

Lookups

The following topics explain how to look up information about entities that may or may not be known to the system:

- Lookups in Firewall Management Center, on page 1
- Requirements for using lookups, on page 1
- Lookup IP address details using Whois, on page 1
- Check the category and reputation of the URLs, on page 2
- Find geolocation information for an IP address, on page 3

Lookups in Firewall Management Center

The lookup feature in Firewall Management Center enables you to find this information:

- Regional Internet Registries (RIR) information (Whois) for any IP address.
- URL category and reputation as classified by the URL Filtering feature.
- Geolocation information for any IP address, including country name, country code, and continent name.

Requirements for using lookups

Before using the manual lookup features in the Firewall Management Center, ensure you meet these requirements.

- You must have **Administrator**, **Security Analyst**, or **Security Analyst (Read only)** privileges to access the lookup features.
- Make sure the Firewall Management Center has Internet access. For more information, refer to Communication Ports and Internet Access.

Lookup IP address details using Whois

Use Whois lookups to investigate the ownership and registration details of an IP address for security and network analysis.

Procedure

Step 1 Choose **Events & Logs** > **+ Show more** > **Advanced** > **Whois**.

Step 2 Enter an IP address you want to investigate and click **Search**.

Check the category and reputation of the URLs

Use this feature to see how particular URLs are evaluated in order to plan, adjust, or troubleshoot policy processing, or to investigate potentially problematic URLs that come to your attention via sources outside your Cisco solution.

The categories and reputations in these results are the same as those that are used by the **URL Filtering** feature.

Before you begin

- URL Filtering and the **Query Cisco cloud for unknown URLs** option must be enabled. See the *URL Filtering* chapter in the *Cisco Secure Firewall Management Center Device Configuration Guide*.
- At least one device must be registered to the Firewall Management Center and have a valid URL Filtering license assigned to it.

Procedure

Step 1 Select **Events & Logs** > **+ Show more** > **Advanced** > **URL Lookup**.

Step 2 Enter one or more URLs or public, routable IP addresses, in any common format (with or without "http", "www", or subdomains; shortened URLs are also accepted).

- Use space or a new line to separate each entry.
- Wildcards such as asterisks (*) are not supported.

Step 3 Click **Search**.

- If you enter many URLs and your network is slow, processing may take several minutes.
- If you see an error message that the URL is not valid, check your spelling or try a different variation of the URL. For example, add or omit the "www" or "http" or "https" prefix.
- A URL may belong to up to six categories but has only one reputation.

Step 4 Sort the results by clicking a column heading. This is optional.

Step 5 To save the results as a CSV file, click **Export CSV**. This is optional.

The CSV file includes an additional column for reputation level so you can sort by risk. Zero (0) means the risk is unknown for URLs with insufficient data.

What to do next

If you want to view lists of possible categories and reputations, go to **Policies** > **Security policies** > **Access Control**, click a policy or add a new one, click **Add Rule**, then click **URLs**.

Find geolocation information for an IP address

Use the geolocation lookup feature to find the country name, ISO 3166-1 three-letter country code, and continent name associated with any IP address.

To ensure that you are using up-to-date geolocation information, update the Geolocation Database (GeoDB) on your Firewall Management Center regularly.

Procedure

Step 1 Choose **Events & Logs** > **+ Show more** > **Advanced** > **Geolocation Lookup**.

Step 2 Enter one or more IP addresses and click **Search**.

- You may specify IPv4 addresses, IPv6 addresses, or both.
- Separate multiple addresses using a comma, semicolon, space, or new line.

Step 3 To sort the data, click the column titles. This is optional.

Step 4 Click **Export CSV** to save the results as a CSV file. This is optional.