# Event Search

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



# Event Searches

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**

Searching Custom Tables

## Search Constraints

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.

## General Search Constraints

When searching for events, observe the following general guidelines:

- Many fields require wildcards for partial-match searches. All fields accept wildcards for these searches.

  See Wildcards and Symbols in Searches, on page 2.

- 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.

**Tip** When searching a field with long complicated values (such as SHA-256 hash values), you can 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`.

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.

You can click **Object** (+) that appears next to a search field where you can use an object as a search criterion.

### Related Topics

The Object Manager

## Time Constraints in Searches

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

***Table 1: Time Specification in Search Fields***

| Time Formats | Example |
|---|---|
| `today [at HH:MMam\|pm]` | `today`<br>`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 following operators:

***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.

For searches that support IPv6 (such as intrusion event, connection data, and correlation event searches) you can enter IPv4 and IPv6 addresses and CIDR/prefix length address blocks in any combination. 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`.

Because IP addresses can be represented by network objects, you can also click the add network **Object** (+) that appears next to an IP address search field to use a network object as an IP address search criterion.

***Table 3: Acceptable IP Address Syntax***

| To specify... | Type... | For example... |
|---|---|---|
| a single IP address | the IP address. | `192.168.1.1`<br>`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`<br>`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`<br>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`<br>`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`<br>`!2001:db8::/32`<br>`!192.168.1.10,!2001:db8::/32` |
| hosts that are blocked or monitored (but would have been blocked)<br>See Host Profile Icons. | In connection and Security Intelligence events, in Initiator IP and Responder IP fields:<br>• block<br>• monitor | -- |

**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

If you group devices—whether just on the 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. |

## Event Fields in Searches

When searching for events, you can use the following fields as search criteria:

- Audit Log Workflow Fields
- Application Data Fields
- Application Detail Data Fields
- Captured File Fields

- Allow List Event Fields
- Connection and Security-Related Connection Event Fields
- Correlation Event Fields
- Discovery Event Fields
- The Health Events Table
- Host Attribute Data Fields
- Host Data Fields
- File and Malware Event Fields
- Intrusion Event Fields
- Intrusion Rule Update Log Details
- Remediation Status Table Fields
- See *Nmap Scan Results Fields* in the Cisco Secure Firewall Management Center Device Configuration Guide
- Server Data Fields
- Third-Party Vulnerability Data Fields
- User-Related Fields
- Vulnerability Data Fields
- Allow List Violation Fields

# Performing a Search

You must have Admin or Security Analyst privileges to perform a search.

### Procedure

**Step 1** Select **Analysis** > **Search**.

**Tip**
You may also click **Search** from any page on a workflow.

**Step 2** From the table drop-down list, select the type of event or data to search.

**Step 3** Enter your search criteria in the appropriate fields. See the following sections for detailed information on the search criteria you can use:

- Search Constraints, on page 1
- Audit Log Workflow Fields
- Application Data Fields

- Application Detail Data Fields
- Captured File Fields
- Allow List Event Fields
- Connection and Security-Related Connection Event Fields
- Correlation Event Fields
- Discovery Event Fields
- The Health Events Table
- Host Attribute Data Fields
- Host Data Fields
- File and Malware Event Fields
- Intrusion Event Fields
- Intrusion Rule Update Log Details
- Remediation Status Table Fields
- See *Nmap Scan Results Fields* in the Cisco Secure Firewall Management Center Device Configuration Guide
- Server Data Fields
- Third-Party Vulnerability Data Fields
- User Data Fields
- User Activity Data Fields
- Vulnerability Data Fields
- Allow List Violation Fields

**Step 4** If you want to use the search again in the future, save the search as described in Saving a Search, on page 7.

**Step 5** 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).

### What to do next

- To analyze the search results using workflows, see Using Workflows.

### Related Topics

Configuring Event View Settings

# Saving a Search

You must have Admin or Security Analyst privileges to save a search.

In a multidomain deployment, the system displays saved searches created in the current domain, which you can edit. It also displays searches saved in ancestor domains, which you cannot edit. To view and edit searches created in a lower domain, switch to that domain.

### Before you begin

- Establish search criteria as described in Performing a Search, on page 6, or load a saved search as described in Loading a Saved Search, on page 8.

### 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.

**Tip**
If you want to use the search as a data restriction for a custom user role, you **must** save it as a private search.

**Step 2** You have two options:

- If you want to save a new version of a loaded search, click **Save As New**.
- If you want to save a new search, or overwrite a custom search using the same name, click **Save**. If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

# Loading a Saved Search

You must have Admin or Security Analyst privileges to load a saved search.

In a multidomain deployment, the system displays saved searches created in the current domain, which you can edit. It also displays searches saved in ancestor domains, which you cannot edit. To view and edit searches created in a lower domain, switch to that domain.

### Procedure

**Step 1** Choose **Analysis** > **Search**.

**Tip**
You may also click **Search** from any page on a workflow.

**Step 2** From the table drop-down list, choose the type of event or data to search.

**Step 3** Choose the search you want to load from the **Custom Searches** list or the **Predefined Searches** list.

**Step 4** If you want to use different search criteria, change the search constraints.

**Step 5** If you want to use a changed search again in the future, save the search as described in Saving a Search, on page 7.

**Step 6** Click **Search**.

# Query Overrides Via the Shell

System administrators can use a Linux shell-based query management tool to locate and stop long-running queries.

The query management tool allows you to locate queries running longer than a specified number of minutes and stop those queries. The tool logs an event to the audit log and to syslog when you stop a query.

Note that the `admin` internal user can access the management center CLI. If you use an external authentication object which grants CLI access, users matching the shell access filter can also log into the CLI.

**Note** Leaving the search page in the web interface does not stop a query. Queries that take a long time to return results impact overall system performance while the query is running.

## Shell-Based Query Management Syntax

Use the following syntax to manage long-running queries:

```
query_manager [-v] [-l [minutes]] [-k query_id [...]] [--kill-all minutes]
```

***Table 5: `query_manager` Options***

| Option | Description |
|---|---|
| `-h, --help` | Prints a brief help message. |
| `-l, --list [minutes]` | Lists all queries taking longer than passed-in minutes. By default it will show all queries taking longer than 1 minute. |
| `-k, --kill query_id [...]` | Kills the query with the passed-in id. The option can take multiple ids. |
| `--kill-all minutes` | Kills all queries taking longer than passed-in minutes. |
| `-v, --verbose` | Verbose output including full SQL queries. |

**Caution** For system security reasons, Cisco strongly recommends that you not establish additional Linux shell users on any appliance.

## Stopping Long-Running Queries

You must be the **admin** user or externally authenticated user with CLI access

### Procedure

**Step 1** Connect to the Secure Firewall Management Center via `ssh`.

**Step 2** Use the CLI `expert` command to access the Linux shell.

**Step 3** Run `query_manager` under `sudo` using the syntax described in Shell-Based Query Management Syntax, on page 9.

# History for Searching for Events

| Feature | Minimum Management Center | Minimum Threat Defense | Details |
|---|---|---|---|
| Partial-match searches in many fields now require wildcards | 6.6 | Any | For example, when searching for URLs, use **`*example.com*`** to find all variations of **`example.com`**.<br>This behavior change applies to searches on the **Analysis > Search** page, when searching for connection or Security Intelligence events. This search page can also be accessed via links on other pages.<br>In fields that do not require wildcards for partial-match searches, they can optionally be used.<br>Affected Platforms: management center |