome of the change such as 'success.' This report relates to GDPR Articles 5, 18, 24, 29, and 32 and Recital 39.

Failed Access Activity by GDPR Assets

Reports the number of times access to a GDPR asset failed. The chart shows the top GDPR assets with failed access attempts. For each GDPR asset, the table provides results by the number of failed events, user accounts with failed attempts, and the number of IP addresses associated with the failed events. This report relates to GDPR Articles 5 and 25 and Recital 49.

Failed Access Activity on GDPR Systems by Users

Reports the number of times users failed to access a GDPR system. The chart shows the users with the most failed access attempts. The table provides results by number of failed events, GDPR assets affected, and IP addresses associated with the failed events for each user with a failed attempt. This report relates to GDPR Articles 5 and 25 and Recital 49.

Failed Access Activity on GDPR Systems Summary

Reports the number attempts that failed to access a GDPR system over time. For each failed attempt, the table provides results by user account, the account's IP address and country, the target server's IP and host name, and the number of failed events. This report relates to GDPR Articles 5 and 25 and Recital 49.

After Hours Access Activity on GDPR Systems Overview

Provides, in charts and a table, an overview of accounts that access GDPR systems outside of regular hours, such as accessing a server on the weekend. You can view the targeted systems, users, and source IPs that generate the most events. This dashboard relates to GDPR Articles 25, 30, and 32 and Recital 82.

By default, the dashboard uses the following time ranges to check for "after hours" access:

- 12 a.m. to 7 a.m., Monday through Friday
- 18 p.m. to 12 a.m., Monday through Friday
- All day on Saturday and Sunday

Authorization Changes on GDPR Systems Overview

Provides an overview of events that indicate authorization change attempts on GDPR Systems. Relevant to GDPR Articles 5, 18, 24, and 32 and Recital 39.

Failed Access Activity by GDPR Asset

Provides, in charts and a table, an overview of failed access activity on the specified GDPR systems. This dashboard relates to GDPR Articles 5 and 25 and Recital 49.

You must specify at least one IP address, Mac address, or host name in lowercase.

Failed Access Activity on GDPR Systems by User

Provides, in charts and a table, an overview of failed access activity by user. This dashboard relates to GDPR Articles 5 and 25 and Recital 49.

You must specify at least one user account in lowercase.

Failed Access Activity on GDPR Systems Overview

Provides an overview of failed access activity on GDPR systems. This dashboard relates to GDPR Articles 5 and 25 and Recital 49.

Failed Access Relationship on GDPR Systems Overview

Provides an overview of the relationship between source and destination addresses and users on events that indicate a failure login activity on GDPR systems. This dashboard relates to GDPR Articles 5 and 25 and Recital 49.

Regulatory Exposure

Select **Reports** > **Portal > Repository** > **Standard Content** > **GDPR** > *Reports* or *Dashboards* > **GDPR Access Activity** > **Regulatory Exposure**.

As part of your compliance measures, you most likely track access events that might have compromised user data, thus breaching GDPR regulations.

Potential Regulatory Exposure on GDPR Systems

Reports the GDPR systems that might have been exposed to a regulatory infraction due to user access activities. The chart shows the systems with the most events. The table provides results by the event name and time by GDPR system. This report relates to GDPR Article 32 and Recital 49.

Threat User Analysis

Select **Reports** > **Portal > Repository** > **Standard Content** > **GDPR** > *Reports* or *Dashboards* > **GDPR Access Activity** > **Threat User Analysis**.

User activities such as changing authorizations or clearing audit logs often indicate malicious activities or potential vulnerabilities. Run the following reports to check for threat activities on your GDPR systems.

Admin Activity from Compromised GDPR System

Reports events associated with administrative activities that occur on GDPR systems. For example, users are executing commands or changing authorizations. The chart shows activity over time. The table provides results by time, user, affected GDPR asset, activity type, and the number of events. This report relates to GDPR Articles 30 and 32 and Recital 49.

Anti-Virus Disabled on GDPR Systems Summary

Reports how often anti-virus services have been stopped or paused on GDPR systems over time. A malicious user might pause an anti-virus service before running an illegal command or script or downloading or installing malicious programs. The table provides results by time, GDPR system, affected service, and number of events. This report relates to GDPR Article 32 and Recital 49.

Audit Log Cleared on GDPR Systems Summary

Reports the audit log has been cleared on GDPR systems. The chart shows the number of events over time. The table provides results by date, user, and host. This report relates to GDPR Articles 5 and 25 and Recital 49.

Threats Executed against GDPR Systems Summary

Reports how often GDPR systems have been threatened. The chart shows the number of events over time. The table provides results by date, system IP address, threat technique, event name, and number of events. This report relates to GDPR Article 32 and Recital 49.

Admin Activity

Select **Reports** > **Portal > Repository** > **Standard Content** > **GDPR** > *Reports* or *Dashboards* > **GDPR Admin Activity > Provisioning Activity**.

Administrators can create and remove users. These admins might inadvertently or deliberately add users to a system or group, giving users access to sensitive systems and information. Alternatively, a malicious user with access to an admin account might attempt to create users for later access or remove necessary accounts. To comply with GDPR, you should track administrator activities related to user creations, deletions, and group assignments.

Dashboards	Reports
n/a	User Creations on GDPR Environment User Deletions on GDPR Environment Users Added to a Group on GDPR Environment Users Removed from a Group on GDPR Environment

User Creations on GDPR Environment

Reports the number of user accounts created over time and by whom in the GDPR environment. The table provides results by date, created account, user creating the account, and their domains. This report relates to GDPR Articles 5, 6, and 7 and Recitals 78, 82, and 84.

User Deletions on GDPR Environment

Reports the number of user accounts deleted over time and by whom in the GDPR environment. The table provides results by date, the deleted account, user deleting the account, and their domains. This report relates to GDPR Article 17 and Recital 66.

Users Added to a Group on GDPR Environment

Reports the number of user accounts added to groups over time and by whom in the GDPR environment. The table provides results by date, subject, user adding the account, and affected group. This report relates to GDPR Articles 5, 6, 7, and 32 and Recitals 78, 82, and 84.

You must specify the name of a user group in lowercase.

Users Removed from a Group on GDPR Environment

Reports the number of user accounts removed from groups over time and by whom in the GDPR environment. The table provides results by date, subject, user removing the account, and affected group. This report relates to GDPR Articles 17 and 32 and Recital 66.

You must specify the name of a user group in lowercase.

Attack Surface Analysis

Select **Reports** > **Portal > Repository** > **Standard Content** > **GDPR** > *Reports* or *Dashboards* > **GDPR Attack Surface Analysis**.

Each point entry in your environment, which unauthorized users or programs can exploit, increases the environment's attack surface. This package helps you analyze the extent of the environment's vulnerability.

Category	Dashboards	Reports
Attack Surface Identification	High Risk Vulnerabilities on GDPR Systems Information Leakage Vulnerabilities on GDPR Systems Password and Authentication Weaknesses on GDPR Systems SQL Injection Vulnerabilities on GDPR Systems SSL or TLS Vulnerabilities on GDPR Systems Vulnerable GDPR Assets by Vulnerability Type Vulnerabilities on GDPR Systems Overview XSS Vulnerabilities on GDPR Systems	High Risk Vulnerabilities on GDPR Systems Information Leakage Vulnerabilities on GDPR Systems Password and Authentication Weaknesses on GDPR Systems SQL Injection Vulnerabilities on GDPR Systems SSL or TLS Vulnerabilities on GDPR Systems Unpatched GDPR Systems Vulnerability Summary by CVE ID Vulnerability Summary by GDPR Asset Vulnerability Summary on GDPR Systems XSS Vulnerabilities on GDPR Systems
Security Controls Risk Identification	DoS Attacks Against GDPR Systems	DoS Attacks Against GDPR Systems

Attack Surface Identification

Select **Reports** > **Portal > Repository** > **Standard Content** > **GDPR** > *Reports* or *Dashboards* > **GDPR Attack Surface Analysis** > **Attack Surface Identification**.

To prevent data breaches, you need to know how much of your GDPR environment is vulnerable to attack. Use the following dashboards and reports to identify, and thus reduce, your environment's attack surface.

High Risk Vulnerabilities on GDPR Systems Dashboard

Provides an overview of high-risk vulnerabilities reported on GDPR systems. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

High Risk Vulnerabilities on GDPR Systems Report

Reports the high-risk vulnerabilities detected in the GDPR environment. The chart shows the systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Information Leakage Vulnerabilities on GDPR Systems Dashboard

Provides an overview of information leakage vulnerabilities reported on GDPR systems. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Information Leakage Vulnerabilities on GDPR Systems Report

Reports the information leakage vulnerabilities detected in the GDPR environment. The chart shows the systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Password and Authentication Weaknesses on GDPR Systems Dashboard

Provides an overview of password and authentication Weaknesses reported on GDPR systems. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Password and Authentication Weaknesses on GDPR Systems Report

Reports the password and authentication weaknesses detected in the GDPR environment. The chart shows the number of events over time. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

SQL Injection Vulnerabilities on GDPR Systems Dashboard

Provides an overview of SQL Injection vulnerabilities reported on GDPR systems. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

SQL Injection Vulnerabilities on GDPR Systems Report

Reports the SQL injection vulnerabilities detected in the GDPR Environment. The chart shows the systems with the most detected vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

SSL and TLS Vulnerabilities on GDPR Systems Dashboard

Provides an overview of SSL and TLS vulnerabilities reported on GDPR systems. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

SSL or TLS Vulnerabilities on GDPR Systems Report

Reports the SSL and TLS vulnerabilities detected in the GDPR Environment. Malicious users can exploit vulnerabilities in SSL and TLS. For example, the Heartbleed Bug is a known SSL vulnerability. The chart shows the systems with the most detected vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Unpatched GDPR Systems

Reports the GDPR Systems with missing security patches. One of the most common ways to reduce your environment's attack surface is to ensure that all systems have the most recent security patches applied. The chart shows the systems with the most missing security patches. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Vulnerable GDPR Assets by Vulnerability Type

Provides an overview of vulnerabilities reported on GDPR systems by Type. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Vulnerabilities on GDPR Systems Overview

Provides an overview of vulnerabilities reported on GDPR systems. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Vulnerability Summary by CVE ID

Reports the vulnerabilities detected in the GDPR environment by specific CVE ID. The chart shows the number of assets with the specified vulnerability over time. The table provides results by host name, IP address, Mac address, signature ID, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

You must specify a CVE ID.

Vulnerability Summary by GDPR Asset

Reports the vulnerabilities detected on a specific GDPR asset. The chart shows the number of vulnerabilities detected over time. The table provides results by host name, IP address, Mac address, signature ID, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

You must specify one GDPR asset by host name, IP address, or Mac address.

Vulnerability Summary on GDPR Systems

Reports the vulnerabilities detected in the GDPR environment. The chart shows the assets with the most detected vulnerabilities. The table provides results by asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

XSS Vulnerabilities on GDPR Systems Dashboard

Provides an overview of XSS vulnerabilities reported on GDPR systems. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

XSS Vulnerabilities on GDPR Systems Report

Reports the cross-site scripting (XSS) vulnerabilities detected in the GDPR environment. Vulnerabilities associated with 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 chart shows the assets with the most detected vulnerabilities. The table provides results by asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Security Controls Risk Identification

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **GDPR** > *Reports* or *Dashboards* > **GDPR Attack Surface Analysis** > **Security Controls Risk Identification**.

Not all malicious users want to breach your systems to access or manipulate data. Some might want to disrupt service and deny users access to information. However, a denial-of-service (DoS) attack might indicate a future threat to your environment.

DoS Attacks Against GDPR Systems

Reports potential DoS events against databases in the GDPR environment. The chart shows the number of attacks over time. The table provides results by the source IP and port, the target IP and port, name of the event, and number of events. This report relates to GDPR Article 32 and Recital 49.

DoS Attacks Against GDPR Systems

Provides a summary overview of DoS Attacks against GDPR Systems. This dashboard relates to GDPR Article 32 and Recital 49.

Corporate Governance

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **GDPR** > *Reports* or *Dashboards* > **GDPR Corporate Governance** > **Record Keeping**.

In some environments, sensitive data is stored in file cabinets or archives. To ensure compliance with GDPR, your organization might control access to the physical environment

where these records are kept. Use the following dashboards and reports to track access to these environments.

Dashboards	Reports
Access Activity on GDPR Systems Overview	Access Activity on GDPR Systems Summary
Geo Access Activity on GDPR Systems Overview	After Work Hours Physical Access Activity on GDPR Systems Summary
Physical Access Activity on GDPR Systems Overview	Physical Access Activity on GDPR Systems Summary

Access Activity on GDPR Systems Summary

Reports access events to GDPR systems. The chart shows access by country over time. The table provides results by user, source IP and country, target IP and host, and number of events. This report relates to GDPR Articles 30, 32, and 25, and Recital 82.

After Work Hours Physical Access Activity on GDPR Systems Summary

Reports access to physical GDPR systems, such as buildings, during after work hours. The chart shows both failed and successful access by user and building. The table provides results by date, user, building, result, and number of attempts. This report relates to GDPR Articles 24 and 32 and Recital 49.

By default, the report uses the following time ranges to check for "after hours" access:

- 12 a.m. to 7 a.m., Monday through Friday
- 18 p.m. (6 p.m.) to 12 a.m., Monday through Friday
- All day on Saturday and Sunday

However, you can modify the time ranges by editing the filters for the report. The time range uses 24-hour values.

Physical Access Activity on GDPR Systems Summary

Reports access to physical GDPR systems, such as building. The chart shows both failed and successful access by building over time. The table provides results by date, user, building, result, and number of attempts. This report relates to GDPR Articles 24 and 32 and Recital 49.

Access Activity on GDPR Systems Overview

Provides an overview of access events reported on GDPR systems. This dashboard relates to GDPR Articles 30, 32, and 25 and Recital 82.

Geo Access Activity on GDPR Systems Overview

Provides an overview of GEO access activity to GDPR systems. This dashboard relates to GDPR Articles 30, 32, and 25 and Recital 82.

Physical Access Activity on GDPR Systems Overview

Provides an overview of physical access events reported on GDPR systems, by default "after Work Hours" charts defined from 12 a.m. to 7 a.m. and 18 p.m. to 12 a.m every Monday to Friday and the whole days of Saturday and Sunday, those can be re-configured to different values using this dashboard charts components filter. This dashboard relates to GDPR Articles 24 and 32 and Recital 49.

Regulatory Exposure

Select **Reports** > **Portal > Repository** > **Standard Content** > **GDPR** > *Reports* or *Dashboards* > **GDPR Regulatory Exposure** > **Composite Regulatory Exposure**.

To comply with GDPR, you might need to track how data flows among GDPR system, and from systems in non-EU countries.

Dashboards	Reports
Data Flow from GDPR Systems	Data Flow from GDPR Systems Summary
Data Flow from GDPR Systems to non EU	Data Flow from GDPR Systems to non EU Summary
Data Flow from non EU to GDPR Systems	Data Flow from non EU to GDPR Systems Summary
Data Flow to GDPR Systems	Data Flow to GDPR Systems Summary
GDPR Systems Communication with non EU Countries	High Risk Events on GDPR Systems Summary
GDPR Systems Communication Overview	Policy Violations on GDPR Systems Summary
High Risk Events on GDPR Systems Overview	Threats on GDPR Systems Summary
Policy Violations on GDPR Systems Overview	
Threat Relationship on GDPR Systems Overview	
Threats on GDPR Systems Overview	

Data Flow from GDPR Systems

Provides a summary overview of data flow from GDPR Systems. This dashboard relates to GDPR Articles 30, 46, 32, 45, 46, and 49 and Recital 82.

Data Flow from GDPR Systems Summary

Reports events that detect the flow of data from GDPR systems. The chart shows the GDPR systems with the most data flowing outward. The table provides results by the IP address of the GDPR source system, the target IP address and host, and the number of events detected. This report relates to GDPR Articles 30, 32, 45, 46, and 49 and Recital 82.

Data Flow from GDPR Systems to non EU

Provides a summary overview of data flow from non EU to GDPR Systems. This dashboard relates to GDPR Articles 30, 46, 32, 45, 46, and 49 and Recital 82.

Data Flow from GDPR Systems to non EU Summary

Reports events that detect the flow of data from GDPR systems to systems in non-European Union countries. The chart shows the GDPR systems with the most data flowing outward by country. The table provides results by the IP address of the GDPR source system, the IP address of the non-EU system, the country code of the target system, and the number of events detected. This report relates to GDPR Articles 30, 32, 45, 46, and 49 and Recital 82.

Data Flow from non EU to GDPR Systems

Provides a summary overview of data flow from non EU to GDPR Systems. This dashboard relates to GDPR Articles 30, 46, 32, 45, 46, and 49 and Recital 82.

Data Flow from non EU to GDPR Systems Summary

Reports events that detect the flow of data to GDPR systems from systems in non-European Union countries. The chart shows the GDPR systems with the most data flowing in by country of origin. The table provides results by the IP address and country code of the source system, the IP address of the GDPR system, and the number of events detected. This report relates to GDPR Articles 30, 32, 45, 46, and 49 and Recital 82.

Data Flow to GDPR Systems

Provides a summary overview of data flow to GDPR Systems. This dashboard relates to GDPR Articles 30, 46, 32, 45, 46, and 49 and Recital 82.

Data Flow to GDPR Systems Summary

Reports events that detect the flow of data to GDPR systems. The chart shows the GDPR systems with the most data flowing into them. The table provides results by the IP address of the source system, the target (GDPR system) IP address and host, and the number of events detected. This report relates to GDPR Articles 30, 32, 45, 46, and 49 and Recital 82.

GDPR Systems Communication Overview

Provides an overview of GDPR Systems communications. This dashboard relates to GDPR Articles 30, 46, 32, 45, 46, and 49 and Recital 82.

GDPR Systems Communication with non EU Countries

Provides an overview of GDPR Systems communications with non EU Countries. This dashboard relates to GDPR Articles 30, 46, 32, 45, 46, and 49 and Recital 82.

High Risk Events on GDPR Systems Overview

Provides an overview of high risk events related to GDPR systems. This dashboard relates to GDPR Article 32 and Recital 49.

High Risk Events on GDPR Systems Summary

Reports high-risk events that involve GDPR systems. The chart shows the targeted GDPR systems with the most high-risk events. The table provides results by the source IP and host of the events, the targeted IP and host GDPR system, the user, and number of events detected. This report relates to GDPR Articles 32 and 83 and Recital 49.

Policy Violations on GDPR Systems Overview

Provides an overview of policy violation events related to GDPR systems. This dashboard relates to GDPR Articles 32 and 83 and Recital 49.

Policy Violations on GDPR Systems Summary

Reports the number of policy violation events on GDPR systems over time. The table provides results by source IP address, the IP address and host of the target GDPR system, user, and number of events. This report relates to GDPR Articles 32 and 83 and Recital 49.

Threat Relationship on GDPR Systems Overview

Provides an overview of relationship between source and destination addresses on events which indicate compromise, reconnaissance, hostile, or suspicious activity on GDPR systems. This dashboard relates to GDPR Article 32 and Recital 49.

Threats on GDPR Systems Overview

Provides an overview of events that indicate compromise, reconnaissance, hostile, or suspicious activity on GDPR systems. This dashboard relates to GDPR Article 32 and Recital 49.

Threats on GDPR Systems Summary

Reports the number of events that indicate compromise, reconnaissance, hostile, or suspicious activity on GDPR systems over time. The table provides results by IP and Mac address of the source system, the IP address and host of the target GDPR system, user, and number of events. This report relates to GDPR Articles 32 and Recital 49.

Threat Analysis

Select **Reports** > **Portal > Repository** > **Standard Content** > **GDPR** > *Reports* or *Dashboards* > **GDPR Threat Analysis**.

GDPR requires that your enterprise establish technical and organizational standards that ensure appropriate security-to-risk levels. To create appropriate security measures, you need to assess the risks and the severity of threats to sensitive data.

- "Select Reports > Portal > Repository > Standard Content > GDPR > Reports or Dashboards > GDPR Threat Analysis > Data Store Risk." below
- "Select Reports > Portal > Repository > Standard Content > GDPR > Reports or Dashboards > GDPR Threat Analysis > Internet Threat Analysis." on page 147

Threat Analysis - Data Store Risk

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **GDPR** > *Reports* or *Dashboards* > **GDPR Threat Analysis** > **Data Store Risk**.

As part of your threat analysis, you should assess the vulnerability of data storage systems.

Dashboards	Reports
n/a	Attacks Against Databases on GDPR Systems Cassandra Vulnerabilities on GDPR Systems CRM and ERP Vulnerabilities on GDPR Systems Database Configuration Changes on GDPR Systems Database Weaknesses on GDPR Systems Elasticsearch Vulnerabilities on GDPR Systems IBM Db2 Vulnerabilities on GDPR Systems MariaDB Vulnerabilities on GDPR Systems Microsoft SQL Server Vulnerabilities on GDPR Systems MongoDB Vulnerabilities on GDPR Systems MySQL Vulnerabilities on GDPR Systems Oracle Vulnerabilities on GDPR Systems PostgreSQL Vulnerabilities on GDPR Systems Redis Vulnerabilities on GDPR Systems

Attacks Against Databases on GDPR System

Reports events that indicate compromise, reconnaissance, hostile, or suspicious activity against GDPR systems databases over time. The table provides results by the source GDPR IP address, IP address and host of the target system, name of the event, and number of events. This report relates to GDPR Article 32 and Recital 49.

Cassandra Vulnerabilities on GDPR Systems

Reports vulnerabilities related to Apache Cassandra on GDPR systems. Apache Cassandra is a free and open-source, distributed, wide-column store, NoSQL database management system. The chart shows the GDPRs reporting the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date

of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

CRM and ERP Vulnerabilities on GDPR Systems

Reports vulnerabilities detected on GDPR systems related to CRM (Customer Relationship Management) and ERP (Enterprise Resource Planning) software. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Database Configuration Changes on GDPR Systems

Reports changes to the database configuration in the GDPR environment. The chart shows the GDPR systems with the most changes. The table provides results by host system, database change, the type of change, agent severity, and date of the most recent event. This report relates to GDPR Article 32.

Database Weaknesses on GDPR Systems

Reports vulnerabilities in databases detected in the GDPR environment over time and by severity. The table provides results by GDPR asset, signature ID, description of the vulnerability, agent severity, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Elasticsearch Vulnerabilities on GDPR Systems

Reports vulnerabilities related to Elasticsearch on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

IBM Db2 Vulnerabilities on GDPR Systems

Reports vulnerabilities related to IBM Db2 on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

MariaDB Vulnerabilities on GDPR Systems

Reports vulnerabilities related to MariaDB on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Microsoft SQL Server Vulnerabilities on GDPR Systems

Reports vulnerabilities related to Microsoft SQL Server on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

MongoDB Vulnerabilities on GDPR Systems

Reports vulnerabilities related to MongoDB on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

MySQL Vulnerabilities on GDPR Systems

Reports vulnerabilities related to MySQL on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Oracle Vulnerabilities on GDPR Systems

Reports vulnerabilities related to Oracle on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

PostgreSQL Vulnerabilities on GDPR Systems

Reports vulnerabilities related to PostgreSQL on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Redis Vulnerabilities on GDPR Systems

Reports vulnerabilities related to Redis on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Threat Analysis - Internet

Select **Reports** > **Portal > Repository** > **Standard Content** > **GDPR** > *Reports* or *Dashboards* > **GDPR Threat Analysis** > **Internet Threat Analysis**.

As part of your threat analysis, you should assess the vulnerability of firewalls, places where information might leak, and existence of malware on your GDPR systems.

Dashboards	Reports
Malware Found on GDPR Systems MITRE ATT&CK on GDPR Systems by GDPR Asset MITRE ATT&CK on GDPR Systems by MITRE ID MITRE ATT&CK on GDPR Systems Overview MITRE ATT&CK Relationship on GDPR Systems Overview	Firewall Blocked Events in GDPR Environment Information Leaks from GDPR Systems Malware Found on GDPR Systems

Firewall Blocked Events in GDPR Environment

Reports firewall blocked events in the GDPR environment. The chart shows the number of events by time and target port. If you pro-actively monitor the firewalls in your enterprise, you can identify problems at an early stage and prevent network attacks. The table provides results by source IP address and port, the targeted GDPR IP address and port, and the number of events. This report relates to GDPR Article 32 and Recital 49.

Information Leaks from GDPR Systems

Reports events that indicate information leaks on GDPR systems over time. The table provides results by date, event name, source IP address and port, the targeted GDPR IP address and port, and the user. This report relates to GDPR Articles 32, 33, and 34 and Recitals 49, 85, and 86.

Malware Found on GDPR Systems Dashboard

Provides an overview of malware reported events on GDPR Systems. This dashboard relates to GDPR Articles 32, 33, and 34 and Recitals 49 and 83.

Malware Found on GDPR Systems Report

Reports malware found on GDPR systems. The chart shows the systems with the most malware activity. The table provides results by GDPR asset, malware program, name of the event, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

MITRE ATT&CK on GDPR Systems by GDPR Asset

Provides an overview of MITRE ATT&CK events by GDPR asset. This dashboard relates to GDPR Article 32 and Recital 49.

MITRE ATT&CK on GDPR Systems by MITRE ID

Provides an overview of MITRE ATT&CK events reported on GDPR Systems by MITRE IDs. This dashboard relates to GDPR Article 32 and Recital 49.

MITRE ATT&CK on GDPR Systems Overview

Provides an overview of MITRE ATT&CK events reported on GDPR Systems. This dashboard relates to GDPR Article 32 and Recital 49.

MITRE ATT&CK Relationship on GDPR Systems Overview

Provides an overview of the relationship between different event entities on MITRE ATT&CK events reported on GDPR systems. This dashboard relates to GDPR Article 32 and Recital 49.

Ensuring Compliance with IT Governance

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **IT GOV** > **ISO-27002**.

To comply with the information security management controls as part of ISO 27002 guidelines, your enterprise needs to establish and follow information security standards and policies. The guidelines help you identify and implement the controls needed to secure data. You can check the security controls in your enterprise against one or more specific ISO 27002 control set, such as *Information Security Policies or Asset Management*.

We provide the **Compliance Pack for IT Governance** to help you comply with Controls 6, 8, 9, 10, 12, 13, 14, 16, and 17. For more information about adding the pack to the Reports repository, see the *Solutions Guide for ArcSight Compliance Pack for IT Governance*.

This package includes dashboards and reports organized by the ISO-27002 requirements:

Category	Dashboards	Reports
"IT Governance – Executive Overview" on page 153	"Overall Risk Management" on page 153	n/a
"6 – Organization of Information Security" on page 154	n/a	"Suspicious Activity in Wireless Network" on page 154
"8 – Asset Management" on page 154	n/a	"Network Active Assets" on page 155 "New Hosts" on page 155 "New Services" on page 155

Category	Dashboards	Reports
"9 – Access Control" on page 155	"User Account Management" on page 157	"Account Lockouts by User" on page 156 "All Login Activity" on page 156 "Authentication with Null Sessions" on page 156 "Authorization Changes" on page 156 "Privileged Account Changes" on page 156 "Removal of Access Rights" on page 156 "Successful Brute Force Logins" on page 156 "Unauthorized User Access to Network Domain" on page 156 "User Account Creation" on page 157 "User Account Deletion" on page 157
"10 – Cryptography" on page 157	n/a	"Insecure Cryptographic Storage" on page 158 "Invalid Certificates" on page 158 "Systems Providing Unencrypted Services" on page 158

Category	Dashboards	Reports
"12 – Operations Security" on page 158	"Authentication Errors" on page 162 "Database Events" on page 162 "Events and Incidents that have Occurred" on page 163 "Malware Activity" on page 164 "Scans Overview" on page 165 "Vulnerabilities Management" on page 167 "Vulnerability Scans and Unauthorized Access" on page 167	"Account Activity Summary" on page 161 "Administrative Actions Events" on page 161 "Administrative Logins and Logouts" on page 161 "Application Configuration Modification" on page 161 "Audit Log Cleared" on page 161 "Authentication Logins with Insecure Ports" on page 161 "Blocked Firewall Traffic" on page 162 "Changes to Operating System" on page 162 "Covert Channel Activity" on page 162 "Device Configuration Changes" on page 162 "Device Logging Review" on page 162 "Exploit of Vulnerabilities" on page 163 "Failed Administrative User Logins" on page 163 "Failed Antivirus Updates" on page 163 "Failed File Access" on page 163 "Failed File Deletions" on page 163 "Failed User Logins" on page 163 "Fault Logs" on page 164 "File Changes in Production" on page 164 "Firewall Configuration Changes" on page 164 "Logins to Database Machines" on page 164 "Machines Conducting Policy Breaches" on page 164

Category	Dashboards	Reports
		"Malicious Code Sources" on page 164 "Network Device Configuration Changes" on page 165 "Policy Violations" on page 165 "Resource Exhaustion" on page 165 "Software Changes in Production" on page 165 "Successful Administrative User Logins" on page 165 "Successful File Deletions" on page 166 "Successful User Logins" on page 166 "Suspicious Activity" on page 166 "Trojan Code Activity" on page 166 "User Actions All Events" on page 166 "User Logins and Logouts" on page 166 "Virus Infected Machines" on page 166 "Vulnerabilities Scanner Results" on page 167
"13 – Communications Security" on page 167	"Email Activities" on page 168 "Peer to Peer Activity" on page 169 "Phishing Activities" on page 169	"Accessed Ports through Firewall" on page 168 "Firewall Open Port Review" on page 168 "Information Interception Events" on page 168 "Insecure Services" on page 168 "Interzone Traffic" on page 168 "Organizational Information Leaks" on page 168 "Personal Information Leaks" on page 169 "Processes by Asset" on page 169

Category	Dashboards	Reports
"14 – System Acquisition, Development, and Maintenance" on page 169	n/a	"Invalid Data Input" on page 170
"16 – Information Security Incident Management" on page 170	"Internal Reconnaissance" on page 171	"Confidential Breach Sources" on page 170 "Denial of Service" on page 170 "File Integrity Changes" on page 171 "Information Systems Failures" on page 171 "Integrity Breach Sources" on page 171 "Internal Reconnaissance by Event" on page 171 "Internal Reconnaissance by Source Address" on page 171 "Internal Reconnaissance by Target Address" on page 172
"17 – Information Security Aspects of Business Continuity Management" on page 172	n/a	"Availability Attacks" on page 172

IT Governance – Executive Overview

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **IT GOV** > **ISO-27002** > **Dashboards** > **Overview**.

To help individuals in management and C-suite positions to quickly understand the current state of your enterprise's compliance with ISO-27002 controls, you can view the following dashboard:

Dashboards	Reports
"Overall Risk Management" below	n/a

Overall Risk Management

Provides, in charts, the overall risk score of your IT environment. You can view the most assets at highest risk, risk score by ISO control, and the rules triggered by an ISO control.

6 – Organization of Information Security

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **IT GOV** > **ISO-27002 > Reports** > **ISO 6 – Organization of Information Security**.

Control 6: *Organization of information security* of the ISO 27002 standard focuses on ensuring that your organization supports and maintains information security operations, both on- and off-site.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
n/a	"Suspicious Activity in Wireless Network" below

Suspicious Activity in Wireless Network

Reports events that indicate suspicious activity in the wireless network. For example, a malicious user might scan ports to discover open doors or weak points in the wireless network. The table provides results by the type of suspicious activity, details about the target and source systems, and the number of events.

In the logical model, use the **iDestinationWirelessNetwork** variable to specify wireless networks. For more information, see the *Solutions Guide for ArcSight Compliance Pack for IT Governance*.

8 – Asset Management

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **IT GOV** > **ISO-27002** > **Reports** > **ISO 8 – Asset Management**.

Control 8: *Asset Management* of the ISO 27002 standard focuses on identifying the physical and information assets in your enterprise, and determining the appropriate level of protection necessary for each.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
n/a	"Network Active Assets" on the next page "New Hosts" on the next page "New Services" on the next page

Network Active Assets

Reports all hosts that have been included as the source address in logged events. The table provides results by the source IP address, user, and zone; the number of events; and when the event occurred.

New Hosts

Reports all new hosts on the network detected by traffic analysis systems. The table provides results by the host name, IP address, and zone of the target system and when the event occurred.

New Services

Reports all new services on the network detected by traffic analysis systems. The table provides results by the service name, IP address, and host name; the port used, the number of events, and when the most recent event occurred.

9 – Access Control

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **IT GOV** > **ISO-27002** > *Dashboards* or *Reports* > **ISO 9 – Access Control**.

Control 9: *Access Control* of the ISO 27002 standard focuses on preventing unauthorized user access to information and the facilities that process information.

To assess your enterprise's compliance with this requirement, use the following dashboard and reports:

Dashboards	Reports
"User Account Management" on page 157	"Account Lockouts by User" on the next page "All Login Activity" on the next page "Authentication with Null Sessions" on the next page "Authorization Changes" on the next page "Privileged Account Changes" on the next page "Removal of Access Rights" on the next page "Successful Brute Force Logins" on the next page "Unauthorized User Access to Network Domain" on the next page "User Account Creation" on page 157 "User Account Deletion" on page 157

Account Lockouts by User

Reports the accounts most often locked out. The table provides results about the locked out user, the target IP address and host name, the number of event, and when the most recent event occurred.

All Login Activity

Reports all successful, failed, and attended login activity by all users in the network. The table provides results by the IP address and name of the target system, the source IP address, the user involved, the outcome of the login attempt, the number of attempts, and when the most recent attempt occurred.

Authentication with Null Sessions

Reports possible null authentication sessions where the outcome is successful, failed, or an attempt. A null session attack exploits an authentication vulnerability for Windows Administrative Shares where a malicious user connects to a local or remote share without authentication. The table provides results by the target IP address and user, the source IP address and user, the outcome of the authentication attempt, the number of attempts, and when the most recent attempt occurred.

Authorization Changes

Reports authorization changes made on systems and the number of events per host. The table provides results by the target zone, IP address, and user; the source user, the type of event, the number of attempts, and when the most recent attempt occurred.

Privileged Account Changes

Reports all changes made to privileged accounts, such as password changes. The table provides results by the event, the name and IP address of the user who made the change, and when the change occurred.

Removal of Access Rights

Reports the access rights removed from user accounts. The table provides results by the access right that was removed, the IP address and host where the change was made, the user who made the change, the number of changes, and when the change occurred.

Successful Brute Force Logins

Reports the details of successful brute force logins. The table provides results by the user logging in, the IP address and host affected, the number of logins and when the event occurred.

Unauthorized User Access to Network Domain

Reports login sessions where the user is unauthorized for the specific network domain. The table provides results by the user attempted access, the target IP address and host, the source IP address for the user, the outcome of the attempt, the number of attempts, and when the event occurred.

To specify authorized users and network domains, update the variables **isDestinationAuthorizeUser** and **isNetworkDomain**. For more information, see the *Solutions Guide for ArcSight Compliance Pack for IT Governance*.

User Account Creation

Reports all events that indicate a user account has been added to a system. The table provides results by the IP address and host where the event occurred, the user adding accounts, the number of events, and when the event occurred.

User Account Deletion

Reports all events that indicate a user account has been removed from a system. The table provides results by the IP address and host where the event occurred, the user removing accounts, the number of events, and when the event occurred.

User Account Management

Provides, in charts, details of scans, probes, and unauthorized access. You can view the number of accounts created and deleted by the user making the change, as well as the hosts that have been added or deleted.

10 – Cryptography

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **IT GOV** > **ISO-27002** > **Reports** > **ISO 10 – Cryptography**.

Control 10: *Cryptography* of the ISO 27002 standard focuses on using cryptographic keys to protect the confidentiality, integrity, and availability of information.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
n/a	"Insecure Cryptographic Storage" on the next page "Invalid Certificates" on the next page "Systems Providing Unencrypted Services" on the next page

Insecure Cryptographic Storage

Reports vulnerabilities associated with insecure cryptographic storage detected on your systems. The table provides results by IP address and name of the asset, the detected vulnerability, and when the most recent event occurred.

Invalid Certificates

Reports events that indicate an error with a server's certificate. The chart displays the number of such occurrences per host. The table provides results by the name of the event, the IP address and host name of the server, the user associated with event, the number of events, and when the event occurred.

Systems Providing Unencrypted Services

Reports the systems that provide unencrypted services. The table provides results by the port, process, service, IP address of the system, and the number of events.

12 – Operations Security

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **IT GOV** > **ISO-27002** > *Dashboards or Reports* > **ISO 12 – Operations Security**.

Control 12: *Operations security* of the ISO 27002 standard focuses on ensuring that the facilities that store and process information are protected from malware, data loss, and the exploitation of technical vulnerabilities. Use the following reports to check for compliance with the standard.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports

"Authentication Errors" on page 162
"Database Events" on page 162
"Events and Incidents that have Occurred" on page 163
"Malware Activity" on page 164
"Scans Overview" on page 165
"Vulnerabilities Management" on page 167
"Vulnerability Scans and Unauthorized Access" on page 167
"Account Activity Summary" on the next page
"Administrative Actions Events" on the next page
"Administrative Logins and Logouts" on the next page
"Application Configuration Modification" on the next page
"Audit Log Cleared" on the next page
"Authentication Logins with Insecure Ports" on the next page
"Blocked Firewall Traffic" on page 162
"Changes to Operating System" on page 162
"Covert Channel Activity" on page 162
"Device Configuration Changes" on page 162
"Device Logging Review" on page 162
"Exploit of Vulnerabilities" on page 163
"Failed Administrative User Logins" on page 163
"Failed Antivirus Updates" on page 163
"Failed File Access" on page 163
"Failed File Deletions" on page 163
"Failed User Logins" on page 163
"Fault Logs" on page 164
"File Changes in Production" on page 164
"Firewall Configuration Changes" on page 164
"Logins to Database Machines" on page 164
"Machines Conducting Policy Breaches" on page 164
"Malicious Code Sources" on page 164
"Network Device Configuration Changes" on page 165
"Policy Violations" on page 165
"Resource Exhaustion" on page 165
"Software Changes in Production" on page 165
"Successful Administrative User Logins" on page 165
"Successful File Deletions" on page 166
"Successful User Logins" on page 166
"Suspicious Activity" on page 166

	"Trojan Code Activity" on page 166 "User Actions All Events" on page 166 "User Logins and Logouts" on page 166 "Virus Infected Machines" on page 166 "Vulnerabilities Scanner Results" on page 167

Account Activity Summary

Reports all account activities by type. The table provides results by the event name, the user associated with the event, the target IP address and host name, and number of events per user.

Administrative Actions Events

Reports the accounts that have performed the most administrative actions. The table provides results by admin account, destination IP address, the name and ID of the detected event, the affected product, the number of events, and when the most recent event occurred.

Administrative Logins and Logouts

Reports the hosts that have had the highest number of logins and logouts by administrative accounts. The table provides results by the name of the event, the admin account, the IP address and name of the affected host, the action taken, the number of events, and when most recent event occurred.

Application Configuration Modification

Reports the applications that have had the highest number of configuration changes. For example, a user might have updated a license file or a program setting. The table provides results by the product modified, the IP address and zone of the host system, and the date that the modification occurred.

Audit Log Cleared

Reports the indication that audit logs have been cleared over time. The table provides results by when the event occurred, the IP address and host of the affected system, the affected account, the source account that might have cleared the audit log, and the affected device.

Authentication Logins with Insecure Ports

Reports assets with authenticated logins that used insecure ports. This report is useful for auditors to track and identify assets that are not following the security standard. The table

provides results by the insecure port, the name of the source and target systems, the target user (if any), the type of event or user, the number of events, and the date of the most recent event.

Authentication Errors

Provides an overview of the authentication failure events in your enterprise. You can view a trend of failed authentication events over time, the different outcomes of the authentication events, and the failed logins by administrative and non-administrative users.

Blocked Firewall Traffic

Reports events generated by devices that have blocked traffic. The table provides results by the target port, the source and target IP address and host name, the type of event, and number of events.

Changes to Operating System

Reports the hosts with the most changes to the operating system. Detected modifications might be to the security options or OS accounts. The table provides results by the change made; the IP address, name, and zone of the affected host system; and the device product that was changed.

Covert Channel Activity

Reports events identified as covert channel activity. These events are generated by IDS devices and could indicate the use of different tools designed to establish an undetected channel to and from your enterprise. The table provides results by the type of event, the IP address and host name of the target and source systems, and when the event occurred.

Database Events

Provides, in charts and a table, an overview of the database events. You can view the trend of events over time, events by product, by the behavior of each event, and user names, IPs involved in the events. The table lists the name of the event; the target user and associated IP address; the source user and associated IP address; the outcome of the event; and the number of events.

Device Configuration Changes

Reports the type and number of modifications made to devices in the network. The table provides results by the date, time, event name, affected product, and the host where the changes occurred.

Device Logging Review

Reports the devices with the most logging events, such as a database. The table provides results by the device host name and address, a count of events received, and when the

device most recently received an event.

Because this report queries the logging activity from all devices, it will have a performance impact each time that you run it.

Events and Incidents that have Occurred

Provides, in charts, an overview of the different security incidents that might indicate that systems or data in your enterprise have been compromised. You can view a trend of events by severity over time, as well as events by geographic location, the techniques used, severity, source IP address, and target IP address. You can also review the relationships between target and source IP addresses.

Exploit of Vulnerabilities

Reports the number of detected events where a user might have exploited a well-known vulnerability. For example, an IDS might report an event associated with a Unicode vulnerability. The table provides results by the vulnerability, the affected host, the source system, and the number of detected events.

Failed Administrative User Logins

Reports the number of failed logins by administrative accounts over time. A high number of failed access attempts can indicate malicious activity. The table provides results by account name, the name and IP address of the host where the login failed, the affected product or operating system, the number of failures detected, and when the most recent event occurred.

Failed Antivirus Updates

Reports number of failures in updating anti-virus software over time. The table provides results by the update that failed; the IP address, name, and zone of the target system; the type of event, and when the failure occurred.

Failed File Access

Reports the details of events that indicate failed attempts to access files. The table provides results by the targeted file, the IP address and name of the target system, the type of event, the number of attempts, and when the most recent attempt occurred.

Failed File Deletions

Reports information about files that failed to be deleted. The table provides results by the targeted file, the IP address and name of the target system, the type of event, the number of attempts, and when the most recent attempt occurred.

Failed User Logins

Reports the number of failed logins over time. A high number of failed access attempts can indicate malicious activity. The table provides results by account name, the name and IP address of the host where the login failed, the affected product or operating system, the number of failures detected, and when the most recent event occurred.

Fault Logs

Reports all events indicating that a system fault has occurred over time. The table provides results by the IP address and name of the host where the fault occurred, the name of the event, the number of events, and when the most recent event occurred.

File Changes in Production

Reports changes made to files in the production network. The table provides results by the target file, the IP address and name of the host of the file, the number of events, and when the most recent event occurred.

Before using this report, you must add the systems that reside in the production network to the variable **isProductionNetwork**. For more information, see the *Solutions Guide for ArcSight Compliance Pack for IT Governance*.

Firewall Configuration Changes

Reports events by host that indicate changes to firewall configuration. The table provides results by the IP address and zone of the firewall, the firewall rule and configuration that was changed, the number of changes, and the time that the event occurred.

Logins to Database Machines

Reports the user accounts with the most attempts to log in to databases in your environment. The table provides results by the user account, the affected host, the number of attempts, whether the attempt was successful, and events per hour.

Machines Conducting Policy Breaches

Reports policy breaches by system, where the event matches the category technique of `/Policy/Breach`. The table provides results by the device group, affected vendor and product, the IP address and name of the host, and when the breach occurred.

Malicious Code Sources

Reports malicious code events by host system. The table provides results by the event name, the IP address and name of the affected device, the affected product, the category of the malicious code, and the outcome.

Malware Activity

Provides, in charts, an overview of the malware events that might indicate systems or data in your enterprise have been compromised. You can view a trend of malware events over

time, as well as events by geographic location, malware category and malicious event, the affected IP addresses and hosts, suspicious IP addresses and hosts names, and target IP addresses. You can also review the relationships between target and source IP addresses. You can also review the techniques used to exploit and launch further attacks.

Network Device Configuration Changes

Reports events that indicate configuration file changes on network equipment such as routers and switches. The table provides results by the change made, the device affected, the IP address where the change originated, the IP address and name of the host where the change occurred, and when the change occurred.

Policy Violations

Reports all policy breaches by source IP address. A policy breach could be IM use or the downloading of unauthorized content. The table provides results by the affected policy, the IP address and name of the source and target hosts, the number of breaches, and when the most recent breach occurred.

Resource Exhaustion

Reports events that indicate resource exhaustion on particular hosts. A malicious user can create or exploit resource exhaustion vulnerabilities by causing the programs to crash or falter, or by interfering with the programs such that the programs do not have enough resources to perform properly. If this occurs, the systems and programs become unavailable for use. The table provides results by the IP address and name of the host where the event occurred, the type of event, the number of events, and when the most recent event occurred.

Scans Overview

Provides an overview of scan results. You can view the signatures of potential vulnerabilities, the most active scanners, and the most scanned ports and assets.

Software Changes in Production

Reports events that indicate changes to daemons, access policies, and other software changes in the production environment. The table provides results by the event, the IP address and name of the target asset, and the target user.

Before using this report, you must add the systems that reside in the production network to the variable **isProductionNetwork**. For more information, see the *Solutions Guide for ArcSight Compliance Pack for IT Governance*.

Successful Administrative User Logins

Reports the number of successful logins by administrative accounts over time. The table provides results by account name, the name and IP address of the host where the logins

occurred, the affected product or operating system, the number of successful logins, and the date of the most recent event.

Successful File Deletions

Reports events that indicate successful attempts to delete files by the target IP address. The table provides results by name of the deleted file, the IP address where the file was deleted, the number of files deleted, and when the deletion occurred.

Successful User Logins

Reports the number of successful logins over time. The table provides results by account name, the name and IP address of the host where the logins occurred, the affected product or operating system, the number of successful logins, and when the most recent event occurred.

Suspicious Activity

Reports suspicious events in your network. The table provides results by the event name, the IP address and name of the host where the event occurred, the number of events, and when the most recent event occurred.

Trojan Code Activity

Reports all the trojan activity detected by IP address in the environment. The table provides results by the type of activity, the IP address that originated the activity, the IP address and name of the target host, and when the event occurred.

User Actions All Events

Reports the actions taken by non-administrative accounts. For example, a user might delete an infected file. The report provides results by the source account, the affected account, the name of the event, the IP address where the action occurred, the affected product, the outcome of the user's action, the number of times that the action was detected, and the date of the most recent event.

Run this report with caution, as it can generate enormous amounts of data. This report will not include events in which both source and destination users are null.

User Logins and Logouts

Reports the user accounts that log in and out the most. The table provides results by the name of the login action and category, the user account, the IP address, name, zone of the affected system, and the date of the event.

Virus Infected Machines

Reports the systems with the most detected viruses by affected product. The table provides results by the virus name, the affected system and product, and the date of the event.

Vulnerabilities Management

Provides an overview of the vulnerabilities detected per host. You can view a trend of vulnerabilities reported over time, the most reported vulnerabilities, the assets with the most vulnerabilities, and vulnerabilities by severity.

Vulnerabilities Scanner Results

Reports vulnerabilities by type as detected by vulnerability scanners. The table provides results by the vulnerability, the IP address and name of the affected host, and the quantity found.

Vulnerability Scans and Unauthorized Access

Provides an overview of the scans, probes, and unauthorized access reported in your environment. You can view results by the systems with the most unauthorized access attempts, severity of events, the most scanned ports, the vulnerabilities scanned, and the signature of the riskiest vulnerabilities.

13 – Communications Security

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **IT GOV** > **ISO-27002** > *Dashboards* or *Reports* > **ISO 13 – Communications Security**.

Control 13: *Communications Security* of the ISO 27002 standard focuses on using cryptographic keys to protect the confidentiality, integrity, and availability of information.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
"Email Activities" on the next page "Peer to Peer Activity" on page 169 "Phishing Activities" on page 169	"Accessed Ports through Firewall" on the next page "Firewall Open Port Review" on the next page "Information Interception Events" on the next page "Insecure Services" on the next page "Interzone Traffic" on the next page "Organizational Information Leaks" on the next page "Personal Information Leaks" on page 169 "Processes by Asset" on page 169

Accessed Ports through Firewall

Reports all ports accessed through a firewall by port and number of events. The table provides results by IP address of the firewall device, the type and vendor of the firewall, and the port used.

Email Activities

Provides an overview of email activities in your enterprise. You can view the accounts by quantity of emails received and sent, as well as by the size of emails received and sent.

Firewall Open Port Review

Reports the ports open in firewalls by the number of access events per port. The table provides results by IP address of the firewall device, the type of firewall, the open port, the number of events, and when the most recent event occurred.

Information Interception Events

Reports the traffic interception events that indicate spoofing and man-in-the-middle attacks. The table provides results by the type of event, the IP address of the target and source systems, the number of events, and when the most recent event occurred.

Insecure Services

Reports the events by port number and type of insecure service, such as FTP or Telnet. The table provides results by the target port, target process, target and source IP addresses, the target host name, the product that reported the insecure service, and the number of events.

Interzone Traffic

Reports the communications that pass between different zones over time. The table provides results by the IP address, name, and zone of the target host; the source zone, the protocol used; and when the most recent communication occurred.

Organizational Information Leaks

Reports events associated with information leaks as reported by IDSs over time. The table provides results by the event, the source and target users, the number of events, and when the most recent event occurred.

Peer to Peer Activity

Provides an overview of peer-to-peer communication events. You can view a trend of communications over time, the total number of communications, communications by source IP address, and the relationship of communications that occur between source and target IP address.

Personal Information Leaks

Reports events that are associated with personal information leaks as reported by IDSs over time. The table provides results by the event, the source and target users, the number of events, and when the most recent event occurred.

Phishing Activities

Provides an overview of phishing activity in your enterprise. You can view a trend of phishing events over time, events received from suspicious domains, and number of events by recipient email and sender's email.

Processes by Asset

Reports the processes running on assets in your environment. The table provides results by the IP address, name, and zone of the host where the processes are running, the process, the application protocol used, the service, the product, and the number of running processes.

14 – System Acquisition, Development, and Maintenance

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **IT GOV** > **ISO-27002** > **Reports** > **ISO 14 – System acquisition development and maintenance**.

Control 14: *System acquisition, development, and maintenance* of the ISO 27002 standard focuses on incorporating information security throughout the lifecycle of the data. Your enterprise is expected to ensure the security of data in both test/development and product environments.

To assess your enterprise's compliance with this requirement, use the following report:

Dashboards	Reports
n/a	"Invalid Data Input" on the next page

Invalid Data Input

Reports events that indicate corrupt data input such as exceptionally long URLs or SNMP requests that exceed the allowed buffer size.

The table provides results by the type of event, the IP address and name for both the target and source of the host, and the number of events.

16 – Information Security Incident Management

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **ITGov** > *Reports* or *Dashboards* > **ISO 16: Information security incident management**

Control 16: *Information security incident management* of the ISO 27002 standard expects your enterprise to effectively and consistently manage information security incidents.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
"Internal Reconnaissance" on the next page	"Confidential Breach Sources" below "Denial of Service" below "File Integrity Changes" on the next page "Information Systems Failures" on the next page "Integrity Breach Sources" on the next page "Internal Reconnaissance by Event" on the next page "Internal Reconnaissance by Source Address" on the next page "Internal Reconnaissance by Target Address" on page 172

Confidential Breach Sources

Reports the number of confidentiality breach events by IP addresses of the source system. The table provides results by the IP address, name, and zone of the source; the number of events; and when the most recent event occurred.

Denial of Service

Reports the number of denial of service (DoS) events by IP addresses of the targeted system. The table provides results by the IP address , name, and zone of the targeted system; the

type of DoS activity; and the number of events.

File Integrity Changes

Reports changes to files where the modification might compromise the integrity of the file. The table provides results by the path to the modified file, the IP address and name of the targeted host, the number of modifications, and when the most recent event occurred.

Information Systems Failures

Reports the number of changes to monitored files by target IP address and type of change. The report includes only events where agent severity is **High** or **Very-High**. The table provides results by the type of event; the IP address, name, and zone of the targeted system; and the number of events.

Integrity Breach Sources

Reports the number of attacks associated with integrity breaches, by source IP and type of breach. The table provides results by the type of breach event; the IP address, name, and zone of the source system; the number of events; and when the most recent event occurred.

Internal Reconnaissance

Provides an overview of events that indicate internal reconnaissance, which are attacks that occur within your organization's network, systems, and premises.

Internal Reconnaissance by Event

Reports the top events by the source IP address associated with the specified internal reconnaissance events. The table provides results by the type of event, the IP address, name, and zone of the target and source hosts; and the number of events.

You must specify at least one event by type.

Internal Reconnaissance by Source Address

Reports the number of internal reconnaissance events associated with the specified source IP address. The table provides results by the type of event, the IP address, name, and zone of the target and source hosts; and the number of events.

You must specify at least one IP address.

Internal Reconnaissance by Target Address

Reports the number of internal reconnaissance events associated with the specified target IP address. The table provides results by the type of event, the IP address, name, and zone of the target and source hosts; and the number of events.

You must specify at least one IP address.

17 – Information Security Aspects of Business Continuity Management

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **IT GOV** > **ISO-27002** > **Reports** > **ISO 17 – Information security aspects of business continuity management**.

Control 17: *Information security aspects of business continuity management* of the ISO 27002 standard expects that your business practices include managing the continuity of information security.

To assess your enterprise's compliance with this requirement, use the following report:

Dashboards	Reports
n/a	"Availability Attacks" below

Availability Attacks

Reports the number of events by targeted zone that indicate attacks to limit or prevent the availability of systems, networks, devices, or services in your enterprise. The table provides results by the type of event; the IP address, name, and zone of the targeted host; the number of events; and when the most recent event occurred.

Ensuring Compliance with PCI DSS

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

The PCI Security Standards Council has established standards to ensure the security of payment account data. To help you comply with the PCI Data Security Standards, we provide the **Compliance Pack for PCI**. For more information about adding the pack to the Reports repository, see the *Solutions Guide for ArcSight Compliance Pack for PCI*.

This pack includes dashboard and reports organized by the following PCI requirements:

Category	Dashboards	Reports
"1 – Maintain Firewalls to Protect Cardholder Data" on page 180	"Overview of Communication Activity from CDE" on page 185 "Overview of Communication Activity to CDE" on page 185	"Accessed Ports Through Firewall" on page 183 "Blocked Inbound Traffic to Card Holder Data Environment" on page 183 "Blocked Outbound Traffic from Card Holder Data Environment" on page 183 "Cardholder Data in the DMZ" on page 184 "External to Internal PCI Systems" on page 184 "Firewall Configuration Changes" on page 184 "Inbound Traffic to the Card Holder Data Environment" on page 184 "Internal PCI Systems to External" on page 184 "Network Routing Configuration Changes" on page 184 "Outbound Traffic from the Card Holder Data Environment" on page 185 "Personal Firewall Installed" on page 185 "Private IP Addresses Disclosure" on page 185 "Unauthorized Access to Card Holder Data Environment" on page 185 "Unauthorized Inbound Traffic to Card Holder Data Environment" on page 185 "Unauthorized Inbound Traffic to DMZ" on page 186 "Unauthorized Outbound Traffic from Card Holder Data Environment" on page 186 "VPN Configuration Changes" on page 186

Category	Dashboards	Reports
"2 – Do Not Use Default Security Parameters" on page 186	"Default Vendor Accounts Overview" on page 187 "Insecure Services – Dashboard" on page 187	"Default Vendor Accounts" on page 187 "Insecure Services – Report" on page 187 "Misconfigured Systems" on page 187 "Multiple Functions Implemented on a Server" on page 187 "Software Inventory" on page 187 "Unencrypted Administrative Accesses" on page 188
"3 – Protect Stored Cardholder Data" on page 188	n/a	"Credit Cards in Clear Text" on page 188
"4 – Encrypt Transmission of Cardholder Data" on page 188	n/a	"Cryptographic Hash Algorithm Related Vulnerabilities" on page 189 "Cryptographic Public Key Related Vulnerability Detected" on page 189 "Cryptographic Symmetric Key Related Vulnerabilities" on page 189 "Cryptographic Weak Protocol Vulnerability Detected" on page 189 "SSL or TLS Vulnerabilities" on page 189 "TLS BREACH Vulnerabilities" on page 190 "TLS CRIME Vulnerabilities" on page 190 "Wireless Encryption Violations" on page 190

Category	Dashboards	Reports
"5 – Use and Regularly Update Antivirus Software or Programs" on page 190	" Antivirus Activity" on page 191 " Malware Activities Overview" on page 192	"Disabled Antivirus and EDR" on page 191 "Failed Antivirus and EDR Updates" on page 191 "Installed Antivirus and EDR" on page 191 "Malicious Code Activities from CDE" on page 191 "Malware Activity" on page 192 "Malware Activity by Host" on page 192 "Spyware and Adware Activity" on page 192

Category	Dashboards	Reports
"6 – Maintain Secure Systems and Applications" on page 192	n/a	"Broken Authentication and Session Management" on page 193 "Buffer Overflows" on page 193 "Configuration Modifications by Host" on page 194 "Cross-Site Request Forgery" on page 194 "Cross-Site Scripting" on page 194 "Database Configuration Changes" on page 194 "Improper Access Control" on page 194 "Improper Error Handling" on page 195 "Injection Flaws" on page 195 "Insecure Cryptographic Storage" on page 195 "Meltdown or Spectre Vulnerable Assets" on page 195 "Operating System Changes" on page 195 "Outbound Communication from Development to Production" on page 195 "Outbound Communication from Production to Development " on page 195 "Security Patch Missing" on page 196 "SQL Injection Vulnerabilities" on page 196 "Use of Custom Accounts in Production" on page 196
"7 – Restrict Access to Cardholder Data" on page 196	"User Access Activity to Card Holder Data Environment" on page 197	"All Accesses to Cardholder Data Environment" on page 197 "All Accesses to Cardholder Data Environment by User" on page 197

Category	Dashboards	Reports
"8 – Assign a Unique ID to Each User" on page 197	"Password Policy Changes Overview" on page 198 "Windows Account Lockout" on page 199	"Clear Text Password Transmission" on page 198 "Password Policy Changes" on page 198 "Password Policy Minimum Age Changed" on page 198 "Successful Password Changes" on page 198 "Terminated User Activity" on page 199 "Terminated Users" on page 199 "Windows Account Lockouts by System" on page 199 "Windows Account Lockouts by User" on page 199
"9 – Restrict Physical Access to Cardholder Data" on page 199	"Failed Physical Facility Access - Dashboard" on page 200 "Successful Physical Facility Access" on page 200	"Failed Physical Facility Access - Report" on page 200 "Physical Facility Access Attempts" on page 200

Category	Dashboards	Reports
"10 – Track and Monitor Access to Cardholder Data" on page 200	"Firewall Events" on page 203	"Account Creation" on page 201 "Account Deletion" on page 201 "Account Modification" on page 202 "Administrative Actions Events" on page 202 "Administrative Authorization Changes" on page 202 "Anonymous User Activity in CDE" on page 202 "Audit Logs Cleared" on page 202 "Clock Synchronization Problems" on page 202 "Empty Origination of Event" on page 203 "Failed Administrative Actions" on page 203 "Failed Administrative Logins" on page 203 "Failed Logins" on page 203 "File Creations Deletions Modifications" on page 203 "IDS Events" on page 203 "Information System Failures" on page 204 "Successful Administrative Logins" on page 204 "Successful Logins to CDE" on page 204 "Successful User Logins" on page 204 "Successful User Logins by Host" on page 204 "User Group Creation" on page 204 "User Group Deletion" on page 204

Category	Dashboards	Reports
"11 – Test Security Systems and Processes Regularly" on page 204	"Attacks and Suspicious Activities Overview" on page 205 "Vulnerabilities Scanning" on page 208 Vulnerability Summary Overview	"Drill Down Assets with Buffer Overflow Vulnerabilities" on page 205 "Drill Down Assets with High Risk Vulnerabilities" on page 206 "Drill Down Assets with SSL and TLS Vulnerabilities" on page 206 "Drill Down CSRF Vulnerable Assets" on page 206 "Drill Down SQL Injection Vulnerable Assets" on page 206 "Drill Down XSS Vulnerable Assets" on page 206 "Exploit of Vulnerability" on page 207 "File Integrity Events" on page 207 "High Risk Vulnerabilities" on page 207 "Information Interception Events" on page 207 "Rogue Wireless AP Detected" on page 207 "Traffic Anomaly on Application Layer" on page 207 "Traffic Anomaly on Network Layer" on page 208 "Traffic Anomaly on Transport Layer" on page 208 "Vulnerability Summary by CVE" on page 208 "Vulnerability Summary by Host" on page 208 "Vulnerability Summary Overview" on page 208
"12 – Maintain a Policy that Addresses Information Security " on page 209	"Policy Violations - Dashboard" on page 209	"All Reporting Devices" on page 209 "Policy Violations - Report" on page 209 "Windows Domain Policy Changes" on page 209

1 – Maintain Firewalls to Protect Cardholder Data

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **PCI** > *Reports* or *Dashboards* > **Requirement 1: Firewall Configuration**.

PCI Requirement 1 requires that you install and maintain a firewall configuration to protect data in a cardholder data environment (CDE). **Firewalls** control computer traffic in and out of your network, as well as to and from sensitive areas within secure or sensitive internal networks. To prove compliance with PCI DSS, you must monitor the firewalls at Internet connections and between any demilitarized zones (DMZs). You must also monitor the devices that manage traffic.

Use the following dashboards and reports to check for potential firewall vulnerabilities in your environment.

Dashboards	Reports

"Overview of Communication Activity from CDE" on page 185 "Overview of Communication Activity to CDE" on page 185	"Accessed Ports Through Firewall" on the next page "Blocked Inbound Traffic to Card Holder Data Environment" on the next page "Blocked Outbound Traffic from Card Holder Data Environment" on the next page "Cardholder Data in the DMZ" on page 184 "External to Internal PCI Systems" on page 184 "Firewall Configuration Changes" on page 184 "Inbound Traffic to the Card Holder Data Environment" on page 184 "Internal PCI Systems to External" on page 184 "Network Routing Configuration Changes" on page 184 "Outbound Traffic from the Card Holder Data Environment" on page 185 "Personal Firewall Installed" on page 185 "Private IP

	Addresses Disclosure" on page 185 "Unauthorized Access to Card Holder Data Environment" on page 185 "Unauthorized Inbound Traffic to Card Holder Data Environment" on page 185 "Unauthorized Inbound Traffic to DMZ" on page 186 "Unauthorized Outbound Traffic from Card Holder Data Environment" on page 186 "VPN Configuration Changes" on page 186

Accessed Ports Through Firewall

Reports the firewalls that allowed the most traffic by port number. The table provides results by IP addresses for the firewall, the source system, and the destination system; the destination port; number of events; and the firewall rule number that triggered the event.

Blocked Inbound Traffic to Card Holder Data Environment

Reports the destination ports with traffic to the CDE from non-CDE systems that has been blocked the most often. The table provides results by IP addresses for the firewall, the source system, and the destination system; the destination port; the protocol used, number of events; and when the most recent event occurred.

Blocked Outbound Traffic from Card Holder Data Environment

Reports an overview of blocked traffic from the CDE to non-CDE systems over time. The table provides results by blocked outbound traffic per firewall. It lists the IP addresses for the firewall, the source system, and the destination system; the source and destination zones; affected port; and when the most recent event occurred.

Cardholder Data in the DMZ

Reports the internal systems that send the most communications to a DMZ, or less secure environment, in the specified time range. The table provides results by IP address of the source and destination systems, the affected ports, when the events occurred, and the number of events.

External to Internal PCI Systems

Reports the external systems that are communicating directly with PCI internal systems most often. The table provides results by the IP addresses and zones of the source and destination systems, the affected port, protocol used, and the number of events.

Firewall Configuration Changes

Reports the firewalls and devices with the most changes to their configuration. The table provides results by the IP address, product, and vendor of the device that was changed; the name and rule related to the change; the number of changes detected; and when the most recent event occurred.

Inbound Traffic to the Card Holder Data Environment

Reports the systems that allowed the most traffic to the CDE from non-CDE systems by destination address and port. The table provides results by the IP addresses for the firewall, the source system, and the destination system; the affected port; the protocol used; the number of events; and when the most recent event occurred.

Internal PCI Systems to External

Reports the CDE systems that communicate directly with external systems. PCI standards expects that your enterprise can justify this type of traffic. The table provides results by the IP address of the source system, destination system, and the device; the destination port; the protocol used; and the number of events.

Network Routing Configuration Changes

Reports the network routing devices that have had the most configuration changes in the specified time range. The table provides results by the IP address for the device, the type of device; the event name; number of events; and when the most recent event occurred.

Outbound Traffic from the Card Holder Data Environment

Reports the systems that allowed traffic from the CDE to non-CDE systems by destination IP address. The table provides results by the IP addresses for the device, the source system, and the destination system; the affected port; the protocol used; number of events; and when the most recent event occurred.

Overview of Communication Activity from CDE

Provides, in charts and a table, an overview of communication going out from the CDE. You can view the target and source IP addresses, target ports, and the block source IP addresses.

Overview of Communication Activity to CDE

Provides, in charts and a table, an overview of communication coming into the CDE. You can view the target and source IP addresses, target ports, and the block source IP addresses.

Personal Firewall Installed

Reports the servers with a personal firewall installed. PCI standards require that users install personal firewall software on any device, such as a laptop, that is used to access the cardholder data environment and also might connect to the Internet when outside the PCI network. The table lists the IP address and name of the system hosting the personal firewall, as well as the more recent time that the firewall was detected.

Private IP Addresses Disclosure

Reports the RFC1918 IP addresses with the most communication with public IP addresses. The table provides results by IP address of the source and associated destination systems, the destination port, the protocol used, and the number of events.

Unauthorized Access to Card Holder Data Environment

Reports the accounts with the most unauthorized attempts to access the CDE. The table provides results by the user account, source and destination IP addresses, time the events occurred, and the number of events.

Unauthorized Inbound Traffic to Card Holder Data Environment

Reports the IP addresses in the cardholder environment that have experienced the most unauthorized traffic to the CDE from non-CDE systems. The table provides results by the source and destination IP addresses, the ports of the destination system, the protocol used, the number of events, and when the most recent event occurred.

Unauthorized Inbound Traffic to DMZ

Reports the systems with the highest amount of unauthorized traffic to the DMZ. The table provides results by the IP addresses for the device, the source system, and the destination system; the source zone; affected port; number of events; and when the most recent event occurred.

Unauthorized Outbound Traffic from Card Holder Data Environment

Reports the ports with the most unauthorized traffic from the CDE to non-CDE systems. The table provides results by the IP addresses for the device, the source system, and the destination system; the destination zone; the affected port; the protocol used; and number of events.

VPN Configuration Changes

Reports the VPN gateways with the most changes to their configuration. The table provides results by IP address of the VPN, the policies or configurations changed, the type of VPN, and number of events.

2 – Do Not Use Default Security Parameters

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **PCI** > *Reports* or *Dashboards* > **Requirement 2: Default Security Parameters**.

PCI Requirement 2 addresses the use of vendor-supplied default settings, such as passwords and account names. These are known values and can be exploited by malicious users. While devices and firewalls installed by IT administrators might have strong security process, users who install software and add devices might not follow good security practices.

Use the following dashboards and reports to check for default security parameters in your environment.

Dashboards	Reports
"Default Vendor Accounts Overview" on the next page "Insecure Services – Dashboard" on the next page	"Default Vendor Accounts" on the next page "Insecure Services – Report" on the next page "Misconfigured Systems" on the next page "Multiple Functions Implemented on a Server" on the next page "Software Inventory" on the next page "Unencrypted Administrative Accesses" on page 188

Default Vendor Accounts

Reports default vendor accounts by username. The table provides results by the IP address and name of the device's address, the vendor's name, the account name, and quantity.

Default Vendor Accounts Overview

Provides, in several charts, an overview of default vendor accounts. You can view the accounts associated with the most events, account activity over time, the IP addresses associated with the accounts, and the most active vendors.

Insecure Services – Dashboard

Provides, in charts and table, insecure events by port number and IP address, activities by day, and the products that report insecure services in other systems.

Insecure Services – Report

Reports insecure events by port number. The table provides results by the target port, target process, target and source IP addresses, the target host name, the product that reported the insecure service, and the number of events.

Misconfigured Systems

Reports systems with the most misconfiguration events reported in your environment. In general, the most common vulnerability in your environment is misconfigured operating systems, frameworks, libraries, and applications. Misconfigurations 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. The table provides results by IP address and name of the misconfigured system, the name of the event, and number of events.

Multiple Functions Implemented on a Server

Reports the servers that have multiple functions installed on them. For example, a server might have functions such as DNS, a Web server, and a database.

Software Inventory

Reports the software found by IP address and host name.

Unencrypted Administrative Accesses

Reports the accounts that have had unencrypted administrative access events. The table provides results by the IP address and name of the host, the affected account, the port used, affected process, and number of events.

3 – Protect Stored Cardholder Data

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **PCI** > **Reports** > **Requirement 3: Protect Stored Cardholder Data**.

PCI Requirement 3 ensures that cardholder data cannot be read or used by individuals who maliciously or unintentionally access encrypted data. You must have security measures to encrypt, truncate, mask, or hash critical components of the data.

To assess your enterprise's compliance with this requirement, use the following report:

Credit Cards in Clear Text

Reports the hosts where credit card data has been detected in clear text format. The table provides results by the affected host and reporting device IP addresses, the signature ID, and when the clear text was detected.

4 – Encrypt Transmission of Cardholder Data

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **Reports** > **Requirement 4: Encryption Transmission**.

PCI Requirement 4 focuses on managing and maintaining the security of the card holder data when it is transmitted over open or public networks. Transmitted data should be encrypted. Malicious users can exploit vulnerabilities in cryptographic hashes and keys, as well as through SSL and TLS. For example, the Heartbleed Bug is a known SSL vulnerability.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
n/a	"Cryptographic Hash Algorithm Related Vulnerabilities" below "Cryptographic Public Key Related Vulnerability Detected" below "Cryptographic Symmetric Key Related Vulnerabilities" below "Cryptographic Weak Protocol Vulnerability Detected" below "SSL or TLS Vulnerabilities" below "TLS BREACH Vulnerabilities" on the next page "TLS CRIME Vulnerabilities" on the next page "Wireless Encryption Violations" on the next page

Cryptographic Hash Algorithm Related Vulnerabilities

Reports events by host name that indicate potential vulnerabilities related to hash algorithms. All cryptographic hashes that directly use the full output of a Merkle–Damgård construction are vulnerable to length extension attacks. The table provides results by name of the event, host and IP address, and number of events.

Cryptographic Public Key Related Vulnerability Detected

Reports flaws found in cryptographic public keys on hosts, as reported by vulnerability scanners in your environment. The table provides results by name of the event, host and IP address, and number of events.

Cryptographic Symmetric Key Related Vulnerabilities

Reports vulnerabilities related to cryptographic symmetric keys by the address or host name of the target asset. The table provides results by the target asset, the device vendor and product, the number of events, and when the most recent event occurred.

Cryptographic Weak Protocol Vulnerability Detected

Reports all vulnerabilities associated with weak cryptographic protocol. The table provides results by the vulnerability name, the affected assets, the number of events, and when the most recent event occurred.

SSL or TLS Vulnerabilities

Reports all SSL and TLS vulnerabilities detected by host name. The table provides results by name of the event, host and IP address, and number of events.

TLS BREACH Vulnerabilities

Reports TLS BREACH vulnerabilities detected by host name. A TLS BREACH attack is a form of the CRIME attack against HTTP compression. The table provides results by name of the event, host and IP address, and number of events.

TLS CRIME Vulnerabilities

Reports the hosts detected with vulnerabilities to a TLS CRIME attack. In a CRIME attack, malicious users access the content of secret authentication cookies, so they can hijack sessions of an authenticated web session, then launch additional attacks. The table provides results by name of the event, host and IP address, and number of events.

Wireless Encryption Violations

Reports the hosts that have wireless encryption violations, as detected by vulnerability scanners. The table provides results by name of the event, host and IP address, and number of events.

5 – Use and Regularly Update Antivirus Software or Programs

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **PCI** > *Reports* or *Dashboards* > **Requirement 5: Antivirus**.

PCI Requirement 5 focuses on preventing malware, such as worms, viruses, and trojans, from infecting the cardholder data environment (CDE). This type of malware can enter the network through common business activities and processes: employee email, Internet usage, cell phones, or storage devices. Malware can then damage systems by exploiting system security vulnerabilities or trying to steal confidential information. Your enterprise should install and maintain antivirus software on all devices frequently affected by malware to protect networks from existing and emerging threats.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
" Antivirus Activity" below " Malware Activities Overview" on the next page	"Disabled Antivirus and EDR" below "Failed Antivirus and EDR Updates" below "Installed Antivirus and EDR" below "Malicious Code Activities from CDE" below "Malware Activity" on the next page "Malware Activity by Host" on the next page "Spyware and Adware Activity" on the next page

Antivirus Activity

Provides charts for an overview of antivirus activities in the CDE. You can view the trends of antivirus cleaning/quarantining attempts and failures over time, a trend of failed cleaning and the number of times antivirus has failed to update and the associated agent, and the number of events by device vendor.

Disabled Antivirus and EDR

Reports events associated with disabling antivirus and EDR programs by target host. The table provides results by the target host, the antivirus or EDR program affected, the user that disabled the program, the number of events, and when the event occurred.

Failed Antivirus and EDR Updates

Reports events where antivirus and EDR programs failed to update by target host. The table provides results by the target host, the antivirus or EDR program affected, the name and userID that disabled the program, the number of events, and when the event occurred.

Installed Antivirus and EDR

Reports events where antivirus and EDR programs are installed by type of program. The table provides results by the type of antivirus or EDR product, the location of the program, and the number of events.

Malicious Code Activities from CDE

Reports malicious code activity sent from the CDE. The table provides results by the source and target addresses, the type of event, the product, and the number of events.

Malware Activities Overview

Provides an overview of all malware activity in the CDE. You can view the trends of malware activities over time, top signature IDs, top affected systems, and the top reporting products.

Malware Activity

Reports the malware detected in the CDE. The table provides results by the type of malware, the target asset, the number of events, and the when the event occurred.

Malware Activity by Host

Reports the malware activity by target host. The table provides results by the type of malware, the target asset, the number of events, and the when the event occurred.

Spyware and Adware Activity

Reports target hosts where spyware or adware has been detected. The table provides results by the affected asset, the type of spyware or adware, the event class, the number of events, and when the event occurred.

6 – Maintain Secure Systems and Applications

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **PCI** > *Reports* or *Dashboards* > **Requirement 6: Secure Systems and Applications**.

PCI Requirement 6 sets the expectation that you apply security patches to all applications and systems in the cardholder data environment (CDE) to protect them from malicious and unintentional misuse. The patches should be evaluated to ensure that they do not conflict with current security configurations. You must also ensure that in-house development teams practice secure coding techniques. Applications that store sensitive data must be able to protect the data.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
n/a	"Broken Authentication and Session Management" below "Buffer Overflows" below "Configuration Modifications by Host" on the next page "Cross-Site Request Forgery" on the next page "Cross-Site Scripting" on the next page "Database Configuration Changes" on the next page "Improper Access Control" on the next page "Improper Error Handling" on page 195 "Injection Flaws" on page 195 "Insecure Cryptographic Storage" on page 195 "Meltdown or Spectre Vulnerable Assets" on page 195 "Operating System Changes" on page 195 "Outbound Communication from Development to Production" on page 195 "Outbound Communication from Production to Development " on page 195 "Security Patch Missing" on page 196 "SQL Injection Vulnerabilities" on page 196 "Use of Custom Accounts in Production" on page 196

Broken Authentication and Session Management

Reports events associated with broken authentication and session management over time. The table provides results by the target asset, name and signature ID of the vulnerability, and the number of events.

Buffer Overflows

Reports vulnerabilities associated with buffer overflows by CDE asset. This type of vulnerability occurs when a developer fails to appropriately manage memory for user-controlled data. A malicious user could put more data into a pre-allocated memory buffer than the buffer can hold, dramatically impacting the operation of a program. The table provides results by the affected asset, the detected vulnerability, the signature ID of the vulnerability, and when the most recent event occurred.

Configuration Modifications by Host

Reports modifications made to CDE assets. The table provides results by the affected asset, the type of modification, the user who made the change, the number of events, and when the most recent event occurred.

Cross-Site Request Forgery

Reports assets that might be vulnerable to a cross-site request forgery (XSRF or CSRF) attack. In an CSRF 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. The table provides results by the targeted asset and when the most recent event occurred.

Cross-Site Scripting

Reports the signature ID of cross-site scripting (XSS) attacks by volume. Vulnerabilities associated with 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. The table provides results by the signature ID of the event, the target asset, the number of events, and when the most recent event occurred.

Database Configuration Changes

Reports changes to the database configuration by affected asset. The table provides results by the database host, the modification made, the user who made the change, the number of changes, and when the most recent change occurred.

Improper Access Control

Reports vulnerabilities associated with improper access controls. The table provides results by the signature ID of the event, the target asset, the number of events, and when the most recent event occurred.

Improper Error Handling

Reports vulnerabilities associated with improper handling of errors by affected assets. The table provides results by the signature ID of the event, the target asset, and when the most recent event occurred.

Injection Flaws

Reports the assets with the most injection flaws. The table provides results by the affected asset, the injection flaw and its signature ID, and when the event occurred.

Insecure Cryptographic Storage

Reports the IP addresses of systems where sensitive data is not stored securely. The table provides results by the affected asset, the event, the number of events, and when the most recent event occurred.

Meltdown or Spectre Vulnerable Assets

Reports the assets with the most Meltdown or Spectre vulnerabilities. The table provides results by the affected asset, the vulnerability and its signature ID, the number of events, and when the most recent event occurred.

Operating System Changes

Reports changes to operating systems. The table provides results by the target asset, the change, the outcome of the change, and the number of changes.

Outbound Communication from Development to Production

Reports all communication sent from the development environment to the production environment. The table provides results by the source and target addresses, the port used, the transportation protocol, and the number of events.

In the logical model, you must edit the `isSourceZonePCIDevelopment` and `isDestinationZonePCIProduction` variables to indicate the respective zones for development and production.

Outbound Communication from Production to Development

Reports all communication sent from the production environment to the development environment. The table provides results by the source and target addresses, the port used, the transportation protocol, and the number of events.

In the logical model, you must edit the **isSourceZonePCIProduction** and **isDestinationZonePCIDevelopment** variables to indicate the respective zones for production and development.

Security Patch Missing

Reports assets by IP address with missing security patches. One of the most common ways to reduce your environment's attack surface is to ensure that all systems have the most recent security patches applied. The table provides results by the affected asset, the vulnerability and signature ID associated with the missing patch, the number of events, and when the most recent event occurred.

SQL Injection Vulnerabilities

Reports SQL injection vulnerabilities by asset. 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. The table provides results by the target assets, the vulnerability and its signature ID, the number of events, and when the most recent event occurred.

Use of Custom Accounts in Production

Reports events in the production environment associated with the specified list of accounts. The table provides results by the specified accounts, the target asset, the number of events, and when the most recent event occurred.

You must enter the accounts that you want to include in the report. Use commas to separate the values.

7 – Restrict Access to Cardholder Data

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **PCI** > *Reports* or *Dashboards* > **Requirement 7: Restrict Access By Business Need to Know**.

PCI Requirement 7 focuses on controlling access to cardholder data, thus limiting access privileges only to users who need to know the data according to your enterprise's needs. Usually, enterprises apply the principle of least privilege when granting access rights in the cardholder data environment (CDE).

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
"User Access Activity to Card Holder Data Environment" below	"All Accesses to Cardholder Data Environment" below "All Accesses to Cardholder Data Environment by User" below

All Accesses to Cardholder Data Environment

Reports the most accessed hosts in the CDE. The table provides results by the target host name and IP address, the target user, the source user and address, and the number of events.

All Accesses to Cardholder Data Environment by User

Reports all access activity in the CDE by the user. By default, the report lists user activities. The table provides results by the target host name and address, the target user, the port used, the source address, and the number of events.

In the logical model, use the **isDestinationUserPCI** variable to specify the users in the CDE that you want to include in the reports. For more information, see the *Solutions Guide for ArcSight Compliance Pack for PCI*.

User Access Activity to Card Holder Data Environment

Provides, in charts and a table, an overview of user access activities in the CDE. You can view a trend of activity over time, as well as events by target users, target IP address, and source IP address.

8 – Assign a Unique ID to Each User

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **PCI** > *Reports* or *Dashboards* > **Requirement 8: Unique User ID**.

PCI Requirement 8 covers identification and authentication for all access to system components in the cardholder data environment (CDE). Basically, your enterprise must maintain and monitor changes to user accounts and password policies to prevent malicious users from gaining access to the CDE through weak passwords or by changing password policies. This requirements applies to all accounts with administrative features, including point-of-sale accounts; accounts used by vendors and third parties; and any account used to view cardholder data or access cardholder data or to access systems with cardholder data. This requirement does not apply to end-user accounts used by consumers.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
"Password Policy Changes Overview" below "Windows Account Lockout" on the next page	"Clear Text Password Transmission" below "Password Policy Changes" below "Password Policy Minimum Age Changed" below "Successful Password Changes" below "Terminated User Activity" on the next page "Terminated Users" on the next page "Windows Account Lockouts by System" on the next page "Windows Account Lockouts by User" on the next page

Clear Text Password Transmission

Reports events by IP address where passwords were transmitted in clear text. The table provides results by the target host name and IP address, the port used, the number of events, and when the clear text password was detected.

Password Policy Changes Overview

Provides, in charts and a table, an overview of policy changes on CDE assets. You can view a trend of changes made over time, changes to target user accounts, changes to target IP addresses, and changes by type.

Password Policy Changes

Reports changes to the password policy over time in the CDE. The table provides results by the target IP address, the user who made the change, the change made, the number of events, and when the change occurred.

Password Policy Minimum Age Changed

Reports changes to the policy for the minimum password age over time in the CDE. The table provides results by the target IP address, the user who made the change, the change made, the number of events, and when the change occurred.

Successful Password Changes

Reports successful password changes over time in the CDE. The table provides results by the target IP address and host name, the affected user account, the number of events, and when the most recent event occurred.

Terminated User Activity

Reports user accounts that have been terminated but show successful authentication events after termination. The table provides results by the terminated account and when successful authentication occurred.

Terminated Users

Reports all user accounts terminated in the CDE by termination date. The table provides results by the terminated account and when the account was terminated.

Windows Account Lockout

Provides, in charts and a table, an overview of Windows accounts that have been locked out. You can view a trend of events over time, events by target IP address, and events by the accounts locked out.

Windows Account Lockouts by System

Reports, by host system, all Windows accounts that have been locked out. The table provides results by the target host name, IP address, domain, and user; the number of lockouts; and when the most recent event occurred.

Windows Account Lockouts by User

Reports, by user and domain, all Windows accounts that have been locked out. The table provides results by the target domain and user, the number of lockouts, and when the most recent event occurred.

9 – Restrict Physical Access to Cardholder Data

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **PCI** > *Reports* or *Dashboards* > **Requirement 9: Physical Access**.

PCI Requirement 9 expects your organization to restrict access to devices that allow an individual physical access to the systems that store cardholder data, thus limiting the ability for malicious users to access or destroy the devices, data, systems, or hard copies.

By default, these reports and dashboards assume all assets are associated with physical access. To specify specific locations and buildings, update the **isPCIBuilding** variable in the data worksheet for each PCI Requirement 9 report or dashboard. For more information, see the *Solutions Guide for ArcSight Compliance Pack for PCI*.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
"Failed Physical Facility Access - Dashboard" below	"Failed Physical Facility Access - Report" below
"Successful Physical Facility Access" below	"Physical Facility Access Attempts" below

Failed Physical Facility Access - Dashboard

Provides, in charts and table, an overview of failed attempts to access physical facilities. You can view a trend of access activity over time, as well as activity by reporting device, location, and user.

Failed Physical Facility Access - Report

Reports the number of failed attempt to access physical facilities by location. The table provides results by the target location, the user involved, the number of attempts, and when the attempt occurred.

Physical Facility Access Attempts

Reports the number of attempts to access physical facilities by location and user. The table provides results by the target location, the user involved, the outcome of the attempt, the number of attempts, and when the most recent event occurred.

Successful Physical Facility Access

Provides, in charts and table, an overview of successful attempts to access physical facilities. You can view a trend of access activity over time, as well as activity by reporting device, location, and user.

10 – Track and Monitor Access to Cardholder Data

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **PCI** > *Reports* or *Dashboards* > **Requirement 10: Track and Monitor Data Access**.

PCI Requirement 10 focuses on tracking changes to user accounts and groups to detect and prevent data breaches within the cardholder data environment (CDE). Malicious users might create groups or accounts to grant them access to sensitive data, then delete their changes to hide their activity.

To assess your enterprise's compliance with this requirement, use the following dashboard and reports:

Dashboards	Reports
"Firewall Events" on page 203	"Account Creation" below "Account Deletion" below "Account Modification" on the next page "Administrative Actions Events" on the next page "Administrative Authorization Changes" on the next page "Anonymous User Activity in CDE" on the next page "Audit Logs Cleared" on the next page "Clock Synchronization Problems" on the next page "Empty Origination of Event" on page 203 "Failed Administrative Actions" on page 203 "Failed Administrative Logins" on page 203 "Failed Logins" on page 203 "File Creations Deletions Modifications" on page 203 "IDS Events" on page 203 "Information System Failures" on page 204 "Successful Administrative Logins" on page 204 "Successful Logins to CDE" on page 204 "Successful User Logins" on page 204 "Successful User Logins by Host" on page 204 "User Group Creation" on page 204 "User Group Deletion" on page 204

Account Creation

Reports all user accounts created. The table provides results by IP address or host name of the system, as well as the name of the new account.

Account Deletion

Reports all user accounts that have been deleted. The table provides results by name of the account that made the change, IP address or host name of the system, and event name for the deleted account.

Account Modification

Reports all user accounts that have been modified. The table provides results by the type of modification, name of the changed account, the account that made the change, and the IP address or host name of the system.

Administrative Actions Events

Reports all actions, except logins, made by administrative users. The table provides results by the user name, device event class, number of events, and when the change occurred.

Administrative Authorization Changes

Reports all changes authorized by administrative users. The table provides results by the source and target user, the number of changes, and when the change occurred.

Anonymous User Activity in CDE

Reports all logins to the CDE by anonymous users. The table provides details about the user, the affected host, the number of attempted logins, and when the most recent event occurred.

By default, the report includes all users who log in to the CDE because the variable `isUserNameAnonymous` is set to *yes*. To make the report more specific, in the logical model, enter the list of anonymous users for the variable `isUserNameAnonymous`, as shown in the example. For more information, see the *Solutions Guide for ArcSight Compliance Pack for PCI*.

Audit Logs Cleared

Reports the audit logs cleared by user. The table provides results by the user, the affected host, the number of events, and when the most recent event occurred.

Clock Synchronization Problems

Reports the number of assets with clock synchronization issues over time. In SSL, clocks are used for certificate validation. A malicious user could modify the server or client clock to disregard dates in certificates. Then that user will be able to impersonate the server forever even if the certificate expires. The table provides details about the affected asset and when the most recent event occurred.

Empty Origination of Event

Reports events in which the source, such as user, address, device or hostname, cannot be identified. The table provides results by the anomaly's name, the number of events, and when the most recent event occurred.

Failed Administrative Actions

Reports failed actions, except logins, by administrative users. The table provides results by the target user and host, device event class, the affected product, the number of failed attempts, and when the most recent event occurred.

Failed Administrative Logins

Reports the number of failed logins by administrative users. The table provides results by the target host, administrative user, and the number of failed attempts.

Failed Logins

Reports the number of failed logins by user. The table provides results by the target host, administrative user, and the number of failed attempts.

File Creations Deletions Modifications

Reports the file creations, deletions, and modifications by host. The table provides results by the asset, the type of activity, outcome of the activity, the number of events, and when the most recent event occurred.

Firewall Events

Provides, in charts and a table, an overview of firewall events. You can view a trend of firewall events overtime, the number of times a firewall rule has been hit, the firewalls by vendor, and products reporting the events.

IDS Events

Reports all events recorded by the IDSs in your enterprise. The table provides results by the IDS device, the type of event, the number of events, and when the most recent event occurred.

Information System Failures

Reports all failures associated with information systems. The table provides results by the target asset, the type of failure, the device vendor, and the number of failure events.

Successful Administrative Logins

Reports all successful logins by administrative users. The table provides results by the target asset, the user, and the number of logins.

Successful Logins to CDE

Reports all successful logins within the CDE. The table provides results by the target asset, the user, the number of logins, and when the most recent login occurred.

Successful User Logins

Reports all successful logins by user. The table provides results by the target asset, the user, the number of logins, and when the most recent login occurred.

Successful User Logins by Host

Reports all successful user logins by host. The table provides results by the target asset, the user, the number of logins, and when the most recent login occurred.

User Group Creation

Reports all user groups created. The table provides results by the event, the new user group, and the user who created the account.

User Group Deletion

Reports all user groups deleted. The table provides results by the event, the user group deleted, and the user who deleted the account.

11 – Test Security Systems and Processes Regularly

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **PCI** > *Reports* or *Dashboards* > **Requirement 11: Test Systems and Processes**.

PCI Requirement 11 focuses on frequently testing your processes and the security system components of your cardholder data environment, such as performing regular vulnerability

scans. PCI expects your enterprise to keep your processes and systems current with evolving security issues.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
"Attacks and Suspicious Activities Overview" below "Vulnerabilities Scanning" on page 208 "Vulnerability Type Overview" on page 208	"Drill Down Assets with Buffer Overflow Vulnerabilities" below "Drill Down Assets with High Risk Vulnerabilities" on the next page "Drill Down Assets with SSL and TLS Vulnerabilities" on the next page "Drill Down CSRF Vulnerable Assets" on the next page "Drill Down SQL Injection Vulnerable Assets" on the next page "Drill Down XSS Vulnerable Assets" on the next page "Exploit of Vulnerability" on page 207 "File Integrity Events" on page 207 "High Risk Vulnerabilities" on page 207 "Information Interception Events" on page 207 "Rogue Wireless AP Detected" on page 207 "Traffic Anomaly on Application Layer" on page 207 "Traffic Anomaly on Network Layer" on page 208 "Traffic Anomaly on Transport Layer" on page 208 "Vulnerability Summary by CVE" on page 208 "Vulnerability Summary by Host" on page 208 "Vulnerability Summary Overview" on page 208

Attacks and Suspicious Activities Overview

Provides, in charts and a table, an overview of attacks and suspicious events. You can view the IP addresses generating the most attacks, the systems that are the target of most attacks, a trend of attacks over time, and the top events.

Drill Down Assets with Buffer Overflow Vulnerabilities

Lists assets that might be vulnerable to buffer overflow. This type of vulnerability occurs when a developer fails to appropriately manage memory for user-controlled data. A

malicious user could put more data into a pre-allocated memory buffer than the buffer can hold, dramatically impacting the operation of a program.

Drill Down Assets with High Risk Vulnerabilities

Reports assets that might be vulnerable to listed high-risk security threats. 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.

Drill Down Assets with SSL and TLS Vulnerabilities

Reports assets that might have the listed TLS or SSL vulnerability. For example, malicious users can exploit a known vulnerability in SSL with the Heartbleed Bug.

Drill Down CSRF Vulnerable Assets

Reports assets that might be vulnerable to the listed cross-site request forgery (XSRF or CSRF) attack. In a CSRF 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.

Drill Down SQL Injection Vulnerable Assets

Reports assets that might be vulnerable to the listed SQL injection attacks. 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.

Drill Down XSS Vulnerable Assets

Reports assets that might be vulnerable to the listed cross-site scripting (XSS) attacks. Vulnerabilities associated with 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 websites, 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 VBSCript, ActiveX, Flash, and CSS. However, this type of injection attack most commonly occurs in Java Script.

Exploit of Vulnerability

Reports events that indicate an attempt to exploit a given detected vulnerability. The table provides results by the vulnerability, IP address and name of the affected system, number of events associated with the vulnerability, and when the most recent event occurred.

File Integrity Events

Reports events that indicate file integrity might be compromised in your environment. File integrity monitoring, also known as change monitoring, checks operating system files, Windows registries, application software, Linux system files, and more, for changes that might indicate an attack. The table provides results by the signature ID, IP address and name of the affected system, the number of events, and when the most recent event occurred.

High Risk Vulnerabilities

Reports the systems with the greatest likelihood of being exploited based on the reported vulnerabilities. The table provides results by the vulnerability, the signature ID, name of the affected system, and when the most recent event occurred.

Information Interception Events

Reports traffic interception events that indicate spoofing or man-in-the-middle attacks. The table provides results by the signature ID, details of the source and destination addresses, the number of events, and when the most recent event occurred.

Rogue Wireless AP Detected

Reports rogue wireless access points (AP) found in your environment. A user might install a rogue AP unintentionally or maliciously in an office or data center without the knowledge or permission from the system administrator via the wired infrastructure. The chart shows rogue APs found over time. The table provides results by the device ID and name, when the event occurred, and the number of events.

Traffic Anomaly on Application Layer

Reports all the traffic anomalies found in the application layer. Malicious users attack the application layer of an application, which specifies the communication protocols and interface methods used by hosts in the network, to disrupt processes and services on a web server or application. The table provides results by signature ID, details of the affected system or product, the number of events, and when the most recent event occurred.

Traffic Anomaly on Network Layer

Reports all the traffic anomalies found in the network layer. This layer supports communications by sending packets of data back and forth between different networks, and thus can be vulnerable to a large variety of attacks. The table provides results by the destination and source systems, the number of events, and when the most recent event occurred.

Traffic Anomaly on Transport Layer

Reports all the traffic anomalies found in the transport layer. In this layer, a malicious user might hijack session by taking control of a session between two nodes after the initial authentication process is complete. The table provides results by signature ID, the destination and source systems, the number of events, and when the most recent event occurred.

Vulnerability Summary by CVE

Reports vulnerabilities by CVE and severity. The table provides results by the CVE, its severity, the affected asset, and when the most recent event occurred.

Vulnerability Summary by Host

Reports vulnerabilities found by host. The table provides results by the CVE, its severity, the affected asset, and when the most recent event occurred.

Vulnerability Summary Overview

Reports all the vulnerabilities found in the PCI environment. The table provides results by the vulnerability name, CVE, the common vulnerability score (CVSS), signature ID, the affected asset, and when the most recent event occurred.

Vulnerabilities Scanning

Provides, in several charts, the details of reported vulnerabilities over time. You can view the assets with the most high-risk vulnerabilities, the most reported vulnerabilities, and the assets with vulnerabilities including the hostnames.

Vulnerability Type Overview

Provides charts for an overview of vulnerabilities by category: SQL, XSS, CSRF, SSL, high-risk, and buffer overflow. You can drill down in the charts to identify the affected assets.

12 – Maintain a Policy that Addresses Information Security

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **PCI** > *Reports* or *Dashboards* > **Requirement 12: Maintain Information Security Policy**.

PCI Requirement 12 expects your enterprise to maintain a policy that addresses the information security for all personnel who are associated with your enterprise or have some form of access to the cardholder's data system. Personnel should know the enterprise's expectations for handling cardholder data, and should know their responsibilities for protecting the sensitivity of the data.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
"Policy Violations - Dashboard" below	"All Reporting Devices" below "Policy Violations - Report" below "Windows Domain Policy Changes" below

All Reporting Devices

Lists all reporting devices in the environment by number of events. PCI expects that you maintain an inventory of devices and check for unapproved devices. The table lists device by product, vendor, IP address, and zone.

Policy Violations - Dashboard

Provides, in charts and a table, an overview of policy violations. You can view the number of violations by day, the IP addresses and signature IDs associated with violations, and the users with the most violations.

Policy Violations - Report

Reports policy violations by IP address. The table lists the details of the affected host system, the number of events, and when the events occurred.

Windows Domain Policy Changes

Reports changes to the Windows domain policy by associated IP address. The table lists the details of the affected host system and the number of changes.

Ensuring Compliance with SOX Standards

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **SOX**.

The Sarbanes-Oxley Act (SOX) is a United States federal law that was enacted in 2002. The stated purpose of the law is to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws and for other purposes.

To help you comply or prove compliance with SOX, we provide the **Compliance Insight Package for SOX**. For more information about adding the package to the Reports repository, see the *Solutions Guide for ArcSight Insight Compliance Package for SOX*. The guide includes information about identifying assets that must comply with SOX.

This package includes the following dashboards and reports, organized by SOX objectives:

Category	Dashboards	Reports
Executive Summary	Control Overview Controls Risk Score Overview Executive Cyber Threat Overview	n/a
ISO 5 Information Security Policies	Policy Violations Overview	Policy Violations
ISO 6 Organization of Information Security	VPN Connection Overview Wireless Attacks and Suspicious Activity	Outbound Communication from Development to Production Environment Outbound Communication from Production to Development Environment VPN Connection Summary Wireless Attacks and Suspicious Activity
ISO 7 Human Resource Security	Activity by User	n/a
ISO 8 Asset Management	Removable Media Activity	n/a

Category	Dashboards	Reports
ISO 9 Access Control	n/a	Account Creations Account Deletions Account Lockouts by System Account Lockouts by User Insecure Ports Insecure Services Password Policy Changes Password Weaknesses User Group Account Creations User Group Account Deletions
ISO 10 Cryptography	n/a	SSH Vulnerabilities SSL or TLS Vulnerabilities VPN Vulnerabilities
ISO 11 Physical and Environmental Security	Failed Physical Physical Access Overview Successful Physical Physical Access Overview	Failed Building Physical Access Activity Summary Failed User Physical Access Activity Summary Successful Building Physical Access Activity Summary Successful User Physical Access Activity Summary

Category	Dashboards	Reports
ISO 12 Operations Security	Administrative Login Overview Application Vulnerabilities Overview Failed Login Overview Failed Login Relationship Firewall Configuration Changes Malware Overview Successful Login Overview Unpatched Systems Vulnerability Overview	Antivirus Stopped or Paused Audit Log Cleared Database Configuration Changes Database Vulnerabilities Failed Administrative Login Summary Failed Antivirus Updates Failed Login by SOX Asset Failed Login Summary Firewall Configuration Changes High Risk Vulnerabilities Malware Summary Network Device Configuration Changes Overflow Vulnerabilities SQL Injection Vulnerabilities Successful Administrative Login Summary Successful Login by SOX Asset Unpatched Systems Vulnerability Summary by CVE ID Vulnerability Summary by SOX Asset Vulnerability Summary on SOX Environment XSRF Vulnerabilities XSS Vulnerabilities
ISO 13 Communications Security	DoS Activity Firewall Blocked Events	Covert Channel Activity DoS Attacks Summary Firewall Blocked Events

Category	Dashboards	Reports
ISO 16 Information Security Incident Management	High Risk Events Overview MITRE ATT&CK Overview Reconnaissance Activity Threat Overview Threat Relationship	High Risk Events Summary MITRE ATT&CK Summary by MITRE Technique MITRE ATT&CK Summary by SOX Asset Reconnaissance Summary Threats Summary
ISO 17 Information Security Aspects of Business Continuity Management	n/a	Asset Shutdown Summary
ISO 18 Compliance	Information Disclosure Vulnerabilities Organization Information Leaks Personal Information Leakage Overview	Information Disclosure Vulnerabilities Organization Information Leaks Summary Personal Information Leakage Summary

Sarbanes-Oxley Executive Summary

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **Executive Summary**.

This category is relevant to all ISO 27002:2013 controls. To assess your enterprise's compliance with this requirement, use the following dashboards:

Dashboards	Reports
Control Overview Controls Risk Score Overview Executive Cyber Threat Overview	n/a

Control Overview

Used as a drill-down dashboard by the Controls Risk Score Overview dashboard.

Controls Risk Score Overview

Provides an overview of ISO 27002:2013 controls based on correlation events reported from ESM.

Executive Cyber Threat Overview

Provides a cyber threat overview for executives. The dashboard shows the top 5:

- Vulnerabilities
- MITRE ATT&CK techniques
- ArcSight categorized attacks
- Attacked assets

5 – Information Security Policies

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **ISO 27002** > *Dashboards* or *Reports* > **ISO 5 Information Security Policies**.

To assess your enterprise's compliance with this requirement, use the following dashboard and report:

Dashboards	Reports
Policy Violations Overview	Policy Violations

Policy Violations Overview

Provides an overview of policy violation events that involve Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 5.1.2.

Policy Violations

Provides a summary of policy violation events that involve Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 5.1.2.

6 – Organization of Information Security

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **ISO 27002** > *Dashboards* or *Reports* > **ISO 6 Organization of Information Security**.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
VPN Connection Overview Wireless Attacks and Suspicious Activity	Outbound Communication from Development to Production Environment Outbound Communication from Production to Development Environment VPN Connection Summary Wireless Attacks and Suspicious Activity

VPN Connection Overview

Provides an overview of VPN connection activity involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 6.2.2.

Before using this dashboard, ensure that variables `isAgentZoneSOX` and `isAgentAddressSOX` are defined in the SOX logical model. For more information, see the *Solutions Guide for ArcSight Insight Compliance Package for SOX*.

Wireless Attacks and Suspicious Activity

Provides an overview of wireless attacks and suspicious activity involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 6.2.1.

Outbound Communication from Development to Production Environment

Provides a summary of outbound communication events from development to production environments involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 6.1.2.

Before using this report, ensure that variables `isSourceZoneSOXDevelopment` and `isDestinationZoneSOXProduction` are defined in the SOX logical model. For more information, see the *Solutions Guide for ArcSight Insight Compliance Package for SOX*.

Outbound Communication from Production to Development Environment

Provides a summary of outbound communication events from production to development environments involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 6.1.2.

Before using this report, ensure that variables `isSourceZoneSOXProduction` and `isDestinationZoneSOXDevelopment` are defined in the SOX logical model. For more information, see the *Solutions Guide for ArcSight Insight Compliance Package for SOX*.

VPN Connection Summary

Provides a summary about VPN connection events which involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 6.2.2.

Before using this report, ensure that variables `isAgentZoneSOX` and `isAgentAddressSOX` are defined in the SOX logical model. For more information, see the *Solutions Guide for ArcSight Insight Compliance Package for SOX*.

Wireless Attacks and Suspicious Activity

Provides a summary of wireless attack and suspicious activity events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 6.2.1.

7 – Human Resource Security

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **ISO 27002** > **Reports** > **ISO 7 Human Resource Security**.

Activity by User

Provides an overview of activity by specific users involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Controls 7.1.1, 7.2.3 , and 7.3.1.

8 – Asset Management

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **ISO 27002** > **Reports** > **ISO 8 Asset Management**.

Removable Media Activity

Provides an overview of removable media activity involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 8.3.1.

9 – Access Control

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **SOX Reports** > **ISO 9 Access Control**.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
n/a	Account Creations Account Deletions Account Lockouts by System Account Lockouts by User Insecure Ports Insecure Services Password Policy Changes Password Weaknesses User Group Account Creations User Group Account Deletions

Account Creations

Provides a summary of account creation activity events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.2.1.

Account Deletions

Provides a summary of account deletion activity events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.2.1.

Account Lockouts by System

Provides a summary of account lockout activity events by system involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.2.1.

Account Lockouts by User

Provides a summary of account lockout activity events by user involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.2.1.

Insecure Ports

Provides a summary of insecure ports that are involved in communication with Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.1.2.

Insecure Services

Provides a summary of insecure services that are involved in communication with Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.1.2.

Password Policy Changes

Provides a summary of password policy change events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.4.3.

Password Weaknesses

Provides a summary of SQL vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.4.3.

User Group Account Creations

Provides a summary of user group account creation events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.2.1.

User Group Account Deletions

Provides a summary of user group account deletion events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.2.1.

10 – Cryptography

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **ISO 27002** > **Reports** > **ISO 10 Cryptography**.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
n/a	SSH Vulnerabilities SSL or TLS Vulnerabilities VPN Vulnerabilities

SSH Vulnerabilities

Provides a summary of SSH vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 10.1.1.

SSL or TLS Vulnerabilities

Provides a summary of SSL or TLS vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 10.1.1.

VPN Vulnerabilities

Provides a summary of VPN vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 10.1.1.

11 – Physical and Environmental Security

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **ISO 27002** > *Dashboards* or *Reports* > **ISO 11 Physical and Environmental Security**.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
Failed Physical Access Overview	Failed Building Physical Access Activity Summary
Successful Physical Access Overview	Failed User Physical Access Activity Summary
	Successful Building Physical Access Activity Summary
	Successful User Physical Access Activity Summary

Failed Physical Access Overview

Provides an overview of failed physical access activity events, relevant to ISO 27002:2013 Control 11.1.2.

Successful Physical Access Overview

Provides an overview of successful physical access activity events, relevant to ISO 27002:2013 Control 11.1.2.

Failed Building Physical Access Activity Summary

Provides a summary of failed physical access activity events by building, relevant to ISO27002:2013 control 11.1.2.

Failed User Physical Access Activity Summary

Provides a summary of failed physical access activity events by user, relevant to ISO27002:2013 control 11.1.2.

Successful Building Physical Access Activity Summary

Provides a summary of successful physical access activity events by building, relevant to ISO27002:2013 control 11.1.2.

Successful User Physical Access Activity Summary

Provides a summary of successful physical access activity events by user, relevant to ISO27002:2013 control 11.1.2.

12 – Operations Security

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **ISO 27002** > *Dashboards* or *Reports* > **ISO 12 Operations Security**.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
Administrative Login Overview	Antivirus Stopped or Paused
Application Vulnerabilities Overview	Audit Log Cleared
Failed Login Overview	Database Configuration Changes
Failed Login Relationship	Database Vulnerabilities
Firewall Configuration Changes	Failed Administrative Login Summary
Malware Overview	Failed Antivirus Updates
Successful Login Overview	Failed Login by SOX Asset
Unpatched Systems	Failed Login Summary
Vulnerability Overview	Firewall Configuration Changes
	High Risk Vulnerabilities
	Malware Summary
	Network Device Configuration Changes
	Overflow Vulnerabilities
	SQL Injection Vulnerabilities
	Successful Administrative Login Summary
	Successful Login by SOX Asset
	Unpatched Systems
	Vulnerability Summary by CVE ID
	Vulnerability Summary by SOX Asset
	Vulnerability Summary on SOX Environment
	XSRF Vulnerabilities
	XSS Vulnerabilities

Administrative Login Overview

Provides an overview of administrative login activity, relevant to ISO 27002:2013 Control 12.4.3.

To define administrative accounts, use the worksheet condition of this dashboard. Use lowercase to define the accounts. For example, add the user "Administrator" as "administrator."

Application Vulnerabilities Overview

Provides an overview of the following application vulnerabilities, relevant to ISO 27002:2013 Control 12.6.1:

- SQL injection
- XSS
- XSRF
- Overflow

Failed Login Overview

Provides an overview of failed login activity, relevant to ISO 27002:2013 Control 12.4.1.

Failed Login Relationship

Based on ArcSight categorization, provides an overview of failed login relationships involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.4.1.

Firewall Configuration Changes

Provides an overview of firewall configuration change events, relevant to ISO 27002:2013 Control 12.1.2.

Malware Overview

Provides an overview of malware activity, relevant to ISO 27002:2013 Control 12.2.1.

Successful Login Overview

Provides an overview of successful login activity, relevant to ISO 27002:2013 Control 12.4.1.

Unpatched Systems

Provides an overview of missing security patches on Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.5.1.

Vulnerability Overview

Provides an overview of vulnerability events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

Antivirus Stopped or Paused

Provides a summary of antivirus services that were stopped or paused, relevant to ISO 27002:20213 Control 12.4.1.

Audit Log Cleared

Provides a summary of audit log cleared events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.4.2.

Database Configuration Changes

Provides a summary of database configuration changes, relevant to ISO 27002:2013 Control 12.1.2.

Database Vulnerabilities

Provides a summary of database vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

Failed Administrative Login Summary

Provides a summary of failed administrative login events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.4.3.

To define administrative accounts, use the worksheet condition of this dashboard. Use lowercase to define the accounts. For example, add the user "Administrator" as "administrator."

Failed Antivirus Updates

Provides a summary of failed antivirus updates, relevant to ISO 27002:20213 Control 12.4.1.

Failed Login by SOX Asset

Provides a summary of failed logins detected on specific SOX assets , relevant to ISO 27002:2013 control 12.4.1.

When you run this report, specify the asset (host name, IP address, or MAC address) in lowercase.

Failed Login Summary

Provides a summary of failed login events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.4.1.

Firewall Configuration Changes

Provides a summary of firewall configuration change events, relevant to ISO 27002:2013 Control 12.1.2.

High Risk Vulnerabilities

Provides a summary of high-risk vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

Malware Summary

Provides a summary of malware events on Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.2.1.

Network Device Configuration Changes

Provides a summary of network device configuration change events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.1.2.

Overflow Vulnerabilities

Provides a summary of overflow vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

SQL Injection Vulnerabilities

Provides a summary of SQL vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

Successful Administrative Login Summary

Provides a summary of successful administrative login events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.4.3.

To define administrative accounts, use the worksheet condition of this dashboard. Use lowercase to define the accounts. For example, add the user "Administrator" as "administrator."

Successful Login by SOX Asset

Provides a summary of successful logins detected on specific SOX assets, relevant to ISO 27002:2013 control 12.4.1.

When you run this report, specify the asset (host name, IP address, or MAC address) in lowercase.

Unpatched Systems

Provides a summary of missing security patches involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.5.1.

Vulnerability Summary by CVE ID

Provides a summary of vulnerabilities detected on SOX environments by specific CVE ID, relevant to ISO 2700:2013 Control 12.6.1.

When you run this report, specify the CVE ID in lowercase.

Vulnerability Summary by SOX Asset

Provides a summary of vulnerabilities detected on specific SOX assets, relevant to ISO 27002:2013 Control 12.6.1.

When you run this report, specify the asset (host name, IP address, or MAC address) in lowercase.

Vulnerability Summary on SOX Environment

Provides a summary of vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

XSRF Vulnerabilities

Provides a summary of XSRF vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

XSS Vulnerabilities

Provides a summary of XSS vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

13 – Communications Security

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **ISO 27002** > *Dashboards* or *Reports* > **ISO 13 Communications Security**.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
DoS Activity	Covert Channel Activity
Firewall Blocked Events	DoS Attacks Summary
	Firewall Blocked Events

DoS Activity

Based on ArcSight categorization, provides an overview of DoS activity involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 13.2.3.

Firewall Blocked Events

Provides an overview of blocked firewall events, relevant to ISO 27002:2013 Control 13.2.1.

Covert Channel Activity

Displays covert channel activities, relevant to ISO 27002:2013 Control 13.2.1.

DoS Attacks Summary

Provides a summary of events that indicate DoS activity, relevant to ISO 27002:2013 Control 13.2.3.

Firewall Blocked Events

Provides a summary of blocked firewall events, relevant to ISO27002:2013 control 13.2.1

16 – Information Security Incident Management

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **ISO 27002** > *Dashboards* or *Reports* > **ISO 16 Information Security Incident Management**.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
High Risk Events Overview	High Risk Events Summary
MITRE ATT&CK Overview	MITRE ATT&CK Summary by MITRE Technique
Reconnaissance Activity	MITRE ATT&CK Summary by SOX Asset
Threat Overview	Reconnaissance Summary
Threat Relationship	Threats Summary

High Risk Events Overview

Provides an overview of high-risk events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

MITRE ATT&CK Overview

Provides an overview of MITRE ATT&CK events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

Reconnaissance Activity

Based on ArcSight categorization, provides an overview of reconnaissance activity involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

Threat Overview

Based on ArcSight categorization, provides an overview of threat activity involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

Threat Relationship

Based on ArcSight categorization, provides overview of threat relationships involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

High Risk Events Summary

Provides a summary of high-risk events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

MITRE ATT&CK Summary by MITRE Technique

Provides a summary of MITRE ATT&CK events involving Sarbanes Oxley systems by MITRE technique, relevant to ISO 27002:2013 Control 16.1.2.

MITRE ATT&CK Summary by SOX Asset

Provides a summary of MITRE ATT&CK events involving Sarbanes Oxley systems by target asset, relevant to ISO 27002:2013 Control 16.1.2.

Reconnaissance Summary

Provides a summary of reconnaissance events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

Threats Summary

Provides a summary of threat events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

17 – Information Security Aspects of Business Continuity Management

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **ISO 27002** > **Reports** > **ISO 17 Information Security Aspects of Business Continuity Management**.

Asset Shutdown Summary

Provides a summary of asset shutdown events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 17.1.3.

18 – Compliance

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **ISO 27002** > *Dashboards* or *Reports* > **ISO 18 Compliance**.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
Information Disclosure Vulnerabilities	Information Disclosure Vulnerabilities
Organization Information Leaks	Organization Information Leaks Summary
Personal Information Leakage Overview	Personal Information Leakage Summary

Information Disclosure Vulnerabilities

Provides an overview of information disclosure vulnerability events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Controls 18.1.4, 13.2.4.

Organization Information Leaks

Based on ArcSight categorization, provides an overview of information leakage activity (for example, company data), relevant to ISO 27002:2013 Controls 18.1.3, 13.2.4.

Personal Information Leakage Overview

Based on ArcSight categorization, provides an overview of personal information leakage activity, relevant to ISO 27002:2013 Controls 18.1.4, 13.2.4.

Information Disclosure Vulnerabilities - Dashboard

Provides a summary of information disclosure vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Controls 18.1.4, 13.2.4.

Organization Information Leaks Summary - Dashboard

Provides a summary of information leakage events (for example, company data leaks), relevant to ISO 27002:2013 Controls 18.1.3, 13.2.4.

Personal Information Leakage Summary - Dashboard

Provides a summary of personal information leakage events, relevant to ISO 27002:2013 Controls 18.1.4, 13.2.4.

Legal Notice

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/en-us/about/legal.