

Event Search

The following topics describe how to search for events within a workflow:

- Event searches, on page 1

Event searches

An event search is a customizable query that

- retrieves specific information stored as events in database tables based on defined search criteria,
- can be saved with custom names and shared with other users or kept private for individual use, and
- returns only records that match the specified criteria for all fields in the search parameters.

Event search functionality

The system generates information that is stored as events in database tables. Events contain multiple fields that describe the activity that caused the appliance to generate the event. You can create and save searches customized for your environment for any of the different event types and save them to reuse later.

When you save a search you give it a name and specify whether the search will be available to you alone or to all users of the appliance. If you want to use the search as a data restriction for a custom user role, you **must** save it as a private search. If you previously saved a search, you can load it, make any necessary modifications, and then start the search. Custom analysis dashboard widgets, report templates, and custom roles can also use saved searches. If you have saved searches, you can delete them from the Search page.

For some event types, the system provides predefined searches that serve as examples and can provide quick access to important information about your network. You can modify fields within the predefined searches for your network environment, then save the searches to reuse later.

The search criteria you can use depends on the type of search, but the mechanics are the same. Searches return only records that match the search criteria specified for all fields.

Note Searching a custom table requires a slightly different procedure.

Related Topics

Search custom tables

Search constraints

A search constraint is a event data search feature that enables you to enter search criteria values to apply to fields defined for event tables and constrain the data displayed to your specific needs.

Each database table has its own search page where you can enter search constraint values to apply to fields defined for the table. Depending on the type of field, special syntax may be used to specify criteria such as wildcard characters or a range of numeric values.

Search results appear on workflow pages displaying each table field in columnar layout. Some database tables can additionally be searched using fields that are not displayed as columns on workflow pages. To determine whether such a constraint applies to your search results when viewing the results on a workflow page, click

Expand Arrow ( ) to view the active search constraints.

Best practice for general search constraints

When searching for events, consider these general guidelines:

- Many fields require wildcards for partial-match searches. All fields accept wildcards for these searches. For more information, refer to Wildcards and symbols in searches, on page 3.
- All fields accept negation (`!`).
- All fields accept comma-separated lists of search values. Records that contain any of the listed values in the specified field match that search criteria.
- All fields accept comma-separated lists enclosed in quotation marks as search values.
  - For fields that may contain only a single value, records with the specified field containing the exact string specified within the quotation marks match the search criteria. For instance, a search for `A, B, "C, D, E"` will match records where the specified field contains `"A"` or `"B"` or `"C, D, E"`. This permits matching on fields that include the comma in possible values.
  - For fields that may contain multiple values at the same time, records with the specified fields containing all of the values in the quote-enclosed comma-separated list match that search criteria.
  - For fields that may contain multiple values at the same time, search criteria may include single values as well as quote-enclosed comma-separated lists. For instance, a search for `A, B, "C, D, E"` on a field that may contain one of more of these letters matches records where the specified field contains `A` or `B`, or all of `C`, `D`, and `E`.
- Specify `n/a` in any field to identify events where information is not available for that field; use `!n/a` to identify the events where that field is populated.
- You can precede many numeric fields with greater than (`>`), greater than or equal to (`>=`), less than (**<**), less than or equal to (`<=`), equal to (`=`), or not equal to (`<>`) operators.

Note When you search a field with long complicated values (such as SHA-256 hash values), copy the search criteria value from source material and paste it into the appropriate field on the search page.

Wildcards and symbols in searches

When searching in all text fields in connection and Security Intelligence events and in most text fields in other event types, searches for partial matches in text fields require an asterisk (*) to represent unspecified characters in a string. Searches without an asterisk are exact-match searches in these fields. Even in fields that do not require wildcards, we recommend always using wildcards for partial-match searches.

For example, to find `example.com`, `www.example.com`, or `department.example.com`, search for `*.example.com`. Searching for `example.com` in most cases returns only `example.com`.

Search for non-alphanumeric characters

If you want to search for non-alphanumeric characters (including the asterisk character), enclose the search string in quotation marks. For example, to search for the string:

```
Find an asterisk (*)
```

enter:

```
"Find an asterisk (*)"
```

Objects and application filters in searches

The system allows you to create named objects, object groups, and application filters that can be used as part of your network configuration. You can use these objects, groups, and filters as search criteria when performing or saving searches.

When you perform a search, objects, object groups, and application filters appear in the format, `${object_name}`. For example, a network object with the object name `ten_ten_network` appears as `${ten_ten_network}` in a search.

Click the **Object** (+) icon that appears next to a search field to use an object as a search criterion.

Related Topics

Use the object manager

Time constraints in searches

The formats accepted by search criteria fields that take a time value are shown in the tables that follow.

Table 1: Time specification in search fields

Time formats	Example
`today [at HH:MMam|PM]`	`today` `today at 12:45pm`
`YYYY-DDMM-HH:MM:SS`	`2006-03-22 14:22:59`

You can precede a time value with one of the operators shown in this table:

Table 2: Time specification operators

Operator	Example	Explanation
<	`< 2006-03-22 14:22:59`	Returns events with a timestamp before 2:23 PM, March 22, 2006.
>	`> today at 2:45pm`	Returns events with a timestamp later than today at 2:45 PM.

IP addresses in searches

When specifying IP addresses in searches, you can enter an individual IP address, a comma-separated list of addresses, an address block, or a range of IP addresses separated with a hyphen (-). You can also use negation.

When you search for hosts by IP address, the results include all hosts for which at least one IP address matches your search conditions, that is, a search for an IPv6 address may return hosts whose primary address in IPv4.

When you use CIDR or prefix length notation to specify a block of IP addresses, the system uses only the portion of the network IP address specified by the mask or prefix length. For example, if you type `10.1.2.3/8`, the system uses `10.0.0.0/8`.

Table 3: Acceptable IP address syntax

To specify...	Type...	For example...
a single IP address	the IP address.	`192.168.1.1` `2001:db8::abcd`
multiple IP addresses using a list	a comma-separated list of IP addresses. Do not add a space before or after the commas.	`192.168.1.1,192.168.1.2` `2001:db8::b3ff,2001:db8::0202`
a range of IP addresses that can be specified with a CIDR block or prefix length	the IP address block in IPv4 CIDR or IPv6 prefix length notation.	`192.168.1.0/24` This specifies any IP in the 192.168.1.0 network with a subnet mask of 255.255.255.0, that is, 192.168.1.0 through 192.168.1.255.
a range of IP addresses that cannot be specified with a CIDR block or prefix	the IP address range using a hyphen. Do not add a space before or after the hyphen.	`192.168.1.1-192.168.1.5` `2001:db8::0202-2001:db8::8329`

negation of any of the other ways to specify IP addresses or ranges of IP addresses	an exclamation point in front of the IP address, block, or range.	`192.168.0.0/32,!192.168.1.10`
		`!2001:db8::/32`
		`!192.168.1.10,!2001:db8::/32`

Related Topics

IP address conventions

URLs in searches

When searching for URLs, include wildcards. For example, use **`*example.com*`** to find all variations of the domain, such as **`https://example.com`** and **`division.example.com`** and **`example.com/division/`**.

Managed devices in searches

When you group devices—whether just on the Firewall Management Center, or as actual high availability or scalability configurations—searching for the name for the group correctly returns results for all devices in the group.

If the system finds a match for a group, it replaces the group name with the appropriate member device names for the purpose of performing the search. When you save a search that uses a device group in the device field the system saves the name specified in the device field and performs the device name replacement again each time the search is executed.

Ports in Searches

The system accepts specific syntax for port numbers in searches. You can enter:

- a single port number
- a comma-separated list of port numbers
- two port numbers separated by a dash to represent a range of port numbers
- a port number followed by a protocol abbreviation, separated by a forward slash (only when searching for intrusion events)
- a port number or range of port numbers preceded by an exclamation mark to indicate a negation of the specified ports



Note Do **not** use spaces when specifying port numbers or ranges.

Table 4: Port Syntax Examples

Example	Description
`21`	Returns all events on port 21, including TCP and UDP events.
`!23`	Returns all events except those on port 23.
`25/tcp`	Returns all TCP-related intrusion events on port 25.
`21/tcp,25/tcp`	Returns all TCP-related intrusion events on ports 21 and 25.
`21-25`	Returns all events on ports 21 through 25.

Perform a search

Search for specific events or data records within the system to analyze health events, and other types of monitored data.

Procedure

Step 1 From the table drop-down list, select the type of event or data to search.

Step 2 Enter your search criteria in the appropriate fields.

Step 3 If you want to use the search again in the future, save the search as described in Save a search, on page 6.

Step 4 Click **Search** to start the search.

Your search results appear in the default workflow for the table you are searching, constrained by time (if applicable).

Related Topics

Configure event view settings

Save a search

Save search criteria for future use to streamline repeated searches and maintain consistent filtering parameters.

Before you begin

- Establish search criteria as described in Perform a search, on page 6, or load a saved search as described in Load a saved search, on page 6.

Procedure

Step 1 From the Search page, if you want to save the search as private so only you can access it, check the **Private** checkbox.

Step 2 You have these options:

- To save a new version of a loaded search, click **Save As New**.
- To save a new search, or overwrite a custom search using the same name, click **Save**.

Load a saved search

Load a saved search to quickly access previously configured search criteria without having to recreate the search constraints.

Procedure

Step 1 From the table drop-down list, choose the type of event or data to search.

Step 2 Choose the search you want to load from the **Custom Searches** list or the **Predefined Searches** list.

Step 3 If you want to use different search criteria, change the search constraints.

Step 4 If you want to use a changed search again in the future, save the search as described in Save a search, on page 6.

Step 5 Click **Search**.