

Using Lookups

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

- Introduction to Lookups, on page 1
- Performing Whois Lookups, on page 1
- Finding URL Category and Reputation, on page 2
- Finding Geolocation Information for an IP Address, on page 3

Introduction to Lookups

If your Firepower Management Center is connected to the Internet, you can use manual lookup features to find the following information:

- Regional Information 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: country name, country code, and continent name. (To ensure that you are using up-to-date geolocation information, Cisco strongly recommends that you regularly update the Geolocation Database (GeoDB) on your Firepower Management Center.)

Related Topics

Update the Geolocation Database

Performing Whois Lookups

Before you begin

- Ensure that the Firepower Management Center has Internet access; see Security, Internet Access, and Communication Ports.

Procedure

Step 1 Choose **Analysis** > **Lookup** > **Whois**.

Step 2 Enter an IP address and click **Search**.

Related Topics

The Context Menu

Finding URL Category and Reputation

You can manually look up category and reputation of 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

- The Firepower Management Center must have Internet access; see Security, Internet Access, and Communication Ports.
- URL Filtering and the **Query Cisco CSI for Unknown URLs** option must be enabled. See Enable URL Filtering Using Category and Reputation and URL Filtering Options.
- You must be an Admin or Security Analyst user to perform this task.

Procedure

Step 1 Select **Analysis** > **Lookup** > **URL**.

Step 2 Enter up to 250 URLs and public, routable IP addresses, in any common format (for example, URLs may be with or without "http", "www", or a subdomain, or may be shortened). Separate each entity with a space or a return.

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 (Optional) Sort the results by clicking a column heading.

Step 5 (Optional) To save the results as a CSV file, click **Export CSV**.

An additional column for reputation level is included in the CSV file so you can sort by risk. Zero (0) represents an unknown risk, for a URL for which the system has insufficient risk data.

What to do next

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

Finding Geolocation Information for an IP Address

You can use the geolocation lookup feature to find the country name, ISO 3166-1 three-digit country code, and continent name associated with any IP address.

Procedure

Step 1 Choose **Analysis** > **Lookup** > **Geolocation**.

Step 2 To view the geolocation information for one or more IP addresses, enter the address or addresses and click **Search**. You may specify IPv4 addresses, IPv6 addresses, or both. Use a comma, semicolon, return, or any white space character to separate multiple addresses.

Tip Click **Clear** to clear the text box.

Step 3 Optionally, click the column titles to sort the data. You can sort by any field except IP Address.

Step 4 (Optional) To save the results as a CSV file, click **Export CSV**.

Related Topics

Update the Geolocation Database