Configure SASE User-Defined Objects

For supported software information, click here.

Objects are configuration elements that you use to build larger configurations, such policy rules and profiles. Versa provides many predefined SASE objects that you can use as they are. You can also define your own objects with which to build policies. You can configure following types of user-defined SASE objects:

- Applications and application groups, which include the following:
    - Internet applications
    - Private applications
    - Client native applications
    - Private application groups
    - Internet application groups

      Note: You can use internet applications and internet application groups only for internet protection rules, and you can use private applications and private application groups only for private protection rules.

- IP address groups
- Schedules
- Security actions
- Services
- URL categories

Note: You must configure the following SASE rules, profiles, and settings in a specific order:

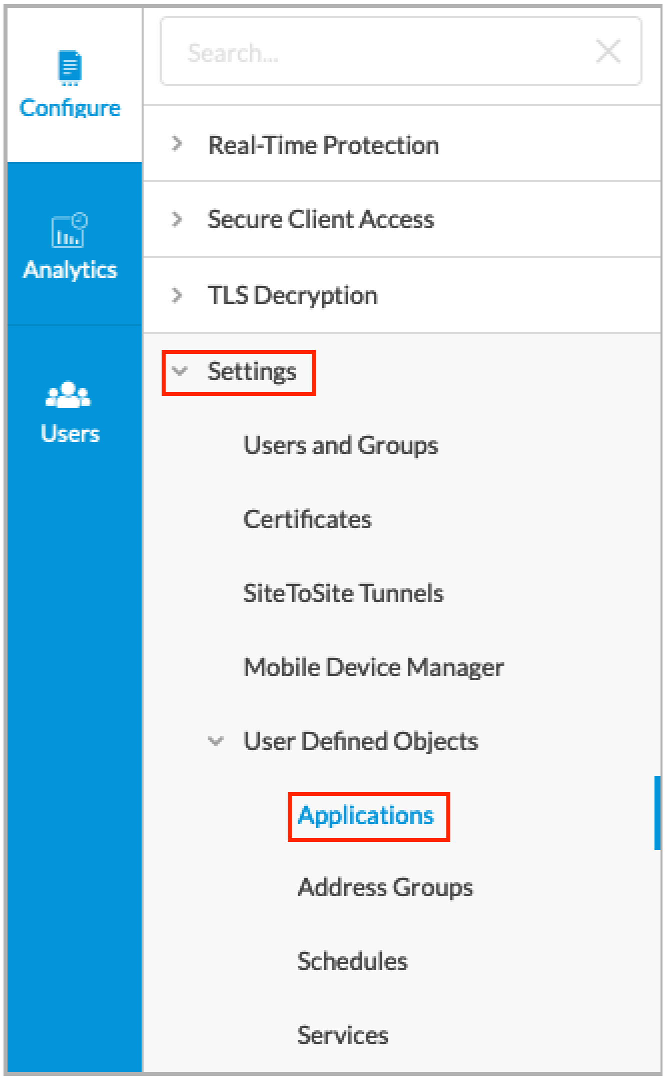
1. Configure site-to-site tunnels. For more information, see Configure SASE Site-to-Site Tunnels.
2. Configure secure client access profiles and rules. For more information, see Configure SASE Secure Client Access Rules.

You do not need to configure the remaining SASE rules, profiles, and settings in any particular order.

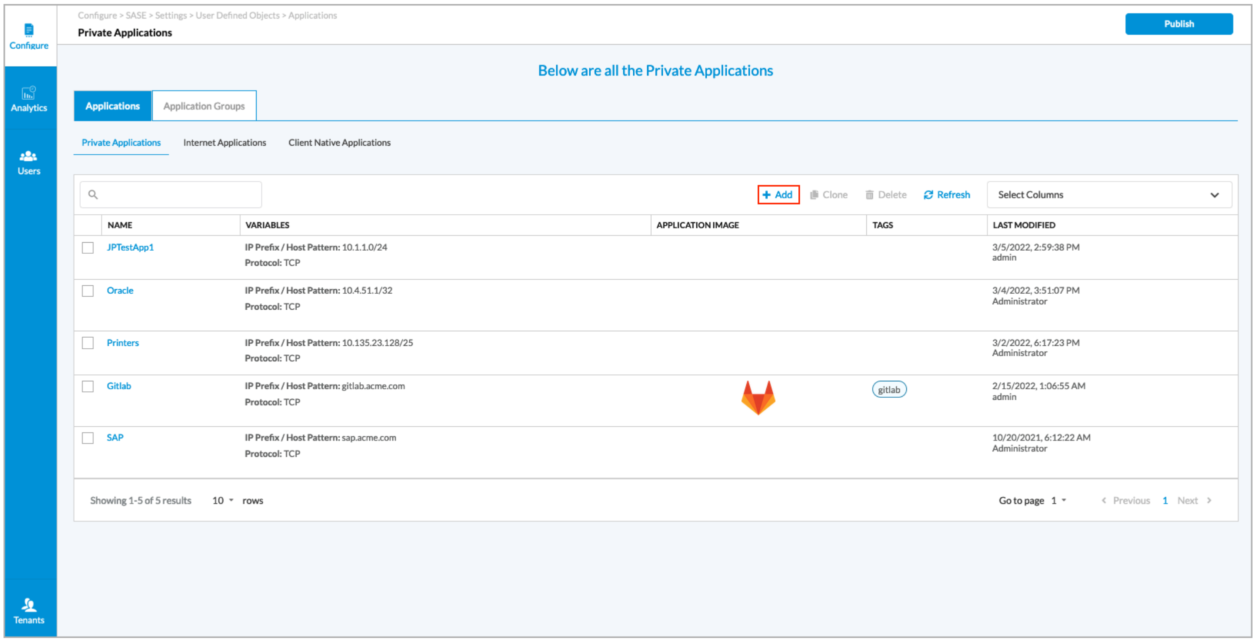
Configure User-Defined Applications and Application Groups

To configure user-defined applications and application groups:

1. Go to Configure > Settings > User Defined Objects > Applications.

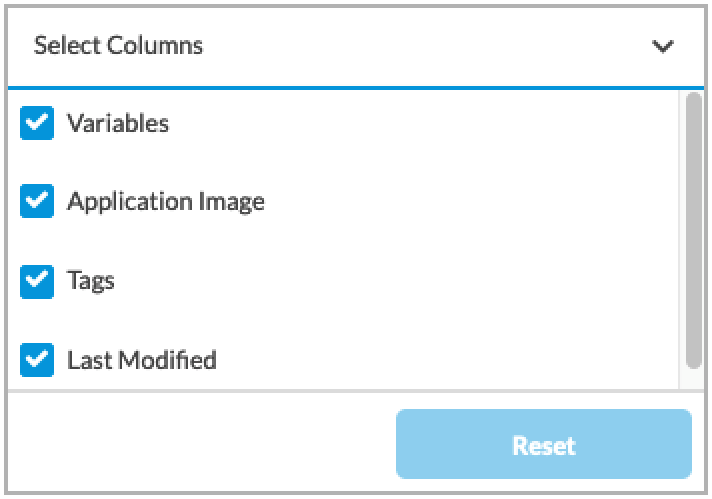


By default, the Private Applications screen displays.



	NAME	VARIABLES	APPLICATION IMAGE	TAGS	LAST MODIFIED
□	JPTestApp1	**IP Prefix / Host Pattern:** 10.1.1.0/24 **Protocol:** TCP			3/5/2022, 2:59:38 PM admin
□	Oracle	**IP Prefix / Host Pattern:** 10.4.51.1/32 **Protocol:** TCP			3/4/2022, 3:51:07 PM Administrator
□	Printers	**IP Prefix / Host Pattern:** 10.135.23.128/25 **Protocol:** TCP			3/2/2022, 6:17:23 PM Administrator
□	Gitlab	**IP Prefix / Host Pattern:** gitlab.acme.com **Protocol:** TCP		gitlab	2/15/2022, 1:06:55 AM admin
□	SAP	**IP Prefix / Host Pattern:** sap.acme.com **Protocol:** TCP			10/20/2021, 6:12:22 AM Administrator

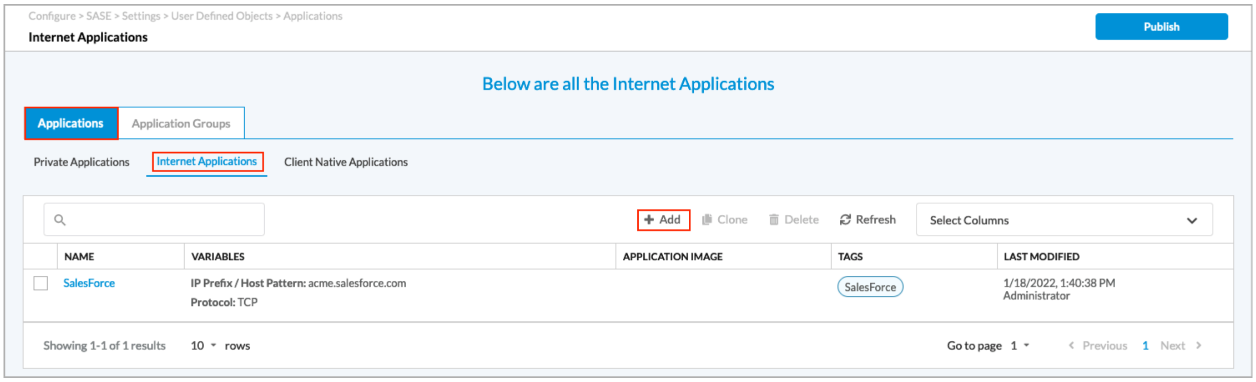
2. To customize which columns display, click Select Columns, and then click the columns select or deselect the columns you want to display. Click Reset to return to the default columns settings.



Configure Internet Applications

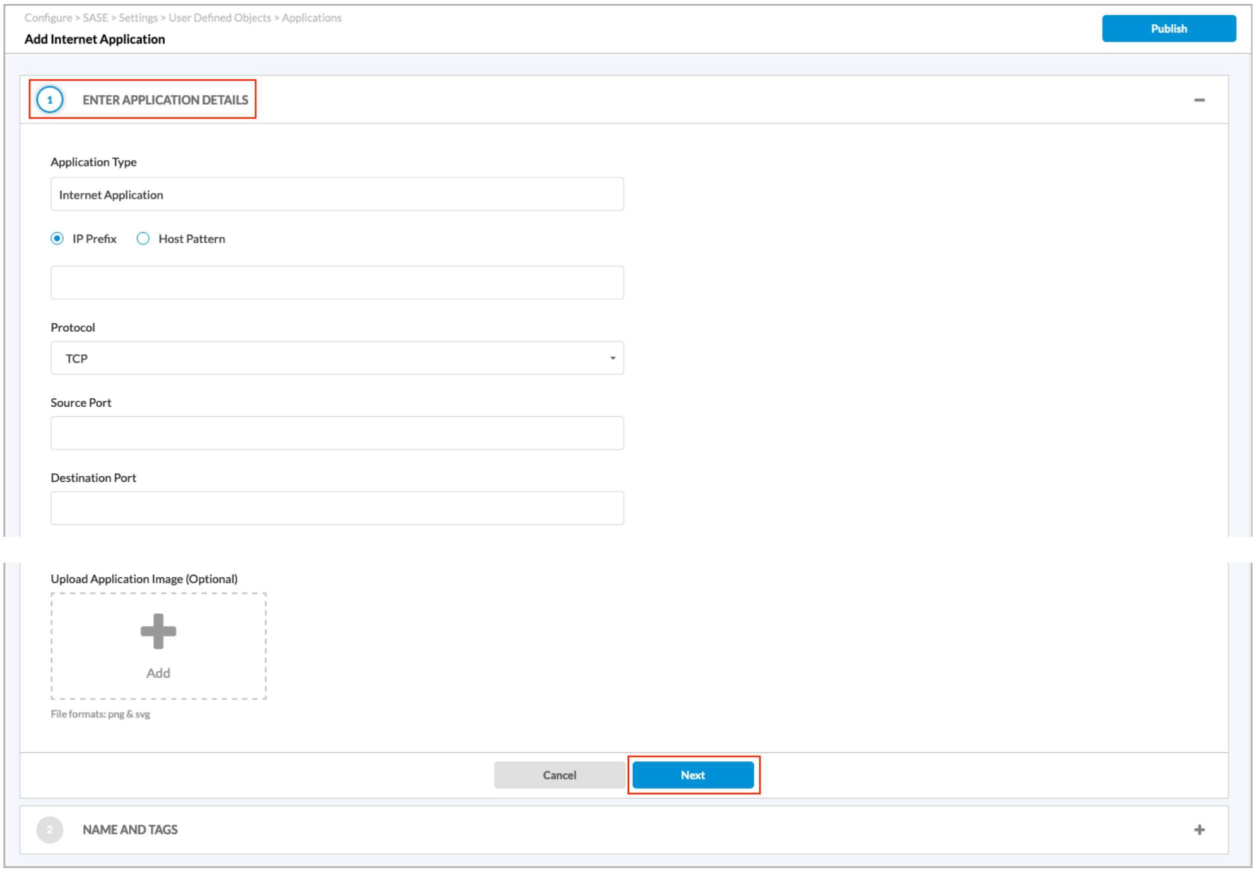
To configure internet applications:

1. In the Private Applications default landing screen, select the Applications tab, the select the Internet Applications tab. The screen displays any internet applications that you have already defined.



NAME	VARIABLES	APPLICATION IMAGE	TAGS	LAST MODIFIED
SalesForce	IP Prefix / Host Pattern: acme.salesforce.com Protocol: TCP		SalesForce	1/18/2022, 1:40:38 PM Administrator

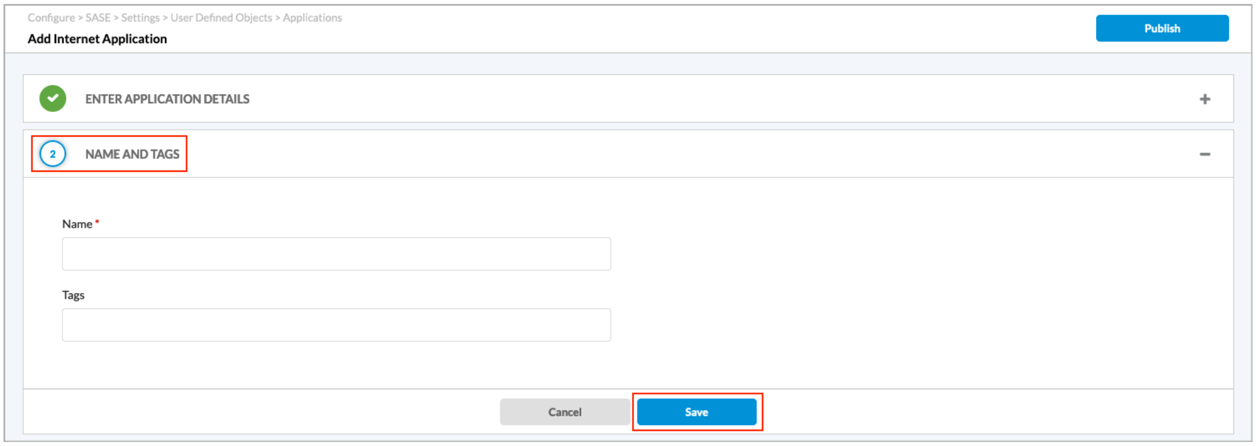
2. Click + Add to add a new internet application. In the Add Internet Application screen, under Enter Application Details, enter information for the following fields.



Field	Description
IP Prefix	Select, and then enter a valid IP prefix and subnet. Note that if you select IP Prefix, you cannot also select Host Pattern.
Host Pattern	Select, and then enter a host pattern to detect. Note

Field	Description
	that if you select Host Pattern, you cannot also select IP Prefix.
Protocol	Select a protocol. If you select Host Pattern, TCP is the only protocol available.
Source Port	If you select the TCP or UDP protocol, enter the source port number. You can enter a single port value or a range of values; for example, 500 or 1-100. *Range*: 0 through 65535 *Default*: None
Destination Port	If you select the TCP or UDP protocol, enter the destination port number. You can enter a single port value or a range of values; for example, 500 or 1-100. *Range*: 0 through 65535 *Default*: None
Upload Application Image	Click the + Add icon, and then select an application image and upload it. Images must be in png or svg format.

3. Click Next.


Configure > SASE > Settings > User Defined Objects > Applications
Add Internet Application
Publish
ENTER APPLICATION DETAILS
2
NAME AND TAGS
Name *
Tags
Cancel
Save

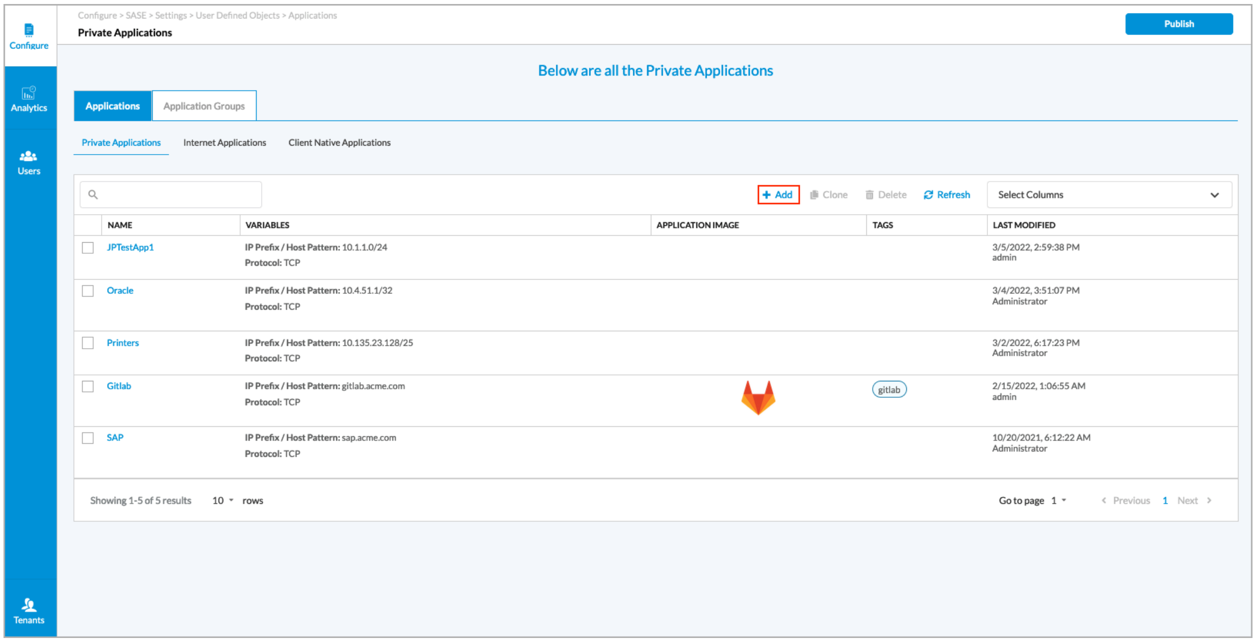
4. In the Enter Name and Tags section, enter a name for the internet application and, optionally, one or more tags to include. A tag is an alphanumeric text descriptor with no spaces or special characters that you use for searching objects.

5. Click Save.

Configure Private Applications

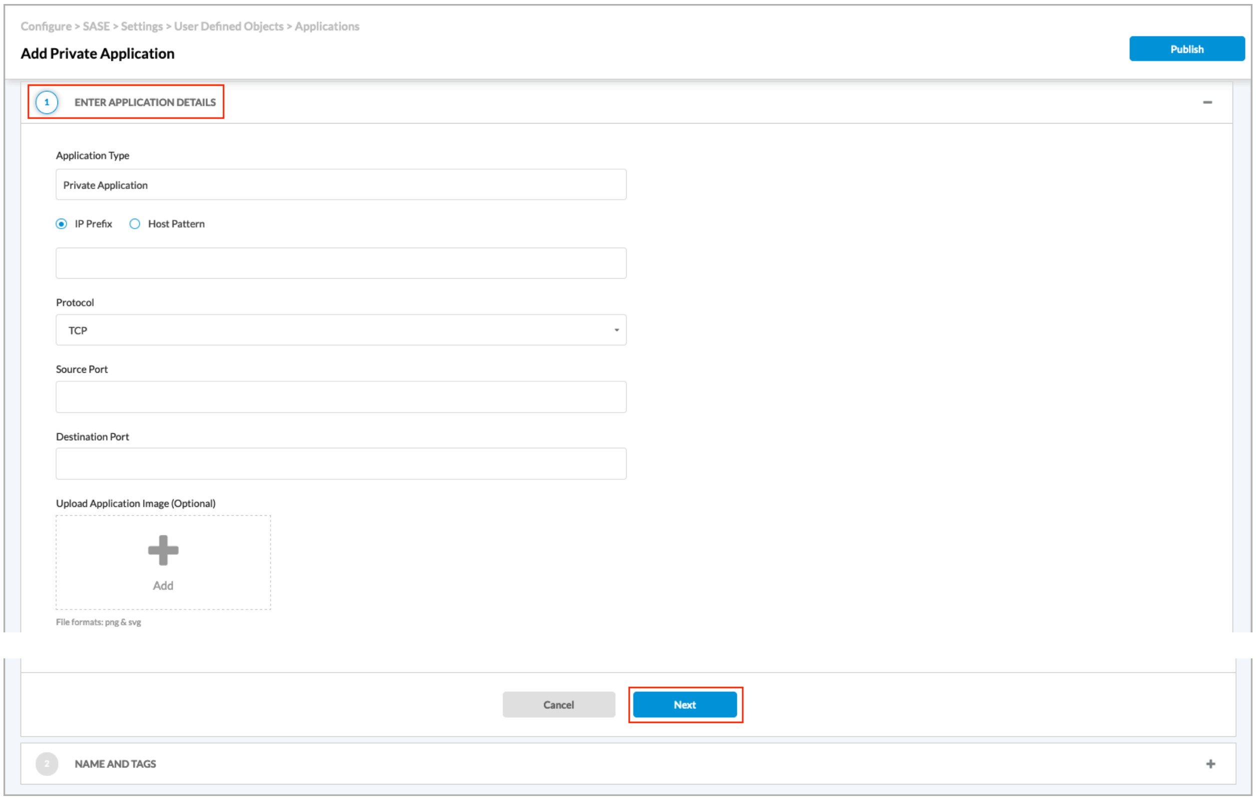
To configure private applications:

1. From the Private Applications default landing screen, select the Applications tab, and then select the Private Applications tab.



	NAME	VARIABLES	APPLICATION IMAGE	TAGS	LAST MODIFIED
□	JPTestApp1	**IP Prefix / Host Pattern:** 10.1.1.0/24 **Protocol:** TCP			3/5/2022, 2:59:38 PM admin
□	Oracle	**IP Prefix / Host Pattern:** 10.4.51.1/32 **Protocol:** TCP			3/4/2022, 3:51:07 PM Administrator
□	Printers	**IP Prefix / Host Pattern:** 10.135.23.128/25 **Protocol:** TCP			3/2/2022, 6:17:23 PM Administrator
□	Gitlab	**IP Prefix / Host Pattern:** gitlab.acme.com **Protocol:** TCP		gitlab	2/15/2022, 1:06:55 AM admin
□	SAP	**IP Prefix / Host Pattern:** sap.acme.com **Protocol:** TCP			10/20/2021, 6:12:22 AM Administrator

2. Click + Add to add a new private application. In the Add Private Application screen, under Enter Application Details, enter information for the following fields.


Configure > SASE > Settings > User Defined Objects > Applications
Publish
1 ENTER APPLICATION DETAILS
Add
Cancel
Next
2 NAME AND TAGS

Add Private Application

Application Type: Private Application

● IP Prefix ○ Host Pattern

Protocol: TCP

Source Port

Destination Port

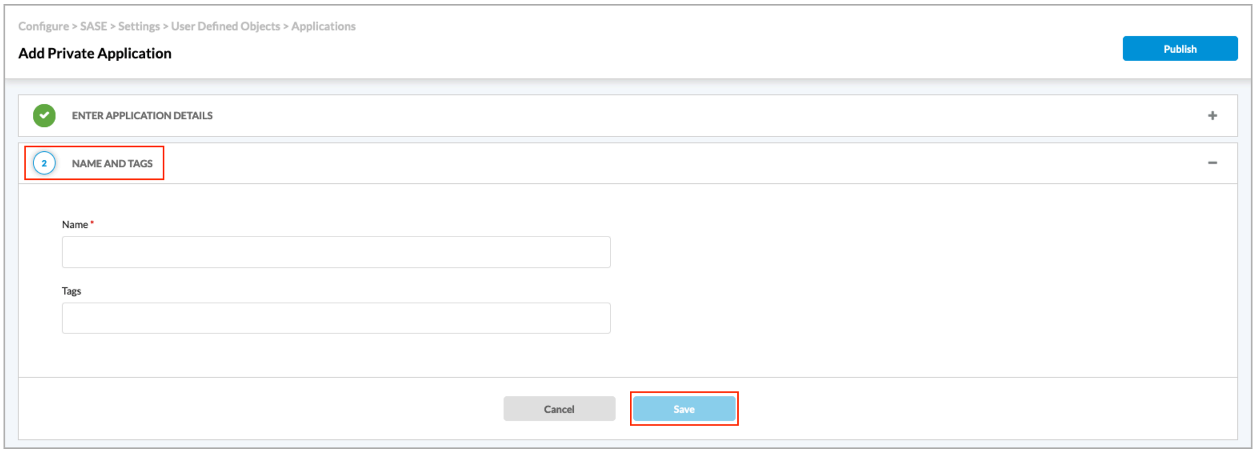
Upload Application Image (Optional)

File formats: png & svg

Field	Description
IP Prefix	Select, and then enter a valid IP prefix and subnet. Note that if you select IP Prefix, you cannot also select Host Pattern.
Host Pattern	Select, and then enter a host pattern to detect. Note that if you select Host Pattern, you cannot also select IP Prefix.
Protocol	Select a protocol. If you selected Host Pattern, TCP is the only protocol that you can choose.
Source Port	If you select the TCP or UDP protocol, enter the source port number. You can enter a single port value or a range of values; for example, 500 or 1-100. *Range*: 0 through 65535 *Default*: None
Destination Port	If you select the TCP or UDP protocol, enter the

Field	Description
	destination port number. You can enter a single port value or a range of values; for example, 500 or 1-100. *Range*: 0 through 65535 *Default*: None
Upload Application Image	Click the + Add icon, then select an application image and upload it. Images can be in png or svg format.

3. Click Next.
4. In the Enter Name and Tags section, enter a name for the private application and, optionally, one or more tags to include. A tag is an alphanumeric text descriptor with no spaces or special characters that you use for searching objects.

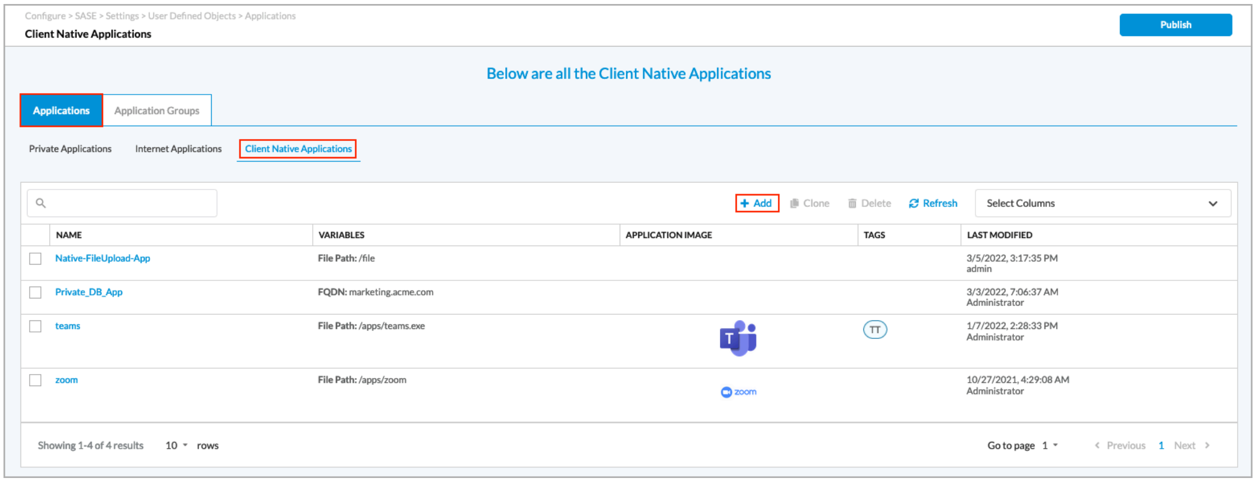

Configure > SASE > Settings > User Defined Objects > Applications
Add Private Application
Publish
ENTER APPLICATION DETAILS
+
2
NAME AND TAGS
−
Name *
Tags
Cancel
Save

5. Click Save.

Configure Client-Native Applications

To configure client-native applications:

1. From the Private Applications default landing screen, select the Applications tab, and then select the Client-Native Applications tab. The screen displays any client-native applications that you have previously defined. Note that you use client-native applications when you configure secure client access rules, but you cannot use client-native applications when you configure internet protection rules or private application rules.



Configure > SASE > Settings > User Defined Objects > Applications

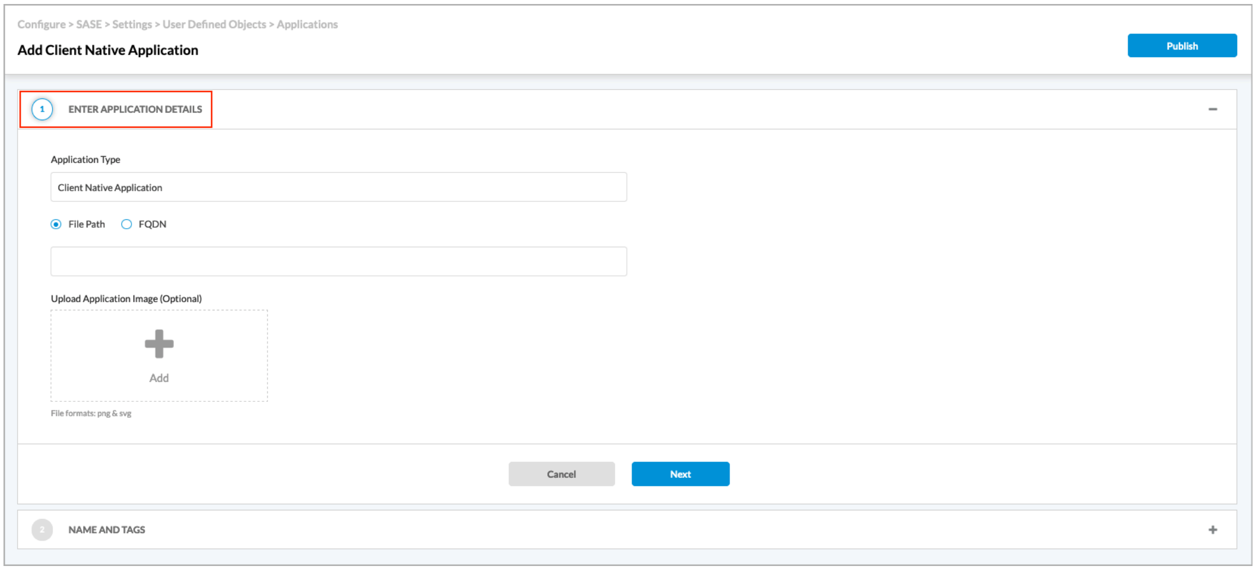
Client Native Applications

Below are all the Client Native Applications

NAME	VARIABLES	APPLICATION IMAGE	TAGS	LAST MODIFIED
Native-FileUpload-App	File Path: /file			3/5/2022, 3:17:35 PM admin
Private_DB_App	FQDN: marketing.acme.com			3/3/2022, 7:06:37 AM Administrator
teams	File Path: /apps/teams.exe		TT	1/7/2022, 2:28:33 PM Administrator
zoom	File Path: /apps/zoom			10/27/2021, 4:29:08 AM Administrator

Showing 1-4 of 4 results 10 rows

2. Click + Add to add a new client application. In the Add Client Native Application screen, under Enter Application Details, enter information for the following fields.



Configure > SASE > Settings > User Defined Objects > Applications

Add Client Native Application

1 ENTER APPLICATION DETAILS

Application Type: Client Native Application

● File Path ○ FQDN

Upload Application Image (Optional)

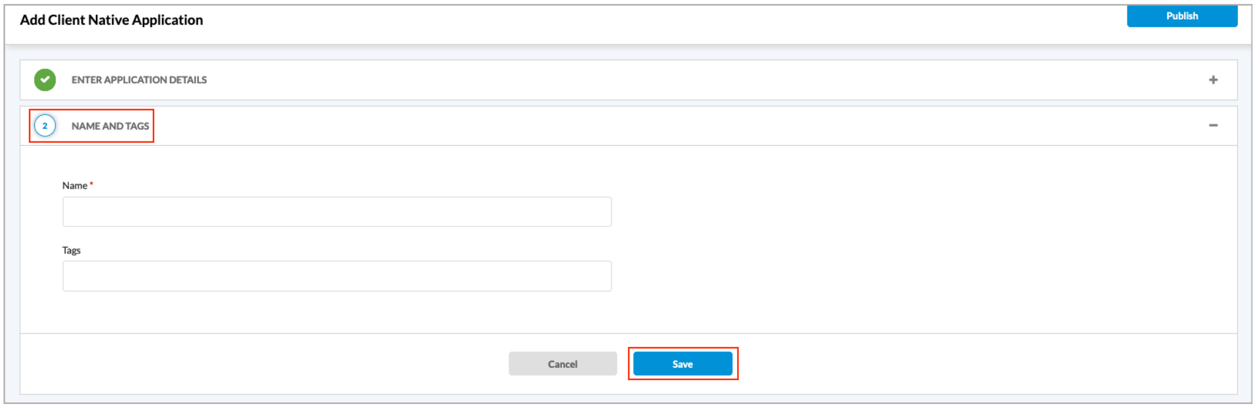
File formats: png & svg

2 NAME AND TAGS

Field	Description
File Path	Enter the path to the new client application on your local computer or laptop. For example, the path to the Outlook application on your local computer or laptop might be /var/lob/apps/outlook.app. Note that if you specify the file path, you cannot also specify the FQDN.
FQDN	Enter the fully qualified domain name (FQDN). Click

Field	Description
	the ⊕ Add icon to enter additional FQDNs. Note that if you specify the FQDN, you cannot also specify the file path.
Upload Application Image	Click the Add icon, and then select an application image and upload it. Images can be in png or svg format.

3. Click Next. The Name and Tags section displays.

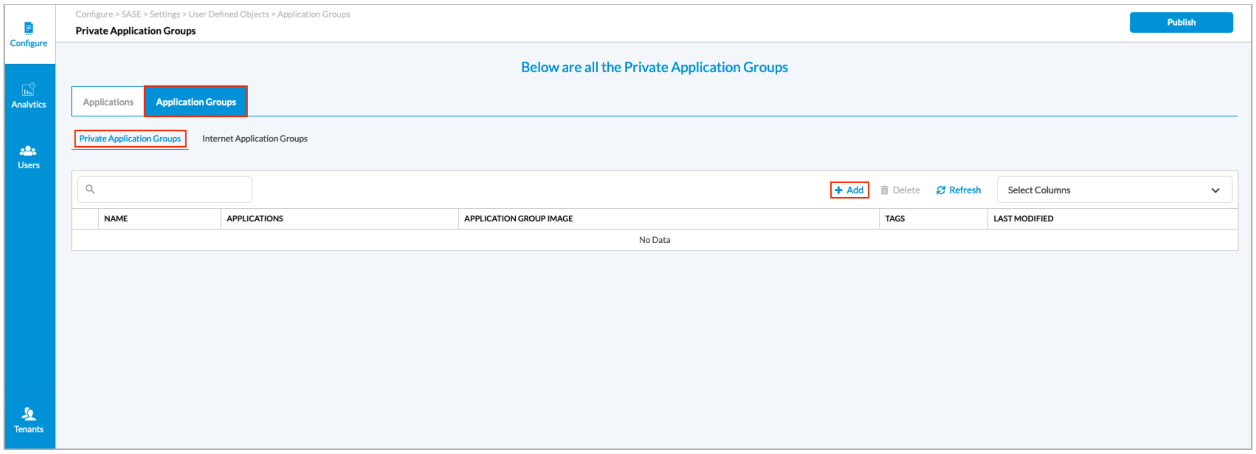


4. In the Enter Name and Tags section, enter a name for the client-native application and, optionally, one or more tags to include. A tag is an alphanumeric text descriptor with no spaces or special characters that you use for searching objects.
5. Click Save.

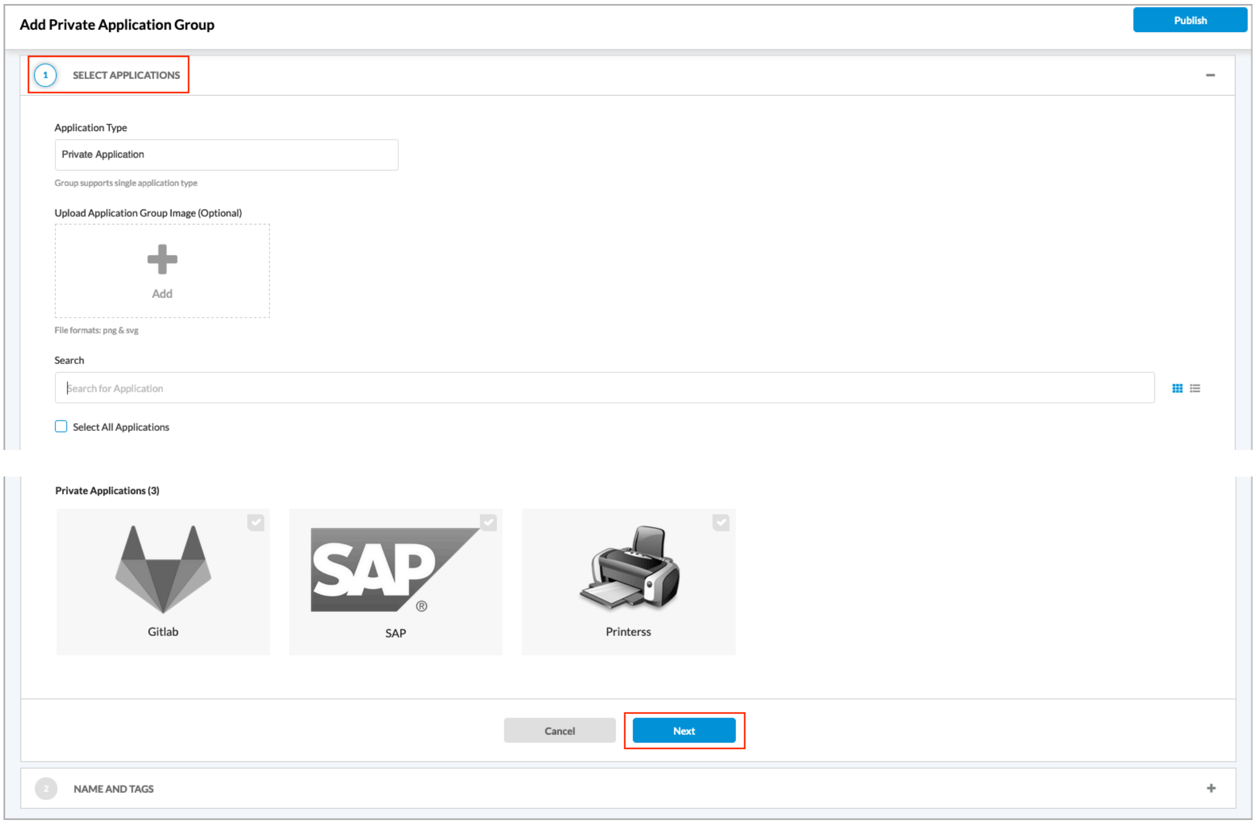
Configure Private Application Groups

To configure private application groups:

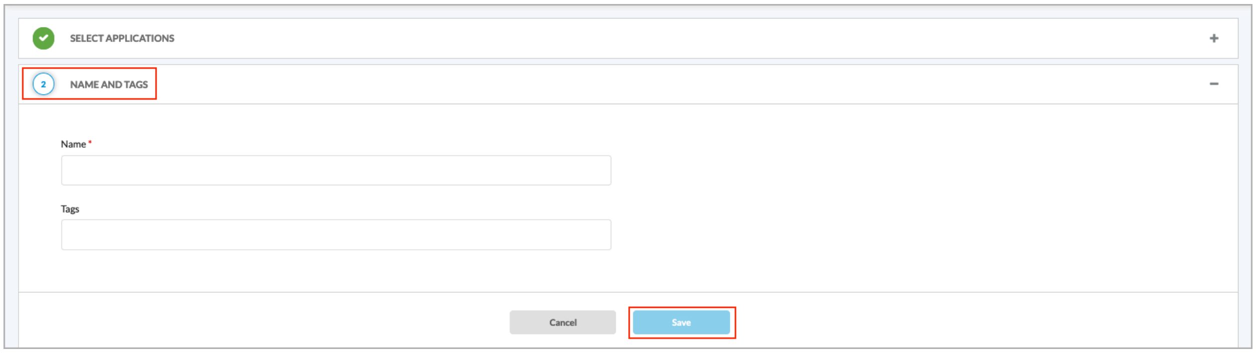
1. In the Private Applications default landing screen, select the Application Groups tab, then select the Private Application Groups subtab. The screen displays any private application groups that you have previously defined. Note that client-native private application groups are not supported. Also, you can include only private applications in private application groups.


Configure > SASE > Settings > User Defined Objects > Application Groups
Private Application Groups
Publish
Configure
Analytics
Users
Tenants
Below are all the Private Application Groups
Applications
Application Groups
Private Application Groups
Internet Application Groups
+ Add
Delete
Refresh
Select Columns
NAME
APPLICATIONS
APPLICATION GROUP IMAGE
TAGS
LAST MODIFIED
No Data

2. Click + Add to add a new private application group.



3. In the Select Applications section, you can click the Add icon to upload an application group image.
4. Use the search bar to find an application, click one or more of the listed applications to add, or click the Select All Application checkbox to add all private applications to the group.
5. Click Next. The Name and Tags section displays.

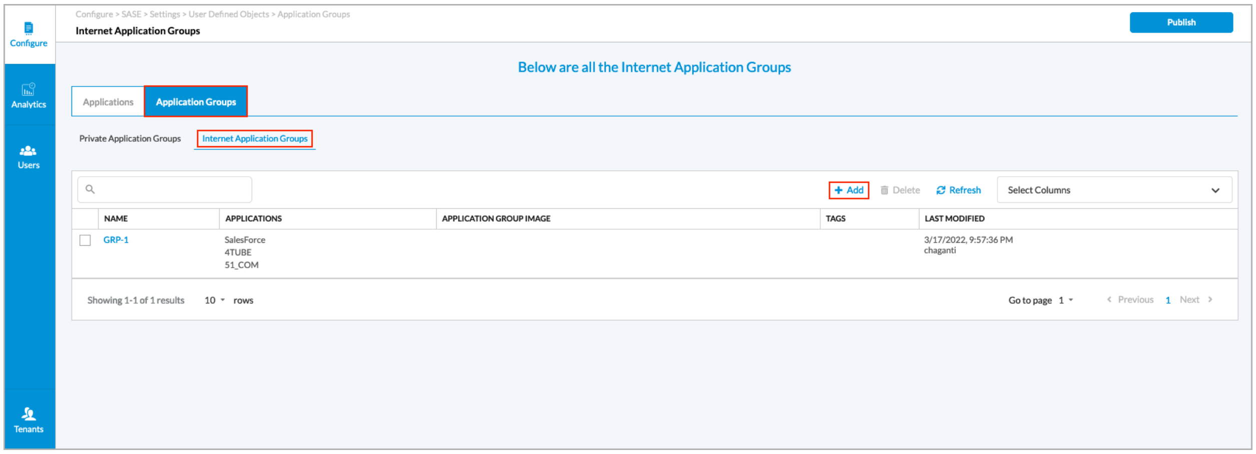


6. Enter a name for the private application group and, optionally, one or more tags to include. A tag is an alphanumeric text descriptor with no spaces or special characters that you use for searching objects.
7. Click Save.

Configure Internet Application Groups

To configure internet application groups:

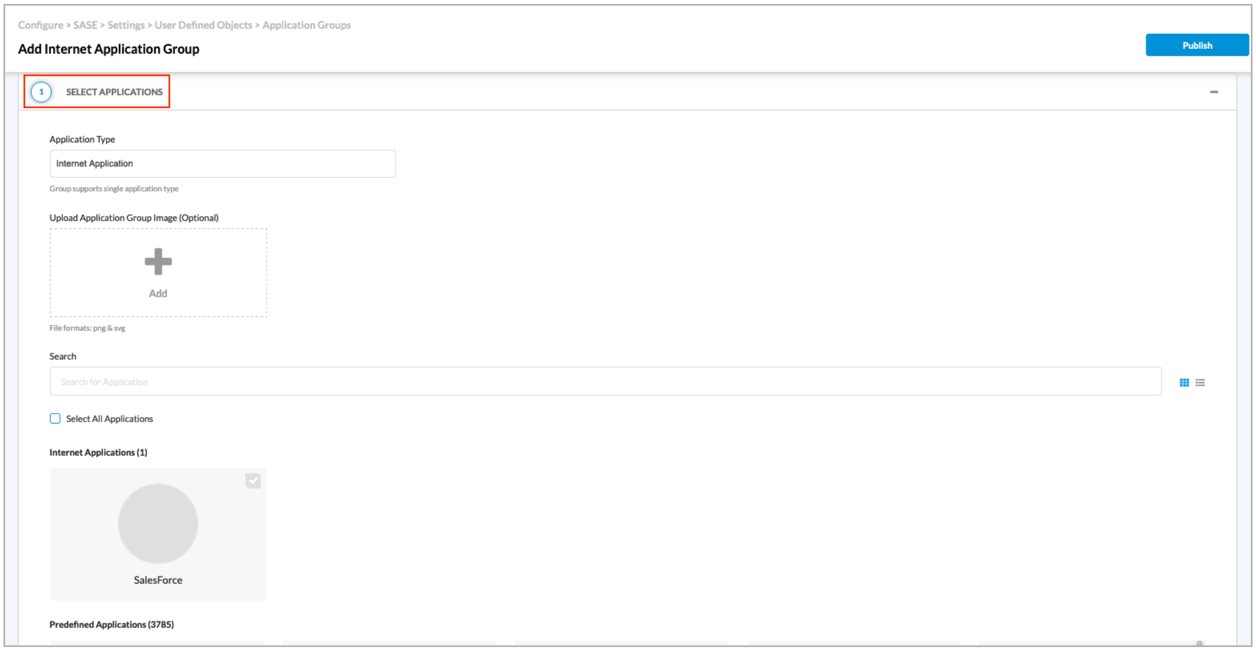
1. In the Private Applications default landing screen, select the Application Groups tab, and then select the Internet Application Groups tab. The screen displays any internet application groups that are already defined and the applications included in each group.


Configure
Analytics
Users
Tenants
Configure > SASE > Settings > User Defined Objects > Application Groups
Internet Application Groups
Publish
Below are all the Internet Application Groups
Applications
Application Groups
Private Application Groups
Internet Application Groups
+ Add
Delete
Refresh
Select Columns

	NAME	APPLICATIONS	APPLICATION GROUP IMAGE	TAGS	LAST MODIFIED
□	GRP-1	SalesForce 4TUBE 51_COM			3/17/2022, 9:57:36 PM chaganti

Showing 1-1 of 1 results 10 rows Go to page 1 Previous 1 Next

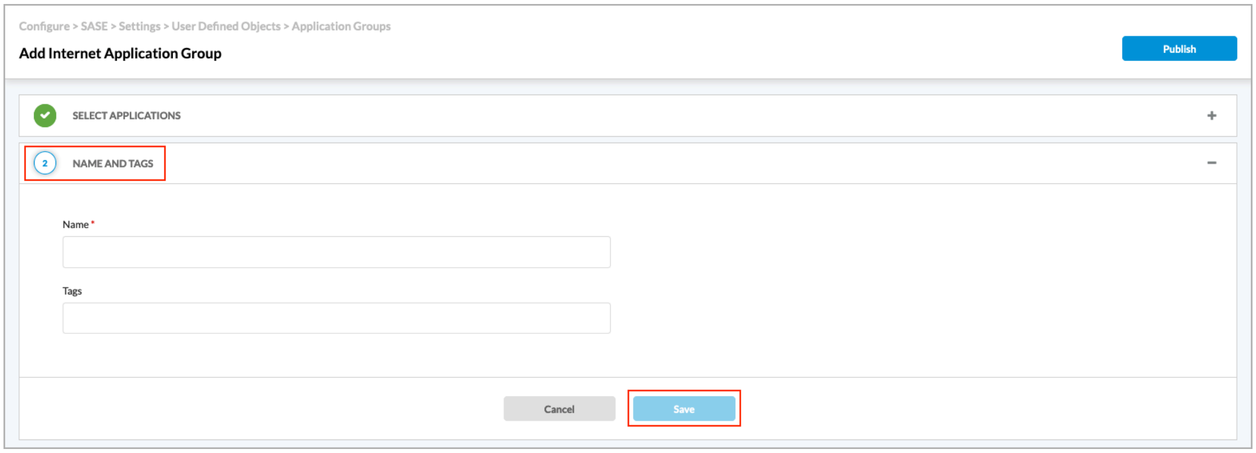
2. Click + Add to add a new internet application group. The Add Internet Application Group screen displays the available internet applications and predefined applications.


Configure > SASE > Settings > User Defined Objects > Application Groups
Add Internet Application Group
Publish
1 SELECT APPLICATIONS
Upload Application Group Image (Optional)
Add
File formats: png & svg
Search
Search for Application
Select All Applications
Internet Applications (1)
SalesForce
Predefined Applications (3785)

Application Type: Internet Application

Group supports single application type

3. In the Select Applications section, click the Add icon to upload an application group image.
4. Click one or more of the listed applications to add them to the group, or click the Select All Applications checkbox to add all internet applications to the group. You can also use the search bar to search for applications to add to the group.
5. Click Next. The Name, Description, and Tags section displays.


Configure > SASE > Settings > User Defined Objects > Application Groups
Add Internet Application Group
Publish
SELECT APPLICATIONS
2 NAME AND TAGS
Name *
Tags
Cancel
Save

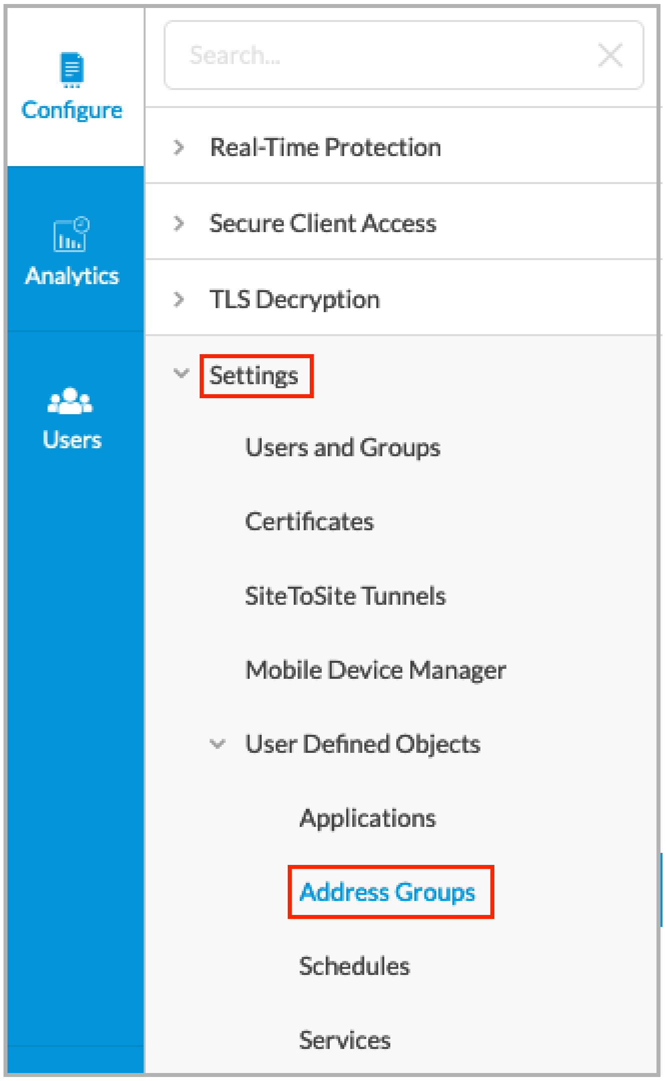
6. Enter a name for the new internet application group and, optionally, one or more tags to include. A tag is an alphanumeric text descriptor with no spaces or special characters that you use for searching objects.
7. Click Save.

Configure Address Group Objects

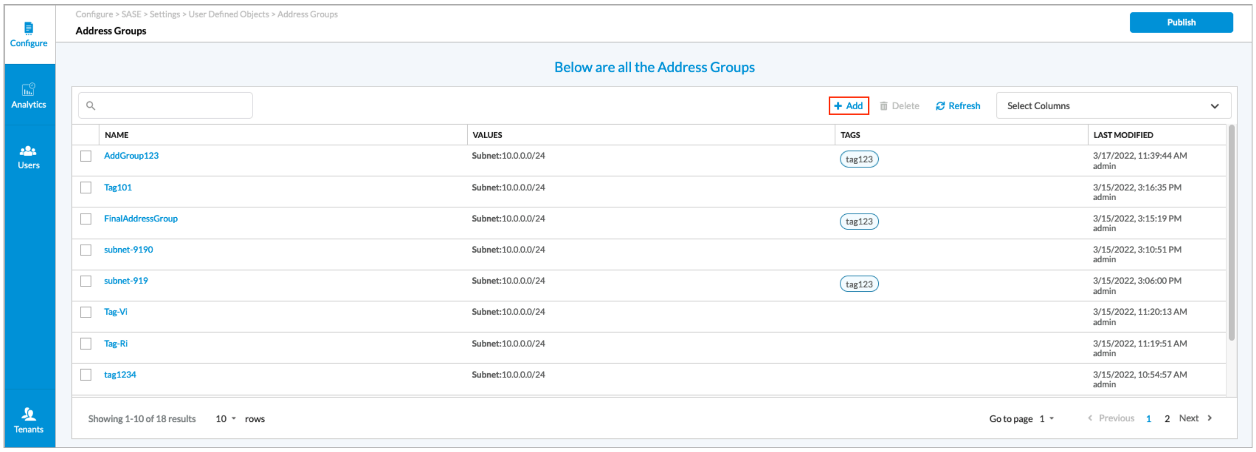
A SASE address group object configures match criteria based on source IP address, destination IP address, or a combination of both. You can define address groups that are then used when defining internet protection rules, private application rules, and secure client access rules.

To define address groups:

1. Go to Configure > Settings > User-Defined Objects > Address Groups in the left menu bar.



The Address Groups screen displays all current address groups.



Configure > SASE > Settings > User Defined Objects > Address Groups

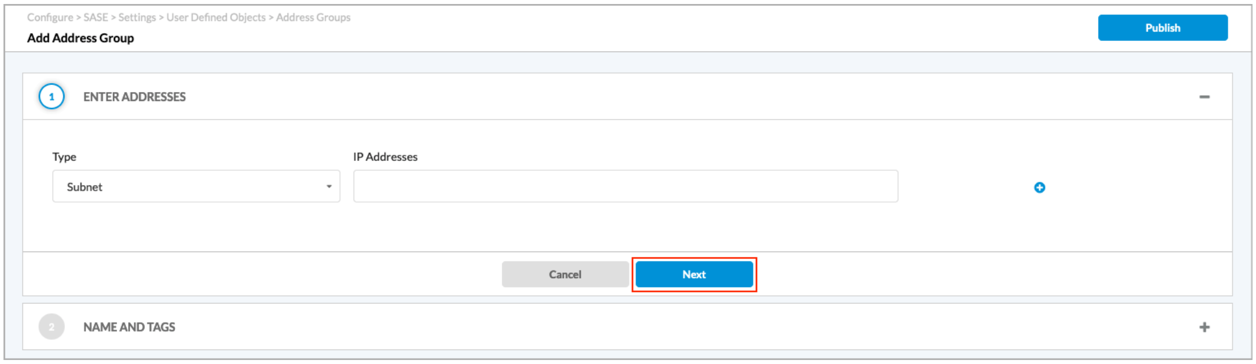
Address Groups

Below are all the Address Groups

NAME	VALUES	TAGS	LAST MODIFIED
AddGroup123	Subnet:10.0.0.0/24	tag123	3/17/2022, 11:39:44 AM admin
Tag101	Subnet:10.0.0.0/24		3/15/2022, 3:16:35 PM admin
FinalAddressGroup	Subnet:10.0.0.0/24	tag123	3/15/2022, 3:15:19 PM admin
subnet-9190	Subnet:10.0.0.0/24		3/15/2022, 3:10:51 PM admin
subnet-919	Subnet:10.0.0.0/24	tag123	3/15/2022, 3:06:00 PM admin
Tag-Vi	Subnet:10.0.0.0/24		3/15/2022, 11:20:13 AM admin
Tag-Ri	Subnet:10.0.0.0/24		3/15/2022, 11:19:51 AM admin
tag1234	Subnet:10.0.0.0/24		3/15/2022, 10:54:57 AM admin

Showing 1-10 of 18 results 10 rows

2. Click + Add to add a new IP address group. In the Add Address Group screen, enter information for the following fields.



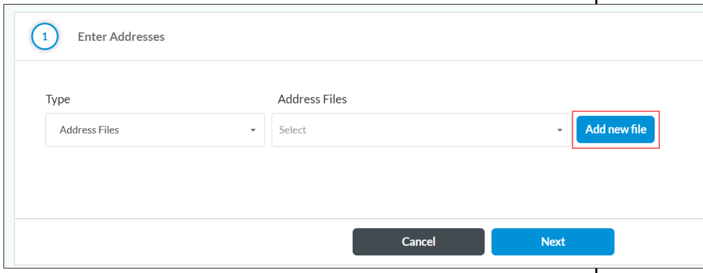
Configure > SASE > Settings > User Defined Objects > Address Groups

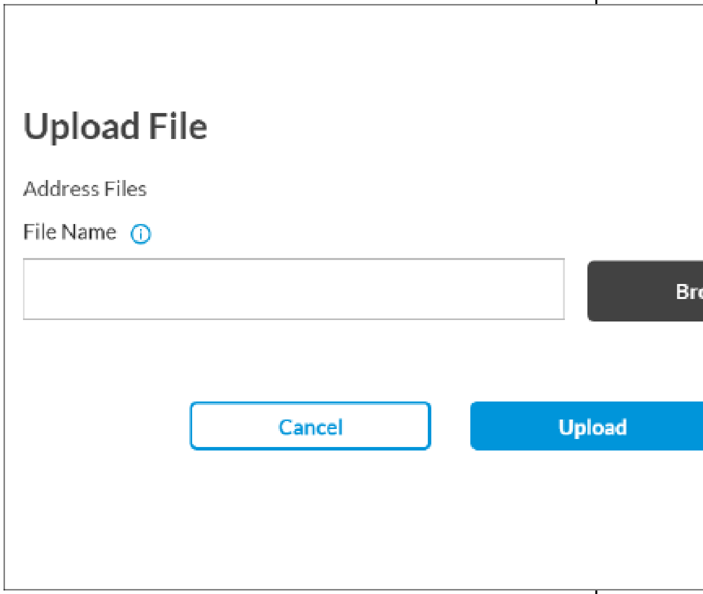
Add Address Group

Type: Subnet

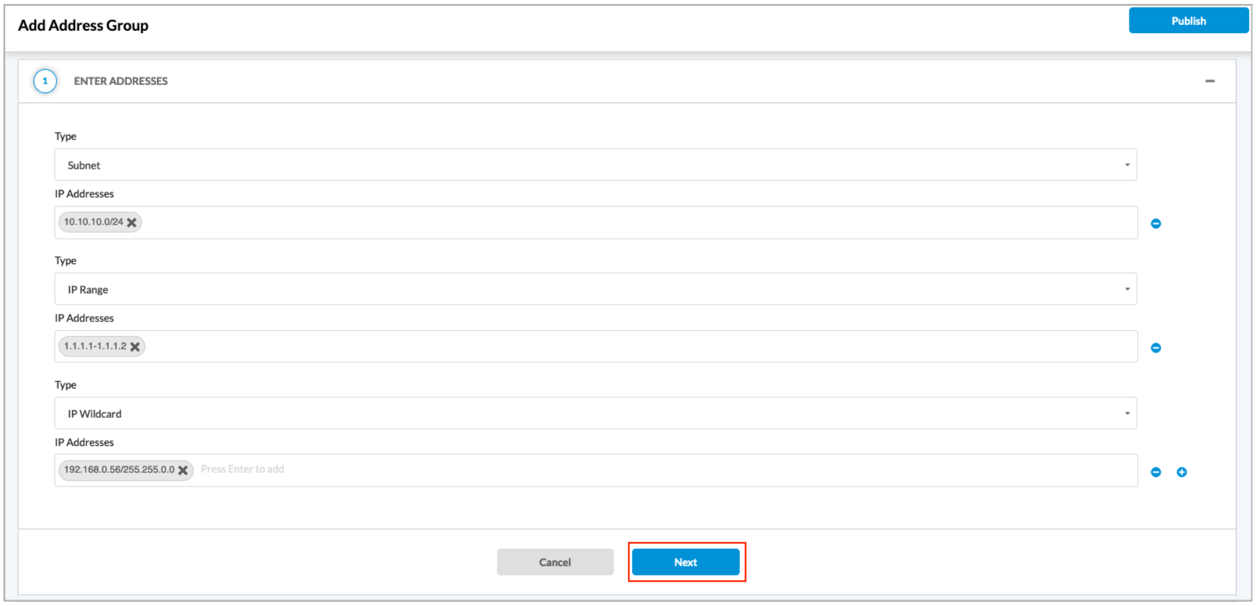
IP Addresses

Field	Description
Type	Select an address group type: ◦ Address Files ◦ Dynamic Address ◦ FQDN ◦ IP range ◦ IP wildcard ◦ IPv6 subnet ◦ Subnet
IP Addresses	Enter IP addresses for the type: ◦ IP range—Valid IP address range, for example, 10.2.1.1-10.2.2.2

Field	Description
	◦ IP wildcard—Valid IP wildcard, for example, 192.168.0.56/255.255.0.255 ◦ IP6 subnet—Valid IPv6 subnet, for example, 2001:0db8:85a3:0000:0000:8a2e:0370:7334 ◦ Subnet—One or more valid IPv4 subnets, for example, 10.1.1.0/24
Address Files	(For Releases 12.1.1 and later.) When you select the Address Files type, select an address file. For more information, see Manage Files and Folders. To add a new address file: 1. Click Add new file.  1 Enter Addresses Type: Address Files Address Files: Select 2. In the Upload File popup window, click Browse and select an address file to upload. The file must be in CSV format.

Field	Description
	 Upload File Address Files File Name Bro Cancel Upload 3. Click Upload.

3. Click the ⊕ Add icon to add a new IP address group. You can add multiple Address Group types, as shown here:



Add Address Group

Publish

1 ENTER ADDRESSES

Type: Subnet

IP Addresses: 10.10.10.0/24

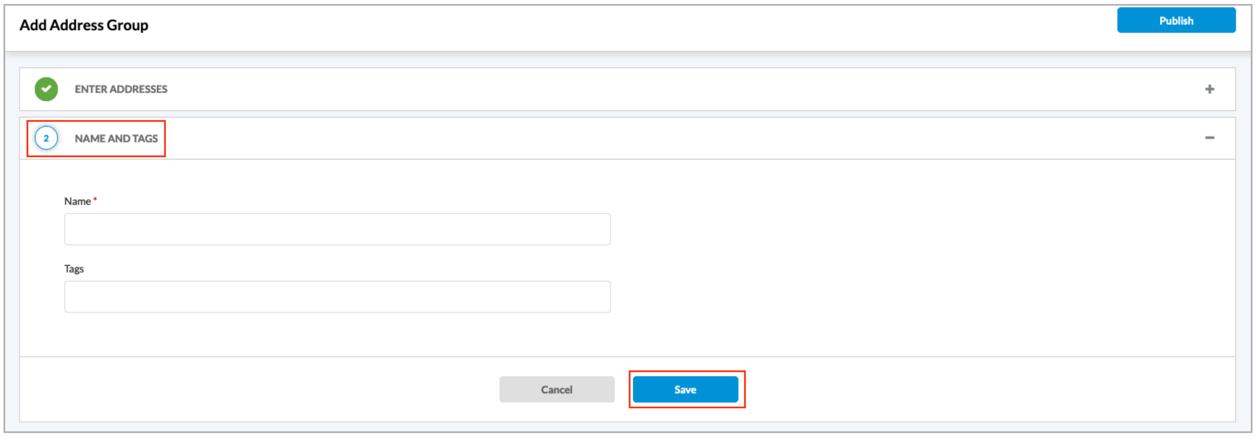
Type: IP Range

IP Addresses: 1.1.1.1-1.1.1.2

Type: IP Wildcard

IP Addresses: 192.168.0.56/255.255.0.0

4. Click Next. The Name and Tags section displays.



5. Enter a name for the new IP address group and, optionally, one or more tags to include. A tag is an alphanumeric text descriptor with no spaces or special characters that you use for searching objects.
6. Click Save.

Configure SASE Schedules

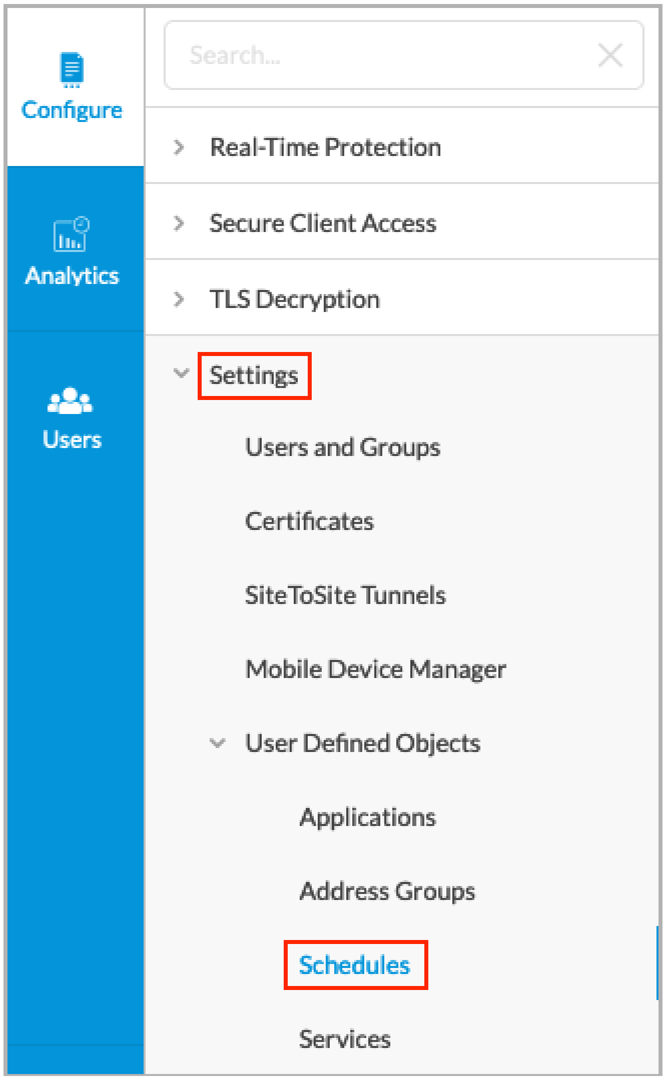
Security policy rules work at all dates and times. You can define a schedule object to limit a security policy to specific times, and you then use the schedule objects when defining internet protection rules, private application rules, and secure client access rules.

Policy objects support match criteria based on the time of day. For example, you can define a policy rule that is effective only during certain times of the day, such as lunch hours or after normal working hours.

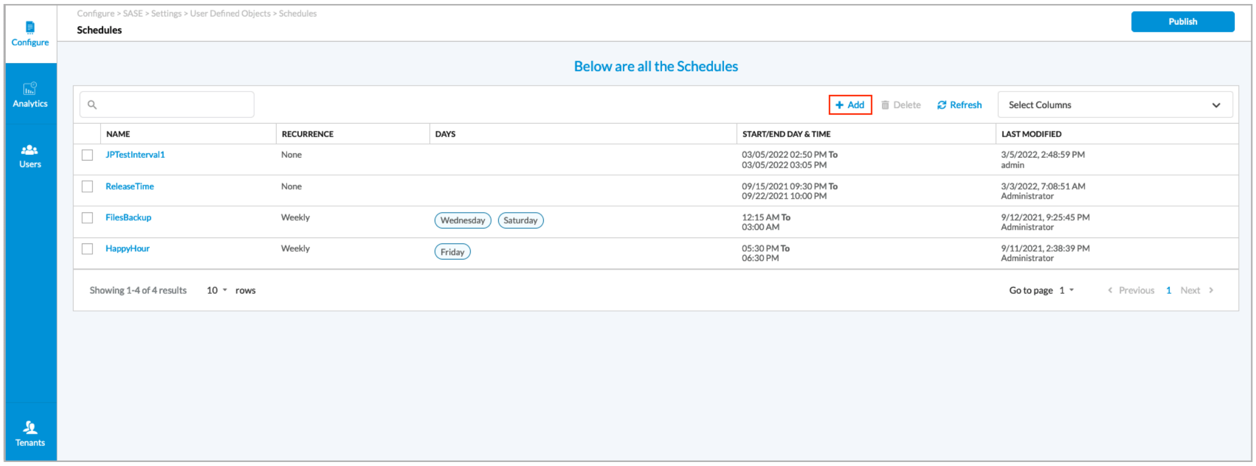
To configure a schedule object, you configure either a fixed date and time range or a recurring daily or weekly schedule.

To configure schedule objects:

1. Go to Configure > Settings > User-Defined Objects > Schedules in the left menu bar.



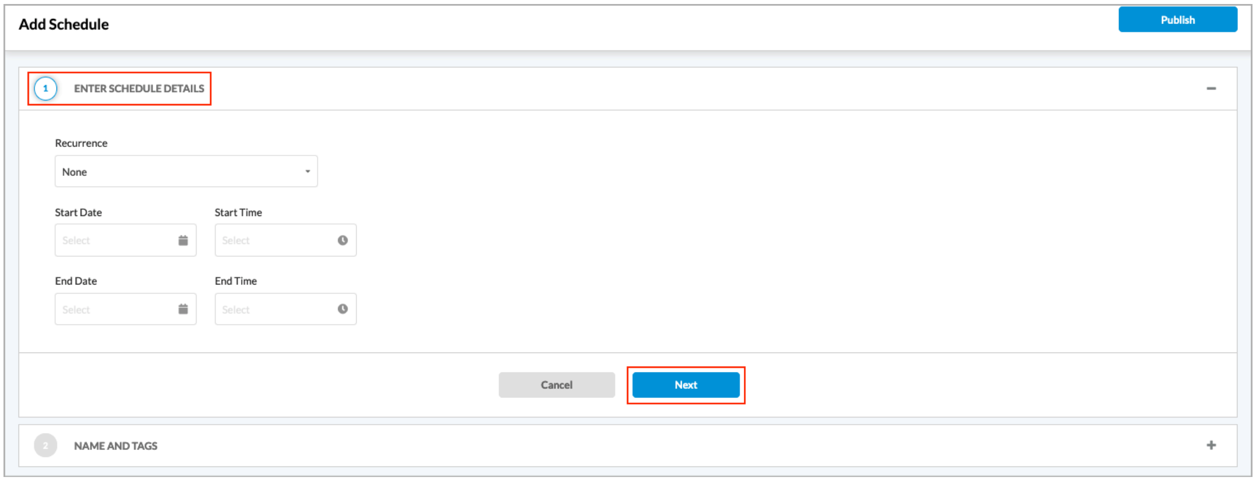
The Schedules screen displays the schedules that are already configured.


Configure > SASE > Settings > User Defined Objects > Schedules
Schedules
Publish
Configure
Analytics
Users
Tenants
Below are all the Schedules
+ Add
Delete
Refresh
Select Columns

	NAME	RECURRENCE	DAYS	START/END DAY & TIME	LAST MODIFIED
□	JPTestInterval1	None		03/05/2022 02:50 PM To 03/05/2022 03:05 PM	3/5/2022, 2:48:59 PM admin
□	ReleaseTime	None		09/15/2021 09:30 PM To 09/22/2021 10:00 PM	3/3/2022, 7:08:51 AM Administrator
□	FilesBackup	Weekly	Wednesday Saturday	12:15 AM To 03:00 AM	9/12/2021, 9:25:45 PM Administrator
□	HappyHour	Weekly	Friday	05:30 PM To 06:30 PM	9/11/2021, 2:38:39 PM Administrator

Showing 1-4 of 4 results 10 rows
Go to page 1 Previous 1 Next

2. Click the + Add icon to add a schedule. In the Add Schedule screen, enter information for the following fields.



Add Schedule

1 ENTER SCHEDULE DETAILS

Recurrence: None

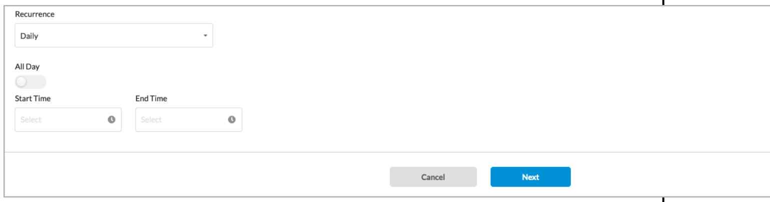
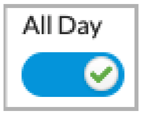
Start Date: Select

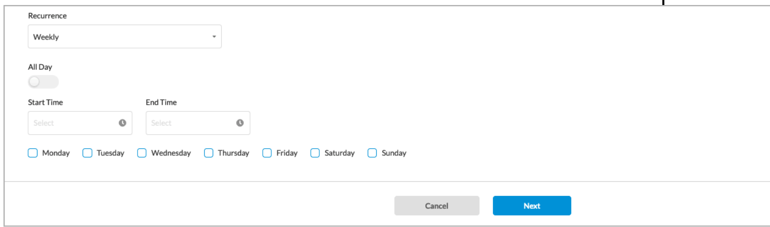
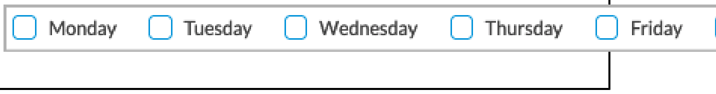
Start Time: Select

End Date: Select

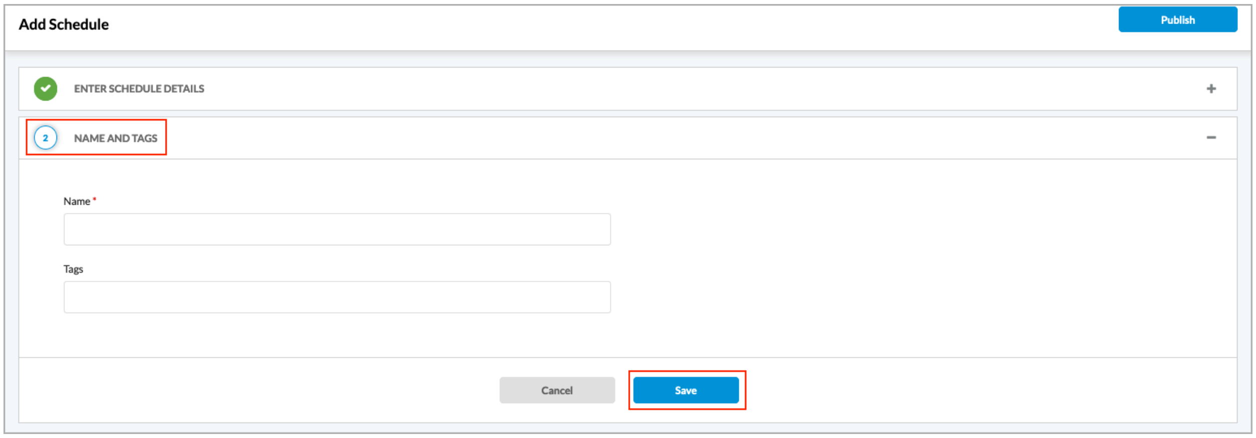
End Time: Select

2 NAME AND TAGS

Field	Description
Recurrence	Select None, Daily, or Weekly.
◦ None	If you select None, enter the following information: ◦ Start Date—Select a start date. ◦ Start Time—Select a start time. ◦ End Date—Select an end date. ◦ End Time—Select an end time.
◦ Daily	If you select Daily, enter information for the following fields:  Recurrence: Daily All Day Start Time: Select End Time: Select ◦ All Day—Click the slider to schedule the security policy to be in effect all day. 

Field	Description
	◦ Start Time—Select a start time from the drop-down list. ◦ End Time—Select an end time from the drop-down list.
◦ Weekly	If you select Weekly, enter information for the following fields:  Recurrence: Weekly All Day Start Time End Time Select Select Monday Tuesday Wednesday Thursday Friday Saturday Sunday Cancel Next ◦ All Day—Click the slider to schedule the security policy to be in effect all day. ◦ Start Time—Select a start time. ◦ End Time—Select an end time. ◦ Select the days the security policy is to be in effect. 

3. Click Next. The Name and Tags section displays.



4. Enter a name for the new schedule and, optionally, one or more tags to include. A tag is an alphanumeric text descriptor with no spaces or special characters that you use for searching objects.
5. Click Save.

Configure SASE Services

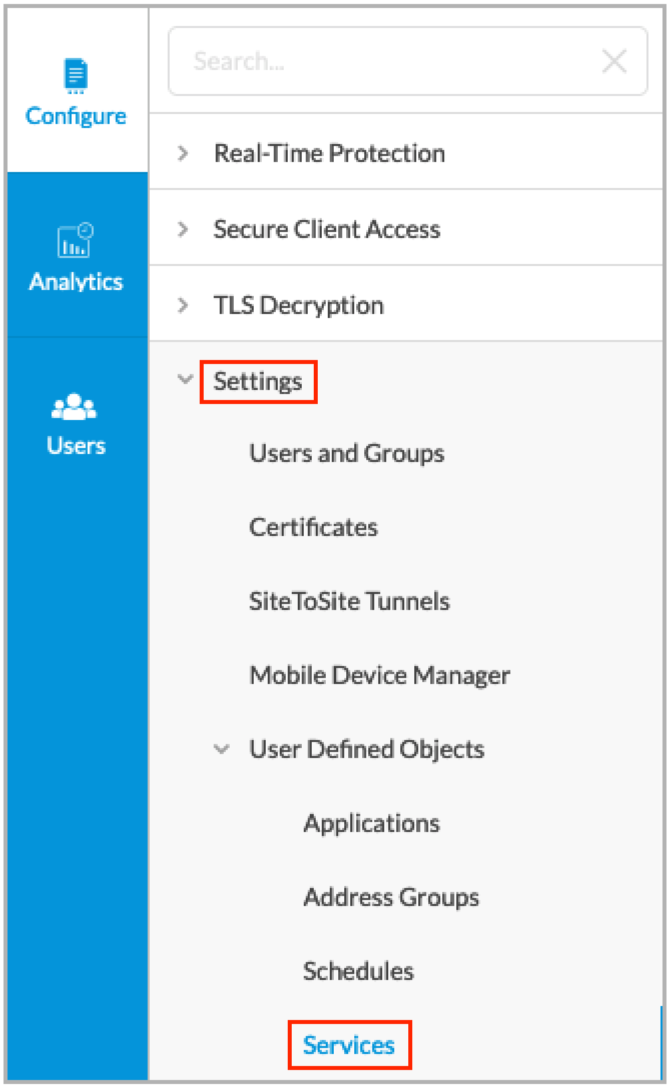
Security policies can reference service objects, which define match criteria based on protocol name and number, and on source and destination port number. Versa provides default predefined services and object definitions, and also provides periodic updates to the default services and objects.

You can also create custom service objects. One reason to do this might be if a well-known service runs on a non-standard port or if the predefined services are missing the desired port and protocol combination. Another reason might be to limit the number of ports that an application can use. For example, you could limit FTP to use only port 21 instead of ports 20 and 21.

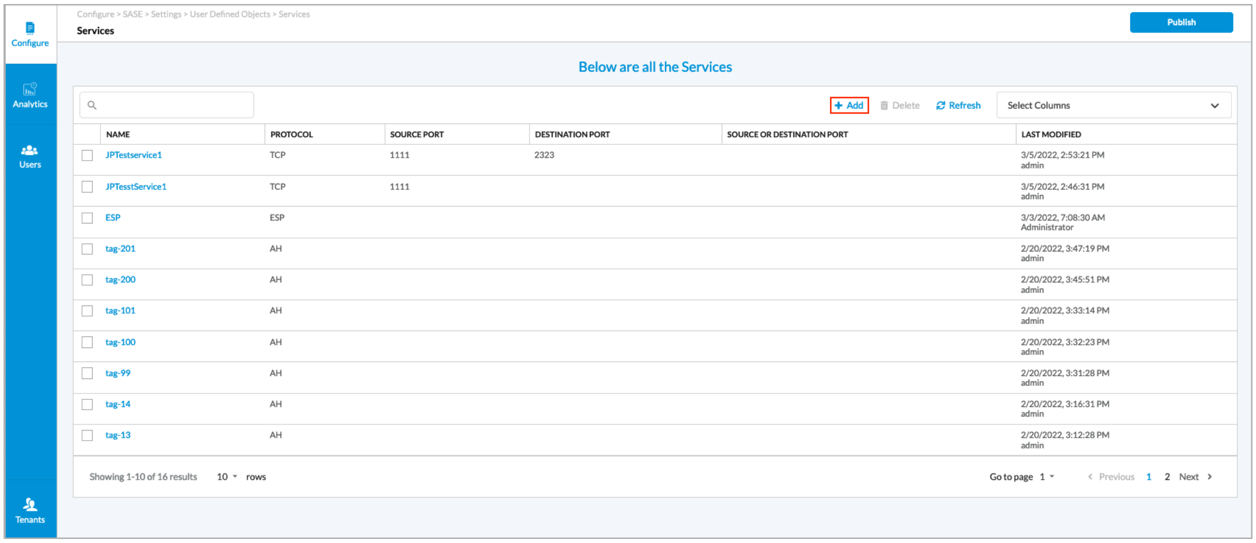
The custom service objects that you define for a tenant can be used only by that tenant, and they are not visible to any other tenants.

To define service objects:

1. Go to Configure > Settings > User-Defined Objects > Services.



The Services screen displays all services that are already configured. To find a particular service, use the search box.



Services

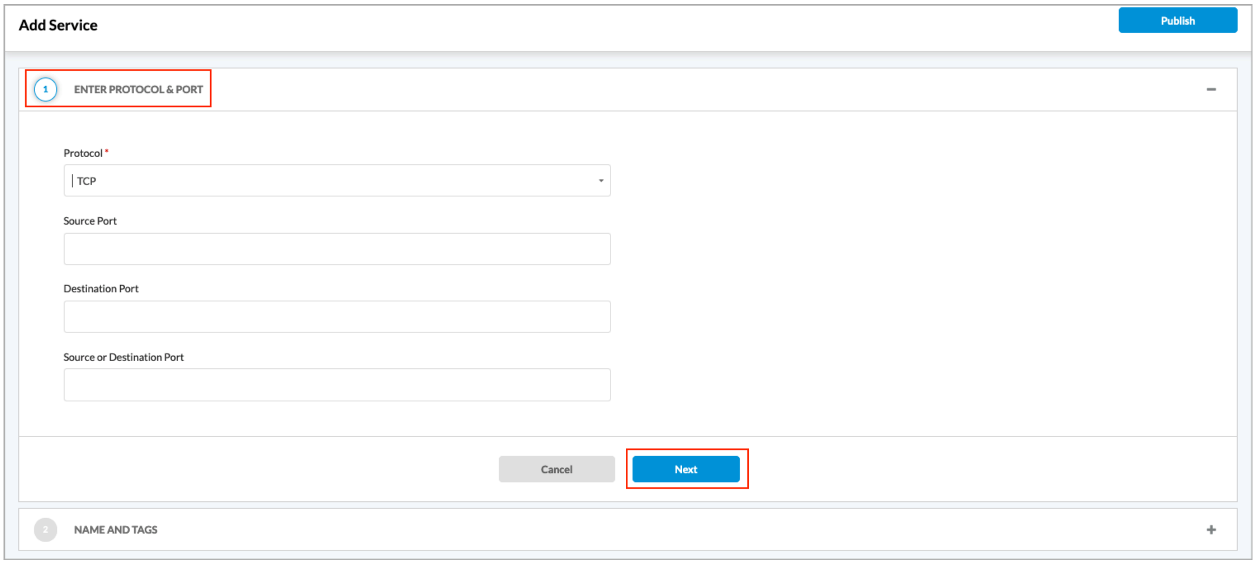
Below are all the Services

	NAME	PROTOCOL	SOURCE PORT	DESTINATION PORT	SOURCE OR DESTINATION PORT	LAST MODIFIED
□	JPTestservice1	TCP	1111	2323		3/5/2022, 2:53:21 PM admin
□	JPTesstService1	TCP	1111			3/5/2022, 2:46:31 PM admin
□	ESP	ESP				3/3/2022, 7:08:30 AM Administrator
□	tag-201	AH				2/20/2022, 3:47:19 PM admin
□	tag-200	AH				2/20/2022, 3:45:51 PM admin
□	tag-101	AH				2/20/2022, 3:33:14 PM admin
□	tag-100	AH				2/20/2022, 3:32:23 PM admin
□	tag-99	AH				2/20/2022, 3:31:28 PM admin
□	tag-14	AH				2/20/2022, 3:16:31 PM admin
□	tag-13	AH				2/20/2022, 3:12:28 PM admin

Showing 1-10 of 16 results 10 rows

Go to page 1 ‹ Previous 1 2 Next ›

2. Click the + Add icon to add a new service. In the Add Service screen, enter information for the following fields. Note that you configure protocol options only for the TCP, TCP and UDP, and UDP protocols.



Add Service

1 ENTER PROTOCOL & PORT

Protocol *
TCP

Source Port

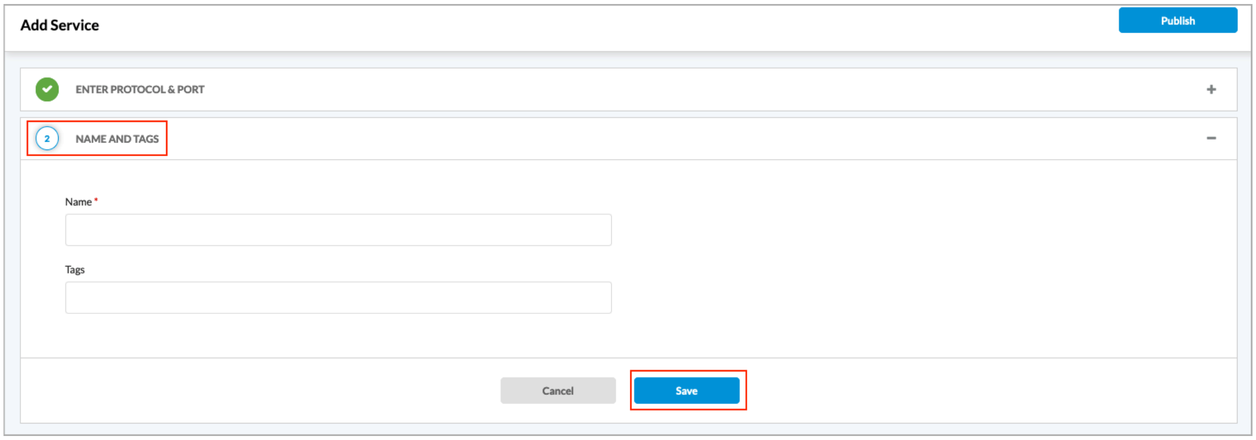
Destination Port

Source or Destination Port

2 NAME AND TAGS

Field	Description
Protocol	Select a protocol.
Source Port	Enter the source port for the protocol. For multiple entries, use comma-separated single port values or range of port values (using hyphens), for example, 1-100,2-200,3.
Destination Port	Enter the destination port for the protocol. For multiple entries, use comma-separated single port values or range of port values (using hyphens), for example, 1-100,2-200,3.
Source or Destination Port	Enter the source or destination port for the protocol.

3. Click Next. The Name and Tags section displays.



4. Enter a name for the new service and, optionally, enter one or more tags.
5. Click Save.

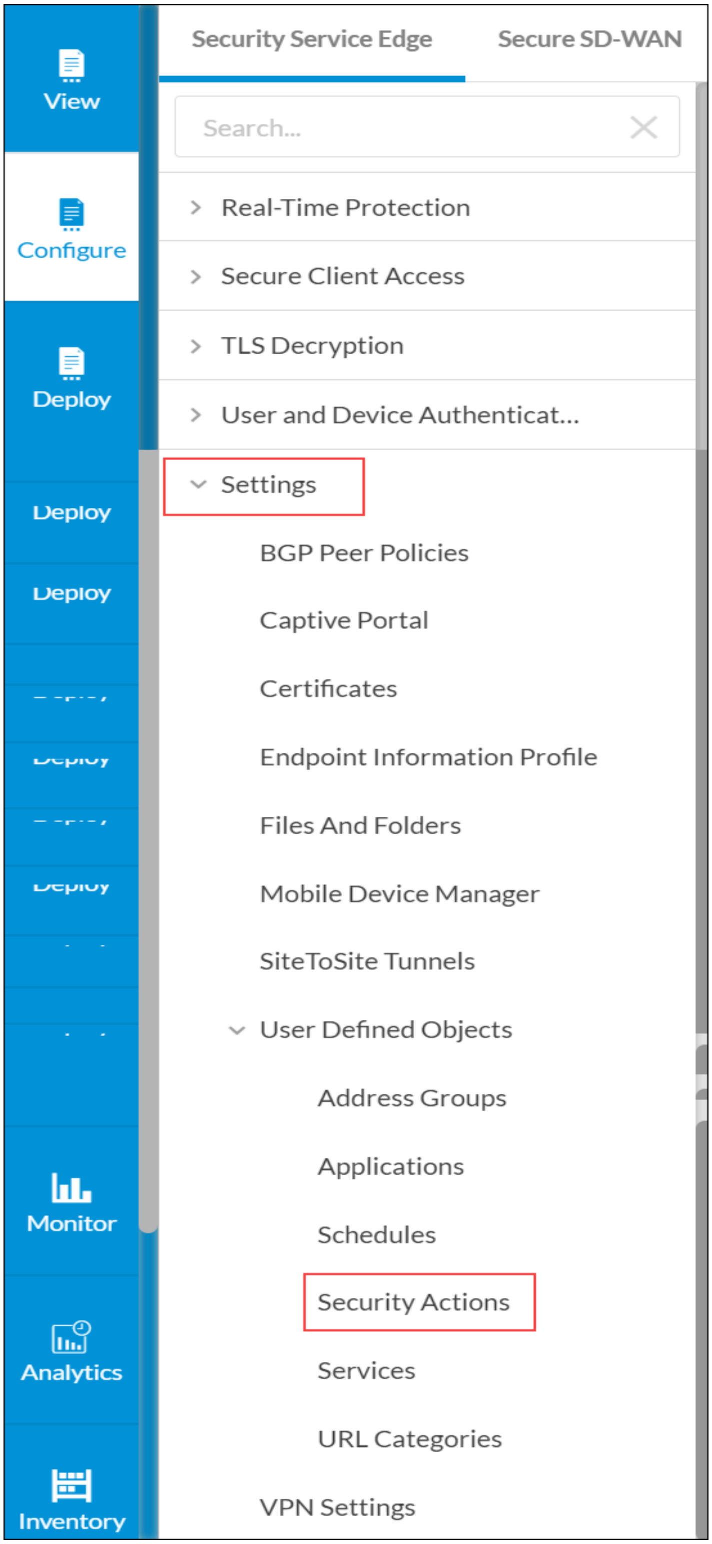
Configure Custom Security Actions

For Releases 11.4.1 and later.

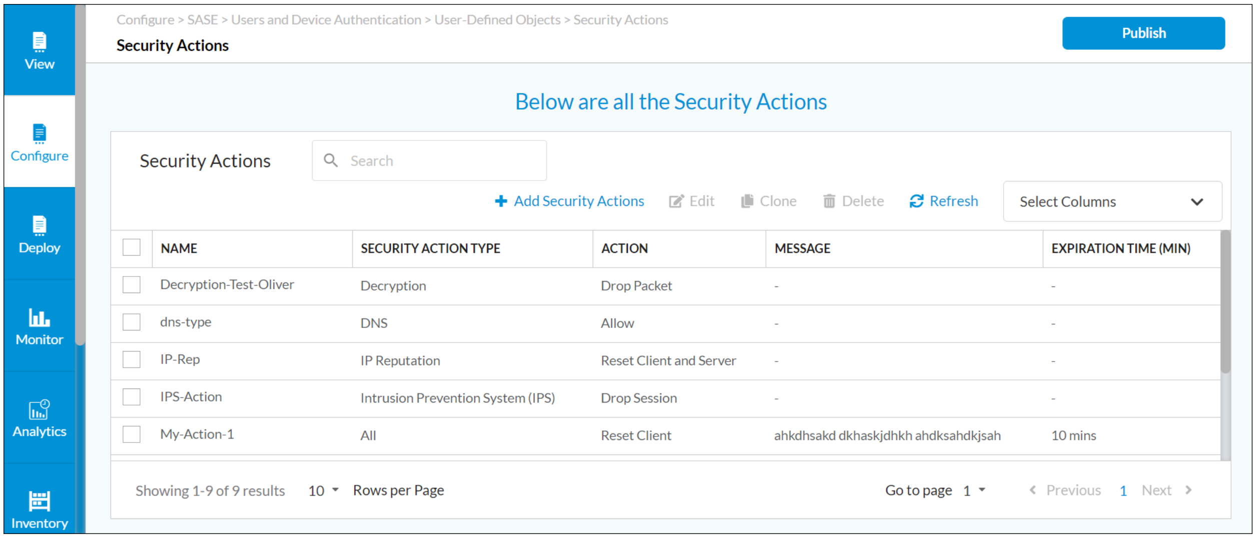
For URL filtering, you can can select a user-defined action as the action to take when a filter matches.

To configure user-defined security actions:

1. Go to Configure > Settings > User-Defined Objects > Security Actions.



The Security Actions screen displays the security actions that are already configured. To locate a particular action, use the search box.



Configure > SASE > Users and Device Authentication > User-Defined Objects > Security Actions

Security Actions

Below are all the Security Actions

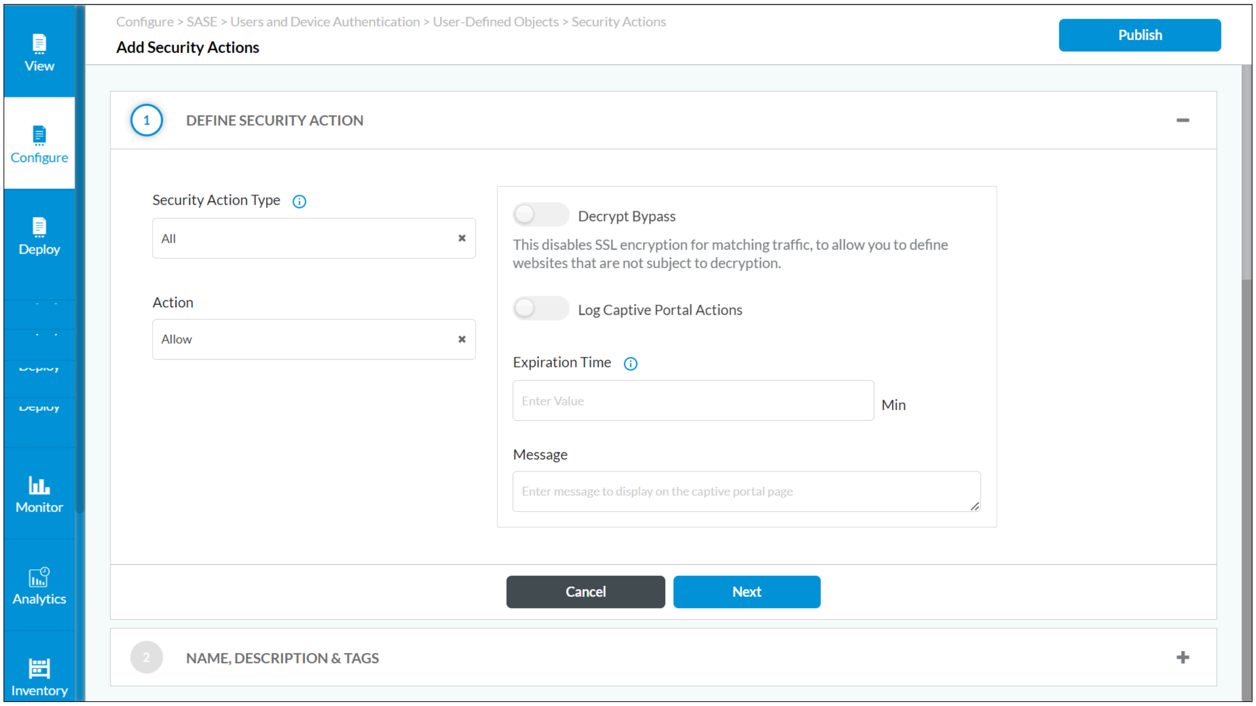
Security Actions   Search

+ Add Security Actions Edit Clone Delete Refresh Select Columns

□	NAME	SECURITY ACTION TYPE	ACTION	MESSAGE	EXPIRATION TIME (MIN)
□	Decryption-Test-Oliver	Decryption	Drop Packet	-	-
□	dns-type	DNS	Allow	-	-
□	IP-Rep	IP Reputation	Reset Client and Server	-	-
□	IPS-Action	Intrusion Prevention System (IPS)	Drop Session	-	-
□	My-Action-1	All	Reset Client	ahkdhsakd dkhaskjdhkh ahdksahdkjsah	10 mins

Showing 1-9 of 9 results 10 Rows per Page Go to page 1 Previous 1 Next

2. Click the + Add Security Actions icon to add a new action. In the Add Security Actions screen, enter information for the following fields.



Configure > SASE > Users and Device Authentication > User-Defined Objects > Security Actions

Add Security Actions

1 DEFINE SECURITY ACTION

Security Action Type: All

Action: Allow

Decrypt Bypass

This disables SSL encryption for matching traffic, to allow you to define websites that are not subject to decryption.

Log Captive Portal Actions

Expiration Time: Enter Value Min

Message: Enter message to display on the captive portal page

Cancel Next

2 NAME, DESCRIPTION & TAGS

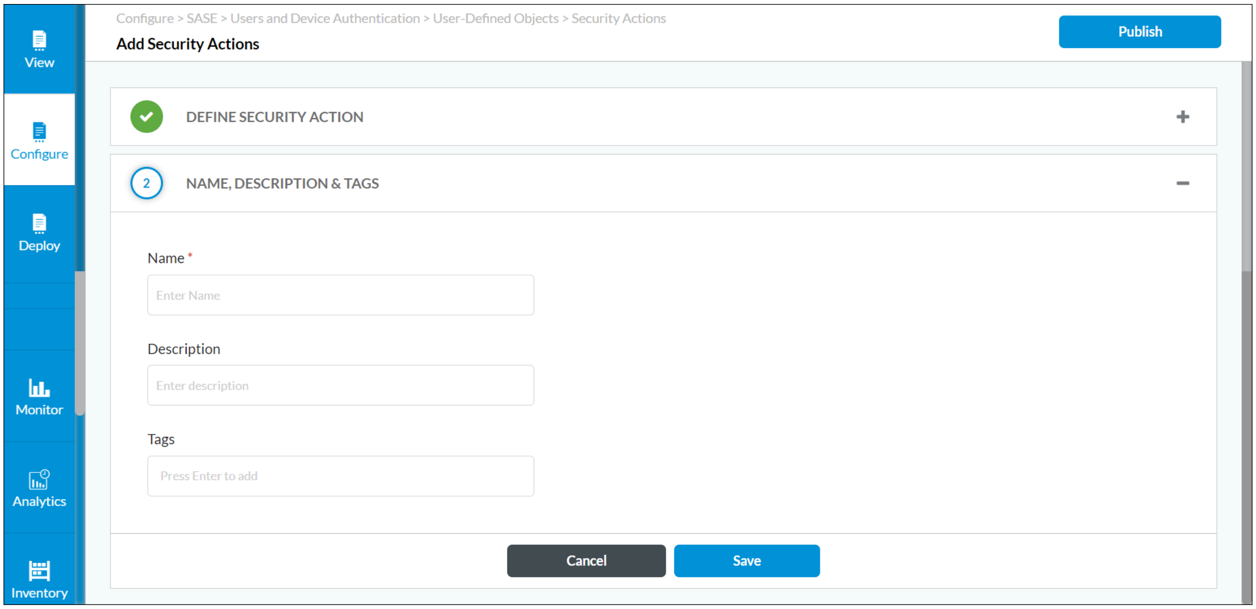
Field	Description
Security Action Type	Select the type of action to which to apply the action when the page is redirected. The action type options represent the module for which the user-defined action was configured. For example, if you select

Field	Description
	URLF, the action can be used only in URL-filtering profiles. ◦ All—Apply to all action types. ◦ CASB—Apply to cloud access security broker (CASB) profiles. ◦ Decryption—Apply for decryption. ◦ DNS—Apply for DNS traffic. ◦ IP Reputation—Apply for IP-filtering profiles. ◦ IPS—Apply for the intrusion detection and prevention system. ◦ URLF—Apply for URL-filtering profiles.
Action	Select the action to take when the user is redirected to a captive portal. Note that not all actions are available for all action types. ◦ Allow—Allow the URL without generating an entry in the 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. ◦ Block—Block the URL and generate an entry in the URL-filtering log. ◦ Custom Redirection—The browser redirects the user to the URL configured in the Redirection URL field. Then, in the Redirection URL field, enter the redirection URL to redirect a user from one URL to another. ◦ Drop Packet—The browser waits for a response from the server and then drops the packets. ◦ Drop Session—The browser waits for a response from the server and then drops the session. ◦ Inform—The browser presents an information page that prompts the user to continue after clicking OK. ◦ 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.

Field	Description
	◦ Override—This action generates an entry in the URL-filtering log. The browser prompts the user to enter a PIN. Then, in the Override PIN field, enter a 4- to 6-digit PIN. ◦ Reset Client—The host responds by sending a TCP Reset packet to the client, and the browser displays an error message indicating that the connection has been reset. ◦ Reset Client and Server—The host responds by sending a TCP Reset packet back to the client and server. The browser displays an error message indicating that the connection was reset. ◦ Reset Server—The host responds by sending a TCP Reset packet to the server. The browser waits for a response from the server and then drops the session. ◦ Sinkhole—Return a false IP address to the URL, thus blocking a DNS sinkhole. A DNS sinkhole spoofs DNS servers to prevent the resolution of the hostnames associated with URLs. This action can help you identify infected hosts in a network if a firewall is unable to find the original source IP address of DNS request sender. Sinkhole malware DNS queries create responses to the client host queries directed at malicious domains and try to connect to a sinkhole IP address instead of connecting to malicious domains. You can check the traffic logs to identify infected hosts. You can apply the sinkhole to all, DNS, IP reputation, and URL-filtering action types. Configure the following sinkhole parameters: ▪ Domain Name—Enter the domain name in which the LDAP server resides. ▪ IP Address—Click the Add icon to enter one or more IP addresses. ▪ TTL—Enter the time-to-live (TTL) value, in seconds. *Range*: 1 through 65535 seconds *Default*: 30 seconds
Decrypt Bypass	Click to disable SSL encryption for matching traffic, to allow you to define websites that are not subject to decryption.
Log Captive Portal Actions	Click to log captive portal actions. If you do not enable

Field	Description
	logging, the custom message that you enter in the Message field is not displayed in the log displayed in Versa Analytics.
Expiration Time	Enter how often to redirect a user to the URL, in minutes. When a user first enters a URL and is redirected to a captive portal page, the Versa Operating System^{TM} (VOS^{TM}) device creates a cache entry, which expires after a global expiration time. While the cache entry is active, the device does not enforce the captive portal action, and users can view the webpage at the initial URL and at all URLs that belong to the same URL category, without seeing the captive portal page, with one exception. If the action is Block, all URLs are redirected to the Block page, regardless of the expiration time *Range:* 1 through 65535 minutes *Default:* 1 minute
Message	Enter a message to display on the captive portal page.

3. Click Next. In the Enter Name, Description, and Tags section, enter information for the following fields.



Field	Description
Name (Required)	Enter a name for the security action.
Description	Enter a text description.
Tags	Enter one or more tags. A tag is an alphanumeric text descriptor with no spaces or special characters that you use for searching tunnels.

4. Click Save.

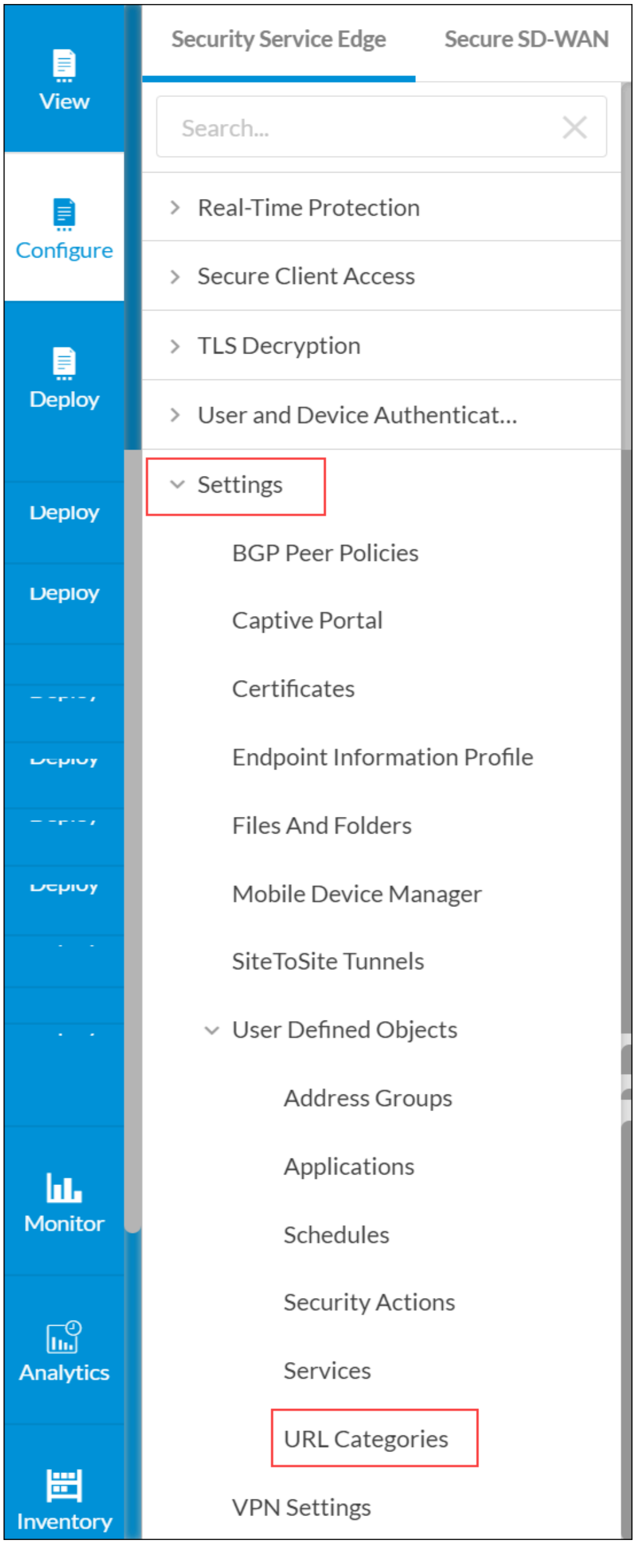
Configure Custom URL Categories

For Releases 11.4.1 and later.

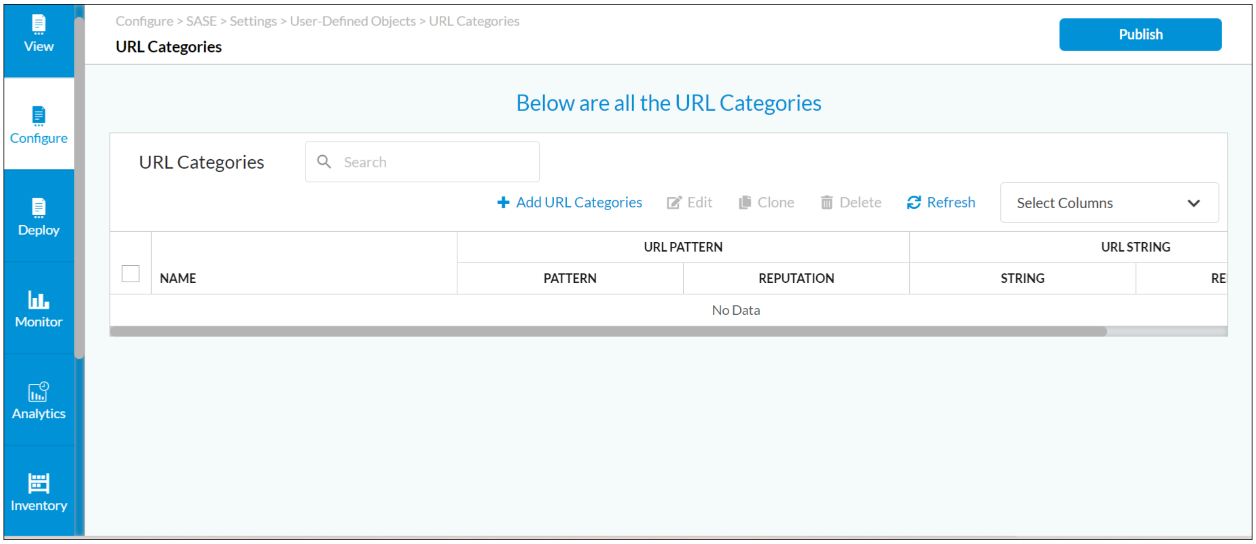
You can create custom URL category objects on a per-tenant basis. You assign a unique name to each custom URL category, and you use a string or pattern match to define information about the URLs. You also associate a reputation value with the URL category. You can use a custom URL category in NGFW and SD-WAN policy rules to specify match criteria for a Layer 7 URL category. You can also specify custom URL categories in the category-based action rules and reputation-based action rules of a URL-filtering profile.

To configure custom URL categories:

1. Go to Configure > Settings > User-Defined Objects > URL Categories.



The URL Categories screen displays the URL categories that are already configure. To find a particular category, use the search box.



Configure > SASE > Settings > User-Defined Objects > URL Categories

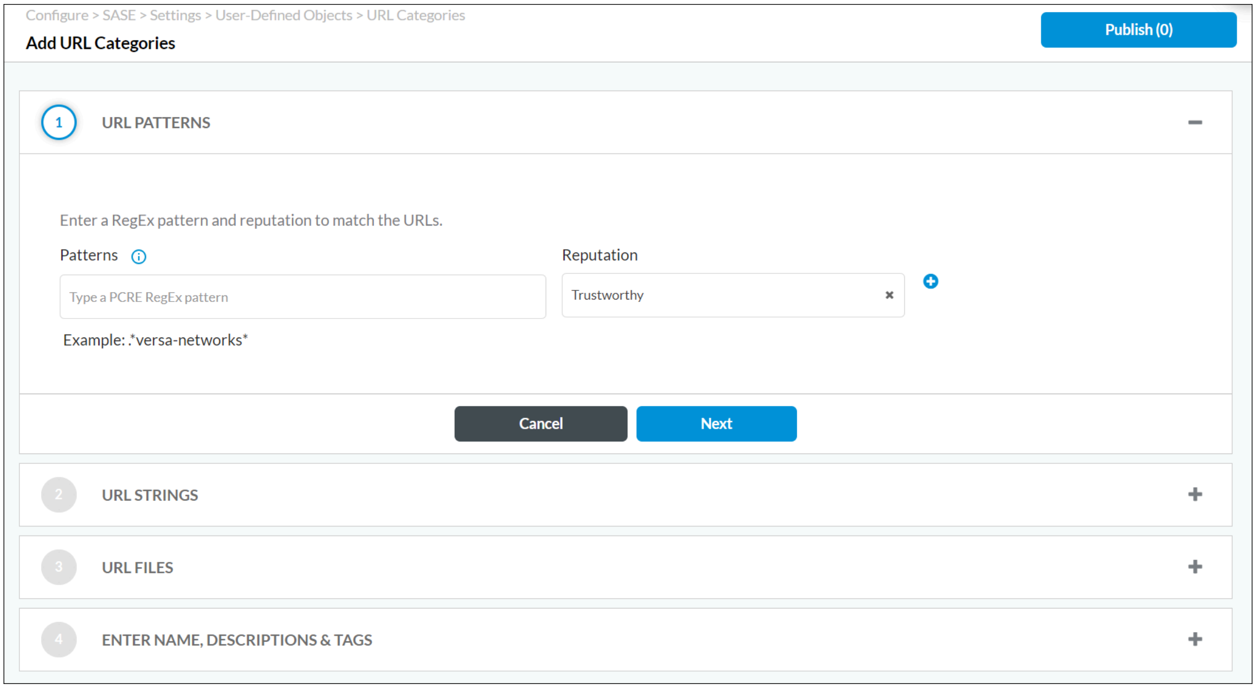
URL Categories

Below are all the URL Categories

URL Categories

		URL PATTERN		URL STRING	
□	NAME	PATTERN	REPUTATION	STRING	RE
		No Data			

2. Click the + Add URL Categories icon to add a new URL category. In the URL Patterns section, enter information for the following fields.



Configure > SASE > Settings > User-Defined Objects > URL Categories

Add URL Categories

1 URL PATTERNS

Enter a RegEx pattern and reputation to match the URLs.

Patterns: Type a PCRE RegEx pattern

Reputation: Trustworthy

Example: .*versa-networks*

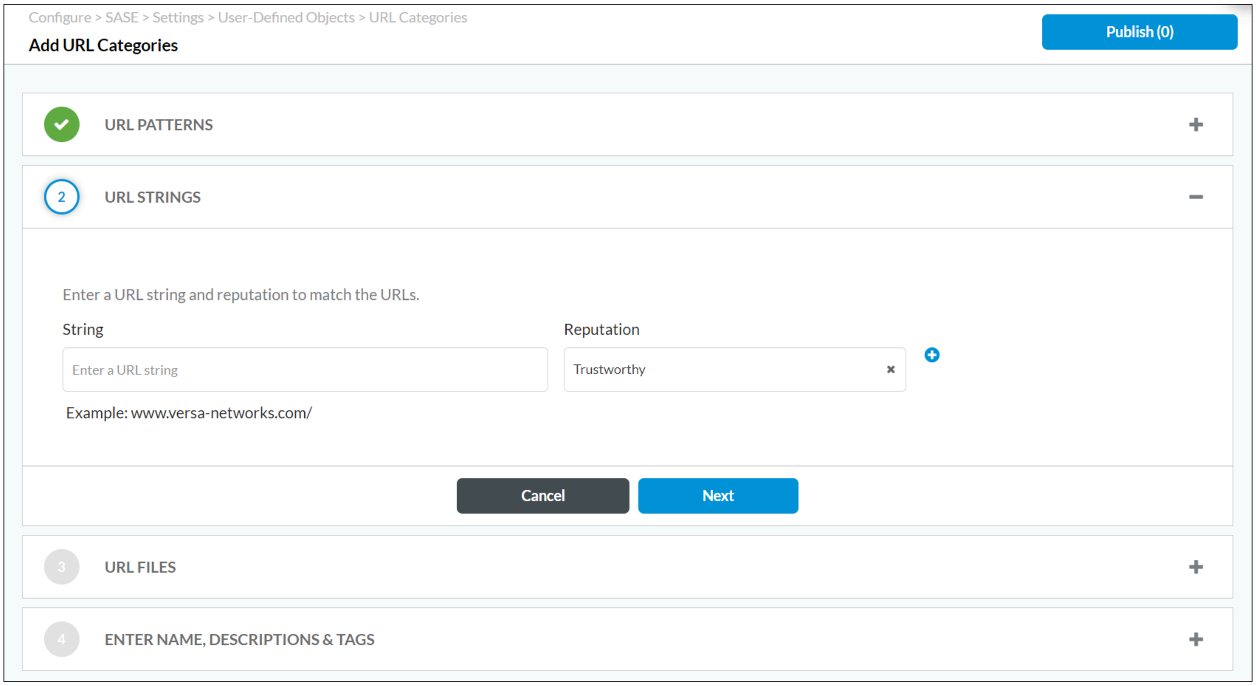
2 URL STRINGS

3 URL FILES

4 ENTER NAME, DESCRIPTIONS & TAGS

Field	Description
Patterns	Enter a URL pattern to match and group the URLs. You can include regex patte www.versa-networks.com, or you can use a wildcard such as *.versa-networks. escape it by preceding it with a backslash.
Reputation	Select a predefined reputation, and then assign it to the URL match pattern.

3. Click Next. In the URL Strings section, enter information for the following fields.


Configure > SASE > Settings > User-Defined Objects > URL Categories
Add URL Categories
Publish (0)
URL PATTERNS
2
URL STRINGS

Enter a URL string and reputation to match the URLs.

String: Enter a URL string

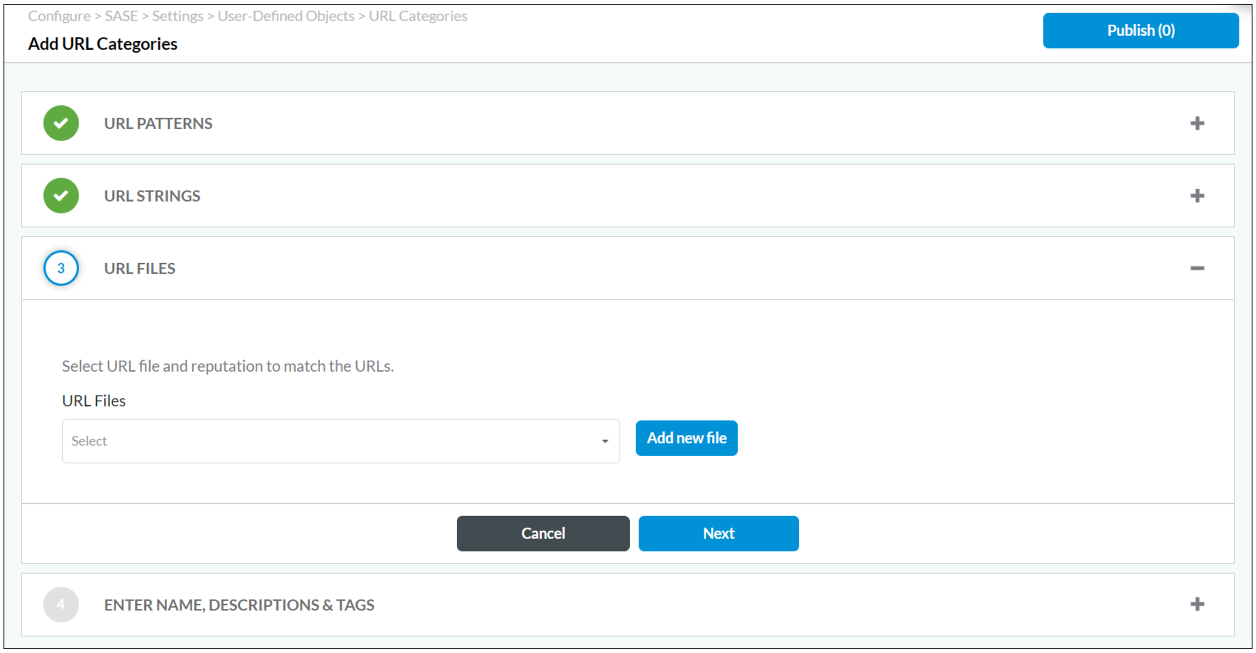
Reputation: Trustworthy

Example: www.versa-networks.com/

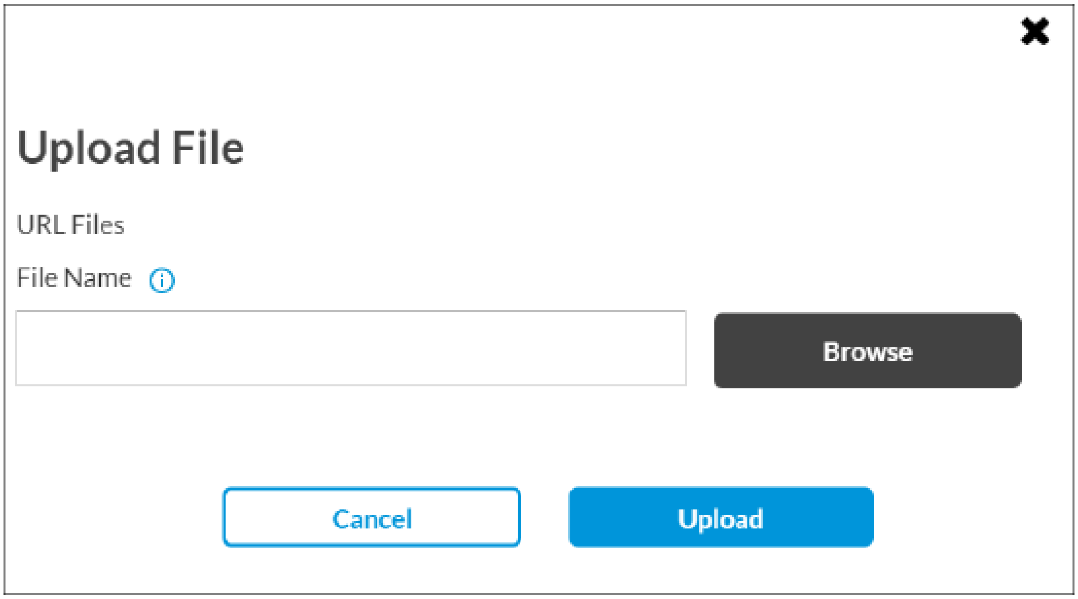
Cancel
Next
3
URL FILES
4
ENTER NAME, DESCRIPTIONS & TAGS

Field	Description
String	Enter a URL string that you want to group.
Reputation	Select a predefined reputation, and then assign it to the URL string.

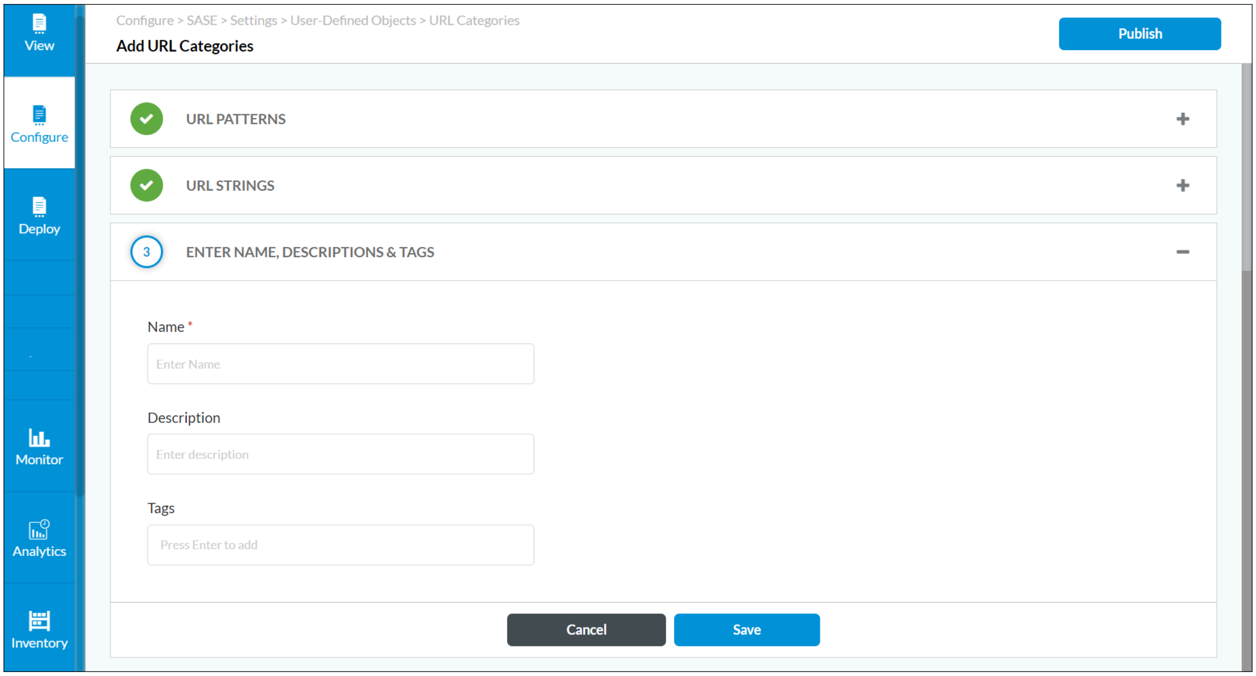
4. (For Releases 12.1.1 and later.) Click Next. In the URL Files section, select a URL file. To add a new URL file, click Add New File.


Configure > SASE > Settings > User-Defined Objects > URL Categories
Add URL Categories
Publish (0)
URL PATTERNS
URL STRINGS
3
URL FILES
Select URL file and reputation to match the URLs.
URL Files
Select
Add new file
Cancel
Next
4
ENTER NAME, DESCRIPTIONS & TAGS

In the Upload File popup window, click Browse, select a URL file to upload, and then click Upload. The file must be in CSV format. For more information, see Manage Files and Folders.



5. Click Next. In the Enter Name, Description, and Tags section, enter information for the following fields.



Configure > SASE > Settings > User-Defined Objects > URL Categories

Add URL Categories

URL PATTERNS

URL STRINGS

3 ENTER NAME, DESCRIPTIONS & TAGS

Name *

Enter Name

Description

Enter description

Tags

Press Enter to add

Field	Description
Name (Required)	Enter a name for the URL category. This name is displayed in the category in the match criteria for URL categories in policy rules.
Description	Enter a text description for the URL category.
Tags	Enter one or more tags for the URL category. A tag is an alphanumeric text that you use for searching URL categories.

6. Click Save.

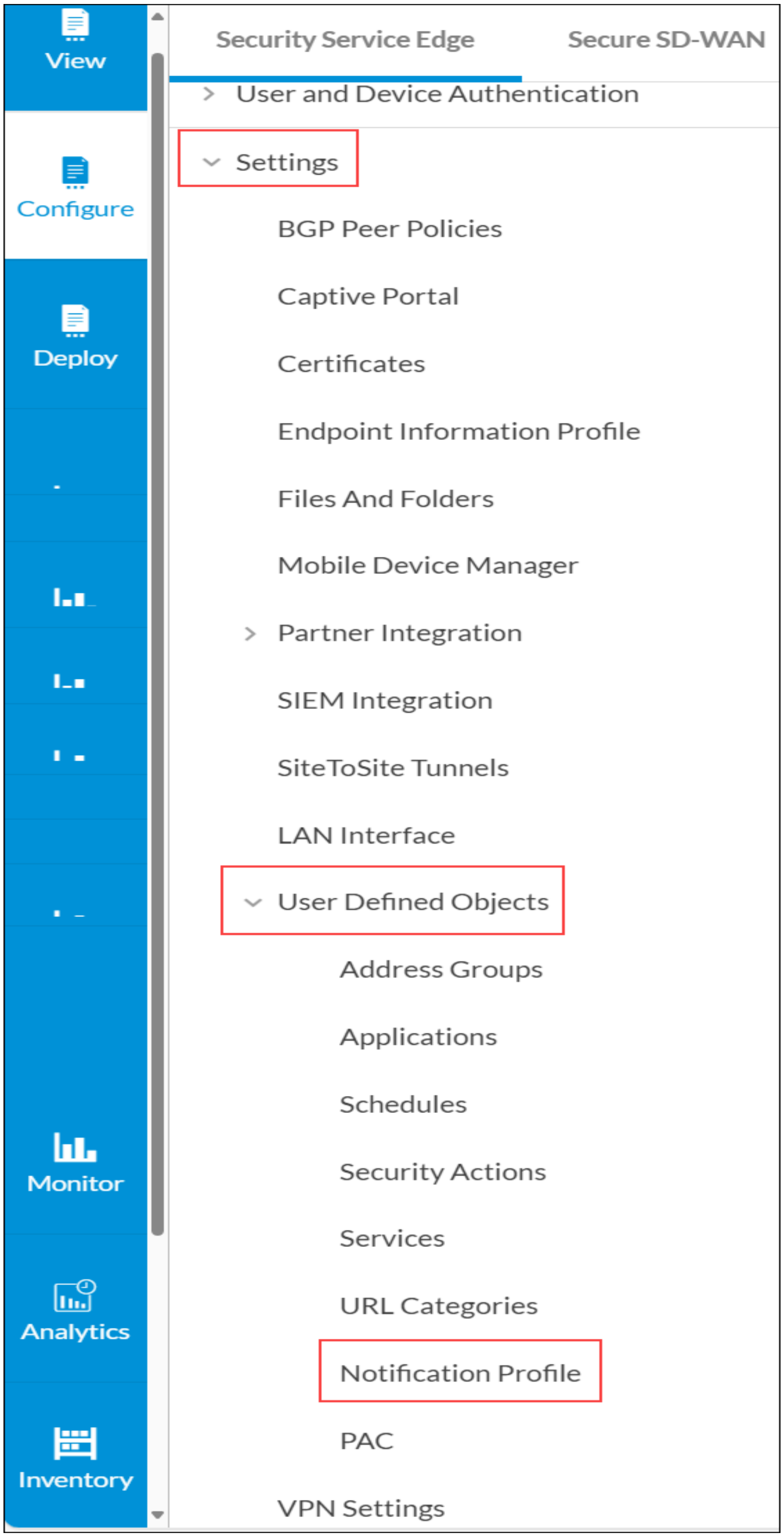
Configure Notification Profiles

For Releases 12.1.1 and later.

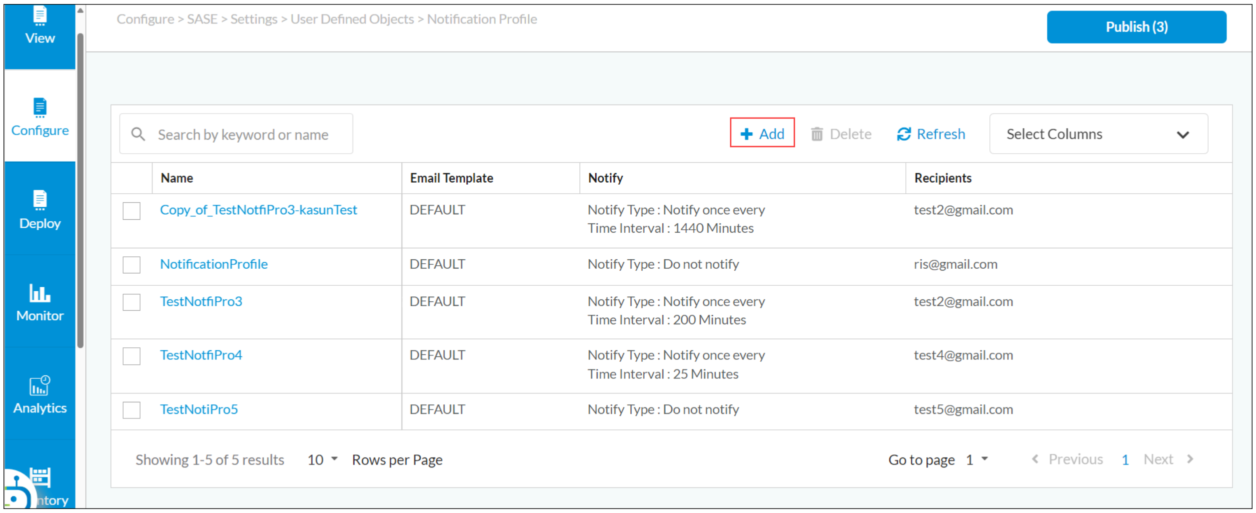
You can configure a notification profile to use to send email notifications at the system level and for individual tenants. You can then use the notification profile in advanced threat protection (ATP), CASB, and data loss prevention (DLP) profiles.

To configure a notification profile:

1. Go to Configure > Security Service Edge > Settings > User-Defined Objects > Notification Profile.



2. In the Notification Profile screen, select a notification profile. To add a new notification profile, Click + Add.

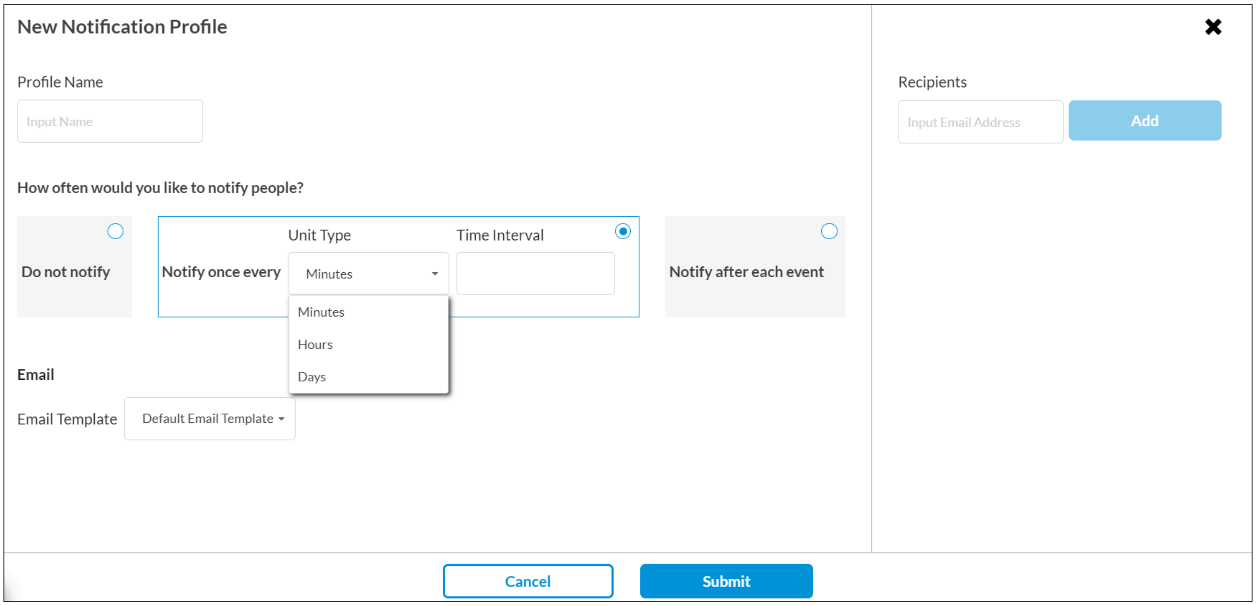


Configure > SASE > Settings > User Defined Objects > Notification Profile

	Name	Email Template	Notify	Recipients
□	Copy_of_TestNotfiPro3-kasunTest	DEFAULT	Notify Type : Notify once every Time Interval : 1440 Minutes	test2@gmail.com
□	NotificationProfile	DEFAULT	Notify Type : Do not notify	ris@gmail.com
□	TestNotfiPro3	DEFAULT	Notify Type : Notify once every Time Interval : 200 Minutes	test2@gmail.com
□	TestNotfiPro4	DEFAULT	Notify Type : Notify once every Time Interval : 25 Minutes	test4@gmail.com
□	TestNotiPro5	DEFAULT	Notify Type : Do not notify	test5@gmail.com

Showing 1-5 of 5 results 10 Rows per Page Go to page 1 Previous 1 Next

3. In the New Notification Profile popup window, enter information for the following fields.



New Notification Profile

Profile Name: Input Name

How often would you like to notify people?

○ Do not notify

● Notify once every — Unit Type: Minutes (Minutes, Hours, Days) — Time Interval:

○ Notify after each event

Email

Email Template: Default Email Template

Recipients: Input Email Address

Field	Description
Profile Name	Enter a notification profile name.
How often would you like to notify people?	Select how often to send the notification: ◦ Do not notify. ◦ Notify once every. Select the duration and time interval: ▪ Days ▪ Hours

Field	Description
	▪ Minutes ◦ Notify after each event.
Recipients	Enter the email address to receive notifications, and then click Add.
Email Template	Select the email template to use for notifications.

4. Click Submit.

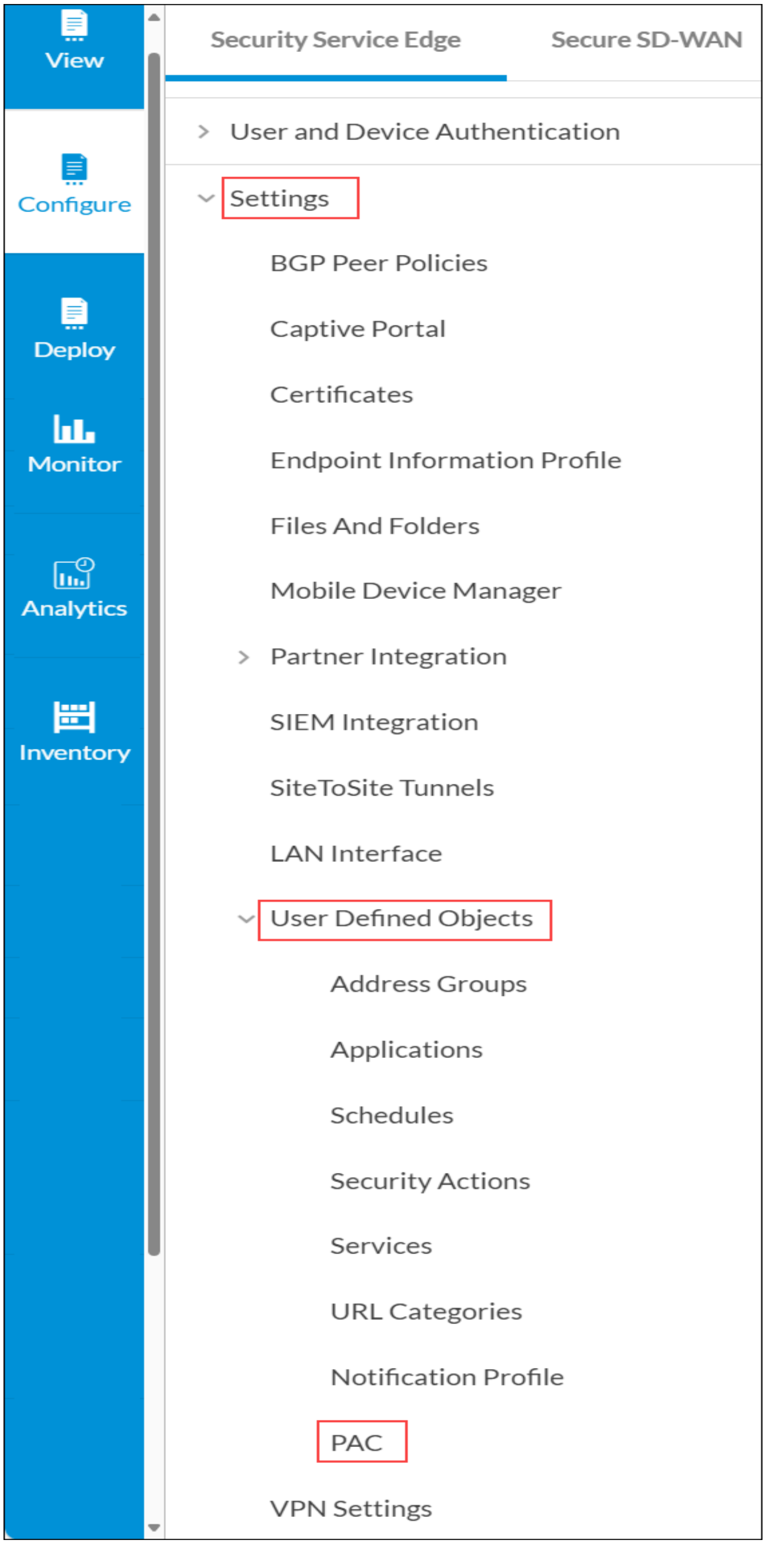
Upload PAC Files

For Releases 12.1.1 and later.

A proxy autoconfiguration (PAC) file defines how web browsers and other user agents can automatically choose the appropriate proxy server to fetch a given URL.

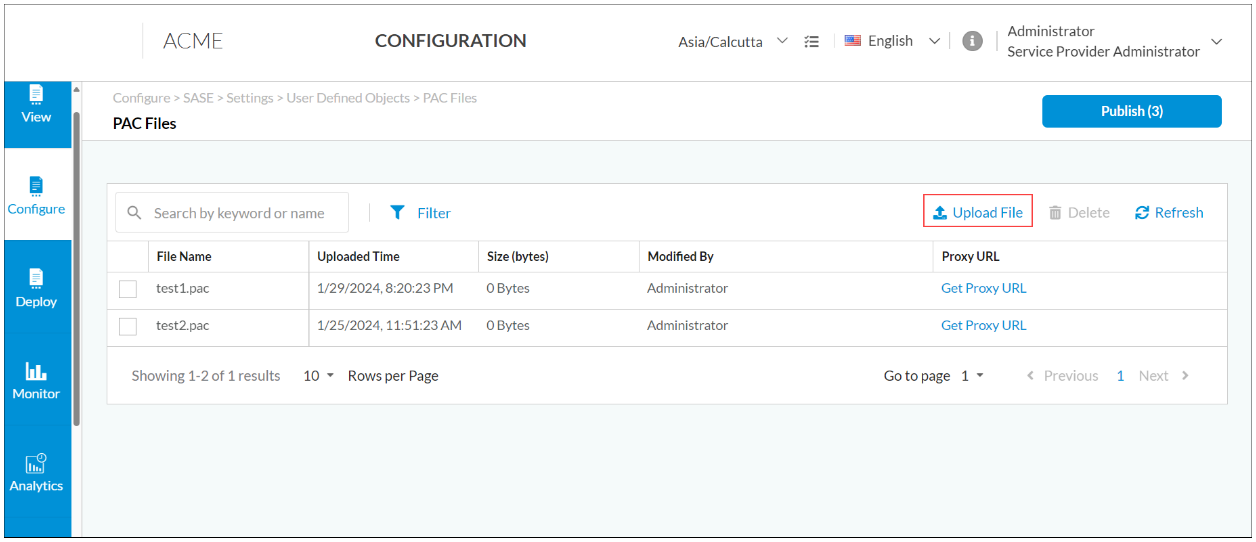
To upload a PAC file to a Concerto node:

1. Go to Configure > SSE > Settings > User-Defined Objects > PAC.



2. The PAC Files screen displays the PAC files that are already uploaded. To find a particular file, use the search box.

3. Click the ⬆ Upload File icon to upload the PAC file to the Concerto node.



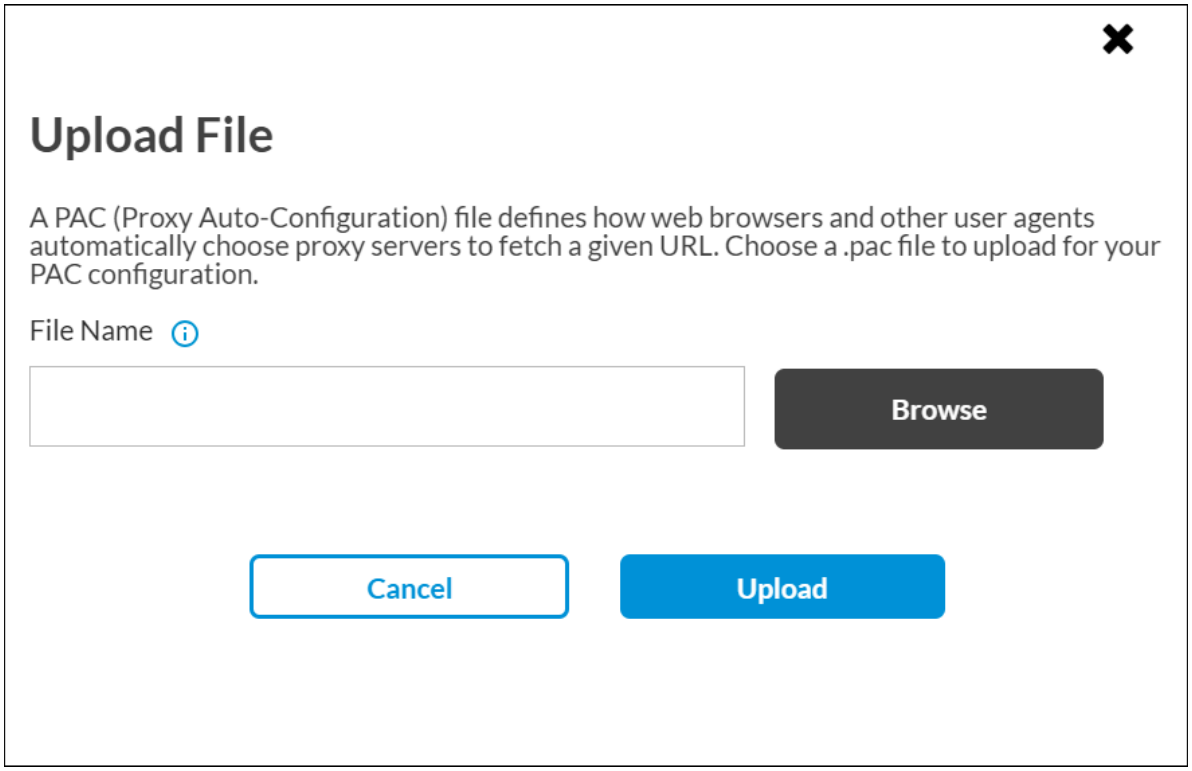
Configure > SASE > Settings > User Defined Objects > PAC Files

PAC Files

	File Name	Uploaded Time	Size (bytes)	Modified By	Proxy URL
□	test1.pac	1/29/2024, 8:20:23 PM	0 Bytes	Administrator	Get Proxy URL
□	test2.pac	1/25/2024, 11:51:23 AM	0 Bytes	Administrator	Get Proxy URL

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

4. Click Browse and choose a .pac file to upload for PAC configuration.

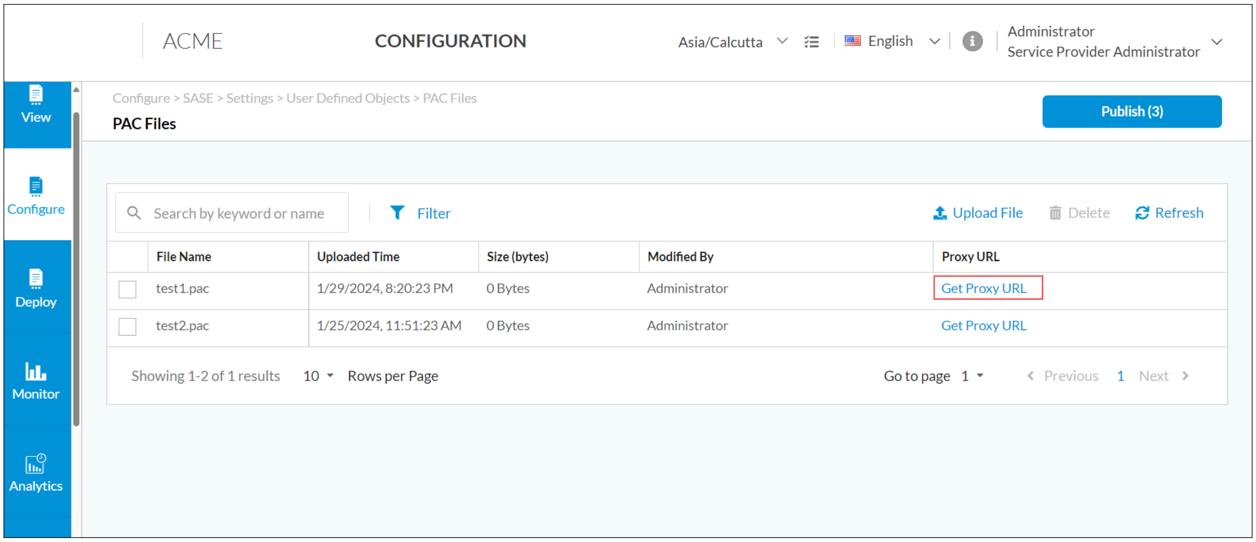


Upload File

A PAC (Proxy Auto-Configuration) file defines how web browsers and other user agents automatically choose proxy servers to fetch a given URL. Choose a .pac file to upload for your PAC configuration.

File Name

5. Click Upload. The PAC Files screen displays the uploaded PAC file.
6. Click the Get Proxy URL link for the PAC file to get the proxy URL for the proxy server.



PAC Files

	File Name	Uploaded Time	Size (bytes)	Modified By	Proxy URL
□	test1.pac	1/29/2024, 8:20:23 PM	0 Bytes	Administrator	Get Proxy URL
□	test2.pac	1/25/2024, 11:51:23 AM	0 Bytes	Administrator	Get Proxy URL

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

Associate Custom Security Actions and Custom URL Categories with Security Profiles

For Releases 11.4.1 and later.

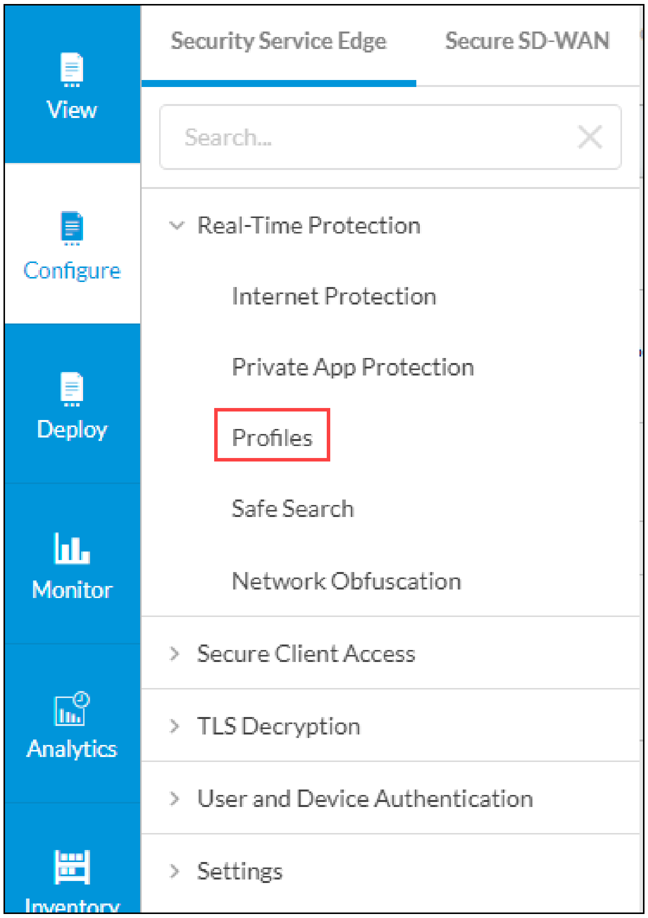
You can associate custom security actions and custom URL categories that you configure with the following security profiles:

- CASB
- Decryption
- DNS filtering
- IP filtering
- IPS
- IPS override
- URL filtering

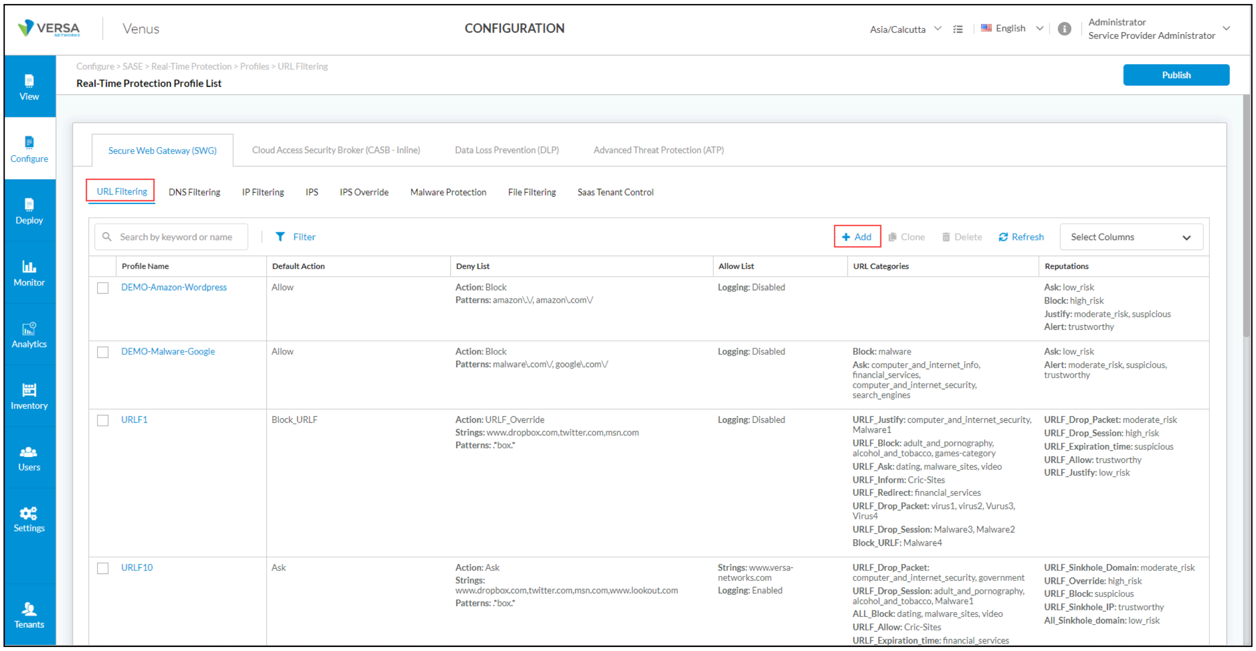
The following use case describes how to associate a custom security action and a URL category with the URL-filtering profiles. You can use the same method for other security profiles, and to associate the predefined security actions with the security profiles. For more information, see Configure Custom URL-Filtering Profiles.

To associate a security action with a URL-filtering profile:

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



The following screen displays:

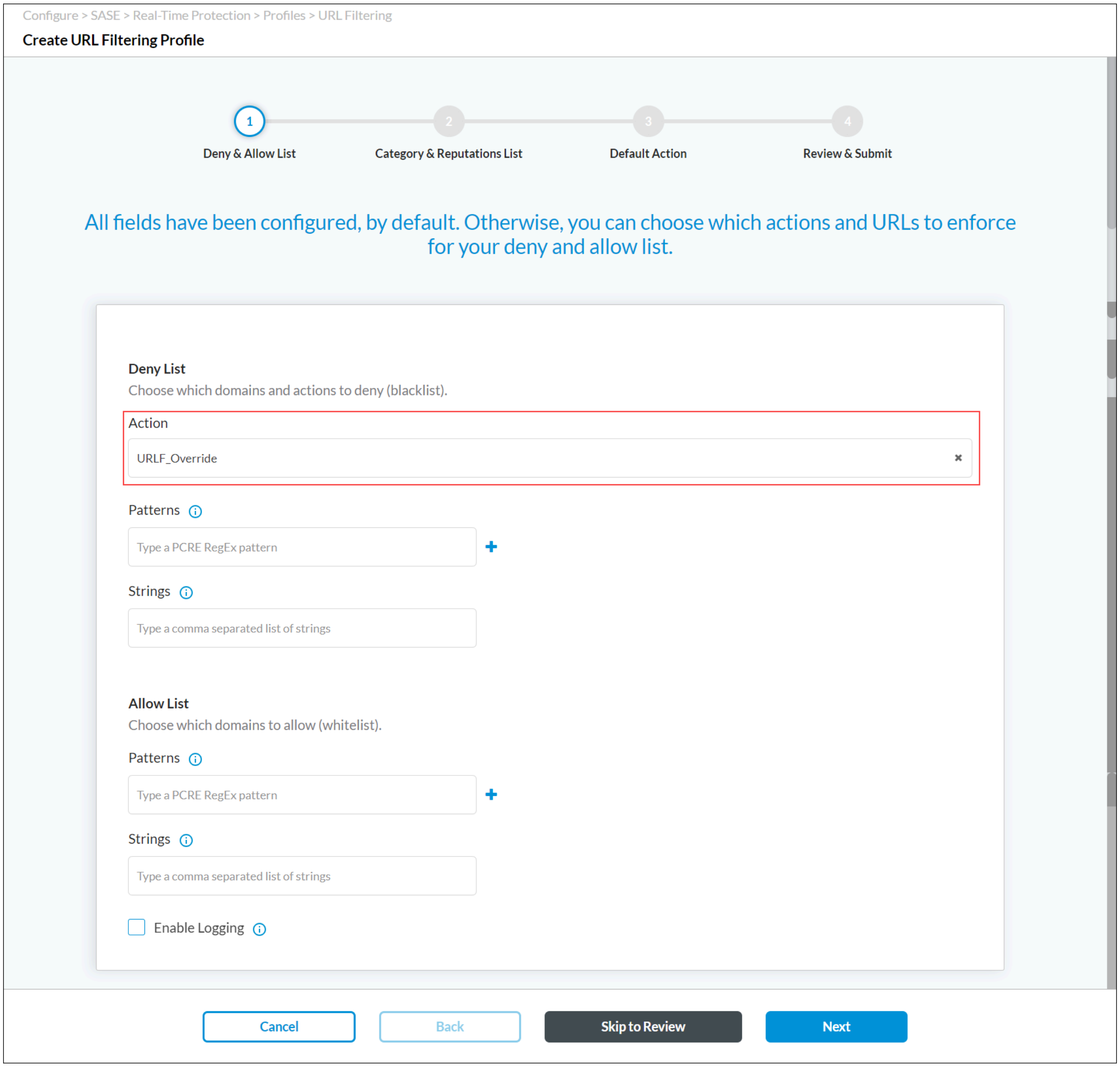


Configure > SASE > Real-Time Protection > Profiles > URL Filtering

Real-Time Protection Profile List

Profile Name	Default Action	Deny List	Allow List	URL Categories	Reputations
DEMO-Amazon-Wordpress	Allow	**Action:** Block **Patterns:** amazon\\.\/, amazon\.com\/	**Logging:** Disabled		**Ask:** low_risk **Block:** high_risk **Justify:** moderate_risk, suspicious **Alert:** trustworthy
DEMO-Malware-Google	Allow	**Action:** Block **Patterns:** malware\.com\/, google\.com\/	**Logging:** Disabled	**Block:** malware **Ask:** computer_and_internet_info, financial_services, computer_and_internet_security, search_engines	**Ask:** low_risk **Alert:** moderate_risk, suspicious, trustworthy
URLF1	Block_URLF	**Action:** URLF_Override **Strings:** www.dropbox.com,twitter.com,msn.com **Patterns:** .*box.*	**Logging:** Disabled	**URLF_Justify:** computer_and_internet_security, Malware1 **URLF_Block:** adult_and_pornography, alcohol_and_tobacco, games-category **URLF_Ask:** dating, malware_sites, video **URLF_Inform:** Cric-Sites **URLF_Redirect:** financial_services **URLF_Drop_Packet:** virus1, virus2, Vurus3, Virus4 **URLF_Drop_Session:** Malware3, Malware2 **Block_URLF:** Malware4	**URLF_Drop_Packet:** moderate_risk **URLF_Drop_Session:** high_risk **URLF_Expiration_time:** suspicious **URLF_Allow:** trustworthy **URLF_Justify:** low_risk
URLF10	Ask	**Action:** Ask **Strings:** www.dropbox.com,twitter.com,msn.com,www.lookout.com **Patterns:** .*box.*	**Strings:** www.versa-networks.com **Logging:** Enabled	**URLF_Drop_Packet:** computer_and_internet_security, government **URLF_Drop_Session:** adult_and_pornography, alcohol_and_tobacco, Malware1 **ALL_Block:** dating, malware_sites, video **URLF_Allow:** Cric-Sites **URLF_Expiration_time:** financial_services	**URLF_Sinkhole_Domain:** moderate_risk **URLF_Override:** high_risk **URLF_Block:** suspicious **URLF_Sinkhole_IP:** trustworthy **All_Sinkhole_domain:** low_risk

2. Click + Add to create a profile. The Create URL Filtering Profile screen displays.
3. In Step 1, Deny and Allow List, in the Action field, select the action to deny (blacklist).



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

Create URL Filtering Profile

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 domains and actions to deny (blacklist).

Action: URLF_Override

Patterns: Type a PCRE RegEx pattern

Strings: Type a comma separated list of strings

Allow List

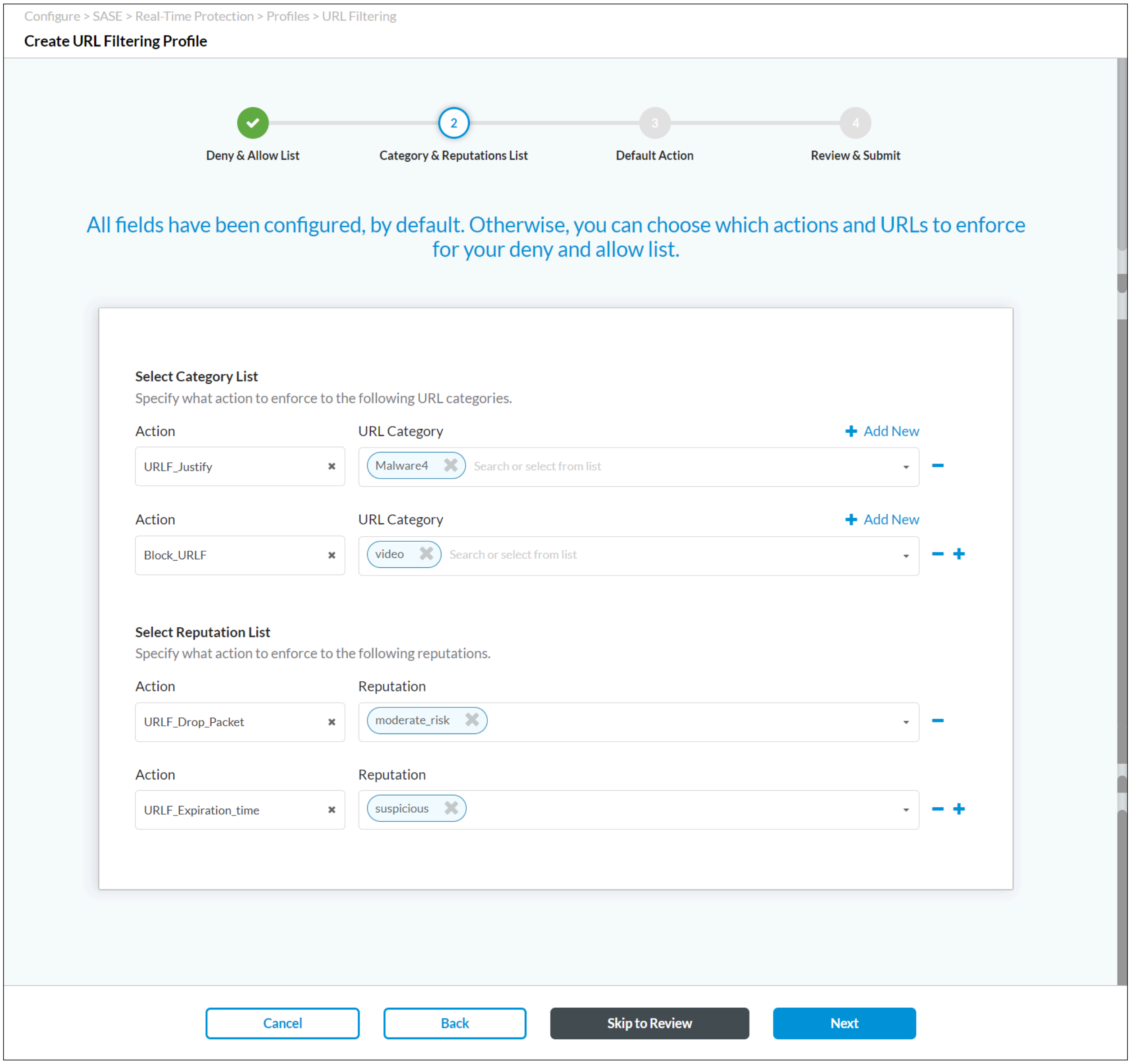
Choose which domains to allow (whitelist).

Patterns: Type a PCRE RegEx pattern

Strings: Type a comma separated list of strings

□ Enable Logging

4. Click Next to go to Step 2, Category and Reputations List, to specify an action, URL category, and reputation. If you specify both category and reputation lists, URLs must match both the category and the reputation. For category list, select a custom URL category or click the + Add New icon to add a new URL category. For more information, see Configure Custom URL Categories, above.



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

Create URL Filtering Profile

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.

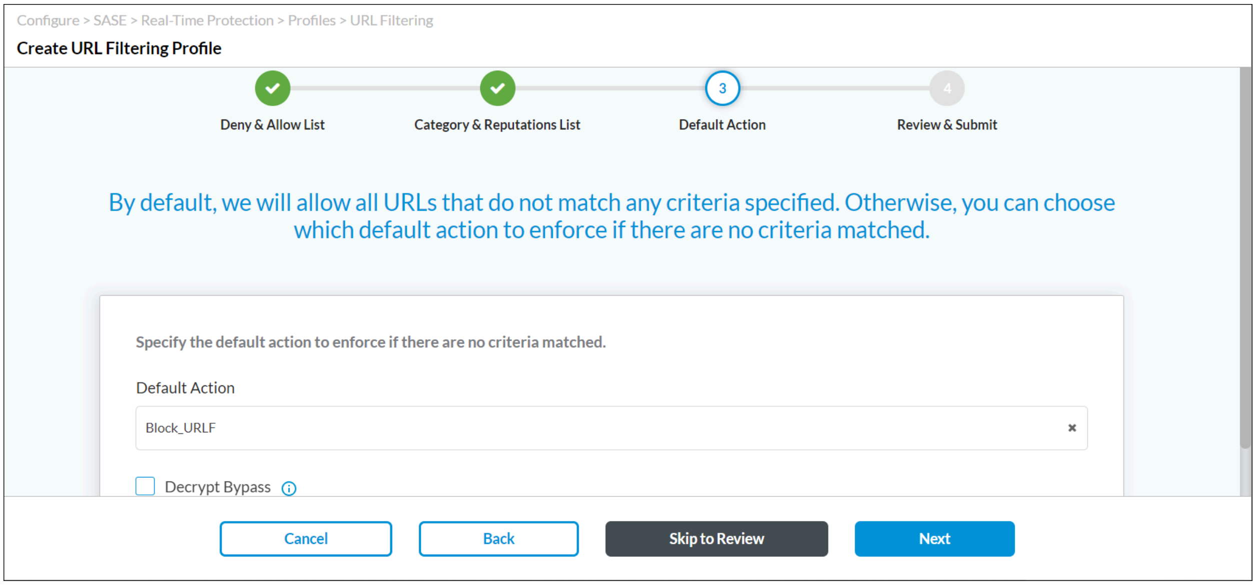
Action	URL Category
URLF_Justify	Malware4
Block_URLF	video

Select Reputation List

Specify what action to enforce to the following reputations.

Action	Reputation
URLF_Drop_Packet	moderate_risk
URLF_Expiration_time	suspicious

5. Click Next to go to Step 3, Default Action, and then select a default action. 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

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: Block_URLF

□ Decrypt Bypass

6. Click Next to go to the Review and Submit screen, and then click Save.

Supported Software Information

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

- Release 11.4.1 adds support for custom security actions and custom URL categories.
- Release 12.1.1 adds support for uploading PAC files, configuring a notification profile, and for uploading address group files and URL files.

Additional Information

Configure SASE Secure Client Access Rules
Configure SASE Site-to-Site Tunnels
Configure User and Device Authentication