
Configure Custom URL-Filtering Profiles

 For supported software information, click [here](#).

URL-filtering profiles enforce actions on HTTP flows based on URL category and URL reputation. You can use predefined URL-filtering profiles, and you can create custom profiles that you can use when configuring internet protection rules. You can use custom URL-filtering profiles for devices that are connected to a Secure Web Gateway (SWG) and want to send traffic to the internet. You can use a single URL-filtering profile with one or more internet protection rules. URL filtering processes any traffic that matches an internet protection rule in a URL-filtering profile. Any logs that are generated are sent to the logging profile associated with the URL-filtering profile.

This article describes how to configure custom URL-filtering profiles and how to view URL categories.

Configure Custom URL-Filtering Profiles

In URL-filtering profiles, you can create allow lists and deny lists of URLs.

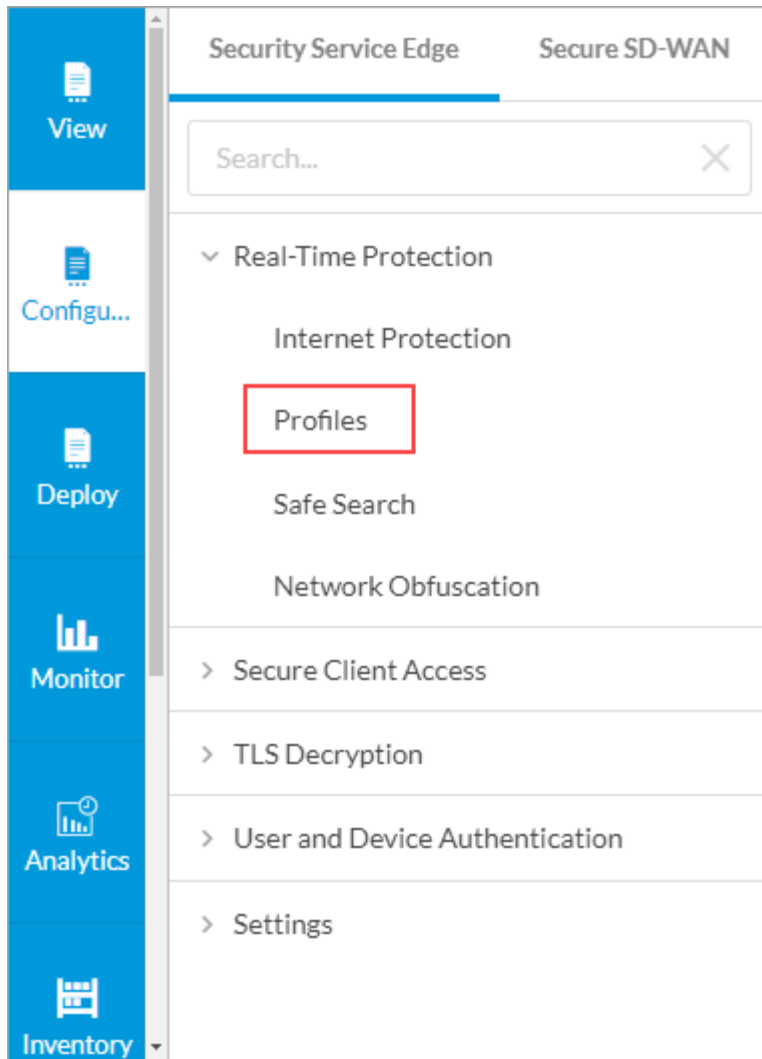
The URL-filtering profile processes enforceable actions for a session in the following order:

- Deny-listed URLs—Specify either fixed strings or regular expression (regex) patterns to match deny-listed URLs. Specify the deny list action to take for all matching HTTP flows. If you do not configure a deny list action, the default action is taken, which is to drop the session.
- Allow-listed URLs—Specify either fixed strings or perl-compatible regular expression (PCRE) patterns to match allow-listed URLs. URLs that match the allow list configuration are allowed, and no security actions are taken. Optionally, you can enable logging to create a log of allow-listed URLs.
- Category action map—Create a set of rules that specify the URL-filtering action to take for each URL category that is associated with a URL. In each rule, you can specify one or more predefined or custom URL categories. The action can be a packet or session action, or a predefined or custom captive portal action. VOS devices evaluate URL category and URL reputation action rules simultaneously, and they enforce the more severe action. For example, if the category rule action is to block and the reputation rule is to allow, the block action is taken.
- Reputation action map—Create a set of rules that specify the URL-filtering action to take for each URL reputation that is associated with the URL. In each rule, you can specify one or more URL reputation values. The action can be a packet or session action, or a predefined or custom captive portal action.

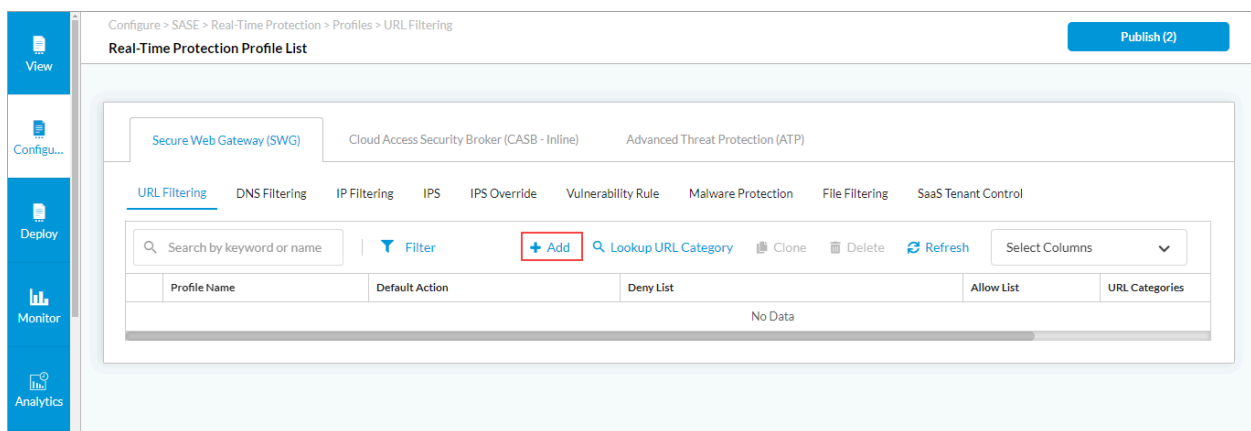
If this evaluation does not determine an action, the default action configured for the URL-filtering profile is taken.

To configure custom URL-filtering profiles:

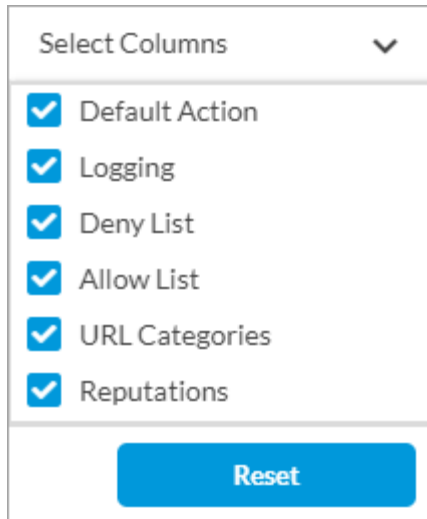
1. Go to Configure > Real-Time Protection > Profiles:



The following screen displays:

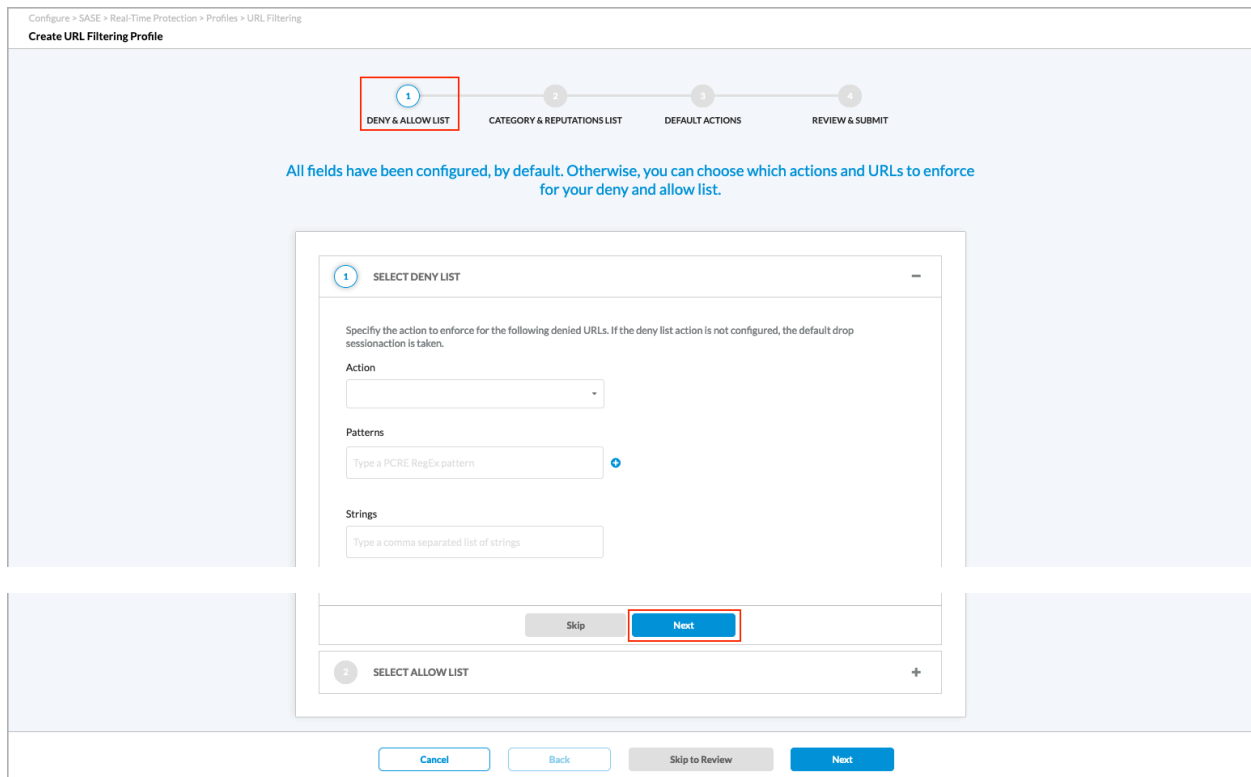


- To customize which columns display, click Select Columns and then click the columns to select or deselect the ones you want to display. Click Reset to return to the default columns settings.



The 'Select Columns' dialog box shows a list of columns with checkboxes: Default Action, Logging, Deny List, Allow List, URL Categories, and Reputations. All are checked. A blue 'Reset' button is at the bottom.

- Click + Add to create a rule. The Create URL Filtering screen displays with Deny and Allow List selected by default. By default, all fields are configured. You can customize the actions and URLs to enforce by entering the following information in the Deny and Allow List section. Enter information for the following fields.



The 'Create URL Filtering Profile' screen shows a progress bar with four steps: 1. DENY & ALLOW LIST (highlighted), 2. CATEGORY & REPUTATIONS LIST, 3. DEFAULT ACTIONS, and 4. REVIEW & SUBMIT. Below the progress bar, a message states: 'All fields have been configured, by default. Otherwise, you can choose which actions and URLs to enforce for your deny and allow list.'

The main content area displays the '1 SELECT DENY LIST' section. It includes a description: 'Specify the action to enforce for the following denied URLs. If the deny list action is not configured, the default drop sessionaction is taken.' Below this are three input fields: 'Action' (a dropdown menu), 'Patterns' (a text field with a placeholder 'Type a PCRE RegEx pattern' and a plus icon), and 'Strings' (a text field with a placeholder 'Type a comma separated list of strings').

At the bottom of the 'SELECT DENY LIST' section are two buttons: 'Skip' and 'Next' (highlighted with a red box). Below this is the '2 SELECT ALLOW LIST' section, which is currently empty and has a plus icon to add items.

At the very bottom of the screen are four buttons: 'Cancel', 'Back', 'Skip to Review', and 'Next'.

For Releases 12.1.1 and later, Deny List and Allow List display on the same screen, and you do not have to click Next to move to the Allow List section. The fields are the same.

Configure > SASE > Real-Time Protection > Profiles > URL Filtering

Create URL Filtering Profile

1 Deny & Allow List
 2 Category & Reputations List
 3 Default Action
 4 Review & Submit

All fields have been configured, by default. Otherwise, you can choose which actions and URLs to enforce for your deny and allow list.

Deny List
Choose which actions and URLs to deny (blacklist).

Action

Patterns ⓘ
Type a PCRE RegEx pattern +

Strings ⓘ
Type a comma separated list of strings

Allow List
Choose which URLs to allow (whitelist).


Patterns ⓘ
Type a PCRE RegEx pattern +

Strings ⓘ
Type a comma separated list of strings

☐ Enable Logging ⓘ

Cancel
Back
Skip to Review
Next

Field	Description
Action	<p>Select the action to apply to the URL filter:</p> <ul style="list-style-type: none"> Alert—Allow the URL and generate an entry in the URL-filtering log. Allow—Allow the URL without generating an entry in the URL-filtering log. Ask—The browser presents an information page

Field	Description
	<p>that allows the user to either cancel the operation by clicking Cancel or continue with the operation by clicking OK (for HTTP and HTTPS).</p> <ul style="list-style-type: none"> ◦ Block—Block the URL and generate an entry in the URL-filtering log. No response page is display, and the user cannot continue with the website. ◦ Drop packet—The browser waits for a response from the server and then drops the packets. It is not possible to determine whether the packet was dropped because of no response from the server or because a firewall blocked access to the website. ◦ Drop session—The browser waits for a response from the server and drops the session. It is not possible to determine whether the session was dropped because of no response from the server or because a firewall blocked access to the website. ◦ Justify—The browser presents an information page that allows the user to either cancel the operation by clicking Cancel or continue with the operation after entering a justification message and clicking OK (for HTTP and HTTPS). ◦ Reject—The browser displays an alert and resets the connection to the server. It is not possible to determine whether this occurred because of no response from the server or because a firewall blocked access to the website. <p>Note that all actions except Allow generate an entry in the URL-filtering log.</p>
Patterns	<p>Add specific URL patterns to block. You can specify a fixed string or a perl-compatible regular expression (PCRE). Click the  Add icon to add more patterns.</p>
Strings	<p>Enter the complete URL string of a URL to block.</p>

4. Click Next. In the Select Allow List section, enter information for the following fields.

2

SELECT ALLOW LIST

Specify the action to enforce for the following allowed URLs. If the allow list action is not configured, the default drop session action is taken.

Patterns

Type a PCRE RegEx pattern

+

Strings

Type a comma separated list of strings

☐

Enable Logging


?

Cancel

Back

Skip to Review

Next

Field	Description
Patterns	Enter specific URL patterns to allow. You can specify a fixed string or a PCRE. Click the  Add icon to add more patterns.
Strings	Enter the complete URL string of a URL to allow.
Enable Logging	Click to send the log information about the listed URLs to Versa Analytics.

- Click Next to go to the Category and Reputations List screen. In the Select Category List section, enter information for the following fields. Note that you can specify a category or a reputation, or both. If you specify both, URLs must match both the category and the reputation.

Configure > SASE > Real-Time Protection > Profiles > URL Filtering

Create URL Filtering Profile

1 2 3 4

DENY & ALLOW LIST
CATEGORY & REPUTATIONS LIST
DEFAULT ACTIONS
REVIEW & SUBMIT

All fields have been configured, by default. Otherwise, you can choose which actions to enforce for categories or reputations.

1
SELECT CATEGORY LIST

Specify what action to enforce to the following URL categories.

Action
URL Category

Skip
Next

2
SELECT REPUTATION LIST

For Releases 12.1.1 and later, Select Category List and Select Reputation List display on the same screen, and you do not have to click Next to move to the Select Reputation List section. The fields are the same.

Configure > SASE > Real-Time Protection > Profiles > URL Filtering

Create URL Filtering Profile

1 2 3 4

Deny & Allow List
Category & Reputations List
Default Action
Review & Submit

All fields have been configured, by default. Otherwise, you can choose which actions and URLs to enforce for your deny and allow list.

Select Category List

Specify what action to enforce to the following URL categories.

Action
URL Category
+ Add New

+


Select Reputation List

Specify what action to enforce to the following reputations.

Action
Reputation

+

Cancel
Back
Skip to Review
Next

Field	Description
Action	<p>Select the action to enforce on a specific URL category match:</p> <ul style="list-style-type: none"> ◦ Alert—Allow the URL and generate an entry in the URL-filtering log. ◦ Allow—Allow the URL without generating an entry in the URL-filtering log. ◦ Ask—The browser presents an information page that allows the user to either cancel the operation by clicking Cancel or continue with the operation by clicking OK (for HTTP and HTTPS). ◦ Block—Block the URL and generate an entry in the URL-filtering log. No response page is display, and the user cannot continue with the website. ◦ Drop packet—The browser waits for a response from the server and then drops the packets. It is not possible to determine whether the packet was dropped because of no response from the server or because a firewall blocked access to the website. ◦ Drop session—The browser waits for a response from the server and drops the session. It is not possible to determine whether the session was dropped because of no response from the server or because a firewall blocked access to the website. ◦ Justify—The browser presents an information page that allows the user to either cancel the operation by clicking Cancel or continue with the operation after entering a justification message and clicking OK (for HTTP and HTTPS). ◦ Reject—The browser displays an alert and resets the connection to the server. It is not possible to determine whether this occurred because of no response from the server or because a firewall blocked access to the website. <p>Note that all actions except Allow generate an entry in the URL-filtering log.</p>
URL Category	<p>Select one or more URL categories on which to take the specified action. Click the  Add icon to add more URL categories.</p>

6. Click Next. In the Select Reputation List section, enter information for the following fields.

2

SELECT REPUTATION LIST

Specify what action to enforce to the following reputations.

Action

Reputation

Cancel

Back

Skip to Review


Next

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Custom_URL-Filteri...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Custom_URL-Filteri...)

Updated: Wed, 23 Oct 2024 08:35:38 GMT

Copyright © 2024, Versa Networks, Inc.

9

Field	Description
Action	<p>Select the action to enforce on a specific URL category match:</p> <ul style="list-style-type: none"> ◦ Alert—Allow the URL and generate an entry in the URL-filtering log. ◦ Allow—Allow the URL without generating an entry in the URL-filtering log. ◦ Ask—The browser presents an information page that allows the user to either cancel the operation by clicking Cancel or continue with the operation by clicking OK (for HTTP and HTTPS). ◦ Block—Block the URL and generate an entry in the URL filtering log. No response page is display, and the user cannot continue with the website. ◦ Drop packet—The browser waits for a response from the server and then drops the packets. It is not possible to determine whether the packet was dropped because of no response from the server or because a firewall blocked access to the website. ◦ Drop session—The browser waits for a response from the server and drops the session. It is not possible to determine whether the session was dropped because of no response from the server or because a firewall blocked access to the website. ◦ Justify—The browser presents an information page that allows the user to either cancel the operation by clicking Cancel or continue with the operation after entering a justification message and clicking OK (for HTTP and HTTPS). ◦ Reject—The browser displays an alert and resets the connection to the server. It is not possible to determine whether this occurred because of no response from the server or because a firewall blocked access to the website. <p>Note that all actions except Allow generate an entry in the URL-filtering log.</p>
Reputation	<p>Select the reputation on which to take the specified action. Click the  Add icon to add more reputations.</p>

- Click Next to go to the Default Actions screen, and then enter information for the following fields. If you do not specify an action in the category and reputation lists, the default action is taken.

Configure > SASE > Real-Time Protection > Profiles > URL Filtering

Create URL Filtering Profile

1

2

3

4

DENY & ALLOW LIST

CATEGORY & REPUTATIONS LIST

DEFAULT ACTIONS

REVIEW & SUBMIT

By default, we will allow all URLs that do not match any criteria specified. Otherwise, you can choose which default action to enforce if there are no criteria matched.

Specify the default action to enforce if there are no criteria matched.

Default Actions

Allow

☐ Decrypt Bypass ⓘ

☐ Cloud Lookup State ⓘ

☐ Enable Logging ⓘ

Cancel

Back

Skip to Review

Next

For Releases 12.1.1 and later, the Default Action screen does not display the Enable Logging field.

Configure > SASE > Real-Time Protection > Profiles > URL Filtering

Create URL Filtering Profile

✓

✓

3

4

Deny & Allow List

Category & Reputations List

Default Action

Review & Submit

By default, we will allow all URLs that do not match any criteria specified. Otherwise, you can choose which default action to enforce if there are no criteria matched.

Specify the default action to enforce if there are no criteria matched.

Default Action

Allow

☐ Decrypt Bypass ⓘ

☐ Cloud Lookup State ⓘ

Cancel

Back

Skip to Review

Next

Field	Description
Action	<p>Select the action to enforce on a specific URL category match:</p> <ul style="list-style-type: none"> ◦ Alert—Allow the URL and generate an entry in the URL-filtering log. ◦ Allow—Allow the URL without generating an entry in the URL-filtering log. ◦ Ask—The browser presents an information page that allows the user to either cancel the operation by clicking Cancel or continue with the operation by clicking OK (for HTTP and HTTPS). ◦ Block—Block the URL and generate an entry in the URL filtering log. No response page is display, and the user cannot continue with the website. ◦ Drop packet—The browser waits for a response from the server and then drops the packets. It is not possible to determine whether the packet was dropped because of no response from the server or because a firewall blocked access to the website. ◦ Drop session—The browser waits for a response from the server and drops the session. It is not possible to determine whether the session was dropped because of no response from the server or because a firewall blocked access to the website. ◦ Justify—The browser presents an information page that allows the user to either cancel the operation by clicking Cancel or continue with the operation after entering a justification message and clicking OK (for HTTP and HTTPS). ◦ Reject—The browser displays an alert and resets the connection to the server. It is not possible to determine whether this occurred because of no response from the server or because a firewall blocked access to the website. <p>Note that all actions except Allow generate an entry in the URL-filtering log.</p>
Decrypt Bypass	<p>Click to enable decrypt bypass, which disables decryption of SSL traffic that matches the predefined captive portal actions for this URL filtering profile after</p>

	<p>captive portal redirection. The decryption policy decrypts SSL sessions to display only the captive portal response. After the captive portal action is performed, SSL decryption is bypassed, and users can directly access the URL. To disable decryption for traffic matching a custom action, select a custom action (Default action) and select Decrypt-Bypass.</p> <p>If you do not select the Decrypt Bypass option, SSL decryption is enabled and URL filtering uses the host and URI of the actual URL for categorization. This action further decrypts captive portal redirection from actions such as Ask and Justify.</p>
Cloud Lookup State	Click to enable cloud lookup. If the cloud lookup state is not enabled for this profile, it is inherited from the tenant VOS device.
(Releases 11.4.1 and earlier) Enable Logging	Click to send log information to Versa Analytics.

8. Click Next to go to the Review and Deploy screen.

Configure > SASE > Real-Time Protection > Profiles > URL Filtering

Create URL Filtering Profile

1 DENY & ALLOW LIST 2 CATEGORY & REPUTATIONS LIST 3 DEFAULT ACTIONS 4 REVIEW & SUBMIT

Please give your rule a name:

General

Name * Description

Tags

Deny & Allow List [Edit](#)

Deny List ☐ Allow ☐

Allow List ☐

Category & Reputations List [Edit](#)

URL Categories

Releases 12.1.1 and later:

Configure > SASE > Real-Time Protection > Profiles > URL Filtering

Create URL Filtering Profile

✓ Deny & Allow List
 ✓ Category & Reputations List
 ✓ Default Action
 4 Review & Submit

Review your URL Filtering configuration below

General

Name * ⓘ

Description

Tags

☐ Logging is Disabled

Deny & Allow List [Edit](#)

Deny List

Allow List **Logging: Disabled**

Reputations

Default Actions [Edit](#)

Default Actions **Allow**

Decrypt Bypass **Disabled**

Cloud Lookup State **Disabled**

- In the General section, enter a name for the URL-filtering profile and, optionally, a description and tags.
- For all other sections, review the information. If you need to make changes, click the [Edit](#) icon.
- Click Save.

Display URL Categories

For Releases 12.1.1 and later.


You can look up the category for a URL in the database of predefined URLs, and you can display information about the URL and its reputation.

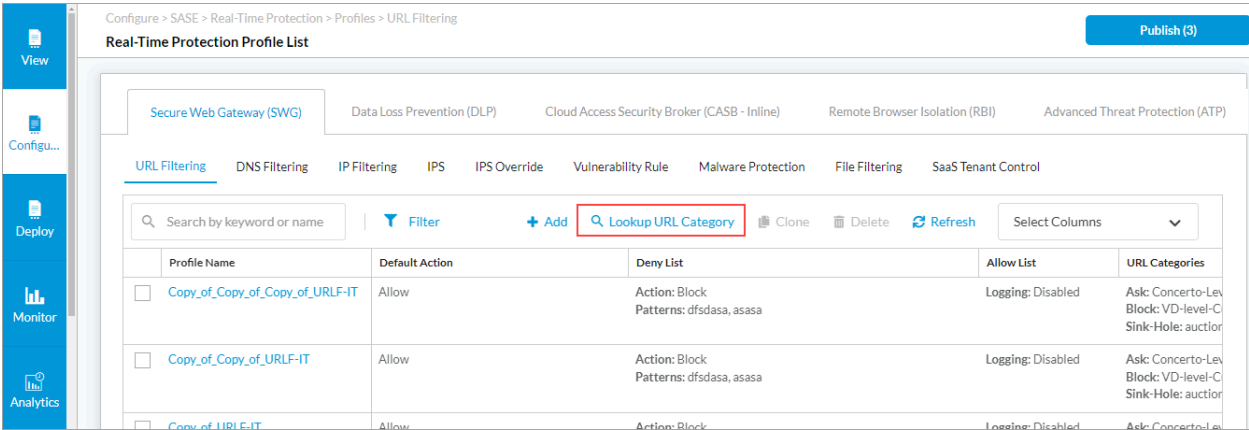
To display information about a predefined URL:

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Custom_URL-Filteri...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Custom_URL-Filteri...)

Updated: Wed, 23 Oct 2024 08:35:38 GMT

Copyright © 2024, Versa Networks, Inc.

- 1. Go to Configure > Real-Time Protection > Profiles > Secure Web Gateway (SWG) > URL Filtering.
- 2. Click  Lookup URL Category.



- 3. In the Look Up URL Category popup window, enter information for the following fields.

Lookup URL Category

Gateway Name

USA-East-GW-1

URL

www.google.com

Test

Cancel

Field	Description
Gateway Name	Select the organization for which you want to look up the URL category.

Field	Description
URL	Enter the URL for which you want to look up the URL category. For example, www.google.com.

- Click Test. The Look Up URL Category popup window displays information about the URL, including its predefined category and reputation. For example:

Lookup URL Category ✕

Gateway Name

USA-East-GW-1

URL

www.google.com

Test

```

URL : www.google.com/
All-one-category : 0
Pre-defined category count : 1
ID: 50, Confidence: 100, Name: search_engines
User-defined category count : 0
Pre-defined reputation,
Index : 81, Name: trustworthy
User-defined reputation,
Index : 0, Name: undefined
NOTE: Predefined results are from spack database. Spack flavor is Premium. Predefined URLF database is loaded successfully.

CSI lookup result,
URL : www.google.com
http_method :
Application Count : 1
Application 1,
name : Google
id : 19050
depth : 2
http_method : *
metadata count : 3
function --> id: 1 name: Unaffiliated
category --> id: 107 name: IT Services and Hosting
organization --> id: 104 name: Alphabet Inc.

```

Cancel

- Click Cancel.

Supported Software Information

Releases 11.1.1 and later support all content described in this article, except:

- Release 12.1.1 adds support for looking up the category of a predefined URL. Fields in Create URL Filtering Profile screen display on a single screen and not sections.

Additional Information

[Configure SASE Internet Protection Rules](#)