



Cisco Secure Cloud Analytics

Query Syntax Reference



Table of Contents




Event Viewer Query Syntax	3
Query Syntax Options	3
Order of Evaluation	4
Query Syntax Examples	4
Event Viewer Nested Field Searches	8
Additional Resources	9
Contacting Support	10

Event Viewer Query Syntax

See the Lucene Query Syntax documentation for more information.

Query Syntax Options

You can use the following query syntax options:

Syntax Option	Syntax	Description
basic field/value evaluation	<code>field1: "value1"</code>	return results where <code>field1</code> equals <code>value1</code>
single character wildcard	<code>?</code>	any character matches this ? <div style="border: 1px solid #00a0e3; padding: 5px; margin-top: 10px;"> <p> Wildcard searches are only supported if the inline filter for a column accepts any alphanumeric string value.</p> </div>
multiple character wildcard	<code>*</code>	any number of any characters match this * <div style="border: 1px solid #00a0e3; padding: 5px; margin-top: 10px;"> <p> Wildcard searches are only supported if the inline filter for a column accepts any alphanumeric string value.</p> </div>
inclusive range search	<code>["value1" TO "value2"]</code>	return <code>value1</code> , <code>value2</code> , or any values in between
exclusive range search	<code>{"value1" TO "value2"}</code>	return any values between <code>value1</code> and <code>value2</code> , but not <code>value1</code> or <code>value2</code>
Boolean AND operator	<code>AND</code>	return results where both the evaluation before and after <code>AND</code> are true <div style="border: 1px solid #00a0e3; padding: 5px; margin-top: 10px;"> <p> If there is no syntax between two search parameters, the query will automatically interpret them as an AND.</p> </div>
Boolean	<code>OR</code>	return results where either the evaluation before or

Syntax Option	Syntax	Description
OR operator		after <code>OR</code> is true
Boolean NOT operator	<code>NOT</code>	return results where the evaluation before <code>NOT</code> is true, and after <code>NOT</code> is false
grouping	<code>()</code>	evaluate within the parentheses on their own
field grouping	<code>field1: ()</code>	evaluate multiple values and operators within the parentheses for a single field

Order of Evaluation



The system evaluates queries in the following order of precedence:

1. grouping, including `()` (parentheses), `[]` (inclusive range searches), and `{}` (exclusive range searches)
2. `:` (equals)
3. `NOT` Boolean operator
4. `AND` Boolean operator
5. `OR` Boolean operator

Query Syntax Examples

The following table provides generic query syntax examples.

Description	Example Syntax	Results Returned
one field, one value	<code>field1: "value1"</code>	all events where field1 equals value1
one field, one value, single character wildcard	<code>field1: "value?"</code>	all events where field1 equals "value?", where ? is any character
one field, one value, multiple character wildcard	<code>field1: "value*"</code>	all events where field1 equals "value*", where * is any number of any characters

Description	Example Syntax	Results Returned
one field, multiple values (field grouping)	<pre>field1: ("value*1" AND "value*2")</pre>	<p>all events where field1 contains value*1 and value*2</p> <div data-bbox="911 394 1417 678" style="border: 1px solid #00a0e3; padding: 10px;"> <p> When searching for multiple values in one field, we recommend that you use wildcards in each value to increase the likelihood of getting a matching result.</p> </div>
one field, either value	<pre>field1: ("value1" OR "value2")</pre>	<p>all events where field1 equals value1 or value2</p>
two fields, AND operator	<pre>field1: "value1" AND field2: "value2"</pre>	<p>all events where field1 equals value1 and field2 equals value2</p> <div data-bbox="911 934 1417 1255" style="border: 1px solid #00a0e3; padding: 10px;"> <p> If you do not explicitly define an operator between multiple field value evaluations, the system implicitly interprets the AND operator between the evaluations.</p> </div>
two fields, OR operator	<pre>field1: "value1" OR field2: "value2"</pre>	<p>all events where field1 equals value1 or field2 equals value2</p>
two fields, NOT operator	<pre>field1: "value1" AND NOT field2: "value2"</pre>	<p>all events where field1 equals value1 and field2 does not equal value2</p>
two fields, OR NOT operator	<pre>field1: "value1" OR NOT field2: "value2"</pre>	<p>all events where field1 equals value1 or field2 does not equal value2</p>
one field, inclusive range search	<pre>field1: ["value1" TO "value2"]</pre>	<p>all events where field1 equals value1, value2, or any value between</p>

Description	Example Syntax	Results Returned
one field, exclusive range search	<code>field1:{"value1" TO "value2"}</code>	all events where field1 equals any value between value1 and value2, but not value1 or value2
one field, mixed inclusive and exclusive range search	<code>field1:["value1" TO "value2"]</code>	all events where field1 equals value1, or any value between value1 and value2, but not value2
multiple fields, mixed operators	<code>field1: "value1" OR field2: "value2" AND field3: "value3"</code>	because the AND Boolean operator has greater precedence than the OR Boolean operator, all events where: <ul style="list-style-type: none"> field2 equals value2 and field 3 equals value 3, or field1 equals value1
multiple fields, mixed operators and parentheses	<code>(field1: "value1" OR field2: "value2") AND field3: "value3"</code>	because grouping has greater precedence than other operations and is evaluated first, all events where: <ul style="list-style-type: none"> field1 equals value1 or field 2 equals value2, and field3 equals value3

The following table lists query examples that a user may run for their deployment:

Description	Example Syntax	Results Returned
internal devices that established successful non-HTTPS connections with an internal	<code>Connected_ip: "192.168.105.28" AND IP: "192.168.0.0/16" AND NOT Port: "443" AND NOT Connected_ port: "443" AND Packets_from: { "10" TO * } AND Packets_to: { "10" TO * }</code>	all events with the following: <ul style="list-style-type: none"> IP equal to the internal CIDR range of 192.168.0.0/16

Description	Example Syntax	Results Returned
web server		<p>(internal entities),</p> <ul style="list-style-type: none"> • <code>Connected_ip</code> equal to <code>192.168.105.28</code> (the internal web server) • <code>Port</code> not equal to <code>443</code> (non-HTTPS traffic), • <code>Connected_port</code> not equal to <code>443</code> (non-HTTPS traffic), • <code>Packets_from</code> equal to <code>11</code> or more (successful connection, traffic passed), and • <code>Packets_to</code> equal to <code>11</code> or more (successful connection, traffic passed)
connections related to remote desktop applications	<pre>Port: ("23" OR "3389" OR ["5800" TO "5803"] OR ["5900" TO "5903"] OR ["6000" TO "6063"]) AND NOT Connected_port: ["0" TO "1023"] AND Packets_from: ["10" TO *] AND Packets_to: ["10" TO *]</pre>	<p>all events with the following:</p> <ul style="list-style-type: none"> • <code>Port</code> equal to <code>23</code>, <code>3389</code>, <code>5800-5803</code>, <code>5900-5903</code>, or <code>6000-6063</code> (common remote desktop application ports), • <code>Connected_port</code> not equal to <code>0-1023</code>

Description	Example Syntax	Results Returned
		<p>(connections using ephemeral ports),</p> <ul style="list-style-type: none"> • Packets_from equal to 10 or more (successful connection, traffic passed), and • Packets_to equal to 10 or more (successful connection, traffic passed)

Event Viewer Nested Field Searches

If an event contains fields with sub-fields, you can search for these field values in the query filter by using dot notation to specify a sub-field.

For example a line-item entry may contain a **Details** field with two sub-fields: **credentials** and **issues**. If you want to search for `username1` in the **credentials** field, use the following dot notation syntax:

```
Details.credentials: "username1"
```

Note that certain fields in different recommendations may contain different sub-fields for each recommendation type.

Additional Resources

For more information about Secure Cloud Analytics, refer to the following:

- <https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html> for a general overview
- <https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html> to sign up for a 60-day Free Trial
- <https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html> for documentation resources
- <https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html> for installation and configuration guides, including the Secure Cloud Analytics Initial Deployment Guide

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: <http://www.cisco.com/c/en/us/support/index.html>
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers:
<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>
- For Secure Cloud Analytics Free Trial customers, open a case by email: swatchc-support@cisco.com

Copyright Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

