Micro Focus Security ArcSight Investigate

Software Version: 2.2

Query Quick Reference Guide

Document Release Date: June 29, 2018
Software Release Date: June 2018

Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Document Revision History

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition of a document, go to the ArcSight Product Documentation Community on Protect 724.

Types of Search Input Queries

To perform a search

Location: Search page > search field

1. Enter the desired query criteria (keywords or information for which you are searching).
2. Select the desired time range.
3. Click **Search**.

   ArcSight Investigate searches for data that matches the criteria that you specified and displays the results.

For details, see the *Micro Focus Security ArcSight Investigate User's Guide*.

Type	Description	Syntax
Full Text Search	Searches across all columns using a 'contains' operation to determine if the value is found.	<value> Example: `ssh`
Field-Based Search	Searches based on the field and operator designation to determine if the value is found in the specified field.	<key> <operator> <value> Example: `sourceAddress = 10.0.111.5`
Hashtag Search (preset searches)	These are predefined queries that are referenced in the search input field using a hashtag, plus the name. In addition to predefined searches, the session searches and save searches can be used in the input field using a hashtag prefix.	

Query syntax requirements

Behavior	Full text search	Field-based search	Hashtag search
Case sensitivity	Case-insensitive	Case-insensitive	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.

Behavior	Full text search	Field-based search	Hashtag search

Implicit Operators	When two values entered 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 following 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 Inner Join:
		`source address in list CustomListName_ CustomColumn Name`
		
		Syntax for 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. For example, “10:34:35”.	Use this format to specify a timestamp in a query:
		`YYYY-MM-DD`
		`YYYY-MM-DD HH:mm`
		`YYYY-MM-DD HH:mm:ss.fff`
		
		Use the in between >< , greater than (>) or less than (<) operators to narrow the time range.
			N/A

Search operators

The following table describes the operators you can specify in the **Search** field.

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

Operator	Operator Alternatives	Example
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

Group alias

Group aliases enable you to specify a group name to represent multiple columns of a specific type.

Group alias	Fields
`category`	List of all category fields
`custom float`	List of all custom float fields
`domain`	List of all domain fields
`hostname`	List of all hostname columns
`id`	List of all ID columns
`ip`	List of all IP address columns
`ip6`	List of all IPv6 address columns
`label`	List of all label columns
`mac`	List of all MAC address columns
`path`	List of all path columns
`port`	List of all port columns
`timestamp` or `time`	List of all time columns (device receipt time, agent receipt time)
`uri`	List of all URI columns
`url`	List of all URL columns
`username` or `user`	List of all user columns

Field aliases

Field aliases enable you to specify a field name by its alias.

Note: For the fields shown in the table, you can also use presentable field names, such as Agent Address. In fact, you are encouraged to use presentable names by ArcSight Investigate's suggestions.

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
applicationProtocol	app protocol
baseEventCount	cnt
bytesIn	in
bytesOut	out
categoryBehavior	behavior
categoryDeviceGroup	device group
categoryObject	object
categorySignificance	significance
categoryTechnique	technique

Field	Aliases
destinationAddress	dst destination ip destinationip dst ip dest ip target ip targetip target
destinationHostName	dhost destination name
destinationMacAddress	dmac destination mac
destinationNtDomain	dntdom
destinationPort	dpt destination port dstport dest port targetport target port
destinationProcessId	dpid
destinationProcessName	dproc
destinationTranslatedAddress	destination translated ip
destinationUserId	duid
destinationUserName	duser dst user dest user destination user dst usr
destinationUserPrivileges	dpriv
deviceAction	act
deviceAddress	dvc deviceaddr deviceip device ip
deviceCustomFloatingPoint1	cfp1
deviceCustomFloatingPoint1Label	cfp1Label
deviceCustomFloatingPoint2	cfp2
deviceCustomFloatingPoint2Label	cfp2Label

Field	Aliases
deviceCustomFloatingPoint3	cfp3
deviceCustomFloatingPoint3Label	cfp3Label
deviceCustomFloatingPoint4Label	cfp4Label
deviceCustomFloatingPoint4	cfp4
deviceCustomIPv6Address1	c6a1 device custom ipv6 1
deviceCustomIPv6Address1Label	c6a1Label
deviceCustomIPv6Address2	c6a2 device custom ipv6 2
deviceCustomIPv6Address2Label	c6a2Label
deviceCustomIPv6Address3	c6a3 device custom ipv6 3
deviceCustomIPv6Address3Label	c6a3Label
deviceCustomIPv6Address4	c6a4 device custom ipv6 4
deviceCustomIPv6Address4Label	c6a4Label
deviceCustomNumber1	cn1
deviceCustomNumber1Label	cn1Label
deviceCustomNumber2	cn2
deviceCustomNumber2Label	cn2Label
deviceCustomNumber3	cn3
deviceCustomNumber3Label	cn3Label
deviceCustomString1	Cs1
deviceCustomString1Label	cs1Label
deviceCustomString2	cs2
deviceCustomString2Label	cs2Label
deviceCustomString3	cs3
deviceCustomString3Labe	cs3Label
deviceCustomString4	cs4
deviceCustomString4Label	cs4Label
deviceCustomString5	cs5
deviceCustomString5Label	cs5Label

Field	Aliases
deviceCustomString6	cs6
deviceCustomString6Label	cs6Label
deviceEventCategory	cat
deviceHostName	dvchost
deviceMacAddress	dvcmac device mac
deviceProcessId	dvcpid
deviceReceiptTime	rt
deviceTimeZone	cat
deviceHostName	dvchost
deviceMacAddress	dvcmac device mac
deviceProcessId	dvcpid
deviceReceiptTime	rt
deviceTimeZone	dtz
deviceTranslatedAddress	device translated ip
endTime	end
eventOutcome	outcome
fileName	fname
fileSize	fsize
message	msg
requestUrl	request URL
sourceAddress	src source ip sourceip src ip
sourceHostName	shost
sourceMacAddress	smac source mac
sourceNtDomain	sntdomain

Field	Aliases
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

Send Documentation Feedback

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

Feedback on Query Quick Reference Guide (Investigate 2.2)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arcsight_doc@microfocus.com.

We appreciate your feedback!