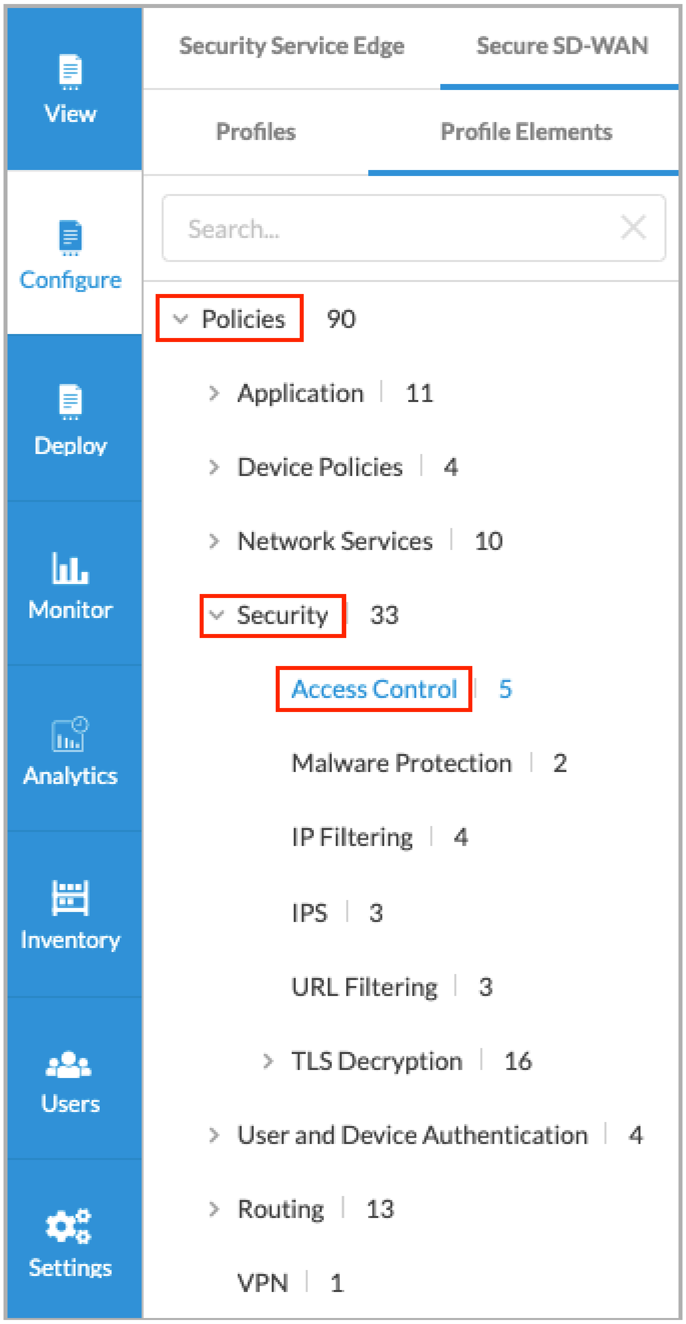
Configure SD-WAN Security Access Control Policies and Rules

For supported software information, click here.

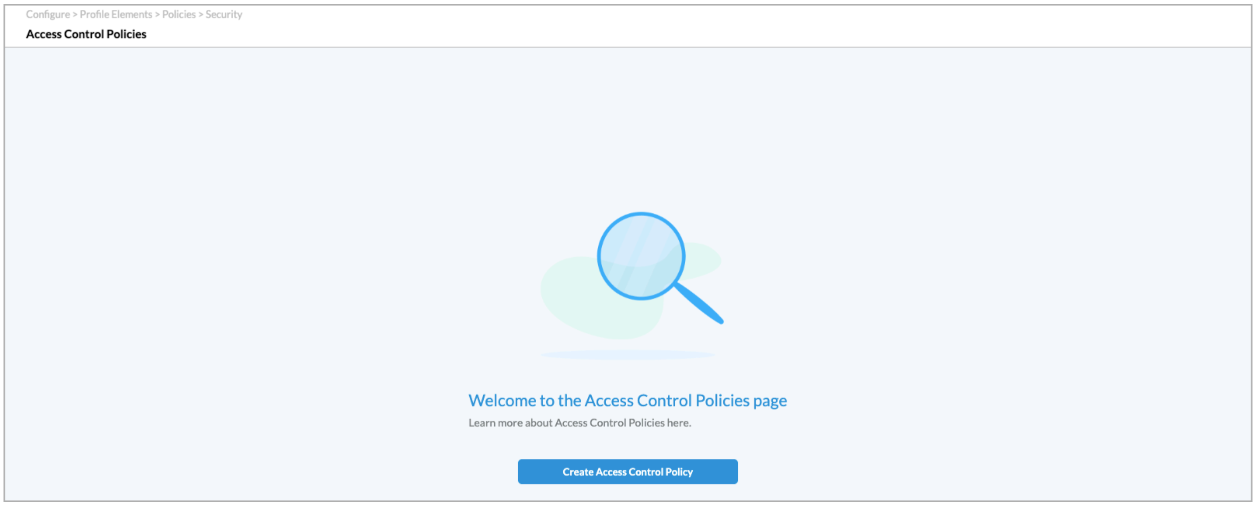
You can configure security access policies to filter traffic based on predefined and custom objects. A security access policy consists of an ordered set of one or more policy rules. Each policy rule consists of a set of match criteria and enforcement actions.

Configure an Access Control Policy

1. In Tenant view, go to the Configure lifecycle in the left menu bar.



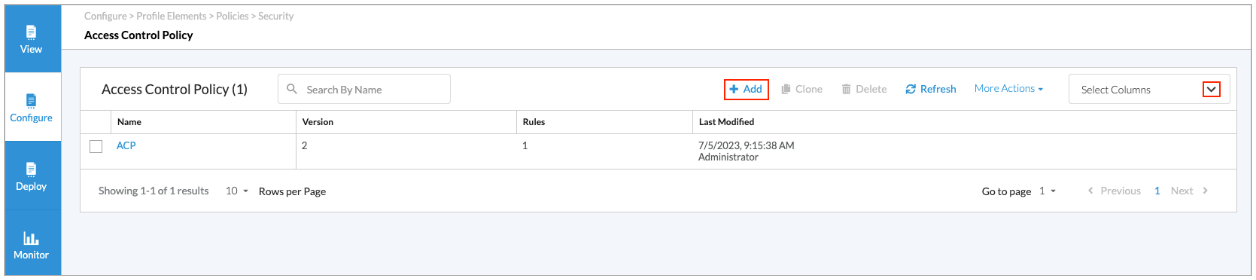
2. Select Profiles > Profile Elements > Policies > Security > Access Control.
    a. If you have not yet configured an access policy, the following screen displays. Click Create Access Control Policy to display the Add Access Control Policy screen. Go to Step 4.


Configure > Profile Elements > Policies > Security
Access Control Policies
Create Access Control Policy

Welcome to the Access Control Policies page

Learn more about Access Control Policies here.

b. If you have configured one or more access policies, the Access Control Policy screen displays the policies that are already configured.

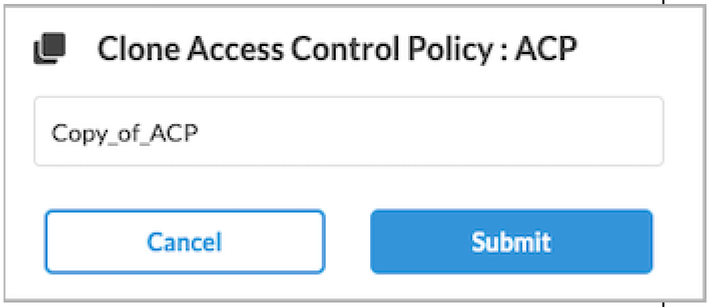
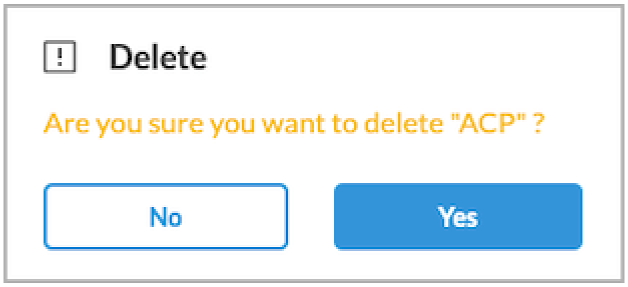


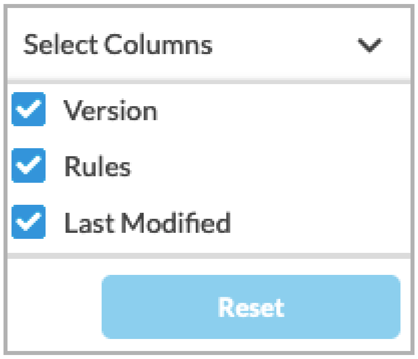
	Name	Version	Rules	Last Modified
□	ACP	2	1	7/5/2023, 9:15:38 AM Administrator

Showing 1-1 of 1 results 10 Rows per Page Go to page 1 Previous 1 Next

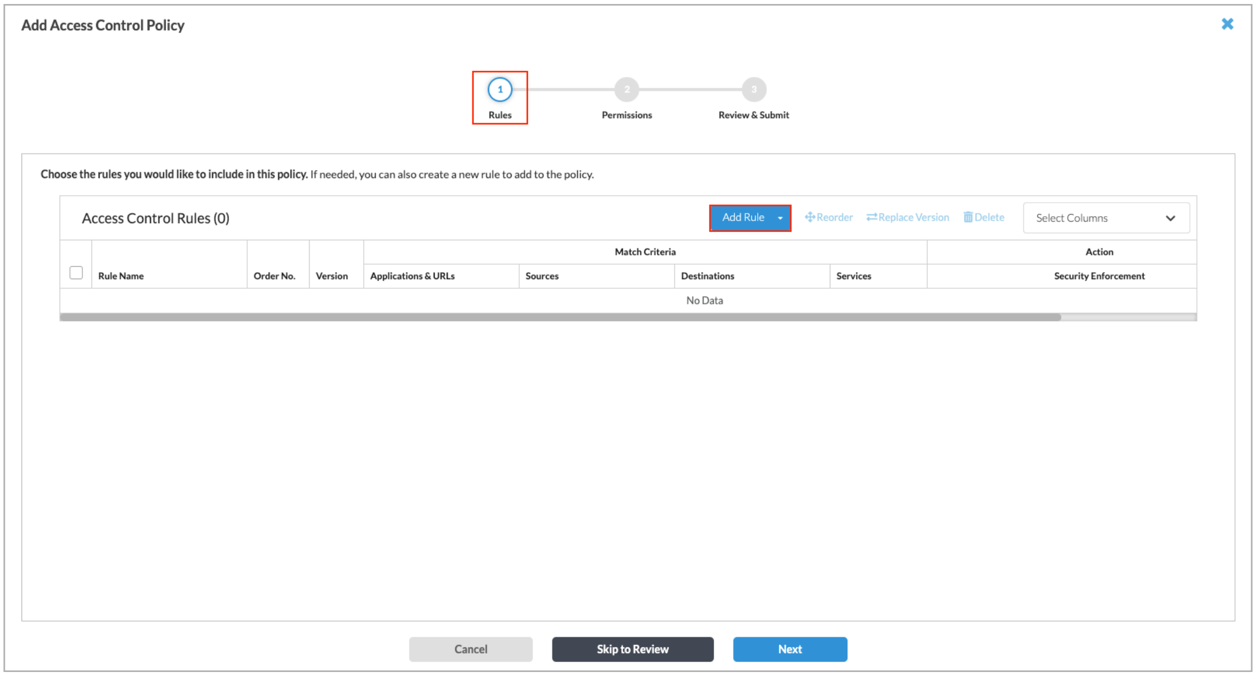
3. In the horizontal menu bar, you can perform the following operations.

Operation	Description
+ Add	Create a new access control policy. This button is active when no existing policy is selected. See Step 4 below.
Clone	Clone the selected access control policy. A popup window similar to the following displays:

Operation	Description
	 Clone Access Control Policy : ACP Copy_of_ACP Rename the default name of the cloned policy (here, Copy_of_ACP), if desired, and then click Submit.
Delete	Delete the selected access control policy. A popup window similar to the following displays:  Delete Are you sure you want to delete "ACP" ? Click Yes to delete the policy, or click No to retain the policy.
Refresh	Refresh the list of existing policies.
More Actions	Perform an action on the selected access control policy: ◦ Compare Versions—View the differences between two versions of a policy. ◦ Disable Auto Delete—Disable the automatic deletion of the policy (auto deletion is enabled by default). For more information, see Configure Automatic Deletion of SD-WAN Object Versions. ◦ Propagate—Propagate changes made to a policy to any entities that use the policy. For more

Operation	Description
	information, see Propagate Object Configuration Changes. ◦ View References—View the objects that refer to the selected policy. For more information, see View References to Objects in the Configuration Hierarchies.
Select Columns	To select the columns that you want to display, click the down arrow. To return to the default column selection, click Reset.  Select Columns ☑ Version ☑ Rules ☑ Last Modified Reset The column headings options are: ◦ Version ◦ Rules ◦ Last Modified

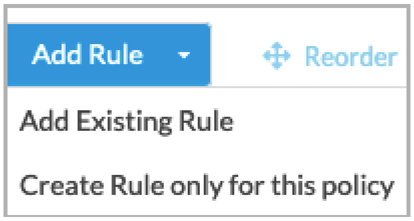
4. Click ✚ Add to create a new access control policy. A policy consists of one or more rules. The following screen displays, and Step 1, Rules is selected.



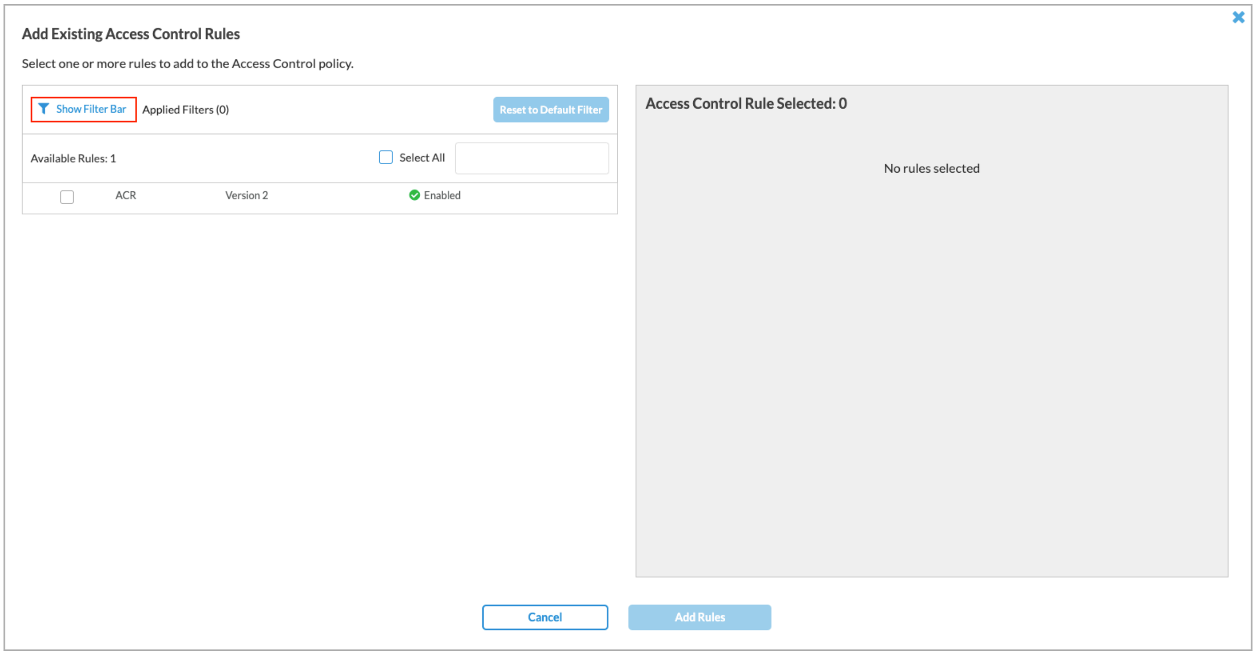
Choose the rules you would like to include in this policy. If needed, you can also create a new rule to add to the policy.

				Match Criteria				Action
□	Rule Name	Order No.	Version	Applications & URLs	Sources	Destinations	Services	Security Enforcement
				No Data				

5. Click Add Rule. The following list displays.



6. To add existing rules to the access control policy, click Add Existing Rule. The Add Existing Access Control Rules screen displays.



Add Existing Access Control Rules

Select one or more rules to add to the Access Control policy.

Show Filter Bar | Applied Filters (0) | Reset to Default Filter

Available Rules: 1 | □ Select All

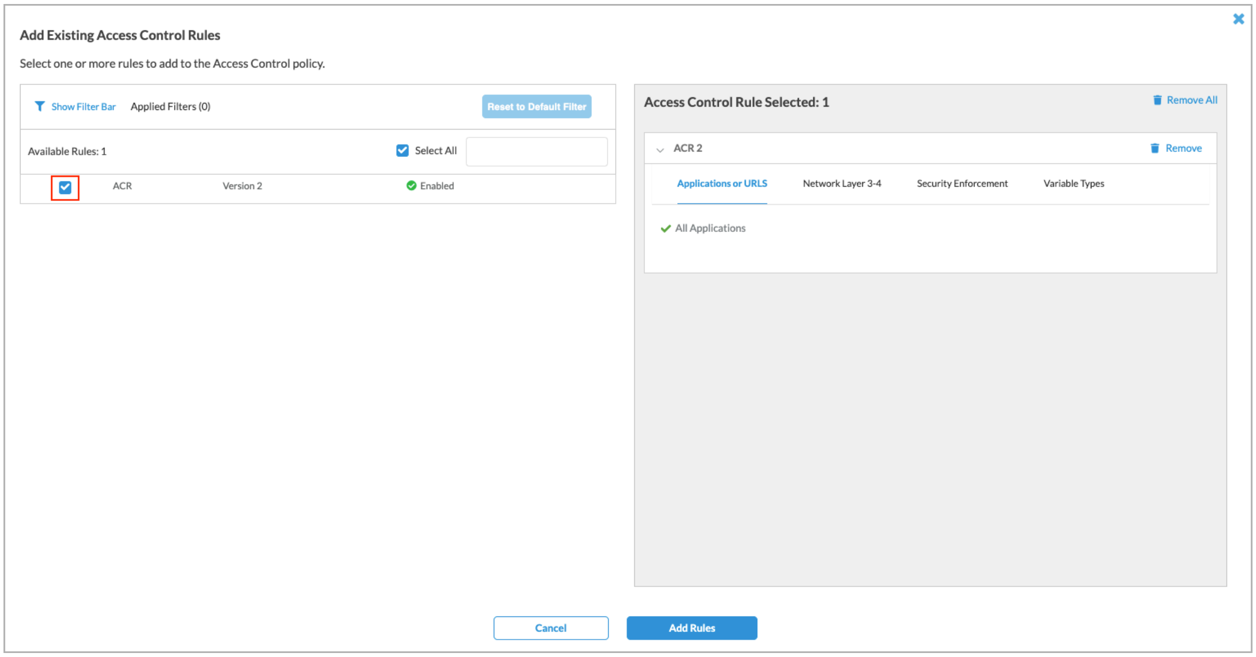
□	ACR	Version 2	✓ Enabled

Access Control Rule Selected: 0

No rules selected

Cancel | Add Rules

a. Select one or more rules in the Available Rules box to add them to the access control policy. The rules display in the Access Control Rule Selected box.



Add Existing Access Control Rules

Select one or more rules to add to the Access Control policy.

Show Filter Bar | Applied Filters (0) | Reset to Default Filter

Available Rules: 1 | ☑ Select All

☑	ACR	Version 2	✓ Enabled

Access Control Rule Selected: 1 | Remove All

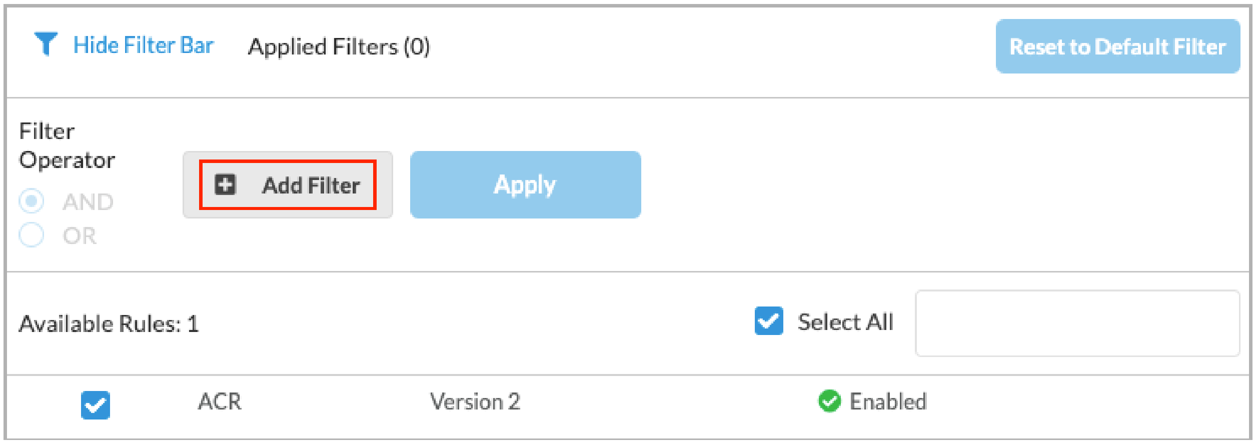
ACR 2 | Remove

Applications or URLS | Network Layer 3-4 | Security Enforcement | Variable Types

✓ All Applications

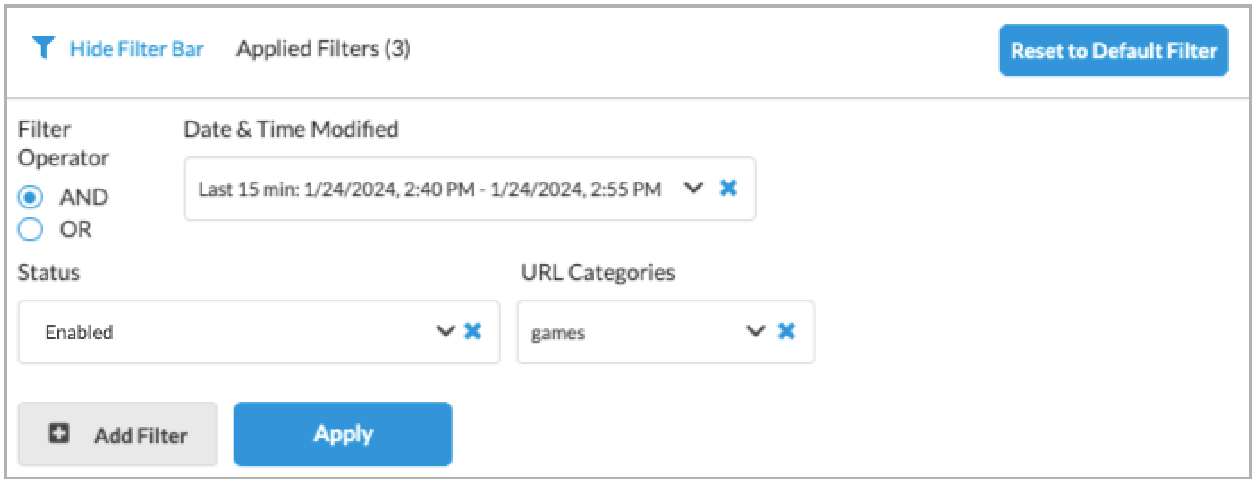
Cancel | Add Rules

b. To locate rules, you can filter them by clicking the ▼ Show Filter Bar icon. The screen changes to the following.



☑ ACR Version 2 ✓ Enabled

c. Click ⊞ Add Filter.
d. Select one or more filter types:
    - Applications
    - Data and Time Modified
    - Destination Address
    - Destination Zone
    - Differentiated Services Code Point (DSCP)
    - Name
    - Reputations
    - Schedule
    - Security Enforcement
    - Services
    - Source Address
    - Source Zone
    - Status
    - URL Categories
    - Variable Name
e. If you select multiple filters, choose the AND or OR Boolean operator for applying the filters. The following example shows that three filters have been applied and that the AND operator has been selected.



Filter Operator

● AND

○ OR

Date & Time Modified: Last 15 min: 1/24/2024, 2:40 PM - 1/24/2024, 2:55 PM

Status: Enabled

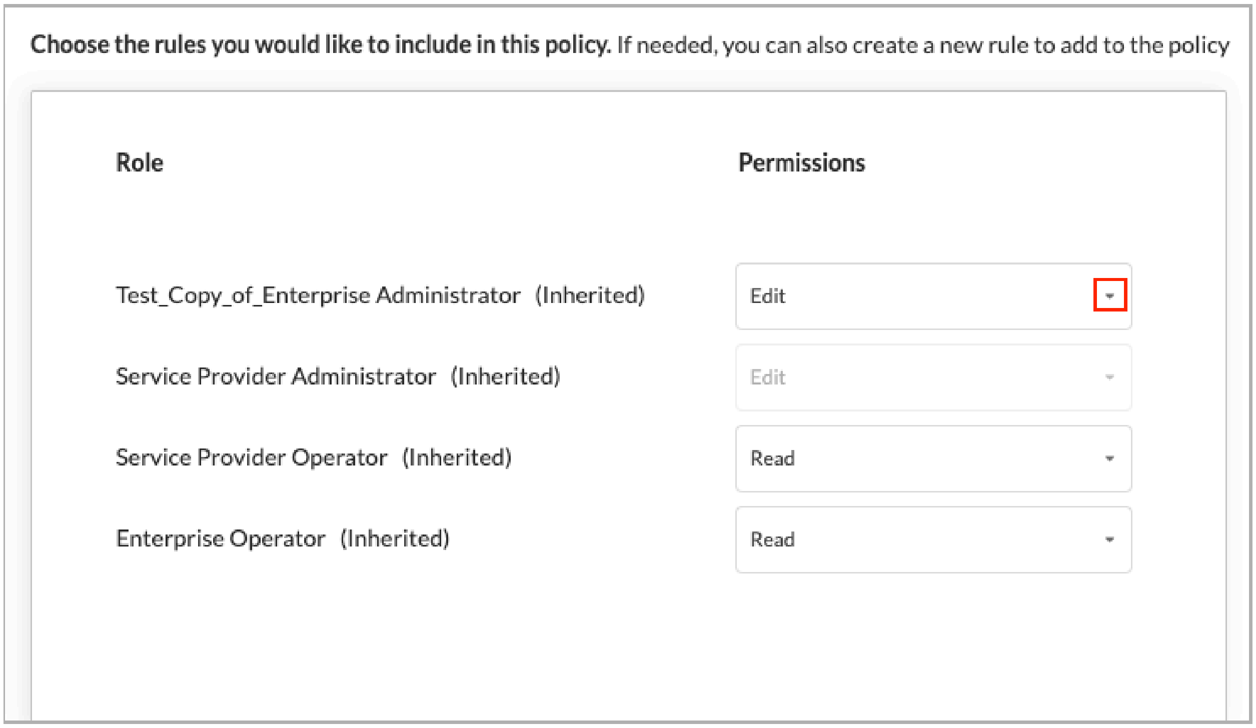
URL Categories: games

f. To apply the filters, click Apply.

g. To clear all filters, click Reset to Default Filter.

h. Click Add Rules at the bottom of the screen.

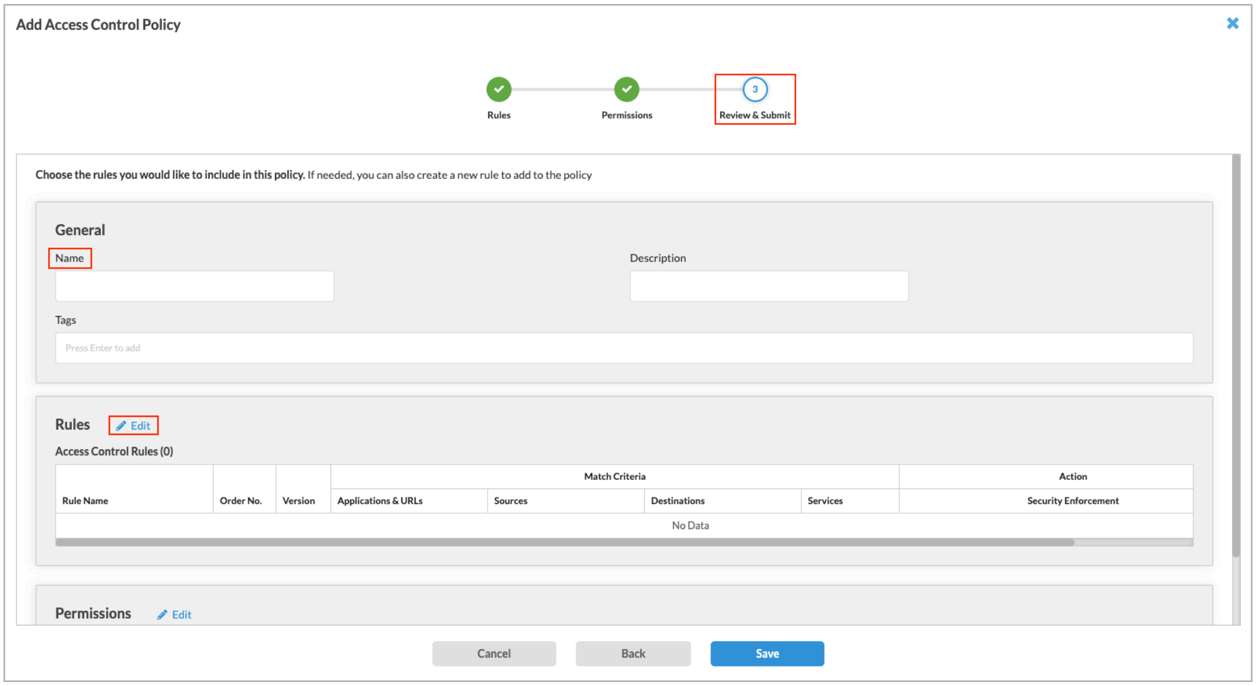
7. If you select the Create Rule Only for this Policy option, the Access Control Rule configuration screen displays. For more information, see Configure Access Control Rules, below.
8. Click Next to go to Step 2, Permissions.



Choose the rules you would like to include in this policy. If needed, you can also create a new rule to add to the policy

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

9. To change the permissions for a role, select Edit, Hide, or Read in the Permissions column.
10. Click Next to go to the Step 3, Review and Submit.



Add Access Control Policy

Choose the rules you would like to include in this policy. If needed, you can also create a new rule to add to the policy

General

Name

Description

Tags

Press Enter to add

Rules ✏ Edit

Access Control Rules (0)

			Match Criteria				Action
Rule Name	Order No.	Version	Applications & URLs	Sources	Destinations	Services	Security Enforcement
No Data							

Permissions ✏ Edit

11. In the General box, enter a name for the access control policy, and optionally enter a text description for the policy and one or more tags. A tag is an alphanumeric text descriptor with no spaces or special characters. You can specify multiple tags added for the same object. The tags are used for searching the objects.

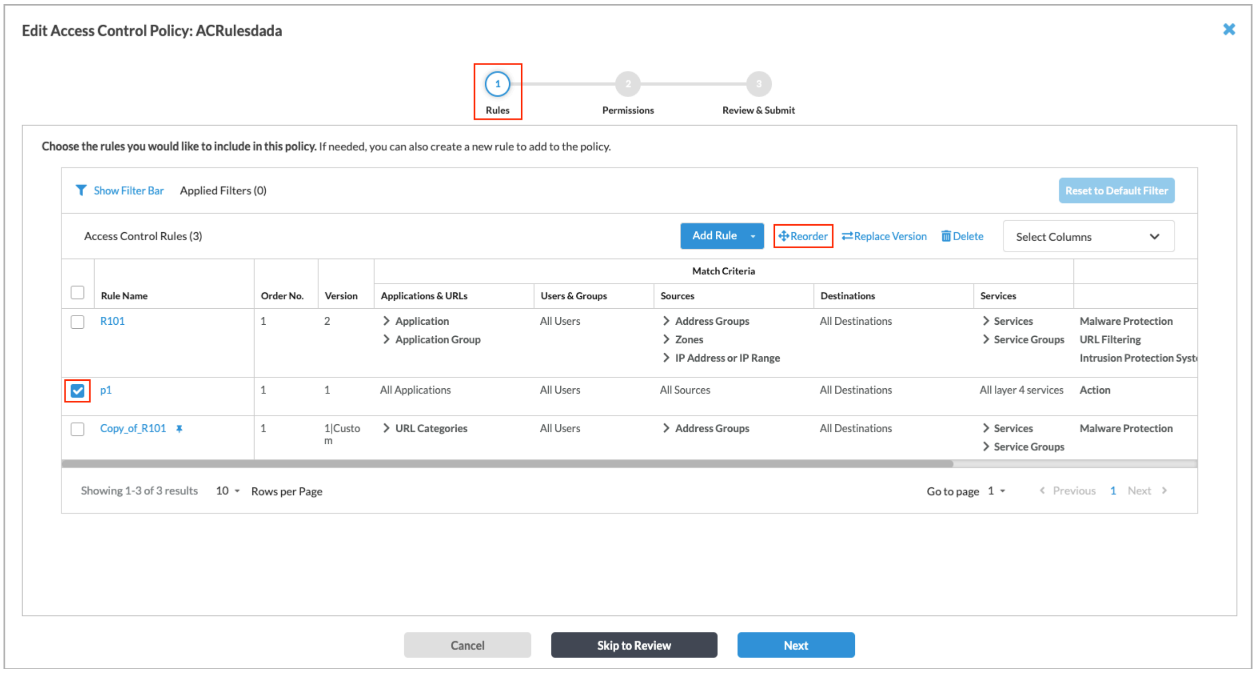
12. Review the settings you have selected. Click the ✏ Edit icon to change a setting, as needed.
13. Click Save to create the access control policy.

Reorder the Rules in an Access Control Policy

An access control policy that has multiple rules processes the rules in the order that they appear on the screen. To process the rules in a different order, you reorder the list of rules.

To reorder the rules in an access control policy:

1. In Tenant view, go to the Configure lifecycle in the left menu bar.
2. Select Profile Elements > Policies > Security > Access Control. The Access Control Rules screen displays all the configured policies.
3. Click the name of a policy. A screen similar to the following displays.



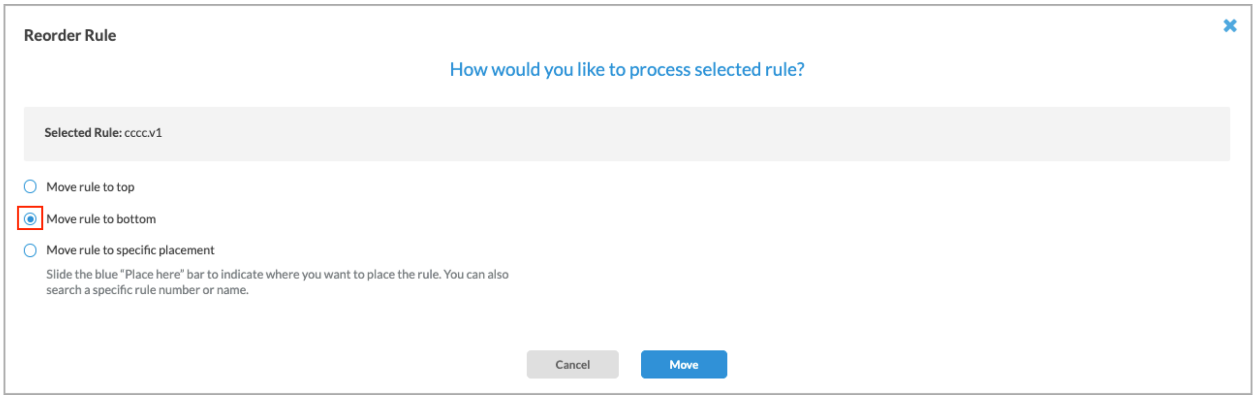
Edit Access Control Policy: ACRulesdada

Choose the rules you would like to include in this policy. If needed, you can also create a new rule to add to the policy.

Access Control Rules (3)

				Match Criteria					
□	Rule Name	Order No.	Version	Applications & URLs	Users & Groups	Sources	Destinations	Services	
□	R101	1	2	> Application > Application Group	All Users	> Address Groups > Zones > IP Address or IP Range	All Destinations	> Services > Service Groups	Malware Protection URL Filtering Intrusion Protection Syst
☑	p1	1	1	All Applications	All Users	All Sources	All Destinations	All layer 4 services	Action
□	Copy_of_R101	1	1|Custom	> URL Categories	All Users	> Address Groups	All Destinations	> Services > Service Groups	Malware Protection

4. Click Step 1, Rules. Select the rule that you want to move, and then click the ✥ Reorder icon. The following screen displays.



Reorder Rule

How would you like to process selected rule?

Selected Rule: cccc.v1

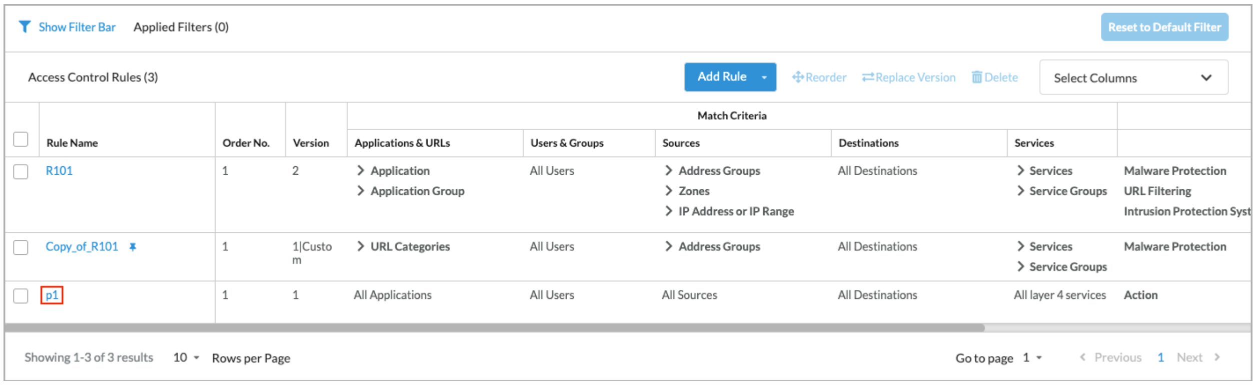
○ Move rule to top

● Move rule to bottom

○ Move rule to specific placement

Slide the blue "Place here" bar to indicate where you want to place the rule. You can also search a specific rule number or name.

5. Click the radio button to move the rule to the desired location.
6. Click Move. The following screenshot shows that rule p1 has been moved to the bottom of the list.



				Match Criteria					
□	Rule Name	Order No.	Version	Applications & URLs	Users & Groups	Sources	Destinations	Services	
□	R101	1	2	> Application > Application Group	All Users	> Address Groups > Zones > IP Address or IP Range	All Destinations	> Services > Service Groups	Malware Protection URL Filtering Intrusion Protection Syst
□	Copy_of_R101	1	1|Custom	> URL Categories	All Users	> Address Groups	All Destinations	> Services > Service Groups	Malware Protection
□	p1	1	1	All Applications	All Users	All Sources	All Destinations	All layer 4 services	Action

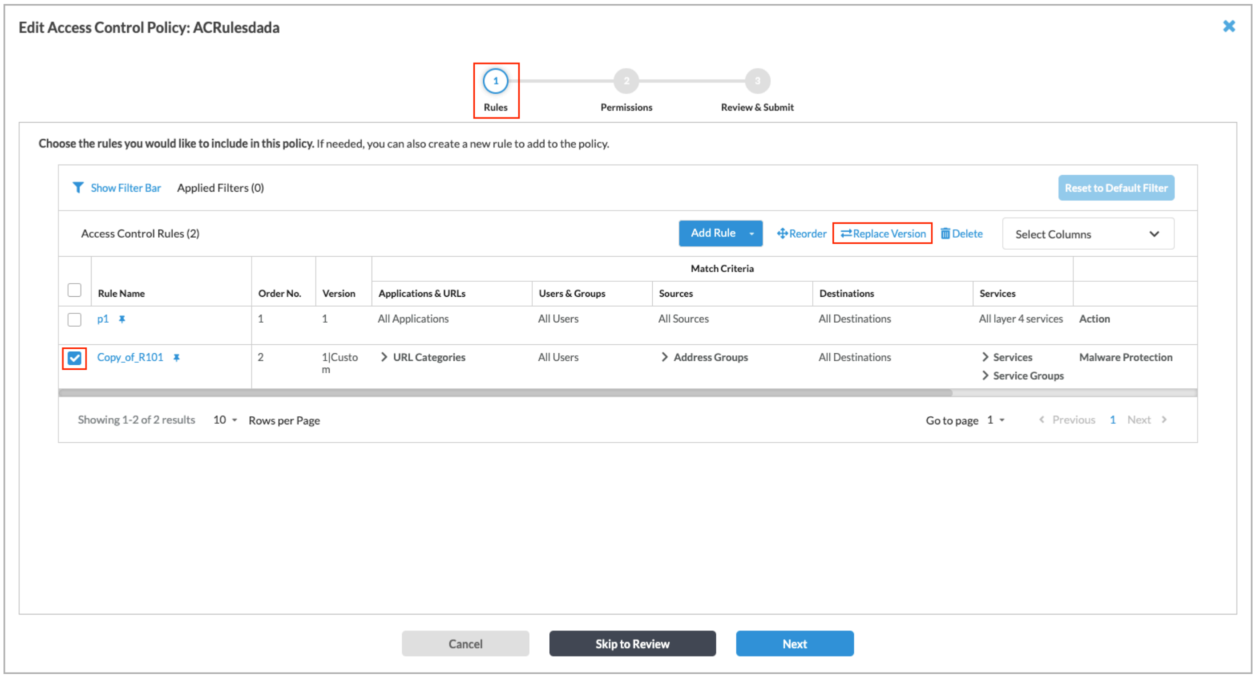
7. Click Next to to go Step 2, Permissions, and revise the permissions as needed.
8. Click Next to go to Step 3, Review and Submit.
9. Review the rule details and make any necessary changes.
10. Click Save to save the changes to the rule.

Replace the Version of a Rule in a Policy

If you create two or more versions of a rule, you can replace one version of the rule with a different version of the same rule.

To replace the version of a rule in an access control policy:

1. In Tenant view, go to the Configure lifecycle in the left menu bar.
2. Select Profiles > Profile Elements > Policies > Security > Access Control. The Access Control Rules screen displays all the configured policies.
3. Click the name of a policy. A screen similar to the following displays.



Edit Access Control Policy: ACRulesdada

Choose the rules you would like to include in this policy. If needed, you can also create a new rule to add to the policy.

				Match Criteria					
□	Rule Name	Order No.	Version	Applications & URLs	Users & Groups	Sources	Destinations	Services	
□	p1	1	1	All Applications	All Users	All Sources	All Destinations	All layer 4 services	Action
☑	Copy_of_R101	2	1|Custom	> URL Categories	All Users	> Address Groups	All Destinations	> Services > Service Groups	Malware Protection

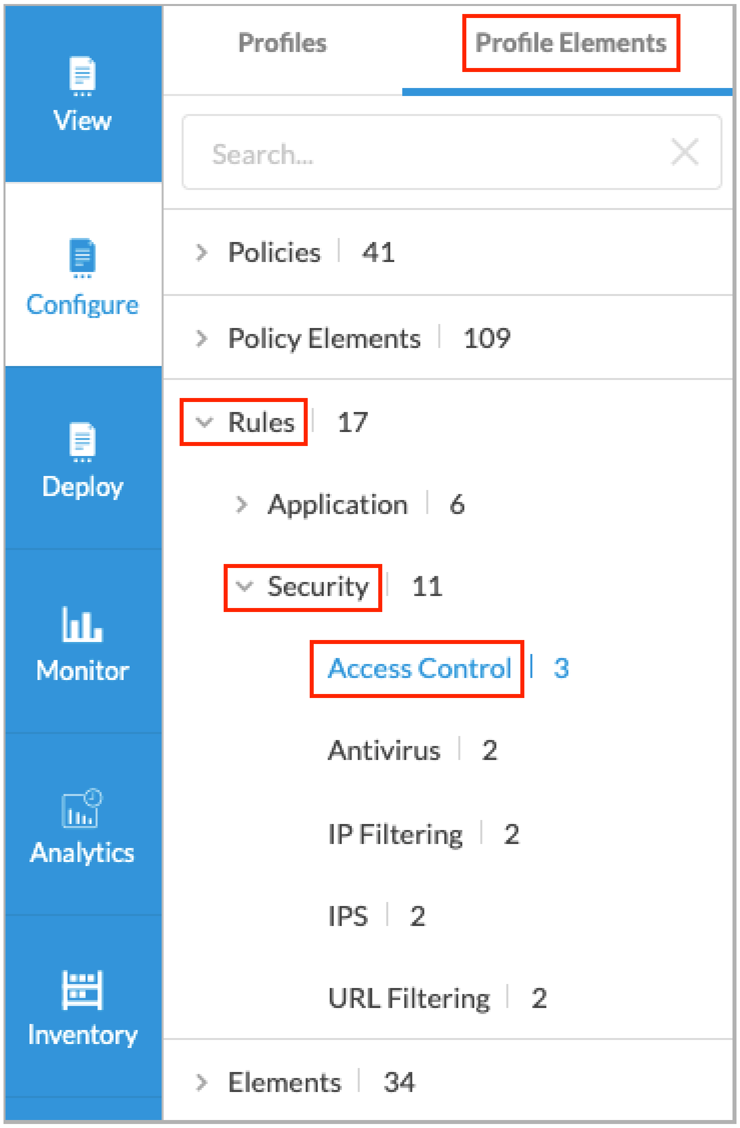
Showing 1-2 of 2 results 10 Rows per Page

Go to page 1 Previous 1 Next

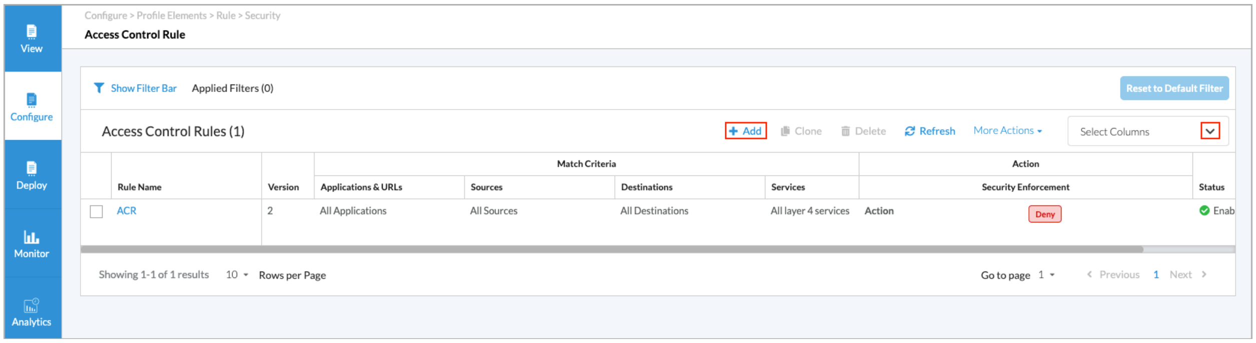
4. Click Step 1, Rules. Select the rule that you want to replace with a different version, and then click the ⇄ Replace Version icon. The Replace Version popup window displays.
5. Select the version of the rule to replace the current version.
6. Click Save.

Configure an Access Control Rule

1. In Tenant view, go to the Configure lifecycle in the left menu bar.
2. Select Profile Elements > Rules > Security > Access Control.



3. The Access Control Rules screen displays the rules that are already configured.



Access Control Rule

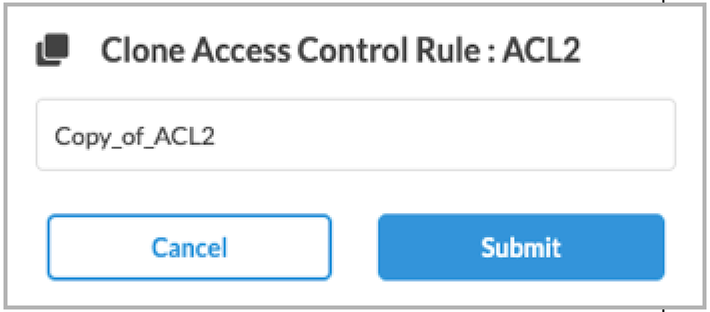
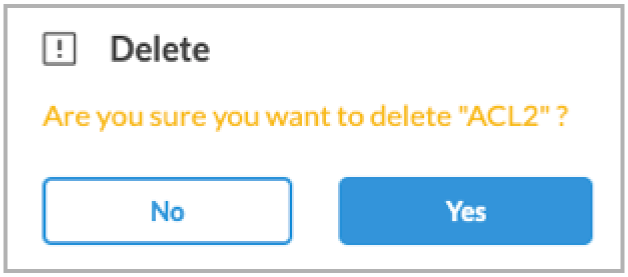
Access Control Rules (1)

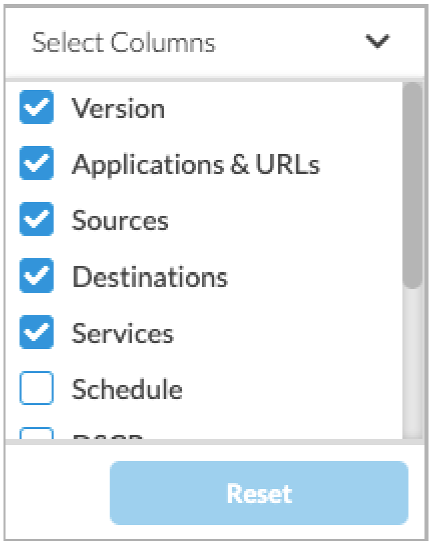
			Match Criteria				Action	
	Rule Name	Version	Applications & URLs	Sources	Destinations	Services	Security Enforcement	Status
□	ACR	2	All Applications	All Sources	All Destinations	All layer 4 services	Action Deny	✓ Enab

Showing 1-1 of 1 results 10 Rows per Page

Go to page 1 Previous 1 Next

4. In the horizontal menu bar, you can perform the following operations.

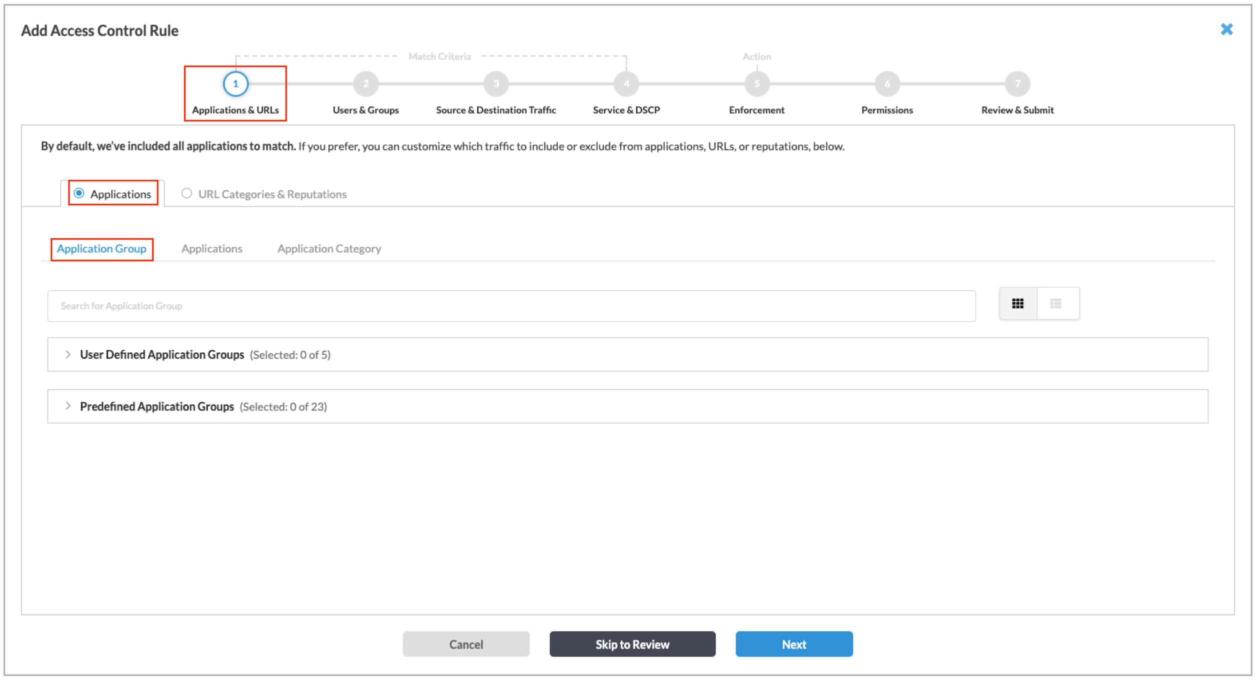
Menu Selection	Description
+ Add	Add a new access control rule. Active when no existing rule is selected. See Step 4 below.
Clone	Clone the selected rule. A popup window similar to the following displays:  Clone Access Control Rule : ACL2 Copy_of_ACL2 Rename the default name of the cloned rule (here, Copy_of_ACL2), if desired, and then click Submit.
Delete	Delete the selected rule. A popup window similar to the following displays:  Delete Are you sure you want to delete "ACL2" ? Click Yes to delete the rule, or click No to retain the rule.
Refresh	Refresh the list of existing rules.
More Actions	Perform an action on the selected rule: ◦ Auto Delete or Disable Auto Delete—Enable or disable the automatic deletion of the rule. For

Menu Selection	Description
	more information, see Configure Automatic Deletion of SD-WAN Object Versions. ◦ Compare Versions—View the differences between two versions of a rule. ◦ Propagate—Propagate changes made to a rule to any entities that use the rule. For more information, see Propagate Object Configuration Changes. ◦ View References—View the objects that refer to the selected rule. For more information, see View References to Objects in the Configuration Hierarchies.
Select Columns	To select the columns that you want to display, click the down arrow. To return to the default column selection, click Reset.  Select Columns ☑ Version ☑ Applications & URLs ☑ Sources ☑ Destinations ☑ Services ☐ Schedule Reset The column headings options are: ◦ Version ◦ Applications & URLs ◦ Sources ◦ Destinations ◦ Services

Menu Selection	Description
	◦ Schedule ◦ DSCP ◦ Security Enforcement ◦ Variables ◦ Status ◦ Last Modified

5. To locate rules, you can filter them by clicking the ▼ Show Filter Bar icon. For more information, see Step 6b in Configure Access Control Policies, above.

6. To create a rule, click the ✚ Add icon. The Access Control Rule configuration wizard displays, and the Step 1, Applications & URLs, the Applications radio button, and the Application Group tab are selected. By default, all applications, URLs, and reputations match the rule.

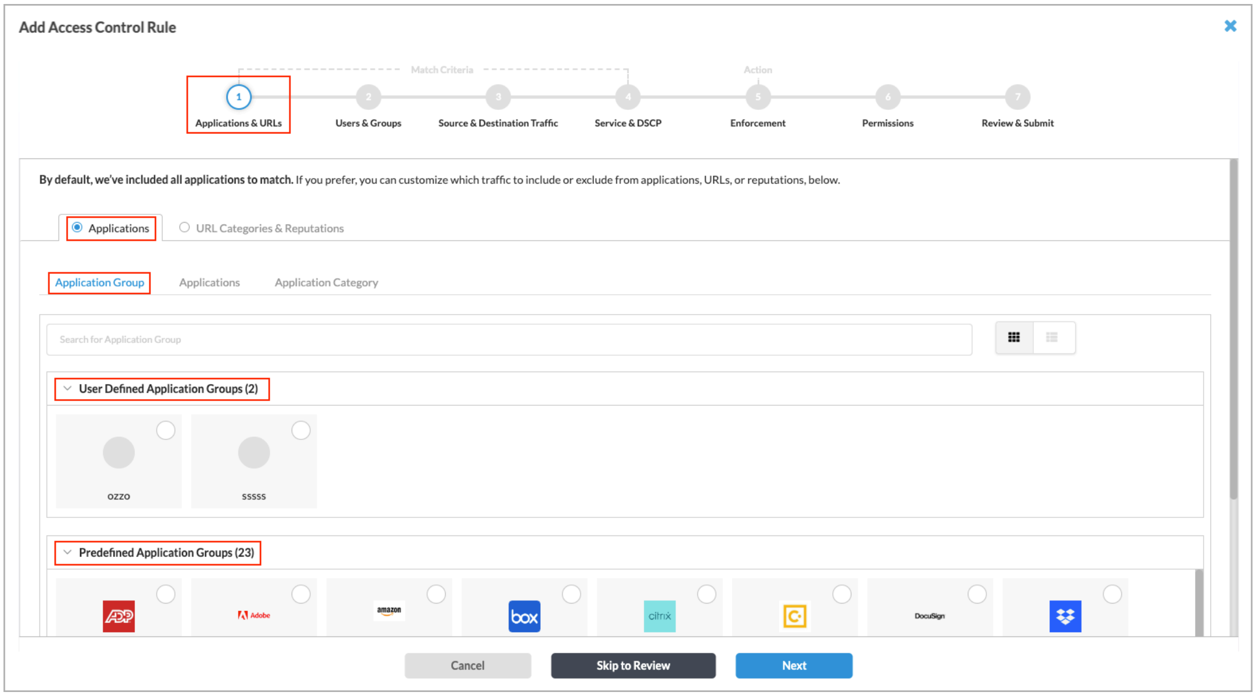


By default, we've included all applications to match. If you prefer, you can customize which traffic to include or exclude from applications, URLs, or reputations, below.

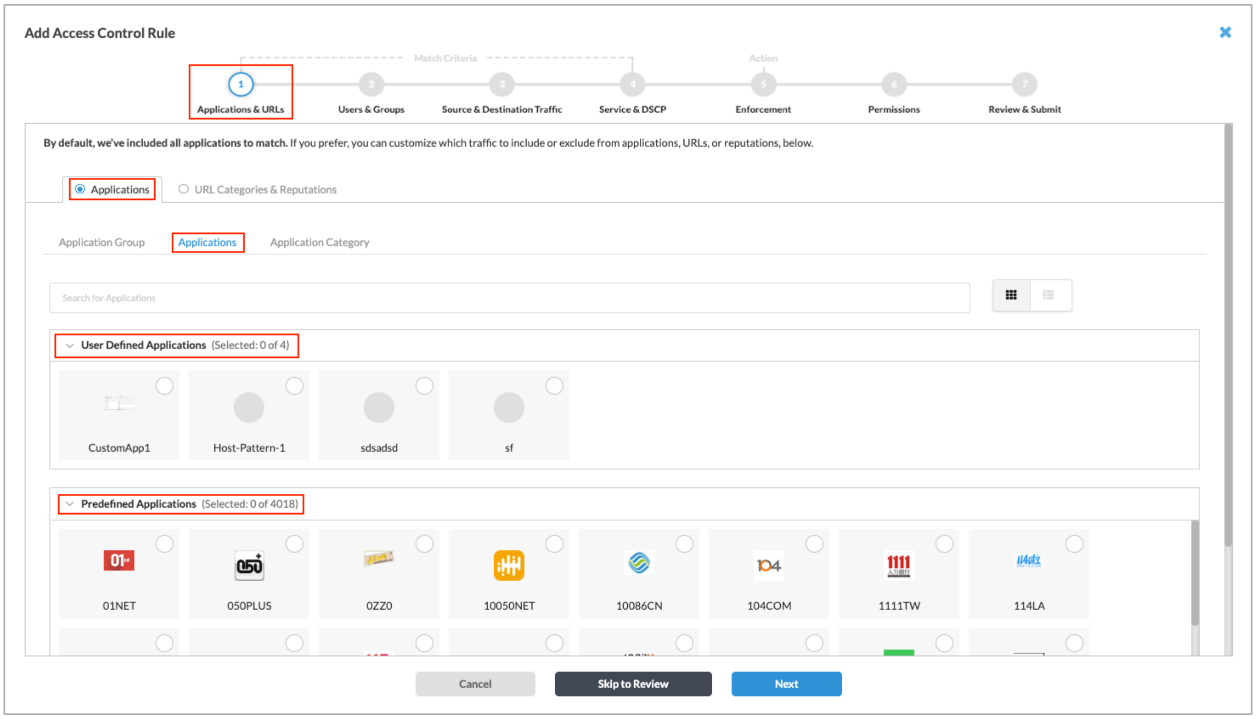
› **User Defined Application Groups** (Selected: 0 of 5)

› **Predefined Application Groups** (Selected: 0 of 23)

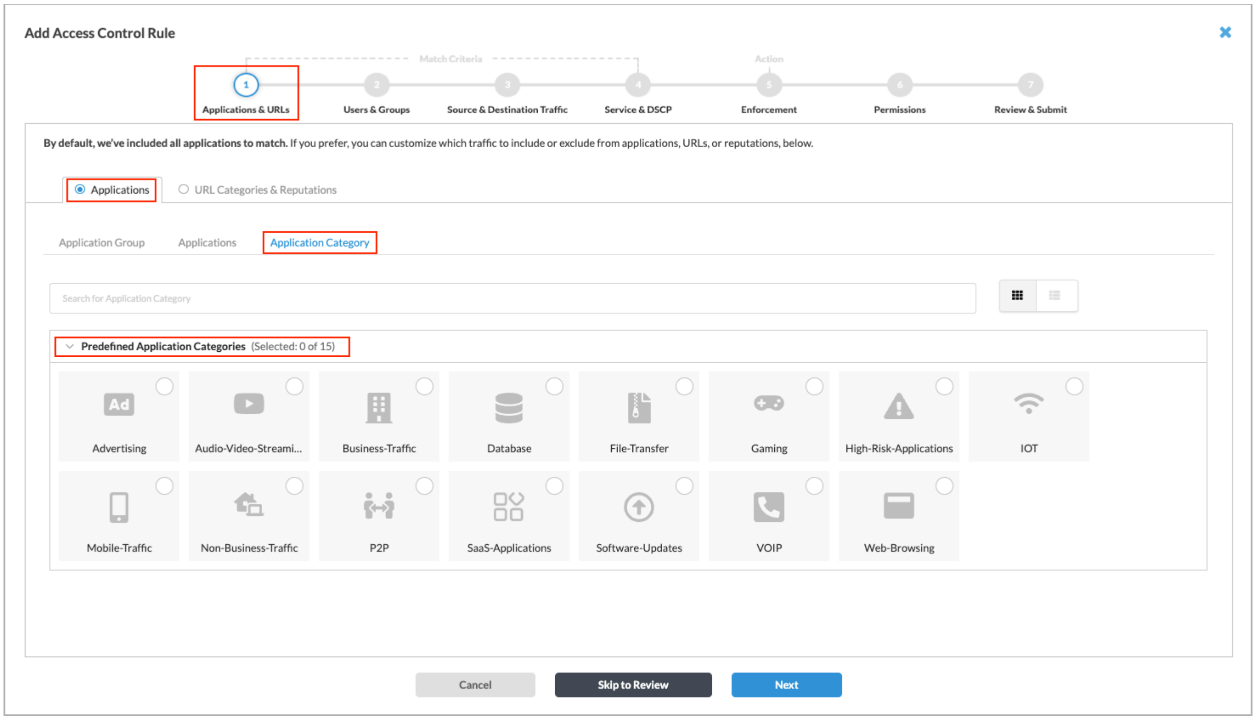
7. To select specific application groups to include or exclude in the rule, click User Defined Application Groups, Predefined Application Groups, or both. Then select the application groups for the rule to match. You can use the Search bar to find specific application groups.


Add Access Control Rule
Match Criteria
Action
1 Applications & URLs
2 Users & Groups
3 Source & Destination Traffic
4 Service & DSCP
5 Enforcement
6 Permissions
7 Review & Submit
By default, we've included all applications to match. If you prefer, you can customize which traffic to include or exclude from applications, URLs, or reputations, below.
● Applications
○ URL Categories & Reputations
Application Group
Applications
Application Category
Search for Application Group
User Defined Application Groups (2)
ozzo
sssss
Predefined Application Groups (23)
Cancel
Skip to Review
Next

8. Select the Applications > Applications tab, and then select one or more user-defined and predefined applications for the rule to match. You can use the Search bar to find specific applications.



9. Select the Applications > Application Category tab, and then select one or more predefined application categories for the rule to match. You can use the Search bar to find specific application categories.



By default, we've included all applications to match. If you prefer, you can customize which traffic to include or exclude from applications, URLs, or reputations, below.

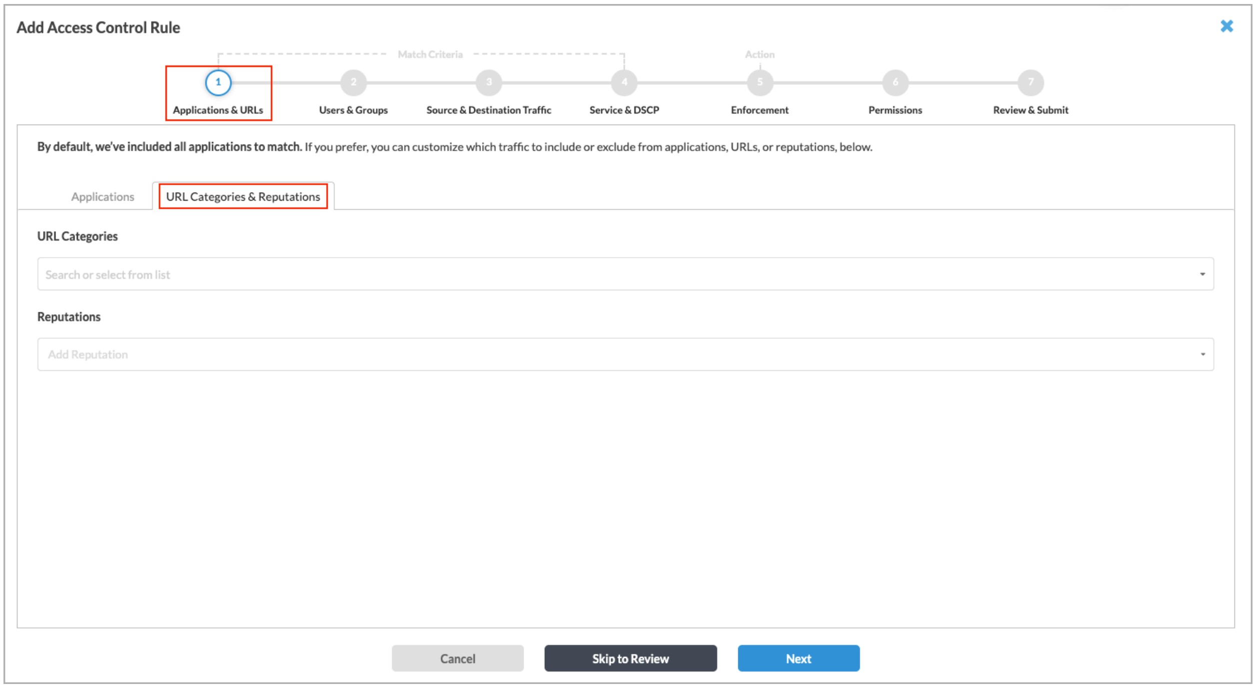
● Applications ○ URL Categories & Reputations

Application Group | Applications | Application Category

Search for Application Category

Predefined Application Categories (Selected: 0 of 15)

10. Select the URLs and Reputations tab. The following screen displays.



By default, we've included all applications to match. If you prefer, you can customize which traffic to include or exclude from applications, URLs, or reputations, below.

Applications | URL Categories & Reputations

URL Categories

Search or select from list

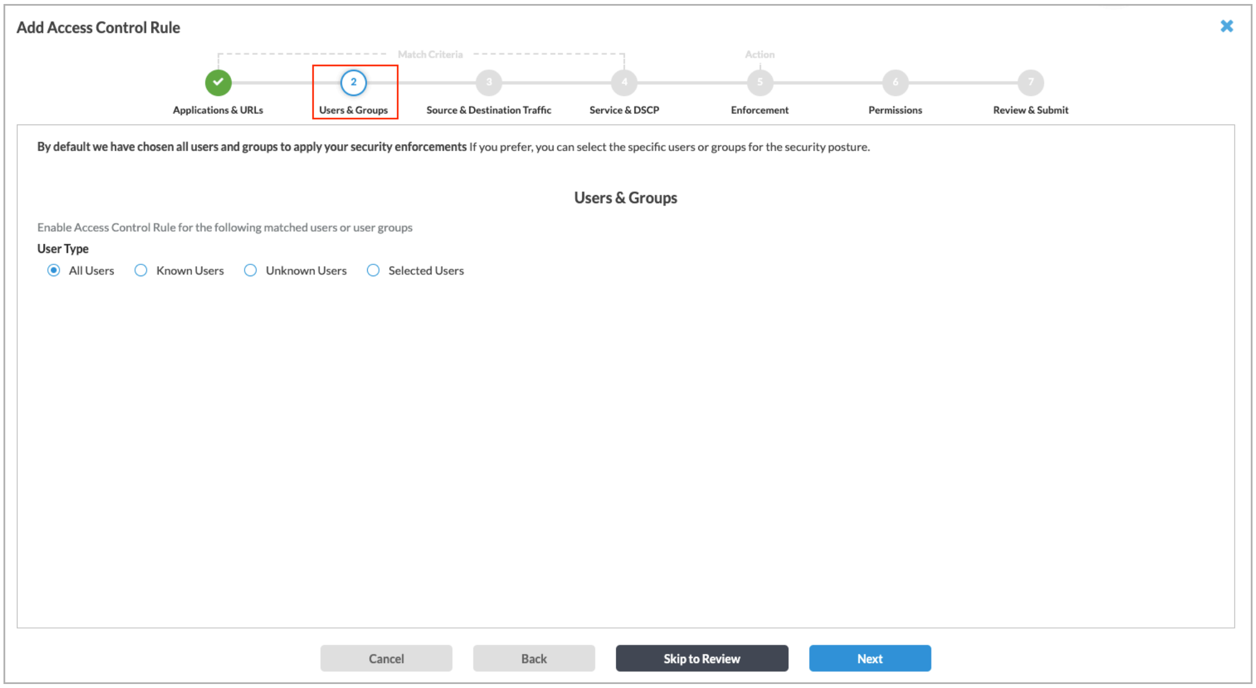
Reputations

Add Reputation

11. In the URL Categories field, click the down arrow, and then select one or more URL categories for the rule to match.

12. In the Reputations field, click the down arrow, and then select one or more reputations to include in the rule:
    - High risk
    - Low risk
    - Moderate risk
    - Suspicious
    - Trustworthy
    - Undefined

13. Click Next or select Step 2, Users and Groups. The following screen displays. By default, access control rules are applied to all users. You can select known users, unknown users, or selected users to which to apply the rule.

    By default we have chosen all users and groups to apply your security enforcements If you prefer, you can select the specific users or groups for the security posture.

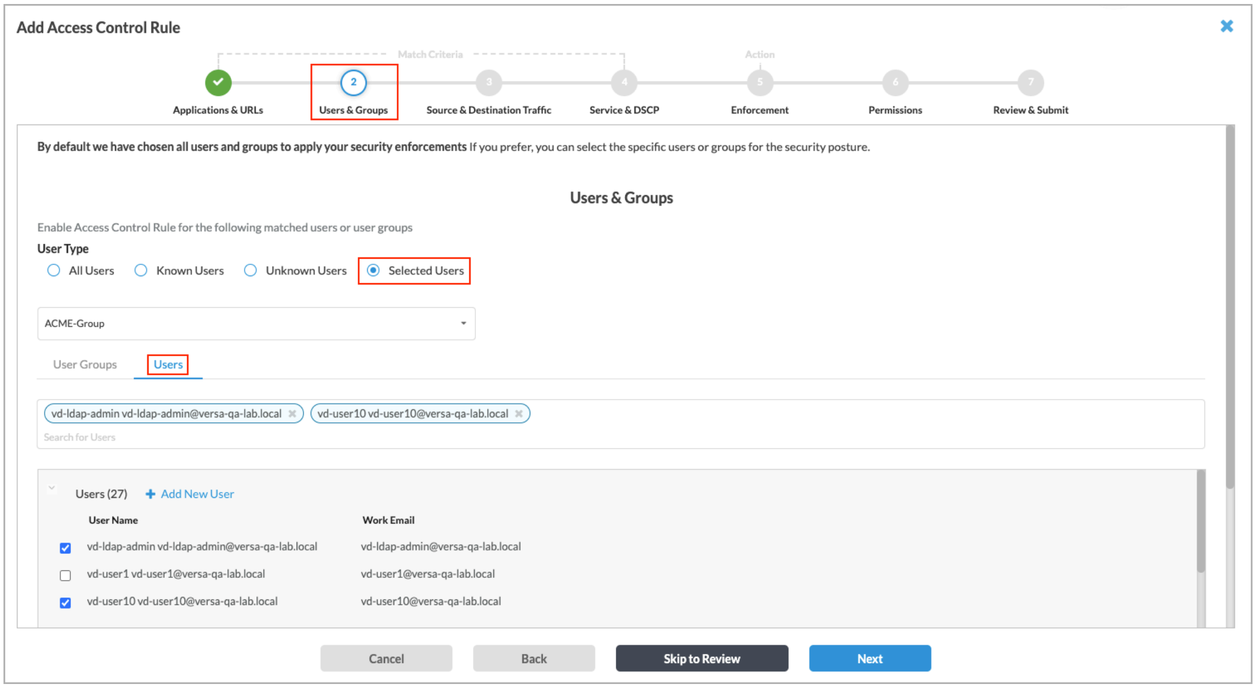
    Users & Groups

    Enable Access Control Rule for the following matched users or user groups

    User Type

    ● All Users ○ Known Users ○ Unknown Users ○ Selected Users

    If you choose Selected Users, the following screen displays.



By default we have chosen all users and groups to apply your security enforcements If you prefer, you can select the specific users or groups for the security posture.

Users & Groups

Enable Access Control Rule for the following matched users or user groups

User Type

○ All Users ○ Known Users ○ Unknown Users ● Selected Users

ACME-Group

User Groups | Users

vd-ldap-admin vd-ldap-admin@versa-qa-lab.local ✕ vd-user10 vd-user10@versa-qa-lab.local ✕

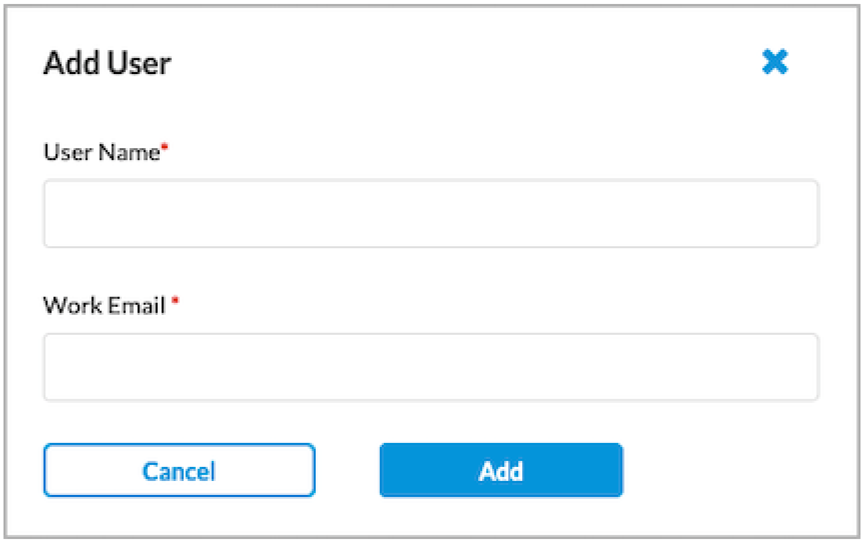
Search for Users

Users (27) ✚ Add New User

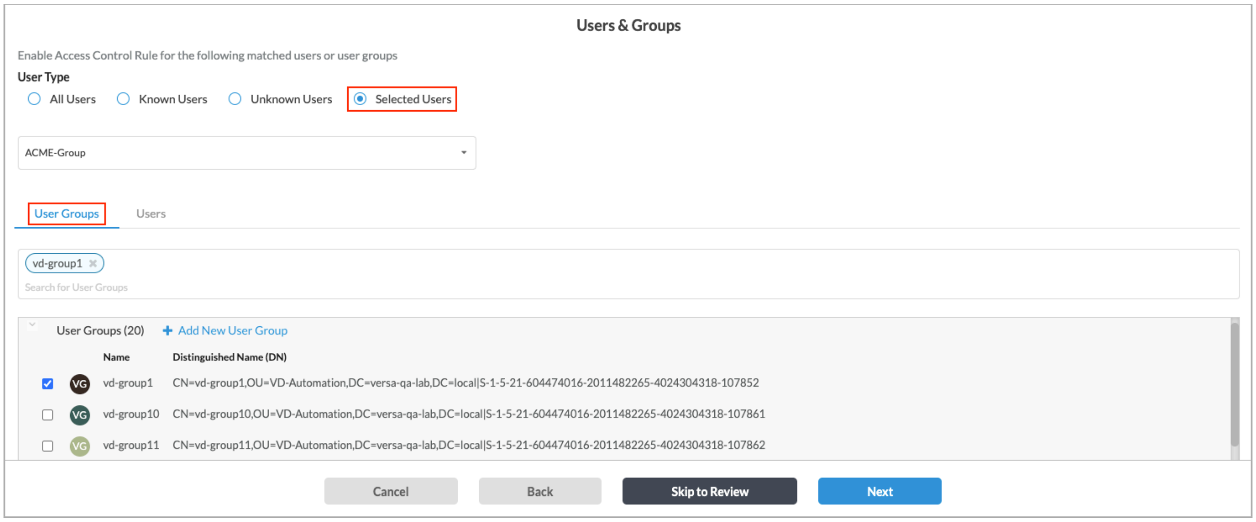
	User Name	Work Email
☑	vd-ldap-admin vd-ldap-admin@versa-qa-lab.local	vd-ldap-admin@versa-qa-lab.local
□	vd-user1 vd-user1@versa-qa-lab.local	vd-user1@versa-qa-lab.local
☑	vd-user10 vd-user10@versa-qa-lab.local	vd-user10@versa-qa-lab.local

14. In the Enable Access Control Rule field, select the access control rule for matched users and groups.

15. Click ✚ Add New User to add a new user. The Add User popup window displays.



16. Enter the user's name and work email in the fields provided, then click Add. You can add multiple users.
17. Select the User Groups tab to apply the access control rule to a user group.



Users & Groups

Enable Access Control Rule for the following matched users or user groups

User Type

○ All Users ○ Known Users ○ Unknown Users ● Selected Users

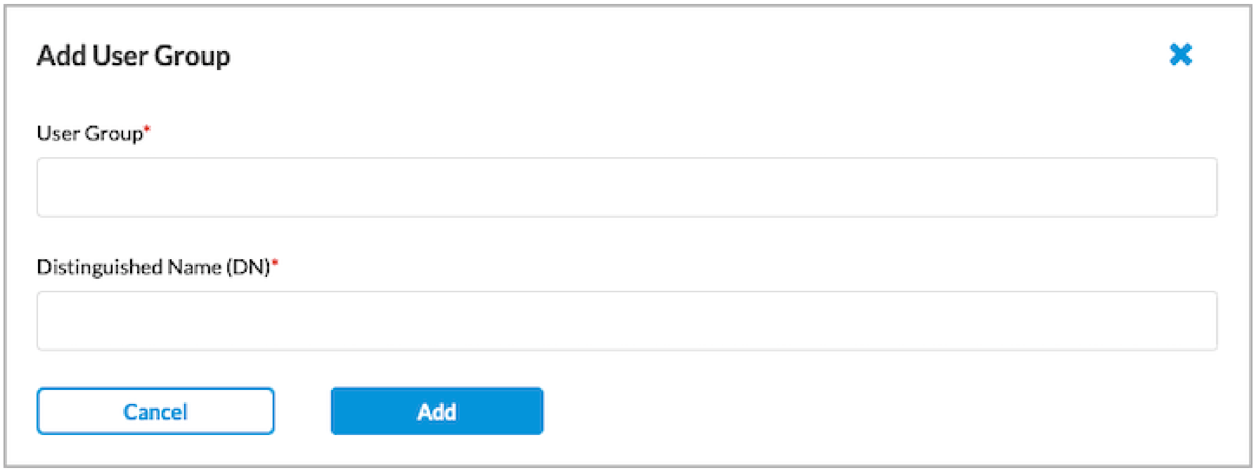
ACME-Group

vd-group1

User Groups (20) + Add New User Group

		Name	Distinguished Name (DN)
☑	VG	vd-group1	CN=vd-group1,OU=VD-Automation,DC=versa-qa-lab,DC=local|S-1-5-21-604474016-2011482265-4024304318-107852
□	VG	vd-group10	CN=vd-group10,OU=VD-Automation,DC=versa-qa-lab,DC=local|S-1-5-21-604474016-2011482265-4024304318-107861
□	VG	vd-group11	CN=vd-group11,OU=VD-Automation,DC=versa-qa-lab,DC=local|S-1-5-21-604474016-2011482265-4024304318-107862

18. Click + Add New User Group to add a new user group. The Add User Group popup window displays.

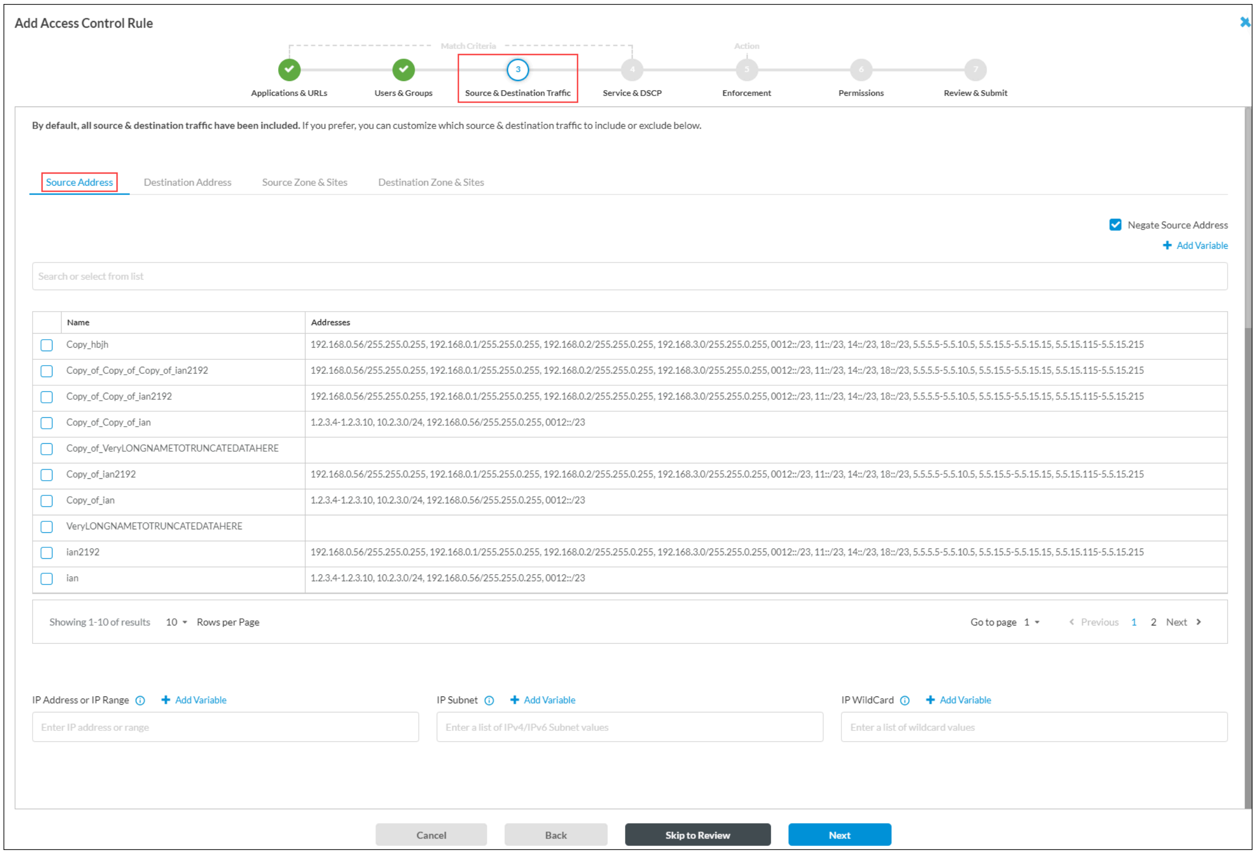


Add User Group

User Group*

Distinguished Name (DN)*

19. Enter a user group name and Distinguished Name in the fields provided, and then click Add. You can add multiple user groups.
20. Click Next or select Step 3, Source & Destination Traffic. The following screen displays with the Source Address tab selected by default. All source and destination traffic is included by default. You can customize which source and destination traffic for the rule to match.



By default, all source & destination traffic have been included. If you prefer, you can customize which source & destination traffic to include or exclude below.

☑ Negate Source Address

	Name	Addresses
□	Copy_hbjh	192.168.0.56/255.255.0.255, 192.168.0.1/255.255.0.255, 192.168.0.2/255.255.0.255, 192.168.3.0/255.255.0.255, 0012::/23, 11::/23, 14::/23, 18::/23, 5.5.5.5-5.5.10.5, 5.5.15.5-5.5.15.15, 5.5.15.115-5.5.15.215
□	Copy_of_Copy_of_Copy_of_ian2192	192.168.0.56/255.255.0.255, 192.168.0.1/255.255.0.255, 192.168.0.2/255.255.0.255, 192.168.3.0/255.255.0.255, 0012::/23, 11::/23, 14::/23, 18::/23, 5.5.5.5-5.5.10.5, 5.5.15.5-5.5.15.15, 5.5.15.115-5.5.15.215
□	Copy_of_Copy_of_ian2192	192.168.0.56/255.255.0.255, 192.168.0.1/255.255.0.255, 192.168.0.2/255.255.0.255, 192.168.3.0/255.255.0.255, 0012::/23, 11::/23, 14::/23, 18::/23, 5.5.5.5-5.5.10.5, 5.5.15.5-5.5.15.15, 5.5.15.115-5.5.15.215
□	Copy_of_Copy_of_ian	1.2.3.4-1.2.3.10, 10.2.3.0/24, 192.168.0.56/255.255.0.255, 0012::/23
□	Copy_of_VeryLONGNAMETOTRUNCATEDATAHERE	
□	Copy_of_ian2192	192.168.0.56/255.255.0.255, 192.168.0.1/255.255.0.255, 192.168.0.2/255.255.0.255, 192.168.3.0/255.255.0.255, 0012::/23, 11::/23, 14::/23, 18::/23, 5.5.5.5-5.5.10.5, 5.5.15.5-5.5.15.15, 5.5.15.115-5.5.15.215
□	Copy_of_ian	1.2.3.4-1.2.3.10, 10.2.3.0/24, 192.168.0.56/255.255.0.255, 0012::/23
□	VeryLONGNAMETOTRUNCATEDATAHERE	
□	ian2192	192.168.0.56/255.255.0.255, 192.168.0.1/255.255.0.255, 192.168.0.2/255.255.0.255, 192.168.3.0/255.255.0.255, 0012::/23, 11::/23, 14::/23, 18::/23, 5.5.5.5-5.5.10.5, 5.5.15.5-5.5.15.15, 5.5.15.115-5.5.15.215
□	ian	1.2.3.4-1.2.3.10, 10.2.3.0/24, 192.168.0.56/255.255.0.255, 0012::/23

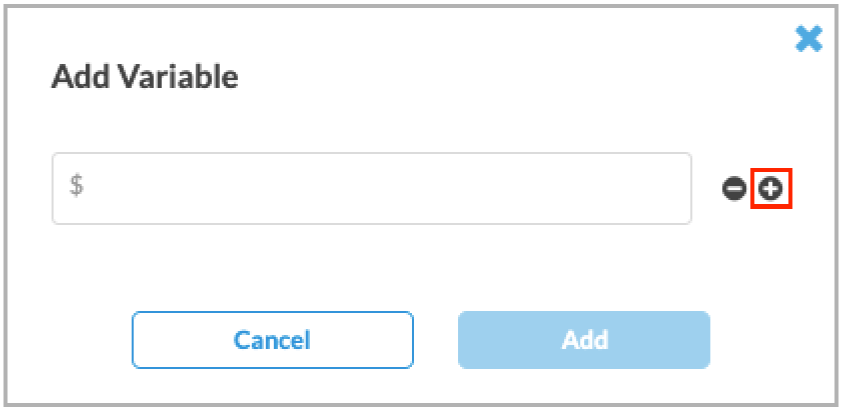
Showing 1-10 of results 10 Rows per Page Go to page 1 Previous 1 2 Next

IP Address or IP Range: Enter IP address or range

IP Subnet: Enter a list of IPv4/IPv6 Subnet values

IP WildCard: Enter a list of wildcard values

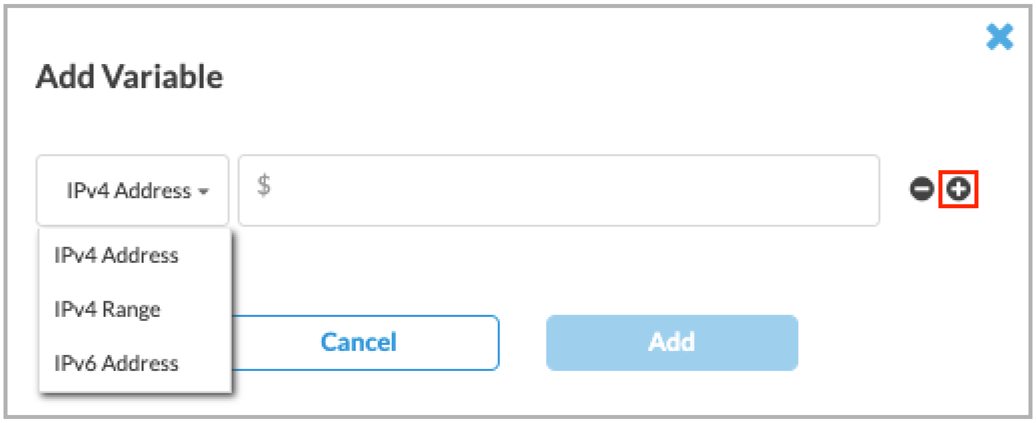
21. (For Releases 12.1.1 and later.) To customize the source traffic, on the Source Address tab, use one of the following methods:
    - To specify source addresses to include in the match criteria, continue with Step 22.
    - To specify source addresses to exclude from the match criteria, select Negate Source Address to match all source addresses except the source addresses that you specify, and then continue with Step 22.
22. Select a source address group to include or exclude for the rule to match. You can click + Add Variable to create a variable for the source address. Enter a name for the variable, click the ⊕ Plus icon, then click Add. You can add multiple variables before clicking the Add button.



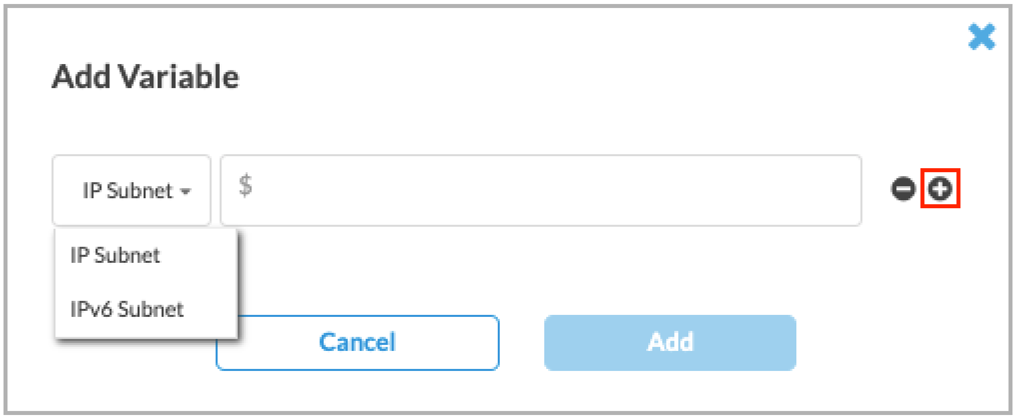
23. Enter values in any of the following fields for the rule to match: IP Address or IP Range, IP Subnet, or IP wildcard.

You can click + Add Variable to create variables for these values, and you can add multiple variables for each one.

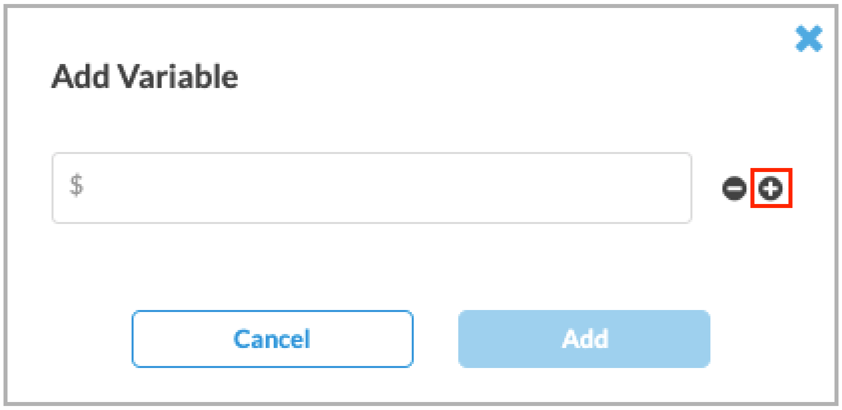
a. To add a variable for the IP address or IP range, select IPv4 Address, IPv4 Range, or IPv6 Address, click the ⊕ Plus icon, and then click Add.



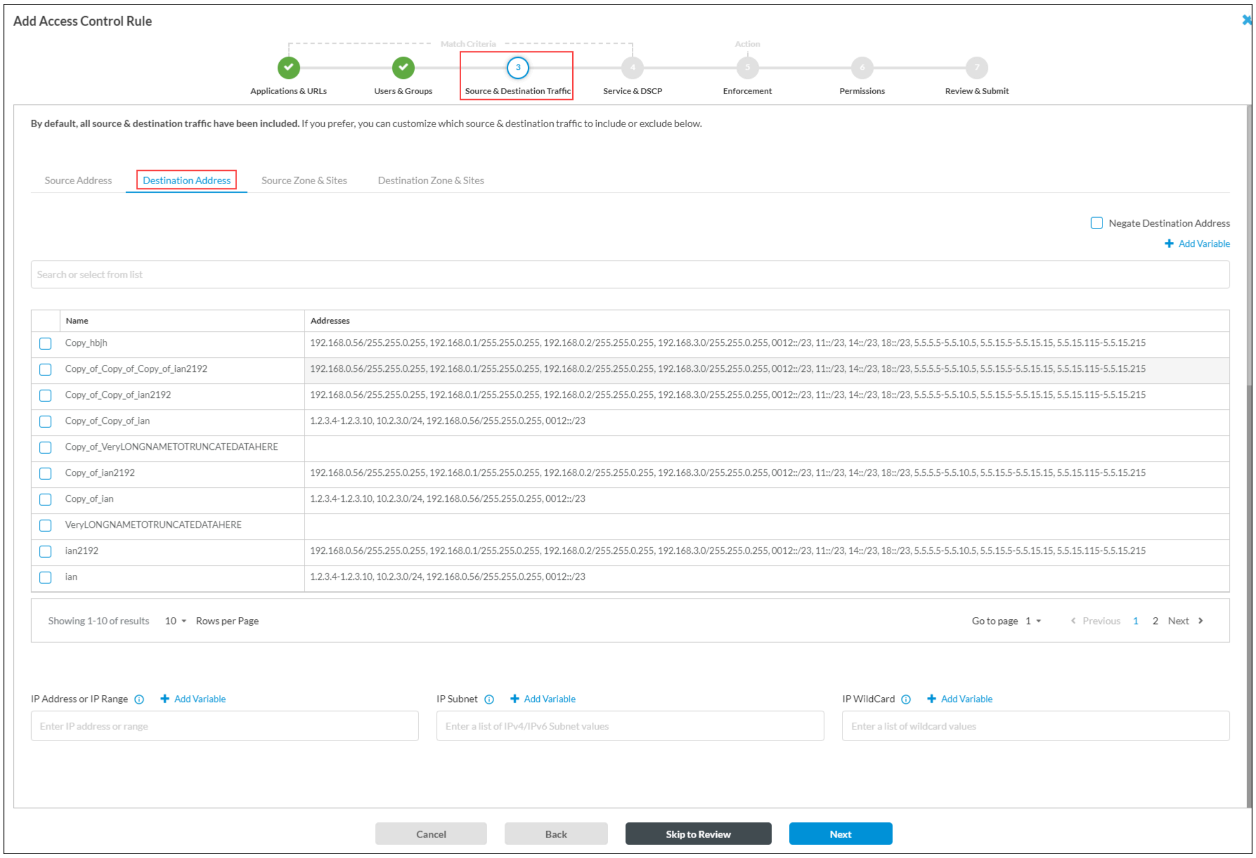
b. To add a variable for the IP subnet, select IP Subnet or IPv6 Subnet, click the ⊕ Plus icon, and then click Add.



c. To add a variable for the IP wildcard, enter a name for the variable, click the ⊕ Plus icon, and then click Add.



24. Click the Destination Address tab, select a destination address group to include or exclude for the rule to match, then enter values in any of the following fields for the rule to match: IP Address or IP Range, IP Subnet, or IP wildcard. You can click + Add Variable to create variables for these values.



By default, all source & destination traffic have been included. If you prefer, you can customize which source & destination traffic to include or exclude below.

□ Negate Destination Address

	Name	Addresses
□	Copy_hbjh	192.168.0.56/255.255.0.255, 192.168.0.1/255.255.0.255, 192.168.0.2/255.255.0.255, 192.168.3.0/255.255.0.255, 0012::/23, 11::/23, 14::/23, 18::/23, 5.5.5.5-5.5.10.5, 5.5.15.5-5.5.15.15, 5.5.15.115-5.5.15.215
□	Copy_of_Copy_of_Copy_of_ian2192	192.168.0.56/255.255.0.255, 192.168.0.1/255.255.0.255, 192.168.0.2/255.255.0.255, 192.168.3.0/255.255.0.255, 0012::/23, 11::/23, 14::/23, 18::/23, 5.5.5.5-5.5.10.5, 5.5.15.5-5.5.15.15, 5.5.15.115-5.5.15.215
□	Copy_of_Copy_of_ian2192	192.168.0.56/255.255.0.255, 192.168.0.1/255.255.0.255, 192.168.0.2/255.255.0.255, 192.168.3.0/255.255.0.255, 0012::/23, 11::/23, 14::/23, 18::/23, 5.5.5.5-5.5.10.5, 5.5.15.5-5.5.15.15, 5.5.15.115-5.5.15.215
□	Copy_of_Copy_of_ian	1.2.3.4-1.2.3.10, 10.2.3.0/24, 192.168.0.56/255.255.0.255, 0012::/23
□	Copy_of_VeryLONGNAMETOTRUNCATEDATAHERE	
□	Copy_of_ian2192	192.168.0.56/255.255.0.255, 192.168.0.1/255.255.0.255, 192.168.0.2/255.255.0.255, 192.168.3.0/255.255.0.255, 0012::/23, 11::/23, 14::/23, 18::/23, 5.5.5.5-5.5.10.5, 5.5.15.5-5.5.15.15, 5.5.15.115-5.5.15.215
□	Copy_of_ian	1.2.3.4-1.2.3.10, 10.2.3.0/24, 192.168.0.56/255.255.0.255, 0012::/23
□	VeryLONGNAMETOTRUNCATEDATAHERE	
□	ian2192	192.168.0.56/255.255.0.255, 192.168.0.1/255.255.0.255, 192.168.0.2/255.255.0.255, 192.168.3.0/255.255.0.255, 0012::/23, 11::/23, 14::/23, 18::/23, 5.5.5.5-5.5.10.5, 5.5.15.5-5.5.15.15, 5.5.15.115-5.5.15.215
□	ian	1.2.3.4-1.2.3.10, 10.2.3.0/24, 192.168.0.56/255.255.0.255, 0012::/23

Showing 1-10 of results 10 Rows per Page

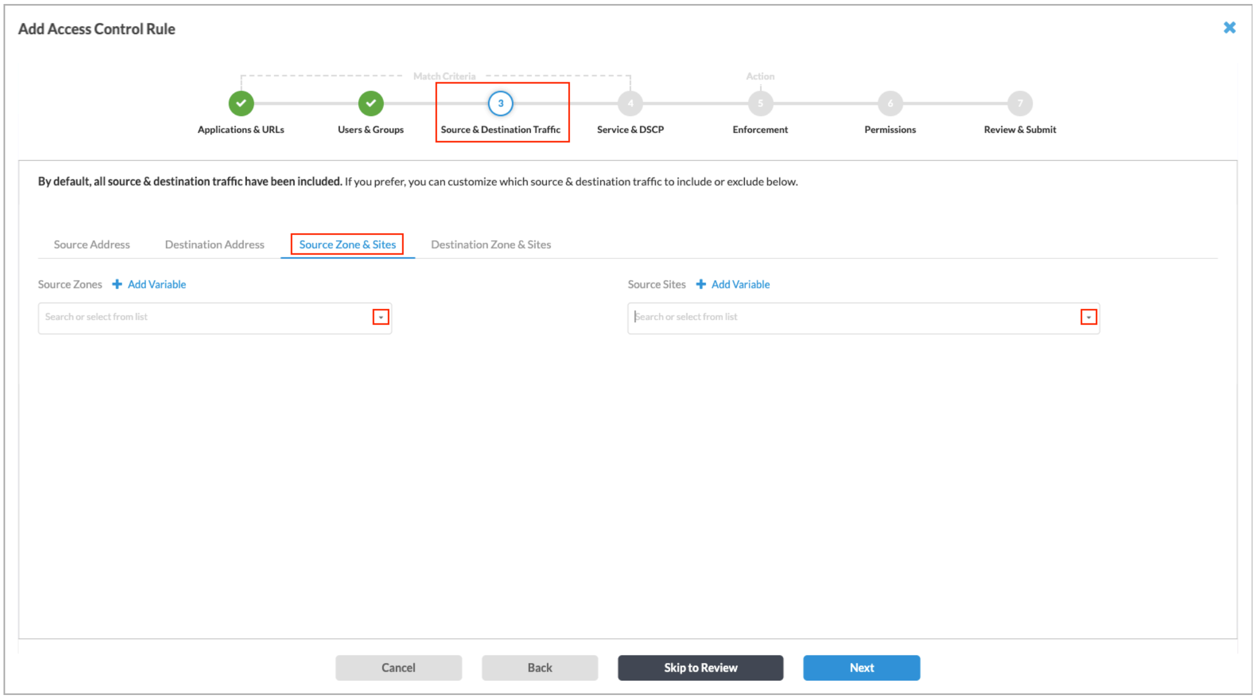
IP Address or IP Range ⓘ + Add Variable
Enter IP address or range

IP Subnet ⓘ + Add Variable
Enter a list of IPv4/IPv6 Subnet values

IP WildCard ⓘ + Add Variable
Enter a list of wildcard values

25. (For Releases 12.1.1 and later.) To customize the destination traffic, on the Destination Address tab, use one of the following methods:
    - To specify destination addresses to include in the match criteria, continue with Step 26.
    - To specify destination addresses to exclude from the match criteria, select Negate Destination Address to match all destination addresses except the destination addresses that you specify, and then continue with Step 26.

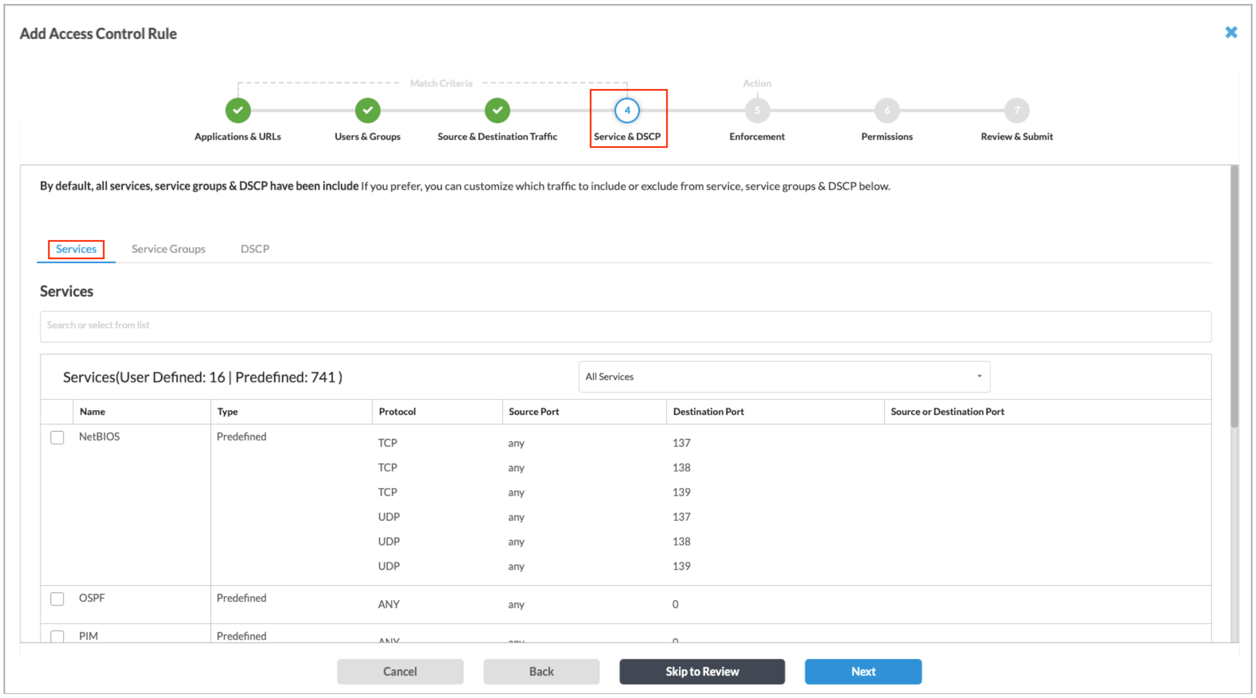
26. To specify a destination address to include or exclude in the match criteria, you can select a destination address from the list or use the search box to find a source address. To create a variable for the destination address, click + Add Variable to the right of the destination address list. As part of the match criter, you can enter values for the fields IP address or IP range, IP subnet, and IP wildcard. To create variables for these values, click + Add Variable for that field. For more information on adding variables, see Steps 22 and 23.
27. Select the Source Zone and Sites tab, and then enter information for the following fields.



By default, all source & destination traffic have been included. If you prefer, you can customize which source & destination traffic to include or exclude below.

Field	Description
Source Zones	Click the down arrow, and then select one or more zones. To create a variable for the source zone, click ✚ Add Variable.
Source Sites	Click the down arrow, and then select one or more sites. To create a variable for the source zone, click ✚ Add Variable.

28. Select the Destination Zone and Sites tab, and then enter the information for the destination zone and destination site. The fields are the same as for the Source Zone and Sites shown above.
29. Click Next or select Step 4, Service & DSCP. The following screen displays with the Services tab selected by default, and all services, service groups, and DSCPs are included in the match criteria. You can customize the services, service groups, and DSCPs for the rule to match.



By default, all services, service groups & DSCP have been include If you prefer, you can customize which traffic to include or exclude from service, service groups & DSCP below.

Services

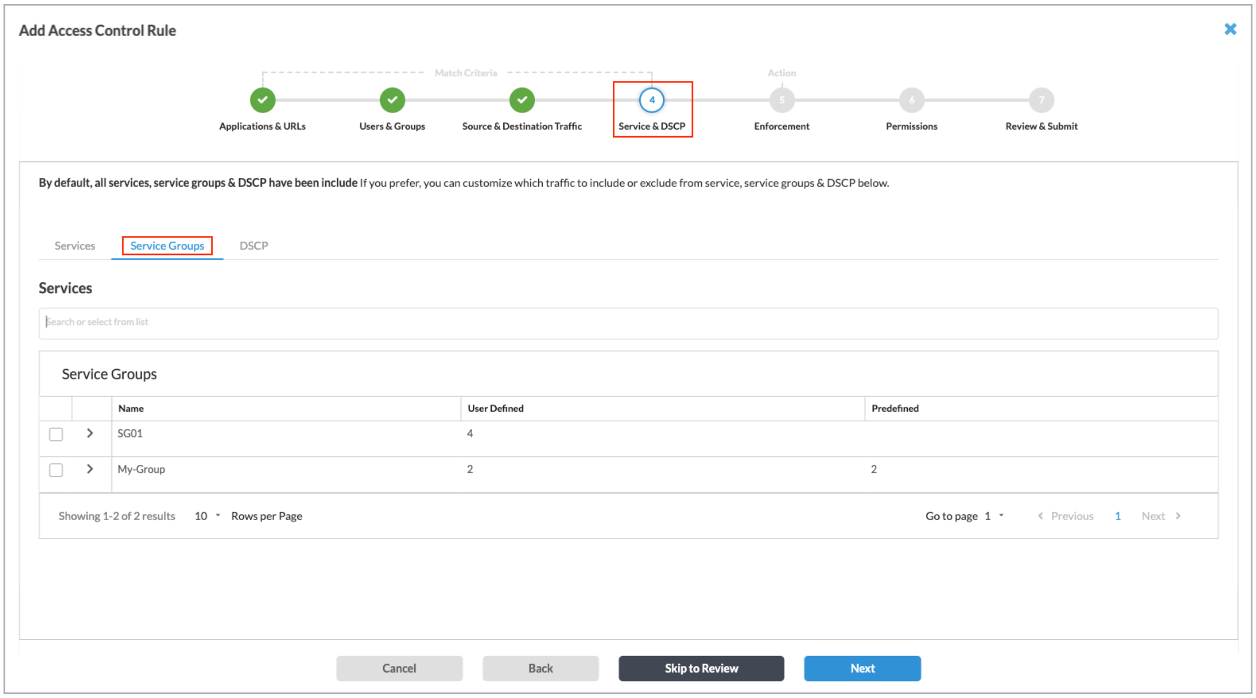
Search or select from list

Services(User Defined: 16 | Predefined: 741)

All Services

	Name	Type	Protocol	Source Port	Destination Port	Source or Destination Port
□	NetBIOS	Predefined	TCP TCP TCP UDP UDP UDP	any any any any any any	137 138 139 137 138 139	
□	OSPF	Predefined	ANY	any	0	
□	PIM	Predefined	ANY	any	0	

30. To specify the services to include, do one or both of the following:
    - In the search box under Services, enter the service name.
    - Select one of the following services to filter:
        - All Services
        - Predefined
        - User Defined
31. Select the Service Groups tab, and then select the user-defined and predefined service groups to which to apply security access control rules. Click the > Toggle Row Expanded icon next to the service group name to view the details for each service group.



By default, all services, service groups & DSCP have been include If you prefer, you can customize which traffic to include or exclude from service, service groups & DSCP below.

Services

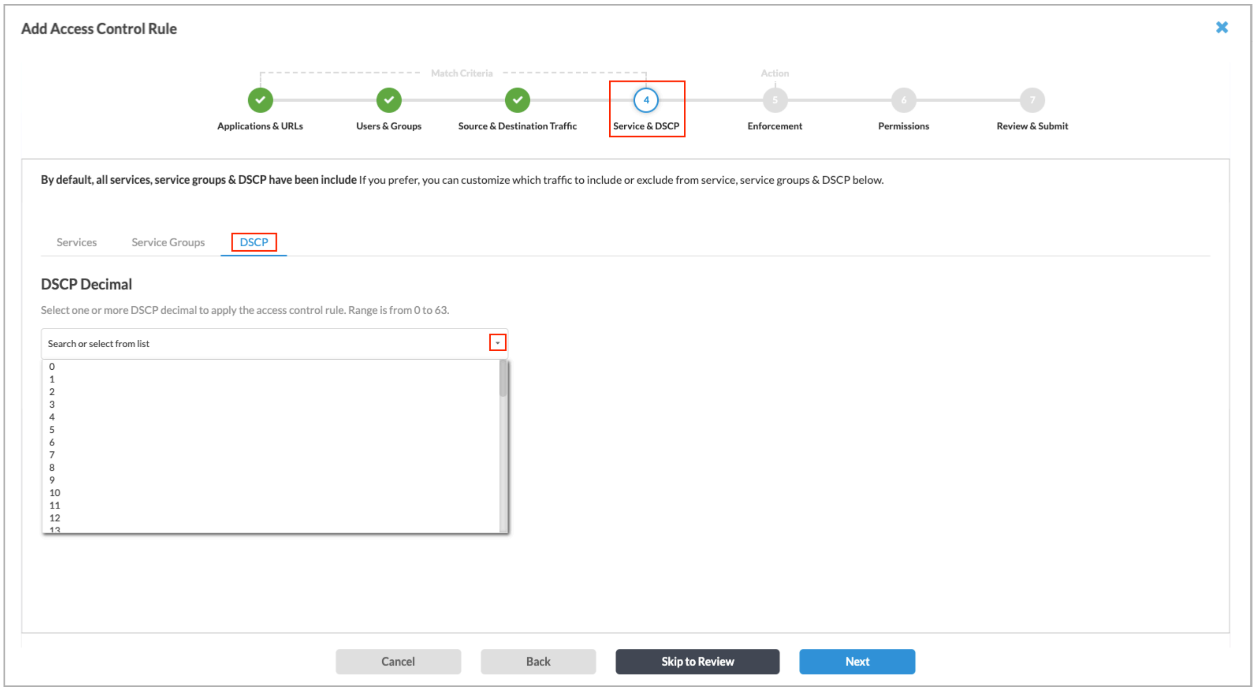
Search or select from list

Service Groups

		Name	User Defined	Predefined
□	>	SG01	4	
□	>	My-Group	2	2

Showing 1-2 of 2 results 10 Rows per Page Go to page 1 Previous 1 Next

32. Select the DSCP tab. All DSCP decimal values are included by default. You can specify which DSCP decimal values to include or exclude.



By default, all services, service groups & DSCP have been include If you prefer, you can customize which traffic to include or exclude from service, service groups & DSCP below.

DSCP Decimal

Select one or more DSCP decimal to apply the access control rule. Range is from 0 to 63.

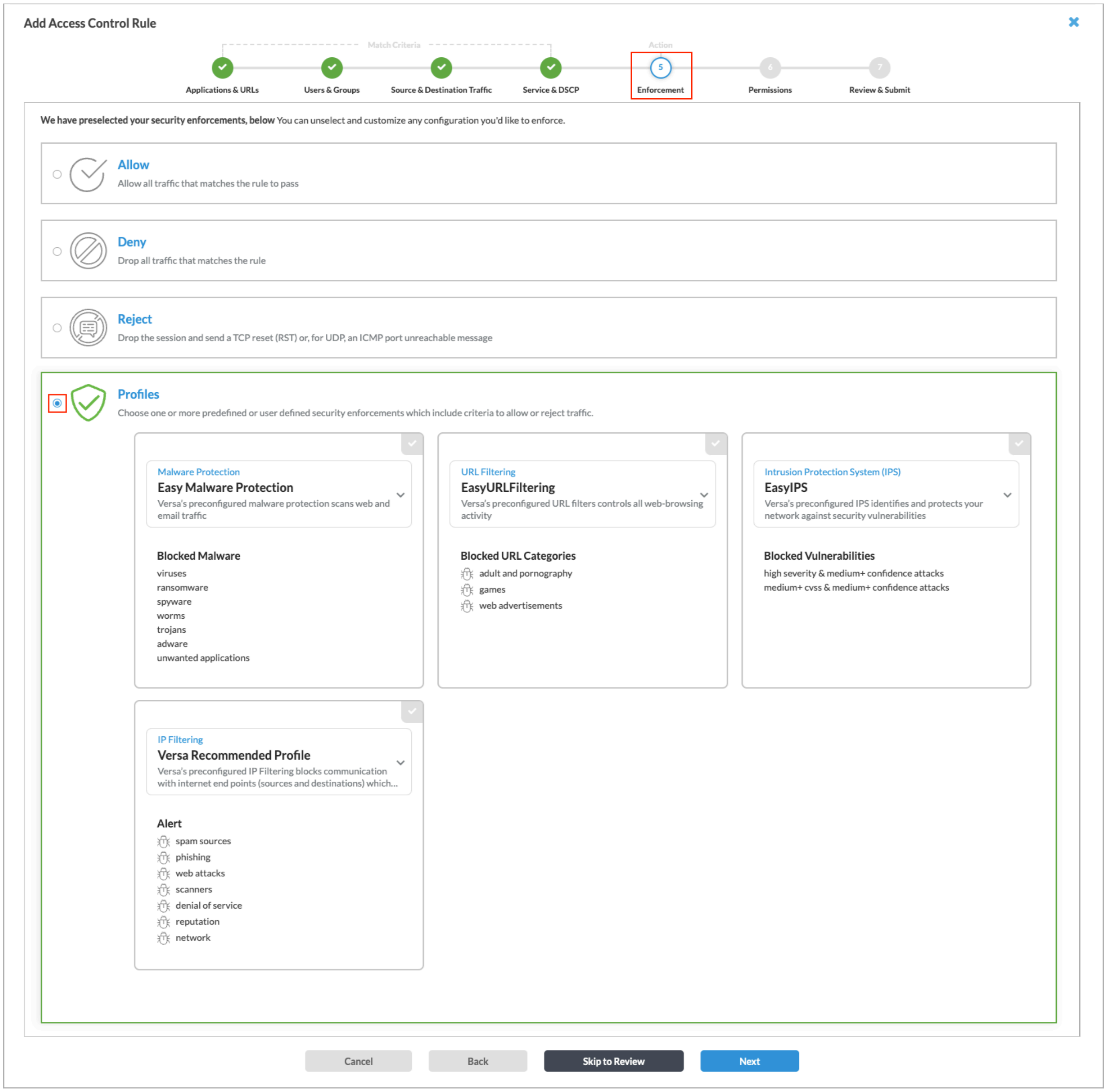
Search or select from list

0
1
2
3
4
5
6
7
8
9
10
11
12
13

33. Select one or more DSCP decimal values, or use the search to locate one or more values.

34. Click Next to go to Step 5, Enforcement. You use the security enforcement rules to define the actions to take on traffic that meets previously defined match conditions and to define the security enforcement actions to apply to

matching traffic. The following screen shows the available security enforcement actions.



We have preselected your security enforcements, below You can unselect and customize any configuration you'd like to enforce.

○ **Allow**
Allow all traffic that matches the rule to pass

○ **Deny**
Drop all traffic that matches the rule

○ **Reject**
Drop the session and send a TCP reset (RST) or, for UDP, an ICMP port unreachable message

● **Profiles**
Choose one or more predefined or user defined security enforcements which include criteria to allow or reject traffic.

Malware Protection
Easy Malware Protection
Versa's preconfigured malware protection scans web and email traffic

Blocked Malware
viruses
ransomware
spyware
worms
trojans
adware
unwanted applications

URL Filtering
EasyURLFiltering
Versa's preconfigured URL filters controls all web-browsing activity

Blocked URL Categories
adult and pornography
games
web advertisements

Intrusion Protection System (IPS)
EasyIPS
Versa's preconfigured IPS identifies and protects your network against security vulnerabilities

Blocked Vulnerabilities
high severity & medium+ confidence attacks
medium+ cvss & medium+ confidence attacks

IP Filtering
Versa Recommended Profile
Versa's preconfigured IP Filtering blocks communication with internet end points (sources and destinations) which...

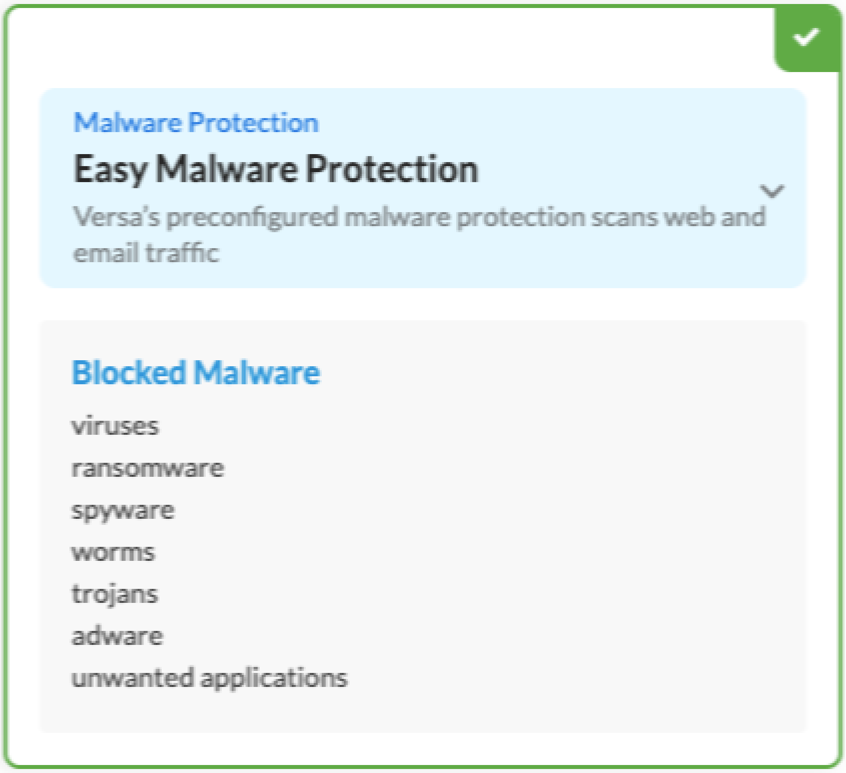
Alert
spam sources
phishing
web attacks
scanners
denial of service
reputation
network

35. You can apply either one security enforcement action or one security enforcement profile for a rule.
    a. To apply a security enforcement action, click one of the following:
        - Allow—Allow all traffic that matches the rule to pass unfiltered.
        - Deny—Drop all traffic that matches the rule.
        - Reject—Drop the session and send a TCP reset (RST) message or a UDP ICMP port unreachable message.
    b. To apply a predefined security enforcement profile to allow or reject traffic, click one of the following:
        - Intrusion protection system (IPS)—Identify malicious activity using signatures, which are rules for

matching suspicious software or patterns in an application's traffic, and by monitoring for unusual events or trends in network traffic.

- IP filtering—Identify network traffic based on the source or destination IP address or fully qualified domain name (such as www.acme.com) and filters or blocks traffic based on its IP address or FQDN and based on the reputation associated with an IP address or FQDN and its geographic location.
- Malware protection—Scan web and email traffic for all types of malicious software (malware), which is a file or code that infects, explores, steals or otherwise damages servers and host devices.
- URL filtering—Prevent access to specific URLs, controlling access to secure (HTTPS) and unsecure (HTTP) websites, thus allowing you to limit web-browsing activity and reduce risks from uncontrolled access to internet websites, including threat propagation, loss of data, and lack of compliance.

c. To change the default settings of a profile, click the down arrow for the profile and select one of the settings listed. For example, the following screen shot of the Malware Protection profile shows that Easy Malware Protection is selected by default. The types of malware that are blocked are listed under Blocked Malware.



Malware Protection

Easy Malware Protection

Versa's preconfigured malware protection scans web and email traffic

Blocked Malware

viruses

ransomware

spyware

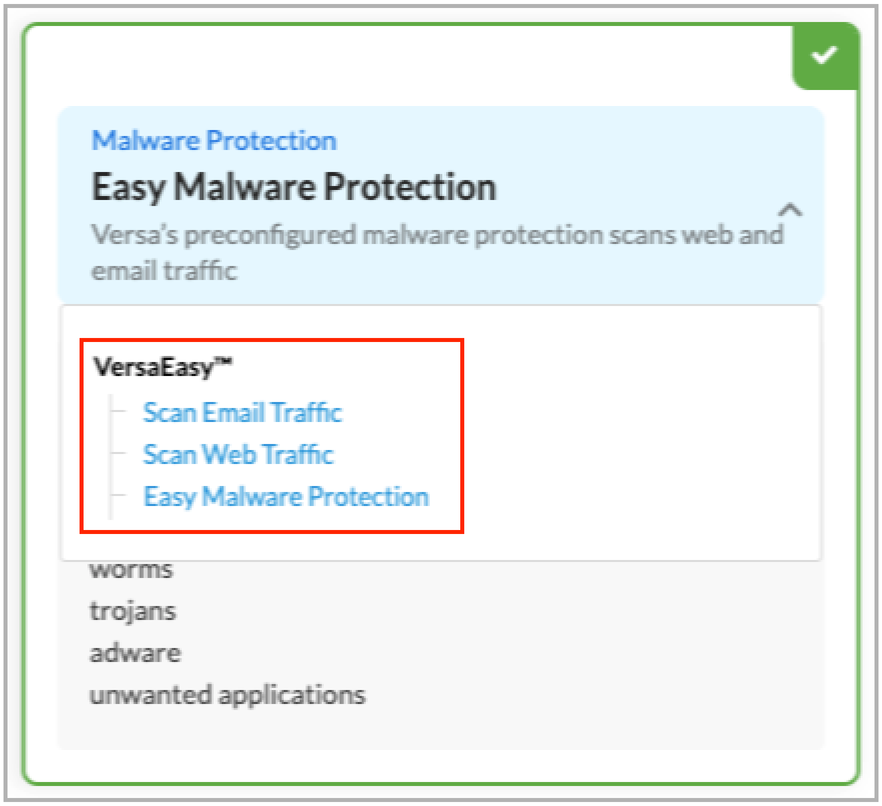
worms

trojans

adware

unwanted applications

- To customize the settings for the Malware Protection profile, click the down arrow, and then choose one of the options: Scan Email Traffic or Scan Web Traffic. (To retain the default settings, select Easy Malware Protection.)



Malware Protection

Easy Malware Protection

Versa's preconfigured malware protection scans web and email traffic

VersaEasy™

- Scan Email Traffic
- Scan Web Traffic
- Easy Malware Protection

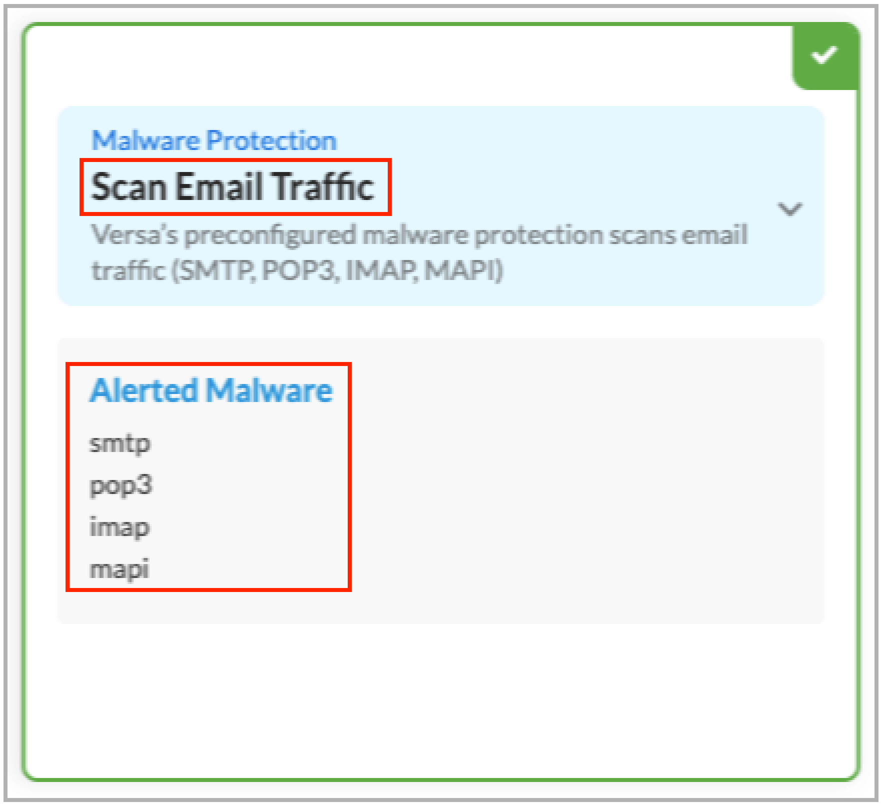
worms

trojans

adware

unwanted applications

- If you select Scan Email Traffic, the following screen displays and the types of malware that trigger alerts are listed under Alerted Malware.



Malware Protection

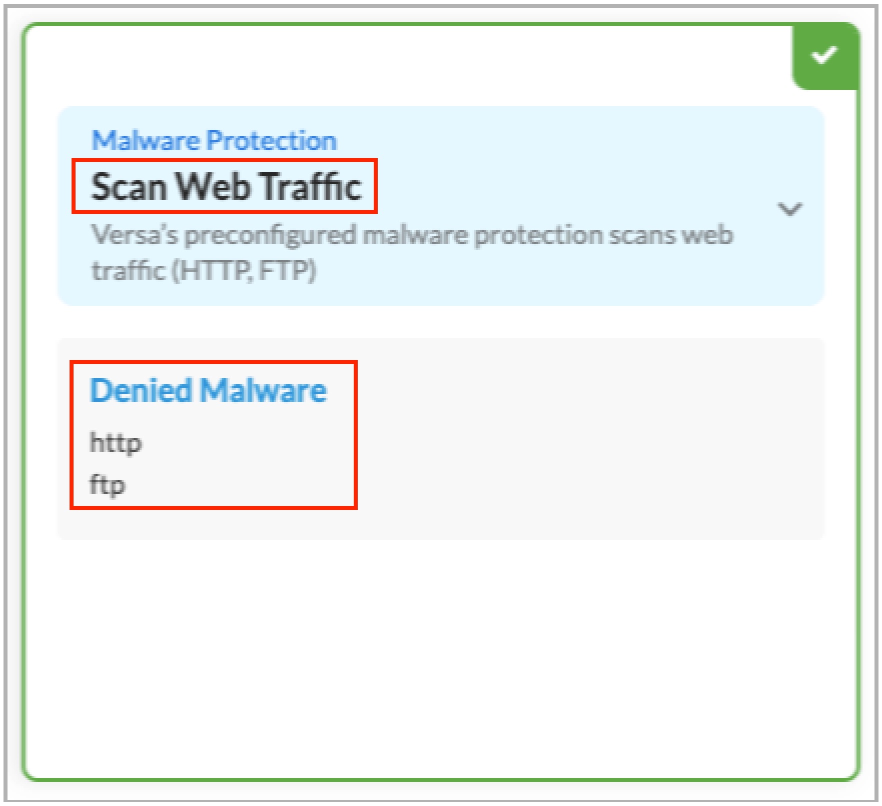
Scan Email Traffic

Versa's preconfigured malware protection scans email traffic (SMTP, POP3, IMAP, MAPI)

Alerted Malware

smtp
pop3
imap
mapi

- If you select Scan Web Traffic, the following screen displays and the types of denied malware affected are listed under Denied Malware.



Malware Protection

Scan Web Traffic

Versa's preconfigured malware protection scans web traffic (HTTP, FTP)

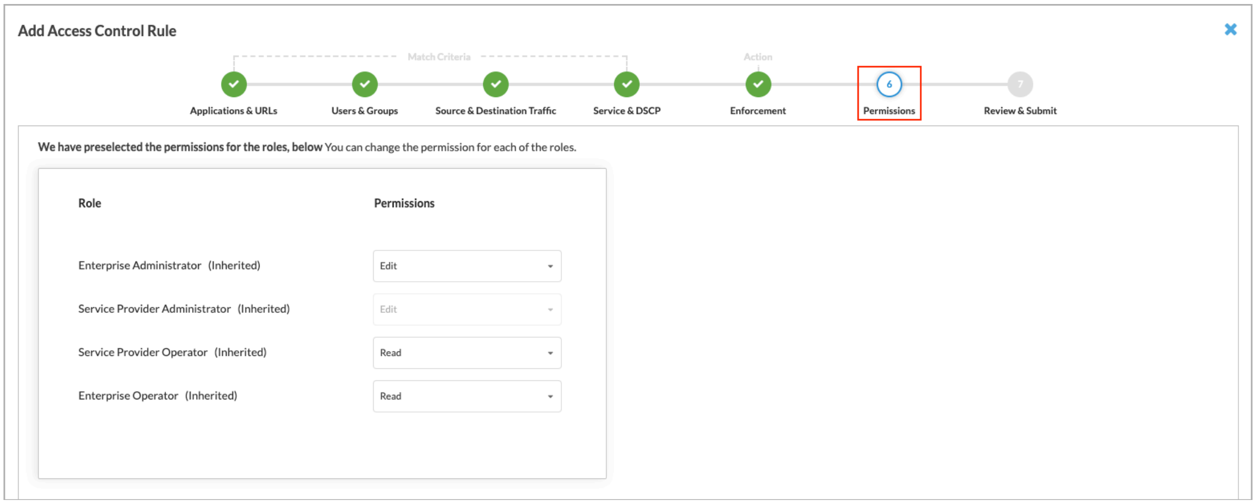
Denied Malware

http

ftp

Select Easy Malware Protection to return to the default settings. For more information about security enforcement profiles, see Configure Security Enforcement Actions for SASE Internet Protection Rules.

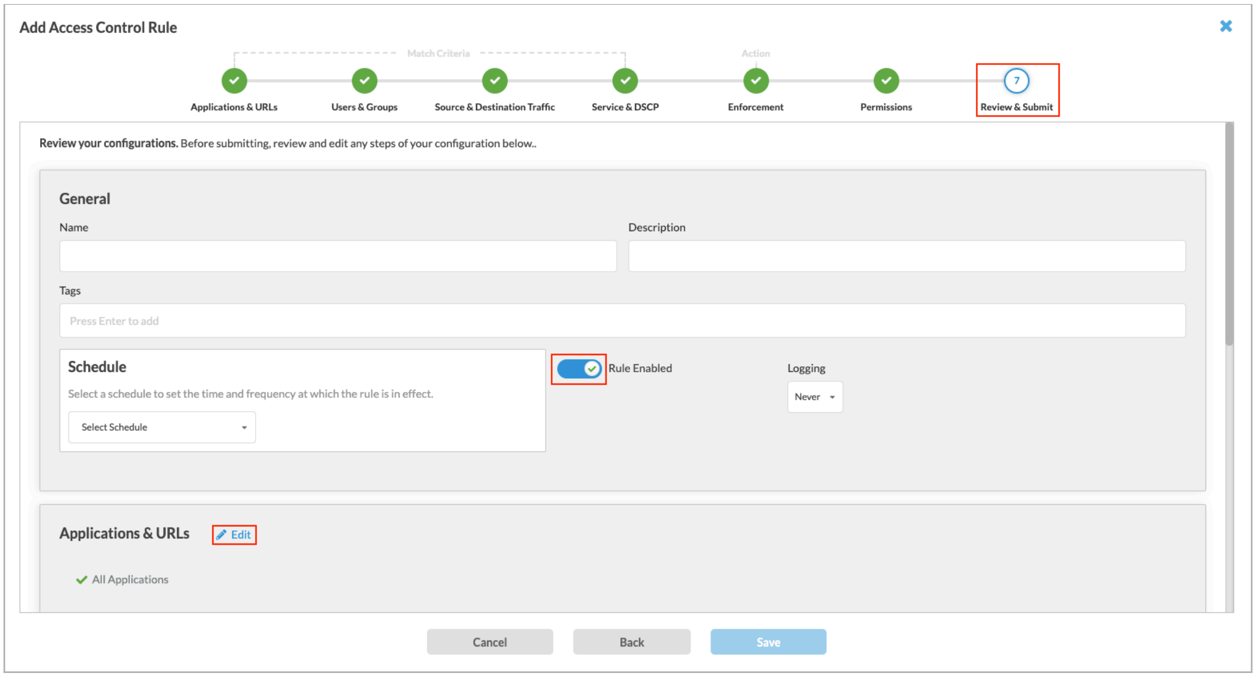
36. Click Next to go to Step 6, Permissions, and revise the permissions, if needed.



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

37. Click Next to go to Step 7, Review and Submit, and then enter the following information.



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

General

Name

Description

Tags

Press Enter to add

Schedule

Select a schedule to set the time and frequency at which the rule is in effect.

Select Schedule

Rule Enabled

Logging

Never

Applications & URLs

✓ All Applications

Field	Description
Name	Enter a name for the rule
Description	Enter a description of the rule.
Tags	Enter one or more tags. A tag is an alphanumeric text descriptor with no spaces or special characters. You can specify multiple tags added for the same object. The tags are used for searching the objects.
Schedule	Select a schedule to set the time and frequency at which the rule is in effect.
Rule Enabled	The rule is enabled by default. Click the slider bar to disable the rule.
Logging	Select an option for sending logs to Versa Analytics: ◦ Never ◦ Start ◦ End ◦ Both

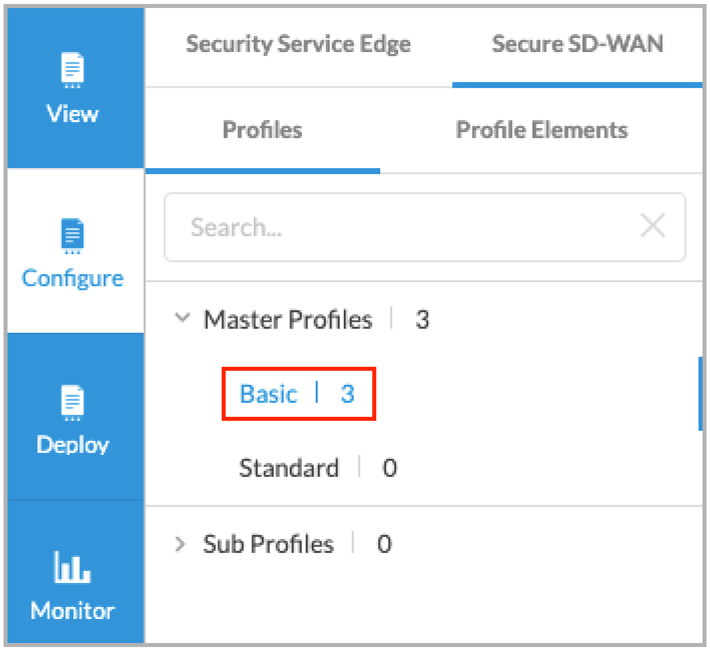
38. Review the selected settings. Click the ✎ Edit icon in a section to change a setting, as needed.
39. Click Save to create the access control rule.

Attach Access Control Policies to a Basic Master Profile

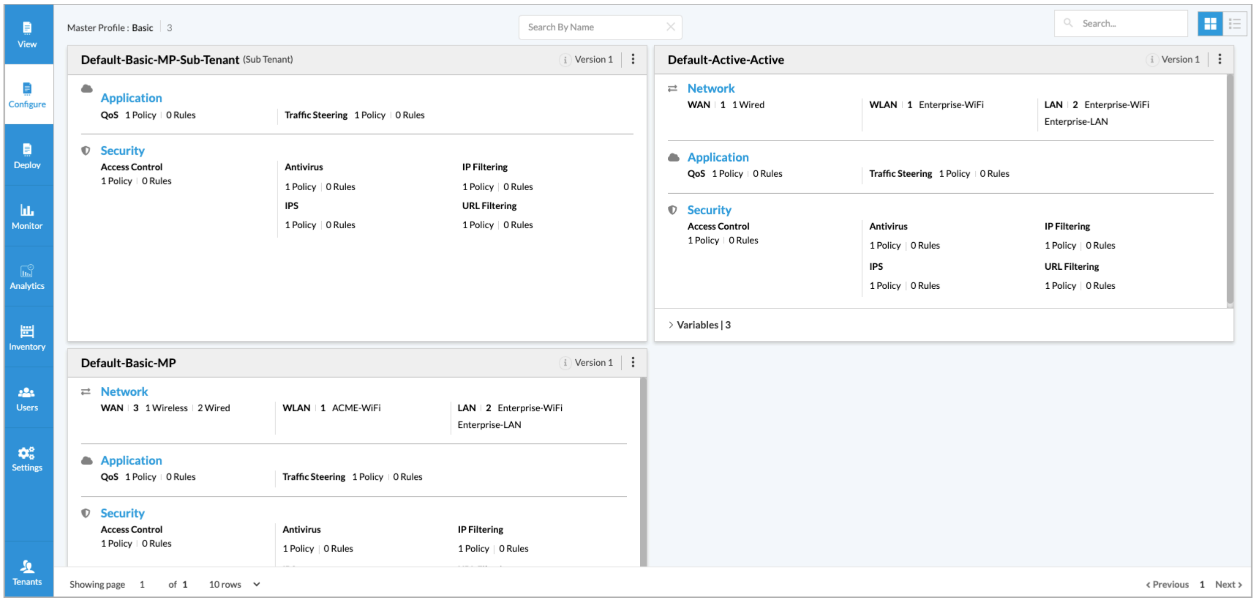
After you create an access control policy, you can attach it to a basic master profile.

To attach access control policies to a basic master profile:

1. Go to Profiles > Master Profiles > Basic.



The screen displays the configured basic master profiles.



Master Profile : Basic | 3

Default-Basic-MP-Sub-Tenant (Sub Tenant) — Version 1

Application
QoS 1 Policy | 0 Rules — Traffic Steering 1 Policy | 0 Rules

Security
Access Control 1 Policy | 0 Rules
Antivirus 1 Policy | 0 Rules
IP Filtering 1 Policy | 0 Rules
IPS 1 Policy | 0 Rules
URL Filtering 1 Policy | 0 Rules

Default-Active-Active — Version 1

Network
WAN | 1 1 Wired — WLAN | 1 Enterprise-WiFi — LAN | 2 Enterprise-WiFi Enterprise-LAN

Application
QoS 1 Policy | 0 Rules — Traffic Steering 1 Policy | 0 Rules

Security
Access Control 1 Policy | 0 Rules
Antivirus 1 Policy | 0 Rules
IP Filtering 1 Policy | 0 Rules
IPS 1 Policy | 0 Rules
URL Filtering 1 Policy | 0 Rules

Variables | 3

Default-Basic-MP — Version 1

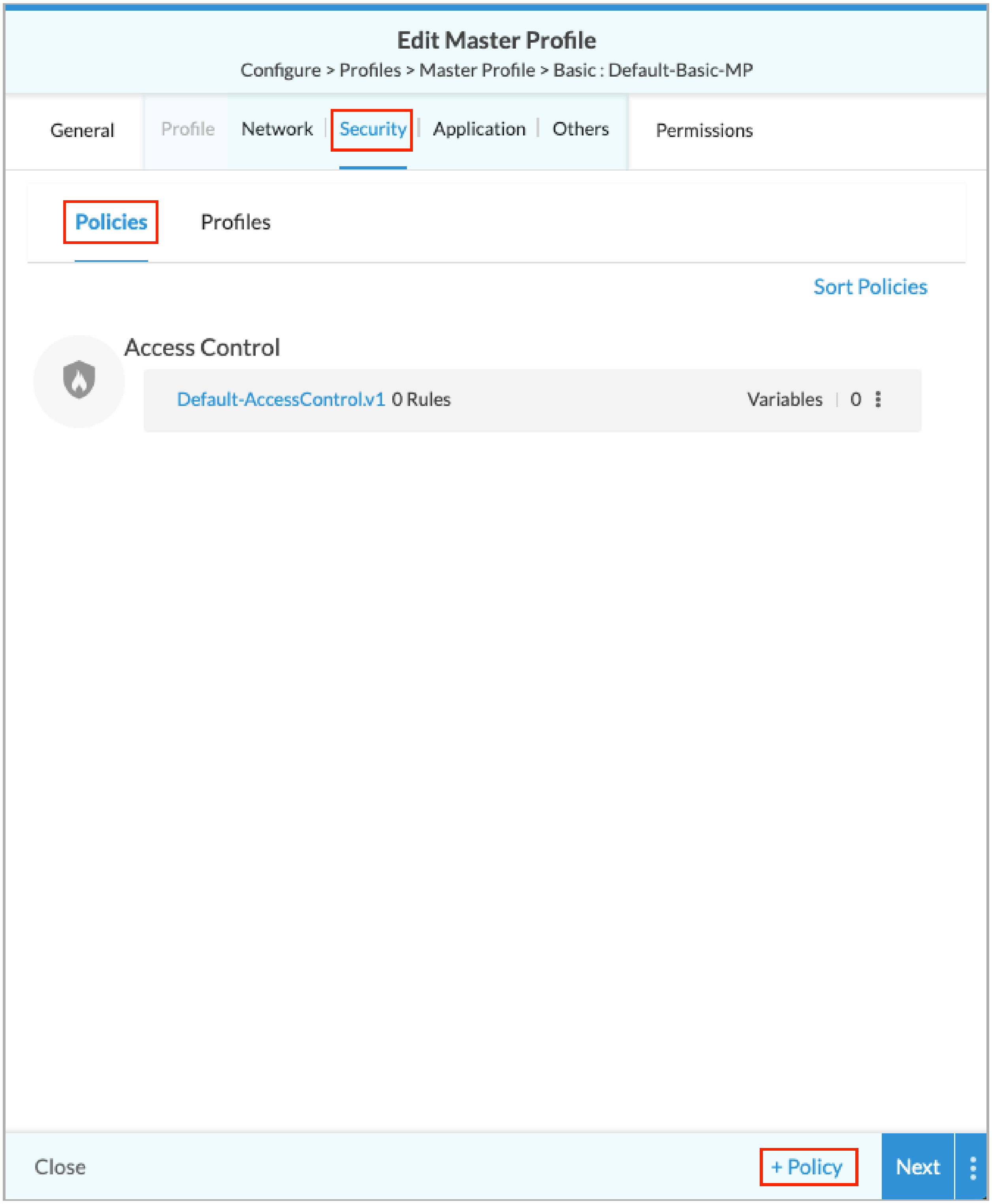
Network
WAN | 3 1 Wireless | 2 Wired — WLAN | 1 ACME-WiFi — LAN | 2 Enterprise-WiFi Enterprise-LAN

Application
QoS 1 Policy | 0 Rules — Traffic Steering 1 Policy | 0 Rules

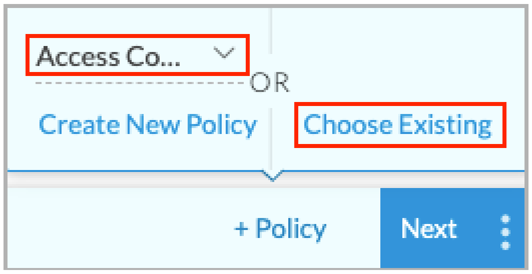
Security
Access Control 1 Policy | 0 Rules
Antivirus 1 Policy | 0 Rules
IP Filtering 1 Policy | 0 Rules

Showing page 1 of 1 10 rows — ‹ Previous 1 Next ›

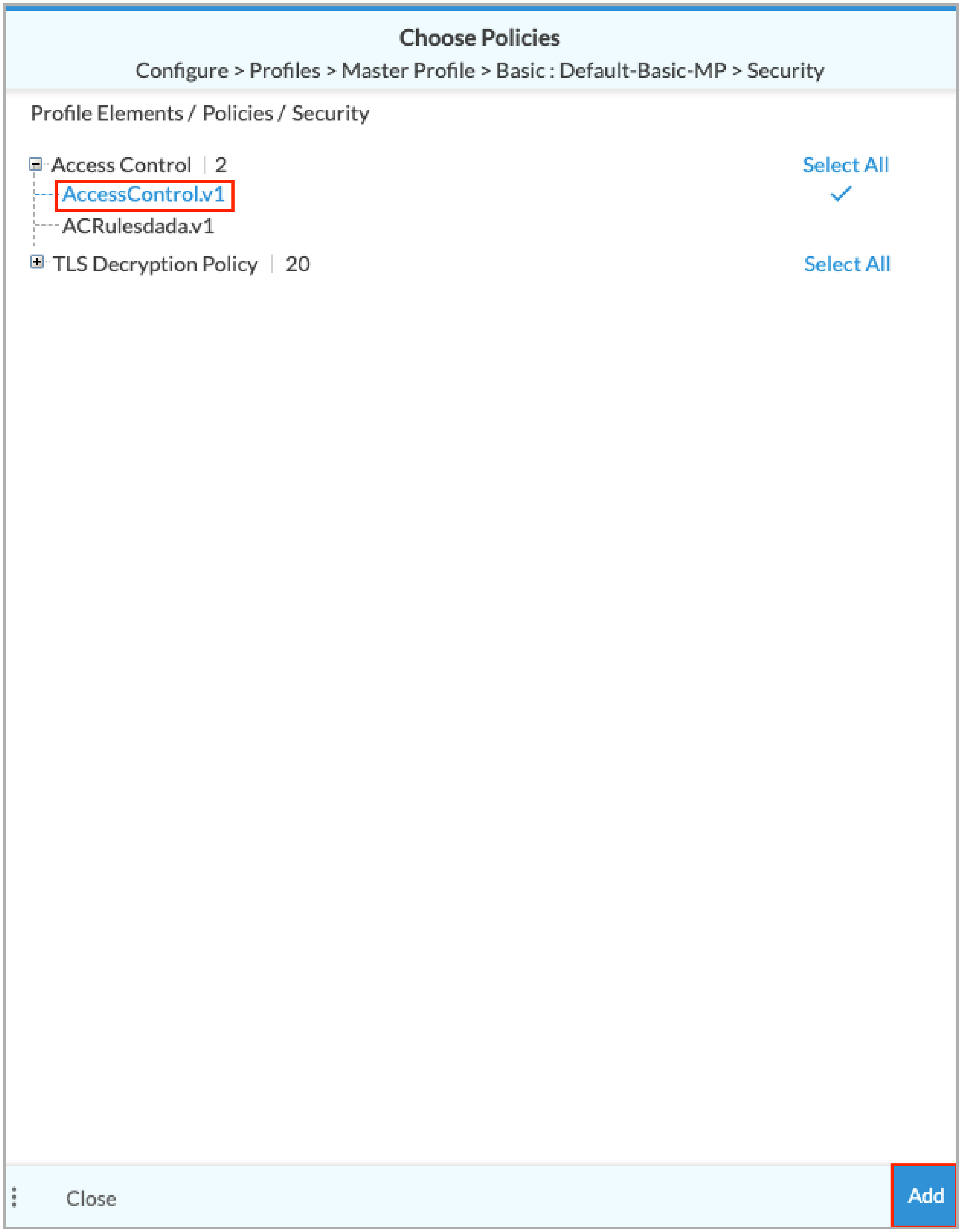
2. Click the master profile to which you want add the access control policy. The Edit Master Profile screen displays.
3. Click Profile > Security in the menu bar. The following screen displays.



4. Select the Policies tab and then click +Policy. The following popup window displays.



5. Click the down arrow, select Access Control, and then select Choose Existing. The Choose Policies screen displays.



Choose Policies

Configure > Profiles > Master Profile > Basic : Default-Basic-MP > Security

Profile Elements / Policies / Security

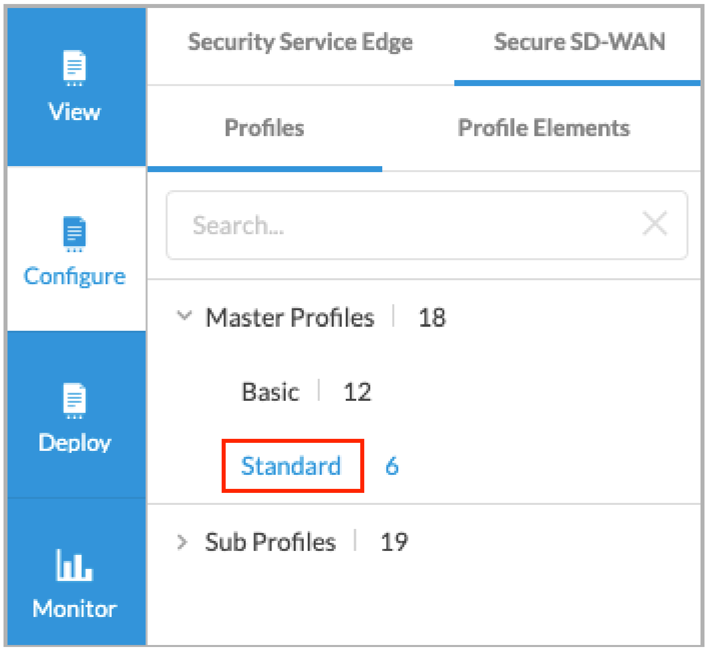
6. Select the access control policy from the list (AccessControl.v1 in the screenshot above), and then click Add.

Attach Access Control Policies to a Standard Master Profile

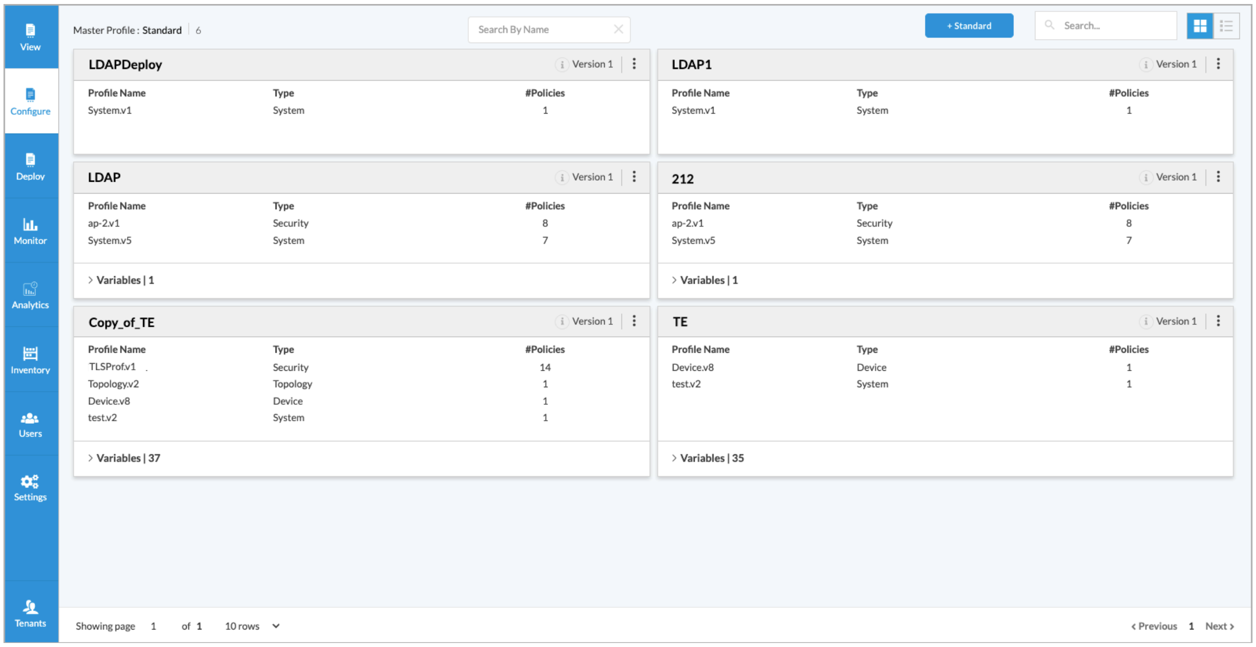
After you create an access control policy, you can attach it to a standard master profile.

To attach access control policies to a standard master profile:

1. Go to Profiles > Master Profiles > Standard.



The screen displays the configured standard master profiles. Note that you can have only one instance of each profile type for each standard master profile. If a standard master profile already has a security profile attached to it, you cannot add another security profile. You can, however, create a new standard master profile and attach an access control policy to it.



Master Profile : Standard | 6

LDAPDeploy Version 1

Profile Name	Type	#Policies
System.v1	System	1

LDAP1 Version 1

Profile Name	Type	#Policies
System.v1	System	1

LDAP Version 1

Profile Name	Type	#Policies
ap-2.v1	Security	8
System.v5	System	7

> Variables | 1

212 Version 1

Profile Name	Type	#Policies
ap-2.v1	Security	8
System.v5	System	7

> Variables | 1

Copy_of_TE Version 1

Profile Name	Type	#Policies
TLSProf.v1	Security	14
Topology.v2	Topology	1
Device.v8	Device	1
test.v2	System	1

> Variables | 37

TE Version 1

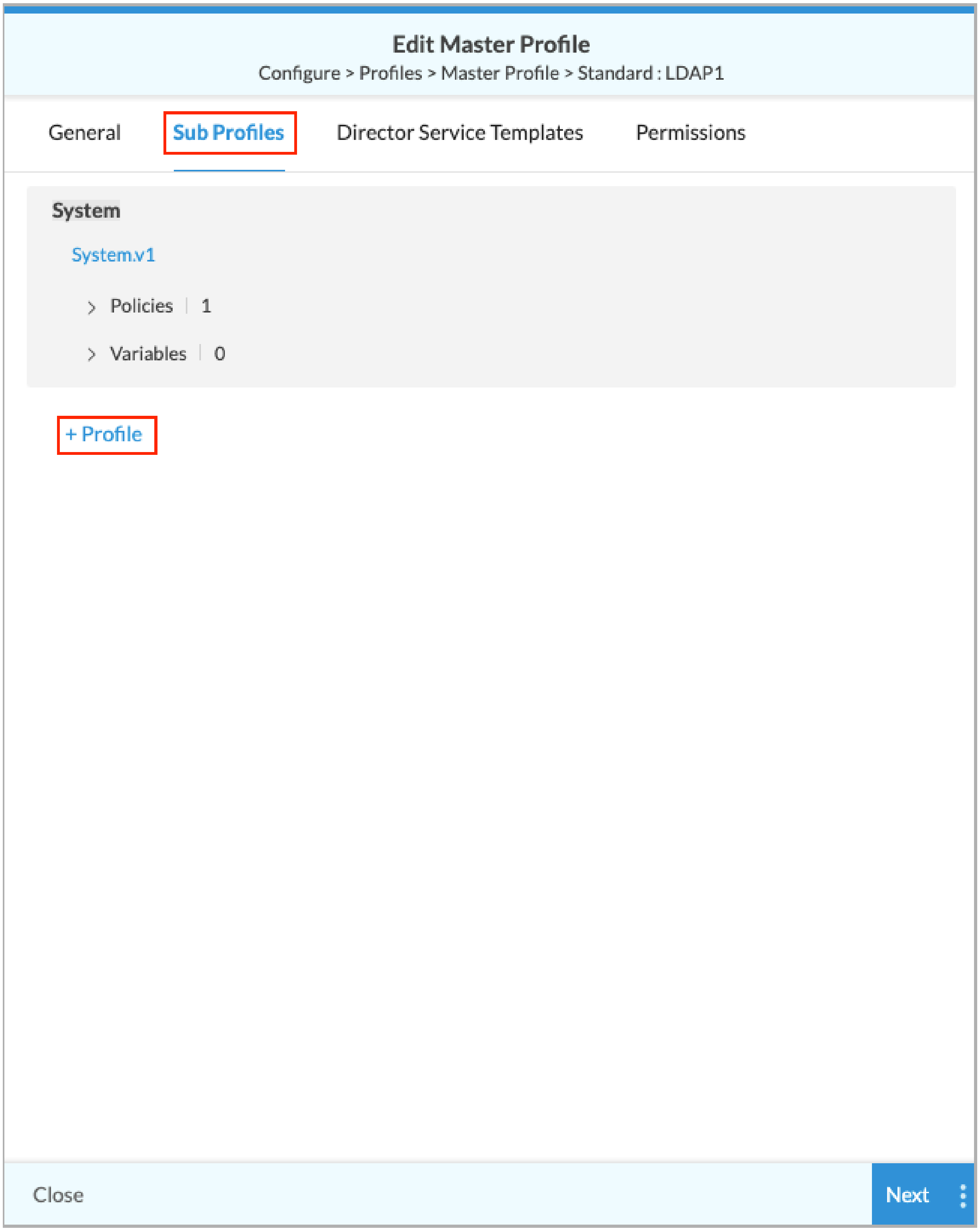
Profile Name	Type	#Policies
Device.v8	Device	1
test.v2	System	1

> Variables | 35

Showing page 1 of 1 10 rows

‹ Previous 1 Next ›

2. Click the standard master profile to which you will add the security access control policy. The Edit Master Profile screen displays.
3. Click Sub Profiles in the menu bar. The following screen displays.



Edit Master Profile

Configure > Profiles > Master Profile > Standard : LDAP1

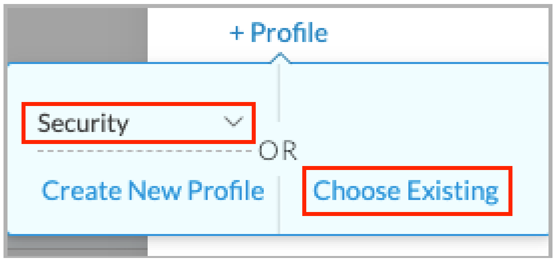
System

System.v1

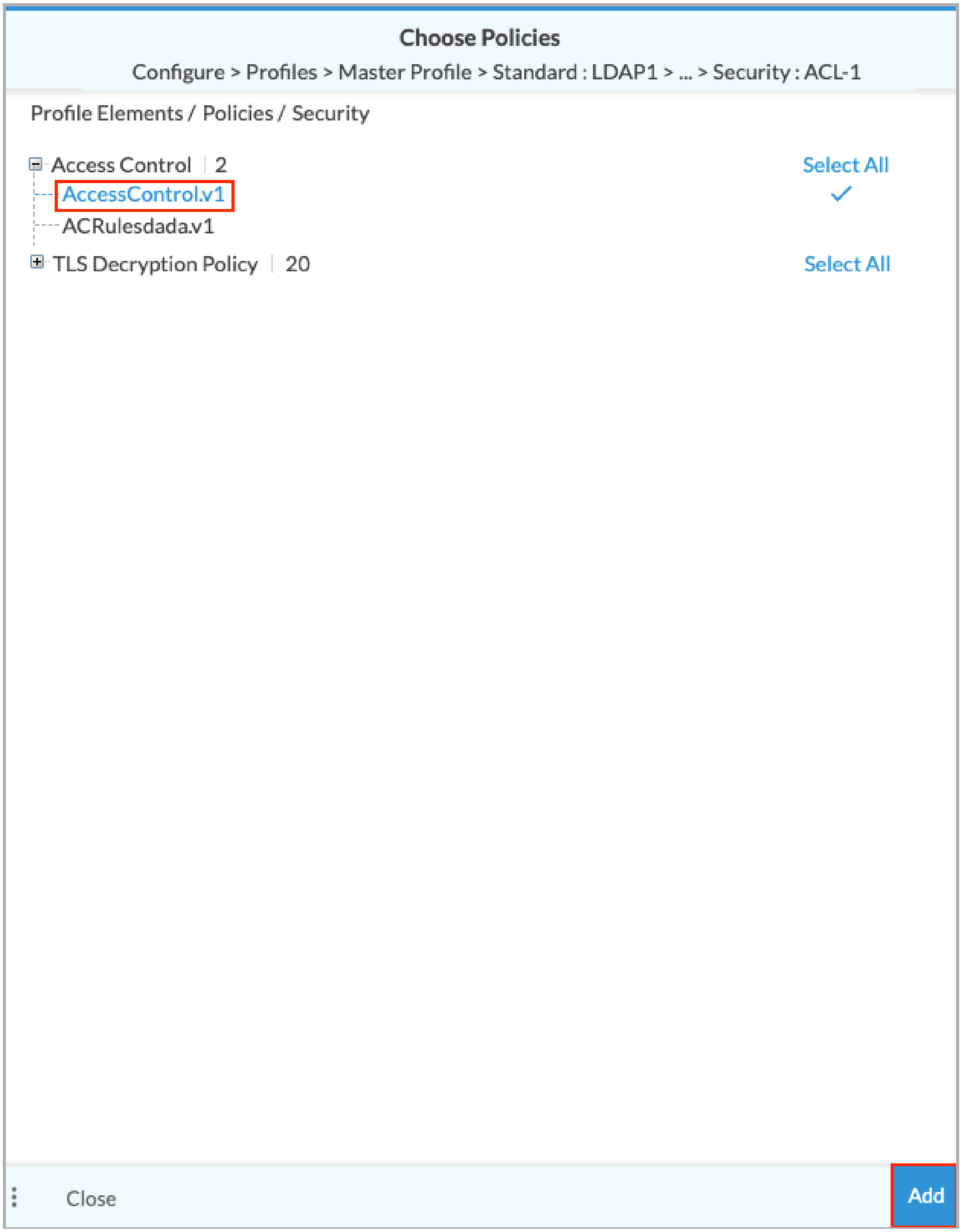
> Policies | 1

> Variables | 0

4. Click +Profile. The following popup window displays.



5. Click the down arrow, select Security, and then click Choose Existing. The Choose Policies screen displays.



Choose Policies

Configure > Profiles > Master Profile > Standard : LDAP1 > ... > Security : ACL-1

Profile Elements / Policies / Security

- Access Control | 2 — Select All
  - AccessControl.v1 ✓
  - ACRulesdada.v1
- TLS Decryption Policy | 20 — Select All

6. Select the access control policy from the list (AccessControl.v1 in the screenshot above), and then click Add.

Supported Software Information

Releases 11.4.1 and later support all content described in this article, except:

- Releases 12.1.1 and later add support for the Negate Source Address and Negate Destination Address options when configuring an access control rule.

Additional Information

Configure Automatic Deletion of SD-WAN Object Versions
Configure Security Enforcement Actions for SASE Internet Protection Rules
Propagate Object Configuration Changes
View References to Objects in the Configuration Hierarchies.