



# URL Filtering

---

- [URL Filtering Overview, on page 1](#)
- [Best Practices for URL Filtering, on page 2](#)
- [Guidelines and Limitations for URL Filtering, on page 3](#)
- [How to Configure URL Filtering with Category and Reputation, on page 5](#)
- [Configure URL Filtering Health Monitors, on page 10](#)
- [Manual URL Filtering, on page 10](#)
- [Troubleshoot URL Filtering, on page 11](#)
- [History for URL Filtering, on page 13](#)

## URL Filtering Overview

Use the URL filtering feature to control the websites that users on your network can access:

- **Category and reputation-based URL filtering**—With a URL Filtering license, you can control access to websites based on the URL's general classification (category) and risk level (reputation). This is the recommended option.
- **Manual URL filtering**—With any license, you can manually specify individual URLs, groups of URLs, and URL lists and feeds to achieve granular, custom control over web traffic. For more information, see [Manual URL Filtering, on page 10](#).

## About URL Filtering with Category and Reputation

With a URL Filtering license, you can control access to websites based on the category and reputation of requested URLs:

- **Category**—A general classification for the URL. For example, ebay.com belongs to the Auctions category, and monster.com belongs to the Job Search category.

A URL can belong to more than one category.

- **Reputation**—How likely the URL is to be used for purposes that might be against your organization's security policy. Reputations range from High Risk (level 1) to Well Known (level 5).

### Benefits of Category and Reputation-Based URL Filtering

URL categories and reputations help you quickly configure URL filtering. For example, you can use access control to block high-risk URLs in the Hacking category. Or, you can use QoS to rate limit traffic from sites in the Streaming Media category. There are also categories for types of threats, such as a Spyware and Adware category.

Using category and reputation data simplifies policy creation and administration. It grants you assurance that the system controls web traffic as expected. Because Cisco continually updates its threat intelligence with new URLs, as well as new categories and risks for existing URLs, the system uses up-to-date information to filter requested URLs. Sites that (for example) represent security threats, or that serve undesirable content, may appear and disappear faster than you can update and deploy new policies.

Some examples of how the system can adapt include:

- If an access control rule blocks all gaming sites, as new domains get registered and classified as Games, the system can block those sites automatically. Similarly, if a QoS rule rate limits all streaming media sites, the system can automatically limit traffic to new Streaming Media sites.
- If an access control rule blocks all malware sites and a shopping page gets infected with malware, the system can recategorize the URL from Shopping to Malware Sites and block that site.
- If an access control rule blocks high-risk social networking sites and somebody posts a link on their profile page that contains links to malicious payloads, the system can change the reputation of that page from Benign Sites to High Risk and block it.

### Related Topics

[Snort® Restart Scenarios](#)

## URL Filtering Data from the Cisco Cloud

URL filtering based on category and reputation requires a data set provided by Cisco Collective Security Intelligence (Cisco CSI), a cloud service.

Generally, by default, when a valid URL Filtering license is applied to an active device, the URL category and reputation data set is downloaded from the Cisco cloud to the Firepower Management Center and pushed to devices. This locally stored data set is updated periodically.

When a user on the network accesses a URL, the system looks for a match in the local (downloaded) data set. If there is no match, the system checks a cache of results that the system previously looked up in the Cisco cloud. If there is still no match, the system looks up the URL in the Cisco cloud and adds the result to the cache.

## Best Practices for URL Filtering

- Use category and reputation-based URL filtering, not manual filtering
- Follow the steps in [How to Configure URL Filtering with Category and Reputation, on page 5](#)
- Carefully review the [Guidelines and Limitations for URL Filtering, on page 3](#)

# Guidelines and Limitations for URL Filtering

## Limitations to URL Identification

The system cannot filter URLs before:

- A monitored connection is established between a client and server.
- The system identifies the HTTP or HTTPS application in the session.
- The system identifies the requested URL (for encrypted sessions, from either the ClientHello message or the server certificate).

This identification should occur within 3 to 5 packets, or after the server certificate exchange in the TLS/SSL handshake if the traffic is encrypted.

If early traffic matches all other rule conditions but identification is incomplete, the system allows the packet to pass and the connection to be established (or the TLS/SSL handshake to complete). After the system completes its identification, the system applies the appropriate rule action to the remaining session traffic.

For access control, these passed packets are inspected by the access control policy's *default* intrusion policy—not the *default action* intrusion policy nor the almost-matched rule's intrusion policy.

## URL Conditions and Rule Order

- For the most effective URL matching, place rules that include URL conditions before other rules, including application rules, particularly if the URL rules are block rules and the other rules meet both of the following criteria:
  - They include application conditions.
  - The traffic to be inspected is encrypted.
- URLs can belong to more than one category. It is possible to want to allow one category of websites and block another—whether explicitly or by relying on the default action. In this case, make sure you create and order URL rules so you get the desired effect, depending on whether the allow or the block should take precedence.

For additional guidelines for rules, see the [Rule Management: Common Characteristics](#) chapter, including the following topics: [Rule Condition Mechanics](#) and [Rule Performance Guidelines](#).

## Uncategorized or Reputationless URLs

When you build a URL rule, you first choose the category you want to match. If you explicitly choose **Uncategorized** URLs, you cannot further constrain by reputation.

If the system does not know the category and reputation of a URL, browsing to that website does not match rules with category and reputation-based URL conditions. You cannot manually assign categories and reputations to URLs, but in access control and QoS policies, you can manually block specific URLs. See [Manual URL Filtering, on page 10](#).

## URL Filtering for Encrypted Web Traffic

When performing URL filtering on encrypted web traffic, the system:

- Disregards the encryption protocol; a rule matches both HTTPS and HTTP traffic if the rule has a URL condition but not an application condition that specifies the protocol.
- Does not use URL lists. You must use URL objects and groups instead.
- Matches HTTPS traffic based on the subject common name in the public key certificate used to encrypt the traffic, and also evaluates the reputation of any other URLs presented at any time during the transaction, including the post-decryption HTTP URL.
- Disregards subdomains within the subject common name.
- Does not display an HTTP response page for encrypted connections blocked by access control rules (or any other configuration); see [Limitations to HTTP Response Pages](#).

## HTTP/2

The system can extract HTTP/2 URLs from TLS certificates, but not from a payload.

## Search Query Parameters in URLs

The system does not use search query parameters in the URL to match URL conditions. For example, consider a scenario where you block all shopping traffic. In that case, using a web search to search for amazon.com is not blocked, but browsing to amazon.com is.

## URL Filtering in High Availability Deployments

For guidelines for URL filtering with Firepower Management Centers in high availability, see [URL Filtering and Security Intelligence](#).

## Memory Limitations for Selected Device Models

- If you are using NGIPSv, see the [Cisco Firepower NGIPSv Quick Start Guide for VMware](#) for information on allocating the correct amount of memory to perform category and reputation-based URL filtering.
- Device models with less memory store less URL data locally, and the system may therefore check the cloud more frequently to determine category and reputation for sites that are not in the local database.

Lower-memory devices include:

- 7100 series
- ASA 5508-X and ASA 5516-X
- ASA 5515-X and ASA 5525-X

## Manual URL Filtering

When manually filtering specific URLs, carefully consider other traffic that might be affected. To determine whether network traffic matches a URL condition, the system performs a simple substring match. If the requested URL matches any part of the string, the URLs are considered to match.

## Related Topics

[The Default Intrusion Policy](#)

## Filtering HTTPS Traffic

To filter encrypted traffic, the system determines the requested URL based on information passed during the TLS/SSL handshake: the subject common name in the public key certificate used to encrypt the traffic.

HTTPS filtering, unlike HTTP filtering, disregards subdomains within the subject common name. Do not include subdomain information when manually filtering HTTPS URLs in access control or QoS policies. For example, use `example.com` rather than `www.example.com`.

HTTPS filtering also does not support URL lists. You must use URL objects and groups instead.



**Tip** In an SSL policy, you can handle and decrypt traffic to specific URLs by defining a distinguished name SSL rule condition. The common name attribute in a certificate's subject distinguished name contains the site's URL. Decrypting HTTPS traffic allows access control rules to evaluate the decrypted session, which improves URL filtering.

### Controlling Traffic by Encryption Protocol

The system disregards the encryption protocol (HTTP vs HTTPS) when performing URL filtering in access control or QoS policies. This occurs for both manual and reputation-based URL conditions. In other words, URL filtering treats traffic to the following websites identically:

- `http://example.com/`
- `https://example.com/`

To configure a rule that matches only HTTP or HTTPS traffic, add an application condition to the rule. For example, you could allow HTTPS access to a site while disallowing HTTP access by constructing two access control rules, each with an application and URL condition.

The first rule allows HTTPS traffic to the website:

Action: Allow  
 Application: HTTPS  
 URL: `example.com`

The second rule blocks HTTP access to the same website:

Action: Block  
 Application: HTTP  
 URL: `example.com`

## How to Configure URL Filtering with Category and Reputation

	Do This	More Information
Step 1	If you will use category and reputation-based URL filtering on an NGIPSv device, allocate the required amount of memory.	<a href="#">Cisco Firepower NGIPSv Quick Start Guide for VMware</a>

	Do This	More Information
Step 2	Ensure that you have the correct licenses.	<p><a href="#">Licensing the Firepower System</a>, including: .</p> <ul style="list-style-type: none"> <li>• <a href="#">URL Filtering Licenses for Firepower Threat Defense Devices</a></li> <li>• <a href="#">URL Filtering Licenses for Classic Devices</a></li> </ul> <p>Assign the URL Filtering license to each managed device that will filter URLs.</p> <p>In order to enable the feature, at least one managed device must have a URL Filtering license assigned to it.</p>
Step 3	Ensure that your Firepower Management Center can communicate with the cloud to obtain URL filtering data.	<a href="#">Internet Access Requirements</a> and <a href="#">Communication Port Requirements</a> .
Step 4	Understand limitations and guidelines and take any necessary actions.	<a href="#">Guidelines and Limitations for URL Filtering</a> , on page 3
Step 5	Enable the URL Filtering feature.	<a href="#">Enable URL Filtering Using Category and Reputation</a> , on page 6
Step 6	Configure policies to filter URLs by category and reputation.	<a href="#">Configuring URL Conditions</a> , on page 8
Step 7	(Optional) Allow users to bypass a website block by clicking through a warning page.	<a href="#">HTTP Response Pages and Interactive Blocking</a>
Step 8	Order your rules so that traffic hits key rules first.	<a href="#">URL Rule Order</a>
Step 9	(Optional) Change handling of URLs that require cloud lookups.	Information about the <b>Retry URL cache miss lookup</b> option in <a href="#">Access Control Policy Advanced Settings</a> .
Step 10	Deploy your changes.	<a href="#">Deploy Configuration Changes</a>
Step 11	Ensure that your system receives future URL data updates as expected.	<a href="#">Configure URL Filtering Health Monitors</a> , on page 10

## Enable URL Filtering Using Category and Reputation

Smart License	Classic License	Supported Devices	Supported Domains	Access
URL Filtering	URL Filtering	Any	Any	Admin

### Before you begin

Complete prerequisites described in [How to Configure URL Filtering with Category and Reputation](#), on page 5.

- 
- Step 1** Choose **System > Integration**.
  - Step 2** Click **Cloud Services**.
  - Step 3** Configure [URL Filtering Options](#), on page 7.
  - Step 4** Click **Save**.
- 

## URL Filtering Options

The following options are on the **System > Integration** page:

### Enable URL Filtering

Allows traffic filtering based on a website's general classification, or category, and risk level, or reputation. Adding a URL Filtering license automatically enables **Enable URL Filtering**. URL filtering must be enabled before you can choose other URL filtering options.

When you enable URL filtering, depending on how long since URL filtering was last enabled, or if this is the first time you are enabling URL filtering, the Firepower Management Center downloads URL data from Cisco Collective Security Intelligence (Cisco CSI). This process may take some time.

### Enable Automatic Updates

Options for updating URL filtering threat data:

- If you enable the **Enable Automatic Updates** option on the **System > Integration** page, the Firepower Management Center checks the cloud every 30 minutes for updates. This option is enabled by default when you add a URL filtering license.
- If you need strict control over when the system contacts external resources, disable automatic updates on this page and instead create a recurring task using the scheduler. See [Automating URL Filtering Updates Using a Scheduled Task](#).

### Update Now

You can perform a one-time, on-demand update by clicking the **Update Now** button at the top of this dialog box, but you should also either enable automatic updates or create a recurring task using the scheduler. You cannot start an on-demand update if an update is already in progress.

Although daily updates tend to be small, if it has been more than five days since your last update, new URL data may take up to 20 minutes to download, depending on your bandwidth. Then, it may take up to 30 minutes to perform the update itself.

### Query Cisco Cloud for Unknown URLs

Allows the system to submit URLs to the cloud for threat intelligence evaluation when users browse to a website whose category and reputation are not in the local dataset. Disable this option if you do not want to submit your uncategorized URLs, for example, for privacy reasons.

This option is enabled by default if at least one managed device has a valid URL Filtering license.

Connections to uncategorized URLs do **not** match rules with category or reputation-based URL conditions. You cannot assign categories or reputations to URLs manually.

If you use SSL rules to handle encrypted traffic, see also [TLS/SSL Rule Guidelines and Limitations](#).

### Cached URLs Expire

This setting is relevant only if **Query Cisco Cloud for Unknown URLs** is enabled.

Caching category and reputation data makes web browsing faster. By default, cached data for URLs never expires, for fastest performance.

To minimize instances of URLs matching on stale data, you can set URLs in the cache to expire. For greater accuracy and currency of threat data, choose a shorter expiration time.

A cached URL refreshes *after* the first time a user on the network accesses it after the specified time has passed. The first user does not see the refreshed result, but the next user who visits this URL does see the refreshed result.

For more information about caching of URL data, see [URL Filtering Data from the Cisco Cloud](#), on page 2.

## Configuring URL Conditions

Smart License	Classic License	Supported Devices	Supported Domains	Access
URL Filtering (cat/rep)	URL Filtering (cat/rep)	Any	Any	Admin/Access Admin/Network Admin
Any (manual)	Any (manual)			

When you build a URL condition, you choose the URL categories whose traffic you want to control. Optionally, you can constrain those URL categories with a reputation.

In access control and QoS rules, you can also filter individual URLs using predefined URL objects, URL lists and feeds, and manual per-rule URLs. You cannot constrain these URLs with a reputation. Manual URL filtering is not supported in SSL rules; instead, use distinguished name conditions.

**Step 1** In the rule editor, click the following for URL conditions:

- Access control or QoS—Click **URLs**.
- SSL—Click **Category**.

**Step 2** Find and choose the URLs you want to control:

- Categories—Choose URL categories, or keep the default of **Any**. In an access control or QoS rule, click **Category** to choose categories.
- URL Objects, Lists, and Feeds—Choose predefined URL objects and URL lists and feeds. In an access control or QoS rule, click **URLs** to choose URLs.

**Step 3** (Optional) Constrain URL categories by choosing a **Reputation**.



Note that if you explicitly match **Uncategorized** URLs, you cannot further constrain by reputation, because uncategorized URLs do not have reputations. Choosing a reputation level also includes other reputations either more or less severe than the level you choose, depending on the rule action:

- Includes less severe reputations—If the rule allows or trusts web traffic. For example, if you configure an access control rule to allow Benign Sites (level 4), it also automatically allows Well Known (level 5) sites.
- Includes more severe reputations—If the rule rate limits, decrypts, blocks, or monitors web traffic. For example, if you configure an access control rule to block Suspicious Sites (level 2), it also blocks High Risk (level 1) sites.

If you change the rule action, the system automatically changes the reputation levels in URL conditions.

**Step 4** Click **Add to Rule**, or drag and drop.

**Step 5** (Optional) In an access control or QoS rule, add any URLs that you want to specify manually by entering a URL and clicking **Add**.

You can enter a URL or IP address. This field does not support wildcards.

**Step 6** Save or continue editing the rule.

**Example: URL Condition in an Access Control Rule**

The following graphic shows the URL condition for an access control rule that blocks all malware sites, all High Risk sites, and all non-benign social networking sites. It also blocks a single site, example.com, which is represented by a URL object.



The following table summarizes how you build the condition.

Blocked URL	Category or URL Object	Reputation
Malware sites, regardless of reputation	Malware Sites	Any
Any URL with a high risk (level 1)	Any	1 - High Risk
Social networking sites with a risk greater than benign (levels 1 through 3)	Social Network	3 - Benign sites with security risks
example.com	The URL object named example.com	None

**What to do next**

- Return to [How to Configure URL Filtering with Category and Reputation](#), on page 5.
- If you are done making changes, Deploy configuration changes; see [Deploy Configuration Changes](#).

**Rules with URL Conditions**

The following table lists rules that support URL conditions, and the types of filtering that each rule type supports.

Rule Type	Supports Category and Reputation Filtering?	Supports Manual Filtering?
Access control	Yes	Yes
SSL	Yes	No; use distinguished name conditions instead
QoS	Yes	Yes

**URL Rule Order**

For the most effective URL matching, place rules that include URL conditions before other rules, particularly if the URL rules are block rules and the other rules meet both of the following criteria:

- They include application conditions.
- The traffic to be inspected is encrypted.

**Configure URL Filtering Health Monitors**

The following health policies alert if the system has problems obtaining or updating URL category and reputation data.

- URL Filtering Monitor
- Threat Data Updates on Device

To ensure that these are configured the way you want them, see [Health Modules](#) and [Configuring Health Monitoring](#).

**Manual URL Filtering**

In access control and QoS rules, you can supplement or selectively override category and reputation-based URL filtering by manually filtering individual URLs, groups of URLs, or URL lists and feeds.




---

**Note** To filter a large number of URLs, use a URL list instead of individual or grouped URL objects. For more information, see [Security Intelligence Lists and Feeds](#).

---

You can perform this type of URL filtering without a special license. Manual URL filtering is not supported in SSL rules; instead, use distinguished name conditions.

For example, you might use access control to block a category of websites that are not appropriate for your organization. However, if the category contains a website that is appropriate, and to which you want to provide access, you can create a manual Allow rule for that site and place it before the Block rule for the category.

### Cautions

When manually filtering specific URLs, carefully consider other traffic that might be affected. To determine whether network traffic matches a URL condition, the system performs a simple substring match. If the requested URL matches any part of the string, the URLs are considered to match.

Example 1:

You want to explicitly block ign.com (a gaming site). However, substring matching means that blocking ign.com also blocks verisign.com, which might not be your intent.

Example 2:

If you allow all traffic to example.com, your users could browse to URLs including:

- <http://example.com/>
- <http://example.com/newexample>
- <http://www.example.com/>

### Related Topics

[Security Intelligence Lists and Feeds](#)

## Troubleshoot URL Filtering

### How can I find the category and reputation of a particular URL?

Do a manual lookup. See [Finding URL Category and Reputation](#).

### Error when attempting a manual lookup: Cloud Lookup Failure for <URL>

Make sure the feature is properly enabled. See the prerequisites in [Finding URL Category and Reputation](#).

### URL appears to be incorrectly handled based on its URL category and reputation

**Problem:** The system does not handle the URL correctly based on its URL category and reputation.

#### Solutions:

- Verify that the URL category and reputation associated with the URL are what you think they are. See [Finding URL Category and Reputation](#).
- The following issues may be addressed by settings described in [URL Filtering Options, on page 7](#), accessible using [Enable URL Filtering Using Category and Reputation, on page 6](#).
  - The URL cache may hold stale information. See information about the **Cached URLs Expire** setting in [URL Filtering Options, on page 7](#).

- The local data set may not be updated with current information from the cloud. See information about the **Enable Automatic Updates** setting in [URL Filtering Options, on page 7](#).
- The system may be configured to *not* check the cloud for current data. See information about the **Query Cisco cloud for unknown URLs** setting in [URL Filtering Options, on page 7](#).
- Your access control policy may be configured to pass traffic to the URL without checking the cloud. See information about the **Retry URL cache miss lookup** setting in [Access Control Policy Advanced Settings](#).
- See also [Guidelines and Limitations for URL Filtering, on page 3](#).
- If the URL is processed using an SSL rule, see [TLS/SSL Rule Guidelines and Limitations](#) and [SSL Rule Order](#)
- Verify that the URL is being handled using the access control rule that you think it is being handled by, and that the rule does what you think it does. Consider rule order.
- Verify that the local URL category and reputation database on the Firepower Management Center is successfully being updated from the cloud and that managed devices are successfully being updated from the Firepower Management Center.

Status of these processes are reported in the Health Monitor, in the **URL Filtering Monitor** module and the **Threat Data Updates on Devices** module. For details, see [Health Monitoring](#).

If you want to immediately update the local URL category and reputation database, go to **System > Integration**, click the **Cloud Services** tab, then click **Update Now**. For more information, see [URL Filtering Options, on page 7](#).

#### **A URL category or reputation is not correct**

For access control or QoS rules: Use manual filtering, paying careful attention to rule order. See [Manual URL Filtering, on page 10](#) and [Configuring URL Conditions, on page 8](#).

For SSL rules: Manual filtering is not supported. Instead, use distinguished name conditions.

#### **Web pages are slow to load**

There is a tradeoff between security and performance. Some options:

- Consider modifying the **Cached URLs Expire** setting. Click **System > Integration**, then select the **Cloud Services** tab. For information, see [URL Filtering Options, on page 7](#).
- Consider deselecting the **Retry URL cache miss lookup** setting in [Access Control Policy Advanced Settings](#).

#### **Events Do Not Include URL Category and Reputation**

- Make sure you have included applicable URL rules in an access control policy, the rules are active, and the policies have been deployed to the relevant devices.
- URL category and reputation do not appear in an event if the connection is processed before it matches a URL rule.

## History for URL Filtering

Feature	Version	Details
The <b>Cisco CSI</b> tab is renamed to <b>Cloud Services</b>	6.4	Modified screens and navigation: <b>System &gt; Integration &gt; Cisco CSI</b> is now <b>System &gt; Integration &gt; Cloud Services</b>  Supported platforms: FMC
Moved URL Filtering information from various locations to this new URL Filtering chapter	6.3	Moved information about configuring cloud communications for URL Filtering to the new URL Filtering chapter. Moved certain other URL Filtering information from other locations to this chapter. Made related changes to the structure of the Cisco CSI topics in the chapter.
New option: Cached URLs Expire	6.3	Use this new control to balance performance with freshness of URL category and reputation data in order to minimize instances of URLs matching on stale data.  Modified screens: <b>System &gt; Integration &gt; Cisco CSI</b> .  Supported Platforms: All.
Changed menu path	6.3	The path to the manual URL Lookup page has changed from <b>Analysis &gt; Lookup &gt; URL</b> to <b>Analysis &gt; Advanced &gt; URL</b> .

