
Configure SD-WAN URL-Filtering Policies

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

URL-filtering policies enforce actions on HTTP flows based on URL category and URL reputation. You create policies that you can use when configuring basic and standard master profiles. Any logs that are generated are sent to the logging profile associated with the URL-filtering policy.

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

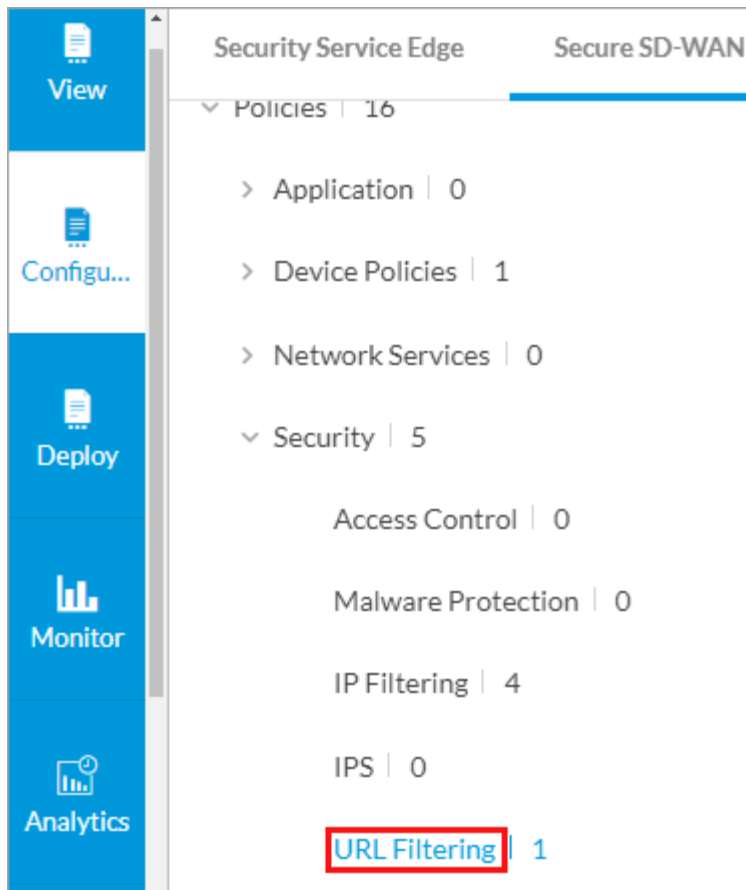
The URL-filtering policy processes enforceable actions for a session in the following order:

- 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.

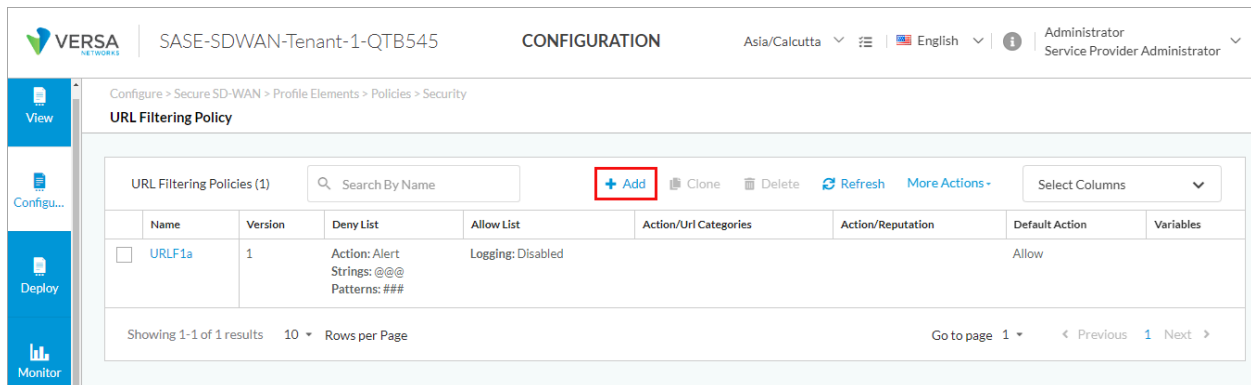
If this evaluation does not determine an action, the default action configured for the URL-filtering policy is taken.

To configure URL filtering policies:

1. Go to Configure > Secure SD-WAN > Profile Elements > Policies > Security > URL Filtering:



The following screen displays:



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

Select Columns

Version

Deny List

Allow List

Action/Url Categories

Action/Reputation

Default Action

Variables

Reset

- Click + Add to create a policy. The Create URL Filtering screen displays, and Step 1, Deny and Allow List is selected. By default, all fields are configured. You can customize the actions and URLs to enforce by entering the following information.

Add URL Filtering Policy

1

2

3

4

5

Deny & Allow List

Category & Reputations List

Default Actions

Permissions

Review & Submit

By default, all fields have been configured. 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

Strings

Allow List

Choose which URLs to allow (whitelist).

Patterns

Strings



Enable Logging

Cancel

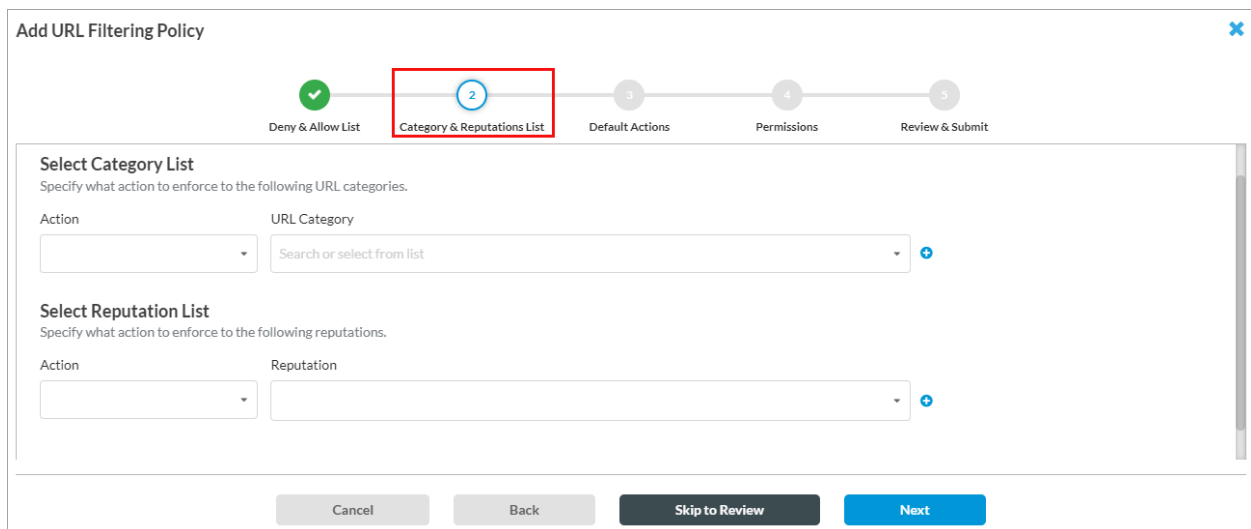
Skip to Review

Next


Field	Description
Deny List (Group of Fields)	
<ul style="list-style-type: none"> 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 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>
<ul style="list-style-type: none"> Patterns 	<p>Add specific URL patterns to block. You can specify a fixed string or a PCRE regular expression. Click the</p>


Field	Description
	 Add icon to add more patterns.
◦ Strings	Enter the complete URL string of a URL to block.
Allow List (Group of Fields)	
◦ Patterns	Enter specific URL patterns to allow. You can specify a fixed string or a PCRE regular expression. 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 Step 2, Category and Reputations List screen. 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.



Field	Description
Select Category List (Group of Fields)	
◦ Action	Select the action to enforce on a specific URL category match:

Field	Description
	<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>
<ul style="list-style-type: none"> ◦ 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>
Select Reputation List (Group of Fields)	

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 Step 3, 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.

Add URL Filtering Policy

✓

✓

3

4

5

Deny & Allow ListCategory & Reputations ListDefault ActionsPermissionsReview & 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 policy 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 policy, it is inherited from the tenant VOS device.

- Click Next to go to the Step 4, Permissions screen to set or update the permission for each role. The roles are Enterprise Administrator, Enterprise Operator, Service Provider Administrator, and Service Provider Operator. The permission for each role is selected by default, and you can update it. The role permissions are Edit, Hide, and Read.

Add URL Filtering Policy

1 Deny & Allow List 2 Category & Reputations List 3 Default Actions 4 Permissions 5 Review & Submit

We have preselected the permissions for the roles, below You can change the permission for each of the roles.

Role	Permissions
Enterprise Administrator (Inherited)	Edit
Service Provider Administrator (Inherited)	Edit
Service Provider Operator (Inherited)	Read
Enterprise Operator (Inherited)	Read

Cancel Back Skip to Review Next

- Click Next to go to the Step 5, Review and Submit screen.

Add URL Filtering Policy

✓

✓

✓

✓

3

Deny & Allow List

Category & Reputations List

Default Actions

Permissions

Review & Submit

Review your configurations. Before submitting, review and edit any steps of your configuration below..

General

Name

Description

Tags

Press Enter to add

Deny & Allow List [Edit](#)

Deny List

Allow List **Logging:** Disabled

Category & Reputations List [Edit](#)

URL Categories

Reputations

Default Actions [Edit](#)

Default Actions **Allow**

Decrypt Bypass **Disabled**

Cloud Lookup State **Disabled**

Permissions [Edit](#)

test-EA	Edit
Enterprise Administrator	Edit
Service Provider Administrator	Edit
EA-Parent2	Edit
Eo-parent	Read
Auth_Read	Edit
Service Provider Operator	Read
EA-Parent	Edit
Enterprise Operator	Read

Cancel

Back

Save

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

You associate URL filtering policies with basic or standard master profiles. For more information, see [Configure Profiles](#).

Supported Software Information

Releases 12.1.1 and later support all content described in this article.

Additional Information

[Configure Custom URL-Filtering Profiles](#)

[Configure Profiles](#)