Concerto SASE End-to-End Configuration

Secure Service Edge Overview and Architecture

The Versa Networks unified Secure Access Service Edge (SASE) solution is one of the most comprehensive SASE solutions available. It encompasses a wide range of functionalities and aligns to the Gartner definition of what a SASE offering should be.

The following figure illustrates the Versa SASE solution, which provides secure networking and SASE services to any user in any location, and access to applications running in private and public clouds. The Versa SASE solution is delivered by the Versa Operating System™ (VOS™) software, either on-premises or in the cloud.

The Versa unified SASE solution includes the following components:

- Cloud Access Service Broker (CASB)—A next-generation firewall service that provides:
  - Secure access to SaaS applications, such as Facebook, Salesforce, and Office 365
  - Application microsegmentation and shadow IT discovery and control
  - Access compliance
- Data Loss Prevention (DLP)—Secures sensitive corporate data and enforces relevant regulatory compliance.
- Firewall as a Service (FWaaS)—Safeguards users, devices, and applications (both on-premises and in the cloud) from internal and external threats.
- Unified Threat Management (UTM)—Protects against advanced threats, such as malware, spyware, trojans, worms, bots, and known vulnerabilities.
- Secure SD-WAN—Provides service level agreement (SLA)-aware connectivity between users and the SASE fabric.
- Secure Web Gateway (SWG)—A cloud delivered component that protects users from internet-based threats and enforces access control to the internet.
- Zero Trust Network Access (ZTNA)—A least-trust architecture that is based on identity access.

Versa SSE Components

Versa unified SASE has two key building blocks: Versa Secure Service Edge (SSE) and Versa Secure SD-WAN. Versa SSE consists of two components:

- Versa Secure Internet Access (VSIA) securely connects users through the Versa SASE fabric of Secure Web Gateways (SWGs) to public clouds, SaaS applications, and the internet.
- Versa Secure Private Access (VSPA) is the remote-access component that provides secure private access with ZTNA to resources within the enterprise. These resources could be located in on-premises data centers or in the public cloud.

Versa Secure Private Access

VSPA is a ZTNA solution that securely connects users to private applications by enforcing identity-based network access, regardless of location or hosting environment. Traditional VPN concentrators implement network-based access using methods such as static access lists to provide some security. However, these traditional methods are unable to differentiate between user contexts. ZTNA enables policies based on the user context. ZTNA not only enforces policy against the user traffic, it also determines the client behavior based on the user context.

VSPA integrates with your existing tools and applications, allowing direct, risk-minimized access using least-privilege control and continuous trust evaluation.

The VSPA component of Versa SSE comprises the following:

- Cloud gateways—The Versa Cloud Gateways (VCGs) form the Versa SASE fabric and process remote user traffic using an efficient single-pass architecture to deliver all the functions of the solution.
- SASE client for end-user devices—The SASE client extends the Versa SASE fabric to the end-user appliance, enabling SD-WAN-like, context-aware connectivity that is centered around user experience. Versa SASE clients are available on Windows, MacOS, iOS, Android, Chromebook, and Linux platforms. Clientless connectivity is also supported in VSPA.
- SD-WAN enabled—As part of the SD-WAN overlay, the VCGs deliver branch and data center connectivity with the following benefits:
  - Provides SLA-aware traffic engineering between the data center and the VCGs to optimize user experience.
  - Enables automatic discovery of the gateways and branches without the need to create and manage manual IPsec tunnels.
- Self-management portal—The single-pane-of-glass management orchestrator that allows enterprise administrators to manage and control their users and applications. It presents a unified interface for policy management between remote users and branch offices.

VSPA provides a three-stage protection for enterprises:

- Stage 1: SASE client registration—At first use, the client must be registered to the SASE portal. This is necessary for two reasons:
  - Client authentication ensures that only authorized users can connect to the enterprise. The authentication process itself is robust, supporting LDAP, single-sign on (SSO), and the Versa Directory of local users. The client-authentication process also supports multifactor authentication (MFA) using a time-based one-time password (TOTP) or email.
  - Client policy—The client policy step locates and downloads the SASE client's configuration from the SASE

portal. The registration process is now complete.

- Stage 2: Connection—This stage determines the type of connectivity required and the behavior of the client based on the context. Features of this stage include fail close/fail open, best gateway selection, gateway-to-client policy (such as encryption levels and EIP policy), and client-always-on functionality to ensure that the VPN is always established without user intervention. In addition, the trusted network detection feature allows the client to determine if the user is on a public network, such as a café WIFI, or in a secure corporate office location.
- Stage 3: Policy enforcement—This final stage enforces corporate policy on user traffic, ZTNA, and other SWG features, such as URL filtering, file filtering, DNS filtering, IP filtering, antivirus, and vulnerability prevention systems. The security and integrity of corporate data is maintained using features such as DLP.

Versa SSE maintains traffic segmentation across each component from the SASE client to the cloud gateways. On the end user device, the SASE client helps differentiate between business-critical applications which must be specifically secured, such as Office 365 traffic, from domestic or casual internet traffic, such as social media or news sites. You can enforce this separation at the application level on the device, at the FQDN level, or at the network level using network prefixes. This separation persists in the cloud gateway, where the different traffic segments can receive different network and security treatment. For example, you can use Network Address Translation (NAT) or a proxy for internet-bound traffic, along with some unified threat management (UTM), while you can simply route private-application traffic with some application filtering.

Versa CSGs can provide network obfuscation to conceal end users and applications, keeping threat actors from enterprise resource knowledge and protecting against attack vectors such as lateral movement and port scanning. Versa's network obfuscation capabilities use a suite of technologies, such as DNS proxy, CGNAT, tunneling protocol, ZTNA, and NGFW to improve upon standard network obfuscation protection.

Versa Secure Internet Access

VCGs are unique in the industry as they offer both network services and security services. They function as an extension of the customer enterprise network, allowing enterprise administrators to perform important networking functions in the cloud. These functions include the following:

- Best gateway selection
- Per-tenant trusted network detection
- Routing protocol support
- Secure connectivity toward users, offices, and private applications
- SLA-based traffic steering

Similarly, VSGs perform security functions using secure web gateway (SWG) capabilities, which include authentication, user and group policy, NGFW functions (such as URL filtering, IP filtering, file filtering, and application filtering), and unified threat management (UTM). The SWG also functions as part of a wider security ecosystem from Versa Networks that delivers capabilities such as SSL decryption, and inline CASB and DLP.

VSIA provides the following features:

- Traffic identification and policy-based filtering—VCGs can identify traffic based on network location, SASE client

version, predefined and user-defined applications, users, and user groups. You can define and apply specific filters and actions at a granular level to ensure the scalability of your security posture.

- CASB—A critical security service that helps an enterprise set policy, monitor behavior, and manage risks, ensuring safe usage of cloud applications and services to prevent accidental data leakage. CASB can sit between the end user and the cloud, allowing visibility and control by shadow IT discovery, firewall log ingestion, data security, threat protection, and compliance management.

- DLP—A cybersecurity solution used to prevent the leakage of sensitive information through the network. An effective DLP solution monitors, detects, and potentially blocks the exfiltration of sensitive data while the data is in motion across the network using various protocols or when it is residing in popular cloud repositories.

Versa SASE Client

Versa SASE client brings SD-WAN-type connectivity to the end host, is simple to use, and can be configured centrally by the administrator. The SASE client features include:

- Best gateway selection based on the load on the gateway
- Device posture check and compliance checks
- Digitial Experience Management (DEM) for end devices
- Intelligent local breakout to the internet
- Location-aware policy
- Multitenancy support
- Network authentication tool for end devices
- Traffic steering based on the application or FQDN
- User identification

The SASE client is available on the following platforms:

- Android, including Chromebook
- iOS
- Linux
- MacOS
- Windows

The process for registering the SASE client and establishing a connection consists of the following steps:

1. You receive an automated email with important information, such as the FQDN of the portal and links to download and install the client.
2. When installation is complete, follow the email instructions to register the client. Additional authentication steps, such as time-based one-time password (TOTP) or email-based one-time password (OTP), can be used to further validate the user.
3. A portal policy is chosen based on match criteria, such as user location or device posture.
4. Once a portal policy match is found, the SASE client configuration is downloaded and applied to the SASE client. The registration process is complete.
5. The SASE client now has the configuration necessary to establish a connection to its gateway. At this point, a best-gateway selection is made based on the reported load from the gateways and the user's proximity to the gateway.
6. The gateway-client policy is then matched for the user traffic. Gateway policies can enforce specific authentication, MFA, or EIP profile.
7. An IPsec tunnel is established.
8. User traffic can then pass over the tunnel and may be further processed by the security modules.

Management Portal

The Concerto SSE management portal is a single pane of glass for provisioning, fault and performance monitoring, and visibility of the SASE fabric. The portal can manage both the SSE and SD-WAN components, allowing the administrator to easily configure end-to-end policies across those elements. You can view historical performance data through the portal, including statistics around traffic types, hits on rules, threats, and other important information. You can also view and query the security logs.

The management portal includes the following features:

- Unified policy language—Versa Concerto provides a unified policy language in which all components are presented in a consistent manner. For example, you configure policies with match criteria as well as the action to be taken when a match is found. A single policy can apply to multiple network segments with support for zones within each rule, providing flexibility to administrators. You can define multiple rules in each module, with rules processed from top to bottom. A wizard-style policy configuration tool guides users through the process in an intuitive manner.
- Policy enforcement—Once you define the match criteria, you can select various actions to enforce the policy depending on the module. Policy can be enforced with a simple action such as allow or deny, or with a more advanced action called from another profile object. For example, you can use a URL filtering profile as the enforcement action. Versa SSE includes a large list of predefined profiles for the most common use cases, and also supports user-defined profiles.
- Review and deploy—Provides a one-page view of the entire policy configuration. You specify a name for the policy, and then review the details of the entire policy at a glance. You can edit individual policy sections as needed. You can also disable a configured policy without deleting the policy. Once you are done, you save the policy.
- Publishing—Saved configurations are not automatically applied. You must publish the configuration to the gateways for it to take effect. You can choose to apply a configuration to some or all of the gateways, and you can publish a configuration to multiple gateways concurrently. The status column displays the progress of this operation for each gateway. You can publish a configuration at any time. A task log provides an audit and status trail of all

changes.

Configuration Overview

To configure and activate a new SASE tenant, you perform the following steps:

1. Configure authentication
2. Configure site-to-site tunnels
3. Configure Versa Secure Access (VSA) client access policies
4. Configure the Versa SASE client
5. Configure TLS decryption
6. Configure SASE internet protection rules
7. Configure real-time protection
8. Configure advanced internet protection:
    a. CASB
    b. DLP
    c. ATP
9. Use Versa Analytics

The following sections describe each of the steps and provide links to articles that provide more detail.

Configure Authentication

User authentication is a critical component of the SASE framework, as it implements Zero Trust Network Access (ZTNA) principles. ZTNA provides micro-segmentation, multi-factor authentication, per-application authorization, and network and user visibility. Remote users can be authenticated using a local database. Versa SASE also supports LDAP, SAML, and RADIUS for user and group authentication.

LDAP is a client-server protocol that enables a network device to access an LDAP server, which provides directory services that store descriptive attribute-based information. When an end user sends a request to access a webpage, the VOS device accesses the LDAP server to validate the user. Based on the authentication result, the user is either authentication or their authentication request is denied. You can configure either a user-based or group-based policy to allow or deny traffic.

SAML authenticates users to access multiple services and applications. SAML is useful when you want to access multiple services or applications and have to authenticate for each service or application, for example, Google and its related services. SAML is a common standard for exchanging authentication between parties, most commonly used for web browser-based single sign-on (SSO).

With Versa Directory authentication, you upload lists of users and groups for authentication purposes. You can also add individual users and groups using the GUI.

To configure authentication, you do the following:

1. Configure User and Device Authentication Profiles—User and group profiles specify the authentication type for user authentication. These profiles are used in user and device authentication rules, to specify the method to authenticate users who match the authentication rule criteria.
2. Configure User and Device Authentication Rules—You can define rules for user and device authentication based on match criteria for destination zones, IP addresses, SASE services, and schedules. User authentication rules are used when there is no SASE client that provides user identity information to the SSE service. When user authentication rules are configured, and the user traffic matches the rule criteria, the user is directed to a captive portal is presented and asked to provide its credentials. Once the user successfully authenticates, the policy can enforce the rules specific to that user.

Configure User and Device Authentication Profiles

To specify the authentication type for user authentication, you configure user and device authentication profiles. For each enterprise, you can configure profiles for Lightweight Directory Access Protocol (LDAP), RADIUS, Security Assertion Markup Language (SAML), and Versa Directory. For Releases 12.1.1 and later, you can also configure user and device certificate-based profiles. You can configure both an LDAP and a SAML profile for an enterprise, but for RADIUS and Versa Directory profiles types, you can configure only one per enterprise. You can configure user and device certificate-based profiles with each other, or with LDAP or SAML authentication profiles.

LDAP is a client–server protocol that allows a network device to access an LDAP server, which provides directory services that store descriptive attribute-based information. When an end user sends a request to access a webpage, the Versa Operating System™ (VOS™) device accesses the LDAP server to validate the user. Based on the authentication result, the user is either authenticated or their authentication request is denied. You can configure either a user-based or group-based policy to allow or deny traffic.

RADIUS is a distributed client–server system that secures networks against unauthorized access. A RADIUS server provides an external database that you can use to authenticate users before allowing them to access a network, a device, or related services.

SAML authenticates users so that they can access multiple services and applications. SAML is useful when you want to access multiple services or applications and have authentication for each service or application, for example, Google and its related services. SAML is a common standard for exchanging authentication between parties and is most commonly used for web browser-based single sign-on (SSO).

With Versa directory authentication, you upload lists of users and groups for authentication purposes. You can also add individual users and groups using the GUI.

Certificate-based authentication is a secure method to validate the identity of users and devices. For Releases 12.1.1 and later, Versa SASE supports user and device certificate-based authentication. When you enable certificate-based authentication, the gateway initiates a request to the SASE client for users to provide their certificates during client portal registration and gateway connection.

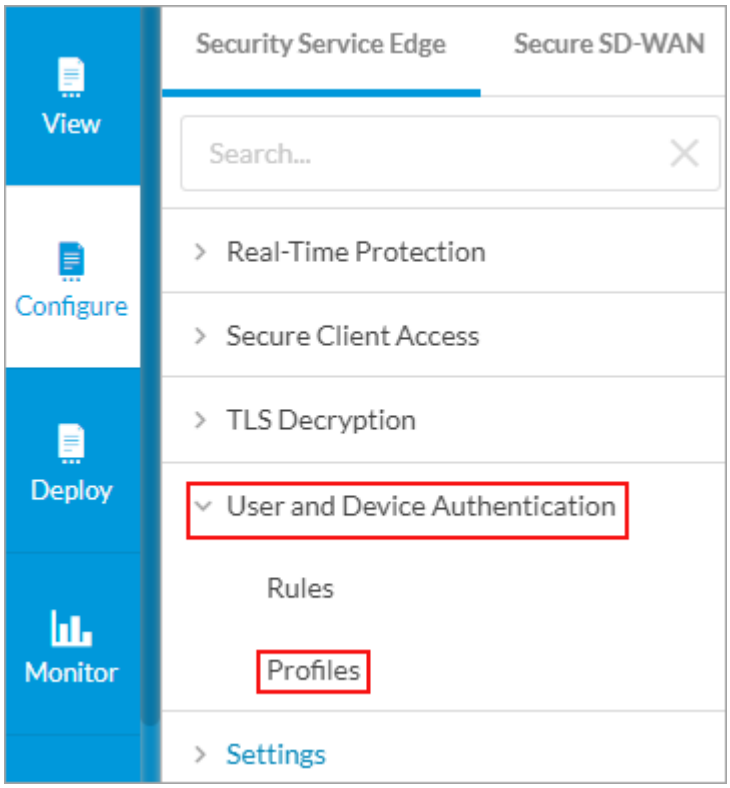
Note: You must configure the following SASE rules, profiles, and settings in a specific order:

1. Configure users and groups, and them publish them to the gateway, as described in this article.
2. Configure site-to-site tunnels. For more information, see Configure SASE Site-to-Site Tunnels.
3. Configure secure client access profiles and rules. For more information, see Configure SASE Secure Client Access Rules.

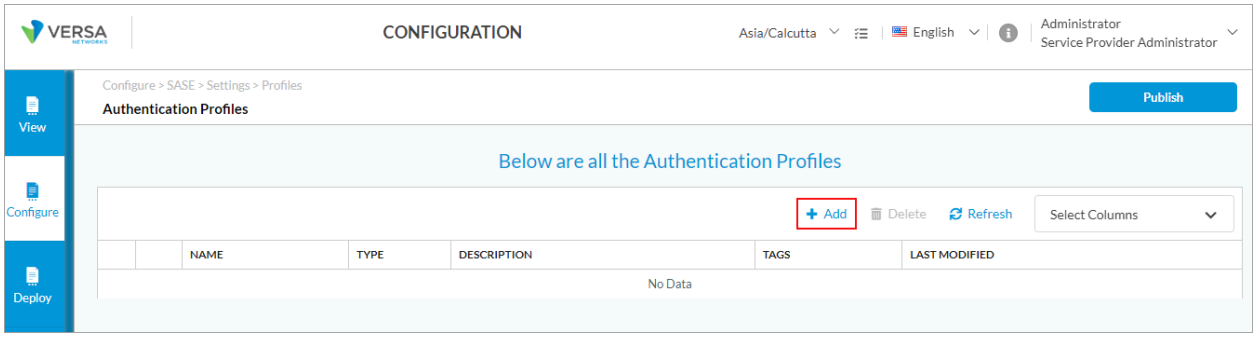
You do not need to configure the remaining SASE rules, profiles, and settings in a specific order.

To configure user and device authentication profiles:

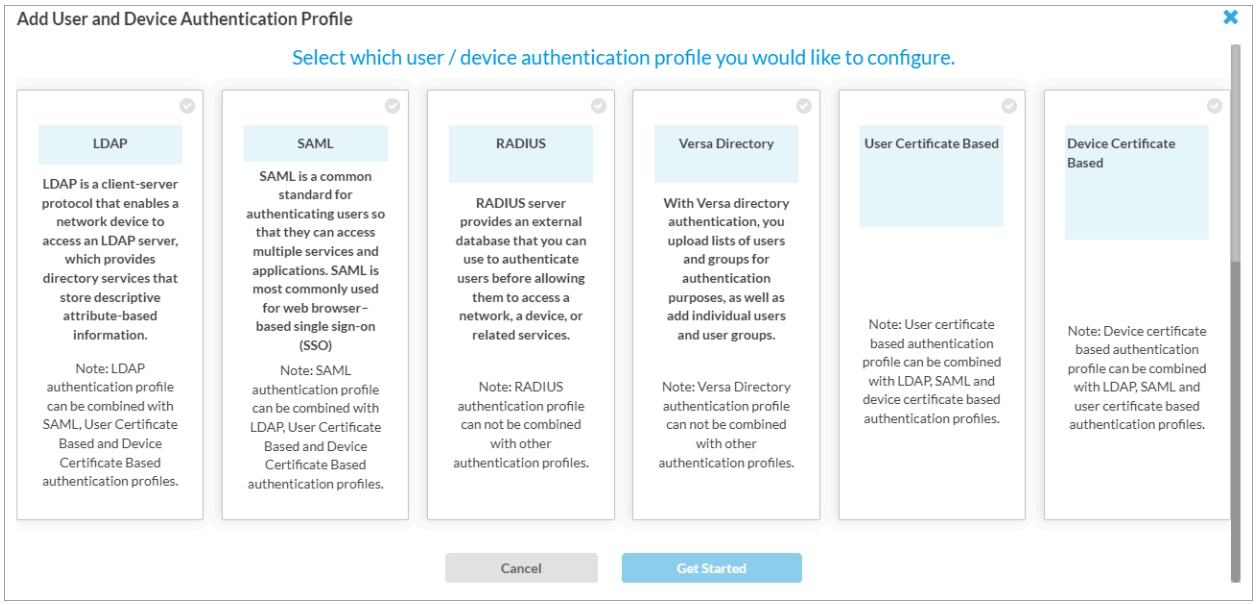
1. Go to Configure > Security Service Edge > User and Device Authentication > Profiles.



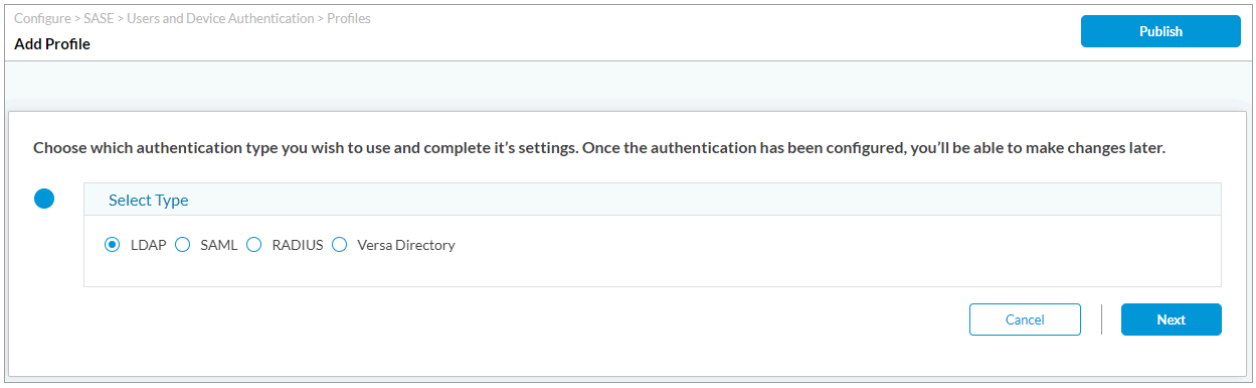
The Authentication Profiles screen displays.



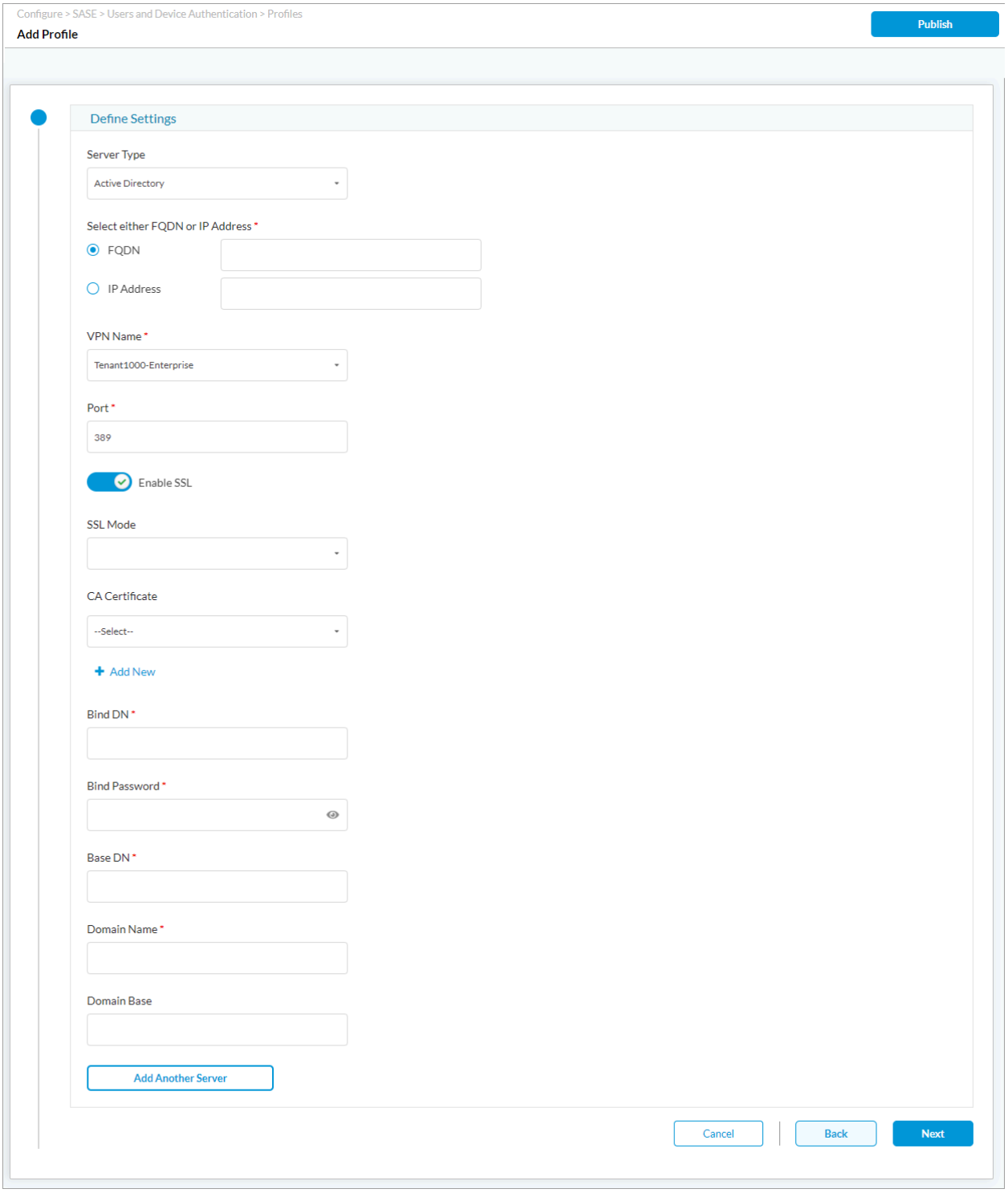
2. To create a new profile, click + Add.
   - For Releases 12.1.1 and later, the Add User and Device Authentication Profile screen displays.



- For Releases 11.4.1 and earlier, the Add Profile screen displays.

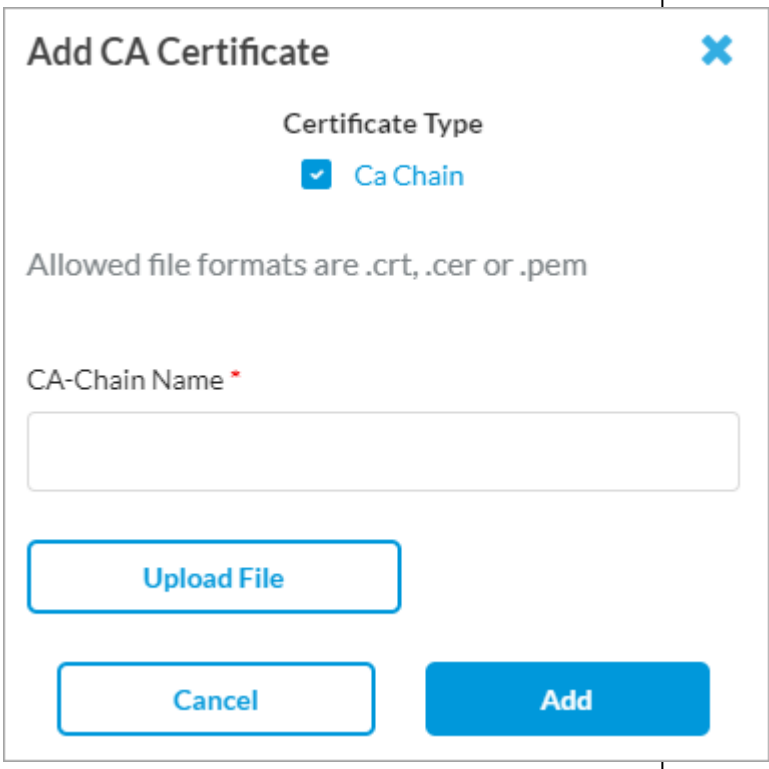


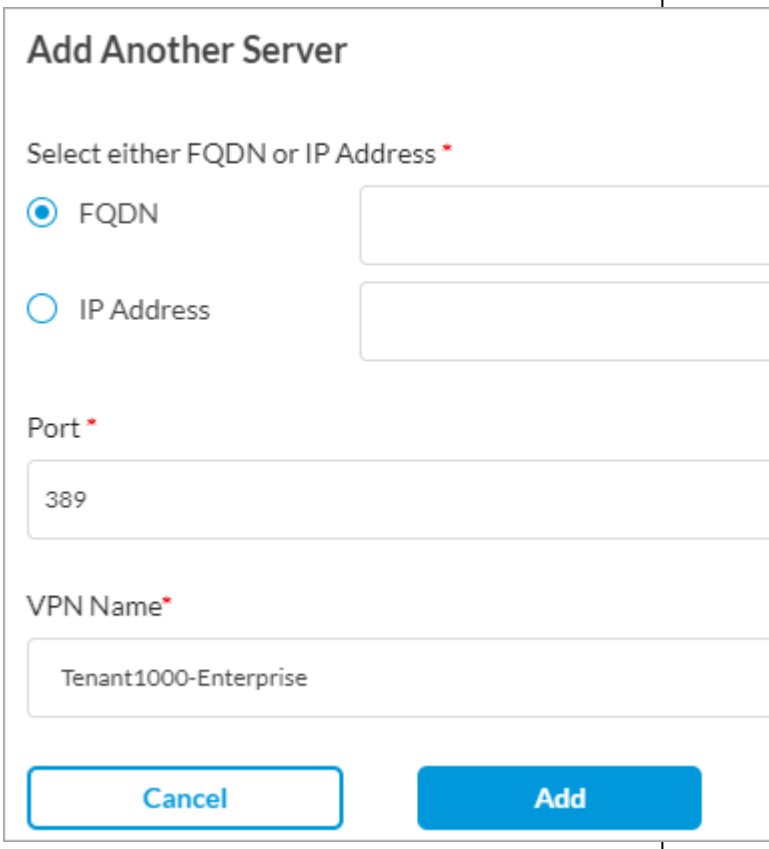
3. Select the type of authentication to configure:
   - (For Releases 12.1.1 and later.) Select one of the following options: Device Certificate Based, LDAP, RADIUS, SAML, User Certificate Based, or Versa Directory.
   - (For Releases 11.4.1 and earlier.) In the Select Type field, click one of the following options: LDAP, RADIUS, SAML, or Versa Directory.
4. Click Next (or Get Started for Releases 12.1.1 and later).
5. For the LDAP authentication type, the following screen displays. Enter information for the following fields.



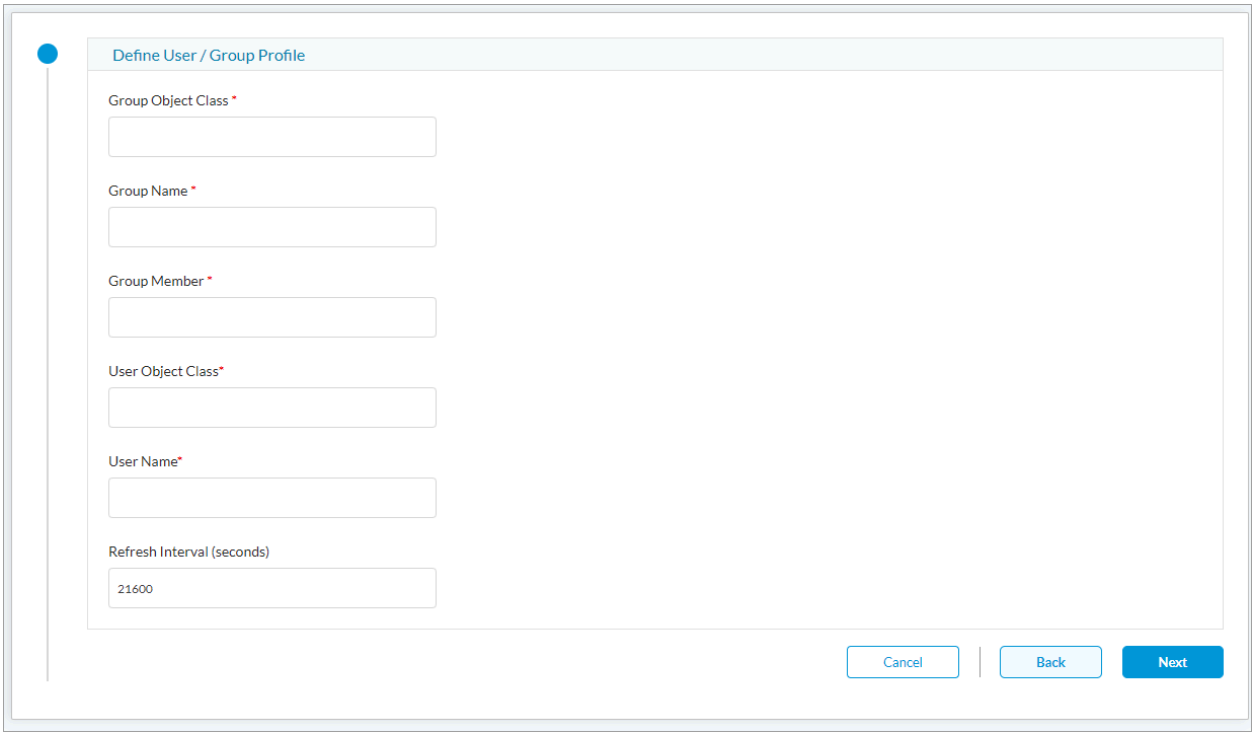
Field	Description
Server Type	Select the server type:

Field	Description
	◦ Active Directory ◦ Open LDAP
Select Either FQDN or IP Address	Click FQDN or IP Address, and then enter the FQDN or IP address of the Active Directory or LDAP server.
VPN Name	Select the name of the tenant VPN to use to reach the LDAP server.
Port	Enter the listening port number on the LDAP server, which allows you to communicate with the LDAP directory service. *Range*: 0 through 65535 *Default*: None
Enable SSL	Click the slider to enable SSL for the LDAP session.  Click the slider again to disable SSL for the LDAP session. 
SSL Mode	If you enable SSL, select the SSL mode for the LDAP session: ◦ LDAPS—Use secure LDAP (LDAP over SSL) ◦ STARTTLS—Use LDAP over TLS
CA Certificate	If you enable SSL, select the CA certificate to use for the secure LDAP connection. To add a new CA

Field	Description
	certificate, click + Add New, and the enter the required information. 
Bind DN	Enter the bind distinguished name (DN) to use when logging in to the LDAP server.
Bind Password	Enter the password that the bind DN uses when logging in to the LDAP server.
Base DN	Enter the base distinguished name DN to use when an LDAP client initiates a search.
Domain Name	Enter the domain name to use for LDAP searches, for example, versa-networks.com.
Domain Base	Enter the name of the base domain.
Add Another Server	Click to add another server of the same type. In the Add Another Server popup window, enter the required information, and then click Add.

Field	Description
	

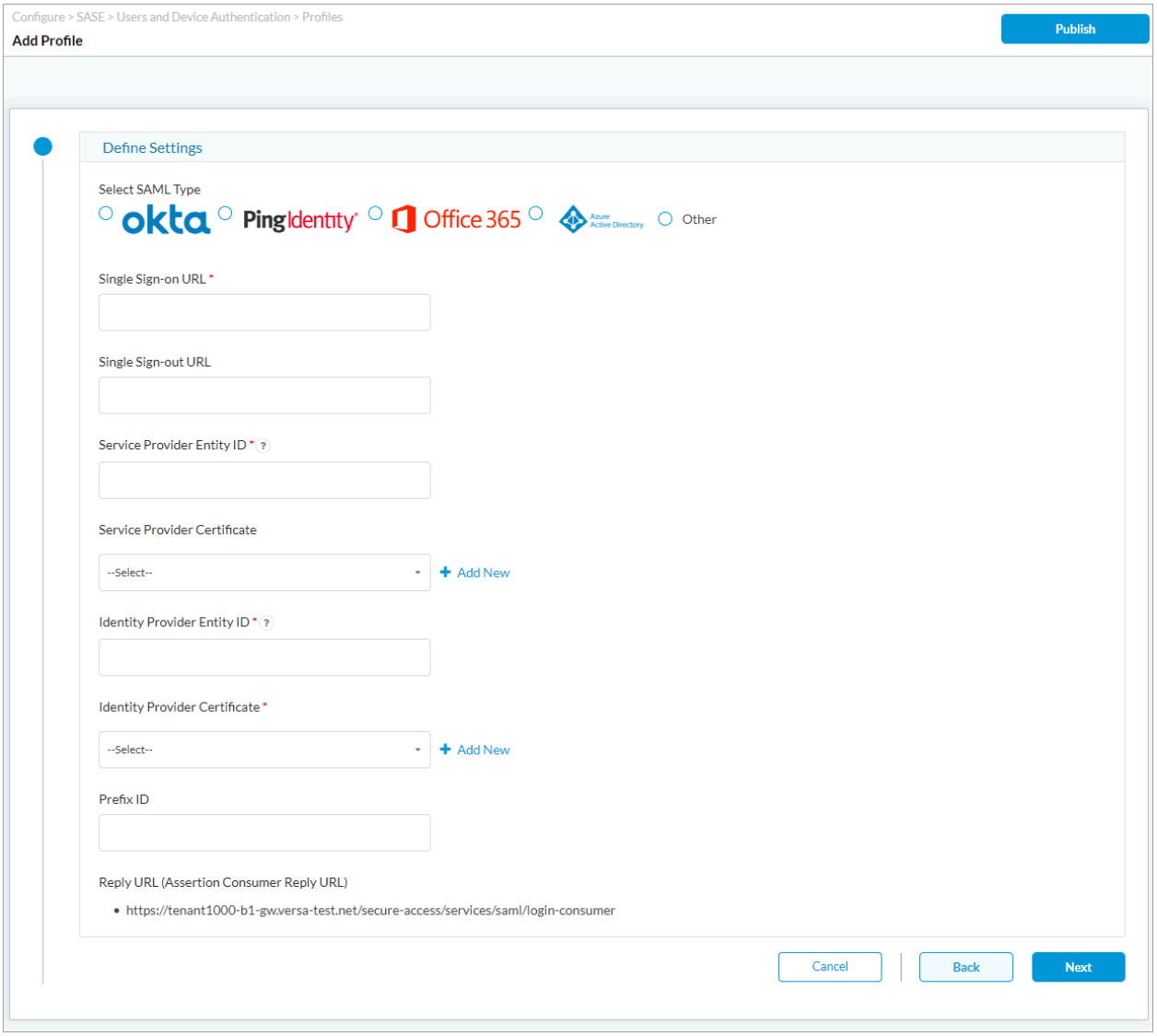
6. Click Next.
7. The Define User/Group Profile screen displays. Enter information for the following fields.



Field	Description
Group Object Class (Required)	Enter the group object class provided by your administrator.
Group Name (Required)	Enter the group name provided by your administrator.
Group Member (Required)	Enter the group member provided by your administrator.
User Object Class (Required)	Enter the user object class provided by your administrator.
User Name (Required)	Enter the format of the username, for example, User Principal Name.
Refresh Interval	Enter how often to refresh the LDAP profile information, in seconds. *Range*: 60 through 86400 seconds *Default*: 21600 seconds

8. Click Next. The Provide Information screen displays. This screen is common for all authentication types. Enter the required information, as described in Step 16.

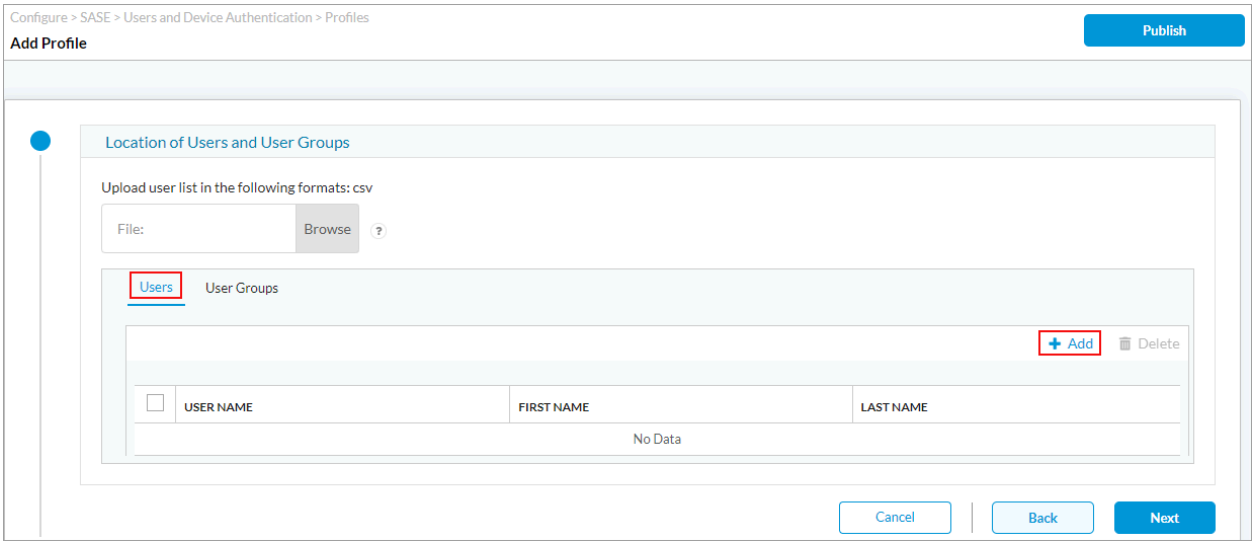
9. For the SAML authentication type, the following screen displays. Enter information for the following fields.



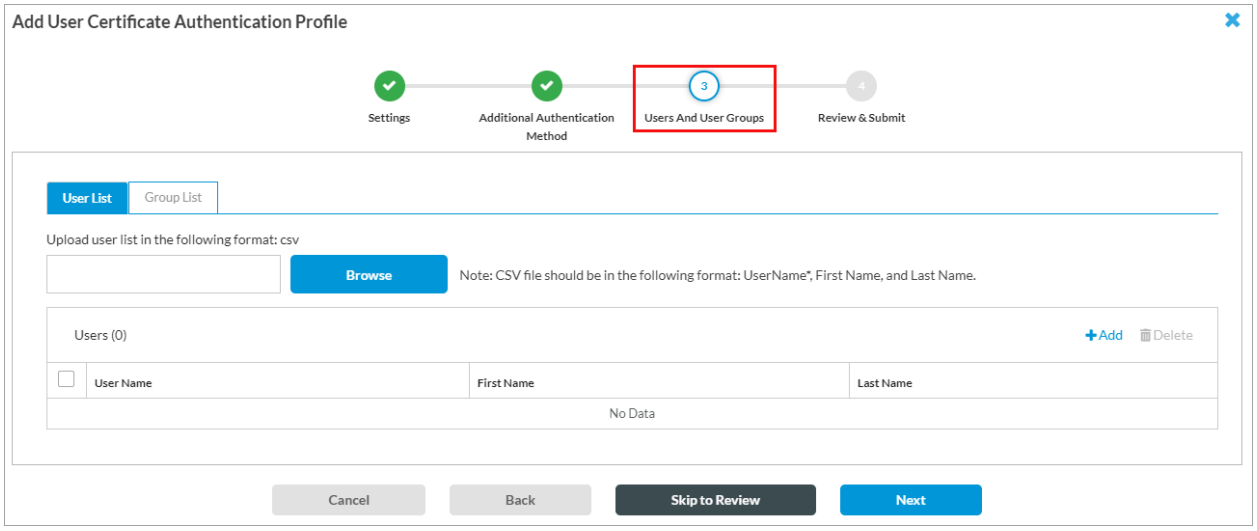
Field	Description
Select SAML Type	Select the SAML type: ◦ Azure Active Directory ◦ Office 365 ◦ Okta ◦ Other ◦ PingIdentity
Single Sign-on URL (Required)	Enter the URL of the identify provider (IdP) to use for

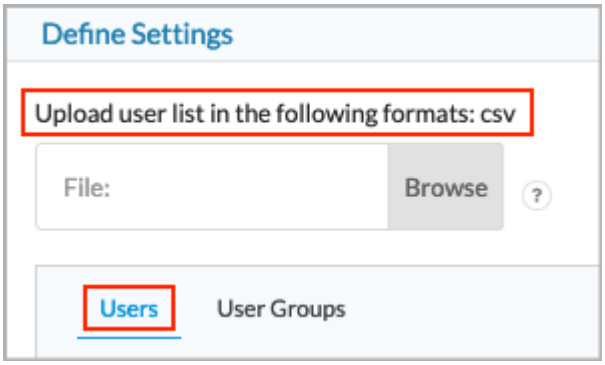
Field	Description
	single sign-on.
Single Sign-out URL	Enter the URL to point to for single sign-out.
Service Provider Entity ID (Required)	Enter the entity ID of the service provider.
Service Provider Certificate	Select the certificate that the service provider uses to authenticate.
Identity Provider Entity ID (Required)	Enter the entity ID that uniquely identifies the SAML IdP.
Identity Provider Certificate (Required)	Select the authentication certificate issued by the IdP.
Prefix ID	Enter the name of the external IdP.
Reply URL (Assertion Consumer Reply URL)	Enter the assertion consumer reply URL from which the application receives the authentication token. SAML also refers to this to as the Assertion Consumer Service (ACS).

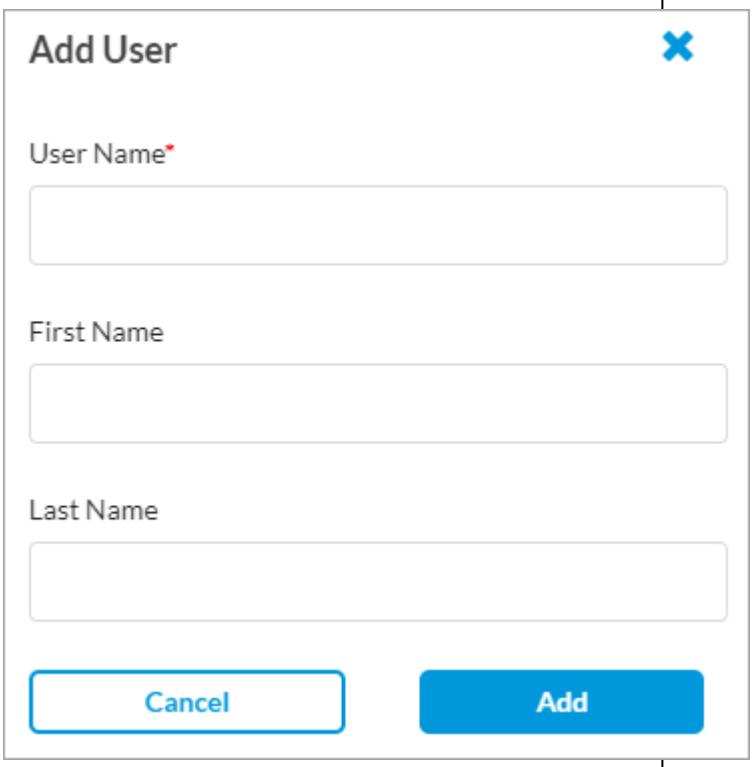
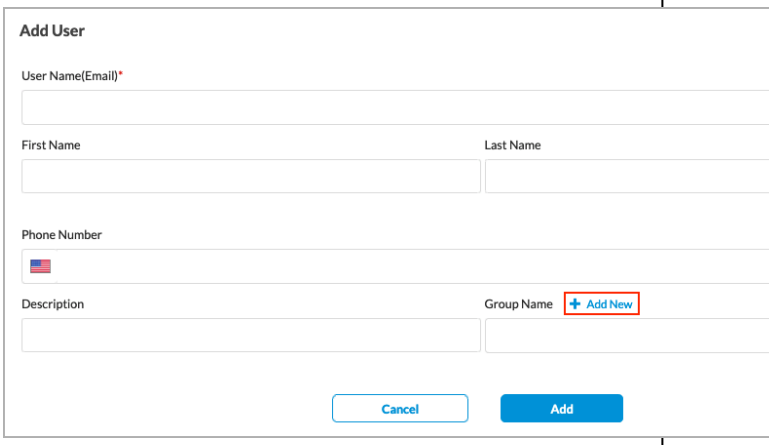
10. Click Next. The Location of Users and User Groups screen displays. Enter information for the following fields.

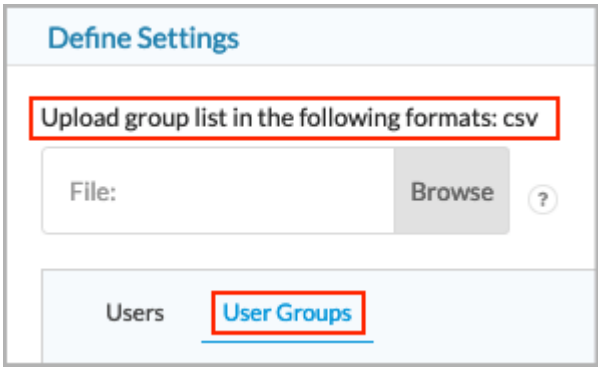
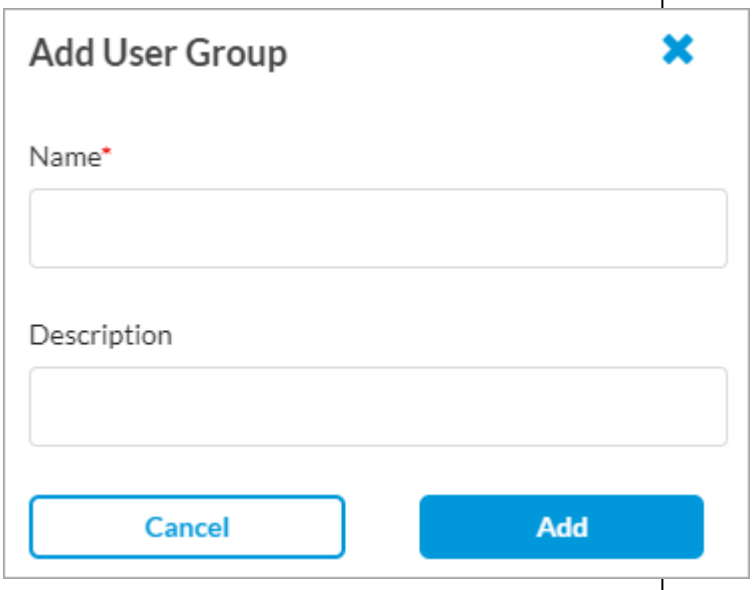


For Releases 12.1.1 and later, the following screen displays.

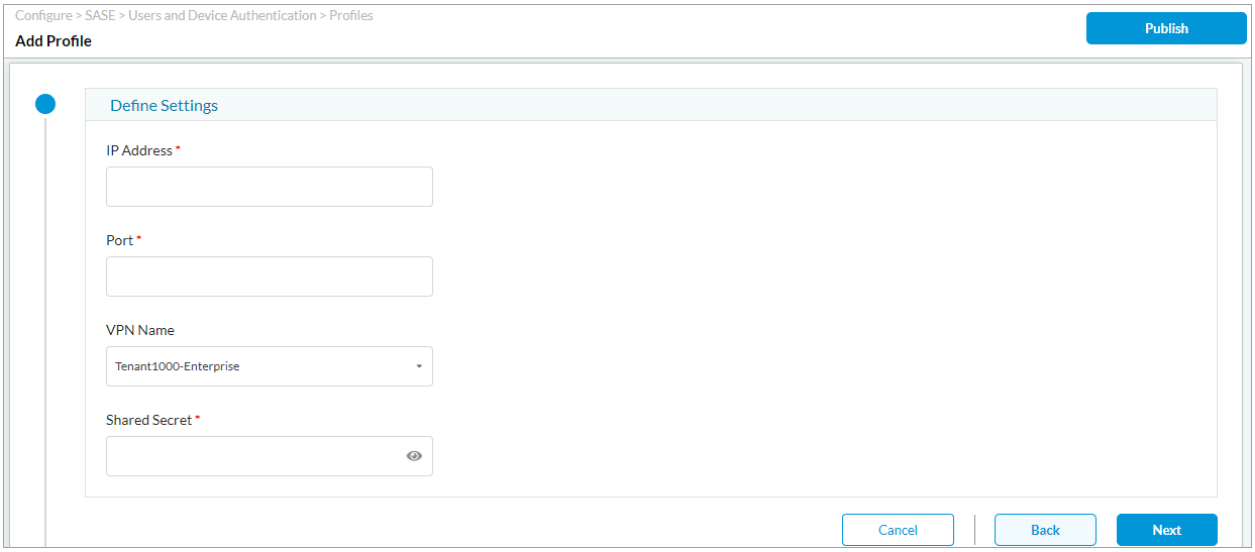


Field	Description
Upload user list in the following formats: csv	If you select the Users tab in the Define Settings section, click File: Browse. In the popup window, select a user list file in CSV format to upload. Each line in the CSV file must be in the following format: ◦ User Name*, First Name, Last Name, Password*, Email*, Phone, Description, Group Name. (Note that fields marked with an asterisk (*) are mandatory.) 
Users tab	Click + Add to add a new user. In the Add User screen, enter the required information. When you select LDAP or SAML as the authentication type, the following screen displays:

	 For Versa Directory, the following screen displays when you click + Add to add a user:  Click + Add New to add a new user group, as shown below in the User Groups tab.
Upload group list in the following formats: csv	If you select the User Groups tab in the Define

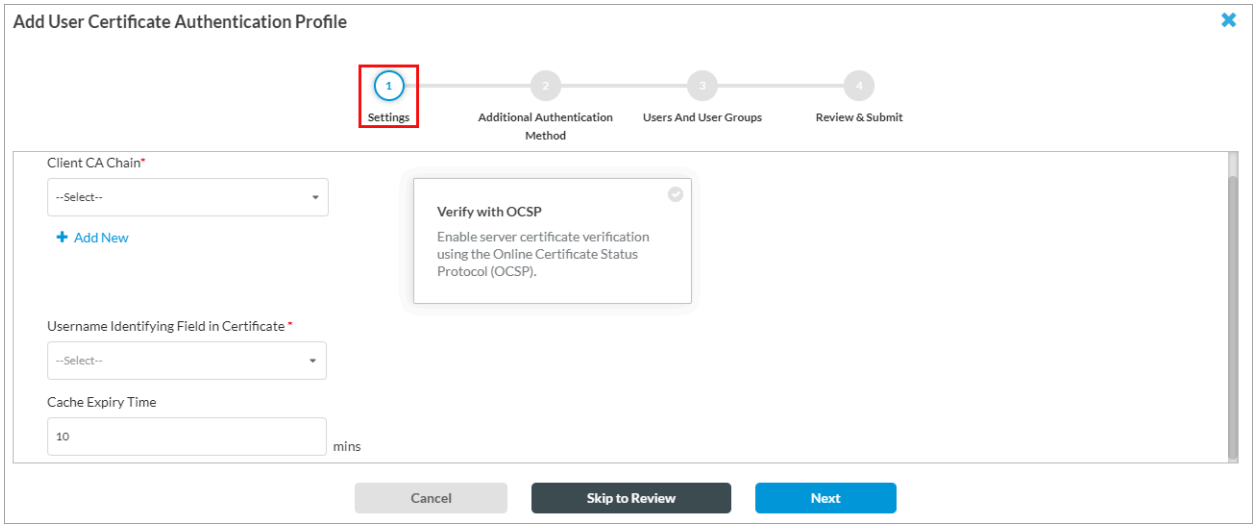
	Settings section, click File: Browse. In the popup window, select a user group file in CSV format to upload. Each line in the CSV file must be in the following format: ◦ Group Name*, Description 
User Groups tab	Click + Add to add a new user group. In the Add User Group screen, enter the required information. 

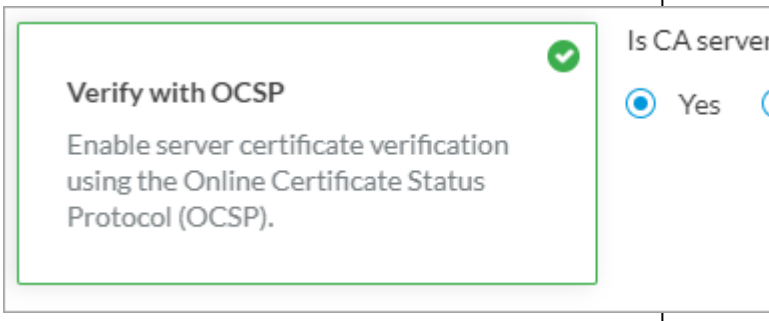
11. Click Next. The Provide Information screen displays. This screen is common for all authentication types. Enter the information as described in Step 16.
12. If you select RADIUS as the authentication type, the following screen displays. Enter information for the following fields.



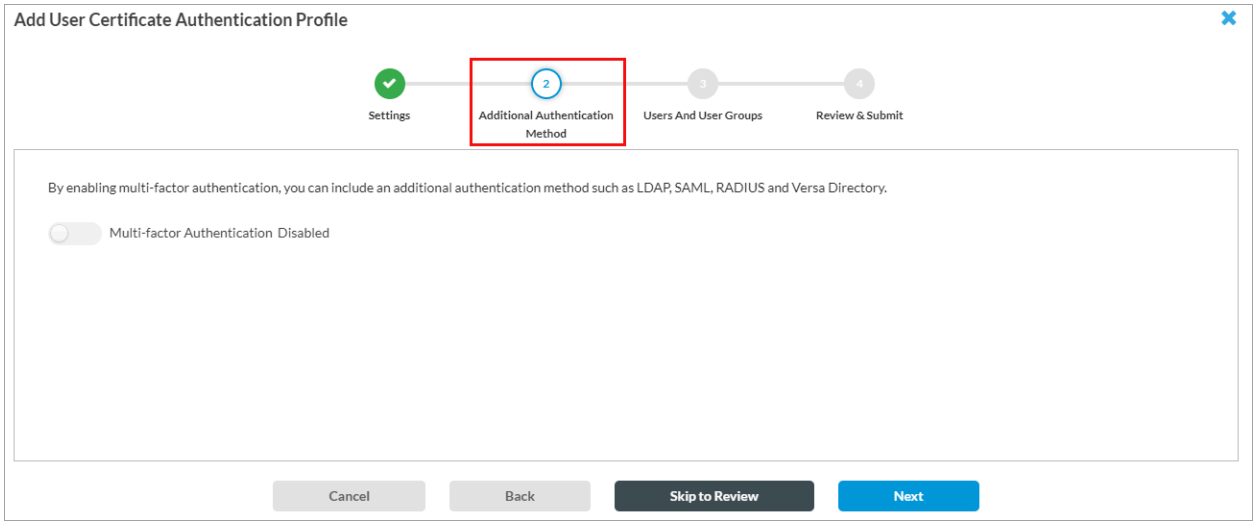
Field	Description
IP Address (Required)	Enter the IP address of the RADIUS server.
Port (Required)	Enter the port number to use on the RADIUS server.
VPN Name	Select the VPN instance to use to connect to the RADIUS server.
Shared Secret	Enter the RADIUS shared secret (password) string.

13. Click Next. The Location of Users and User Groups screen displays. Enter the information as described in Step 10.
14. Click Next. The Provide Information screen displays. This screen is common for all authentication types. Enter the information as described in Step 16.
15. If you select Versa Directory as the authentication type, the Location of Users and User Groups screen displays. Enter the information as described in Step 10.
16. (For Releases 12.1.1 and later.) If you select User Certificate Based as the authentication type, the Add User Certificate Authentication Type screen displays. In the Settings screen, enter information for the following fields.

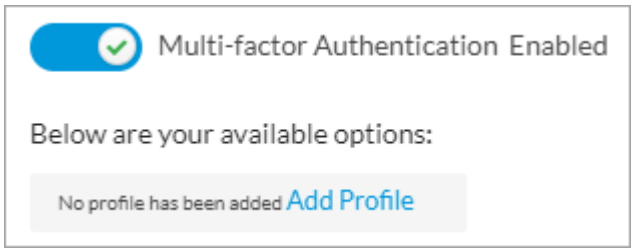


Field	Description
Client CA Chain (Required)	Select the client CA certificate chain to authenticate the user. To add a new CA certificate, click + Add New. The Add CA Certificate window displays. For more information, see Configure SASE Certificates.
Username Identifying field in Certificate (Required)	Select the field that Concerto uses to validate a name match in the client certificate: ◦ Subject-Alternative-name Email ◦ Subject Alternative-name Principal Name ◦ Subject Common-name
Cache Expiry Time	Enter the time in minutes after which the cache expires. *Default*: 10 minutes
Verify with OSCP	Click to enable verification of server certificate using Online Certificate Status Protocol (OCSP). The following fields display:  Yes is selected by default and if you select Yes, Concerto uses the CA server on the internet for OCSP verification. If you select No, enter the VPN name to check for to server certificate.

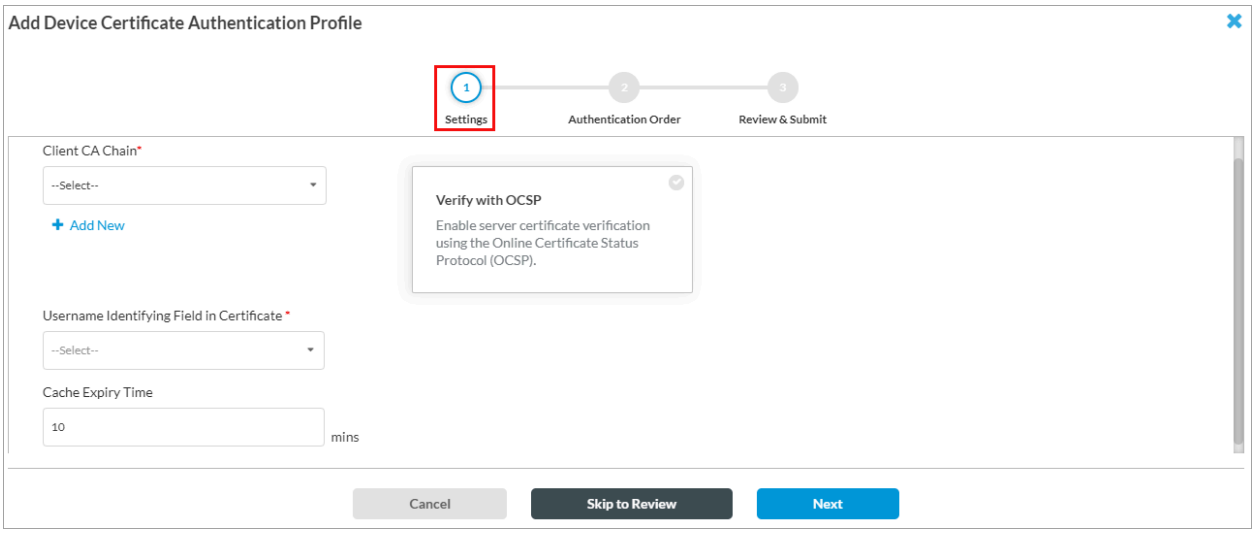
17. Click Next or select Step 2, Additional Authentication Method. The following screen displays.



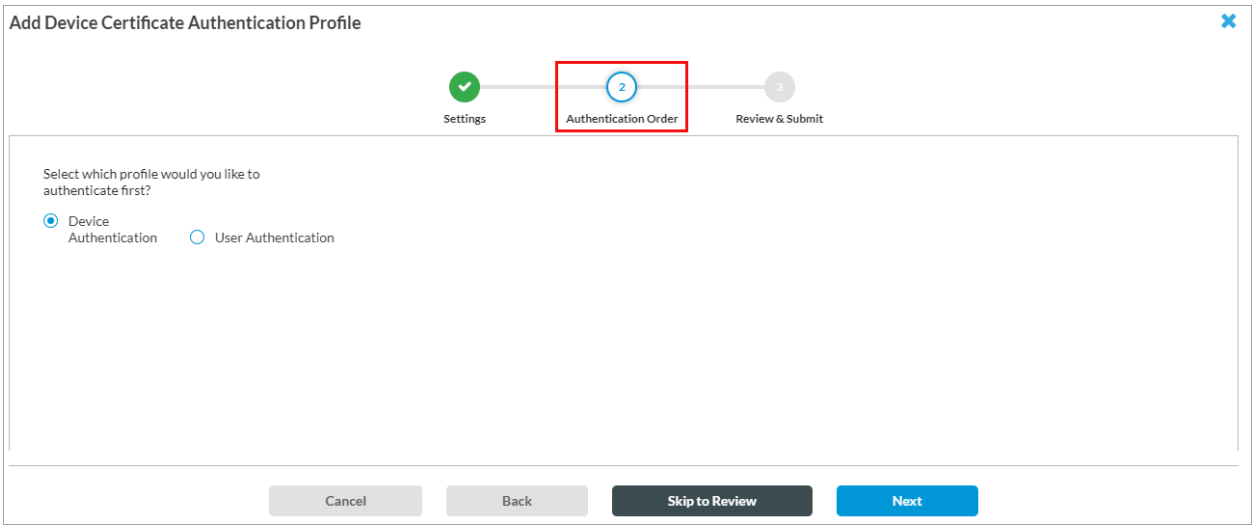
18. To enable multi-factor authentication using LDAP or SAML profiles, slide the Multi-factor Authentication Disabled toggle. This is disabled by default.



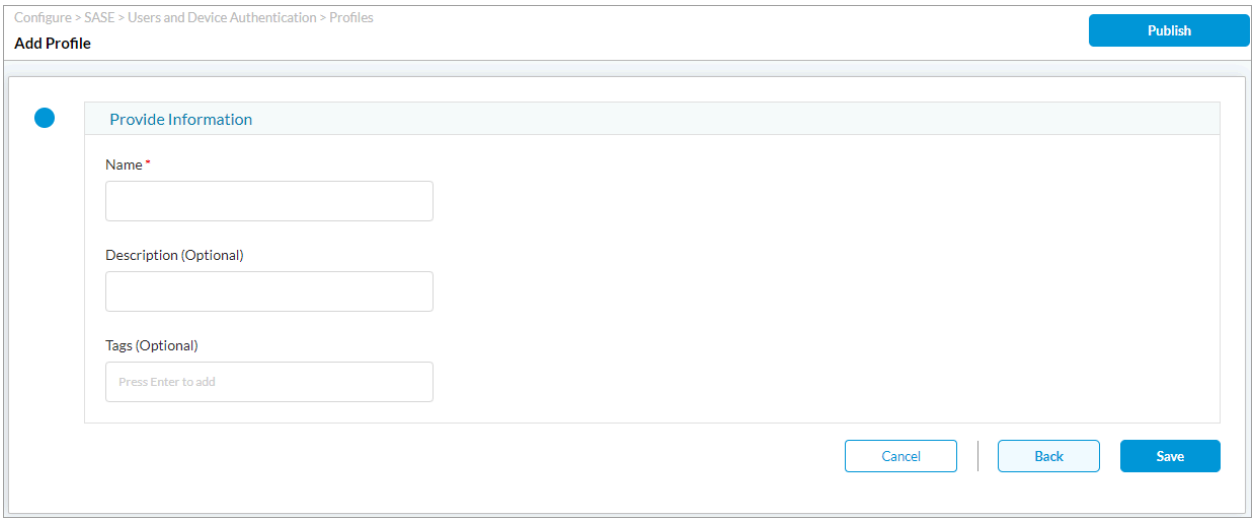
19. If LDAP and SAML profiles are configured, the profiles display.
20. Click Add Profile to add a profile. For adding LDAP profiles, follow Step 5 through 7 and for SAML profile, follow Steps 9 through 11.
21. Click Next. The Users and User Groups screen displays. Enter the information as described in Step 10.
22. (For Releases 12.1.1 and later.) If you select Device Certificate Based as the authentication type, the Add Device Certificate Authentication Type screen displays. In the Settings screen, enter information as described in Step 16.



23. Click Next or select Step 2, Authentication Order. The following screen displays.

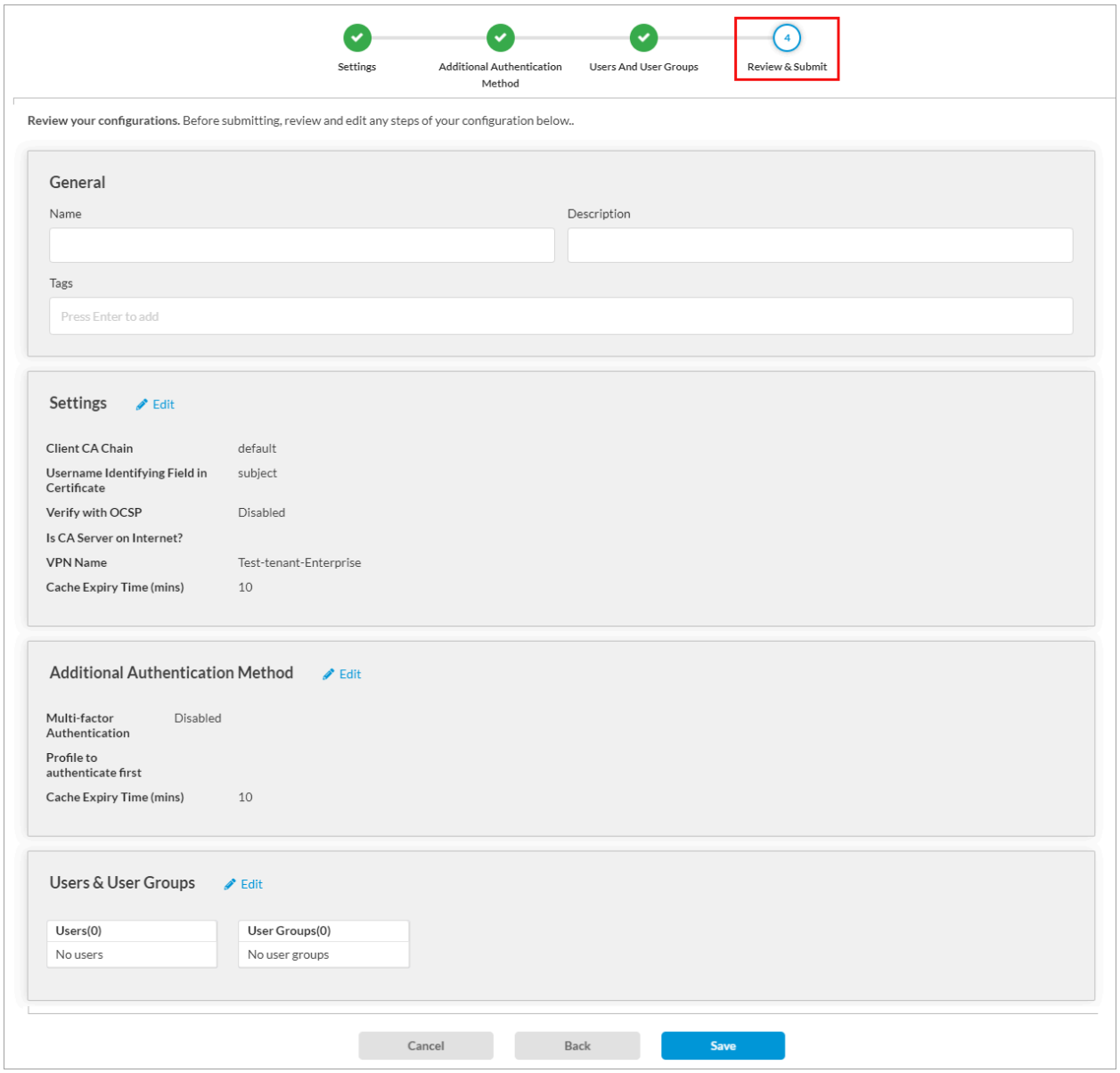


24. If you have configured a user certificate-based authentication profile, select Device Authentication or User Authentication to specify which profile to use first for authentication. Device Authentication is select by default.
25. (For Releases 11.4.1 and earlier.) Click Next. In the Provide information screen, enter information for the following fields



Field	Description
Name	Enter a name for the authentication profile, for example, ACME-SAML-Profile or ACME-LDAP-Profile.
Description	Enter a text description for the text authentication profile.
Tags	Enter tags to associate with the authentication profile.

26. Click Save.
27. (For Releases 12.1.1.) Click Next. The Review and Submit screen displays. This screen is common for all authentication types.



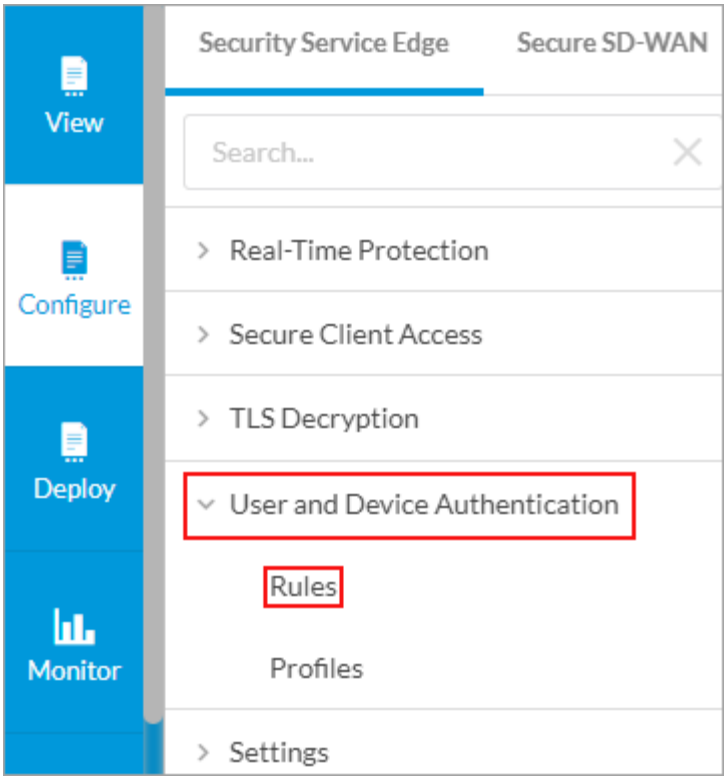
28. In the General box, enter a name for the rule, and optionally, enter a text description for the rule and one or more tags.

29. Review the selected settings. Click the Edit icon to change a setting, as needed.
30. Click Save to create the authentication profile.

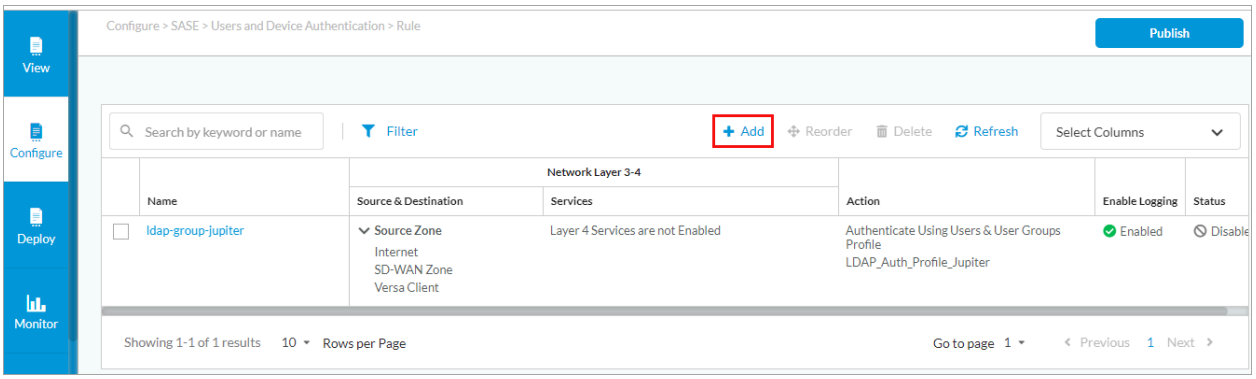
Configure User and Device Authentication Rules

To configure user and device authentication rules for SASE users and groups:

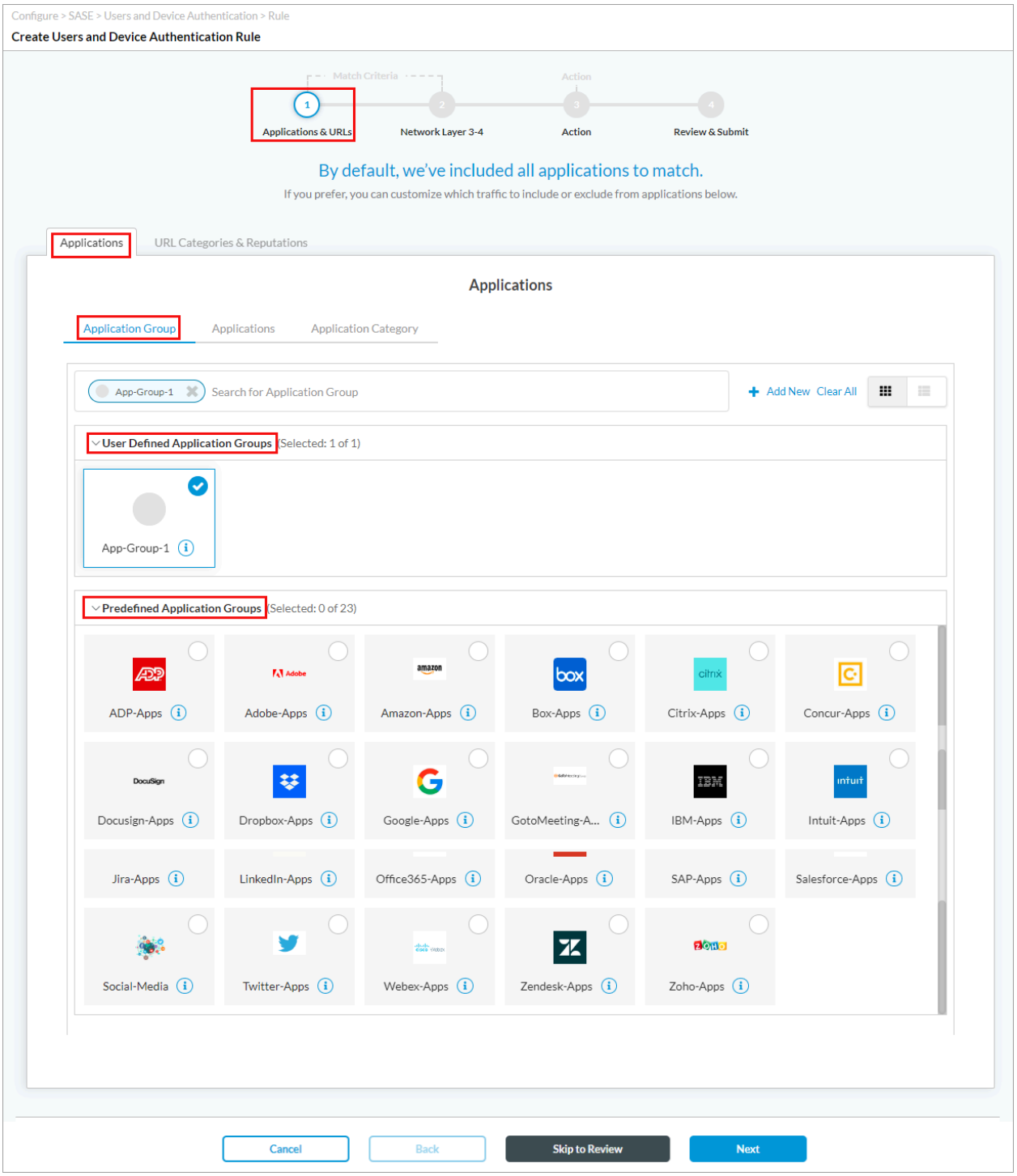
1. Go to Configure > Security Service Edge > User and Device Authentication > Rules.



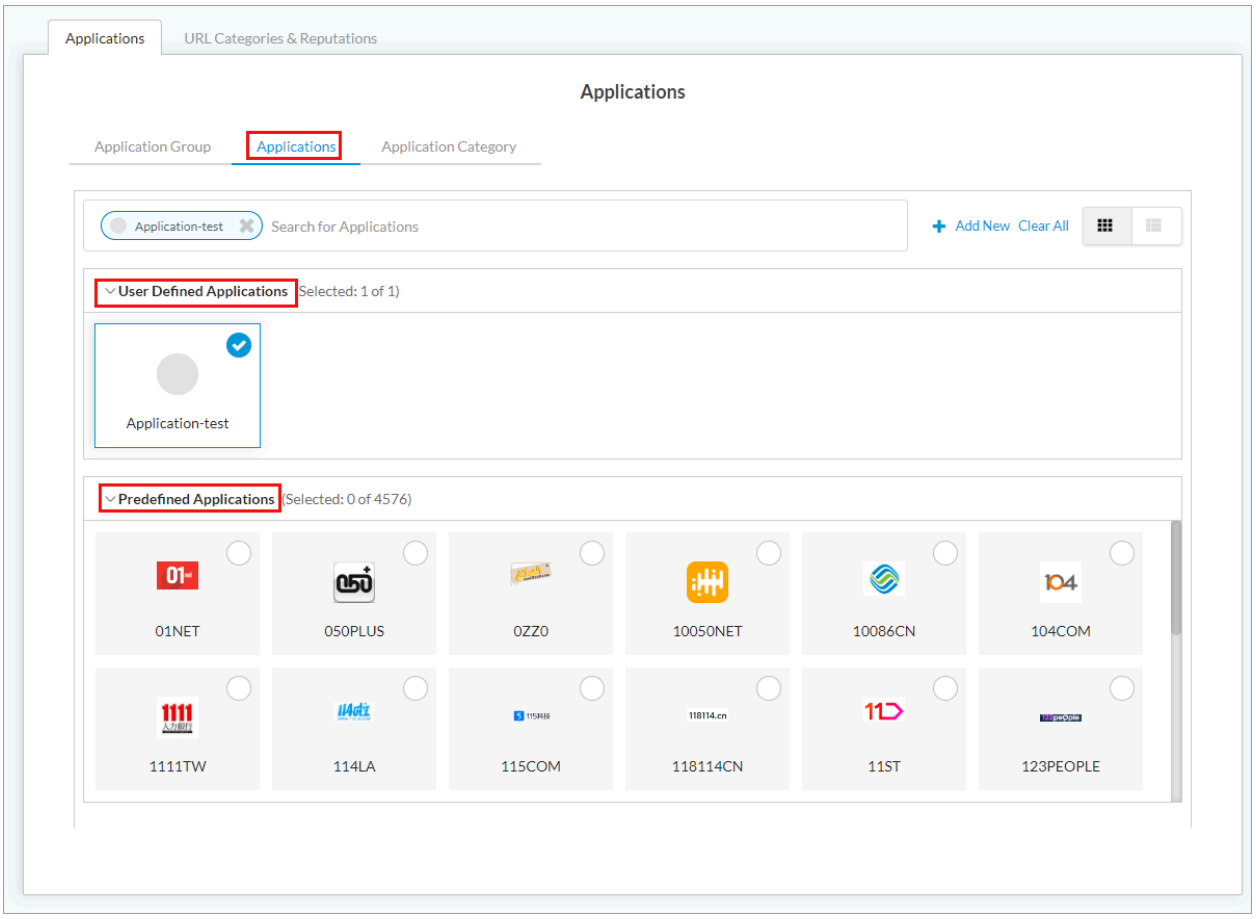
The Rule screen displays.



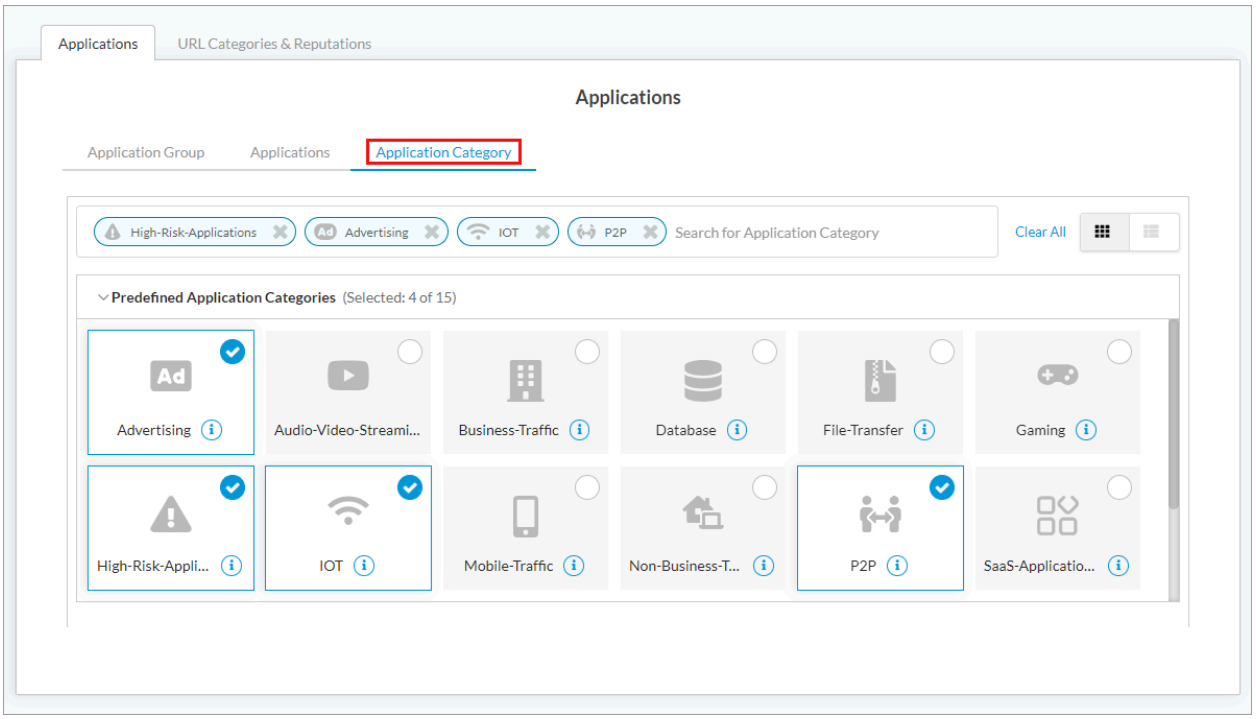
2. To create a new users and groups profile, click + Add. The Create Users and Device Authentication Rule window displays the first step of the workflow:
   - For Releases 12.1.1 and later, the first step is Applications and URLs.
   - For Releases 11.4.1 and earlier, the first step is Network Layer 3-4. Skip to Step 11 of this procedure to continue.
3. For Releases 12.1.1 and later, in Step 1, Applications and URLs, select the match criteria for applications, reputations, and URLs. By default, all applications, URLs, and reputations are included in the match criteria.



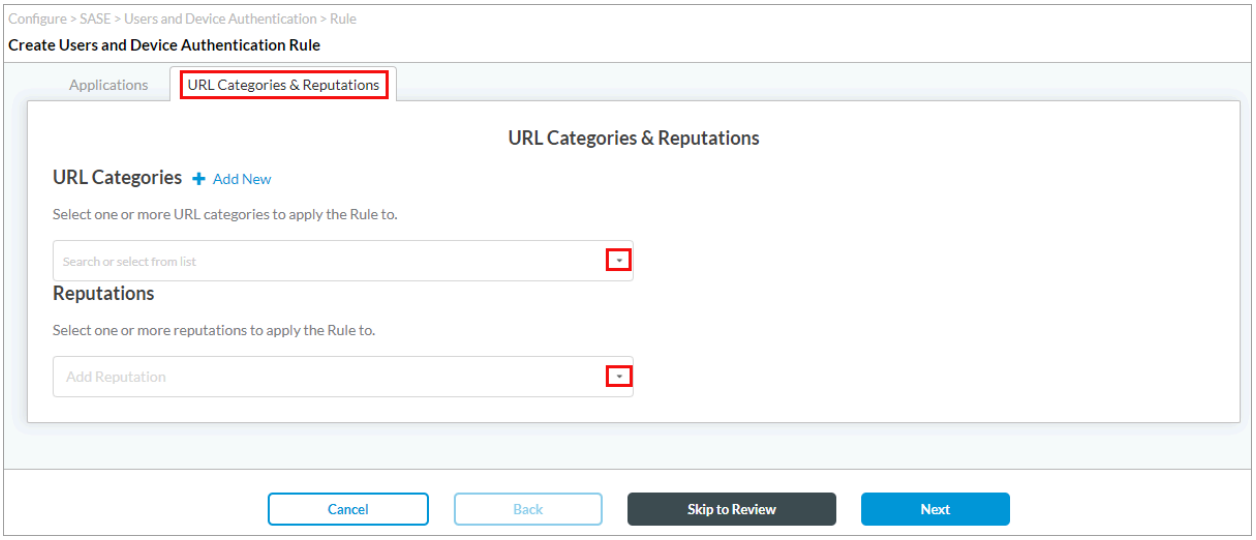
4. Select the Applications > Application Group tab, and then select one or more user-defined and predefined application groups for the rule to match.
5. Select the Applications > Applications tab, and then select one or more user-defined and predefined applications for the rule to match.



6. Select the Applications > Application Category tab, and then select one or more predefined application categories for the rule to match.



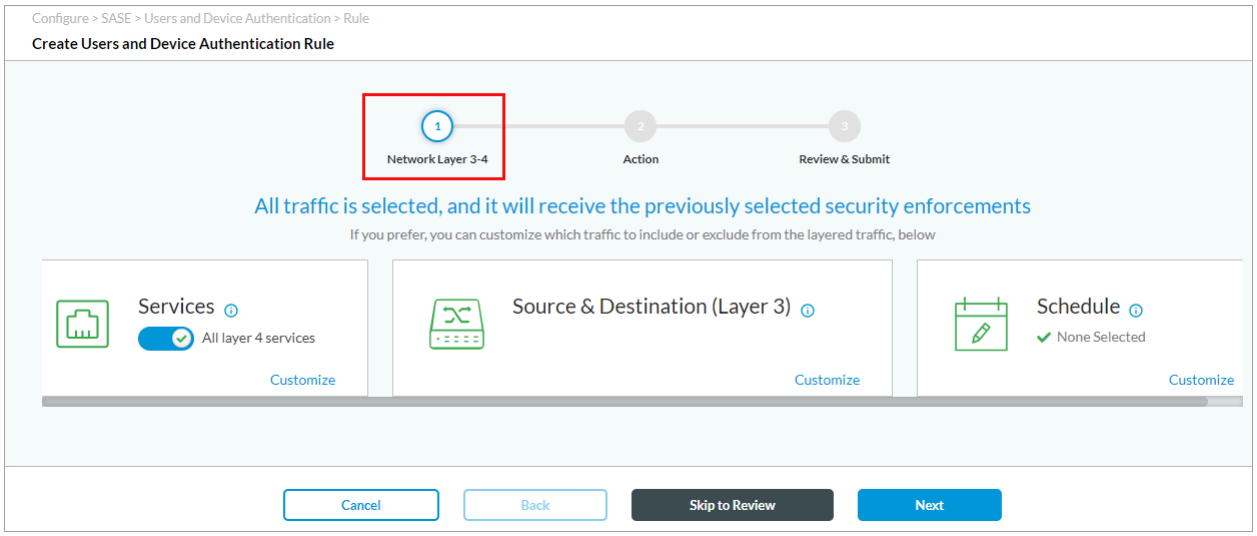
7. Select the URL Categories and Reputations tab. The following screen displays.



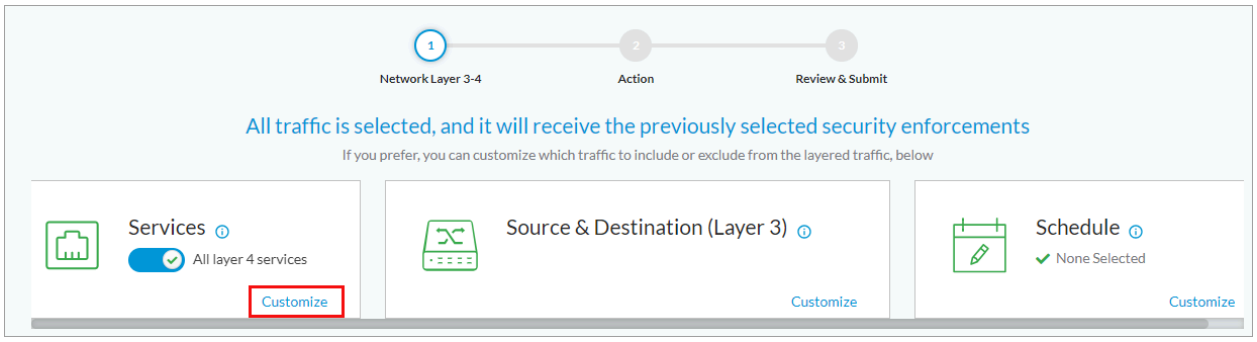
8. In the URL Categories field, click the down arrow, and then select one or more URL categories for the rule to match.
9. In the Reputations field, click the down arrow, and then select one or more reputations for the rule to match:
   - High risk
   - Low risk
   - Moderate risk
   - Suspicious
   - Trustworthy

- Undefined

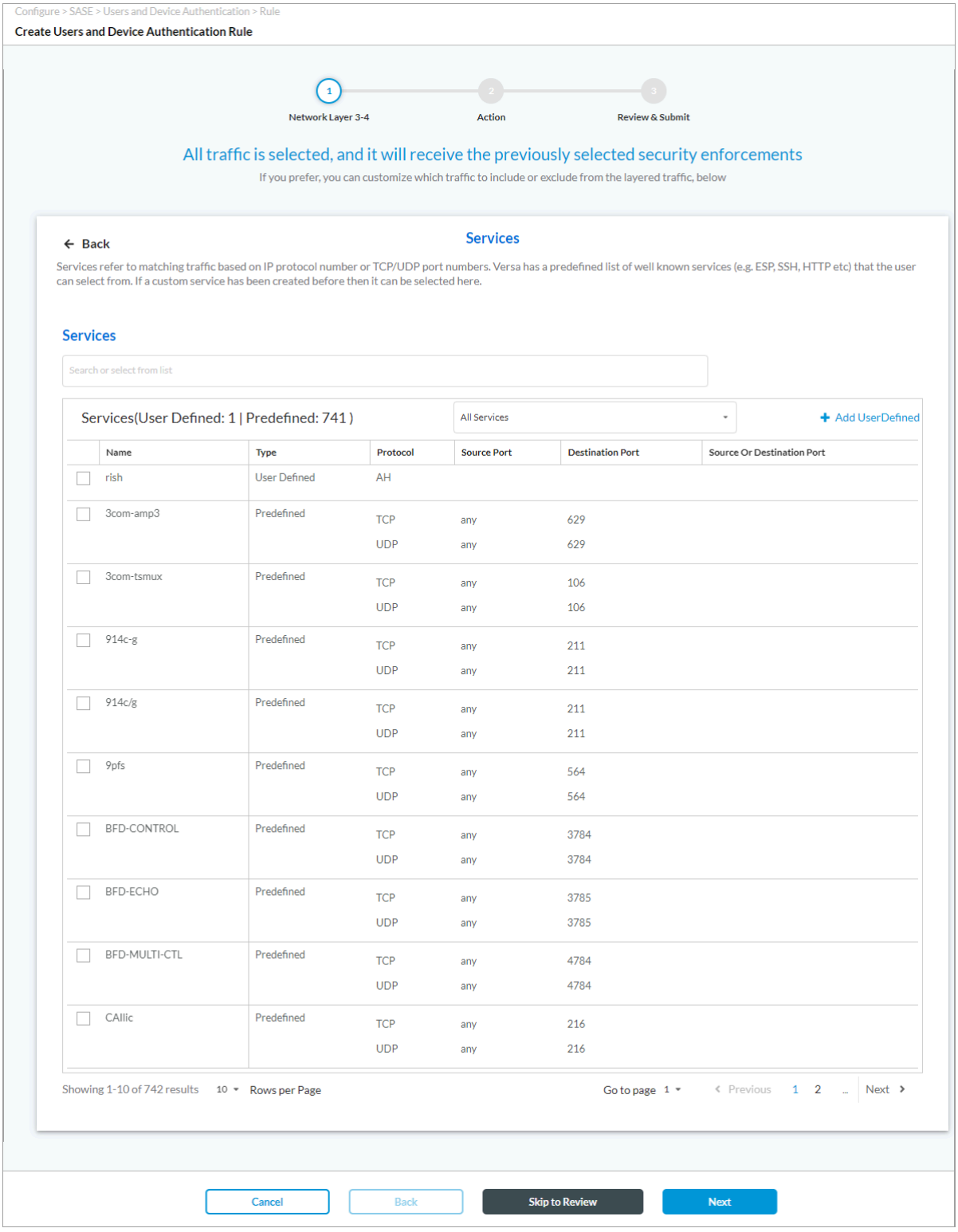
10. Click Next.
11. In Step 1, Network Layer 3-4 (for Release 11.4.1) or in Step 2, Network Layer 3-4 (for Releases 12.1.1 and later), you can customize the Layer 4 services, Layer 3 source and destination information, and schedules to which the previously selected security enforcements should apply. By default, all traffic receives the previously selected security enforcements.



12. To customize the Layer 4 services, click Customize in the Services pane.

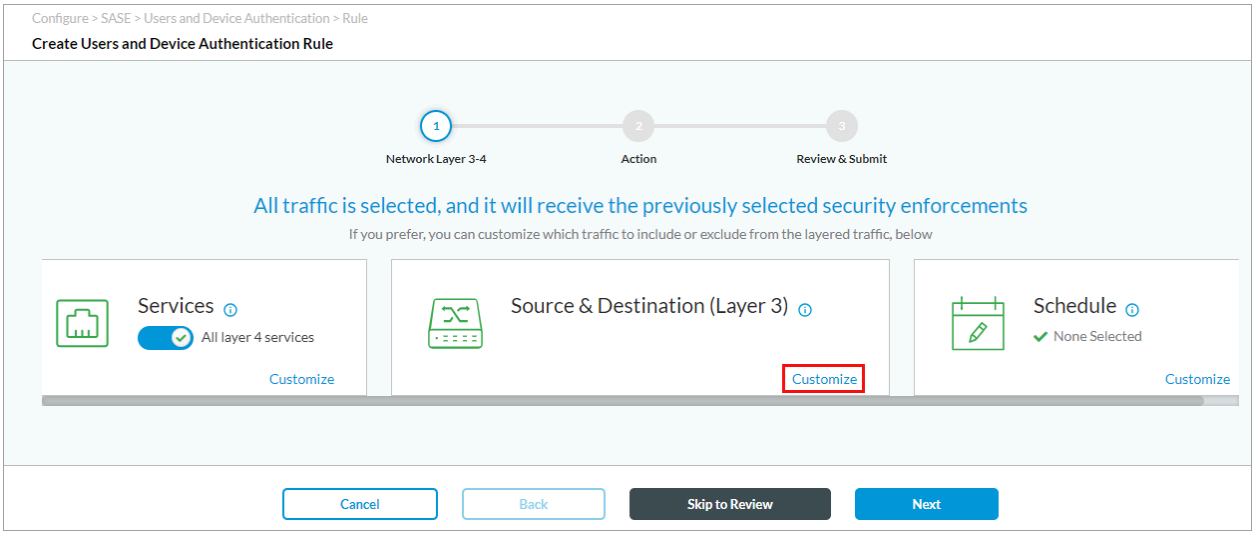


The Services window displays.

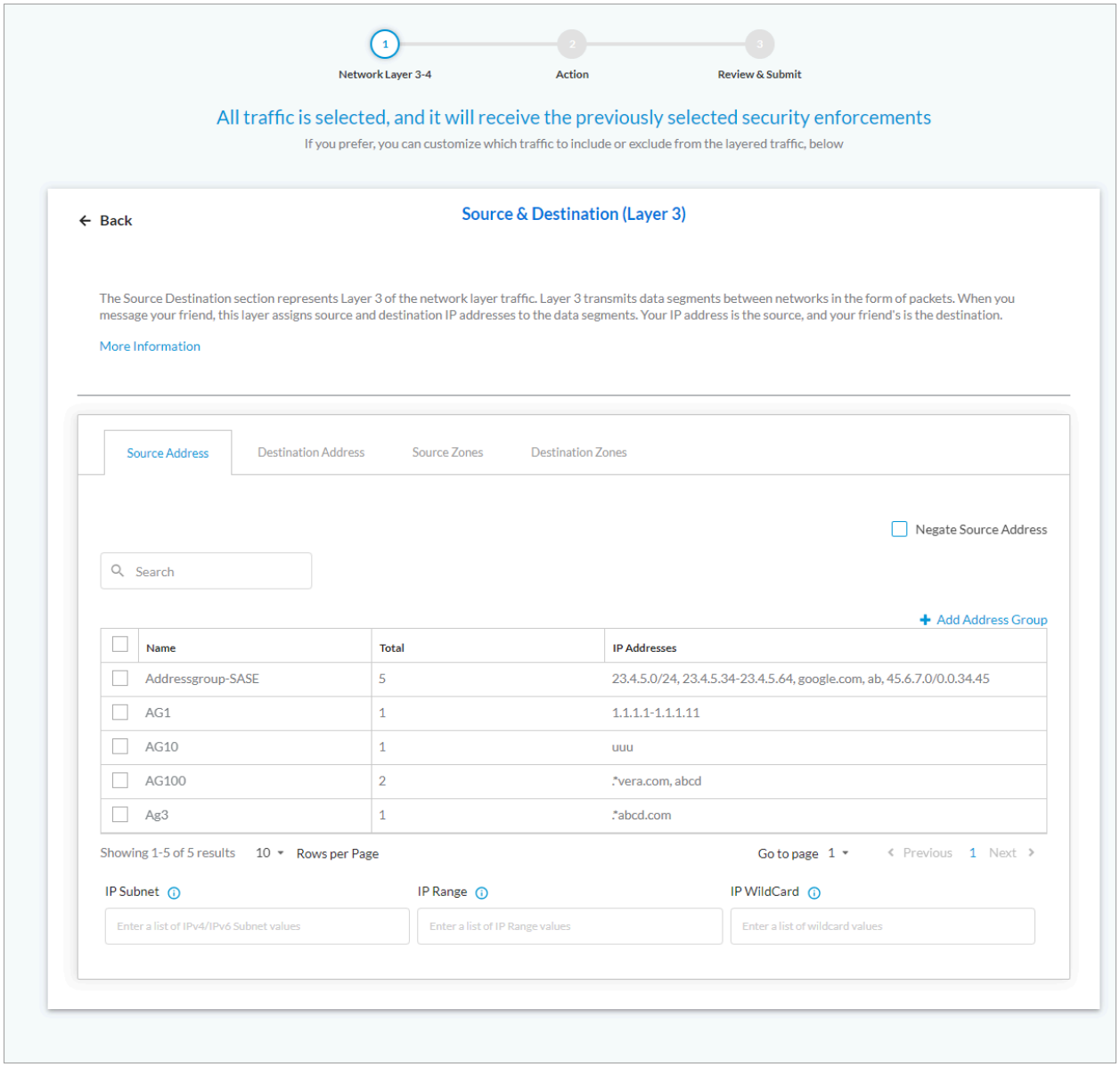


13. To find a service, enter the name of the service in the Services field, and then press Enter, or click All Services and then select User-defined Services or Predefined Services to filter the list of service objects.
14. To add a custom service object, click + Add User-Defined. The Service window displays. For more information, see Configure SASE Services.

15. To customize the source and destination information for a rule, in Network Layer 3-4 screen, click Customize in the Source and Destination Layer box.

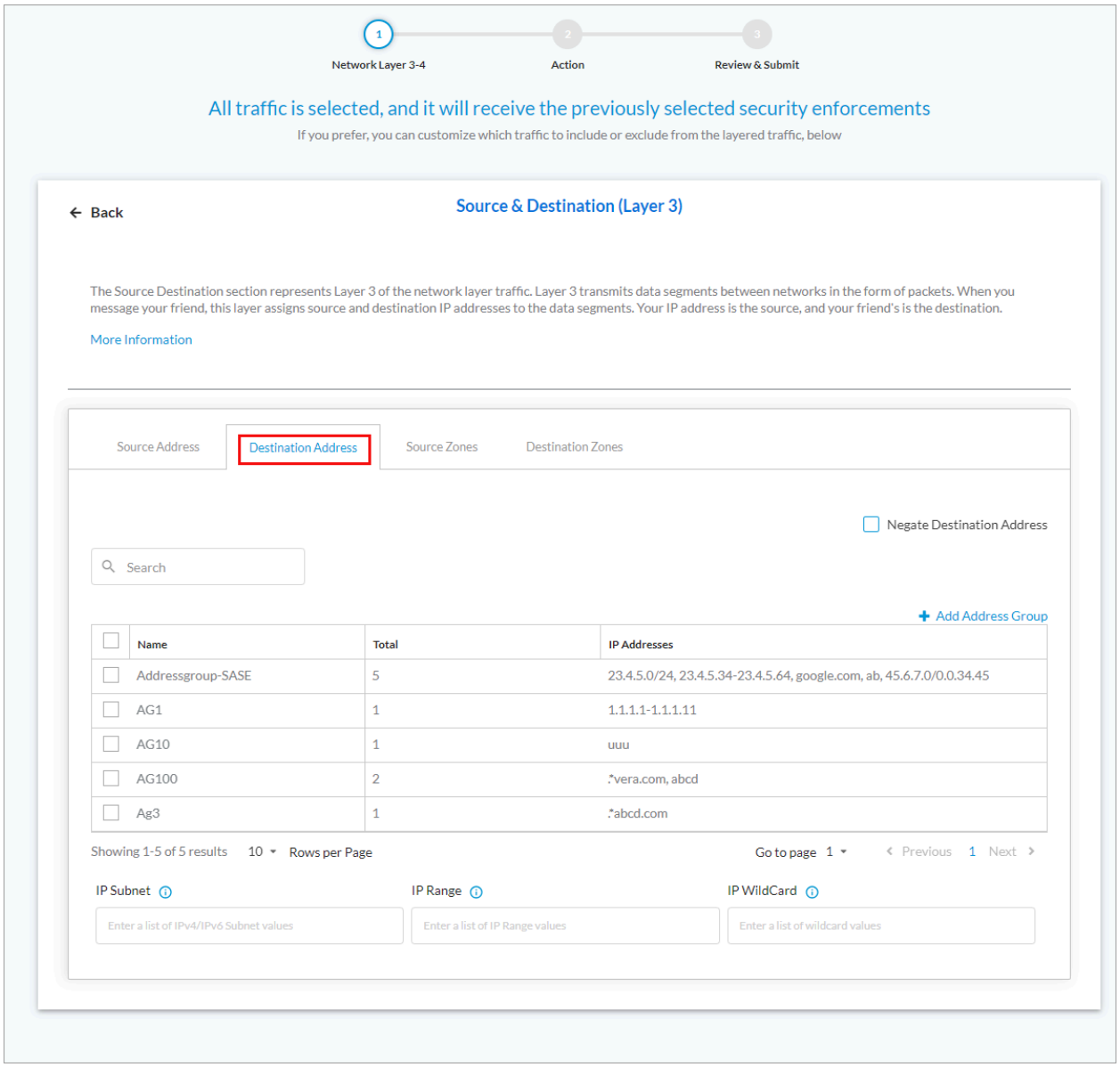


16. The Source and Destination (Layer 3) window displays. Select the Source Address tab, and then enter information for the following fields.



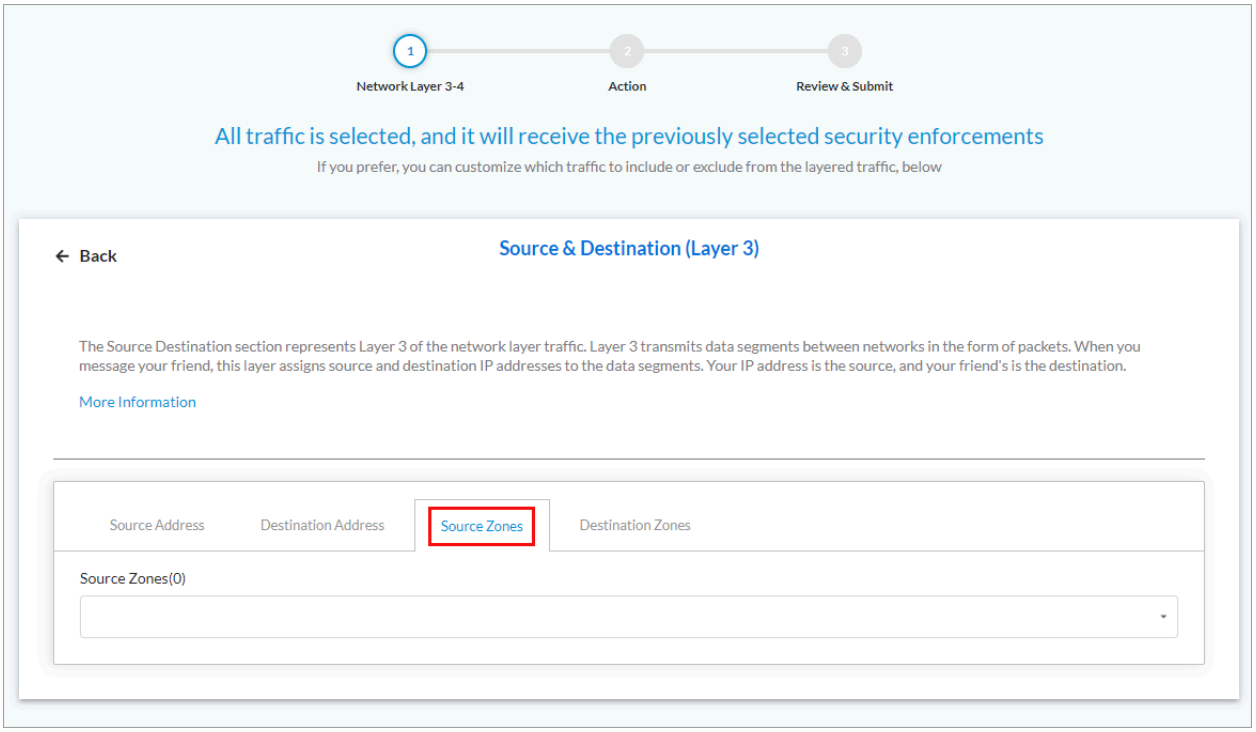
Field	Description
Negate Source Address	Click to match any source addresses except the configured addresses.
Address Group	Select an address group to match. To add a source address group, click + Add Address Group. The Address Group screen displays. For more information, see Configure Address Group Objects.
IP Subnet	Enter an IPv4 or IPv6 subnet.
IP Range	Enter an IP address range.
IP Wildcard	Enter a list of wildcard IP addresses.

17. Select the Destination Address tab, and then enter information for the following fields.

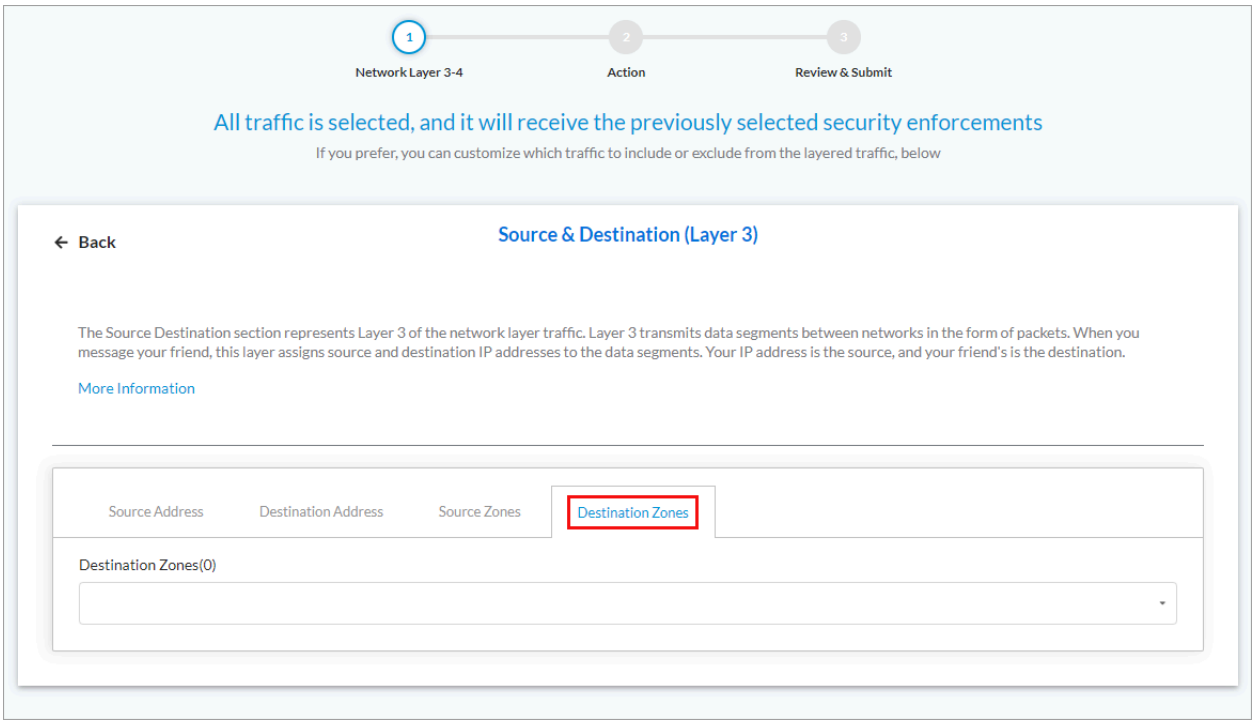


Field	Description
Negate Destination Address	Click to match any destination addresses except the configured addresses.
Address Group	Select an address group to match. To add a source address group, click + Add Address Group. The Address Group screen displays. For more information, see Configure Address Group Objects.
IP Subnet	Enter an IPv4 or IPv6 subnet.
IP Range	Enter an IP address range.
IP Wildcard	Enter a list of wildcard IP addresses.

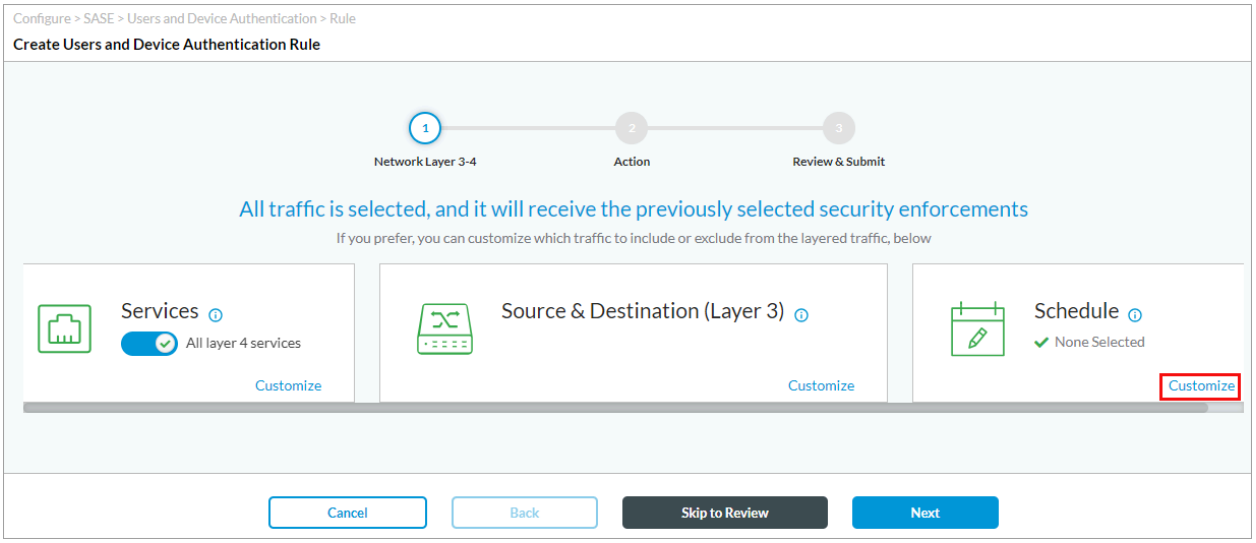
18. Select the Source Zone tab, the and select the user source zone for which to create authentication rule. You must configure a source zone.



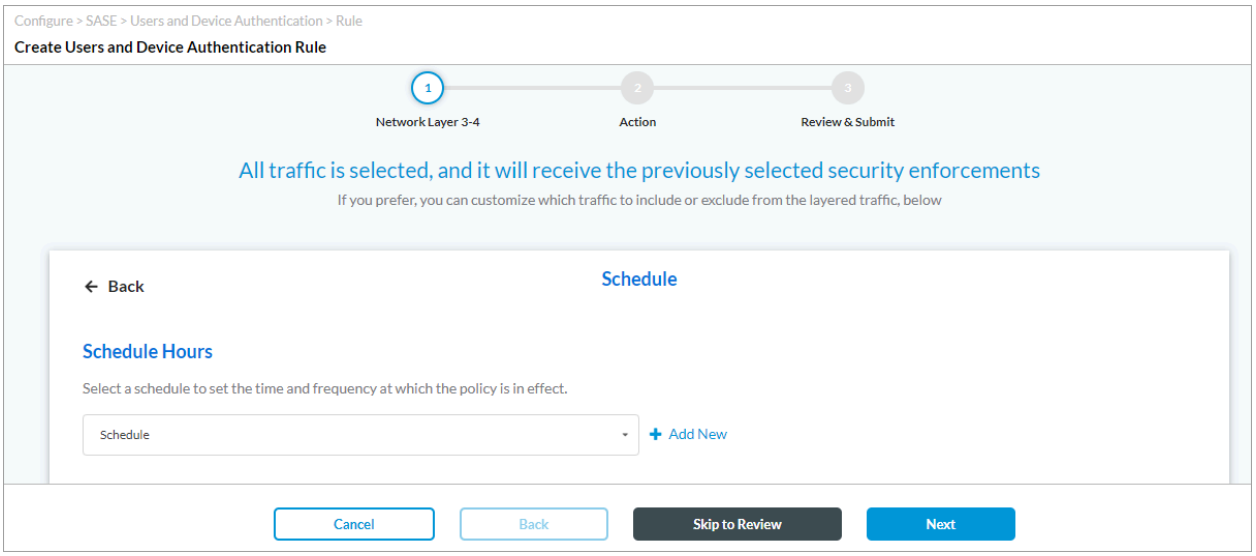
19. Select the Destination Zone tab, and then select the user destination zone for which to create authentication rule.



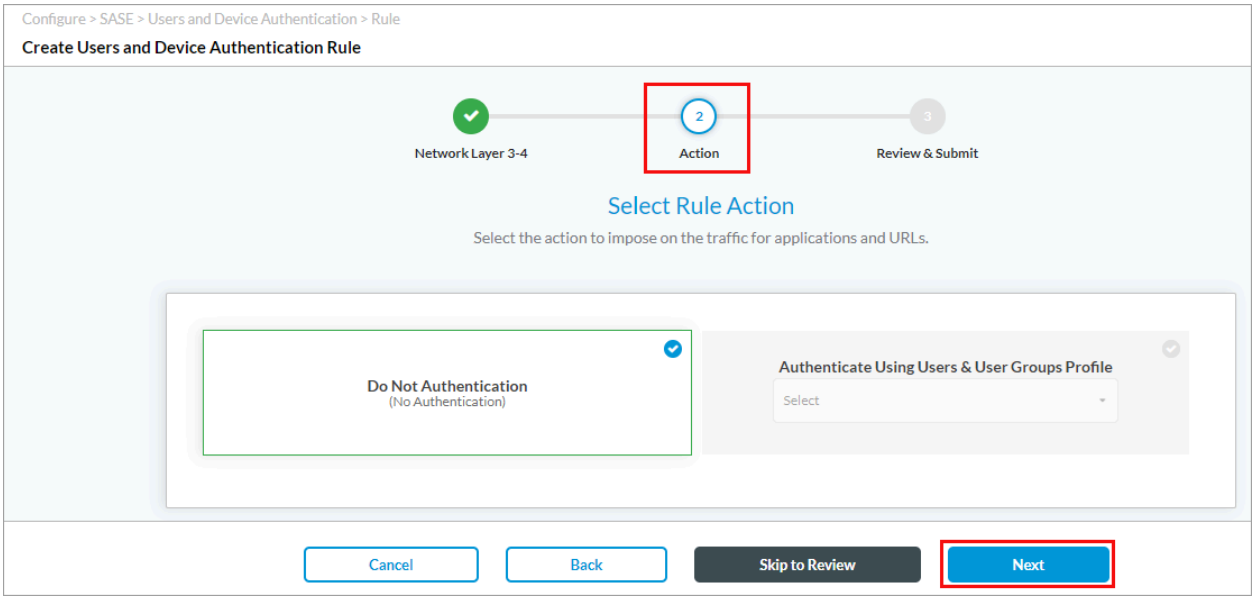
20. To customize the schedule for when the rule is in effect, in Network Layer 3-4 screen, click Customize in the Schedule box.



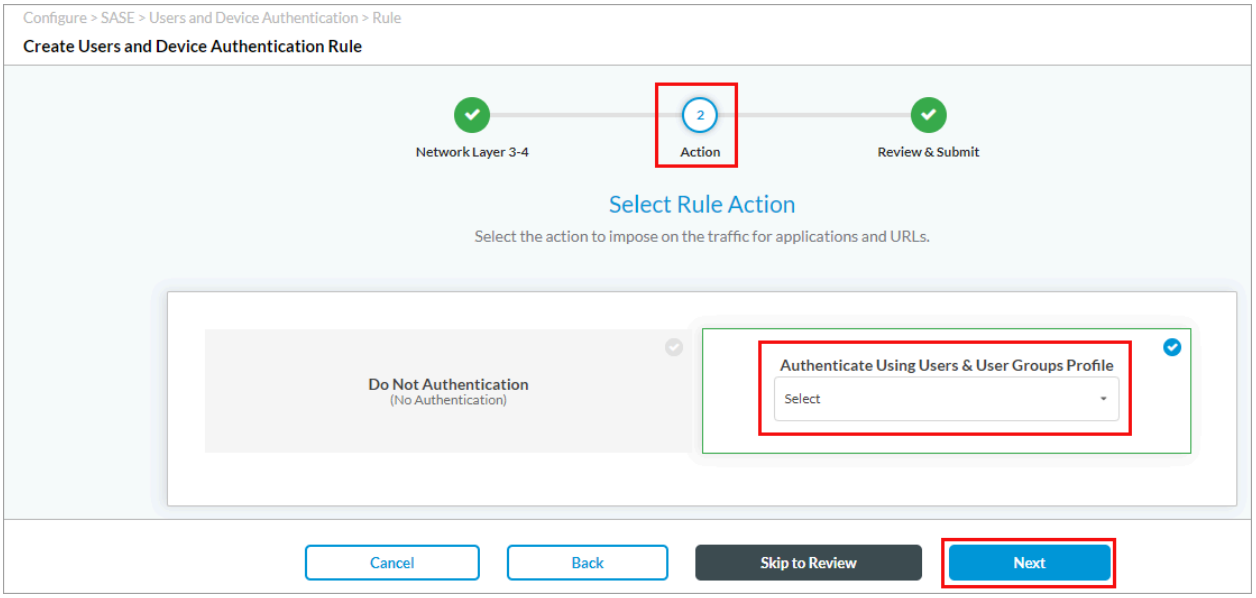
The Schedule window displays.



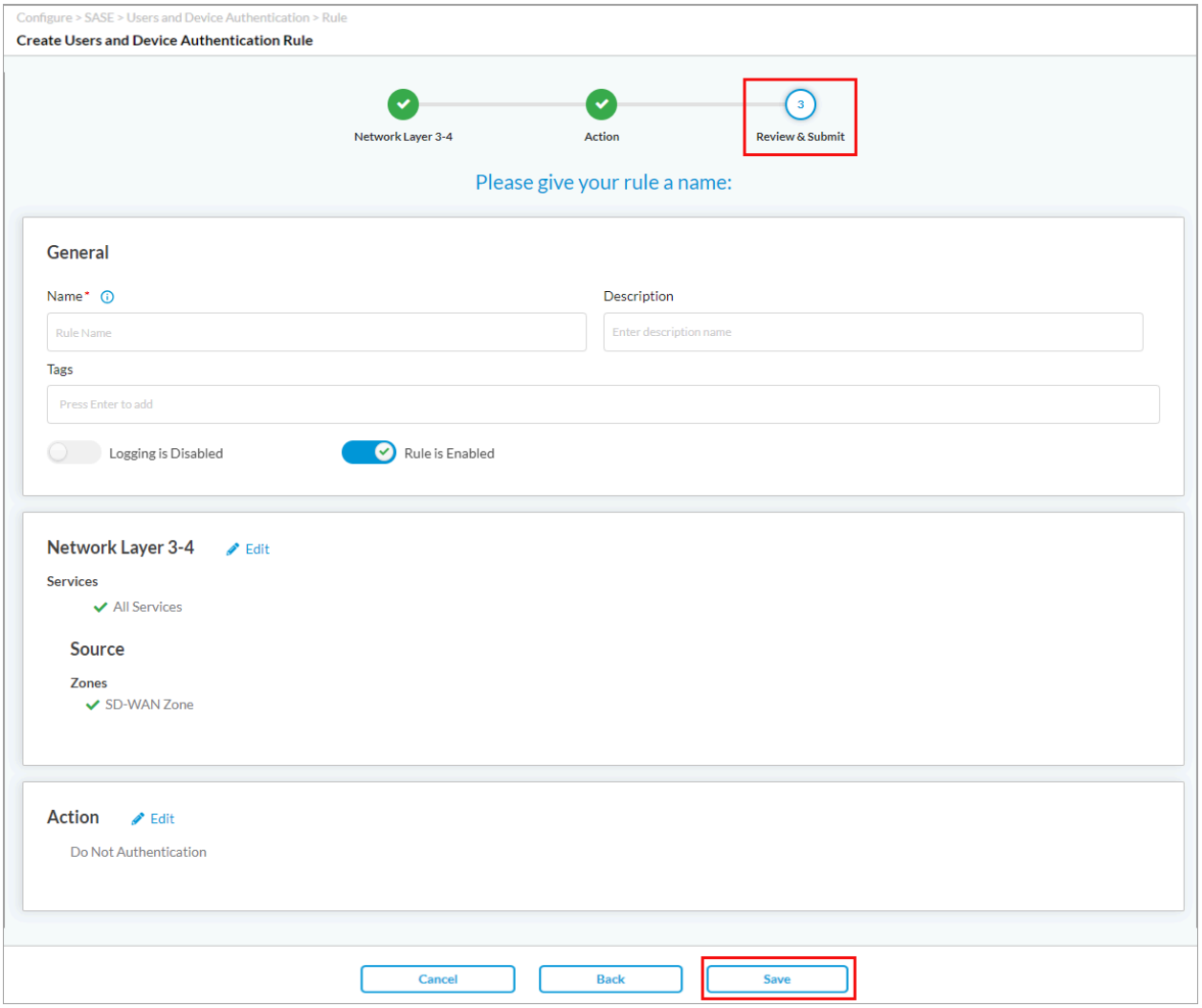
21. Select a schedule object to set the time and frequency when the rule to take effect.
22. Click + Add New to add a new schedule. The Schedule window displays. For more information, see Configure SASE Schedules.
23. Click Next. The Step 2, Action (for Release 11.4.1) or Step 3, Action (for Releases 12.1.1 and later) displays.



24. If you do not want to authenticate users for the match criteria you selected above, click Do Not Authenticate.
25. If you want to use a profile to specify the authentication type, click Authenticate Using User and Group Profile, and then select a profile that you configured in Configure User and Device Authentication Profiles, below.



26. Click Next. The Step 3, Review and Submit (for Release 11.4.1) or Step 4, Review and Submit (for Releases 12.1.1 and later) displays.

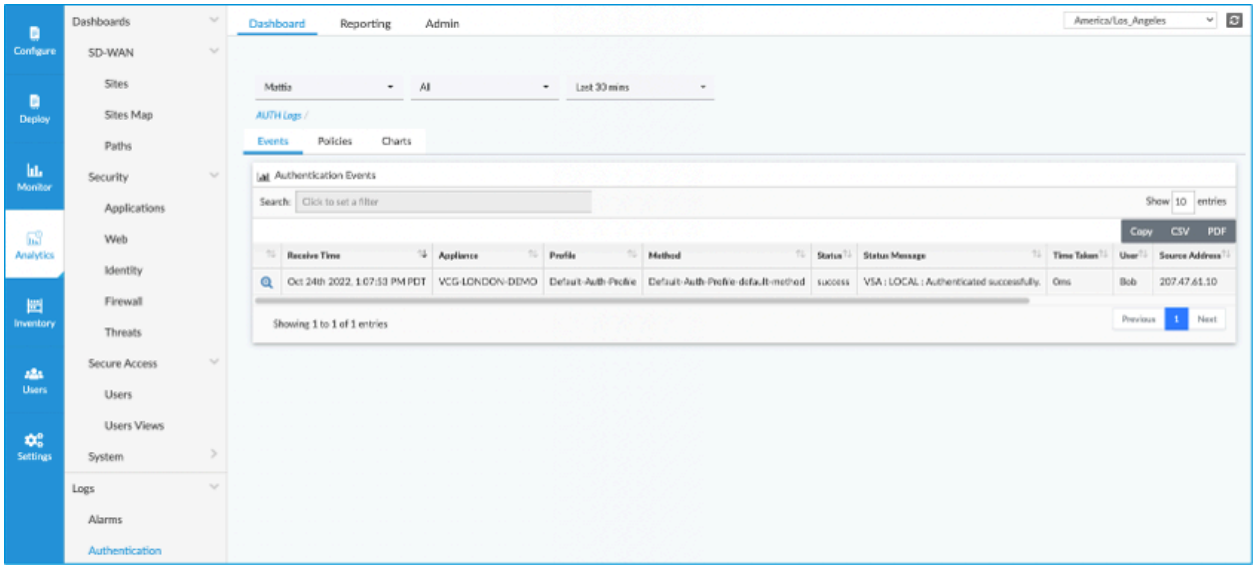


27. In the General section enter a name for the rule. Optionally, enter a description and add tags for the rule.
28. To enable logging for the rule, slide the toggle to Enabled.
29. The rule is enabled by default. Slide the Rule is Enabled toggle to disable the rule.
30. Click Edit next to any section to make changes.
31. Click Save.

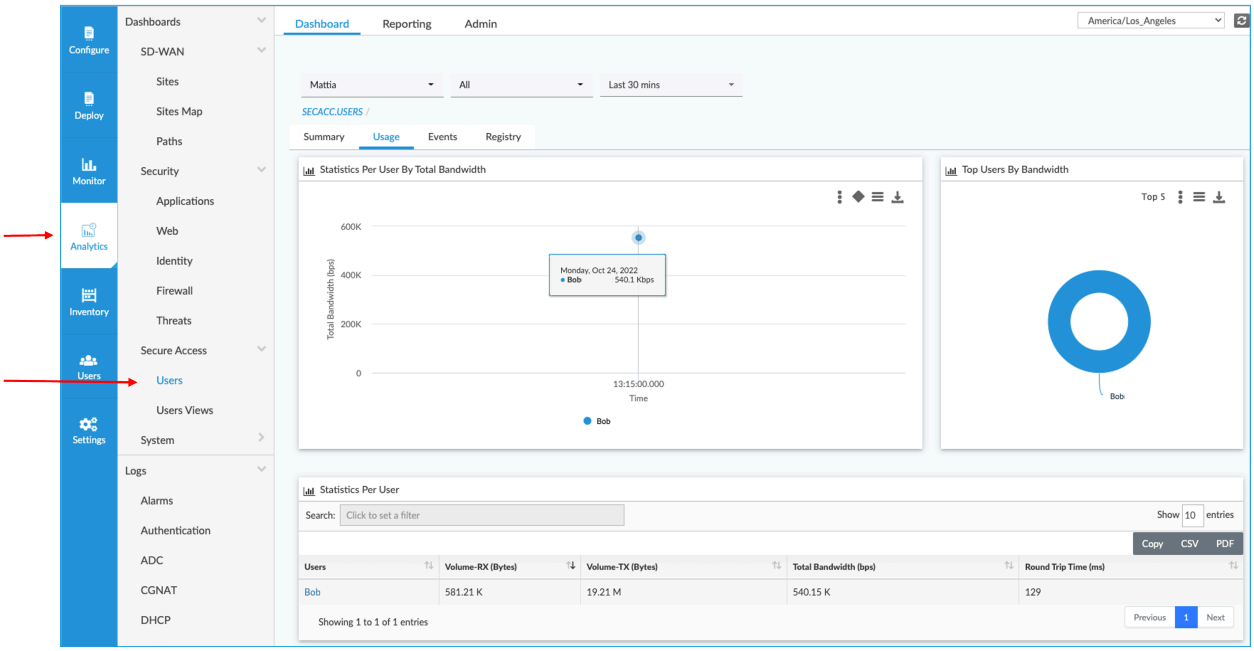
Verification

To monitor and validate user authentication in the SASE portal, click the Analytics tab in the left menu.

- To view user authentication events, go to Logs > Authentication.



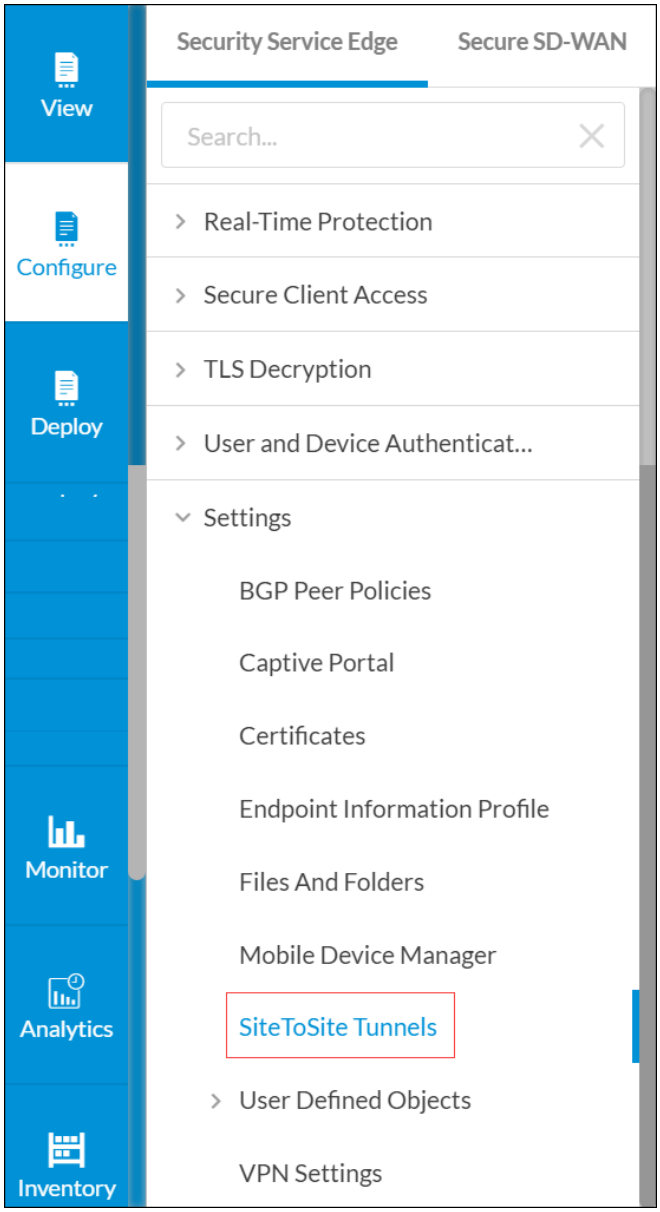
- To view usage and statistics for users, go to Dashboards > Secure Access > Users.



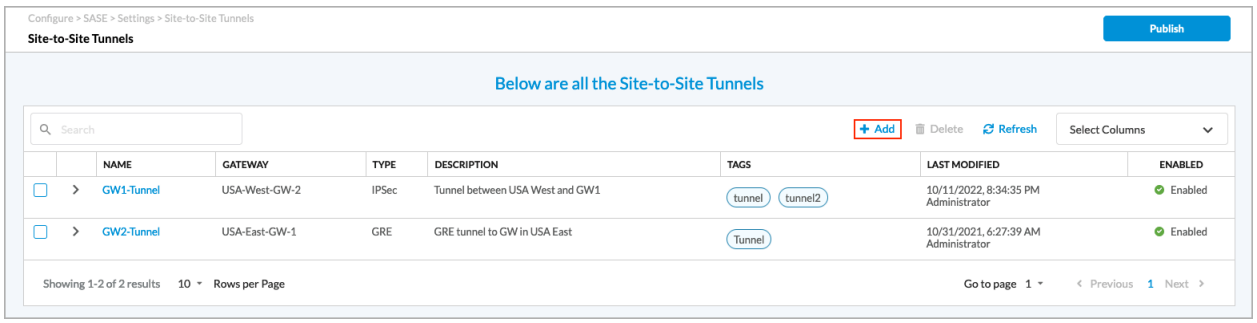
Configure Site-to-Site Tunnels

Site-to-site tunnels establish a Virtual Private Network (VPN) for networking devices to communicate over the public internet with the SSE gateway. This point-to-point private connection allows remote users to securely access private cloud-hosted applications, and allows onsite users to securely access the internet through the Versa SASE platform.

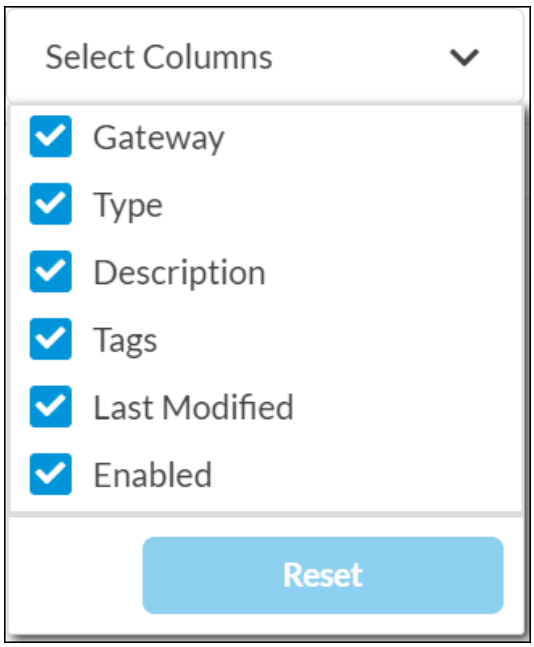
1. Go to Configure > Settings > SiteToSite Tunnels.



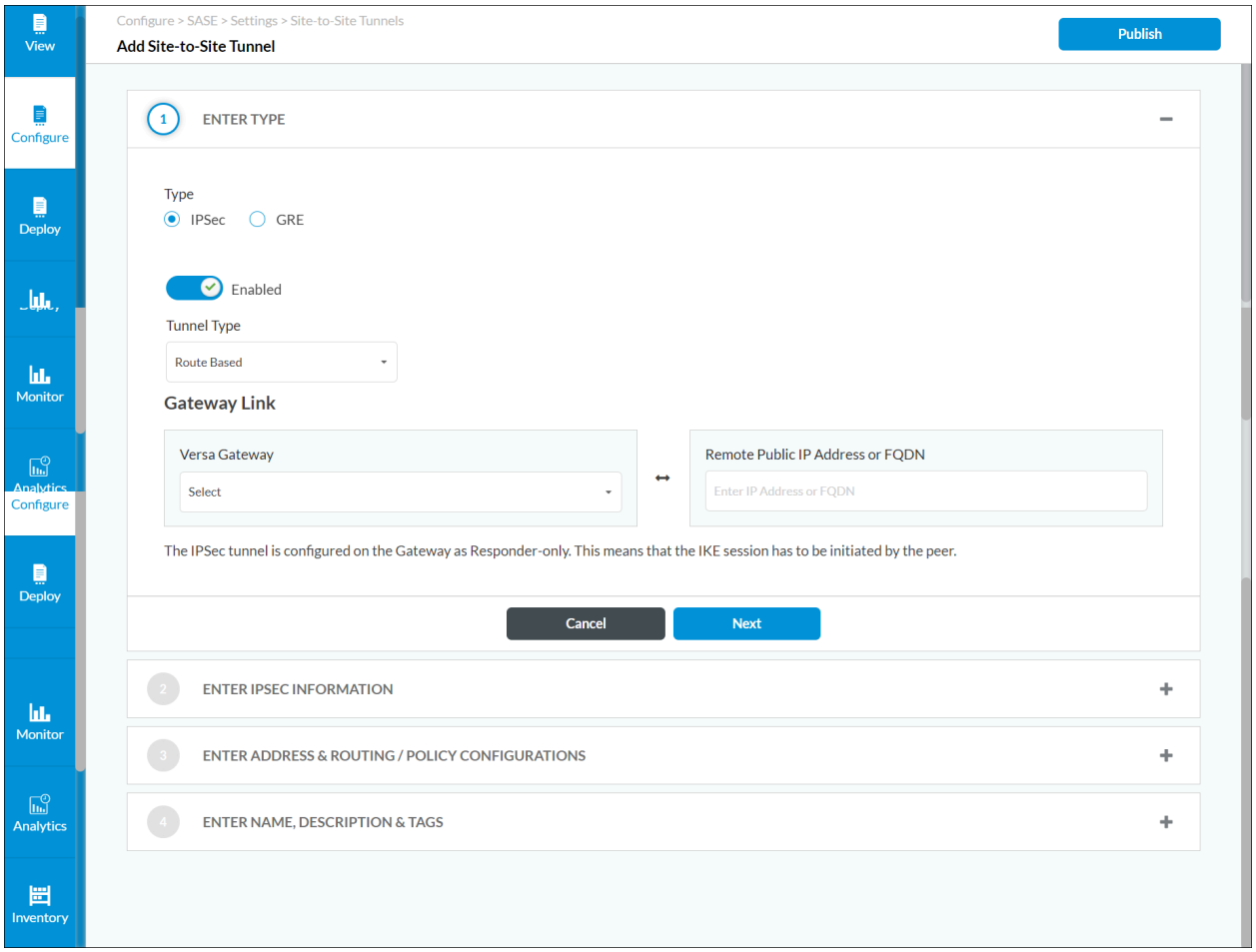
The following screen displays.



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



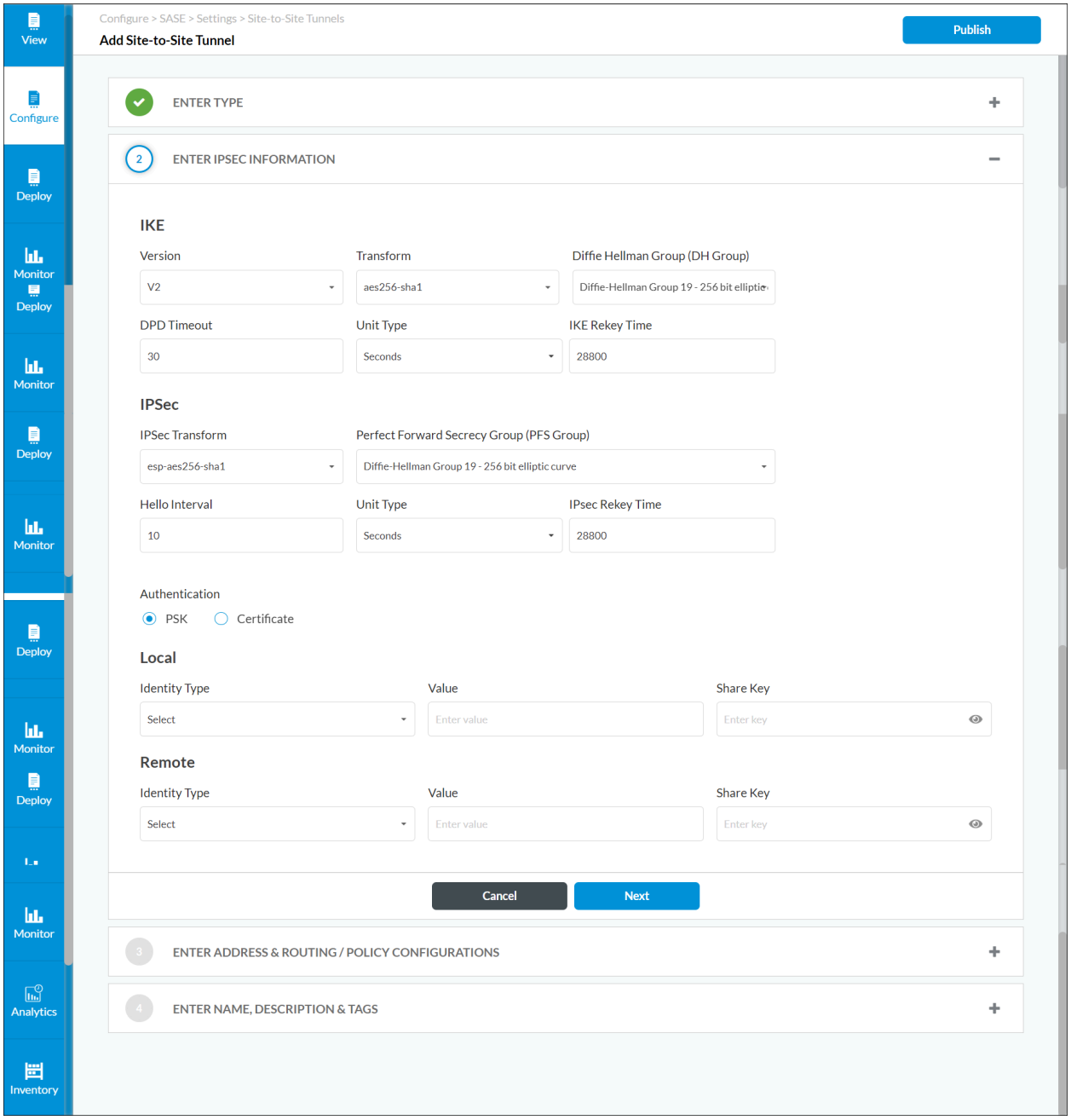
3. Click + Add to create a new tunnel. In the Add Site-to-Site Tunnel screen, enter information for the following fields in the Enter Type section.



Field	Description
Type	Select the tunnel type: ◦ GRE ◦ IPsec (for Releases 11.4.1 and later)
Enabled	Click the slider to enable the tunnel.
Tunnel Type	For the IPsec tunnel type, select the tunnel configuration to use: ◦ Policy-based (for Releases 11.4.1 and later) ◦ Route-based
Gateway Link (Group of Fields)	

Field	Description
◦ Versa Gateway	For an IPsec tunnel type, select a gateway, and then enter the IP address or FQDN of the remote device. For Releases 11.4.1 and later, optionally enter a remote public IP address or FQDN.  For the GRE tunnel type, select a gateway, then select a gateway circuit, and then enter the IP address of the remote device. 

4. Click Next. For the IPsec tunnel type, enter information for the following fields in the Enter IPsec Information section. For the GRE tunnel type, continue with the next step, Enter Address and Routing/Policy Configurations.

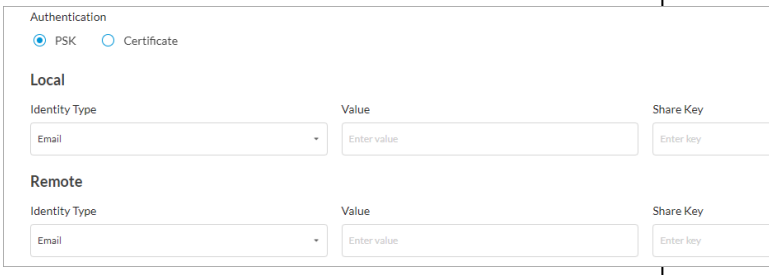


Field	Description
IKE (Group of Fields)	
◦ Version	Select the IKE version: ◦ V1 ◦ V2

Field	Description
	◦ V1 or V2
◦ Transform	Select the IKE transform type to use: ◦ 3des-md5 ◦ 3des-sha1 ◦ aes128-sha1 ◦ aes128-md5 ◦ aes256-sha1 ◦ aes256-md5 ◦ aes128-sha256 ◦ aes256-sha256 ◦ aes128-sha384 ◦ aes256-sha384 ◦ aes128-sha512 ◦ aes256-sha512
◦ Diffie-Hellman Group (DH Group)	Select the Diffie-Hellman group to use: ◦ Diffie-Hellman Group 1—768-bit modulus ◦ Diffie-Hellman Group 2—1024-bit modulus. This is the default. ◦ Diffie-Hellman Group 5—1536-bit modulus ◦ Diffie-Hellman Group 14—2048-bit modulus ◦ Diffie-Hellman Group 15—3072-bit modulus ◦ Diffie-Hellman Group 16—4096-bit modulus ◦ Diffie-Hellman Group 19—256-bit elliptic curve ◦ Diffie-Hellman Group 20—384-bit elliptic curve ◦ Diffie-Hellman Group 21—521-bit elliptic curve ◦ Diffie-Hellman Group 25—192-bit elliptic curve ◦ Diffie-Hellman Group 26—224-bit elliptic curve ◦ No PFS *Default:* Diffie-Hellman Group 2—1024-bit modulus
◦ DPD Timeout	Enter how long to wait for traffic from the destination peer on the tunnel before sending a dead-peer-

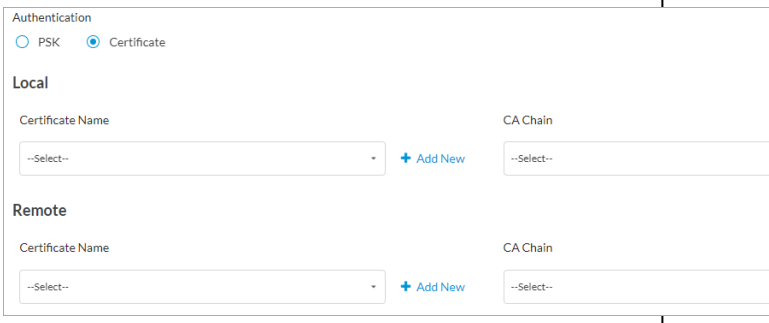
Field	Description
	detection (DPD) request packet. *Range:* 10 through 180 seconds *Default:* 30 seconds
◦ Unit Type	Select the time units for how often to regenerate the IKE key, and then enter the time interval: ◦ Hours ◦ Minutes ◦ Seconds
◦ IKE Rekey Time	Enter how often to regenerate the IKE key. The value range depends on the units you select in the Unit Type field. *Range:* ◦ 132 through 86400, for seconds ◦ 3 through 1440, for minutes ◦ 1 through 24, for hours *Default*: 28800 seconds
IPsec (Group of Fields)	
◦ IPsec Transform	Select the IPsec transform type to use: ◦ esp-3des-md5 ◦ esp-3des-sha1 ◦ esp-aes128-ctr-sha1 ◦ esp-aes128-ctr-xcbc ◦ esp-aes128-gcm ◦ esp-aes128-md5 ◦ esp-aes128-sha1 ◦ esp-aes128-sha256 ◦ esp-aes128-sha384 ◦ esp-aes128-sha512 ◦ esp-aes256-gcm

Field	Description
	◦ esp-aes256-md5 ◦ esp-aes256-sha1 ◦ esp-aes256-sha256 ◦ esp-aes256-sha384 ◦ esp-aes256-sha512 ◦ esp-null-md5
◦ Perfect Forward Secrecy Group (PFS Group)	Select the Diffie-Hellman groups to use for PFS: ◦ Diffie-Hellman Group 1—768-bit modulus ◦ Diffie-Hellman Group 2—1024-bit modulus. ◦ Diffie-Hellman Group 5—1536-bit modulus ◦ Diffie-Hellman Group 14—2048-bit modulus ◦ Diffie-Hellman Group 15—3072-bit modulus ◦ Diffie-Hellman Group 16—4096-bit modulus ◦ Diffie-Hellman Group 19—256-bit elliptic curve ◦ Diffie-Hellman Group 20—384-bit elliptic curve ◦ Diffie-Hellman Group 21—521-bit elliptic curve ◦ Diffie-Hellman Group 25—192-bit elliptic curve ◦ Diffie-Hellman Group 26—224-bit elliptic curve ◦ No PFS. This is the default. *Default*: No PFS
◦ Hello Interval	Enter the IPsec keepalive timeout, which is how often to send a Hello message to the peer to determine whether the peer is still up and operational. *Range*: 0 through 36000 seconds *Default*: 10 seconds
◦ Unit Type	Select the time units for how often to regenerate the IPsec key, and then enter the time interval: ◦ Hours ◦ Minutes ◦ Seconds

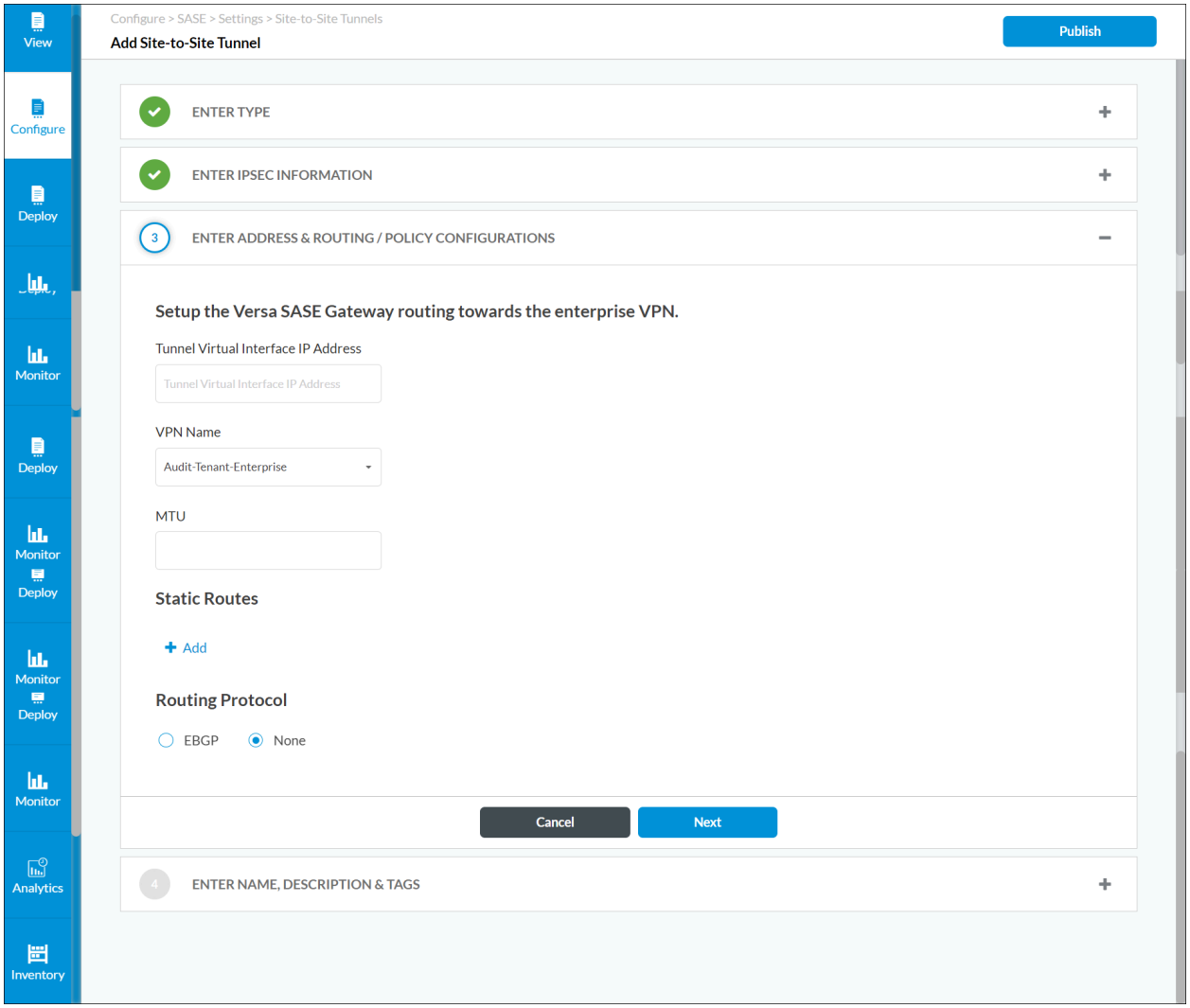
Field	Description
	Default: Seconds
◦ IPsec Rekey Time	Enter how often to regenerate the IPsec key. The value range depends on the units you select in the Unit Type field. *Range*: ◦ 132 through 86400, for seconds ◦ 3 through 1440, for minutes ◦ 1 through 24, for hours *Default*: 28800 seconds
◦ Authentication	Select the authentication: ◦ Certificate Authentication ◦ PSK
◦ Local—PSK Authentication (Group of Fields)	For PSK authentication, enter information for the following fields: 

Field	Description
Local (Group of Fields)	
◦ Identity Type	Select an identity type:

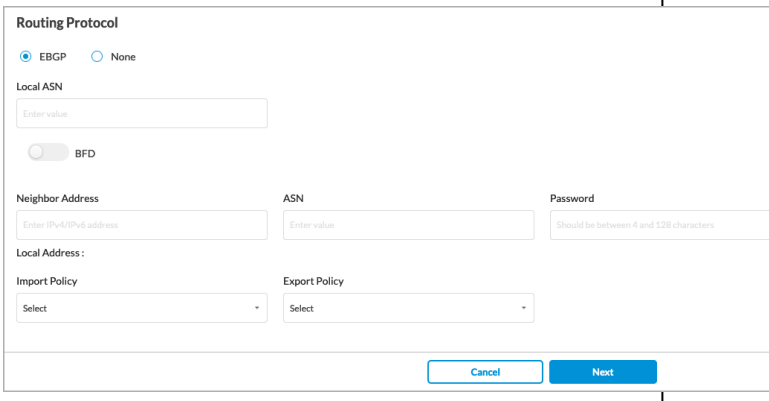
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>◦ Email
◦ FQDN
◦ IP address</td></tr>
<tr><td>◦ Value</td><td>Enter a value for the identity type:
◦ Email—Enter a valid email address.
◦ FQDN—Enter a valid FQDN.
◦ IP Address—Enter a valid IP address.</td></tr>
<tr><td>◦ Share Key</td><td>Enter the share key for the local devices.</td></tr>
<tr><td colspan="2">Remote (Group of Fields)</td></tr>
<tr><td>◦ Identity Type</td><td>Select an identity type:
◦ Email
◦ FQDN
◦ IP address</td></tr>
<tr><td>◦ Value</td><td>Enter a value for the identity type:
◦ Email—Enter a valid email address.
◦ FQDN—Enter a valid FQDN.
◦ IP Address—Enter a valid IP address.</td></tr>
<tr><td>◦ Share Key</td><td>Enter the share key for the remote devices.</td></tr>
</table>
</td></tr>
</table>

Field	Description
◦ Local—Certificate Authentication (Group of Fields)	For Certificate Authentication, enter information for the following fields:  ◦ Certificate Name—Select a certificate name for both the local and remote devices. ◦ CA Chain—Select a CA chain for both the local and remote devices. Click + Add New to add new certificates names and CA chains for the local and remote devices. Fore more information, see Configure SASE Certificates.

5. Click Next.
6. For the GRE tunnel type and for a route-based tunnel configuration for an IPsec tunnel type, enter information for the following fields in the Enter Address and Routing/Policy Configurations section, and then continue with Step 8. Note that Enter IPsec Information section is not applicable for GRE tunnel type. For the Policy-based tunnel configuration for an IPsec tunnel type, continue with Step 7.

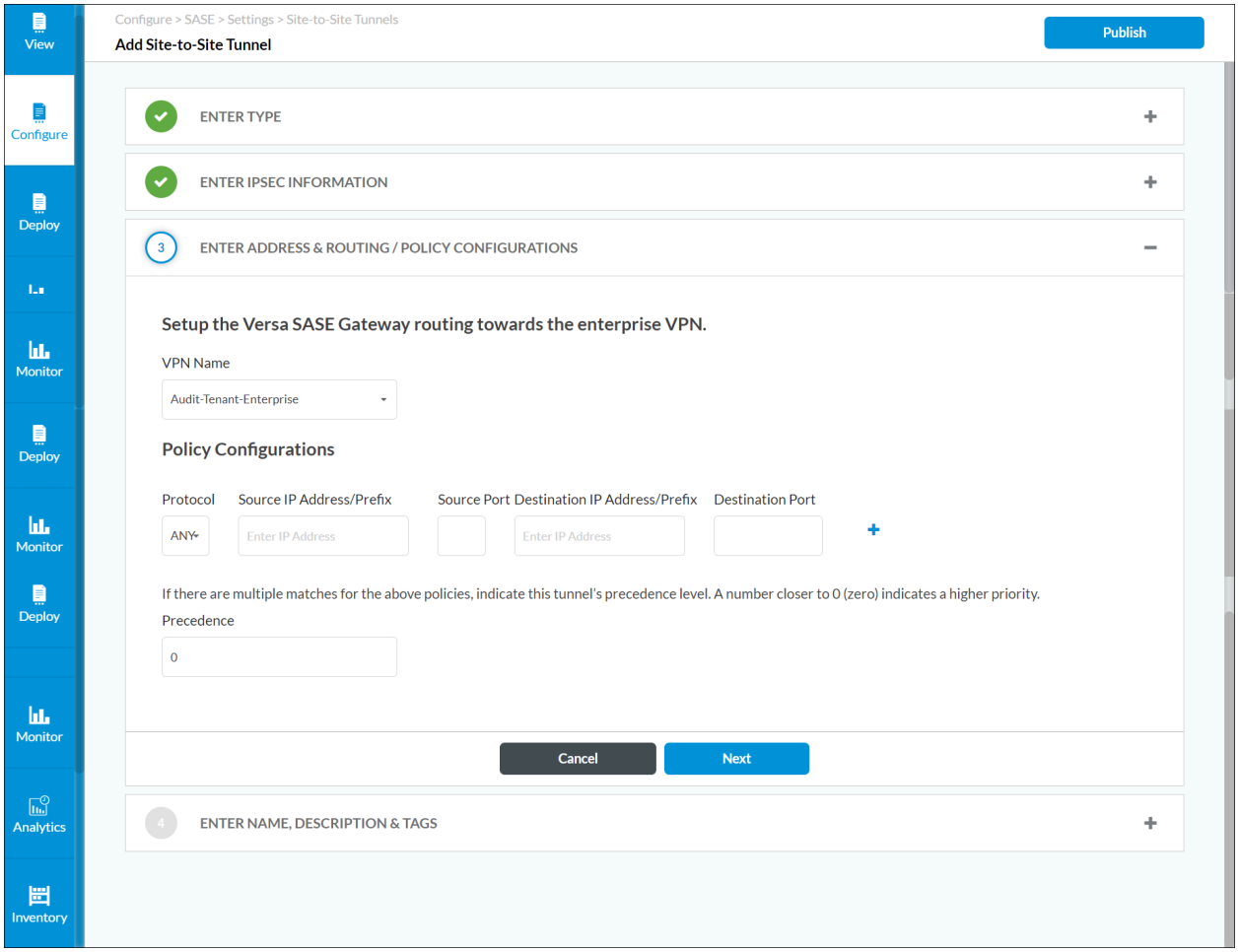


Field	Description
Tunnel Virtual Interface IP Address	Enter the tunnel virtual interface IP address.
VPN Name	Select the VPN through which the IP address is reachable.
MTU	(For Releases 11.4.1 and later.) Enter the maximum transmission unit size, in bytes, of the largest protocol data unit that the port can receive or transmit. *Range:* 256 through 9000 bytes
Static Routes (Group of Fields)	

Field	Description
◦ + Add	Click to add a static route. Enter information for the following fields.  ◦ IPv4 Destination—Enter the IPv4 destination address. ◦ Preference—Enter a preference value for the static route. *Range*: 1 through 255 *Default*: None ◦ Minus icon—Click to delete a static route entry. ◦ Plus icon—Click to add a static route entry.
Routing Protocol	Select the routing protocol: ◦ EBGP ◦ None If you select None, no further information is required. If you select EBGP, enter information for the following fields. 

Field	Description
	◦ Local ASN—Enter the local AS number. ◦ BFD—Click the slider to enable Bidirectional Forwarding (BFD). ◦ Neighbor Address—Enter the IP address of the peer device. ◦ ASN—Enter the AS number of the peer device. ◦ Password—Enter the password for the peer device. ◦ Local Address (Group of Fields)— ▪ Import Policy—(Optional) Select an EBGP import policy from the drop-down list. ▪ Export Policy—(Optional) Select an EBGP export policy from the drop-down list. For information about creating import and export policies, see Configure SASE BGP Peer Policies

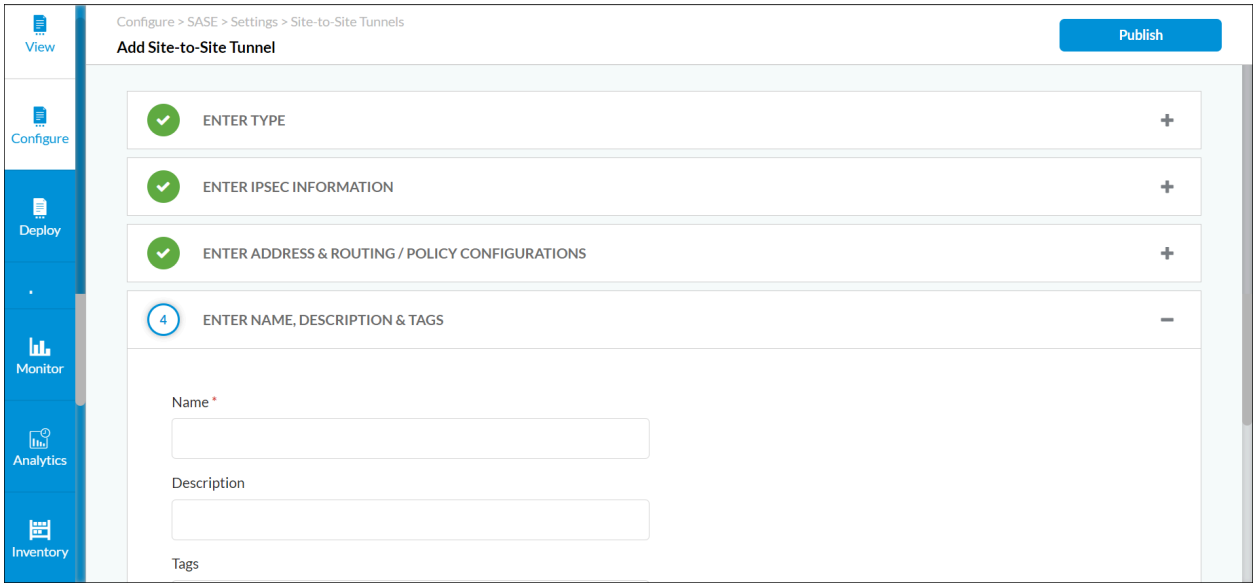
7. (For Releases 11.4.1 and later.) For the policy-based tunnel configuration for an IPsec tunnel type, enter information for the following fields.



Field	Description
VPN Name	Select the VPN through which the IP address is reachable.
Policy Configurations (Group of Fields)	
◦ Protocol	Select a protocol: ◦ Any ◦ ICMP ◦ TCP ◦ UDP
◦ Source IP Address/Prefix	Enter the IPv4 source prefix.

Field	Description
◦ Source Port	Enter the source port number. *Range:* 0 through 65535
◦ Destination IP Address/Prefix	Enter the IPv4 destination prefix.
◦ Destination Port	Enter the destination port number. *Range:* 0 through 65535
◦ Precedence	If there are multiple matches for the policies, indicate the precedence level of the tunnel. A number closer to 0 indicates a higher priority. *Range:* 0 through 512

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



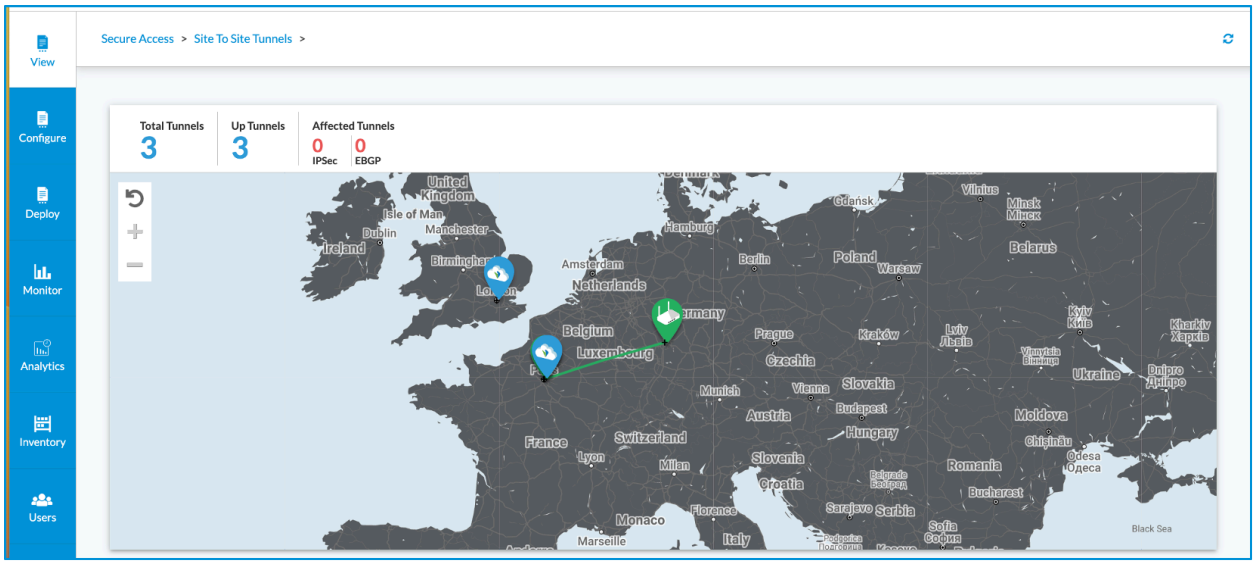
Field	Description
Name (Required)	Enter a name for the tunnel.

Field	Description
Description	Enter a description for the tunnel.
Tags	Enter one or more tags for the tunnel.

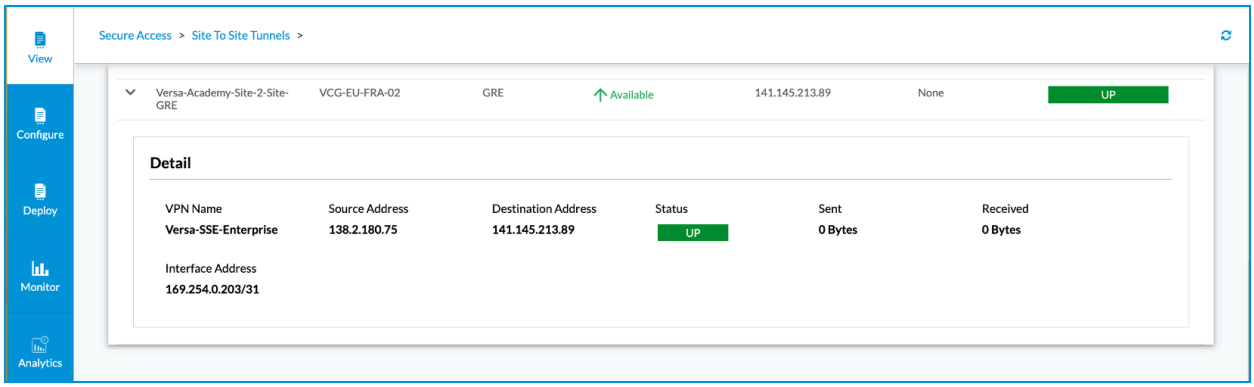
10. Click Save.

Verification

To verify site-to-site tunnel status information, click the View tab in the left menu, and then go to Secure Access > Site-to-Site Tunnels.



Site-to-site tunnel details displays tunnel name, gateway connected to, type of tunnel, status, destination IP address, type of routing, and routing status.



Configure Versa Secure Client Access Policies

Versa secure client access policies define the conditions and authorization for remote users when connecting to the SSE service. When a user registers the SASE client, the SASE portal checks for a secure client access policy, matches the user to a policy based on identity and context, and downloads the appropriate SASE client configuration. Depending on their end-device security posture, access location, or compliance state, the user may get restricted access to the network. The scope of access is defined by the secure client access policy.

The portal policy is looked up based on a match criteria which could include user location, device posture, etc. Once a portal policy match is found, the sase client configuration is downloaded and applied to the sase client.

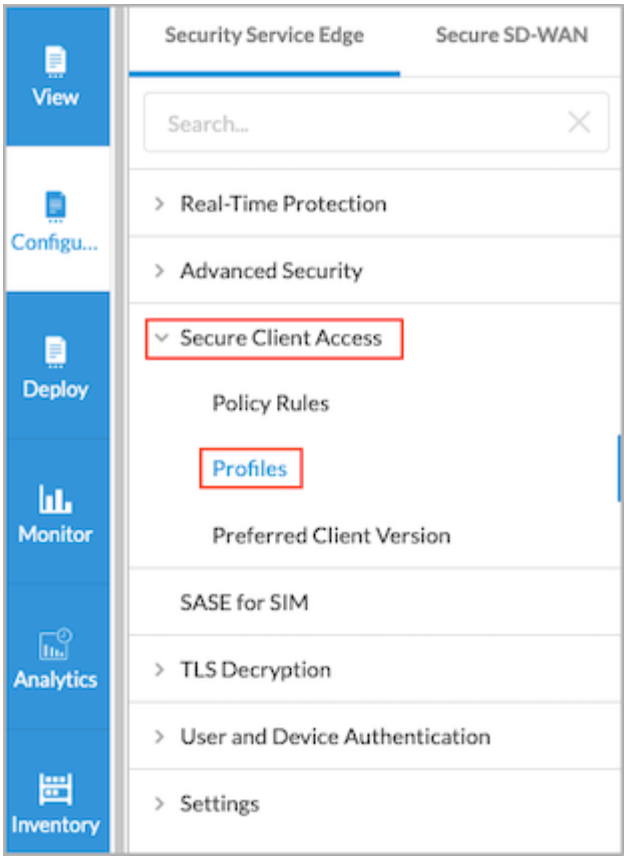
To configure Versa secure client access policies, you do the following:

1. Configure secure client access profiles.
2. Configure secure client access rules.

Configure Secure Client Access Profiles

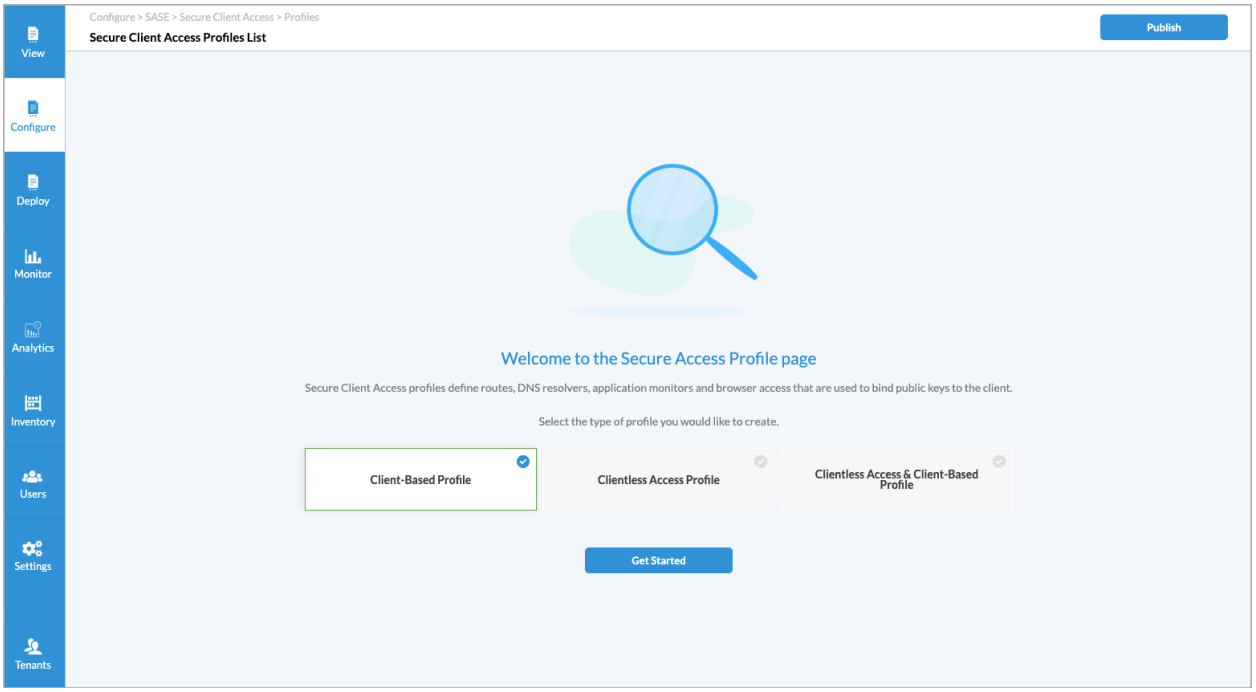
To configure SASE secure client access application monitors, browser access, DNS resolvers, and routes:

1. Go to Configure > Security Service Edge > Secure Client Access > Profiles.

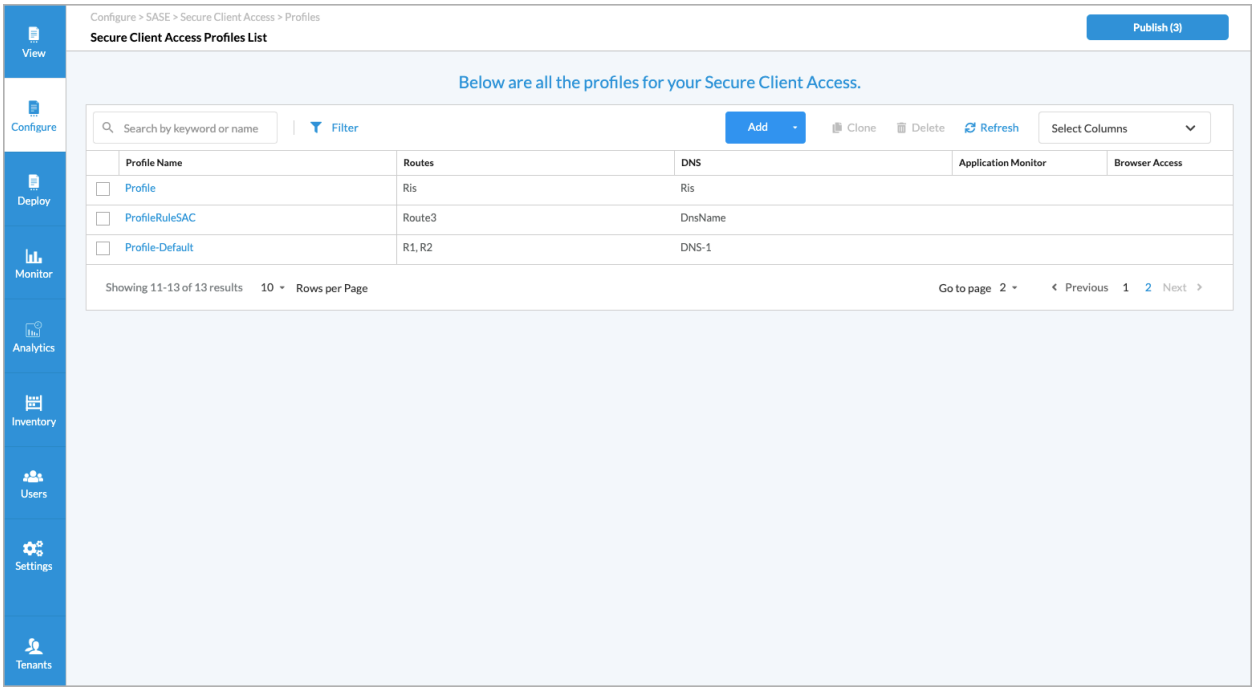


If you have not configured a secure access client profile, the Welcome to the Secure Access Profile page displays. On this page, you can choose to configure one of the following types of profiles:

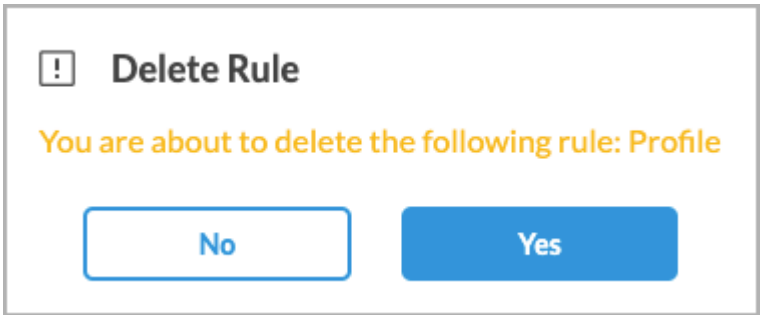
- Client-based profile
- Clientless access profile
- Both client-based and clientless access profile



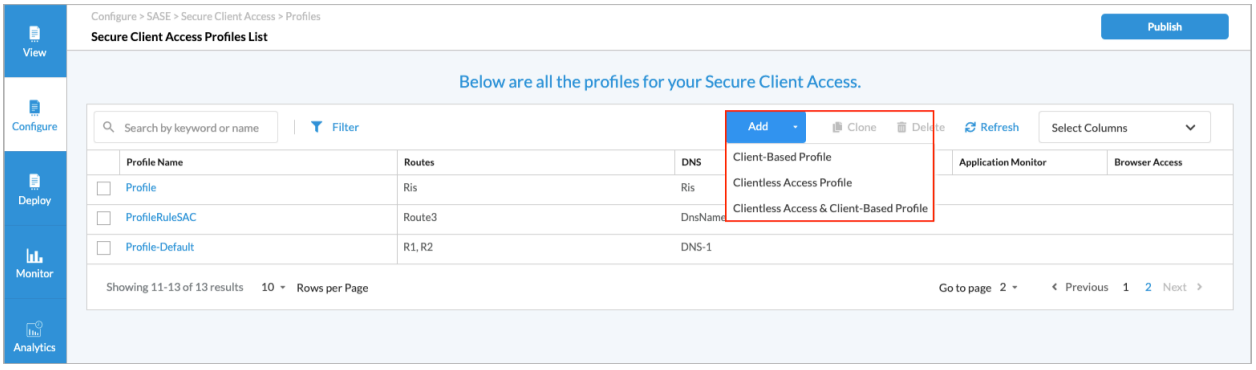
If you have configured one or more secure access client profiles, the Secure Client Access Profile List screen displays the profiles that are already configured.



2. In the horizontal menu bar, you can select one of the following operations.

Operation	Description
Add	Create a new secure client access profile. This button is active when no existing
Clone	Clone the selected secure client access profile. When you click Clone, the confi configuration. In the Review & Deploy screen, rename the default name of the c
Delete	Delete the selected access control policy. A popup window similar to the followir  Click Yes to delete the profile, or click No to retain the profile.
Refresh	Refresh the list of existing policies.
Select Columns	To select the columns that you want to display, click the down arrow. To return t

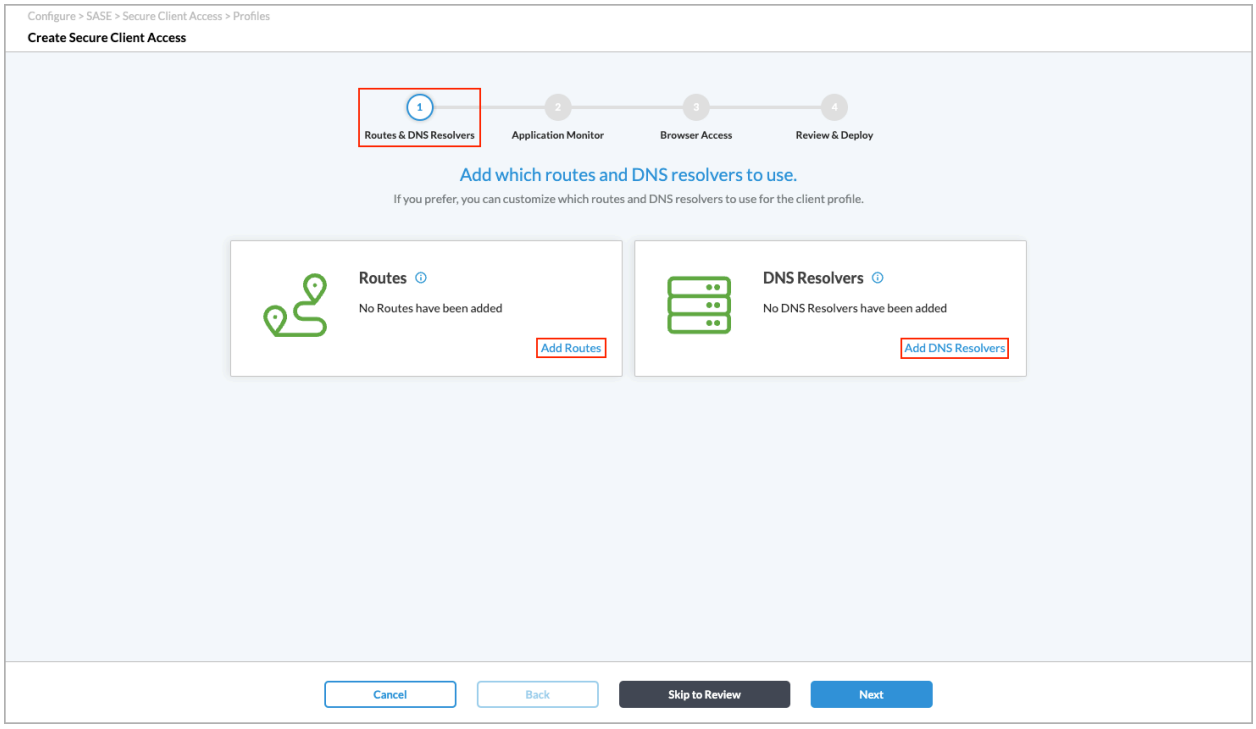
3. To edit an existing profile, click the profile name, edit the entries as needed, and then click Save.
4. To configure a new profile, click the + Add icon, then select a type of profile to create, and then click Next.



   - Client-Based Profile—You are then prompted to configure routes, DNS resolvers and applications for monitoring. Then you are prompted to review and deploy the profile.

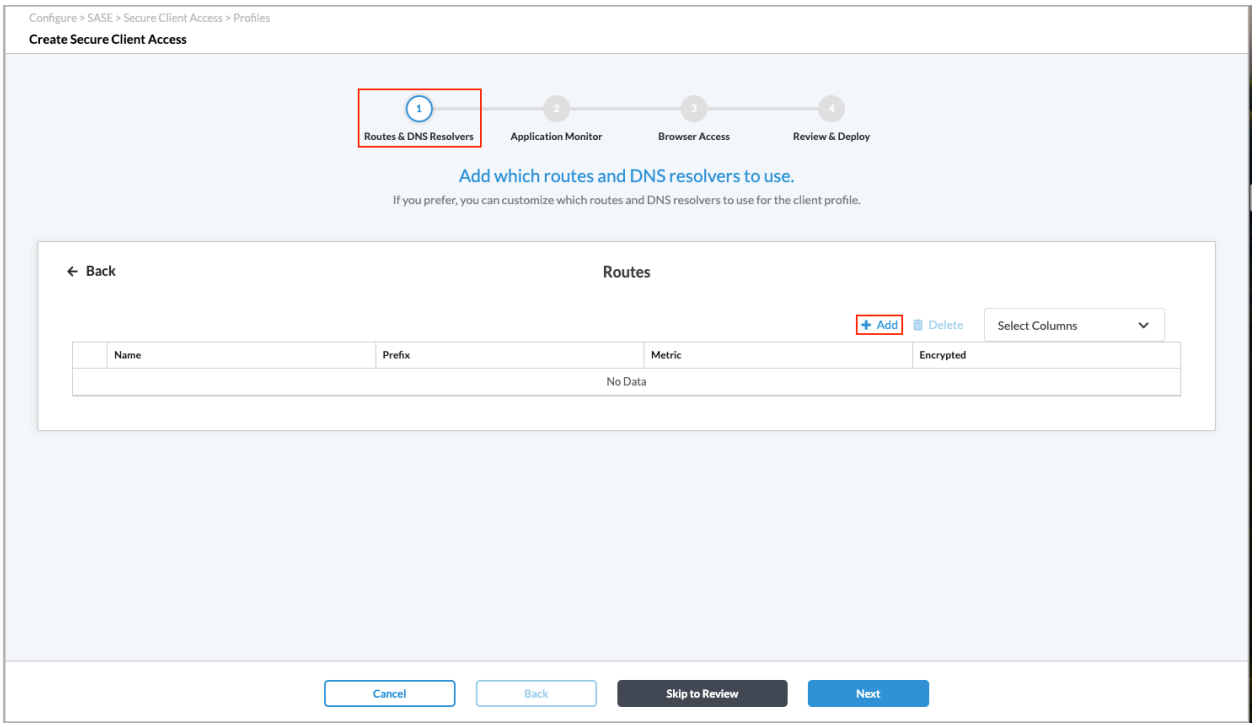
- Clientless Access Profile—For browser access, you are prompted to select custom and predefined applications for clientless VPN access. Then you are prompted to review and deploy the profile.

- Clientless Access & Client-Based Profile—You are prompted to configure routes, DNS resolvers, applications for monitoring, and custom and predefined applications for clientless VPN access. Then you are prompted to review and deploy the profile.

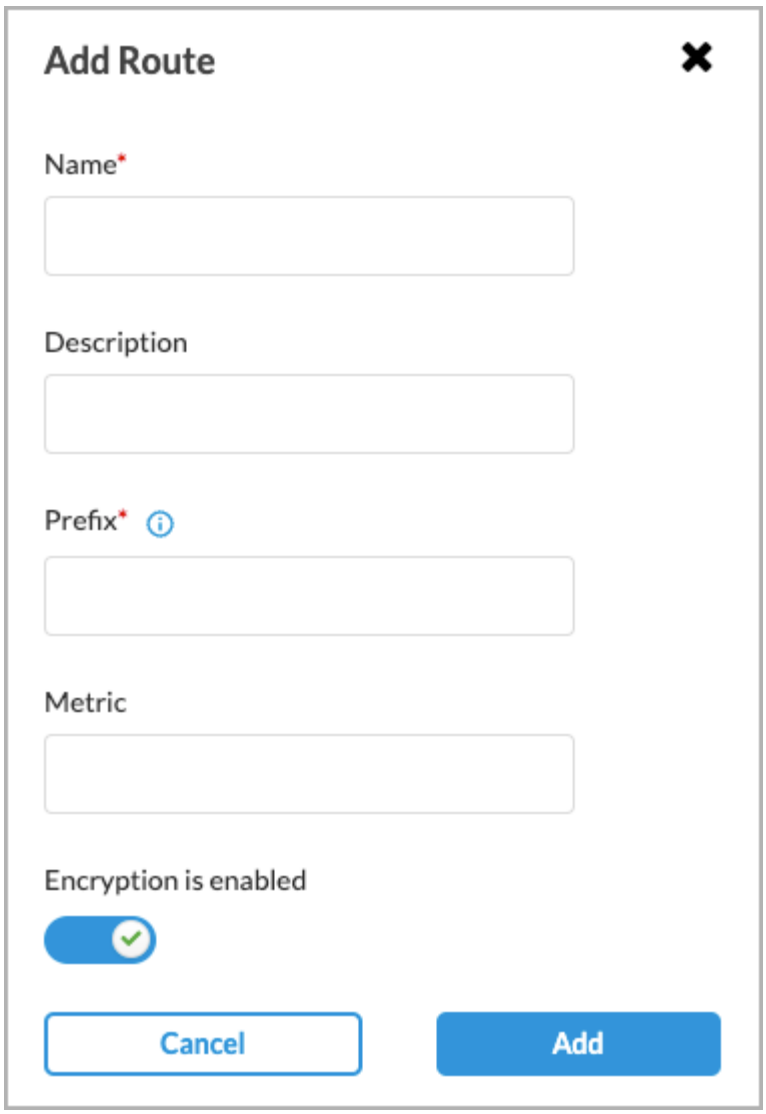


Note: The remaining steps in this procedures show how to configure both a client-based and a clientless access profile. To configure only a client-based or only a clientless access profile, follow the same procedure, performing only the relevant steps.

5. In Step 1, Routes and DNS Resolvers, click Customize in the Routes pane to add routes to the profile. Routes are prefixes that can be reached over the remote access VPN. The Routes pane displays the routes that are already configured.



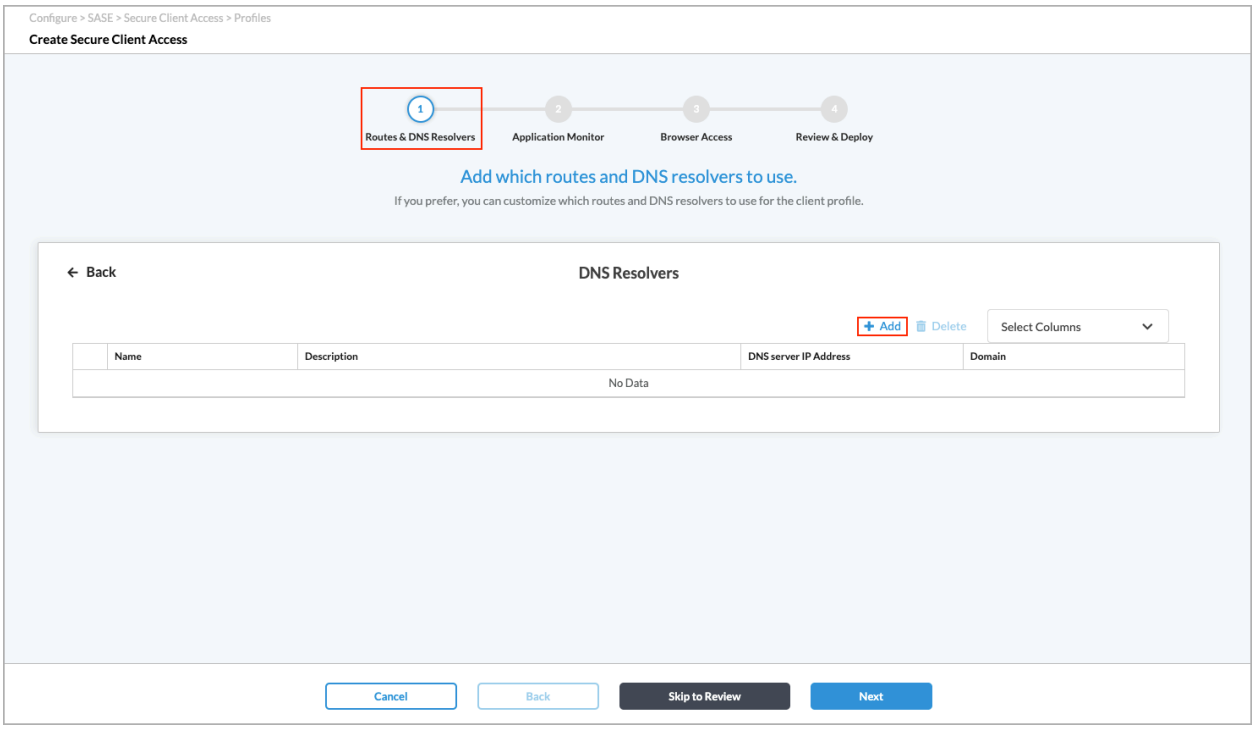
6. Click + Add to add a new route. In the Add Route popup window, enter information for the following fields.



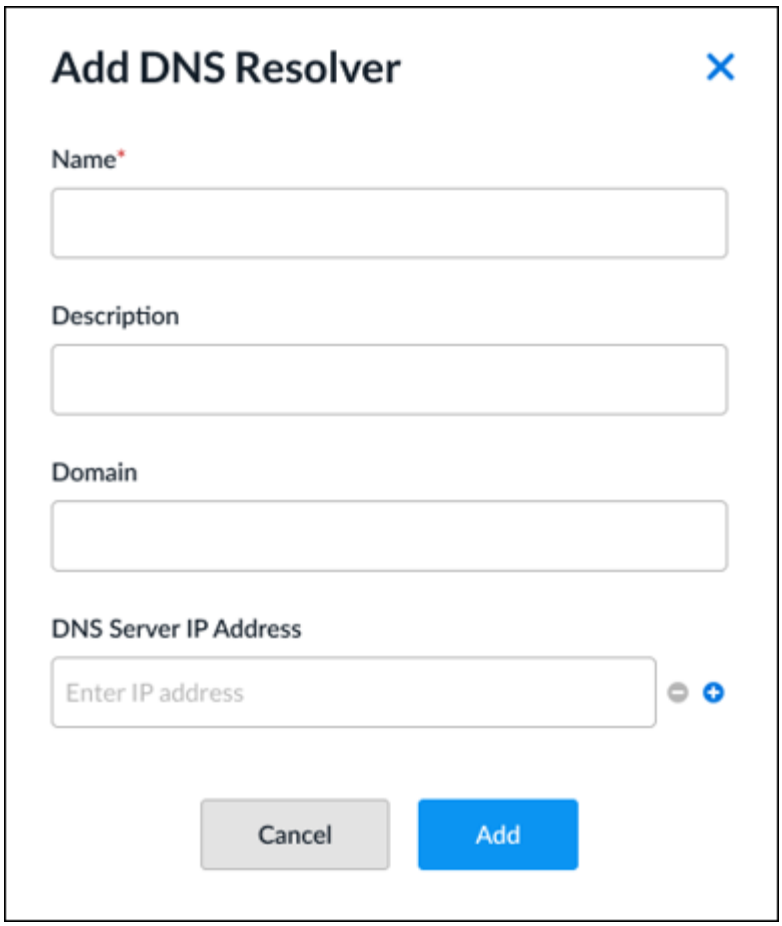
Field	Description
Name Required)	Enter a name for the route.
Description	Enter a text description for new route.
Prefix (Required)	Enter a prefix for the route. By default, if you are using Versa Secure Internet Access (VSIA), the 0.0.0.0/0 subnet is advertised to the client. If you are using Versa Secure Private Access (VSPA), the prefix must be in the private access subnet range as defined in RFC 1918 (10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16).
Metric	Enter a value for the route metric.

Field	Description
	Range: 0 through 4294967295 *Default*: None
Encryption	Select to encrypt the route and to route the traffic for applications and domains to an encrypted tunnel. By default, encryption is enabled.  To disable encryption, click the slider.  If you disable encryption, traffic is routed on an encrypted or non-encrypted (clear-text) route, depending on the configuration, for applications and domains. If the route is not encrypted, the Versa secure client access creates two tunnels, encrypted and clear text, and then routes traffic. In this case, you might consider securing the application using a different method, such as SSL/TLS.

7. Click Add. The Routes screen displays the new route.
8. Click Back. The Routes and DNS resolvers screen displays.
9. To add DNS resolvers to the profile, click Customize in the DNS Resolvers pane. The DNS Resolvers screen displays the DNS resolvers that are already configured.

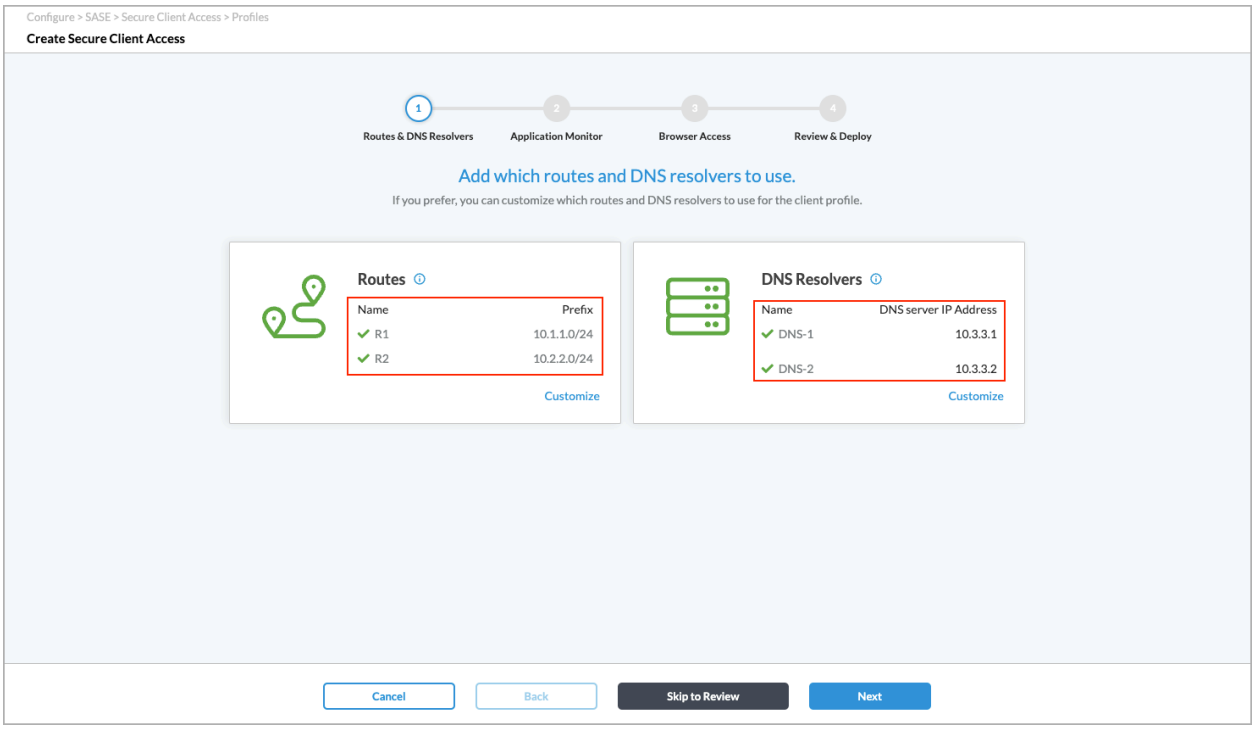


10. Click + Add to add a new DNS resolver. In the Add DNS Resolver popup window, enter information for the following fields.

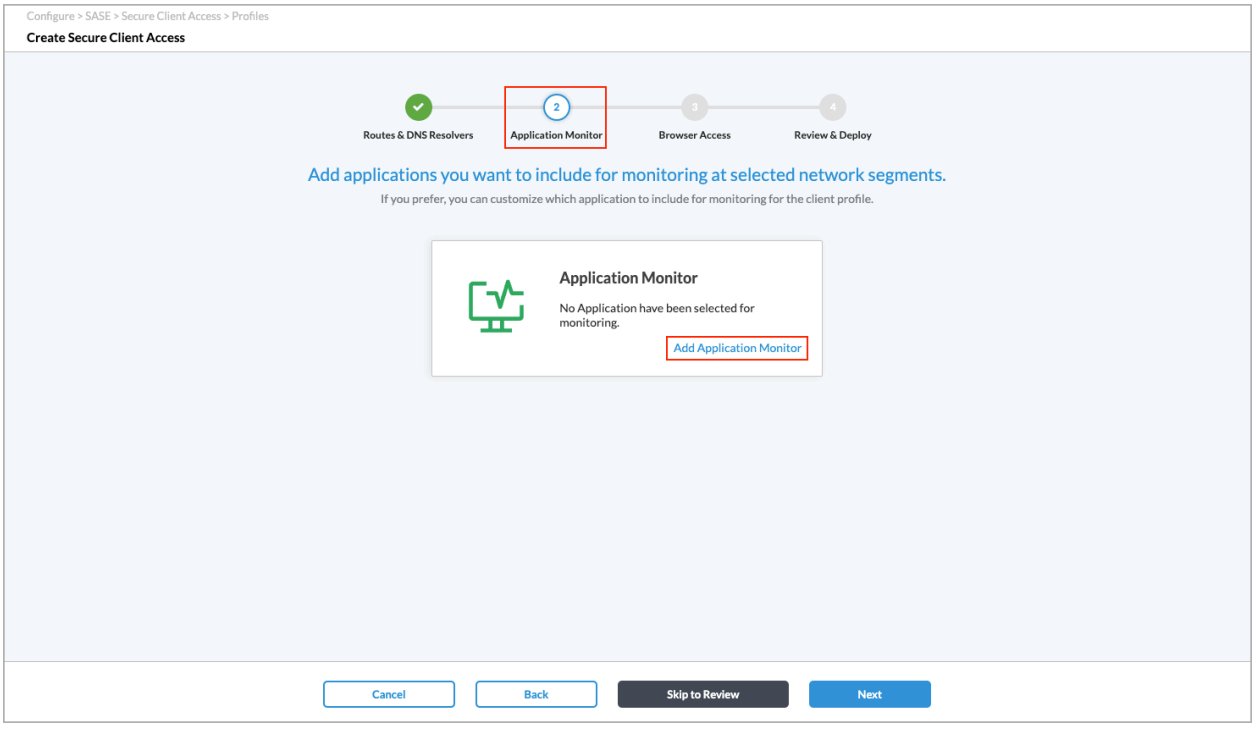


Field	Description
Name	Enter a name for the DNS resolver.
Description	Enter a text description for the DNS resolver.
Domain	Enter a valid domain name for the DNS resolver to send to the client. The client uses the DNS resolver to perform DNS lookups for all traffic.
DNS Server IP Address	Enter a valid IP address for the DNS server. To enter additional addresses, click the Plus icon.

11. Click Add to add the new DNS resolver to the secure client access profile. The DNS Resolvers screen displays the new DNS resolver.
12. Click Back. The Routes and DNS resolvers screen displays the routes and DNS resolvers that you added.

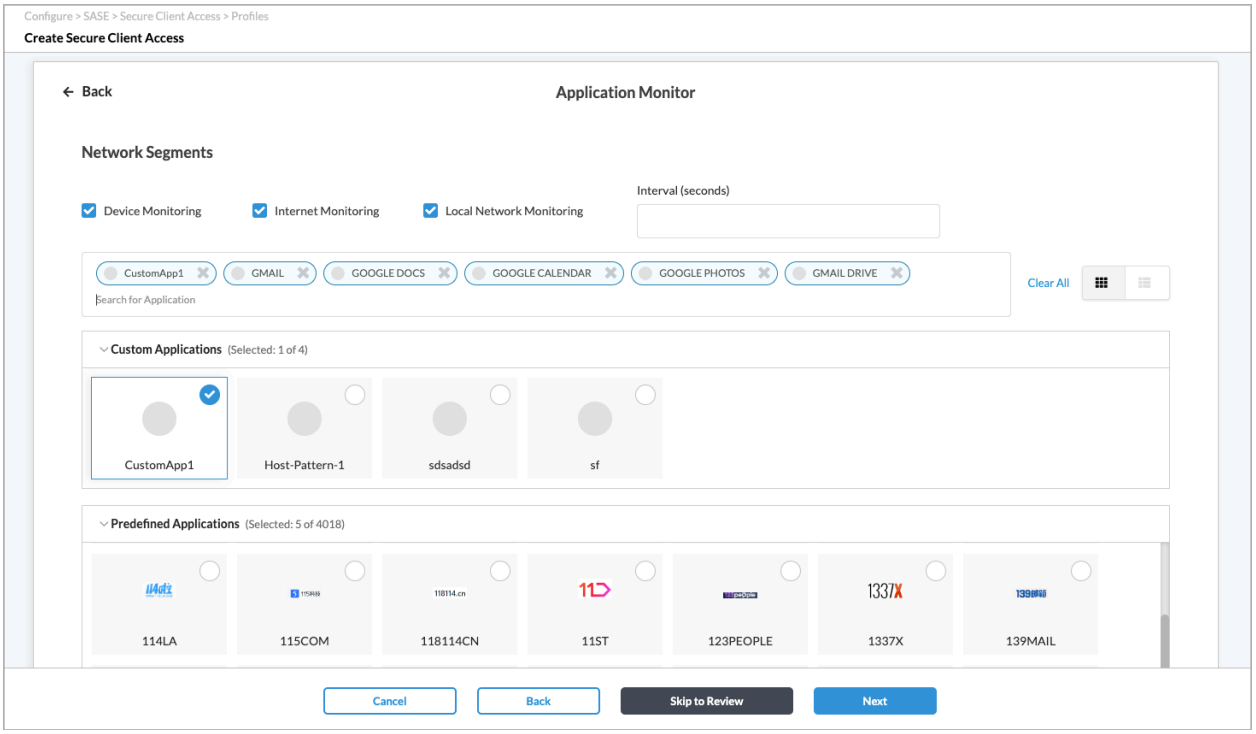


13. Click Next to continue to Step 2, Application Monitor. To configure DEM, click Customize in the Application Monitor pane.



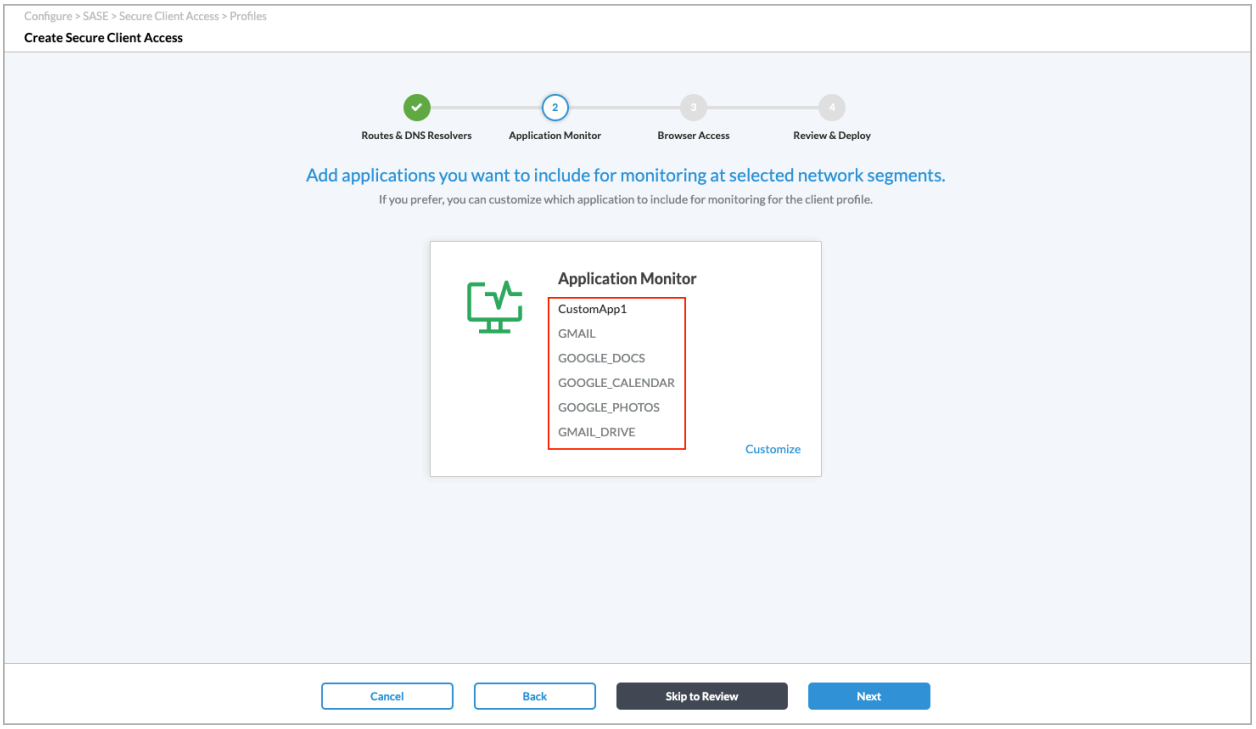
14. In the Application Monitor screen, enter information for the following fields. These parameters are downloaded to

the SASE client when a user registers the client with the SASE client portal.

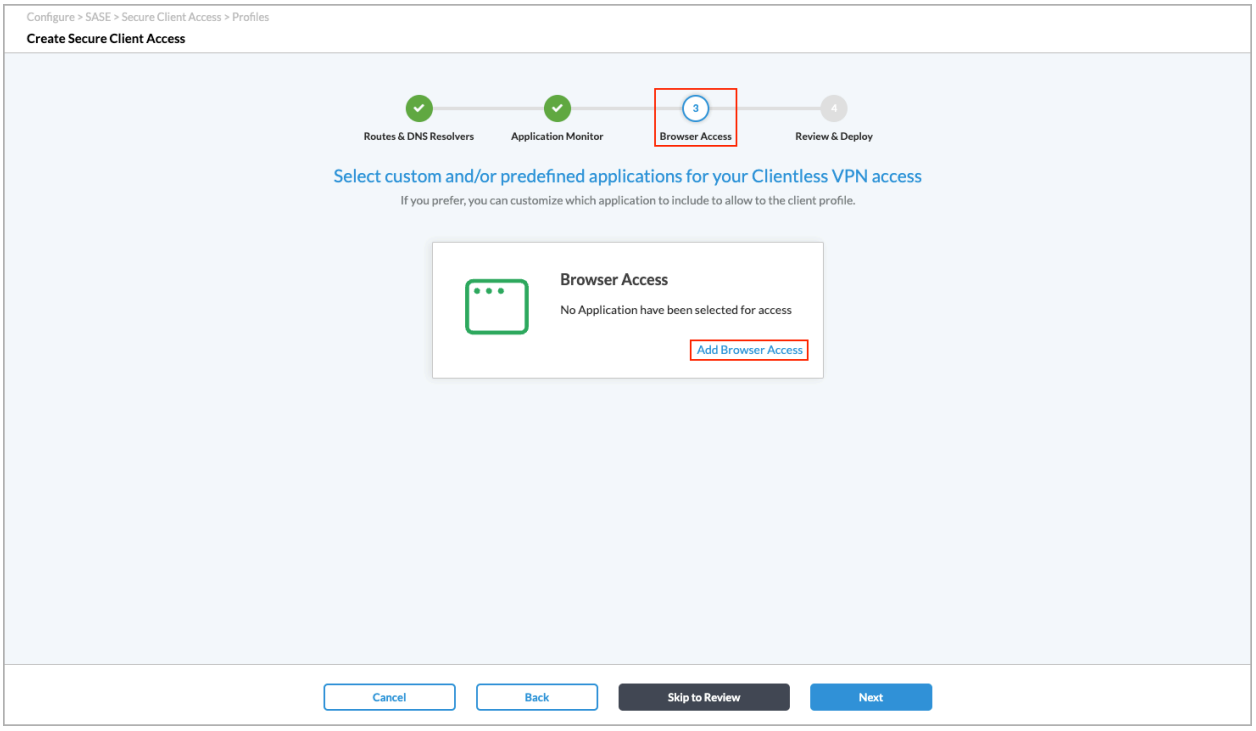


Field	Description
Network Segments (Group of Fields)	
◦ Device Monitoring	Click to monitor the health of devices, including memory, CPU, disk utilization, and battery life.
◦ Internet Monitoring	Click to monitor internet performance, including delay, hops, hop-by-hop latency, jitter, and packet loss.
◦ Local Network Monitoring	Click to monitor the performance of the local network, including latency, jitter, packet loss, WiFi SSID, and signal strength.
◦ Interval	Enter how often to monitor an application, in seconds.
Application Monitoring (Group of Fields)	
◦ Custom Applications	Select one or more user-defined applications.
◦ Predefined Application	Select one or more predefined applications.

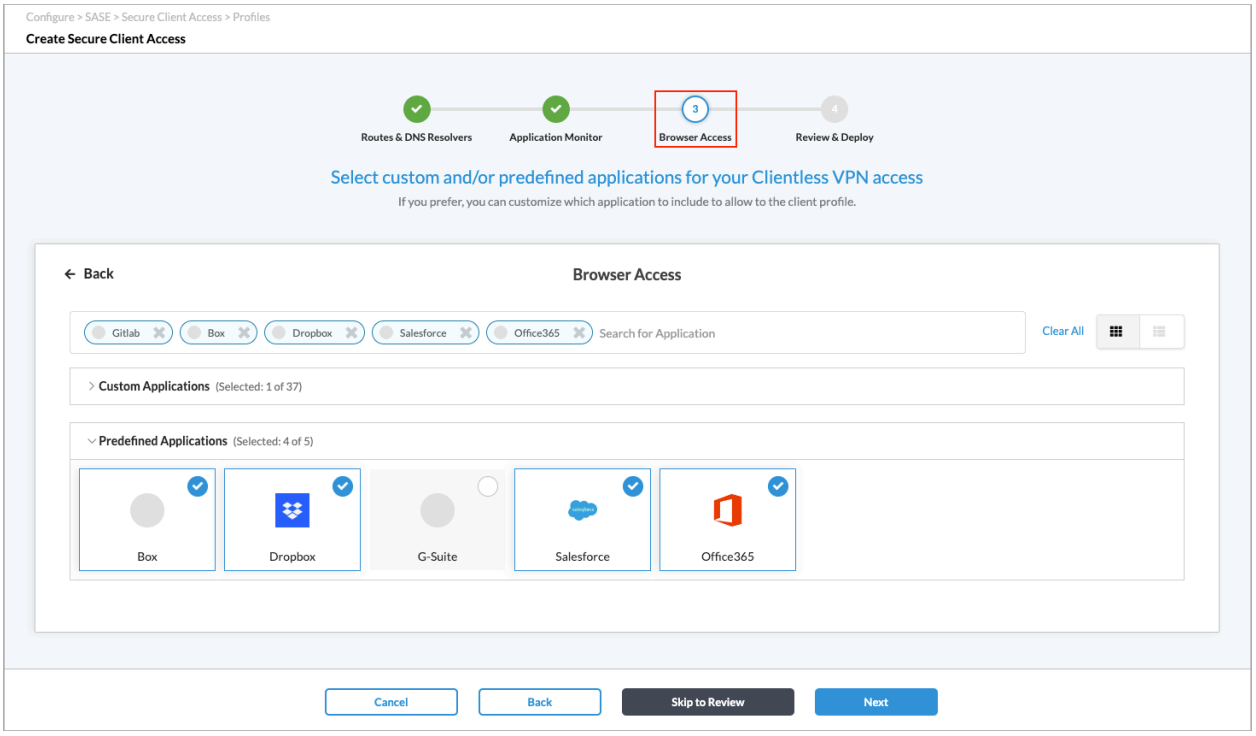
15. Click Back. The Application Monitor screen displays the applications that you added.



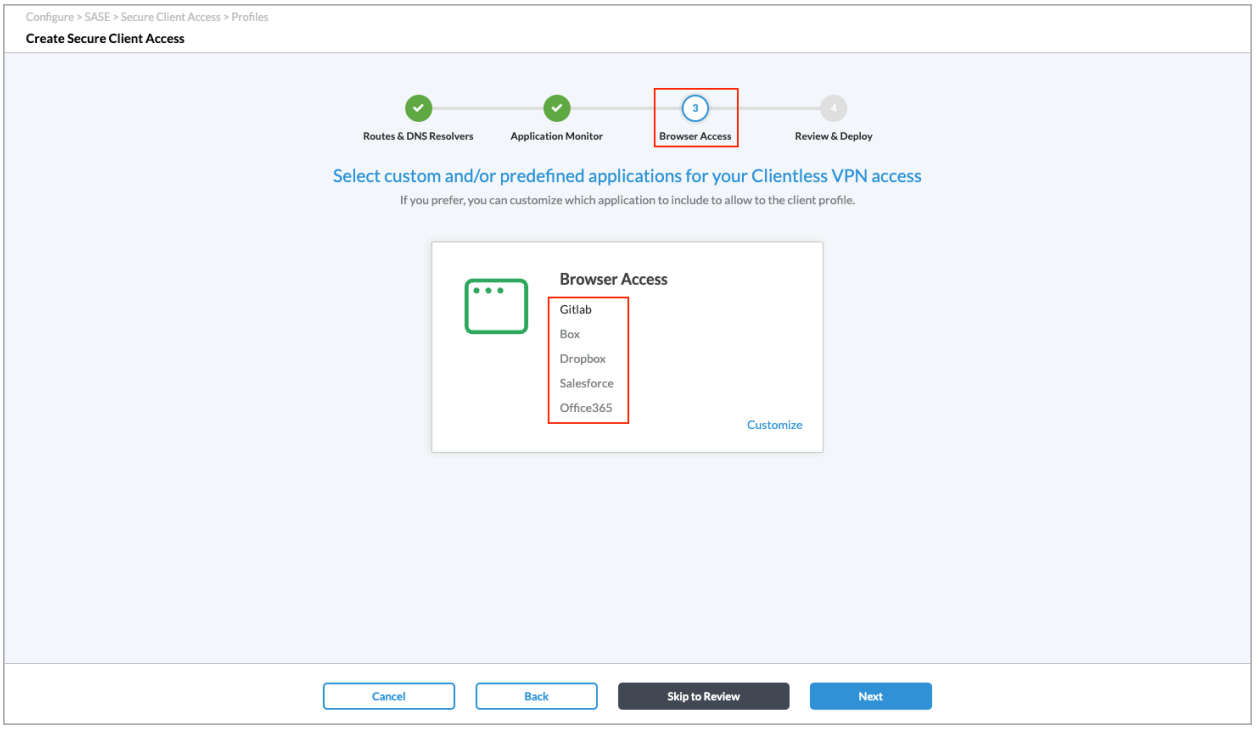
16. Click Next to continue to Step 3, Browser Access. To select custom and predefined applications for clientless VPN access, click Customize in the Browser Access pane.



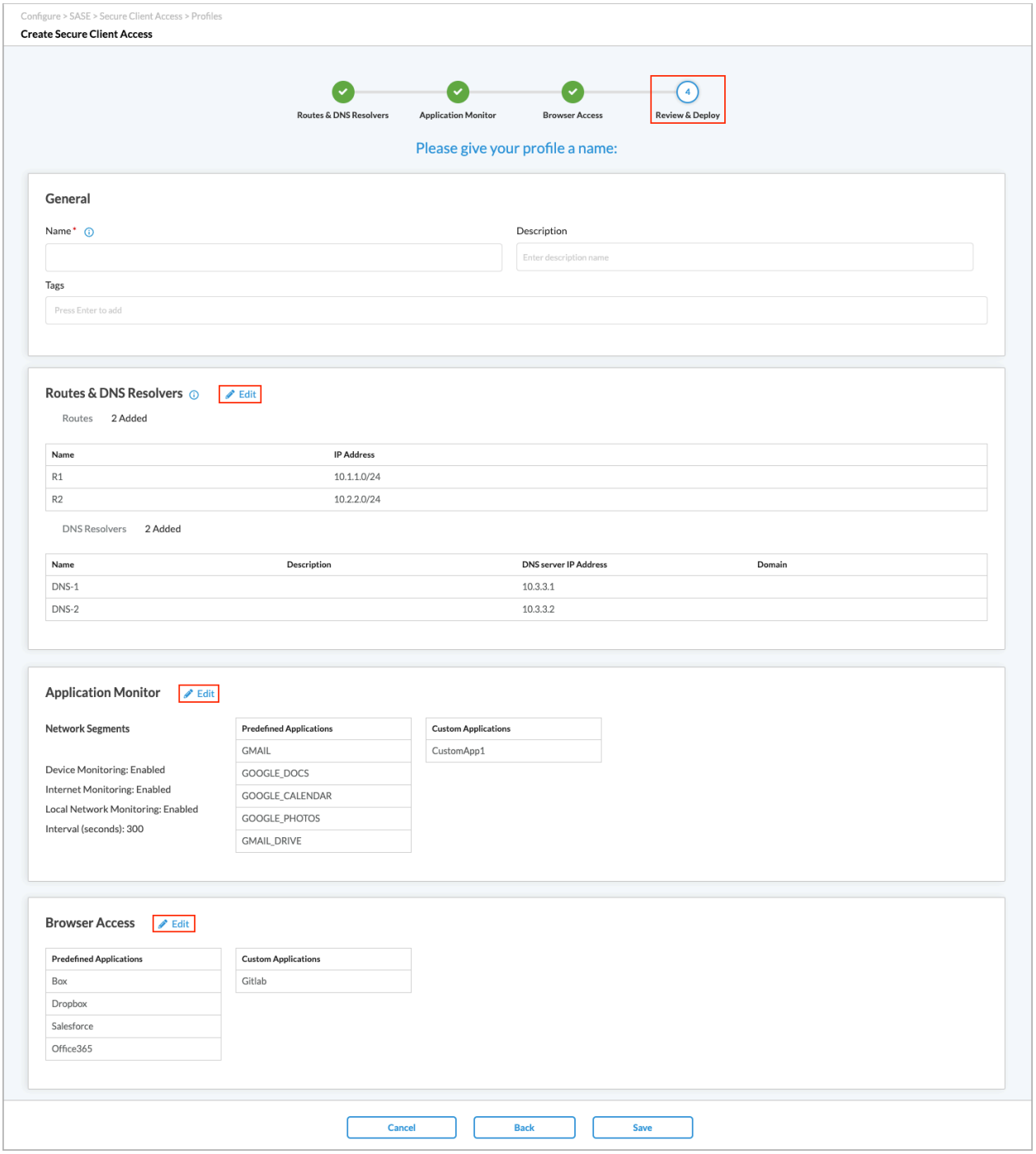
17. In the Browser Access screen, select custom applications or predefined applications, or both.



18. Click Back. The Browser Access screen displays with custom and predefined applications that you added.



19. Click Next. In the Review & Submit screen, enter information for the following fields.



Field	Description
Name (Required)	Enter a name for the profile.
Description	Enter a text description for the profile.

Field	Description
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.

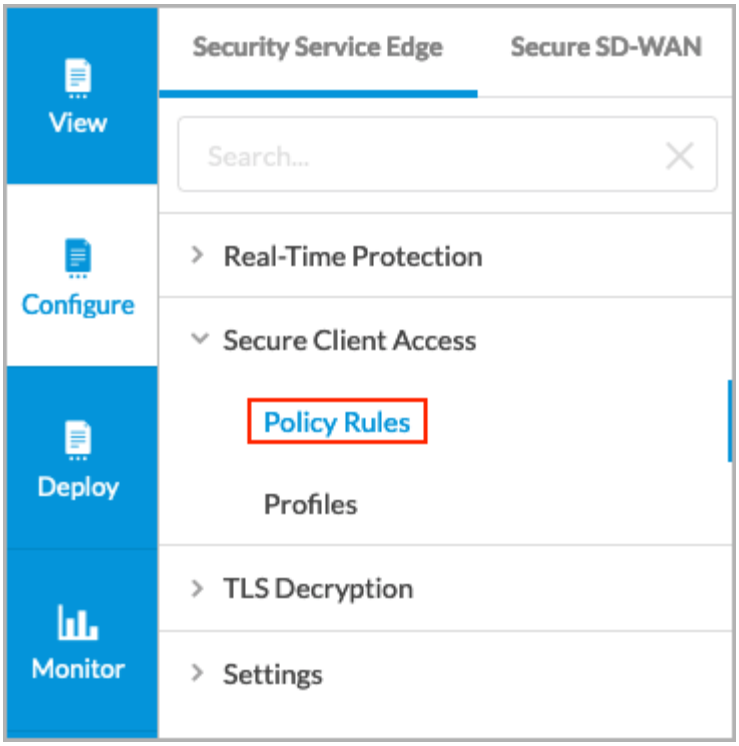
20. Review the remaining information. Click the Edit icon to make changes to any of the sections.
21. Click Submit.

Configure Secure Client Access Rules

The first time you create a VSA rule, a wizard displays (shown in the screenshot below) that guides you through the configuration steps. Thereafter, you do not see the wizard. You configure subsequent rules manually using the Policy Rules screens, as described below.

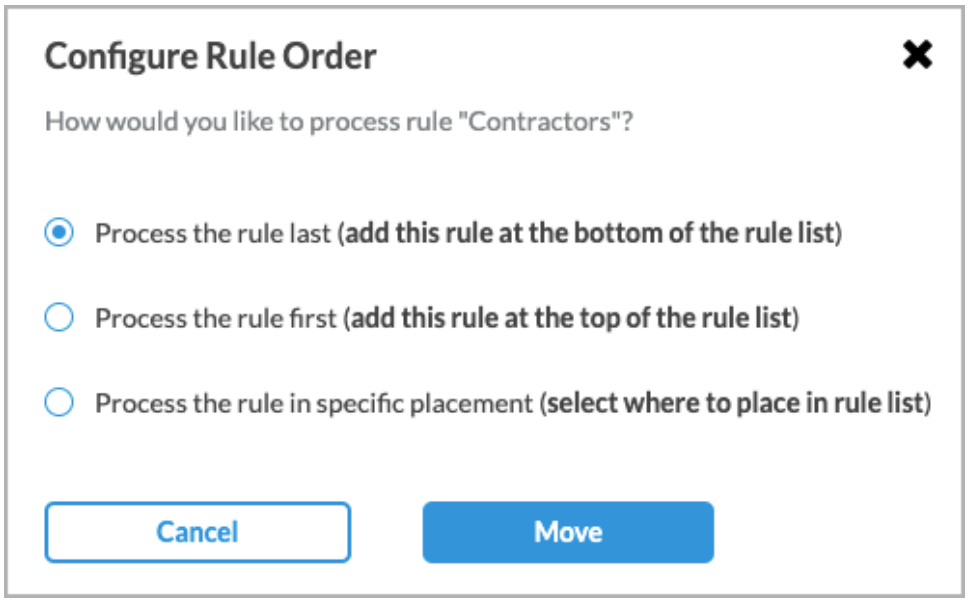
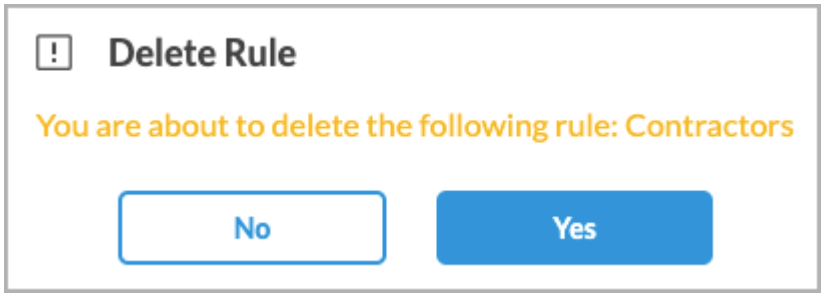
To configure secure client access rules:

1. Go to Configure > Secure Services Edge > Secure Access Client > Policy Rules.

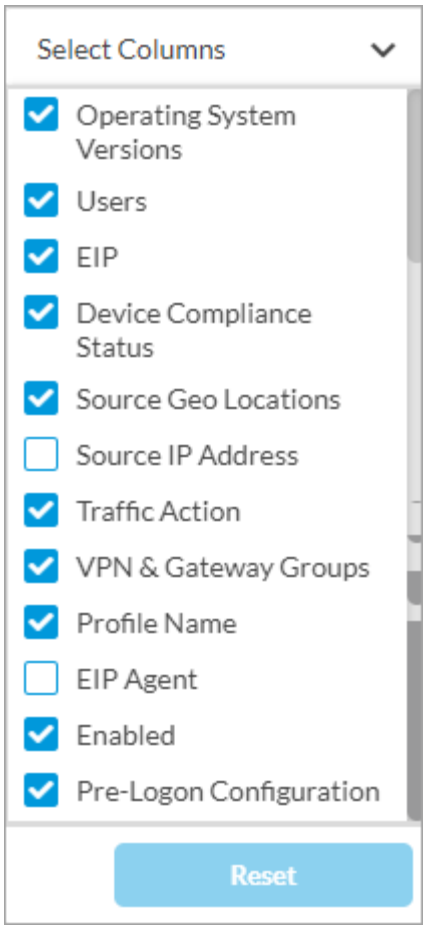


2. In the horizontal menu bar, you can perform the following operations.

Operation	Description
Add	Create a new internet protection rule. This button is active when no existing rule is selected.
Clone	Clone the selected internet protection rule. When you select this option, the configuration wi the default name of the cloned rule, if desired, then click Save.
Reorder	Reorder the selected internet protection rule. A popup window similar to the following displa

Operation	Description
	 1. Select one of the three options: ◦ Process the rule last ◦ Process the rule first ◦ Process the rule in specific placement—A list of the existing rules displays. Click the po 2. Click Move.
Delete	Delete the selected internet protection rule. A popup window similar to the following displays  Click Yes to delete the internet protection rule, or click No to retain the rule.
Refresh	Refresh the list of existing rules.

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



Note that the Pre-Logon Configuration column only appears if you have enabled pre-logon in the tenant configuration. See Configure SASE Tenants for more information.

4. Click the + Add icon to configure the policy rule. The Create Secure Client Access Rule screen displays.

From here, you configure the match criteria and enforcement actions. For more information, see:

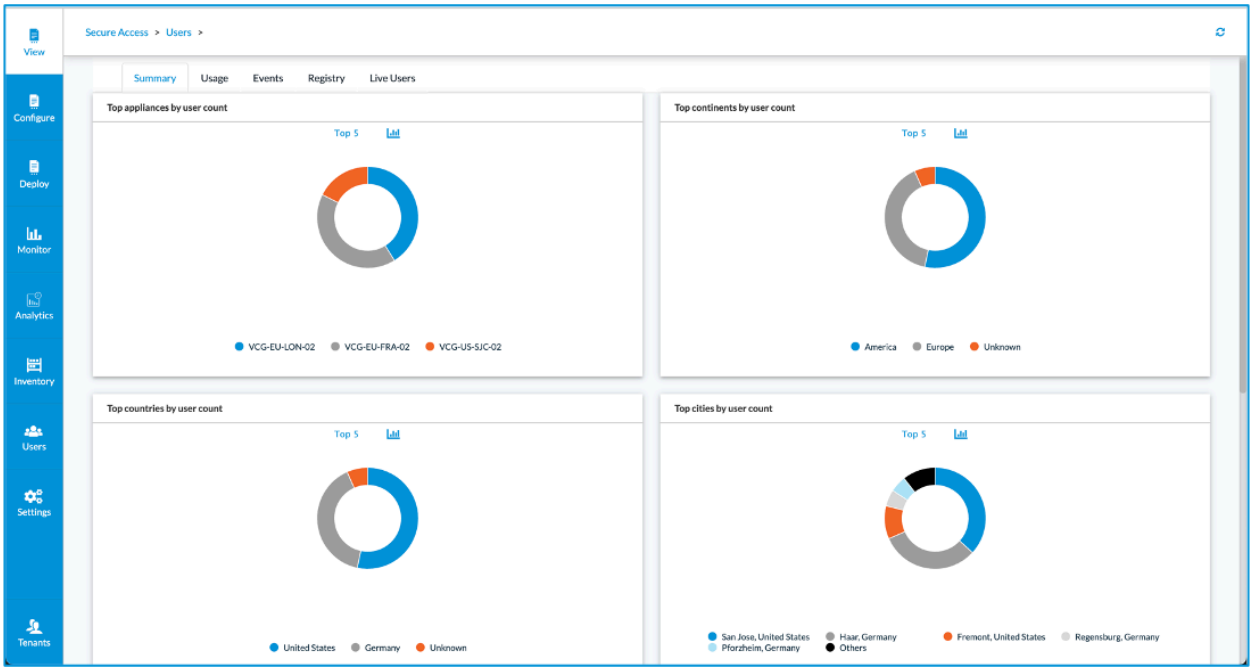
- Match Criteria:
  - Operating System—Select the operating system to use with the rule.
  - Users/User Groups—Define the users and user groups to which the secure client access rules apply.
  - Dev Risk Info—Select which devices managed by the enterprise and which unmanaged devices are allowed to access the network.
  - Source Geolocation and Source IP Address—Define which geographic locations and IP addresses can access the network.
- Actions:
  - Traffic Action—Select which traffic to send to the Versa Cloud Gateway or directly to the internet, and which traffic to block and not sent to the Versa Cloud Gateway.

- Gateways—Select which gateway groups VSPA clients can use.
- Client Configuration—Configure multifactor authentication (MFA) and other client parameters.
- Agent Profile from EIP—Define the conditions that the SASE client uses to filter information from endpoint devices.

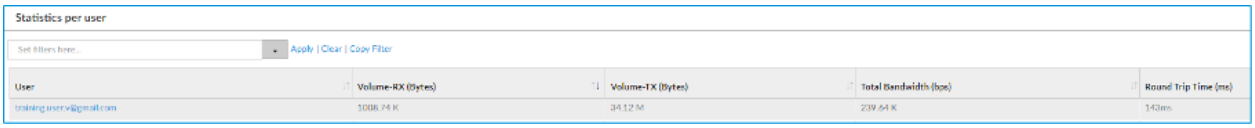
Verification

To verify secure access operations, select View in the left navigation pane, and then go to Secure Access > Users:

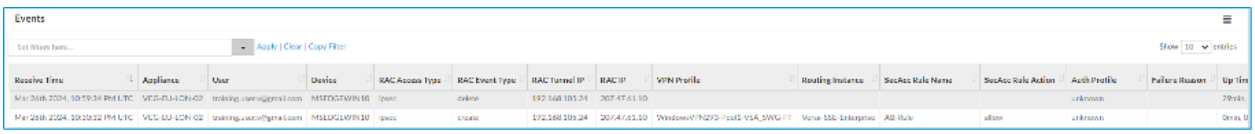
- Select the Summary tab to view a summary of user analytics statistics by user count for top devices, continents, countries, and cities.



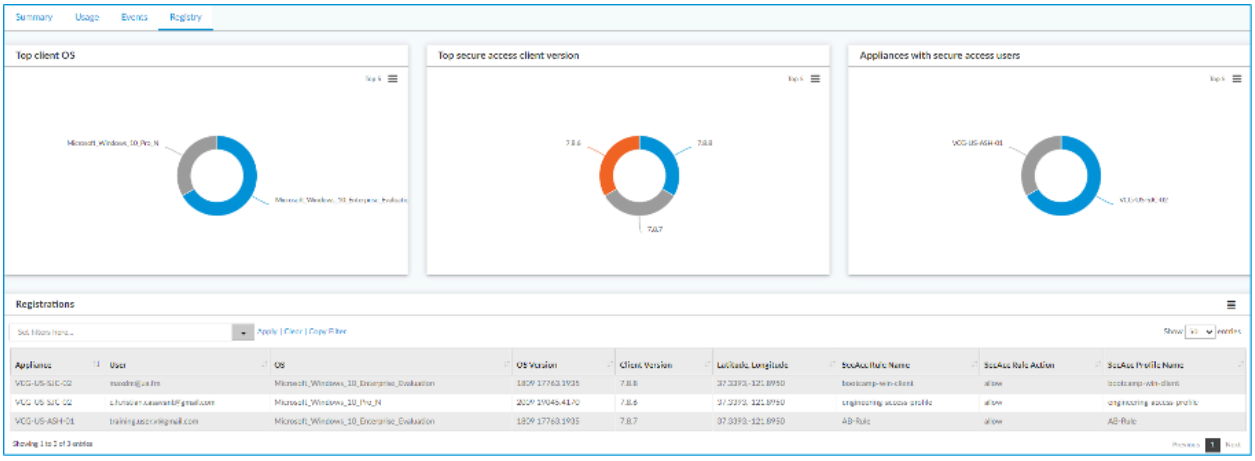
- Select the Usage tab to view analytics statistics per user and top users.



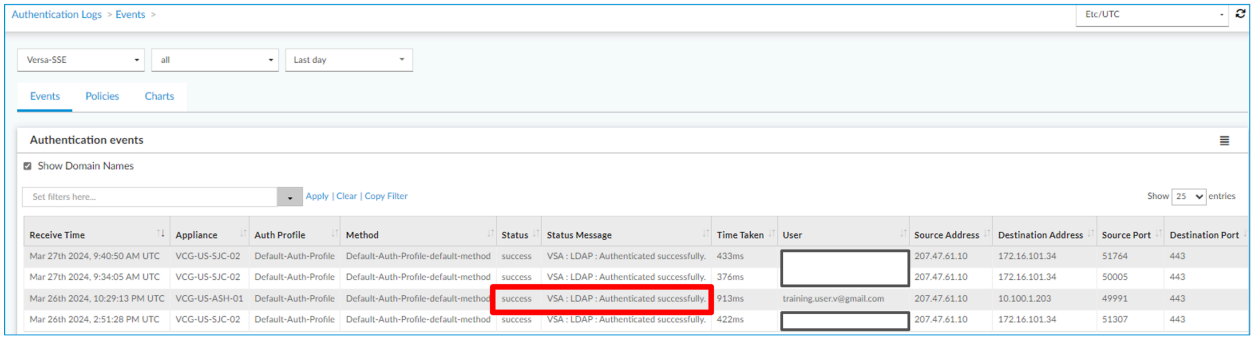
- Select the Events tab to view detailed information about client connection or disconnection events, along with the Versa Secure Access Rule, matched for each user, and the VCG used.



- Select the Registry tab to view detailed information about client registration events, along with Versa SASE Client and OS details for each user.



- To view client authentication event details, click Analytics in the left menu, and then go to Logs > Authentication.



Configure the Versa SASE Client

The Versa SASE client application is a native VPN client that supports Android, iOS, Linux, MacOS, and Windows operating systems.

Note that in earlier software releases, for releases prior to Release 7.4.3 for Android, Release 7.3.7 for MacOS, and Release 7.4.5 for Windows, the product was called the Versa Secure Access (VSA) client application software.

To configure the Versa SASE client, you do the following:

1. Install the VSA client on a device.
2. Register the VSA client (includes authentication).
3. Connect to a VSA gateway.

Install a SASE Client on a MacOS Device

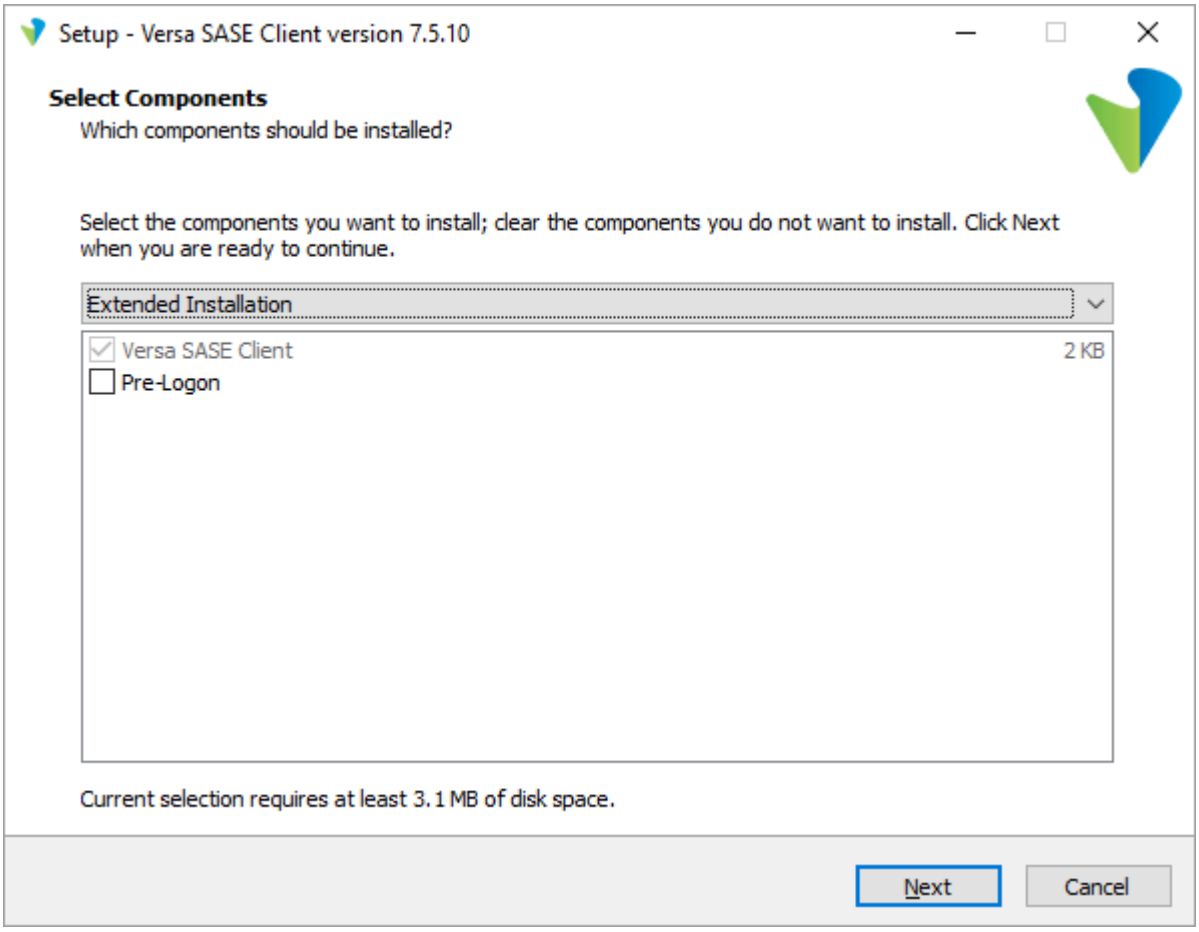
To install the Versa SASE client on a MacOS device:

1. Download and install the Versa SASE client from this location.
2. Open the SASE client. The Register screen displays. For more information, see Register the SASE Client section below.

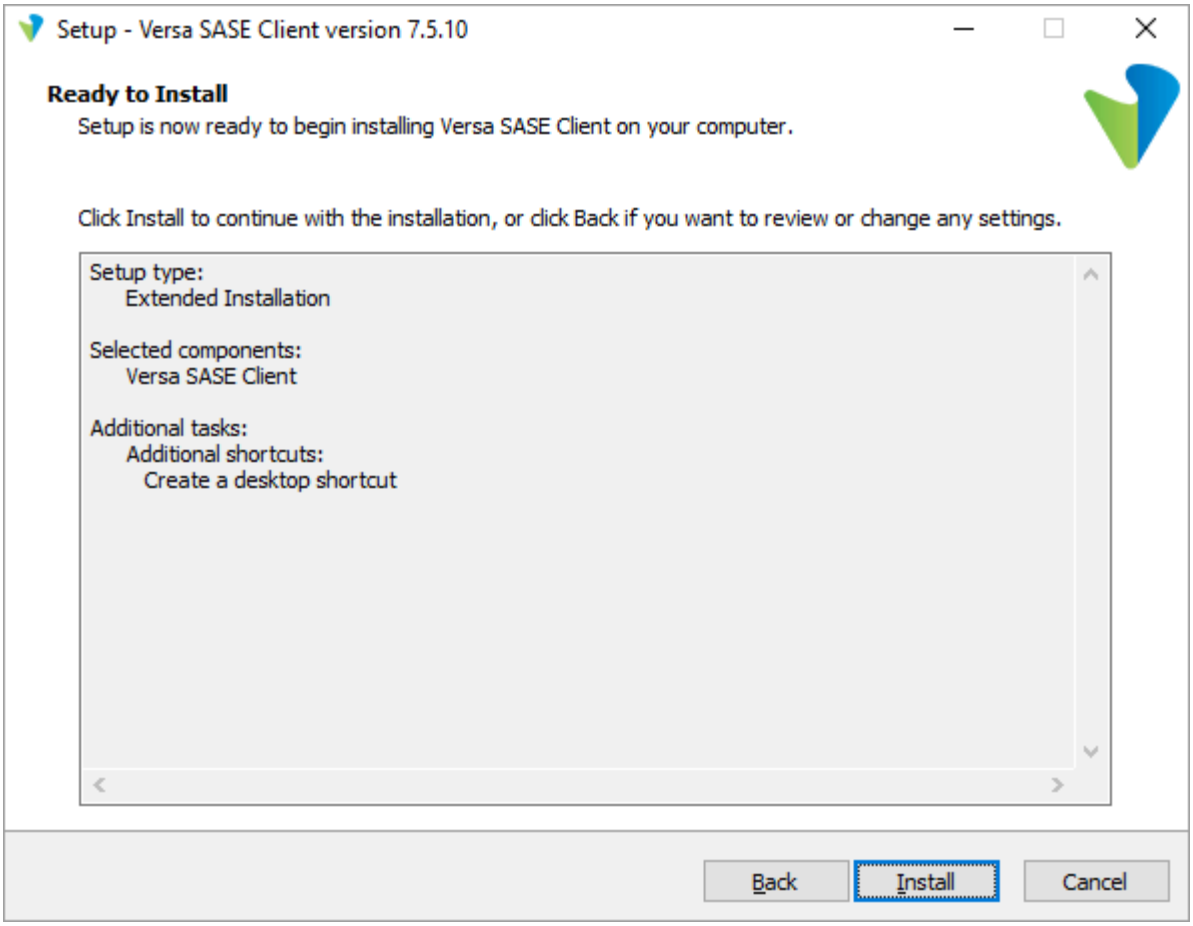
Install a SASE Client on a Windows Device

This section describes how to install the SASE client on a Windows device. To install the SASE client on a Windows device:

1. Download and install the application from this location. Confirm the download link with your organization's IT administrator before you download the SASE client.
2. Start the application. The Select Components wizard screen displays. By default, Versa SASE Client is selected.
3. Click Next in the setup wizard screen.



4. In the last wizard window, click Install to complete the installation.



The Register screen displays, unless you deselected Launch Versa SASE Client. For more information, see Register the SASE Client section below.

Register the SASE Client

After you install the SASE client, register to the SASE platform using the following information from the email notification that you received. This information is provided to your organization's IT administrator:

- Link to the registration portal's FQDN or IP address
- Your enterprise name
- Your user ID

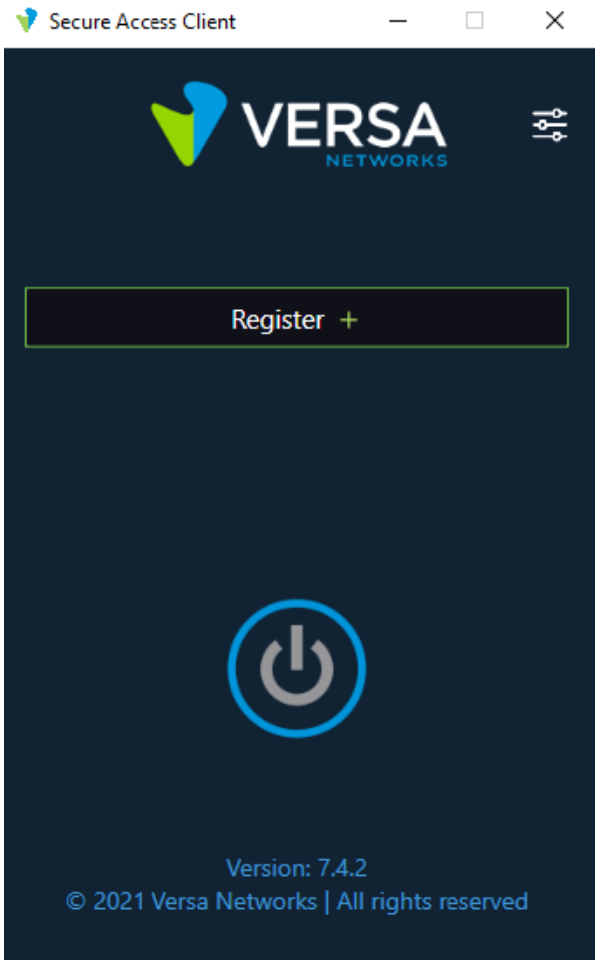
To authenticate with the SASE portal, the following types of authentication are supported:

- Basic local authentication
- SAML

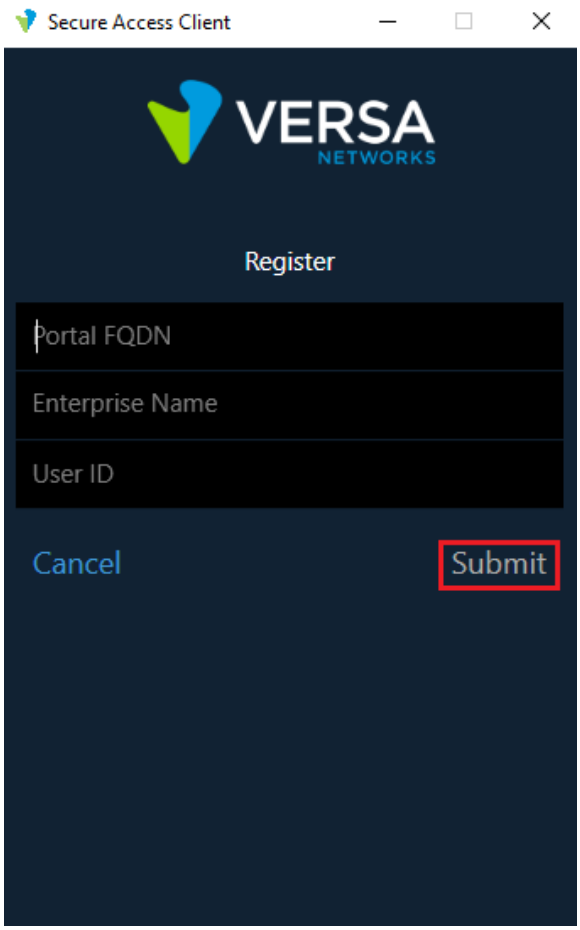
- Time-based one-time password (TOTP)
- Two-factor authentication

To register the SASE client:

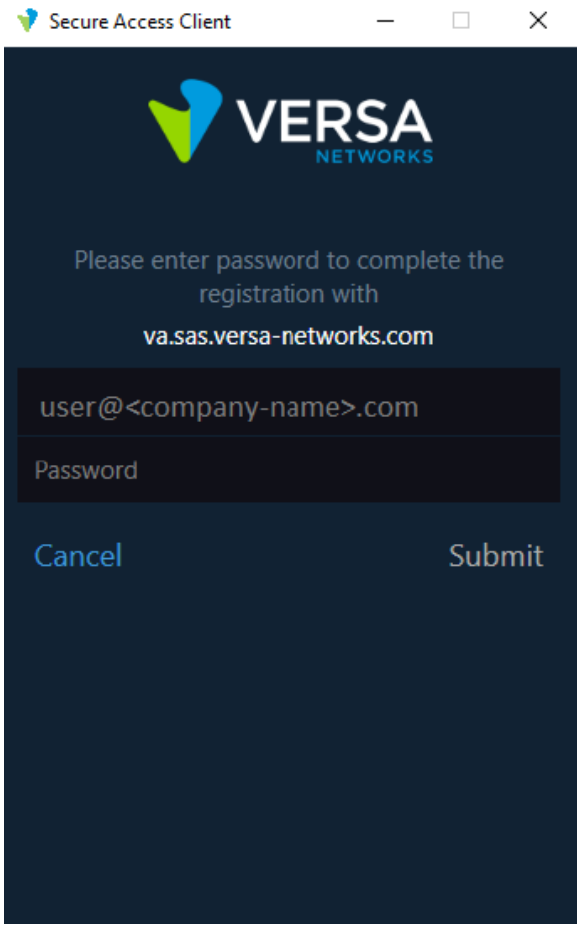
1. Click the link to the registration portal that was included in the email.
2. Open the SASE Client, and click Register.



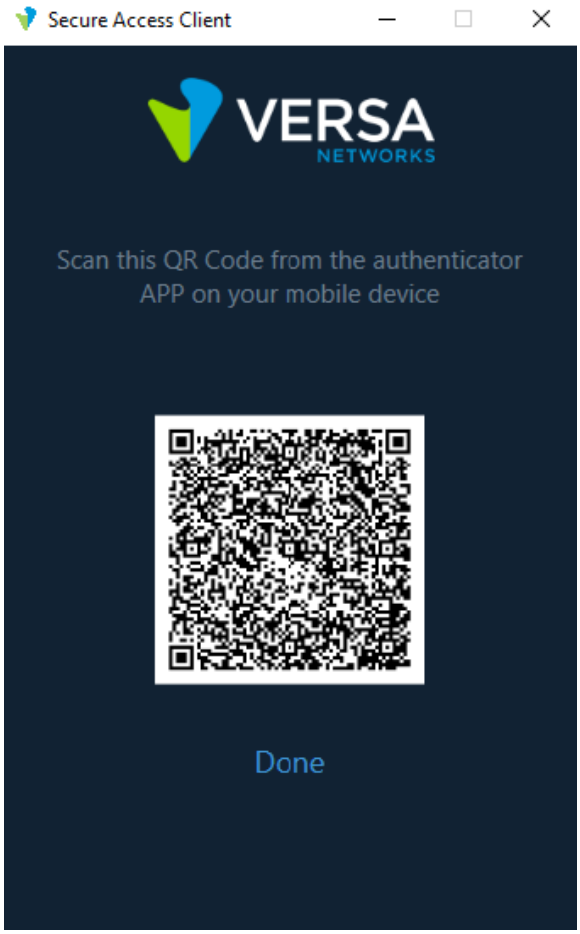
3. Enter the portal's FQDN or IP address, enterprise name, and your user ID, and then click Submit.



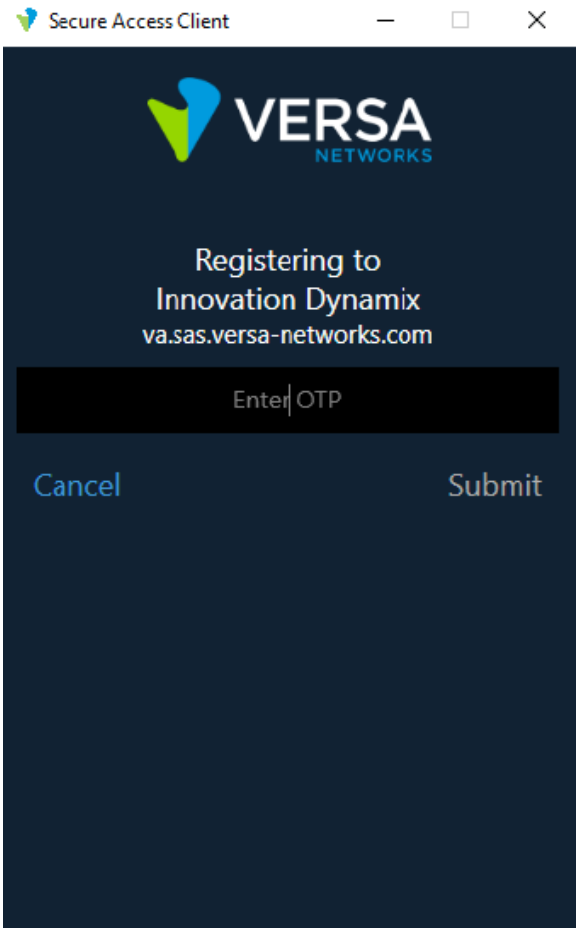
4. Enter the username and password that you received from the administrator, and then click Submit.



5. If authentication using two-factor authentication is required, enter the one-time password that you received in email or SMS, and click Submit. After the one-time password is validated, the registration process is complete.
6. If TOTP authentication is required, the screen displays a QR code:

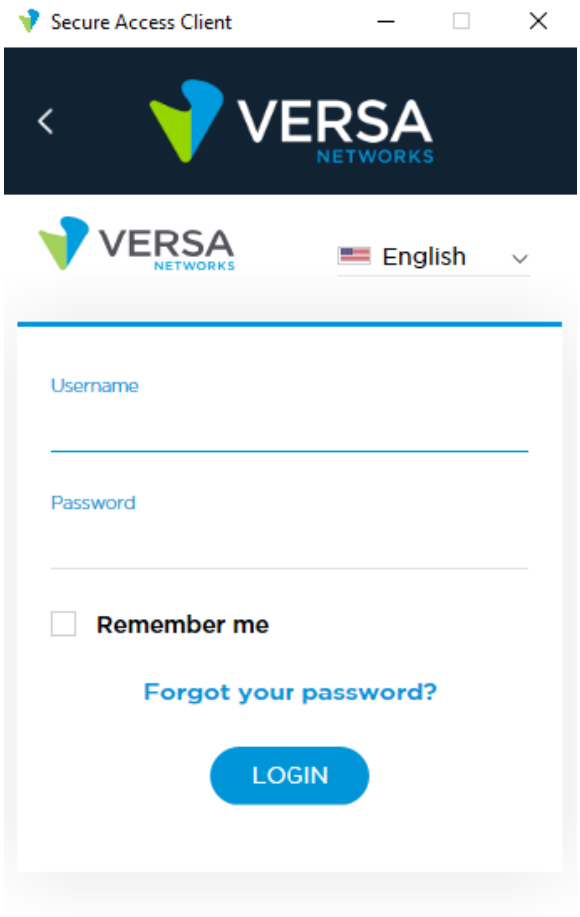


a. Scan the QR code using any authenticator application.
b. Click Done after you scan the QR code. The following screen displays with a field to enter OTP.



c. Enter the OTP that the authenticator application displays and click Submit.
d. After the TOTP is validated, the registration process is complete.

7. If SAML authentication is used, the client login page similar to the following displays:



a. Enter the user name and password, and then click Login.
b. After the login credentials are validated, the registration process is complete.

Connect to a VSA Gateway

Configure TLS Decryption

To take advantage of the advanced security inspection features of the Versa Secure Services Edge (SSE), you configure Transport Layer Security (TLS) decryption. Most internet traffic is encrypted using TLS, which may hide malicious content, payloads, and flows. This makes it difficult to apply content-specific security policies to the traffic. TLS decryption enables the Versa SASE solution to enforce security policies on encrypted traffic.

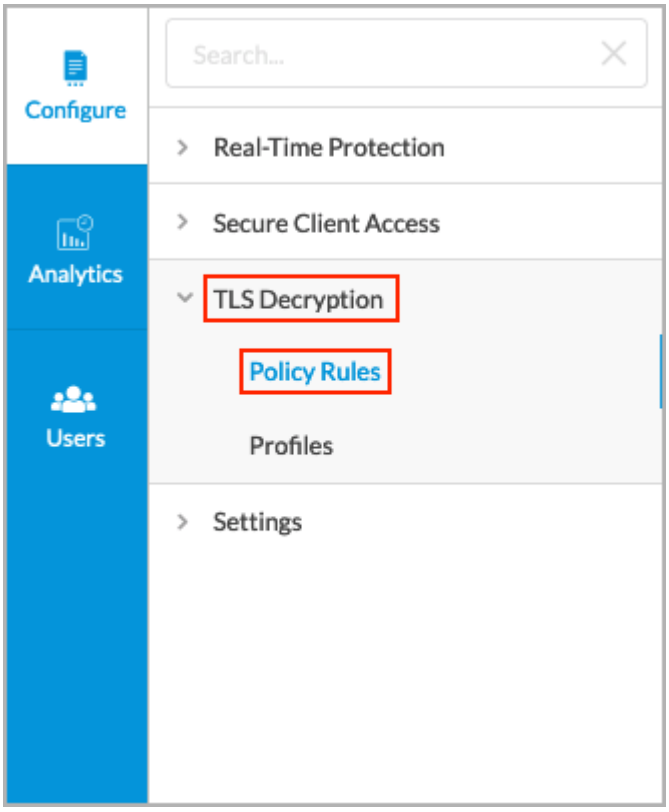
TLS decryption is an industry-standard protocol that is used to provide a secure communications channel between clients (end devices) and servers (destination sites) over the internet. TLS decryption uses two mechanisms to secure traffic:

- Handshake protocol—Authenticates the client and server devices at both ends of a secure communications channel, negotiates cryptographic modes and parameters, and establishes shared keying material used to negotiate the security parameters of a connection. The handshake protocol then sends messages to the TLS record protocol.
- Record protocol—Takes transmitted messages from the handshake protocol, fragments the data into manageable blocks, protects the records, and transmits the result. The data received is verified, decrypted, reassembled, and then delivered to higher-level clients.

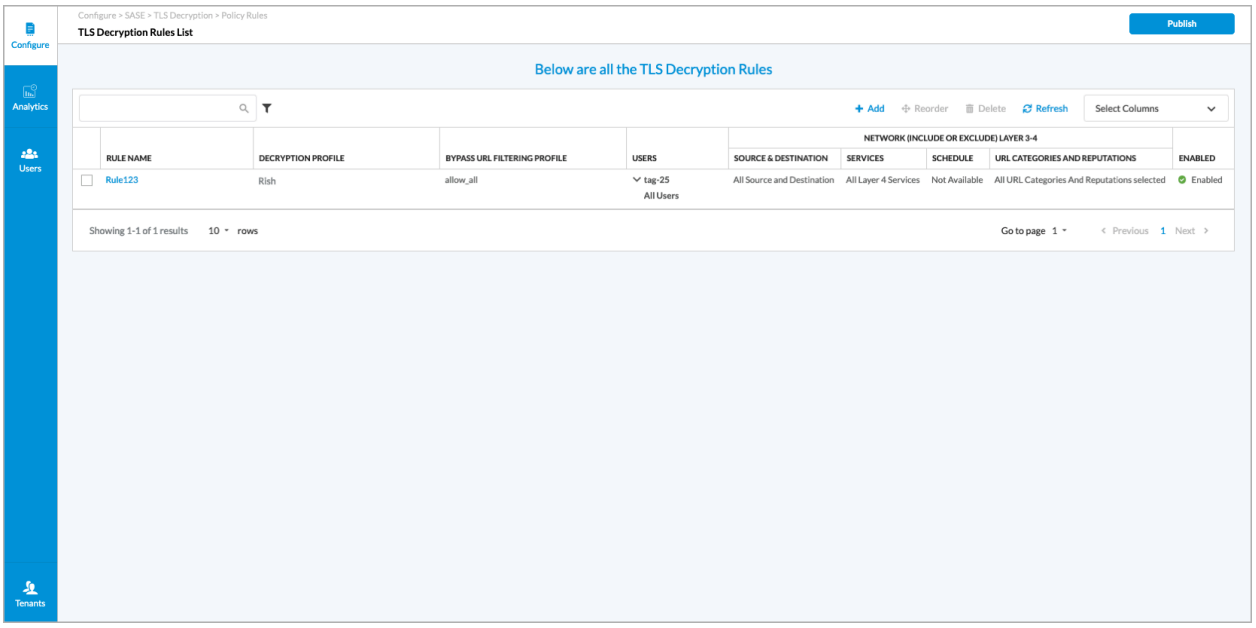
Configure TLS Decryption Rules

To configure TLS decryption rules:

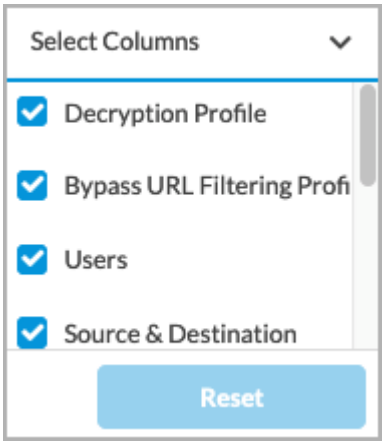
1. Go to Configure > TLS Decryption > Policy Rules.



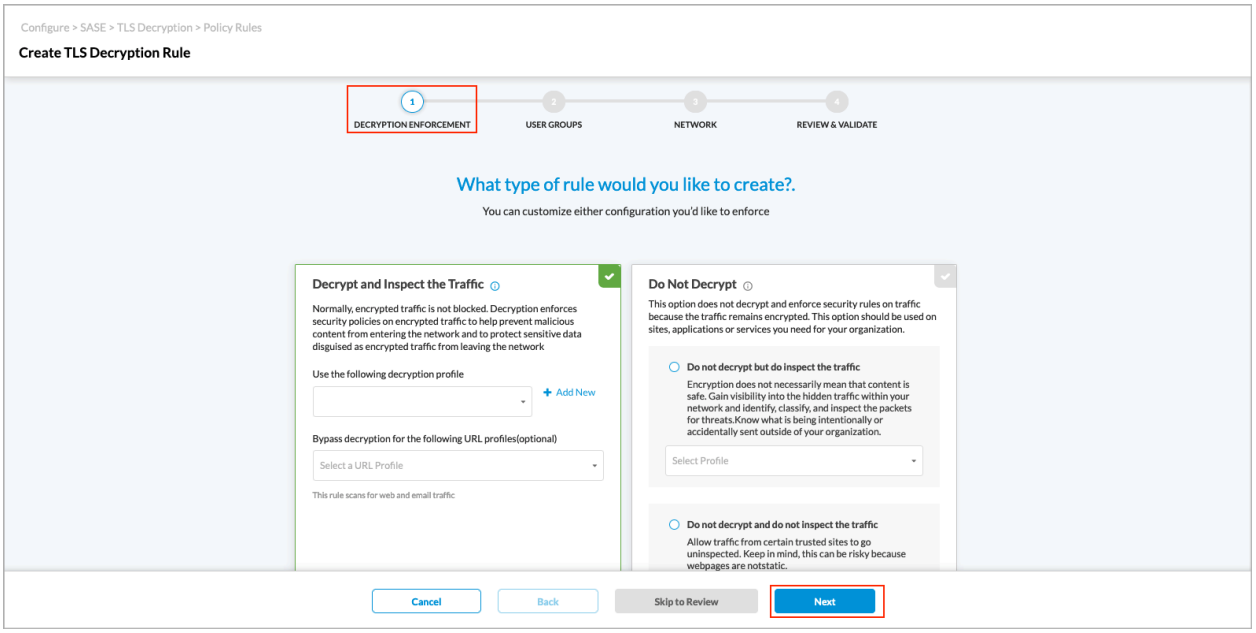
The TLS Decryption Rules List screen displays all current rules.



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

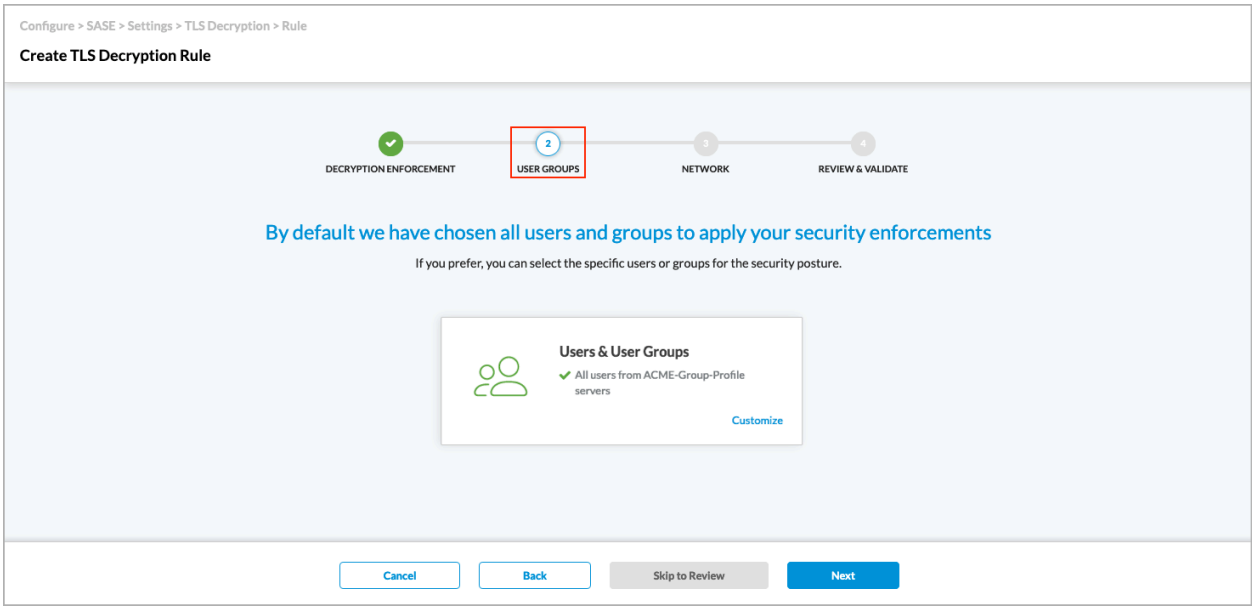


3. Click + Add to add a TLS decryption rule. The Create TLS Decryption Rule screen displays. In the first step, Decryption Enforcement, enter information for the following fields.

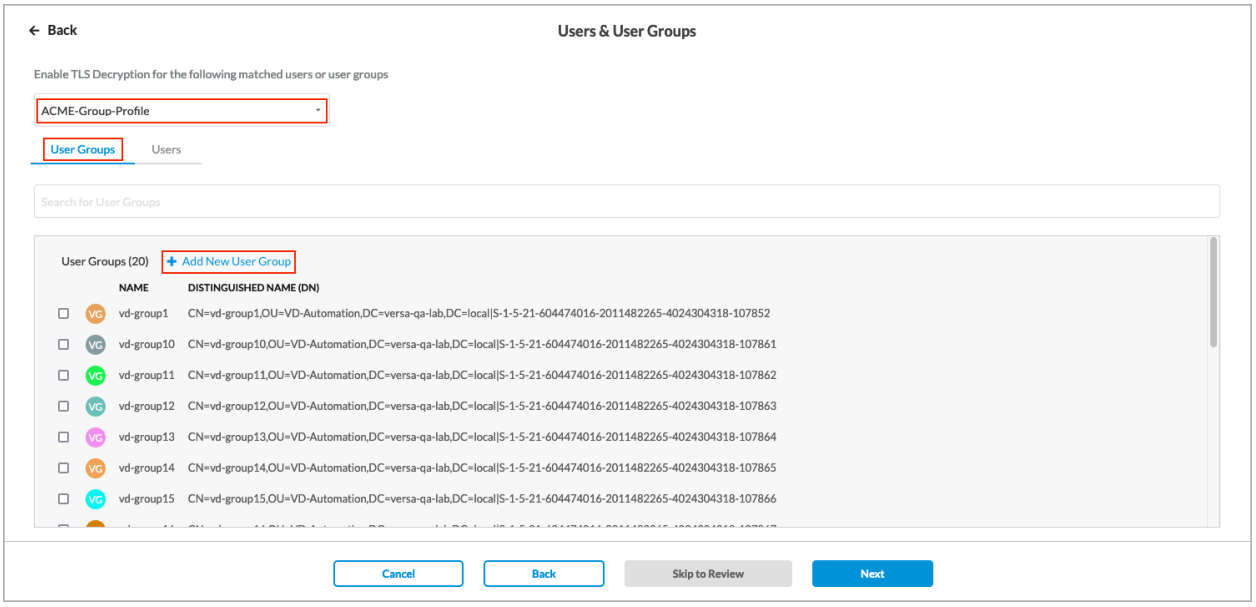


Field	Description
Decrypt and Inspect the Traffic (Group of Fields)	Select to decrypt and inspect all traffic.
◦ Use the following decryption profile	Select a decryption profile.
◦ + Add New	Click to add a decryption profile. To create a profile, see Create a TLS Decryption Profile.
◦ Bypass decryption for the following URL-filtering profile	To bypass the decryption action in a URL filtering profile, select a URL-filtering profile. This URL-filtering profile must be one in which decrypt bypass is enabled. The user-defined URL profile must be created in the Tenant-Common template in the Director before it displays in the drop-down list. Contact Versa Support to configure this option.
Do Not Decrypt (Group of Fields)	Select how to bypass decryption of the traffic.
◦ Do not decrypt but do inspect the traffic	Do not decrypt the traffic but inspect the traffic to identify, classify, and inspect the traffic for threats. Select a profile.
◦ Do not decrypt and do not inspect the traffic	Click to allow traffic from certain trusted sites to no be inspected.

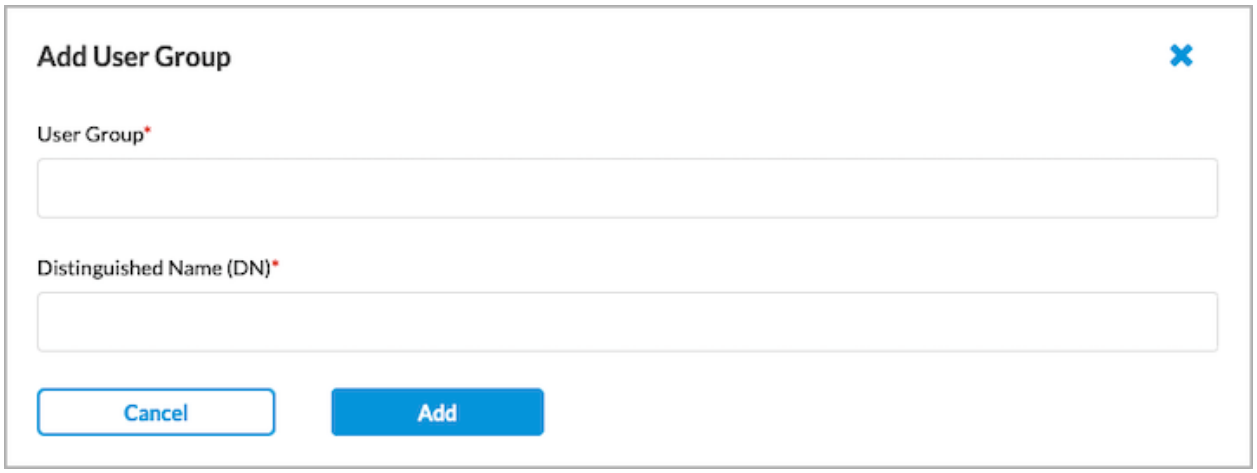
4. Click Next to go to the second step, User Groups. The User Groups screen displays. By default, security enforcement is applied to all users and user groups.



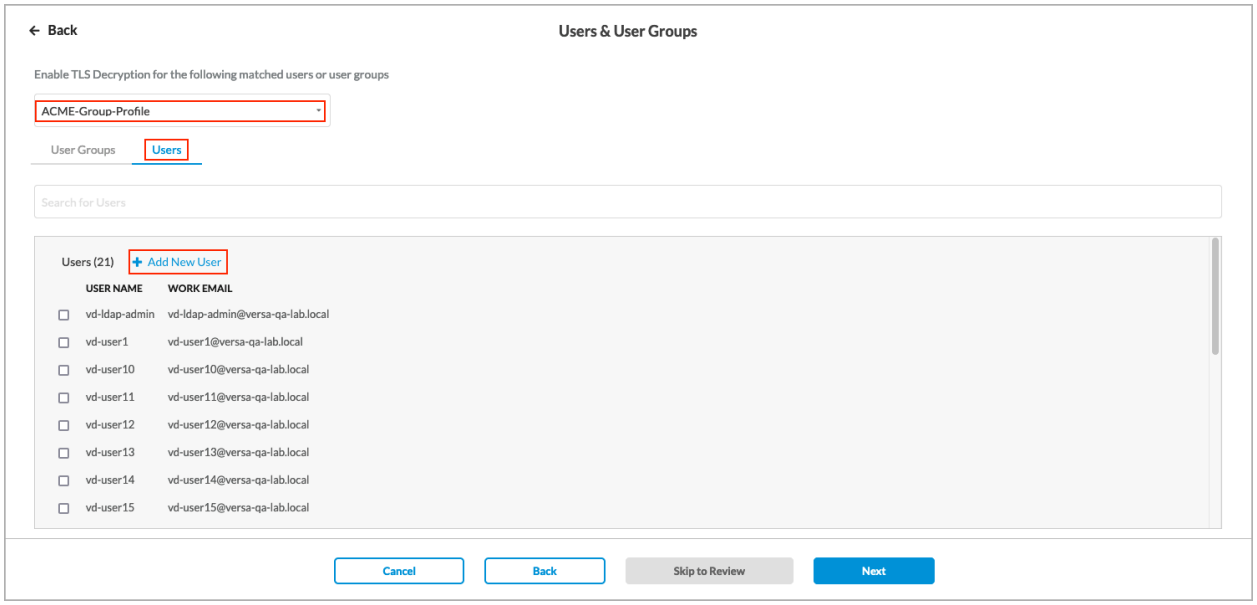
5. To accept the default, click Next to continue the Geolocations match criteria.
6. To change these settings, click Customize. The Users and User Groups screen displays.



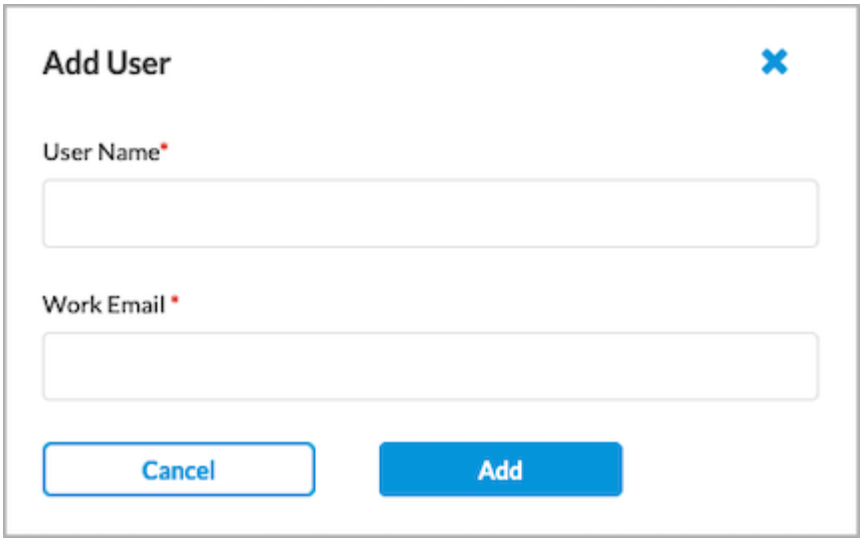
7. Select the group profile to use.
8. Under the User Groups tab, select the user groups to include in the match list, or type the name of a user group in the search box and then select it from the search results.
9. To create a user group based on LDAP authentication, select an LDAP group profile, and then click + Add New User Group. In the Add User Group window, enter a user group name and a distinguished name (DN).



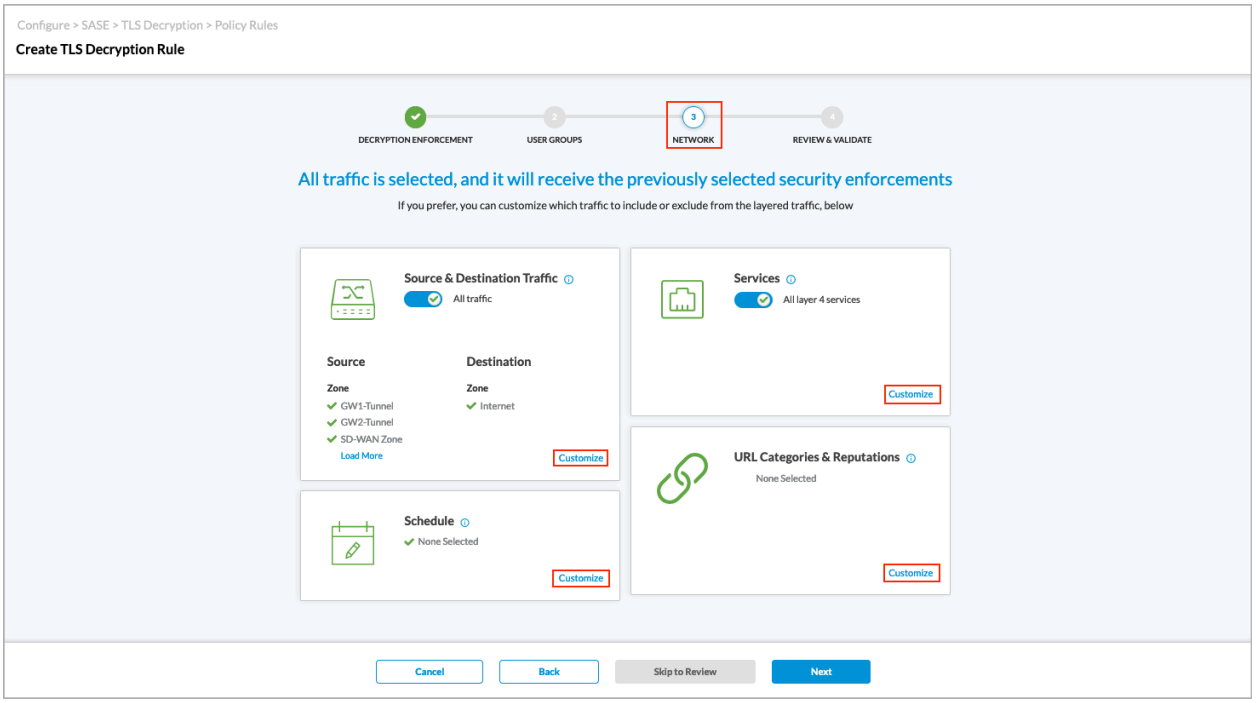
10. Click the Users tab in the submenu. The following screen displays.



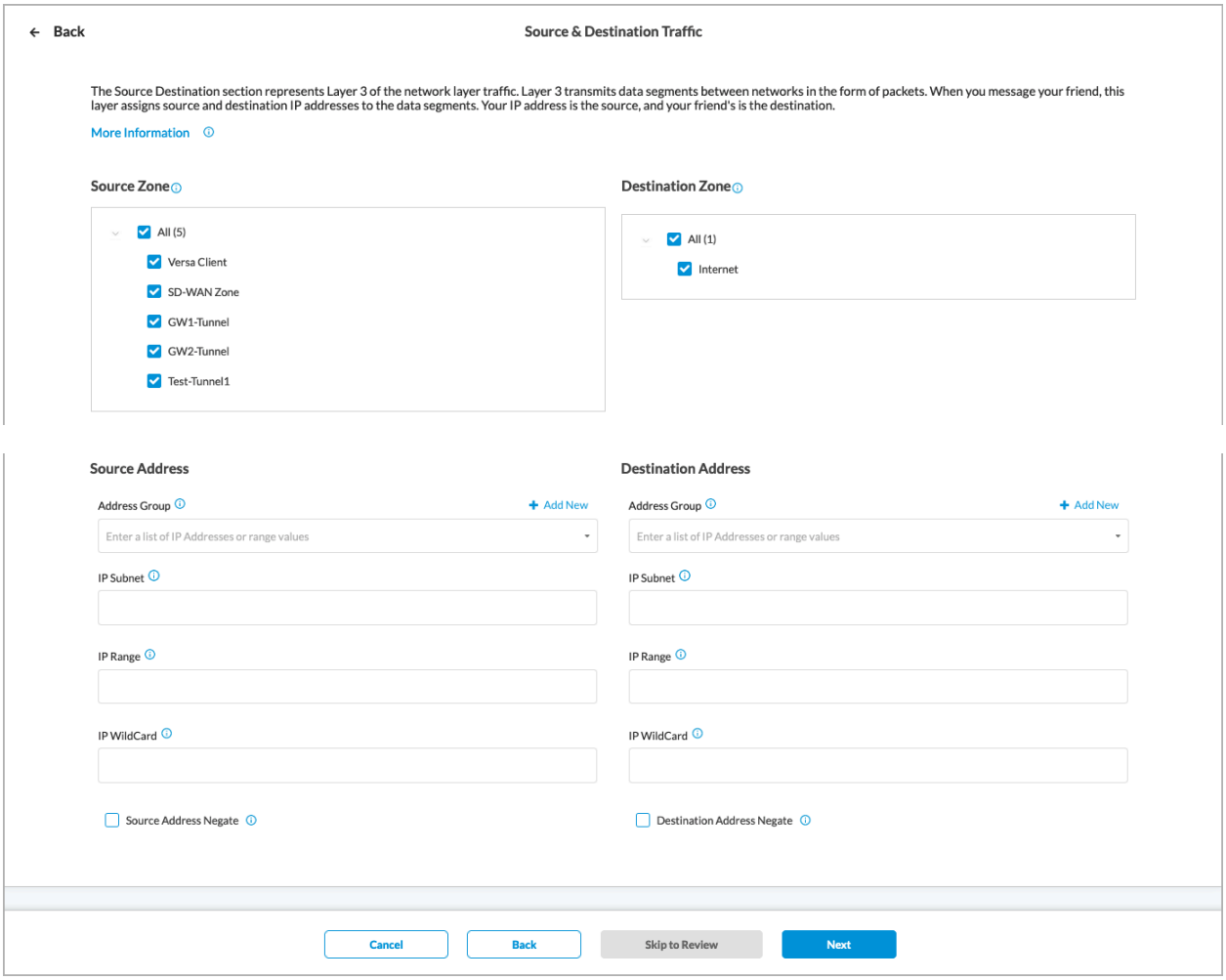
11. Select the group profile to use.
12. Under the Users tab, select the users to include in the match list, or type the name of a user in the search box and then select it from the search results.
13. To create a user based on LDAP authentication, select an LDAP group profile, and then click + Add New User. In the Add User window, enter a username and the user's work email in the fields provided.



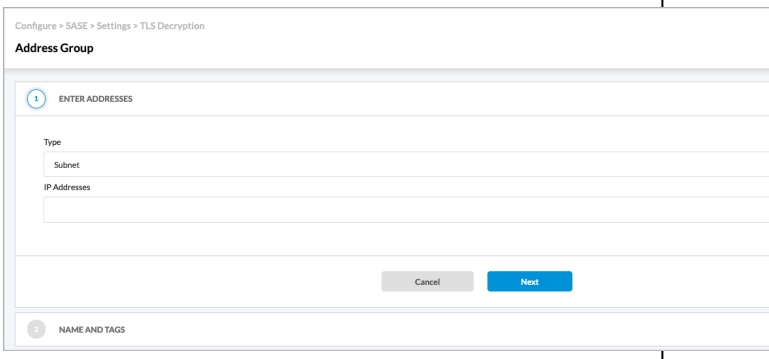
14. Click Add.
15. Click Next to go to the Network screen, or click Back to return to the Create TLS Decryption Rule screen, and then click Next. The following screen displays.

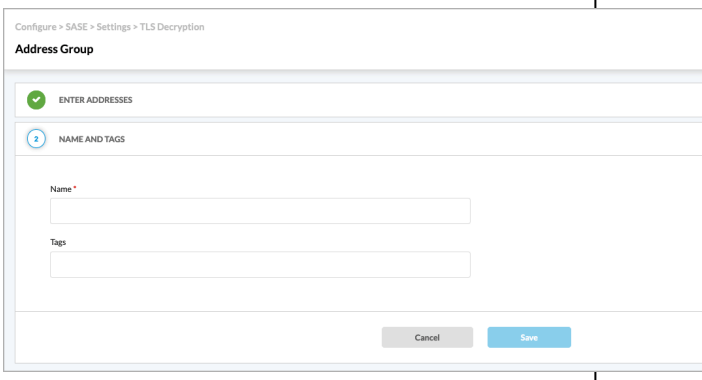


16. By default, all source and destination traffic is included in the match list. To change the source and destination traffic to include in the match list, click Customize under Source & Destination Traffic. In the Source & Destination Traffic screen, enter information for the following fields.

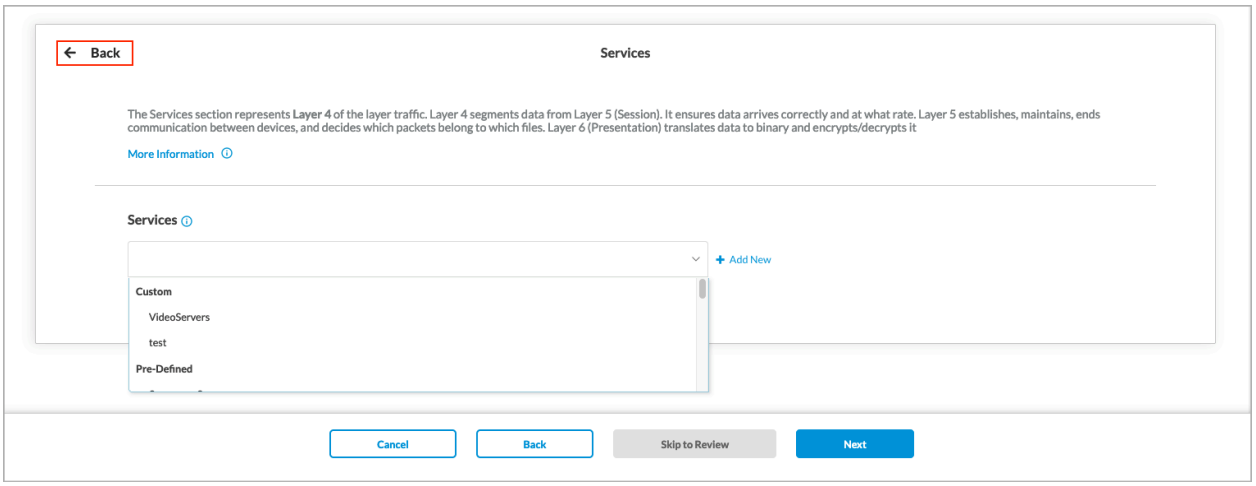


Field	Description
Source Zone	Select one or more source zones to include in the match list. By default, three source zones are available: ◦ SD-WAN Zone—Select if traffic comes from an SD-WAN device. ◦ User-defined zones—Select for zones, such as zones for IPsec or GRE tunnels. ◦ Versa Client—Select if traffic comes from a Versa Secure Access (VSA) client application.
Source Address (Group of Fields)	
◦ Address Group	Click in the box, and then select one or more address

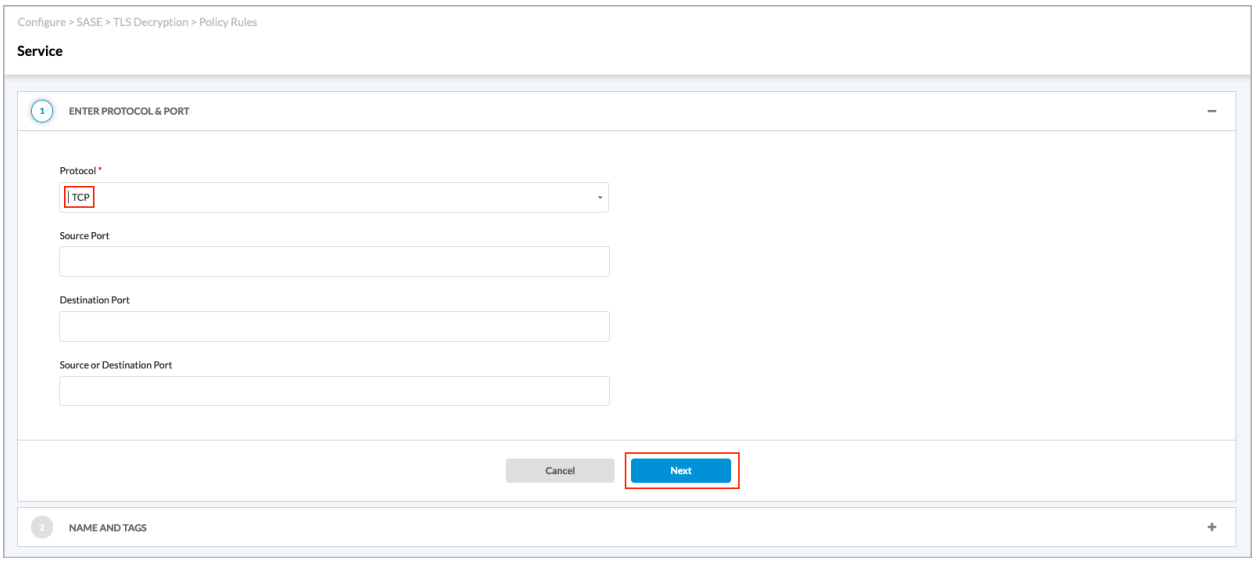
Field	Description
	groups. These address groups are defined in the User Defined Objects section. Note: You do not need to select an address group if you want to provide one or more specific source IP addresses, in which case you use the IP Wildcard field to enter the IP addresses. To create an address group, click + Add New, and then enter the following information.  1. Click the Enter Addresses section, and then select the group Type. The type can be Subnet, IP range, IP wildcard, or IPv6 subnet. 2. Based on the type selected, enter one of the following and then press Return: —Subnet: One or more IP addresses and subnet masks, for example, 10.2.1.0/24 —IP range: One or more IP address ranges, for example, 10.2.1.1-10.2.2.2 —IP wildcard: One or more specific IP addresses, for example, 192.68.0.56/ 255.255.0.255 —IPv6 subnet: One or more valid IPv6 subnets 3. To add additional IP address types, click the Plus icon. To remove an address type, click the Minus icon. 4. Click the Name and Tags section, and then

Field	Description
	enter a name for the address group and tags.  5. Click Save.
◦ IP Wildcard	Enter a list of comma-separated IP addresses and masks to include in the match list, for example, 192.68.0.56/255.255.0.255.
◦ IP Subnet	Enter a list of comma-separated subnets to include in the match list, for example, 10.2.1.0/24.
◦ IP Range	Enter a list of comma-separated IP addresses or ranges to include in the match list, for example, 10.2.1.1-10.2.2.2.
Source Address Negate	Select to apply the rule to any source addresses except the ones in the Source Address field.
Destination Zone	Internet—Select this zone if traffic comes from the internet.
Destination Address	Complete the fields under Destination Address in the same way as you did for the Source Address.

17. To customize services or schedules, click the Back button to return to the Network screen.
18. To change the services to include in the match list, click Customize under Services. The following screen displays.



19. Select one or more of the predefined services. To add a custom service, click + Add New. The following screen displays.

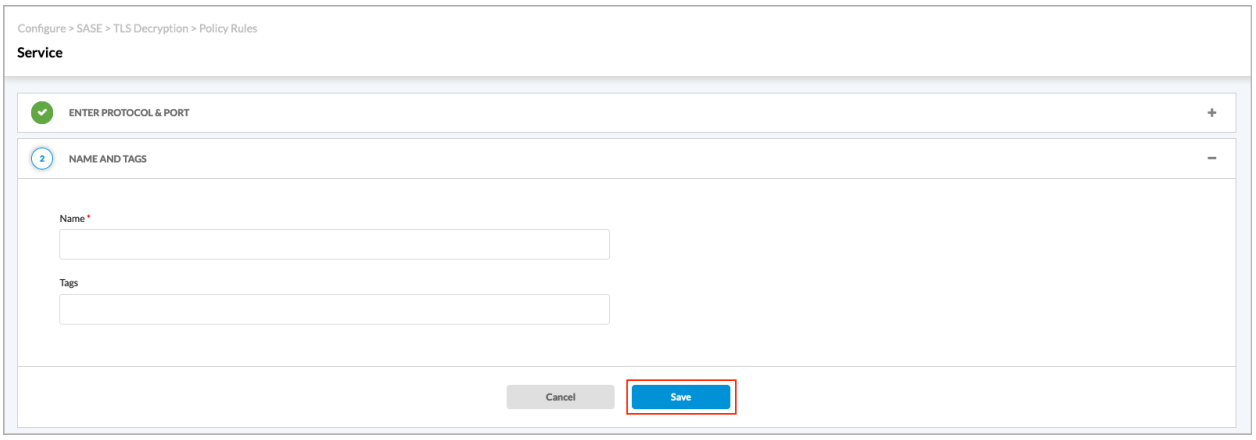


20. In the Protocol field, select a protocol. If you select TCP, UDP, or TCP and UDP, enter information for the following fields.

Field	Description
Source Port	Enter the source port number. *Range*: 0 through 65535 *Default*: None

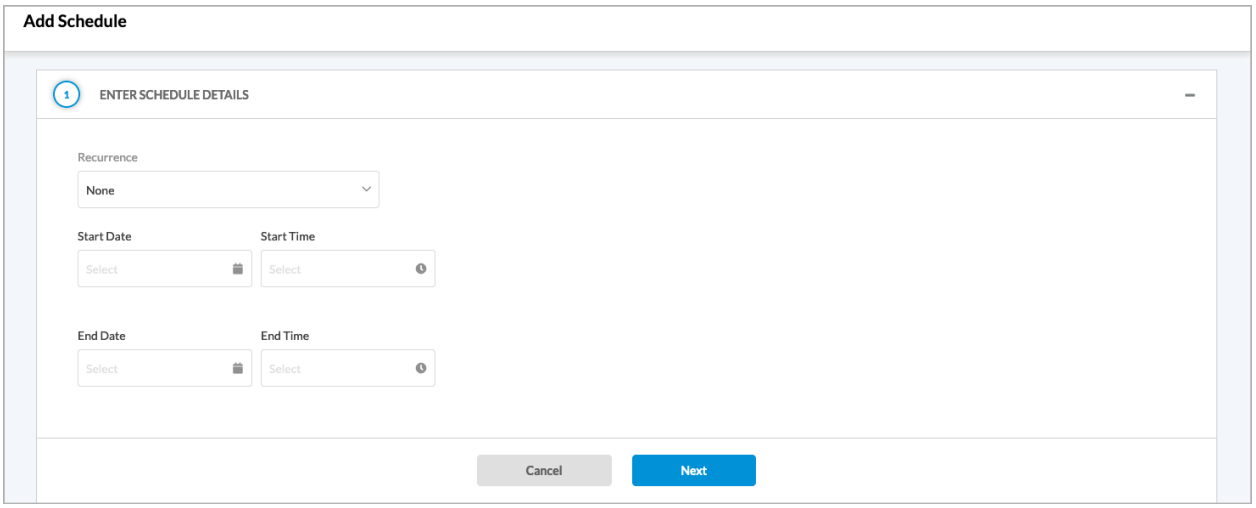
Field	Description
Destination Port	Enter the destination port number. *Range*: 0 through 65535 *Default*: None
Source or Destination Port	Enter the source or destination port number. *Range*: 0 through 65535 *Default*: None

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



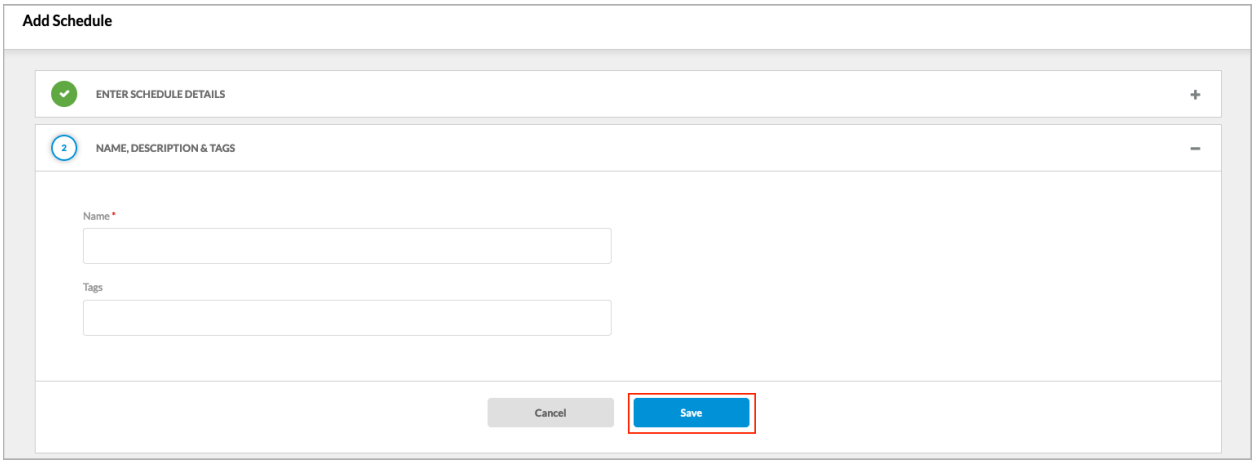
22. In the Name field, enter a name for the new service, and optionally, enter tags and a description for the service
23. Click Save to add the service to the protocol list. You can then select the service in the drop-down list.
24. To customize schedules, click the Back button to return to the Network screen.
25. To create a schedule for the policy to be in effect, click Customize under Schedule. The following screen displays.

26. Click the drop-down list under Schedule Hours to select a schedule. If no schedules exist, create one by clicking + Add New. Under Enter Schedule Details, enter information for the following fields.

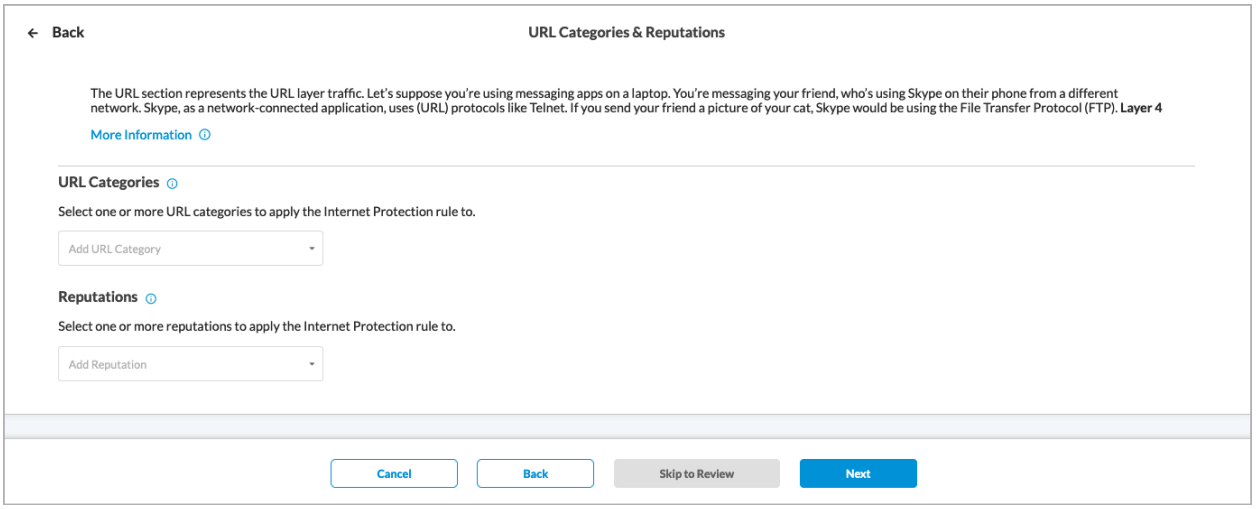


Field	Description
Recurrence	Select None, Daily, or Weekly.
Start Time	Enter the start time for the policy to be in effect.
End Time	Enter the end time for the policy to be in effect.
Days of the Week	If you select the recurrence to be weekly, select the days of the week for the policy to be in effect. 

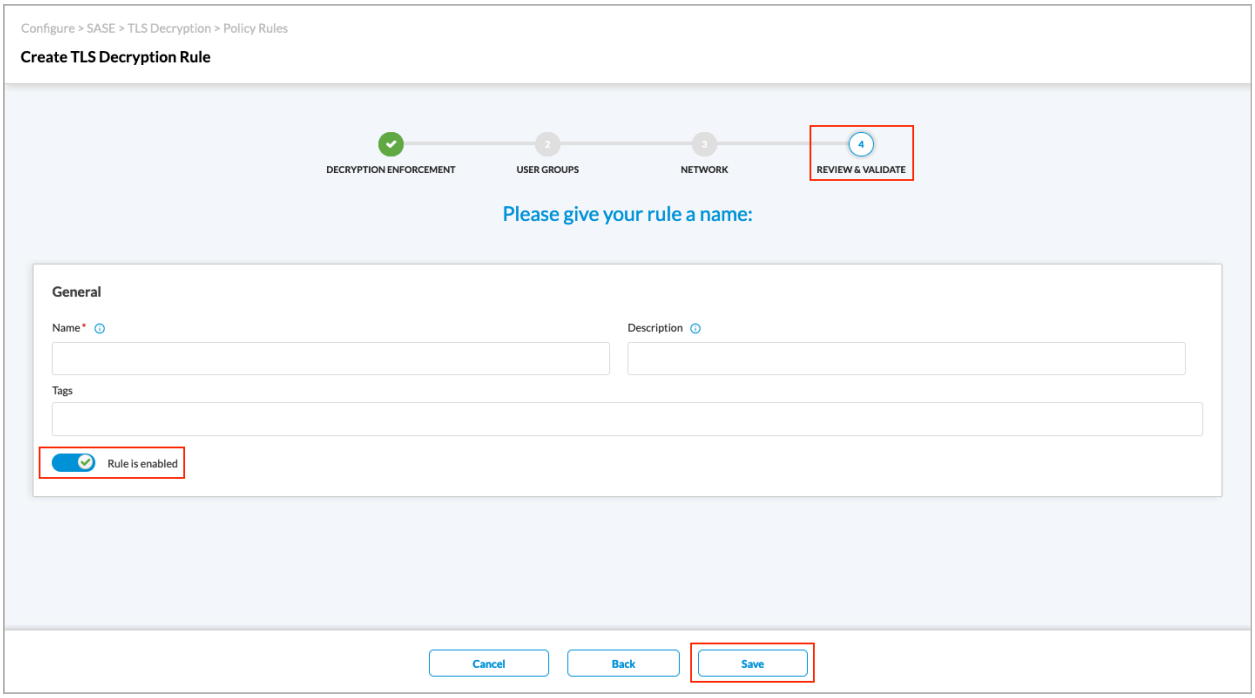
27. Click Next. The Name and Tags section displays.



28. In the Name field, enter a name for the new schedule, and optionally, enter tags for the service.
29. Click Save.
30. Click the Back button to return to the Network screen.
31. To customize URL categories and reputations, click Customize under URL Categories & Reputations. The following screen displays.



32. To specify the URL categories to which the rule applies, select one or more URL categories in the URL Categories field.
33. To specify the reputations to which the rule applies, select one or more reputations in the Reputations field.
34. Click Next. The Review and Validate screen displays.



Field	Description
Name	Enter a name for the new rule.
Description	Enter a description of the new rule.
Tags	Enter one or more tags for the new rule. A tag is an alphanumeric text descriptor with no spaces or special characters that is used for searching rules. You can specify multiple tags.
Rule is enabled	Click the slider to enable the rule.  Click the slider again to disable the rule. 

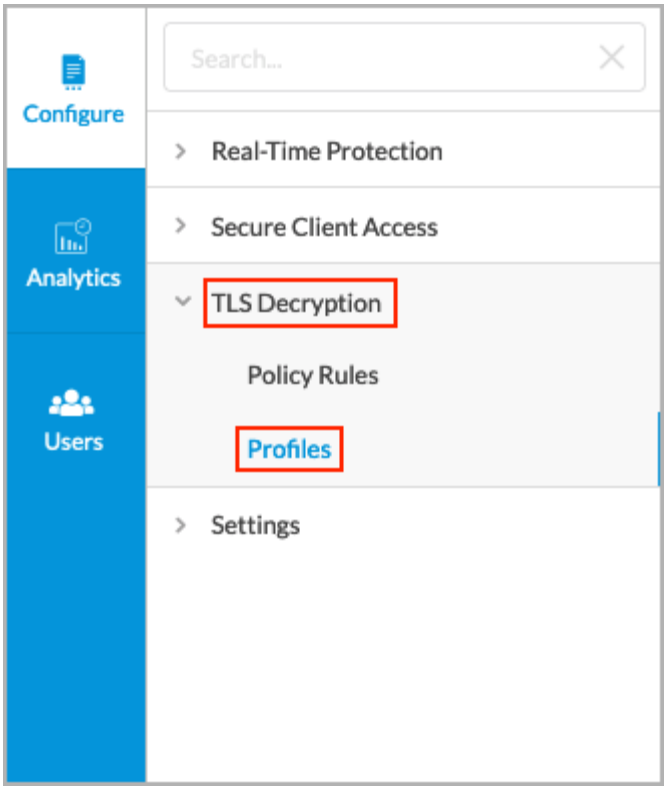
35. Click Save.

Create a TLS Decryption Profile

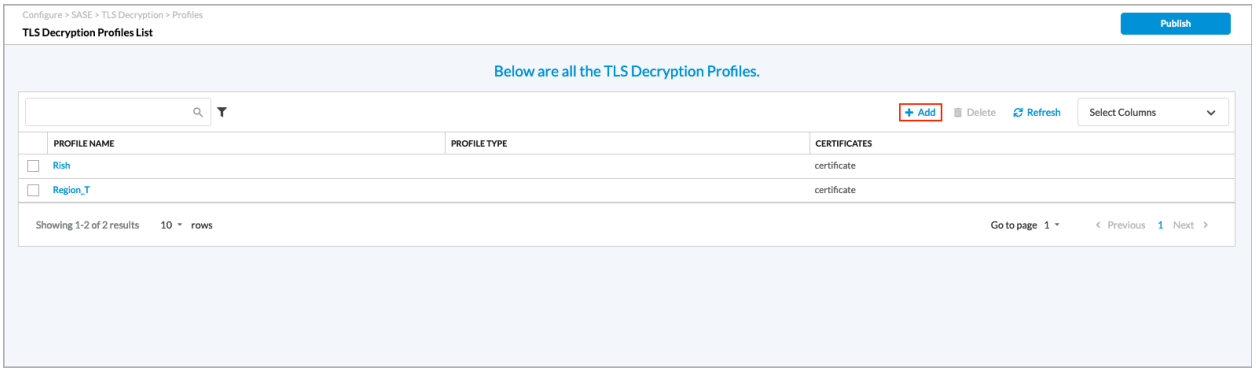
When you configure TLS decryption for a tenant, the VOS device behaves as an SSL proxy, and it generates a TLS/SSL certificate for each HTTPS URL that the tenant tries to access (for example, https://example.com). The certificate allows the VOS device to inspect the data flow and take any necessary actions. To optimize the SSL proxy behavior, the VOS device uses the same generated public–private key pair for certificates issued across domains. This key pair is generated for each configured decryption profile, and hence is unique for each tenant.

To create a TLS decryption profile:

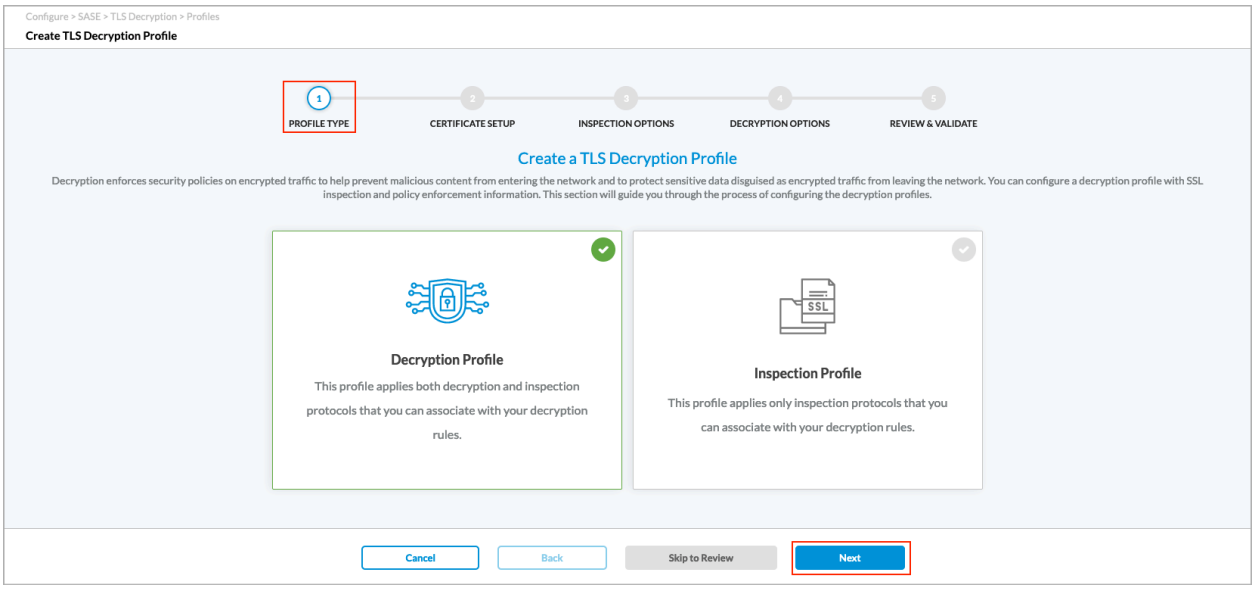
1. Go to Configure > TLS Decryption > Profiles.



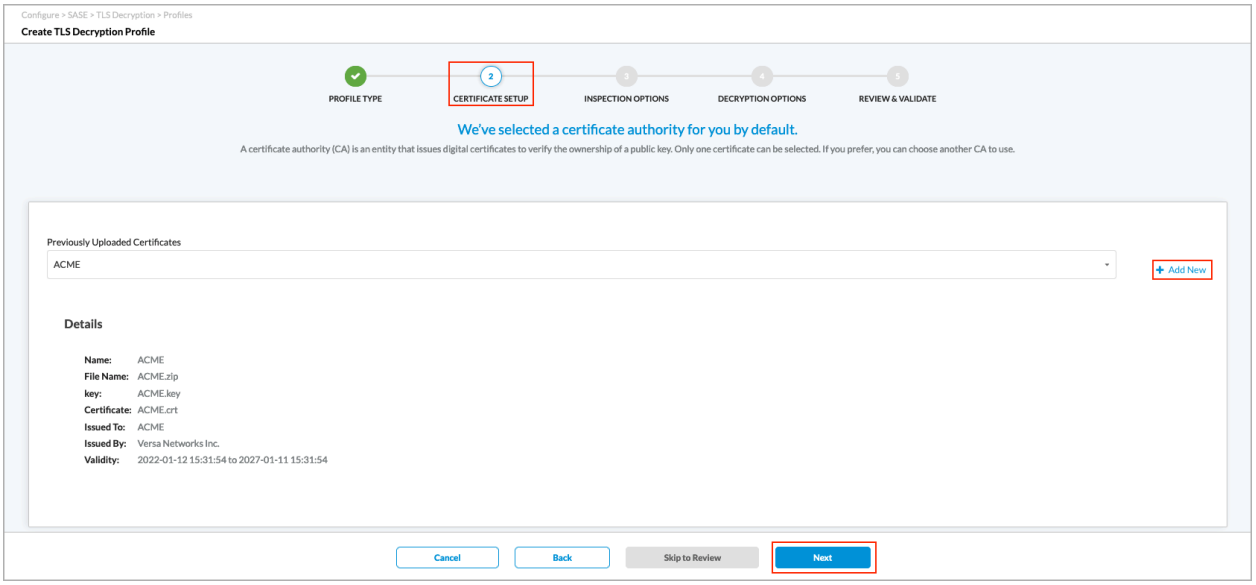
The TLS Decryption Profiles List screen displays all current profiles.



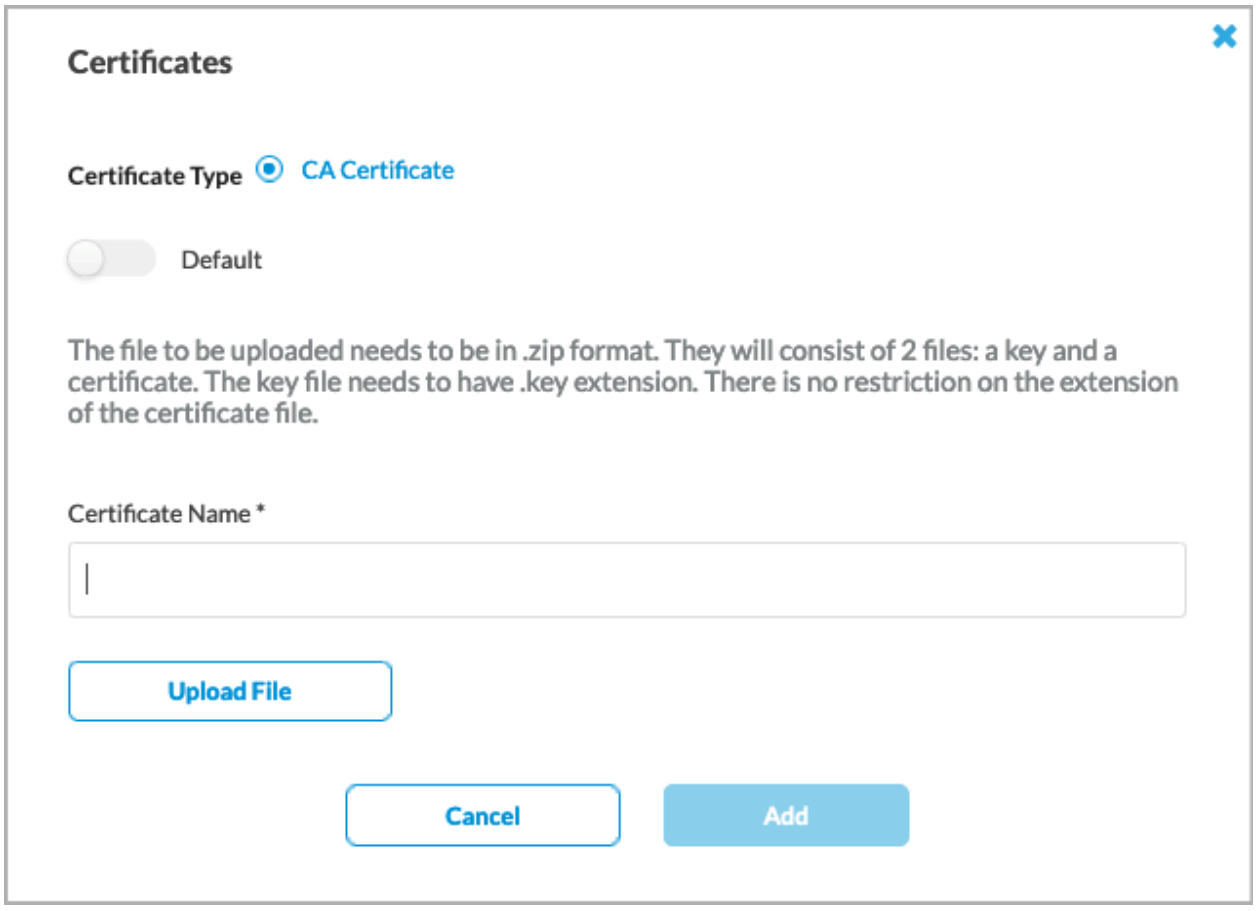
2. Click + Add New to add a TLS decryption profile. The Create TLS Decryption Profile screen displays with the first step, Profile Type, selected by default. Decryption enforces security policies on encrypted traffic to help prevent malicious content from entering the network and to protect sensitive data disguised as encrypted traffic from leaving the network. You can configure a decryption profile with SSL inspection and policy enforcement information.



3. Select a decryption profile or an inspection profile:
   a. Decryption Profile—Applies both decryption and inspection protocols that you can associate with your decryption rules.
   b. Inspection Profile—Applies only inspection protocols that you can associate with your decryption rules.
4. Click Next to go to Step 2, Certificate Setup.

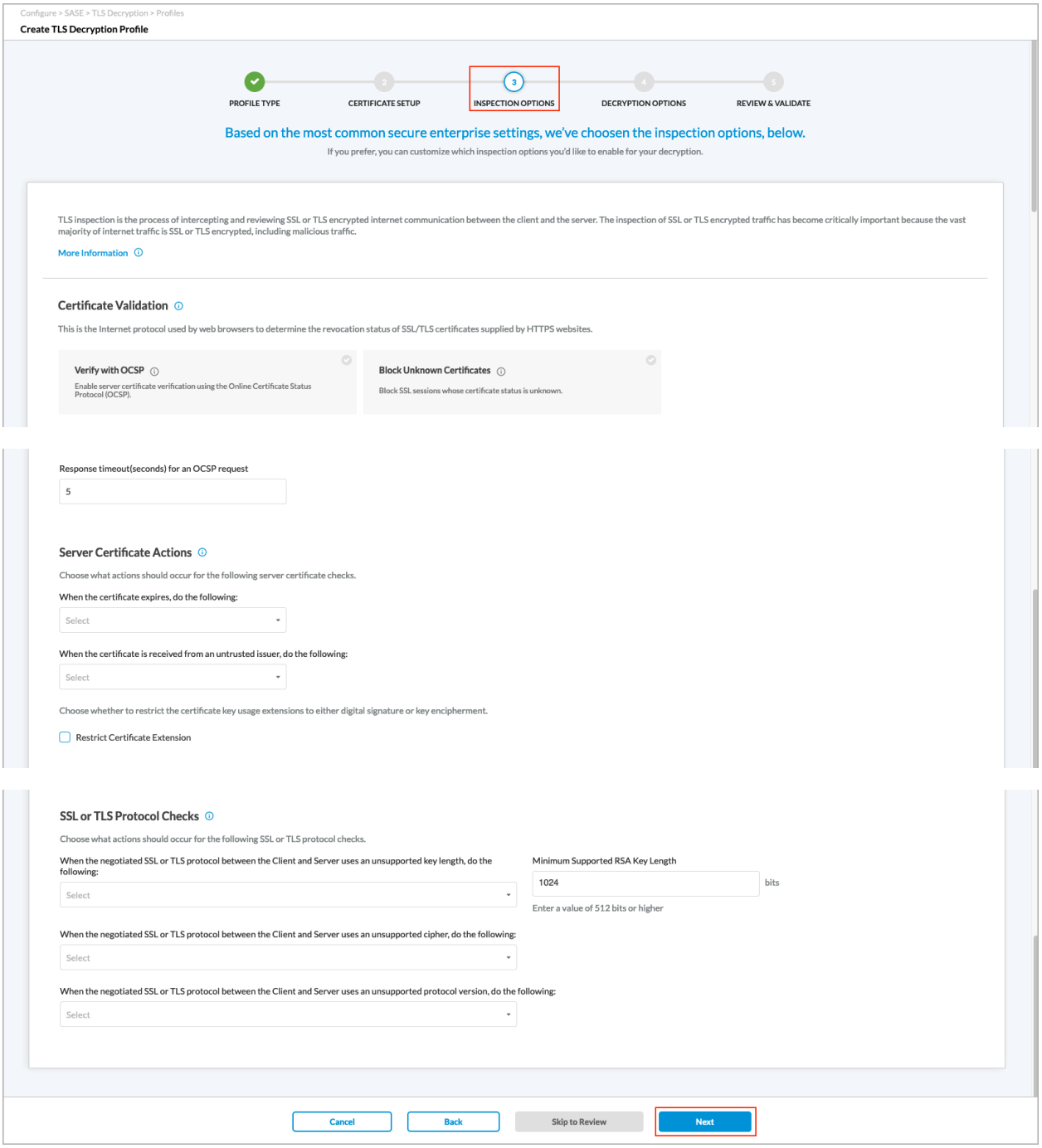


5. Click Next to accept the default certificate authority (CA). To use a different CA, select one of the previously uploaded certificates, or click + Add New to configure a new CA. In the Certificates popup window, enter information for the following fields.



Field	Description
Certificate Type	Click CA Certificate.
Default slide	Click the slider to have the added CA certificate to be the default CA certificate. 
Certificate Name	Enter a name for the certificate.
Upload File	Click to upload a CA certificate file.
Add	Click to add the new certificate.

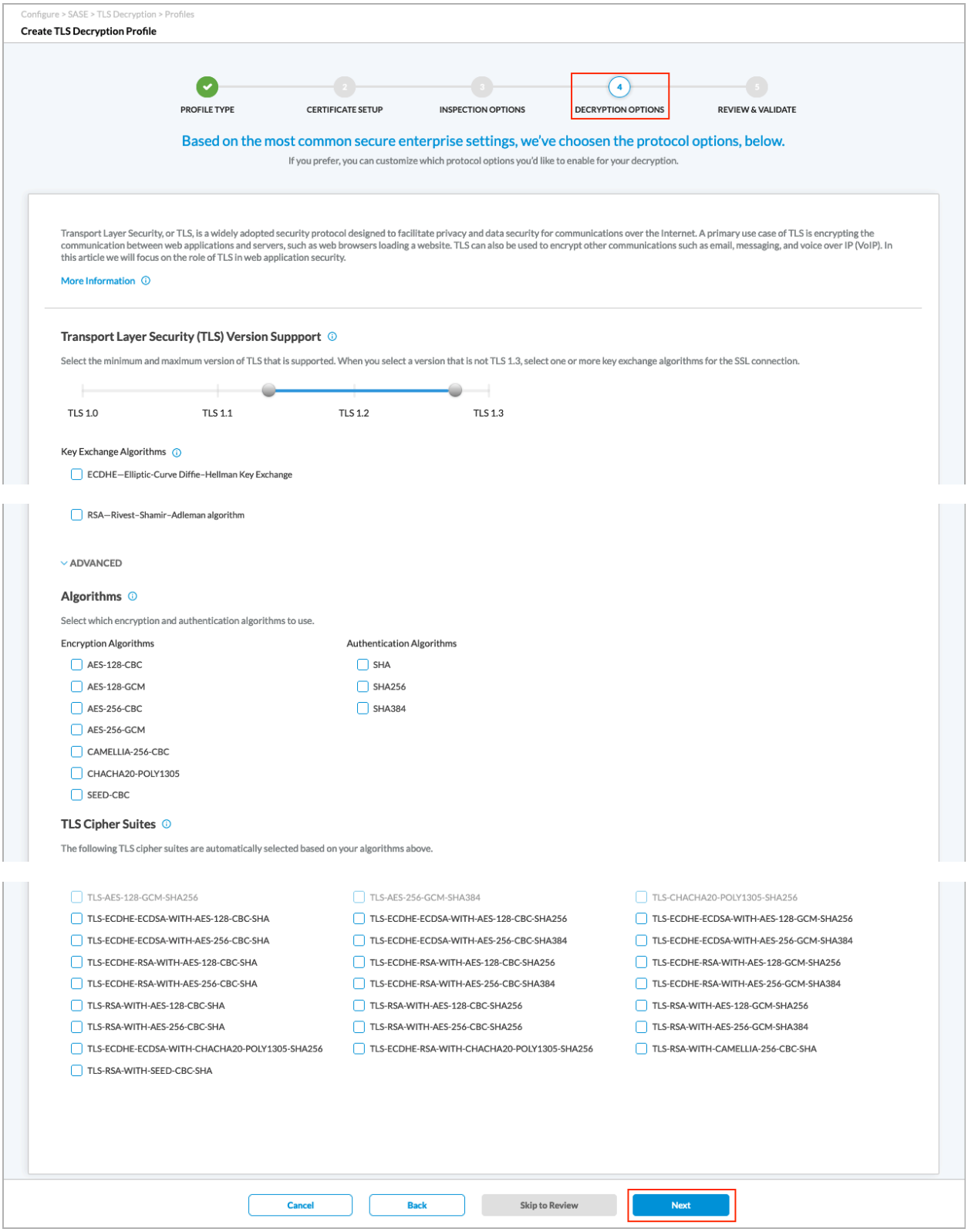
6. Click Next to go to Step 3, Inspection Options.



Field	Description
Certificate Validation (Group of Fields)	
◦ Verify with OCSP	Select to use the Online Certificate Status Protocol (OCSP) to verify a server certificate.

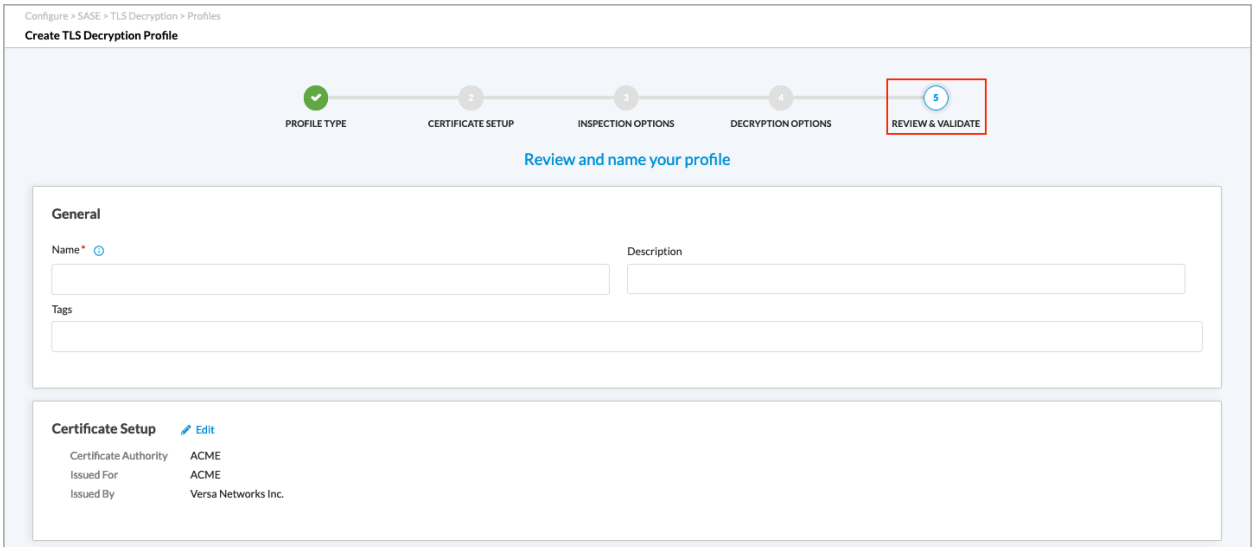
Field	Description
◦ Block Unknown Certificates	Select to block SSL sessions whose certificate status is unknown.
◦ Response timeout (seconds) for an OCSP request	Enter how long, in seconds, before an OCSP request times out. *Default*: 5 seconds *Range*: 1 to 255 seconds
Server Certificate Actions (Group of Fields)	
◦ When the certificate expires, do the following:	Select an action to take when the certificate expires.
◦ When the certificate is received from an untrusted issuer, do the following	Section an action to take when a certificate is received from an untrusted issuer.
◦ Restrict Certificate Extension	Click to choose whether to restrict the certificate key usage extensions to either digital signature or key encipherment.
SSL or TLS Protocol Checks (Group of Fields)	
◦ When the negotiated SSL or TLS protocol between the client and server uses an unsupported key length, do the following:	Select an action to take when SSL or TLS between the client and server uses an unsupported key length.
◦ Minimum Supported RSA Key Length	Enter the minimum supported RSA key length, in bits. *Default*: 1024 bit *Range*: 512 bits or longer
◦ When the negotiated SSL or TLS protocol between the client and server uses an unsupported cipher, do the following:	Select an action to take when SSL or TLS between the client and server uses an unsupported cipher.
◦ When the negotiated SSL or TLS protocol between the client and server uses an unsupported protocol version, do the following:	Select an action to take when SSL or TLS between the client and server uses an unsupported protocol version.

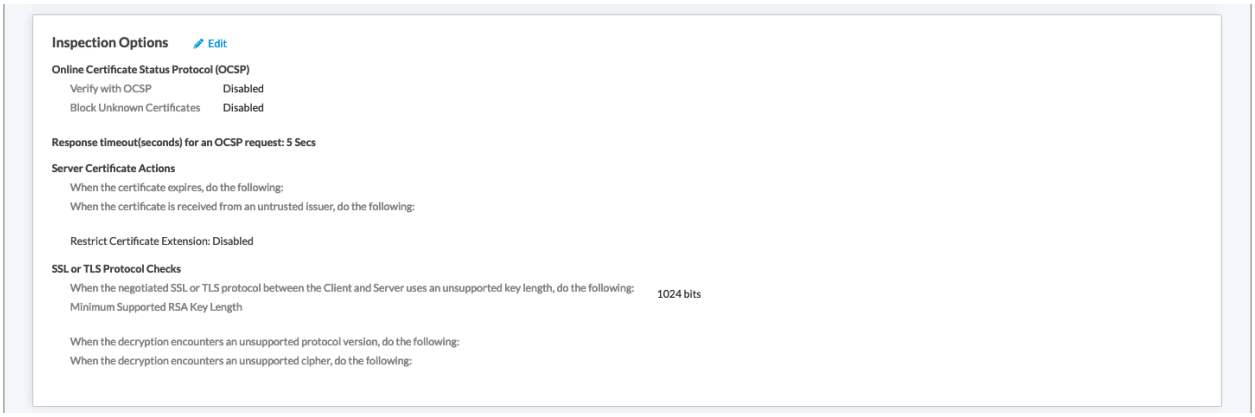
7. Click Next to go to Step 4, Decryption Options, and then enter information for the following fields.

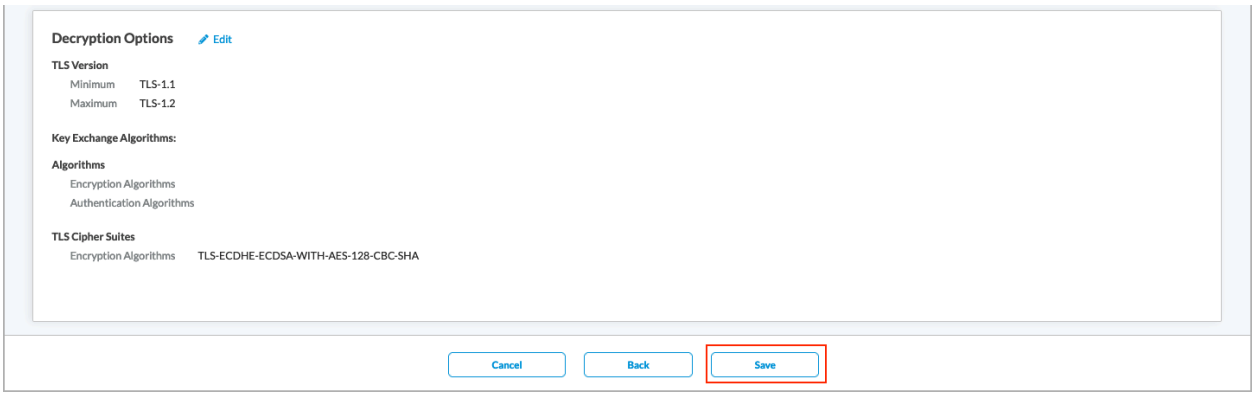


Field	Description
Transport Layer Security (TLS) Version Support (Group of Fields	
◦ Minimum and maximum version of TLS that is supported	Use the slider to select the minimum and maximum TLS version that is supported. If you select a version that is not TLS 1.3, select one or more key exchange algorithms for the SSL connection.
◦ Key Exchange Algorithms	Select one or more key exchange algorithms: ◦ ECDHE—Elliptic-Curve Diffie-Hellman Key Exchange ◦ RSA—Rivest-Shamir-Adleman algorithm.
Advanced	Click to configure algorithms and TLS cipher suites.
Algorithms	Select which encryption and authentication algorithms to use.
TLS Cipher Suites	Displays the TLS cipher suites selected depending on the algorithms.

8. Click Next to go to Step 5, Review & Validate, and then enter information for the following fields.







Field	Description
General (Group of Fields)	
◦ Name	Enter a name for the TLS decryption profile.
◦ Description	Enter a text description for the profile.
◦ Tags	Enter one or more tags. A tag is an alphanumeric text descriptor with no spaces or special characters that is used for searching profiles. You can specify multiple tags.

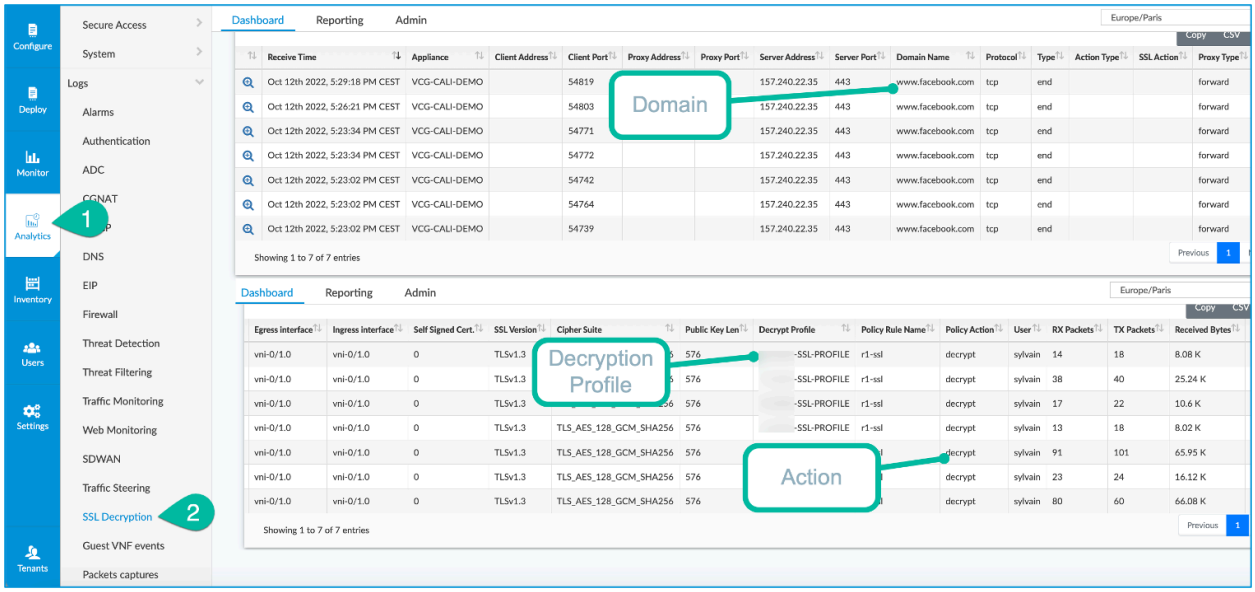
9. Review the Certificate Setup, Inspection Options, and Encryption Option sections.
10. To change any of the information, click the Edit icon in the section and then make the required changes.
11. Click Save to save the new TLS decryption profile.

Verification

To verify TLS decryption at the client level, you can check the certificate in the browser, or you can view real-time

analytics in the SASE portal.

To view real-time analytics, click Analytics in the left menu, and then go to Logs > SSL Decryption.



Configure Real-Time Protection

Real-time protection policies define the actual behavior of the firewall inside the Versa SASE platform. You can configure the following types of real-time protection in Concerto:

- Internet protection rules—Firewall rules are applied on the Versa Secure Web Gateway for internet-bound traffic.
- Private application protection rules—Firewall rules are applied on the Versa Gateway for traffic that stays within the enterprise VPN.

The following sections define the different protection rules and how to use them.

Configure SASE Internet Protection Rules

Internet protection rules are firewall rules that are applied to internet-bound traffic on a per-tenant basis. They provide network protection by establishing match criteria and enforcement actions. To configure internet protection rules, you configure the following match criteria and enforcement actions:

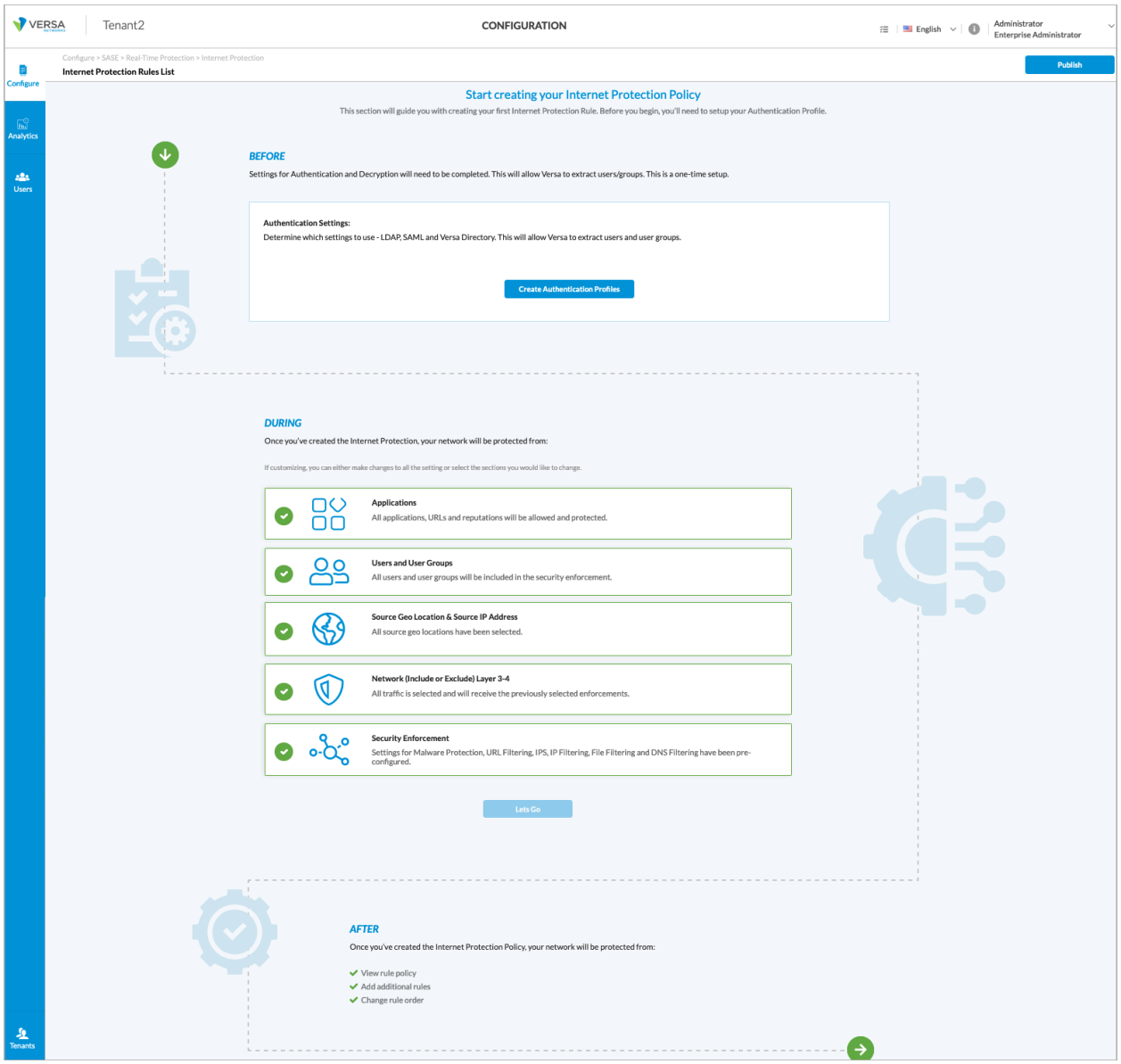
- Applications—Match criteria based on individual applications, groups of applications, categories of applications, predefined URL categories (such as business and economy, computer and internet security, and entertainment and arts), and predefined reputations (such as high and low risk).
- User and user groups—Match criteria based on individual users or groups of users.
- Source geolocation and source IP address—Match criteria based on the geographic location of source or destination traffic.
- Network Layer 3 and Layer 4—Match criteria based on the IP address of the source and destination traffic or on

custom or predefined protocol-based services.

- Security enforcement—After you select the match conditions, you specify a security enforcement action, which is either allow, deny, or reject. You can also create custom security enforcement profiles in which you specify the enforcement criteria.

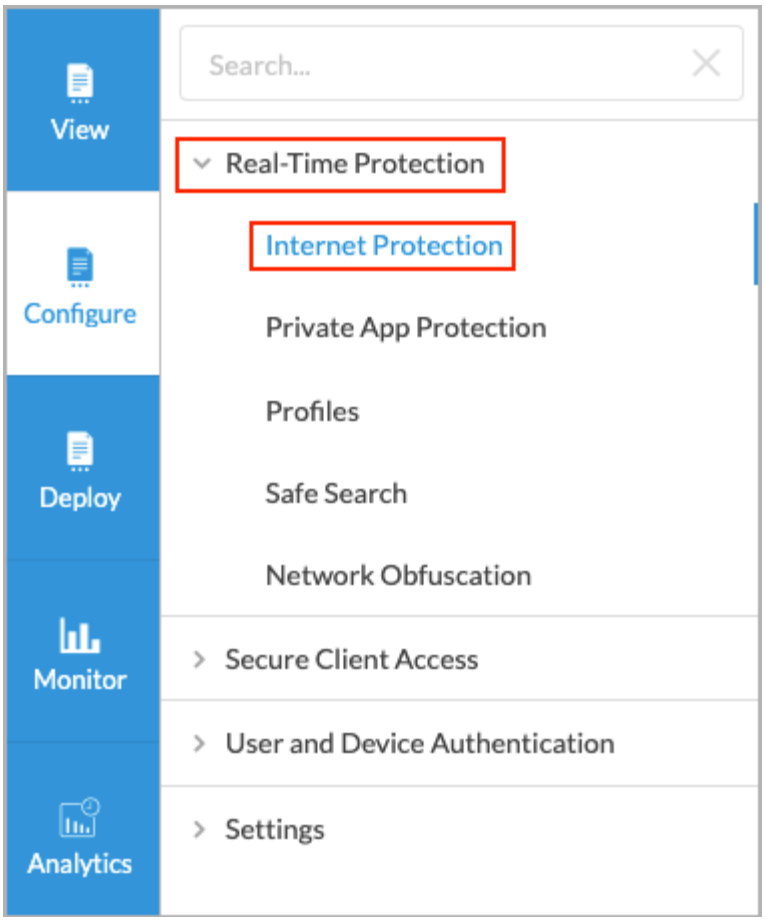
After you configure match criteria and security enforcement actions, you review and deploy the internet protection rule.

The first time you create an internet protection policy rule, a wizard displays (shown in the screenshot below) that guides you through the configuration steps. Thereafter, you do not see this wizard. You configure subsequent rules manually using the Internet Protection Rules screens.



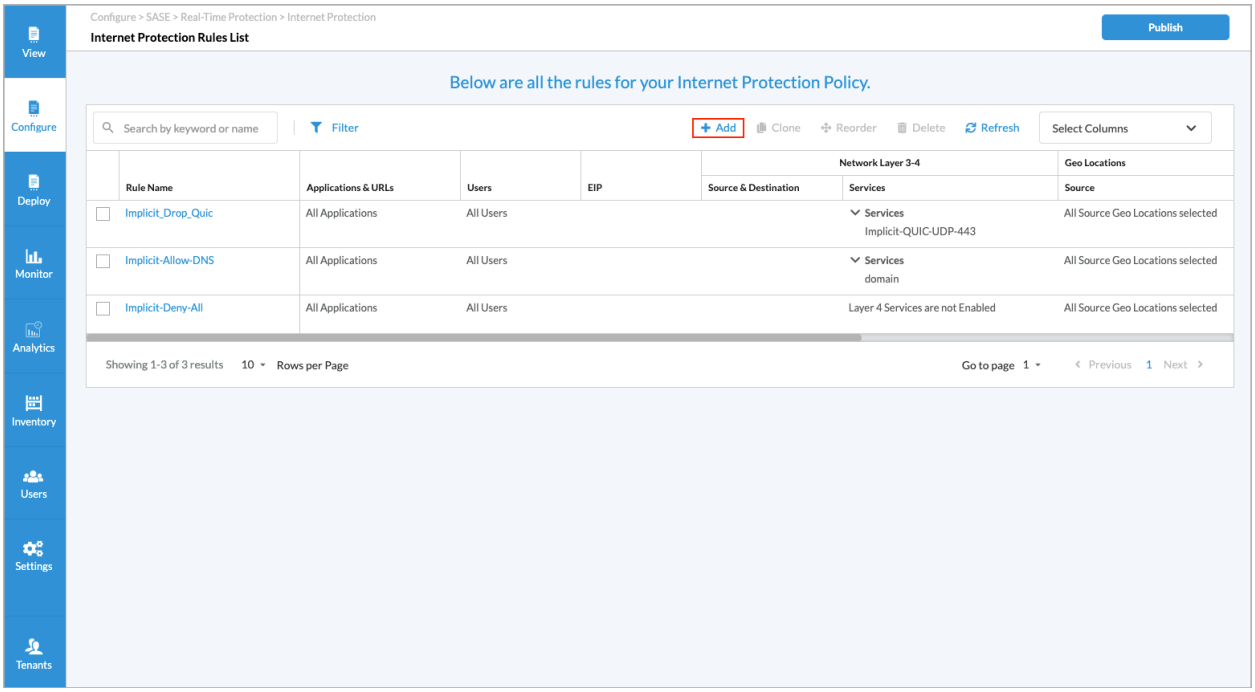
To configure an internet protection rule:

1. Go to Configure > Real-Time Protection > Internet Protection.



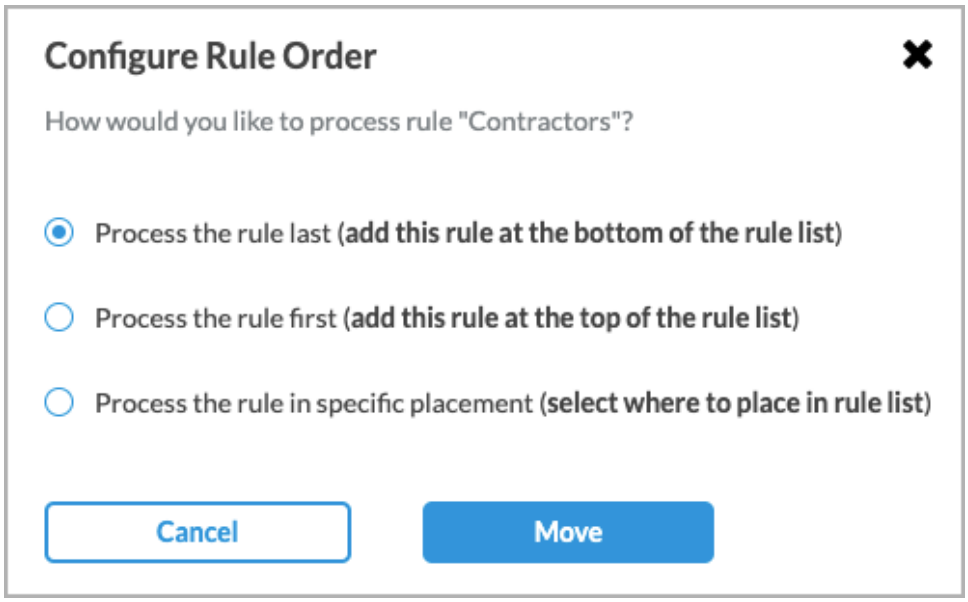
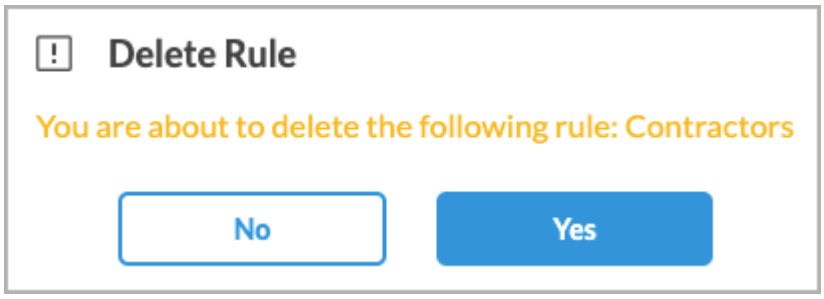
The Internet Protection Rules List screen displays all configured internet protection rules.

Updated: Wed, 23 Oct 2024 08:37:20 GMT



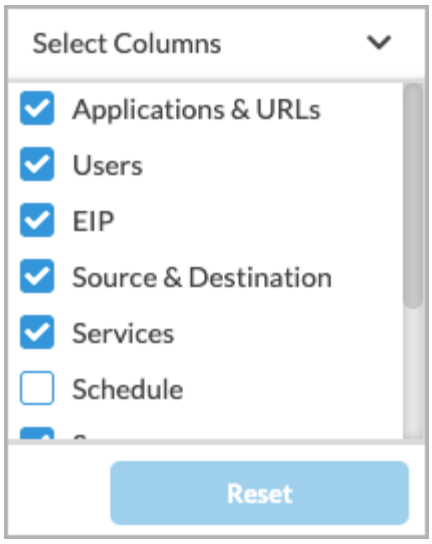
2. In the horizontal menu bar, you can select one of the following operations.

Operation	Description
Add	Create a new internet protection rule. This button is active when no existing rule is se
Clone	Clone the selected internet protection rule. When you select this option, the configura Review & Deploy screen selected. You can rename the default name of the cloned ru
Reorder	Reorder the selected internet protection rule. A popup window similar to the following

Operation	Description
	 1. Select the rule order: ◦ Process the rule last. ◦ Process the rule first. ◦ Process the rule in specific placement—A list of the existing rules displays. Click place the rule. 2. Click Move.
Delete	Delete the selected internet protection rule. A popup window similar to the following d  Click Yes to delete the internet protection rule, or click No to retain the rule.
Refresh	Refresh the list of existing rules.

3. To customize which columns display, click Select Columns and then click the columns to display or hide. Click

Reset to return to the default column settings.



4. In the Internet Protection Rules List screen, click + Add to create a rule. The Create Internet Protection Rule screen displays.

From here, you configure the match criteria and enforcement actions. For more information, see:

- Configure SASE Internet Protection Rule Match Criteria
- Configure Security Enforcement Actions for SASE Internet Protection Rules

Configure SASE Private Application Protection Rules

SASE private application protection rules are firewall rules that you configure to define protection for custom applications. You configure these protection rules on a per-tenant basis. Private application protection is similar to internet protection, except that private application protection applies only to custom applications. You cannot configure private application protection for predefined applications or for application groups.

Private application protection rules consist of match criteria and enforcement actions. You can configure the following match criteria and enforcement actions:

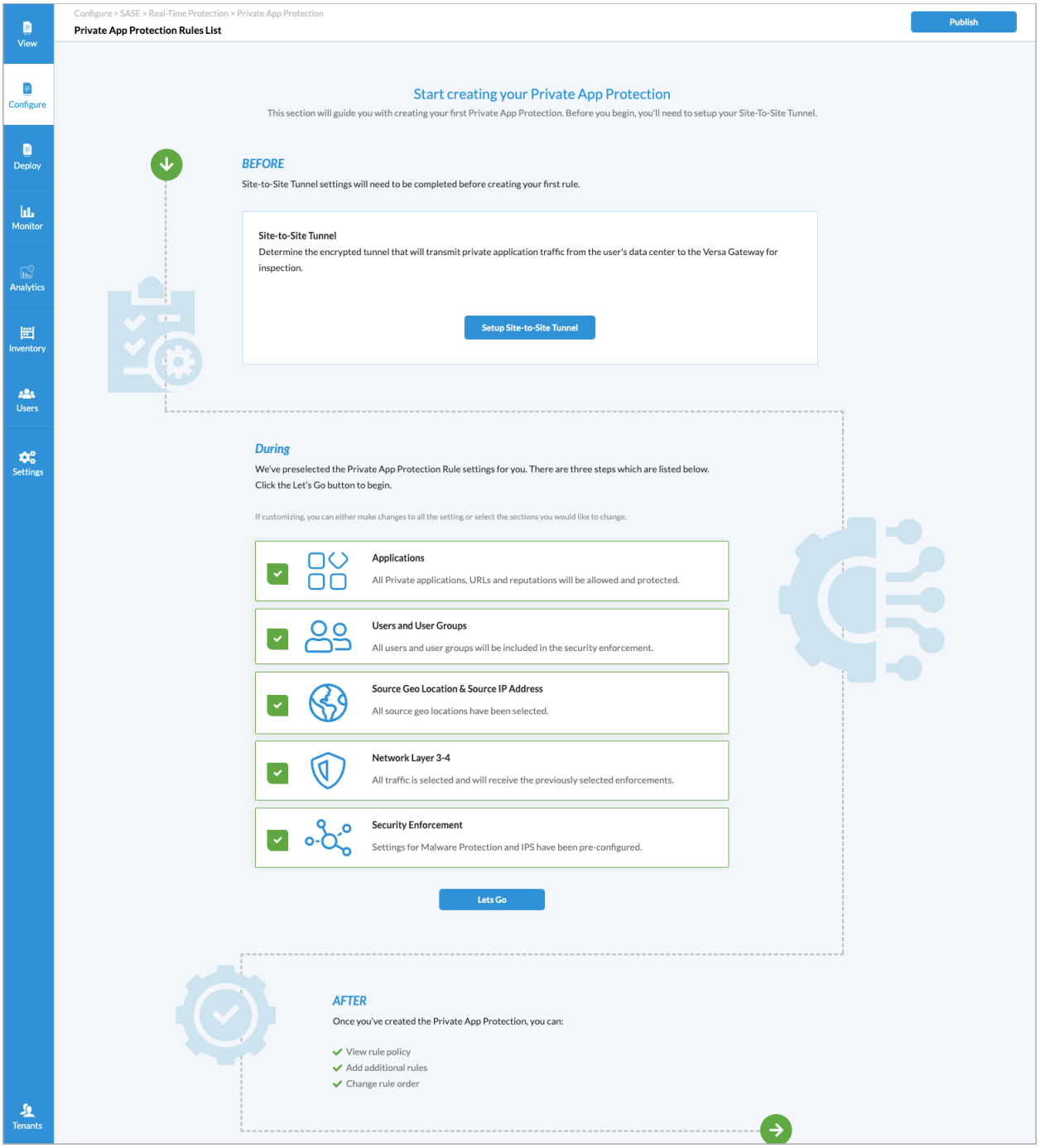
- Applications—Match criteria based on individual applications, groups of applications, categories of applications, predefined URL categories (such as business and economy, computer and internet security, and entertainment and arts), and predefined reputations (such as high and low risk).
- User groups—Match criteria based on individual users or groups of users.
- Geolocation—Match criteria based on the geographic location of the source or destination traffic.
- Network Layer 3 and Layer 4—Match criteria based on the IP address of the source and destination traffic or on custom or predefined protocol-based services.
- Security enforcement—Security enforcement actions that are applied to traffic that matches the match criteria. You

can allow, deny, or reject the traffic, and you can also create custom security enforcement profiles.

After you configure match criteria and security enforcement actions, you review and deploy the private protection rule.

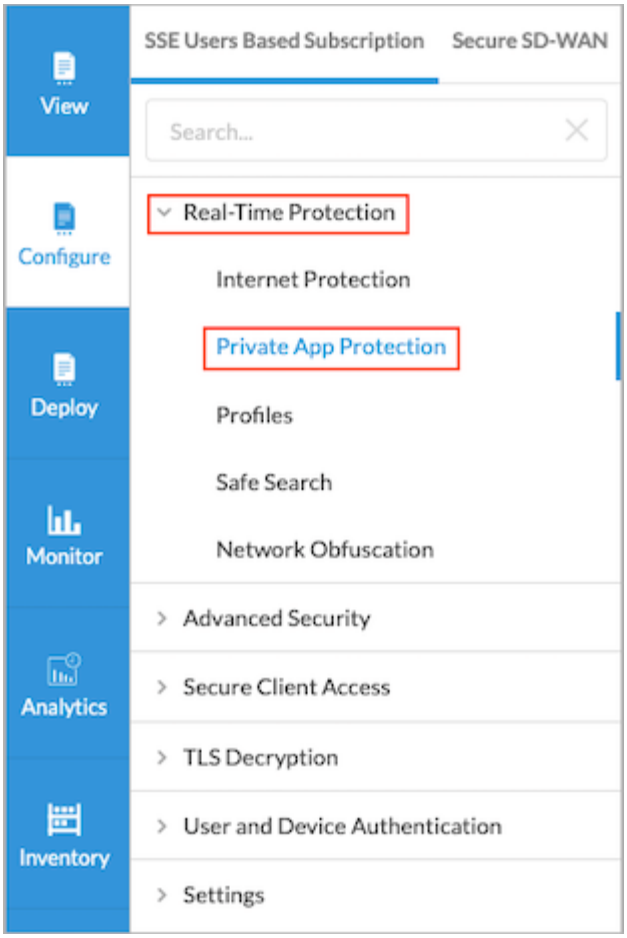
To configure private application protection, you must first create one or more private applications under Configure > Settings > User-Defined Objects > Applications. For more information, see Configure SASE User-Defined Objects. After you have created a private application, you create a private application rule in much the same way that you configure an internet protection rule.

The first time you create a private application protection policy rule, a wizard (shown in the screenshot below) guides you through the configuration steps. Thereafter, you do not see this wizard. You configure subsequent rules manually using the Private Application Protection Rules screens.

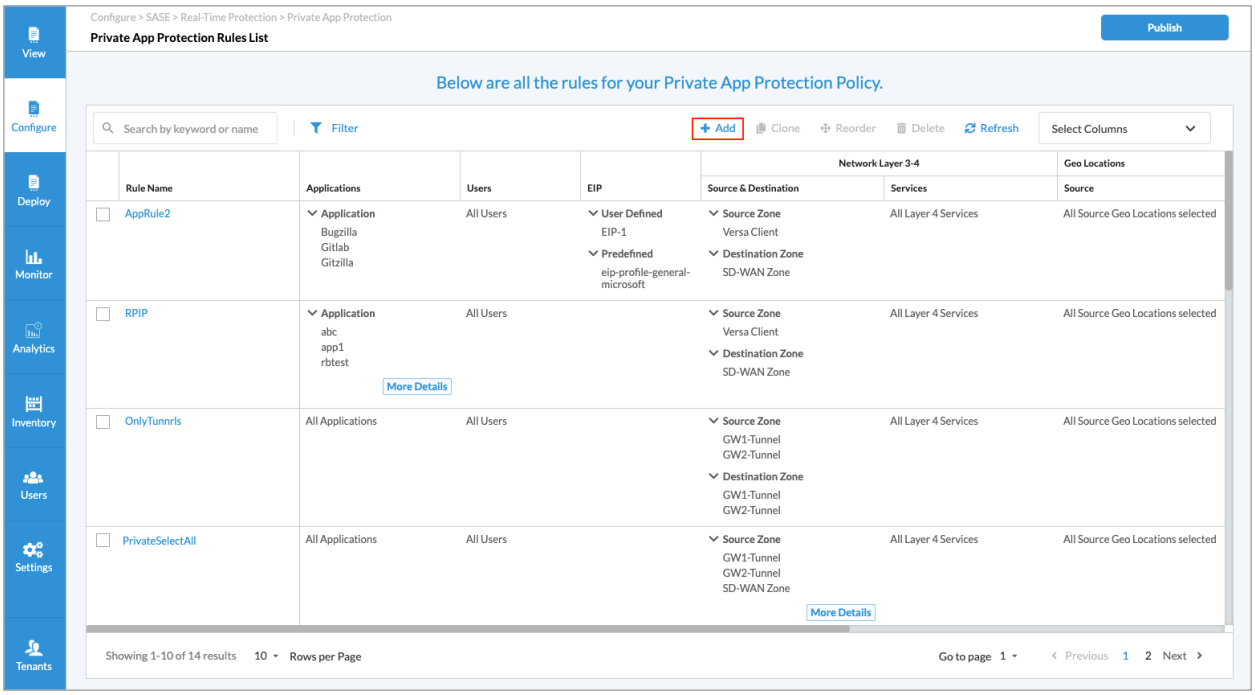


To configure a private application protection rule:

1. Go to Configure > Real-Time Protection > Private Application Protection.

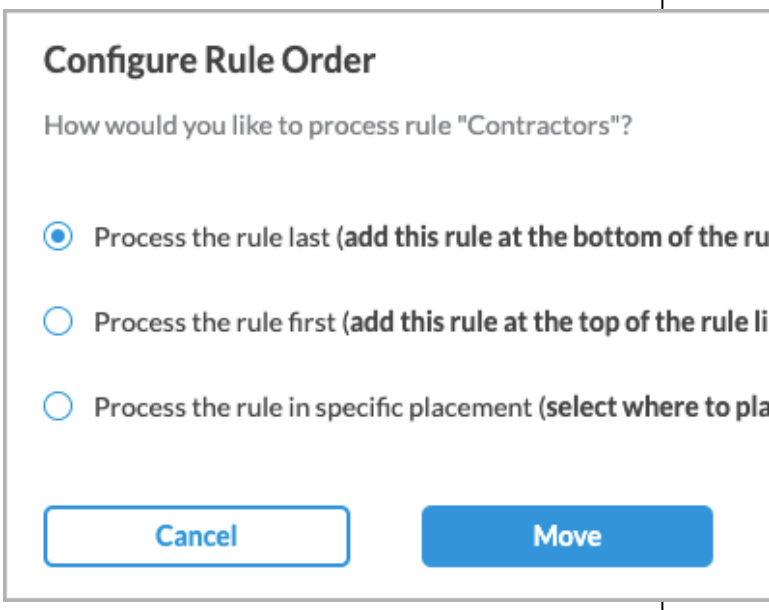
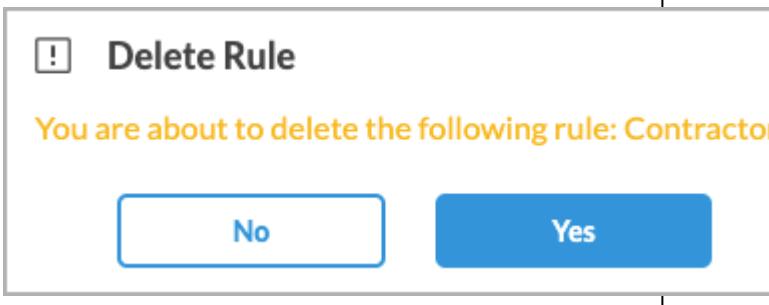


The Private Application Protection Rules List screen displays all the private application protection rules that are already configured.



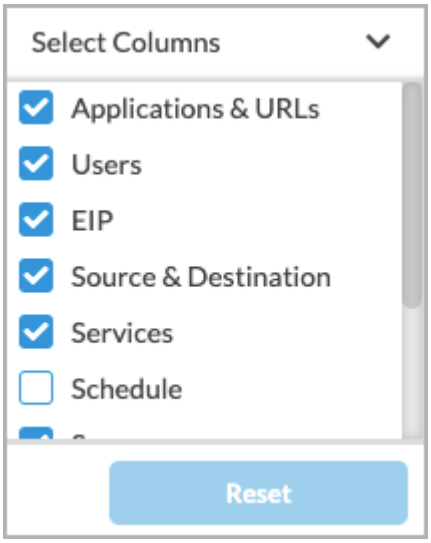
2. In the horizontal menu bar, you can perform the following operations.

Operation	Description
Add	Create a new internet protection rule. This button is active when no existing rule is selected.
Clone	Clone the selected private application protection rule. If you select this option, the configuration wizard for the rule displays with the Review & Deploy screen selected. You can rename the default name of the cloned rule, if desired, then click Save.
Reorder	Reorder the selected private application protection rule. A popup window similar to the following displays.

Operation	Description
	 1. Select one of the three options: ◦ Process the rule last ◦ Process the rule first ◦ Process the rule in specific placement—A list of the existing rules displays. Click the position in the list where you want to place the rule. 2. Click Move.
Delete	Delete the selected private application protection rule. A popup window similar to the following displays.  Click Yes to delete the internet protection rule, or click

Operation	Description
	No to retain the rule.
Refresh	Refresh the list of existing rules.

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



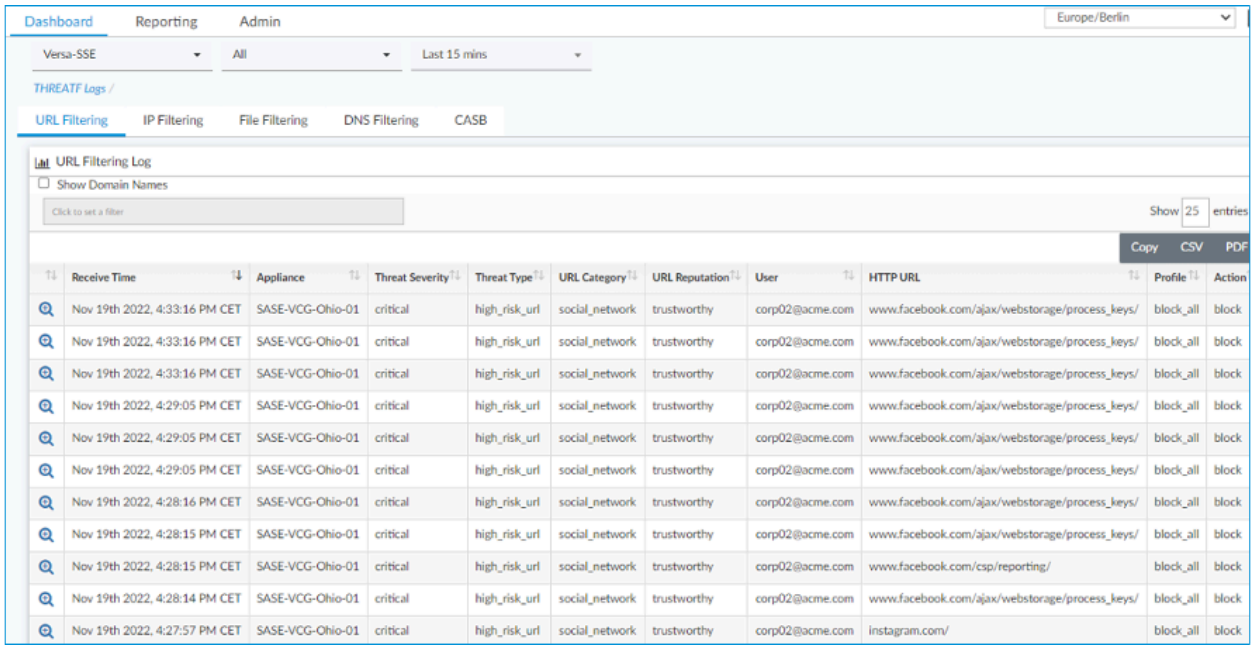
4. In the Private Application Protection Rules List screen, click + Add to create a rule. The Create Private Application Protection Rule screen displays.

From here, you configure the match criteria and enforcement actions. For more information, see:

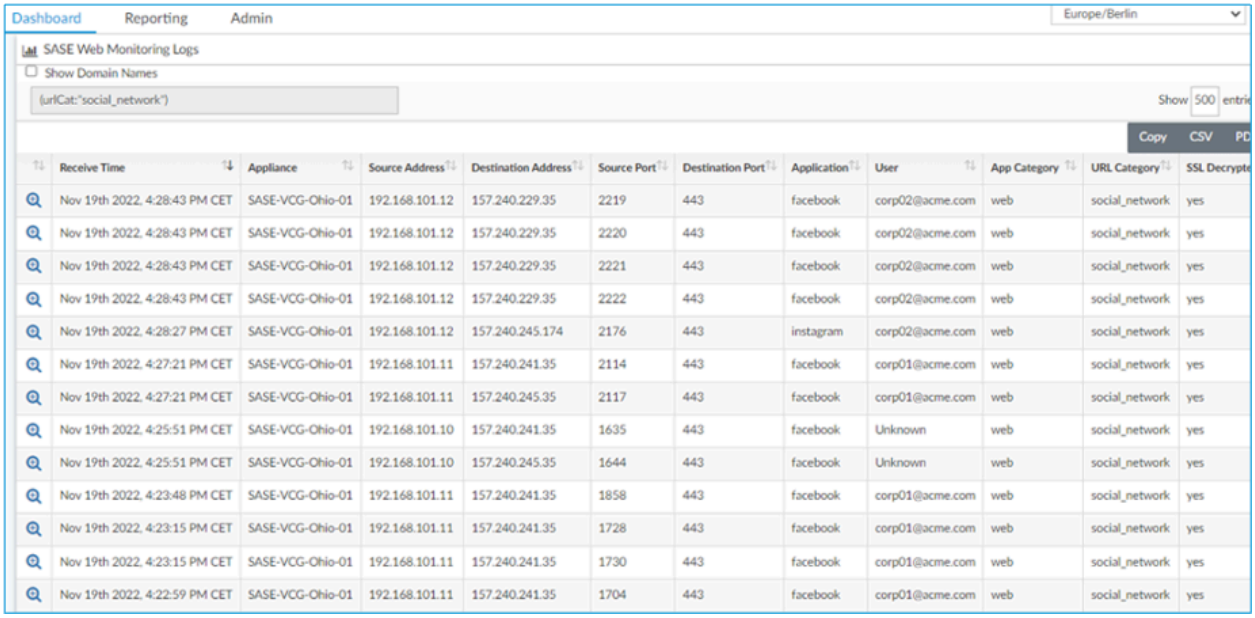
- Configure SASE Private Application Protection Rule Match Criteria
- Configure Security Enforcement Actions for SASE Private Application Protection Rules

Verification

To verify the session details for filtered or blocked sessions, click Analytics in the left menu, and then go to Logs > Threat Filtering.



To view a log of all Web sessions which were allowed or denied, click Analytics in the left menu, and then go to Dashboards > SASE Web Monitoring.



Configure Advanced Internet Protection with CASB

Cloud Access Security Broker (CASB) is on-premises or cloud-based policy enforcement that secures the data flowing between users and cloud applications in order to comply with corporate and regulatory requirements. CASB applies enterprise security policies when users access cloud-based resources.

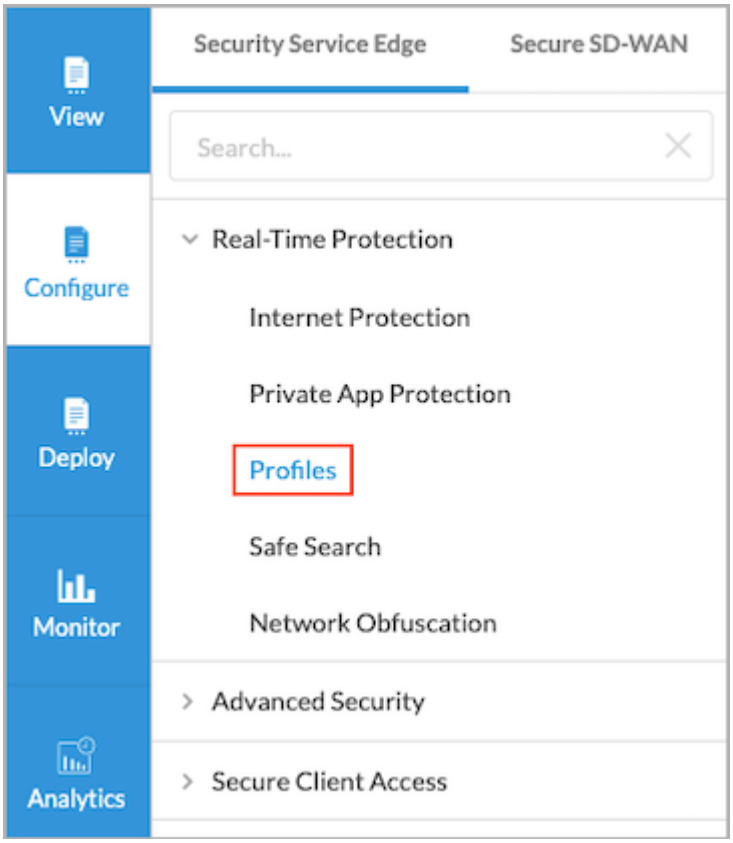
To enforce CASB security policies, you create one or more CASB profiles, specify match criteria for applications, and then associate CASB profiles with an internet protection rule. For Releases 12.1.1 and later, you add CASB rules to configure CASB profiles. You can also add constraint profiles to configure constraints from and to users or user groups. You associate constraint profiles with CASB profiles.

To use CASB, you must be using premium security pack (SPack) Version 1939 or later.

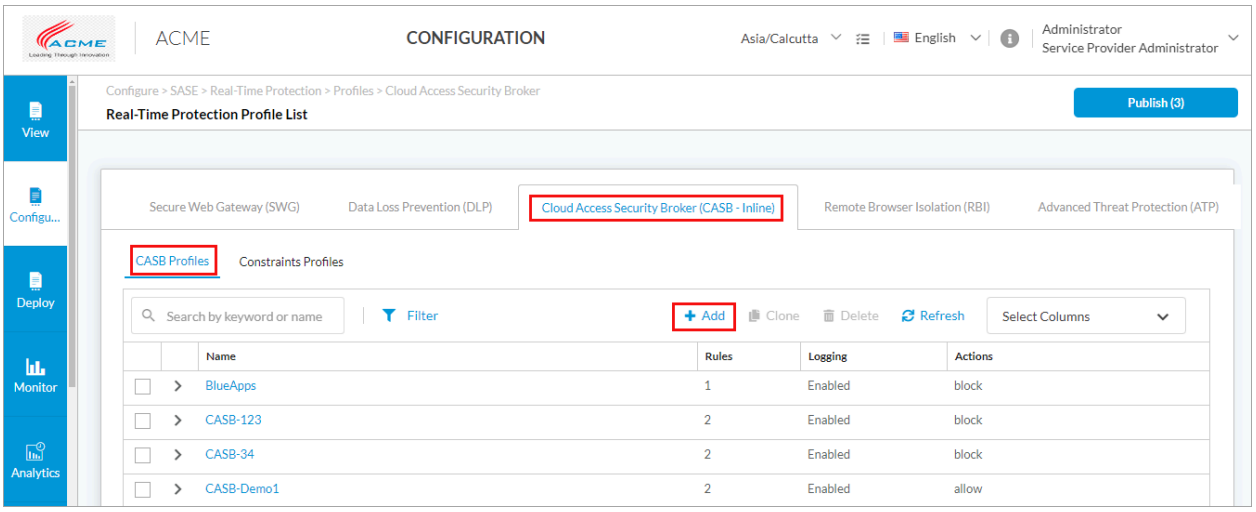
Configure a Custom CASB Profile

For Releases 12.1.1 and later.

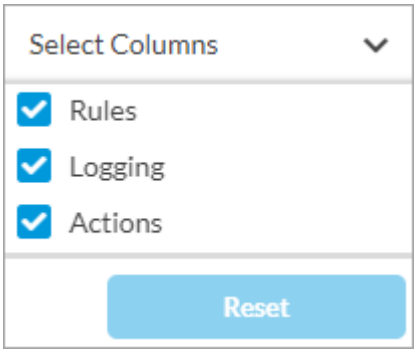
1. Go to Configure > Secure Services Edge > Real-Time Protection > Profiles.



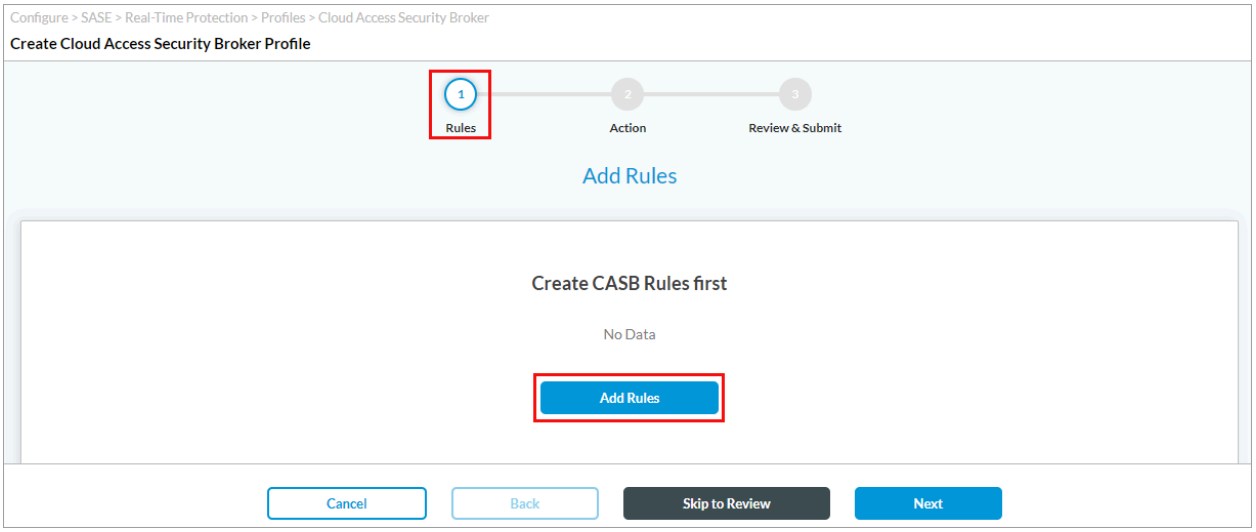
The following screen displays.



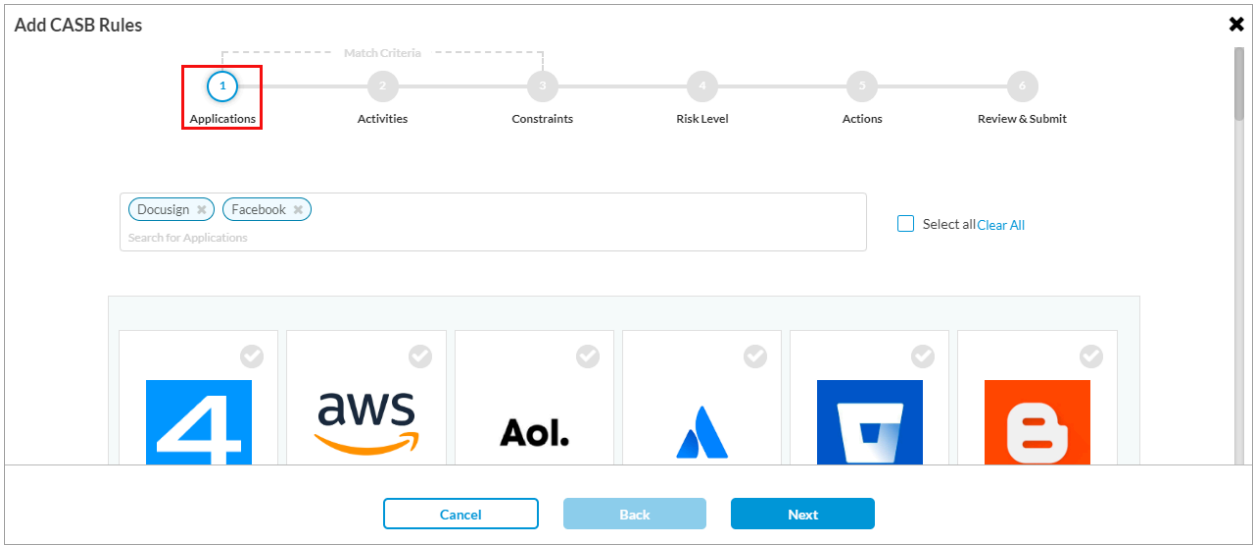
2. Select the Cloud Access Security Broker (CASB Inline) tab.
3. To customize which columns display, click Select Columns, and then click Applications to display or hide the applications. Click Reset to return to the default columns settings.



4. Select the CASB Profiles tab.
5. Click + Add to create a profile. The Create Cloud Access Security Broker Profile screen displays.



6. In Step 1, Rules, click Add Rules to create CASB rules. You must add at least one rule to proceed. The Add CASB Rules screen displays.



7. In Step 1, Applications, select the cloud applications for which you want to configure actions. You can also search for applications to select. The following web-based applications and activities are supported:

Application	Activity
4shared	Download file, login, share, upload file
Amazon AWS	Login
AOL	Login
Atlassian	Login
Bitbucket	Download file, login
Blogger	Download file, upload file
Box.net	Download file, login, search, share, upload file
Craigslist	Login, search
Dailymotion	Like, login, upload file, watch stream
Daum Mail	Download file, search, upload file
DocuSign	Login, upload file
Dropbox	Download file, login, search, share, upload file
eBay	Login, search, upload file
Evernote	Login
Excel Online	Download file, share

Facebook	Download file, login, post, upload file
Facebook Workplace	Login, upload file
Flickr	Upload file
GitHub	Download file, like, login, upload file
Gmail	Download file, send, upload file
Google Accounts	Login
Google Docs	Download file, login, share, upload file
Google Photos	Download file
Google Talk	Audio, video
imo	Audio, audio video, video
Instagram	Like, login, search, share, upload file
Jira	Login, upload file
Join.Me	Upload file
LastPass	Download file, login
Line	Audio, video
LinkedIn	Download file, like, login, post, search, upload file

Mail.ru	Download file, login
Microsoft OneNote	Download file, share
Microsoft Outlook	Download file
Microsoft Teams	Audio, audio video, download file, file transfer, like, search, share, upload file, video
Naver Mail	Download file, share, upload file
Netflix	Login
Office 365	Login
Okta	Login
OneDrive	Download file, login, share, upload file
OneLogin	Login
Pandora	Search
PayPal	Login
Pinterest	Download file, like, login, search, share, upload file
PowerPoint Online	Share
ProtonMail	Search, upload file
Reddit	Like, login, post, upload file

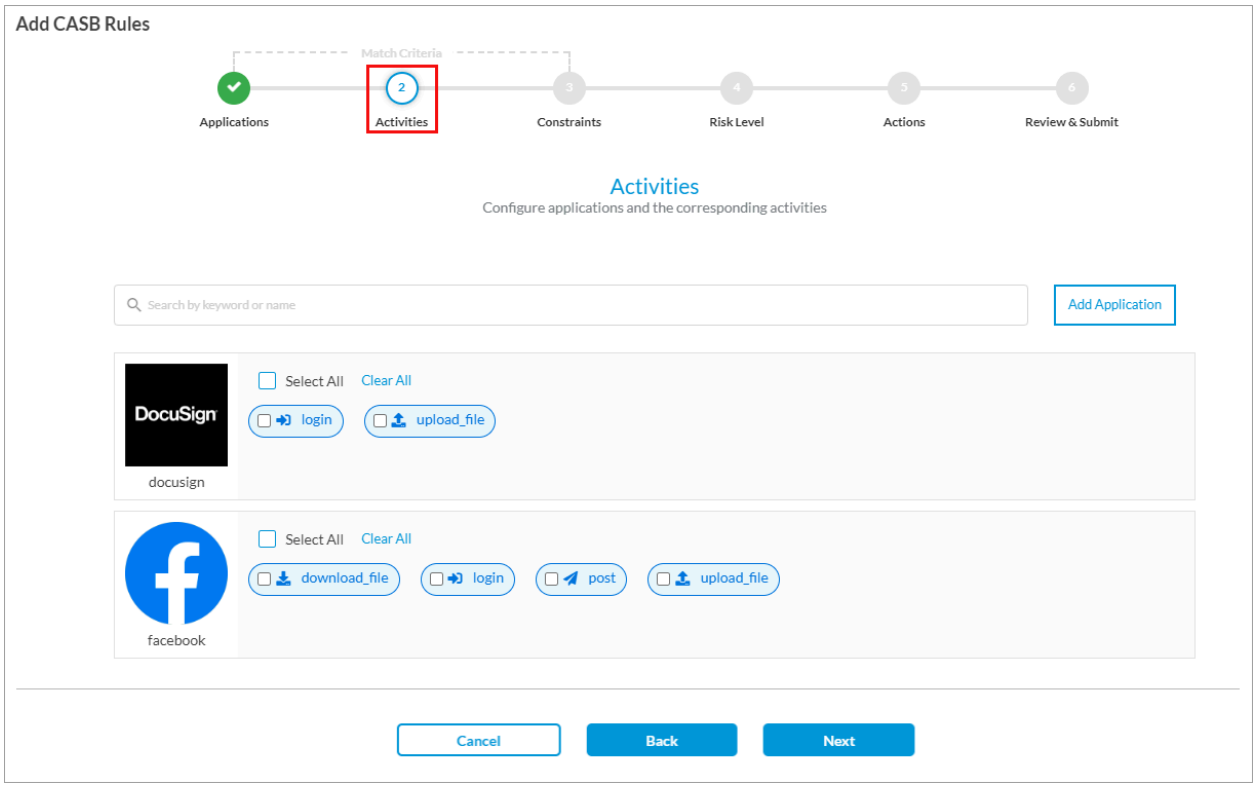
Salesforce	Login, download file
ShareFile.com	Download file, login, search, upload file
SharePoint Online	Search, share
Shopify	Login
Skype	Audio_video, file transfer, like, audio, video
Slack	Download file, like, login, post, search, share, upload file
SlideShare	Login, search, upload file
SoundCloud	Download file, login, search, upload file
SourceForge	Download file, login, search, upload file
Spotify	Like, login, search, upload file
Stack Overflow	Login, search, upload file
Tango	Audio, video
Telegram	Audio
Trello	Search, upload file
Twitch	Login, upload file, watch stream
Twitter	Like, login, post, search, upload file

Viber	Audio, video
Vimeo	Comment, like, search, upload file, watch stream
VMware	Login
Webex	Audio, audio video, login, search, video
WeChat	File transfer
WeTransfer	Download file, share
WhatsApp	Audio, audio video, video
Word Online	Download file, share, upload file
WordPress	Download file, login, upload file
Xero	Login
Yammer	Download file
Yandex	Login
Yandex Mail	Download file
YouTube	Broadcast stream, comment, download file, like, search, share, upload file, watch stream
Zalo	Audio, video
Zoom	Login

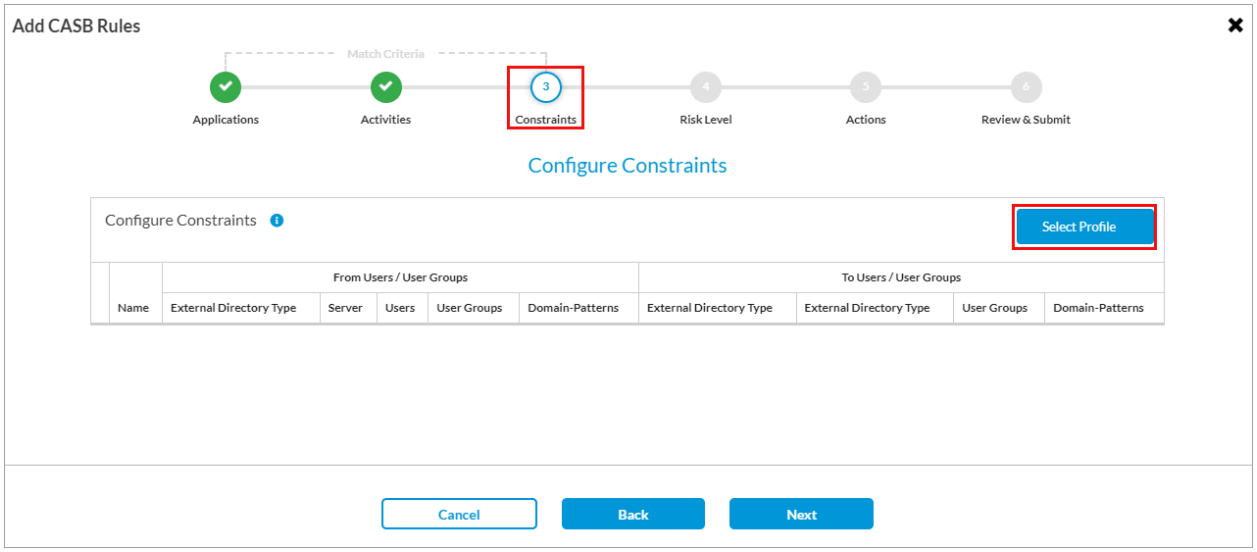
Note: The list shown above is for web-based applications. For mobile applications, a subset of applications are supported, as follows. If an application is not listed in the following table, it is supported as a web-based application and will not work in mobile devices due to certificate pinning.

SaaS Application	Web Activities Supported	Mobile Activities Supported—iOS
Box.net	Yes	Yes
Gmail	Yes	Yes—Send, upload file, download file
Google Accounts	Yes	Yes—Login
Google Docs	Yes	Yes—Upload file, login, share, download file
Gtalk	Yes	Yes—Audio, video
imo	Not applicable	Yes—Audio, video, audio video
Line	Not applicable	Yes—Audio, video
LinkedIn	Yes	Yes—Login, like, upload file, post
Office365	Yes	Yes—Login
Telegram	Not applicable	Yes—Audio
Twitch	Yes	Yes—Login, watch stream
Viber	Yes	Yes—Audio, video
WhatsApp	Yes	Yes—Audio, video, audio video
YouTube	Yes	Yes—Broadcast stream, comment, like, watch str
Zoom	Yes	Yes—Login

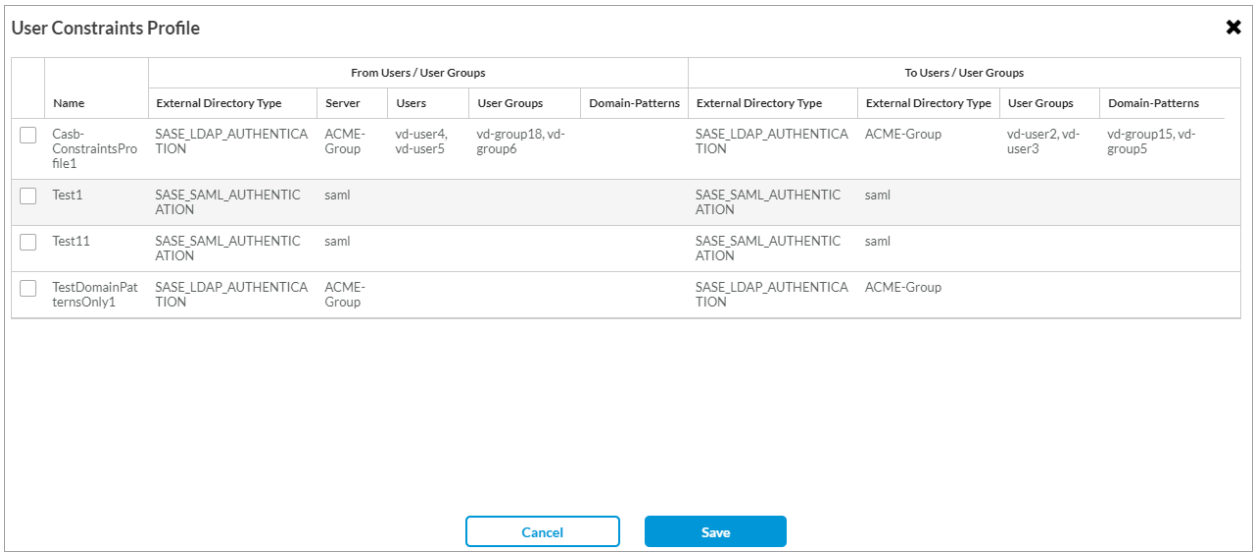
8. Click Next to go to Step 2, Activities. The screen displays the applications that you selected in Step 1, Applications.



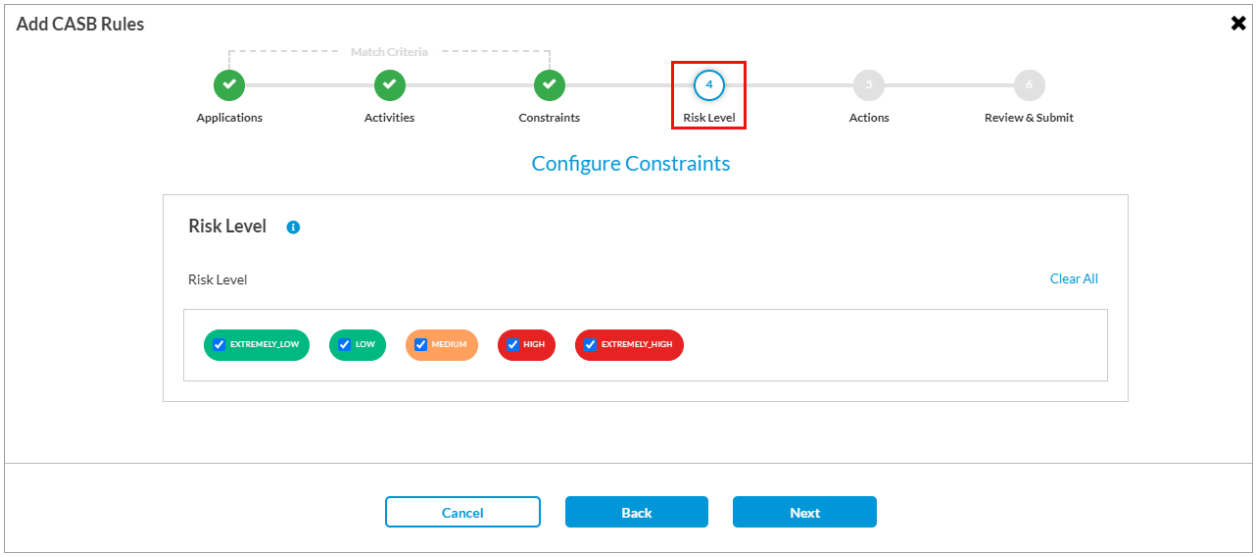
9. To add more applications, click Add Application to select more applications on the Step 1, Application screen.
10. Select the application activities for which you want to configure actions.
11. Click Next to go to Step 3, Constraints to select constraints for applications.



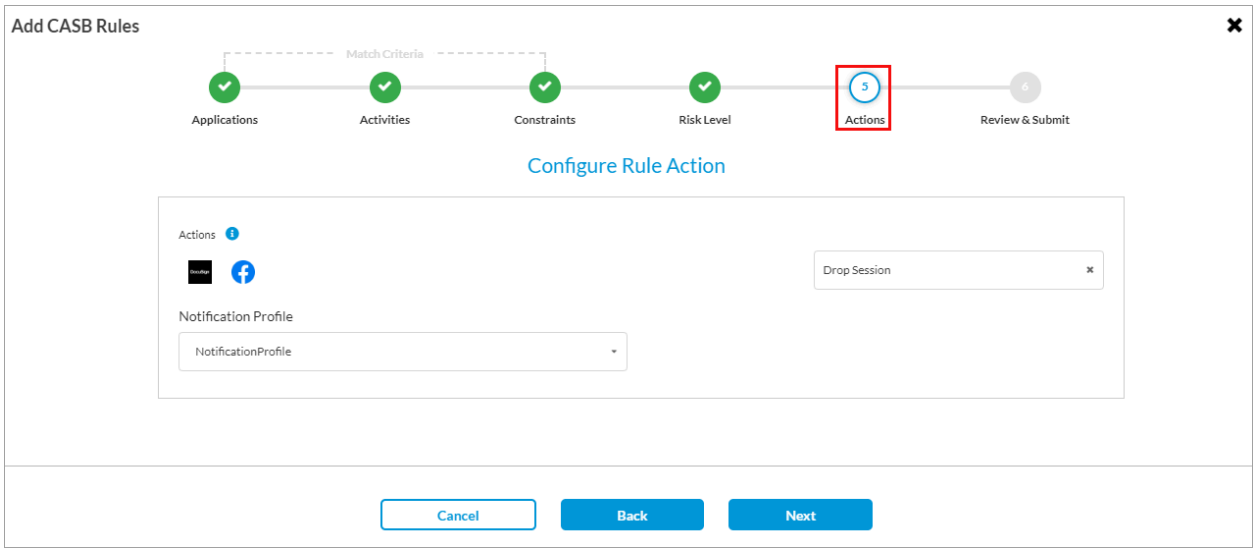
12. Click Select Profile to select a constraint profile. The User Constraints Profile screen displays.



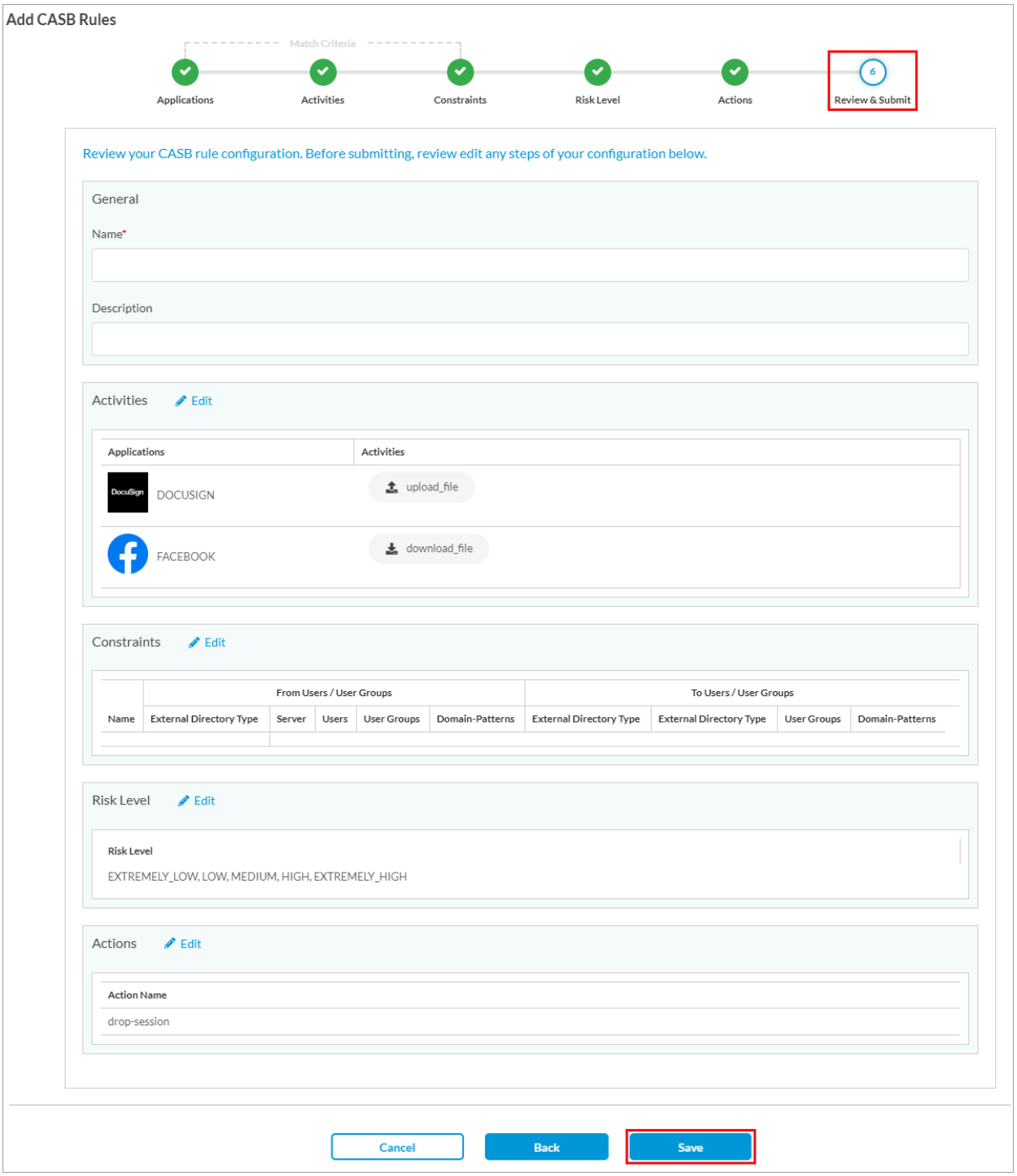
13. Select a constraint profile and click Save. You can select only one constraint profile for a CASB rule. For more information, see Configure Constraint Profiles, below.
14. In the Add CASB Rules screen, click Next to go to Step 4, Risk Level.



15. Select the risk level, which can be Extremely Low, Low, Medium, High, and Extremely High. A color is associated with each risk level.
16. To clear the selections, click Clear All.
17. Click Next to go to Step 5, Actions.

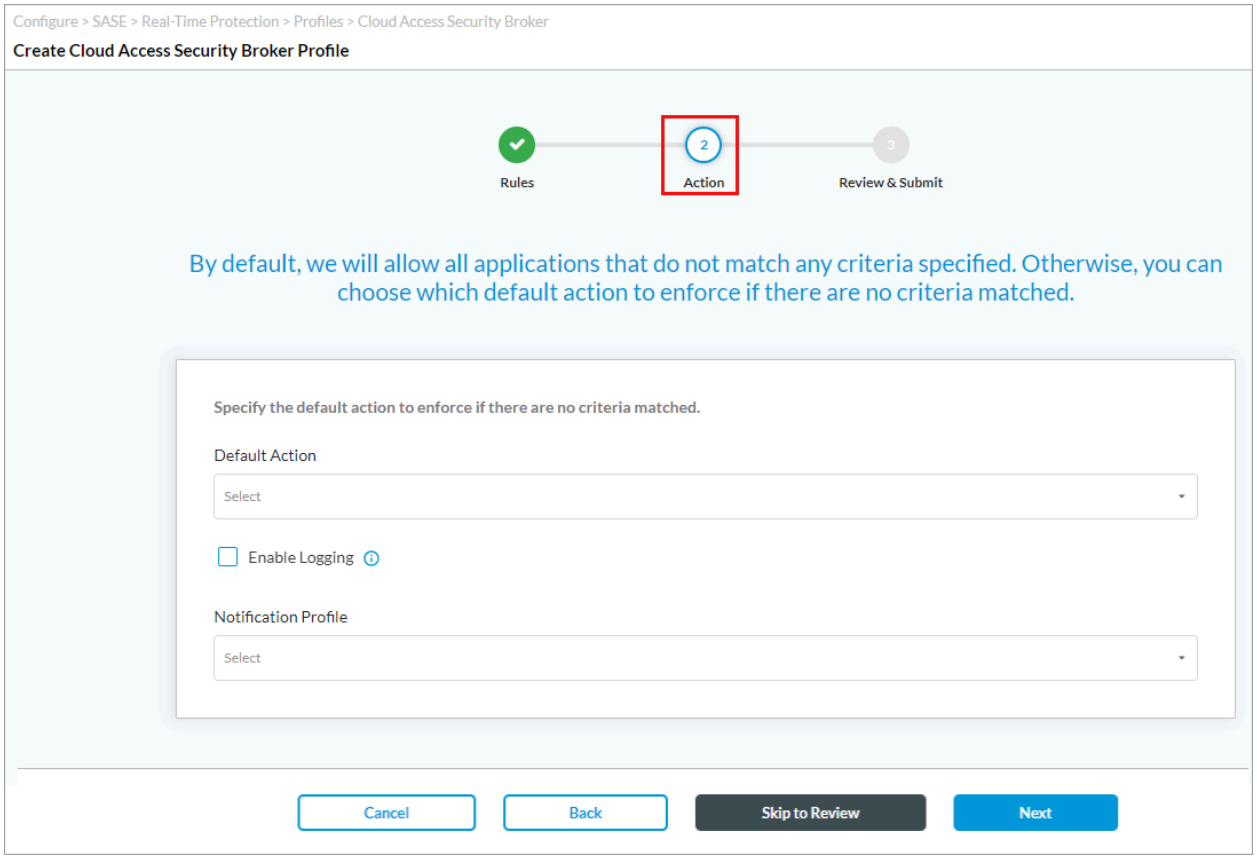


18. In the field on the right, select a predefined or custom action to perform when there are no matching criteria. For more information, see Configure Custom Security Actions. The predefined actions are:
    - Allow—Allow cloud applications.
    - Block—Block cloud applications.
    - Drop Session—Drop cloud application sessions.
19. In the Notification Profile field, select a profile to send email notifications. For more information, see Configure a Notification Profile.
20. Click Next to go to Step 6, Review and Submit.



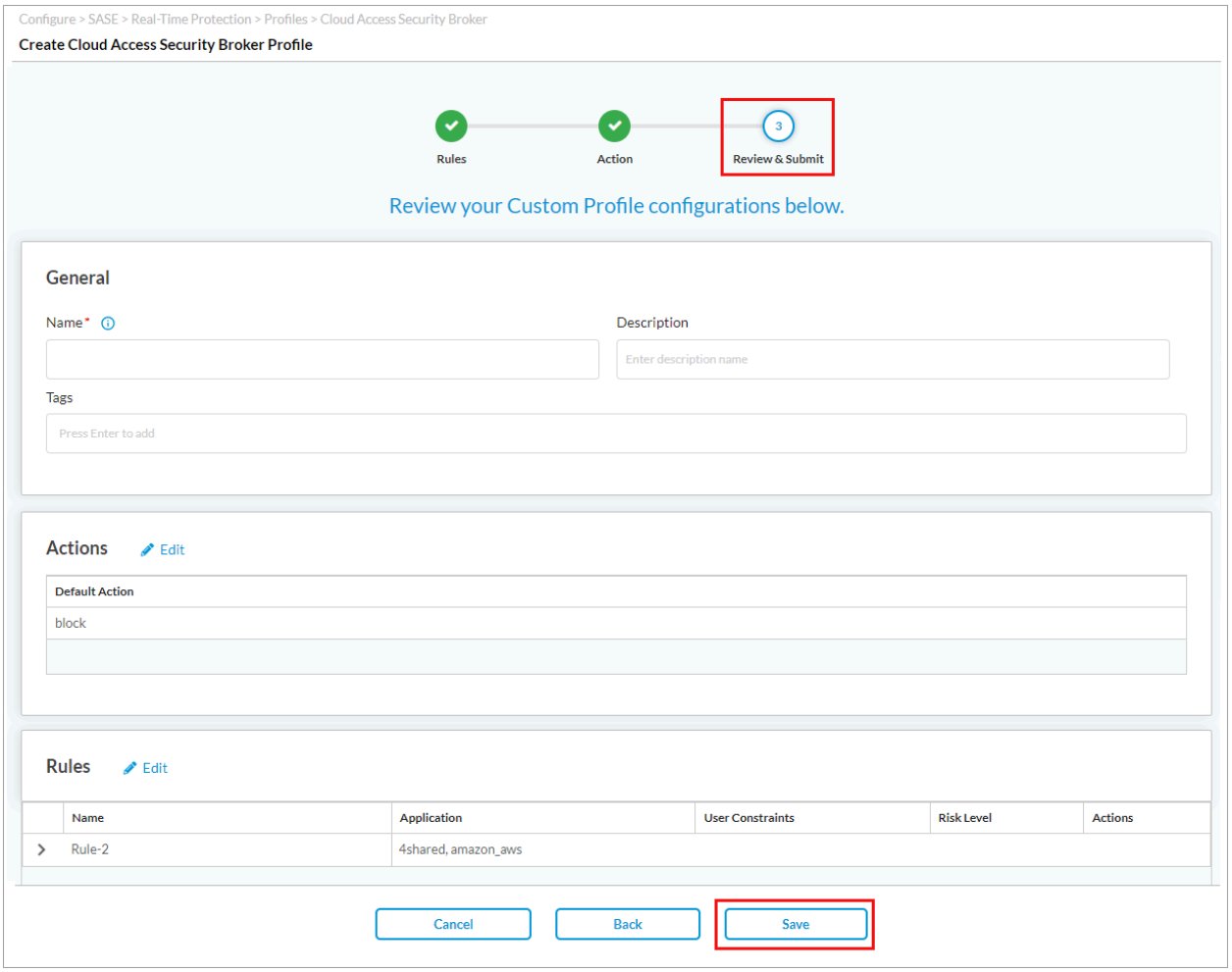
21. In the General section, enter a name for the CASB profile and, optionally, a description and tags.
22. For all other sections, review the information. To make changes, click the Edit icon.
23. Click Save.
24. In the Create Cloud Access Security Broker Profile screen, click Next to go to Step 2, Action, to select the default action to perform when there are no matching criteria. By default, applications that do not match any criteria are

allowed. Enter information for the following fields.



Field	Description
Default Action	Select the default action to perform when there are no matching criteria: ◦ Allow—Allow cloud applications. ◦ Block—Block cloud applications. ◦ Drop Session—Drop cloud application sessions. ◦ Reject—Reject cloud applications.
Enable Logging	Click to enable CASB logging.
Notification Profile	Select a profile to send email notifications. For more information, see Configure a Notification Profile.

25. Click Next to go to Step 3, Review and Submit.



26. In the General section, enter a name for the CASB profile and, optionally, a description and tags.
27. For all other sections, review the information. To make changes, click the Edit icon.
28. Click Save.

Configure Constraint Profiles

For Releases 12.1.1 and later.

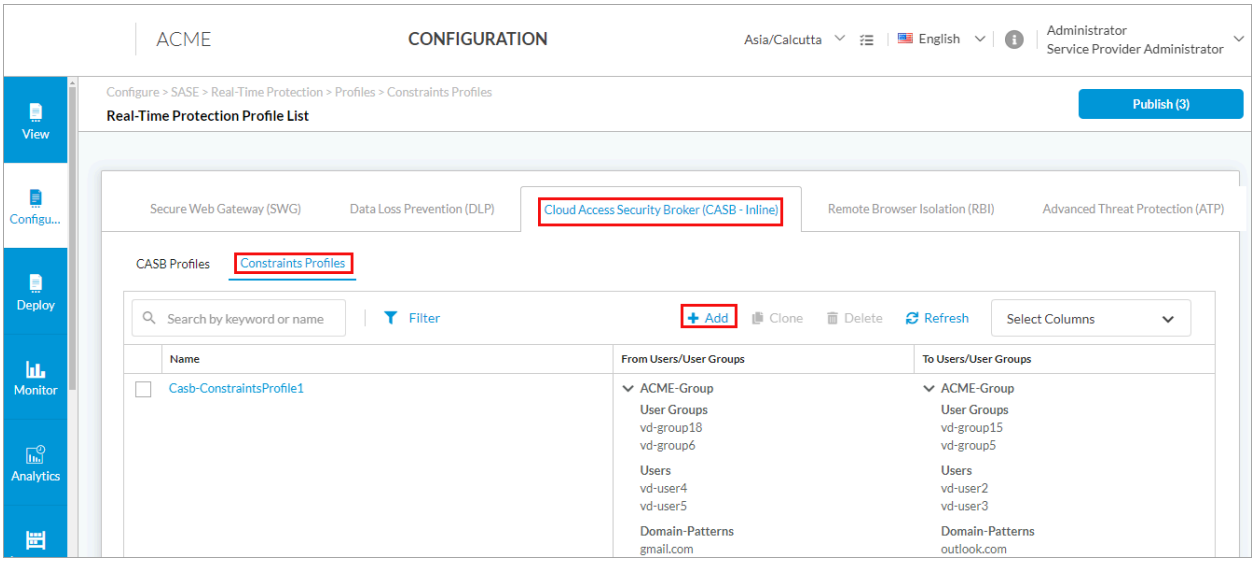
You configure CASB constraint profiles to control which users and groups can access the activities configured in CASB. You can apply the CASB constraint profiles when you configure a CASB profile rule. The following table shows activities and applications that you can configure as a CASB constraint.

Activity	Description	Applications
Call From User	Users who can initiate a call in the application	MS Teams–audio

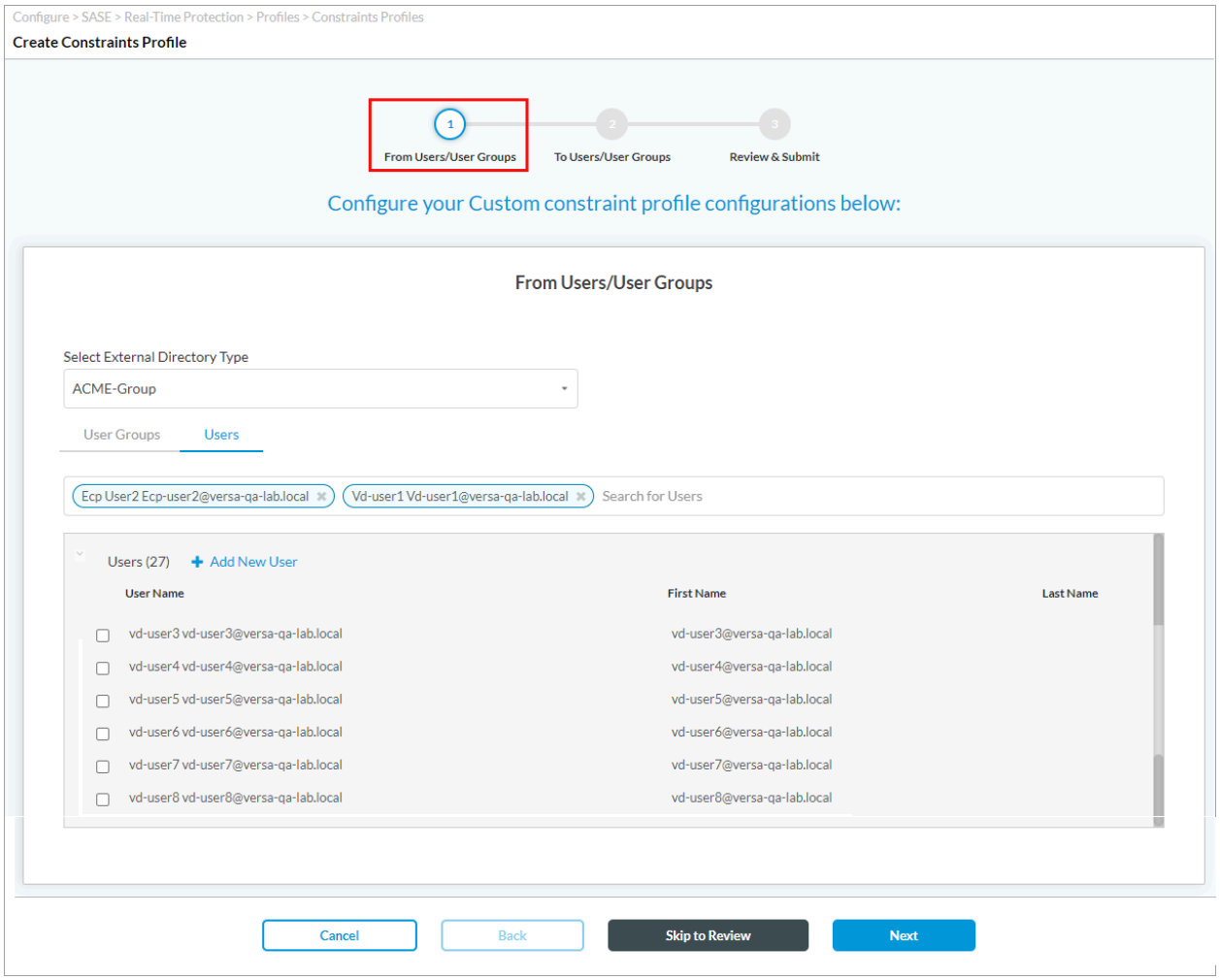
Activity	Description	Applications
Call To User	Users who can receive a call in the application	MS Teams–audio
Send From User	Users who can send content in the application	Outlook
Share From User	Users who can share content in the application	Sharepoint Online
Share To User	Users who can received shared content in the application.	Box, Dropbox, One Drive, Sharepoint Online

To add constraint profiles:

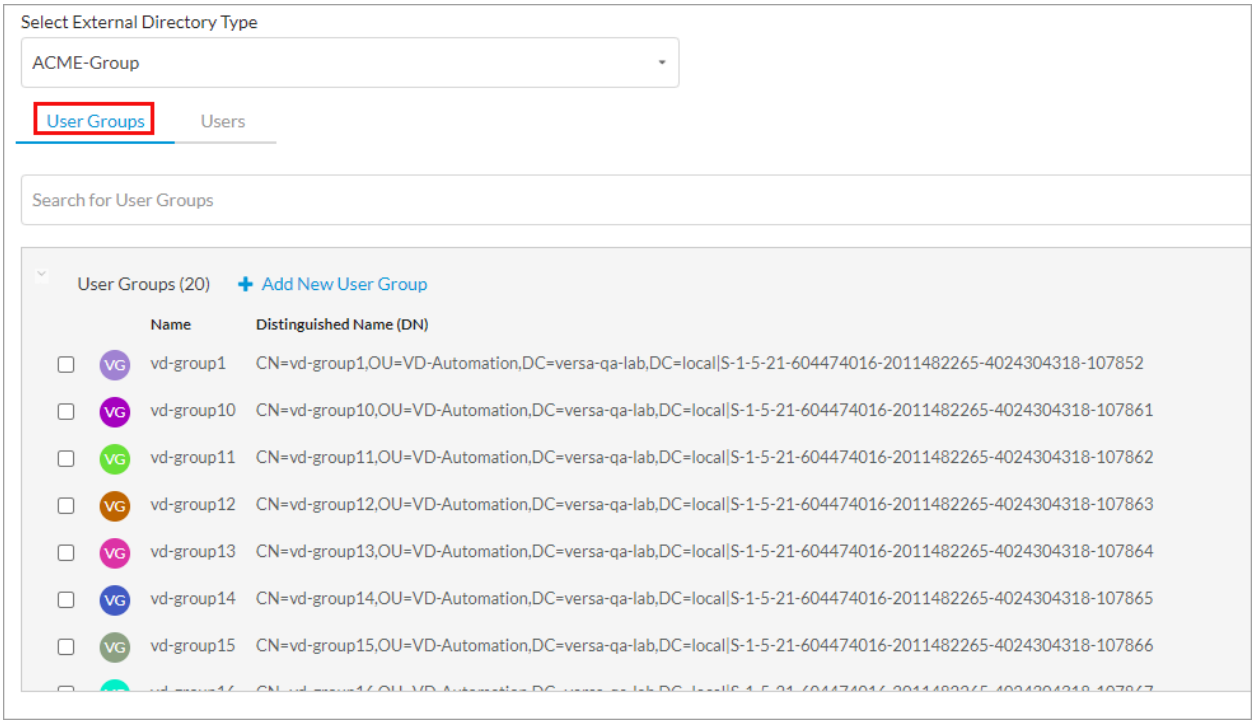
1. In the Cloud Access Security Broker (CASB Inline) tab, select Constraints Profiles.



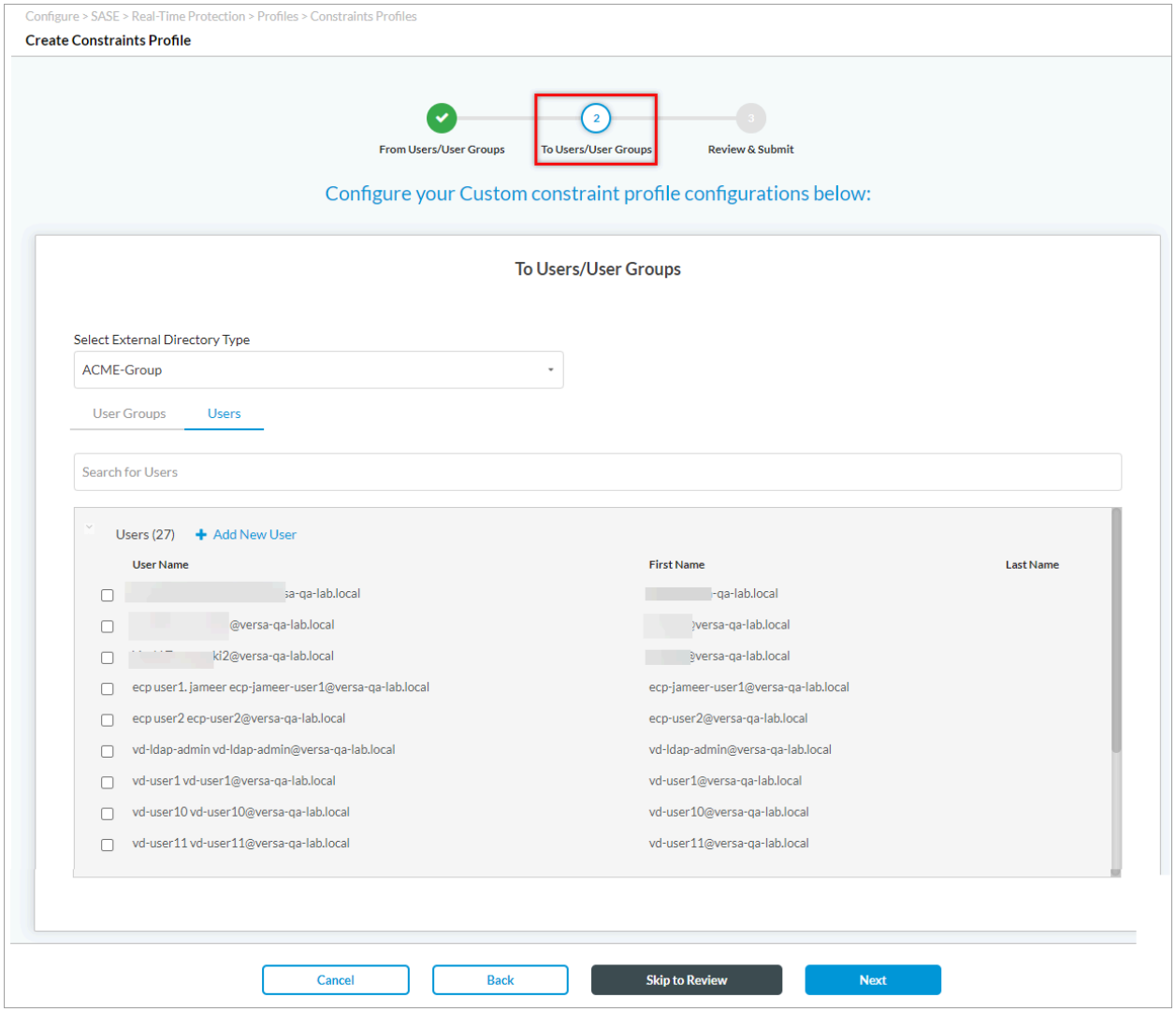
2. Click + Add. The Create Constraints Profile screen displays. In Step 1, From Users/User Groups, configure a custom constraint profile.



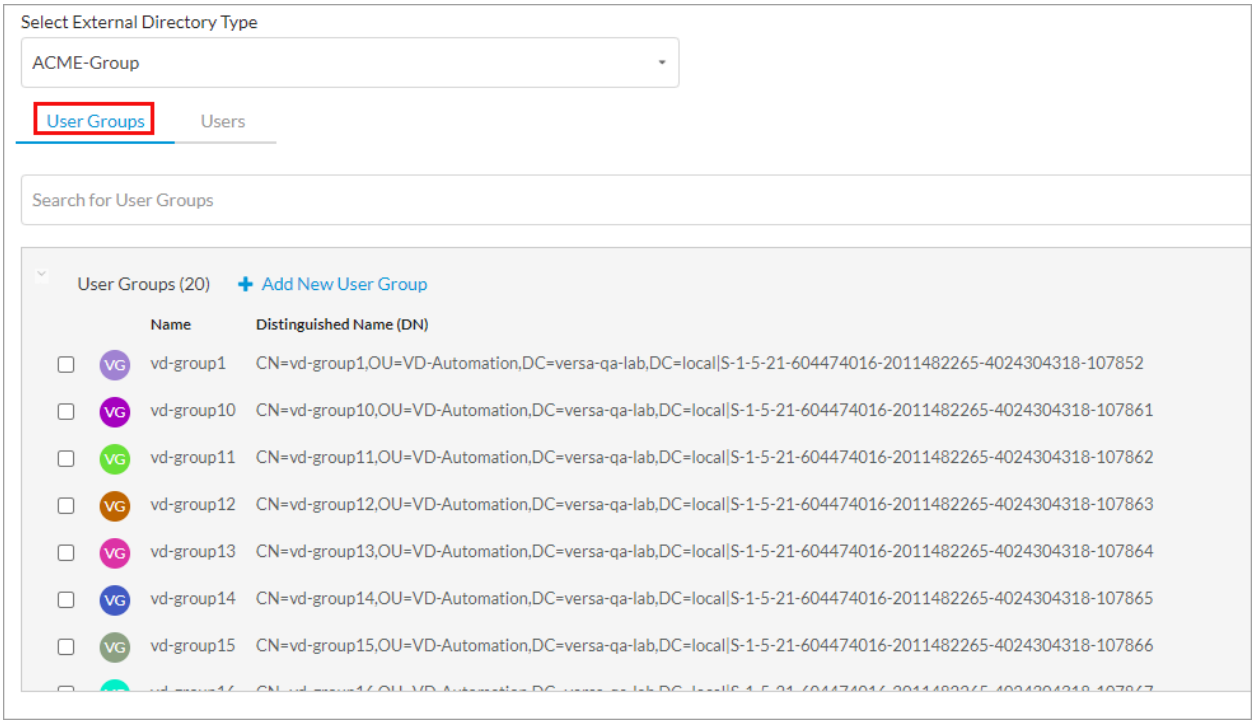
3. Select the external directory type, and then add users in the Users Tab.
4. Select the User Groups tab, and then select user groups.



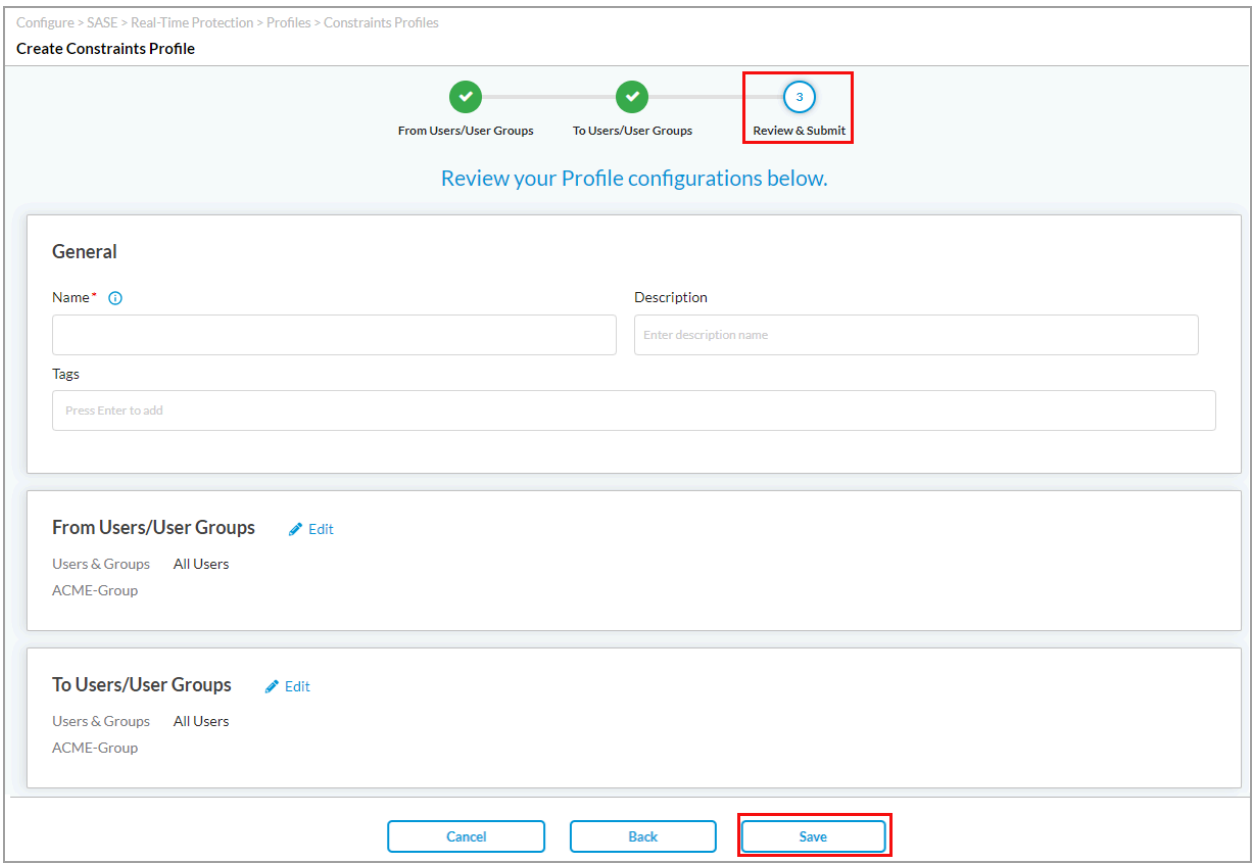
5. Click Next to go to Step 2, To Users/User Groups screen.



6. Select the external directory type, and then add users in the Users Tab.
7. Select the User Groups tab, and then select user groups.



8. Click Next to go to Step 3, Review and Submit.



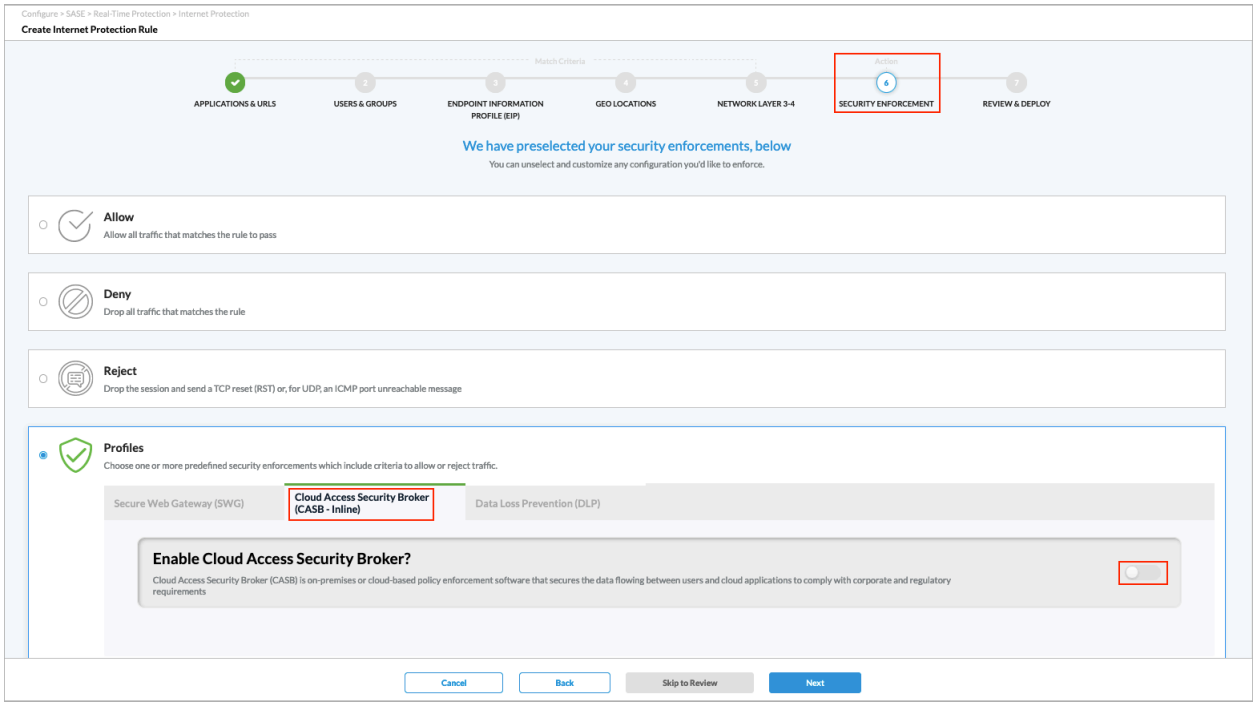
9. In the General section, enter a name for the constraints profile and, optionally, a description and tags.
10. For all other sections, review the information. To make changes, click the Edit icon.
11. Click Save.

Associate a CASB Profile with a SASE Internet Protection Rule

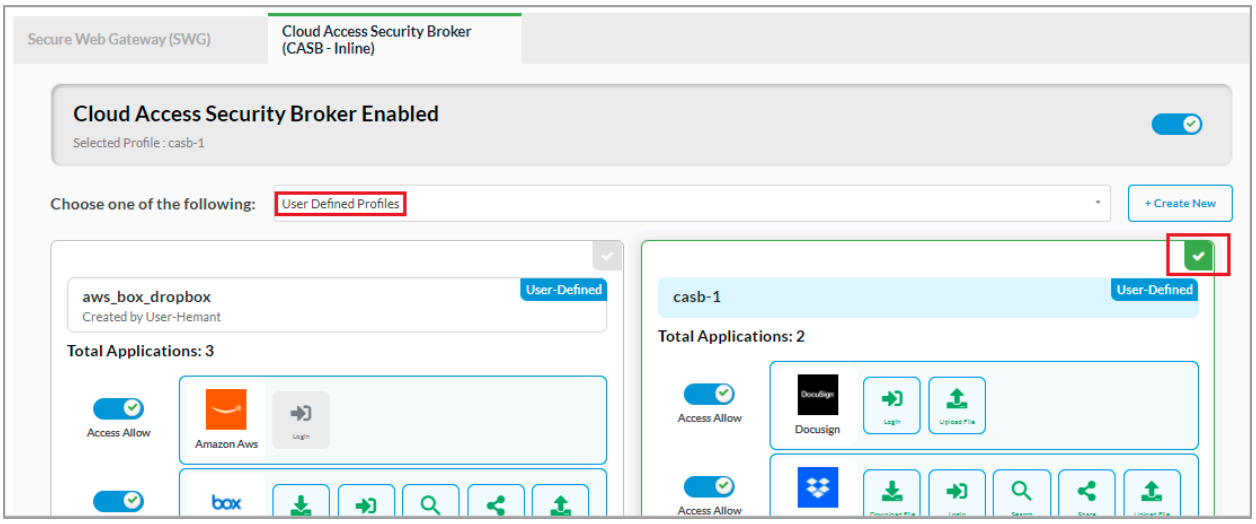
To allow or deny traffic, you associate a CASB profile with a SASE internet protection rule. CASB secures the data flowing between users and cloud applications in order to comply with corporate and regulatory requirements.

To associate a CASB profile with a SASE internet protection rule:

1. Go to Configure > Real-Time Protection > Internet Protection.
2. In the Internet Protection Rules List screen, click + Add to create a rule. The Create Internet Protection Rule screen displays. For more information, see Configure SASE Internet Protection Rules.
3. Select the Security Enforcement screen, and then select Profiles.
4. Select the Cloud Access Security Broker (CASB Inline) tab, and then enable CASB.



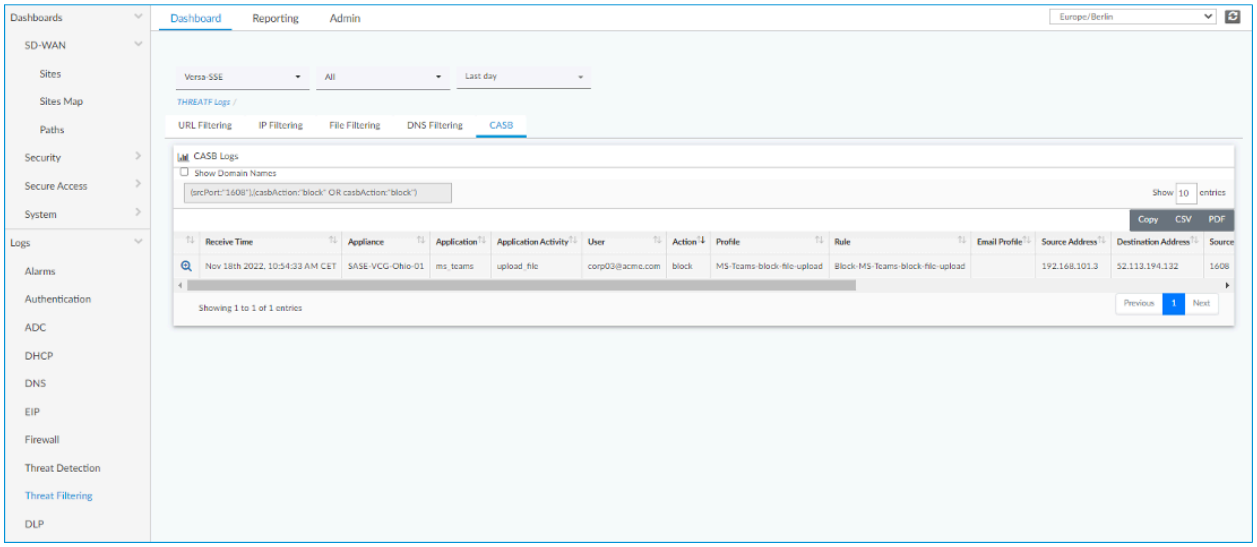
5. Select User-Defined Profiles, and then select the CASB profile to associate with the internet protection rule.



6. Review and then deploy the internet protection rule.

Verification

To view the logs for CASB policy enforcement actions in the SASE portal, click Analytics in the left menu, and go to Logs > Threat Filtering. On the Dashboard tab, click CASB.



Configure Advanced Internet Protection with DLP

Data loss prevention (DLP) is a set of tools and processes for detecting and preventing data breaches, cyber exfiltration, and unwanted destruction of sensitive data. You use DLP to protect and secure an organization's data and to comply with regulations.

To configure DLP, you do the following:

1. Define a data protection profile—You associate data patterns with a data protection profile, and you then use the data protection profile when you create DLP rules.
2. Define DLP rules—You create the rules that are used in a DLP profile to match data.
3. Configure a DLP profile—Create an ordered set of DLP rules that you can then apply to a security policy or to an internet protection rule.

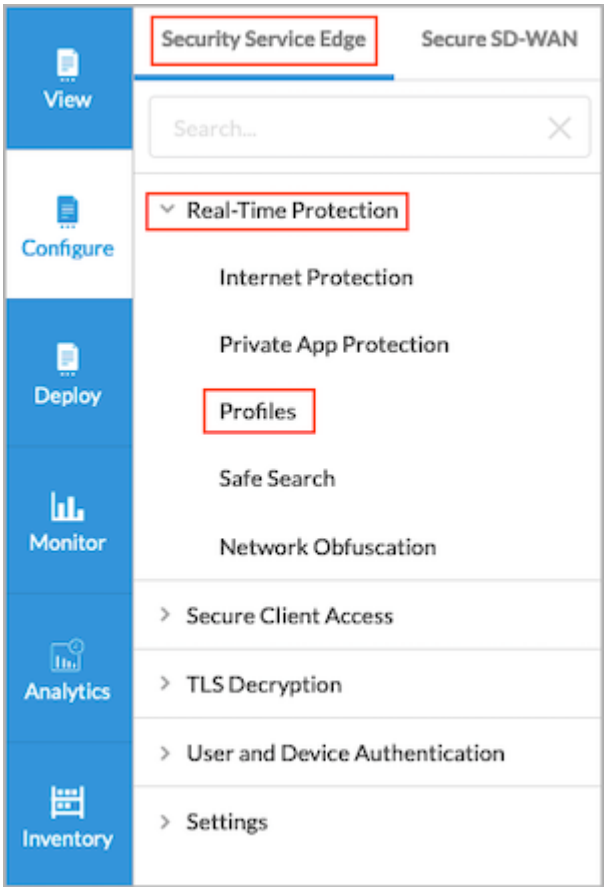
Configure Data Protection Profiles

A data protection profile consists of an ordered set of rules in which each rule has one or more match conditions and an action. You can configure a data protection profile to stop evaluating rules after the first rule that matches (Exit on First Rule Match option) or to evaluate all rules and apply all those that match (default behavior).

After you create a data protection profile, you can use it as part of the enforcement actions on a policy rule in a security access control policy.

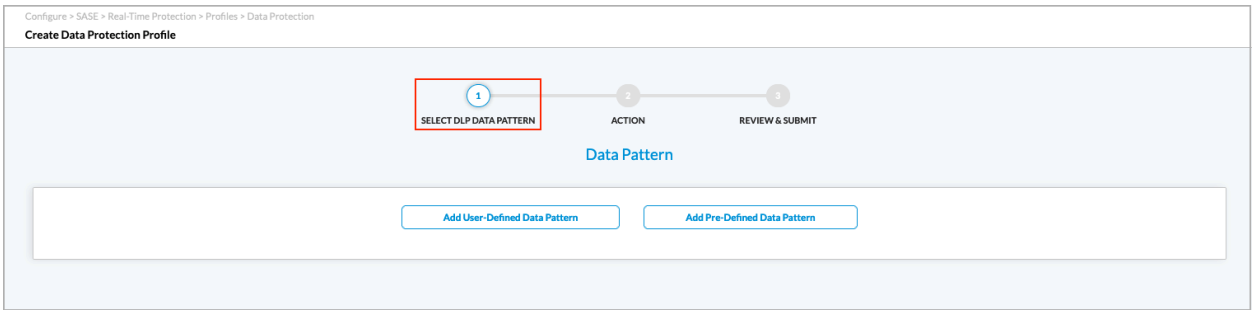
To configure a data protection profile:

1. Go to Configure > Secure Services Edge > Real-Time Protection > Profiles.

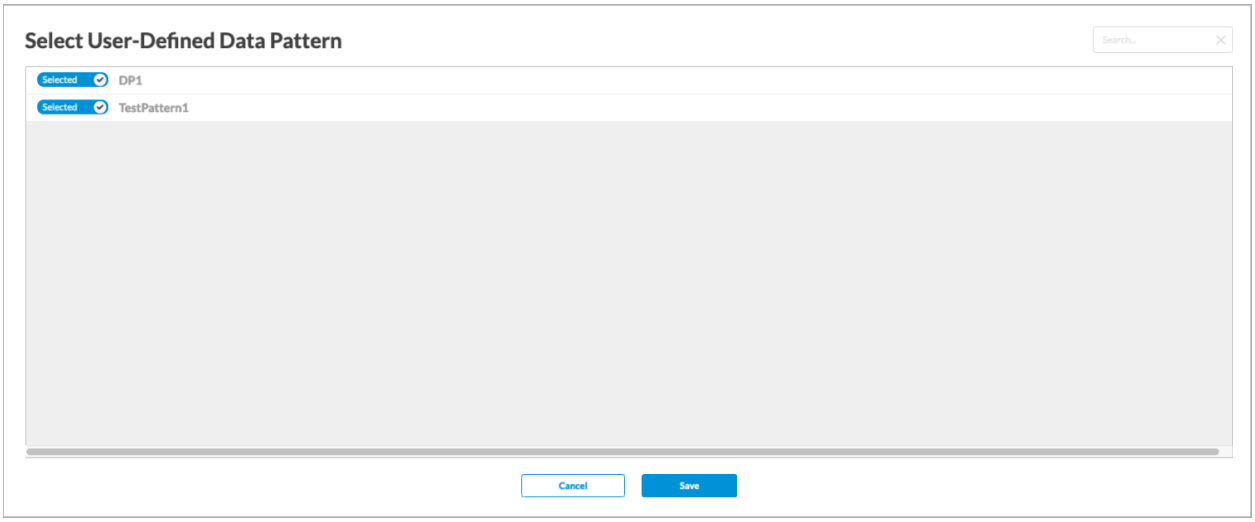


The following screen displays.

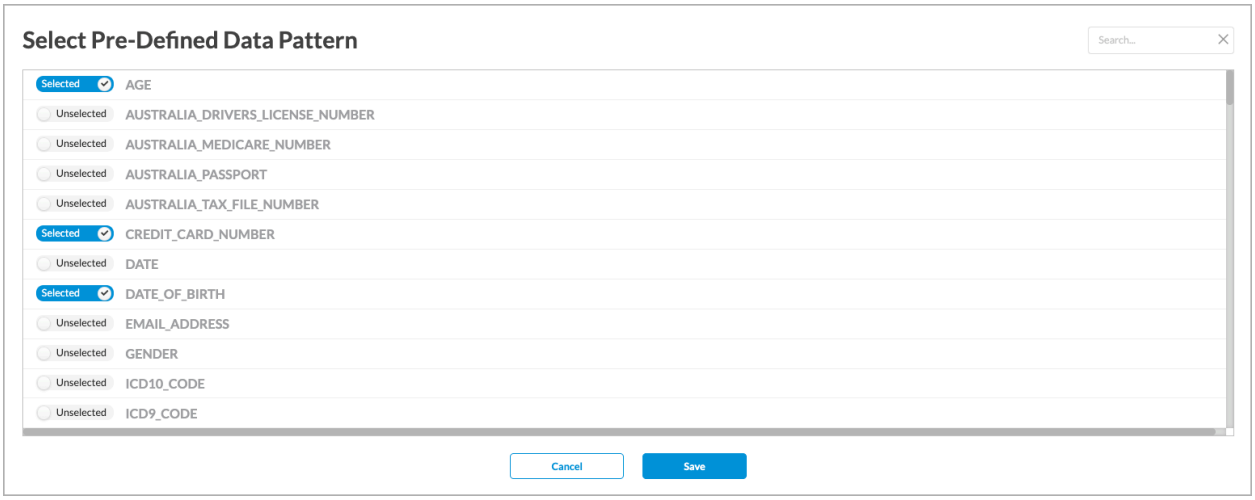
2. Select the Data Loss Prevention (DLP) tab, and then select the Data Protection Profiles tab.
3. Click + Add. In Step 1, Select DLP Data Pattern, you can select either user-defined (custom) or predefined data patterns.



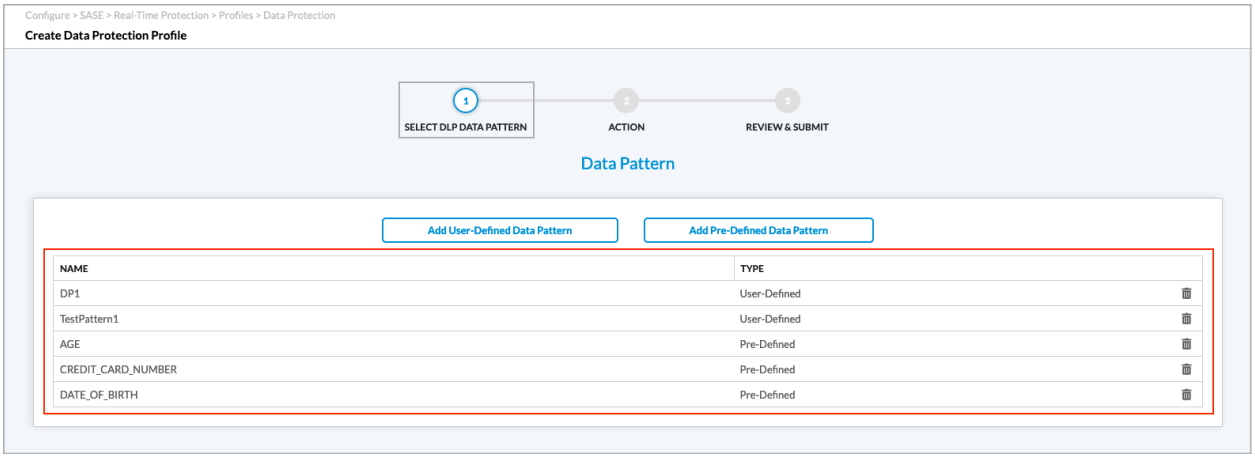
   a. To select user-defined data patterns, click Add User-Defined Data Pattern, and then select one or more custom data patterns to use in the data protection profile.



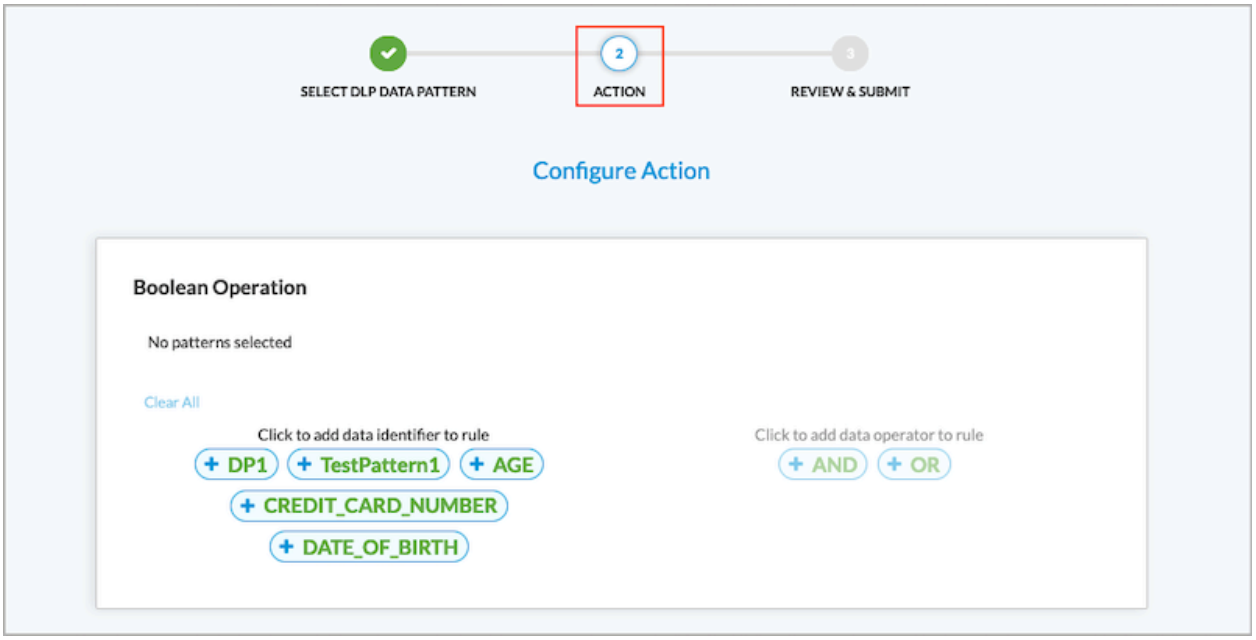
   b. Click Save to add the user-defined data patterns to the data protection profile.
   c. To select predefined data patterns, click Add Predefined Data Pattern, and then select one or more predefined data patterns to use in the data protection profile.



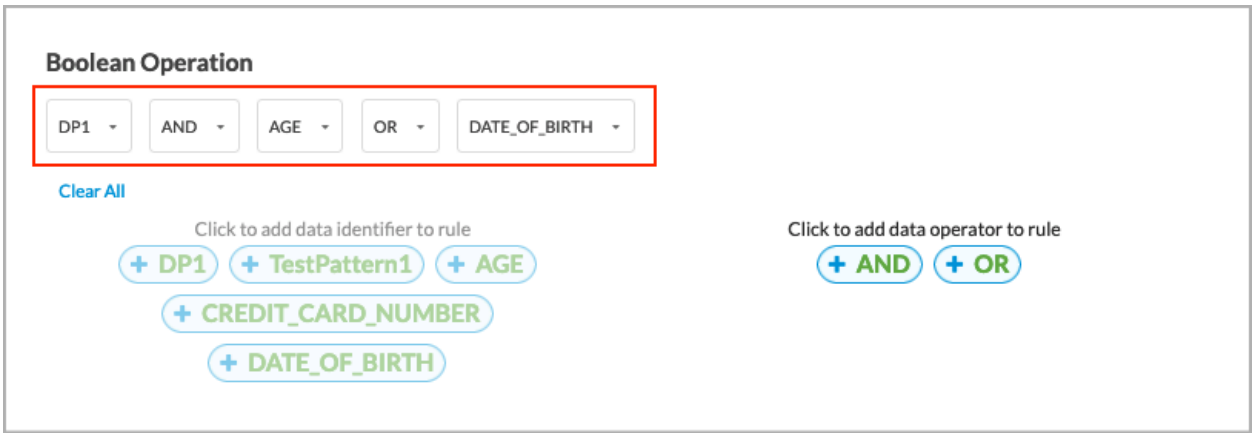
d. Click Save. The Data Pattern screen displays the selected data patterns.



4. Click Next.



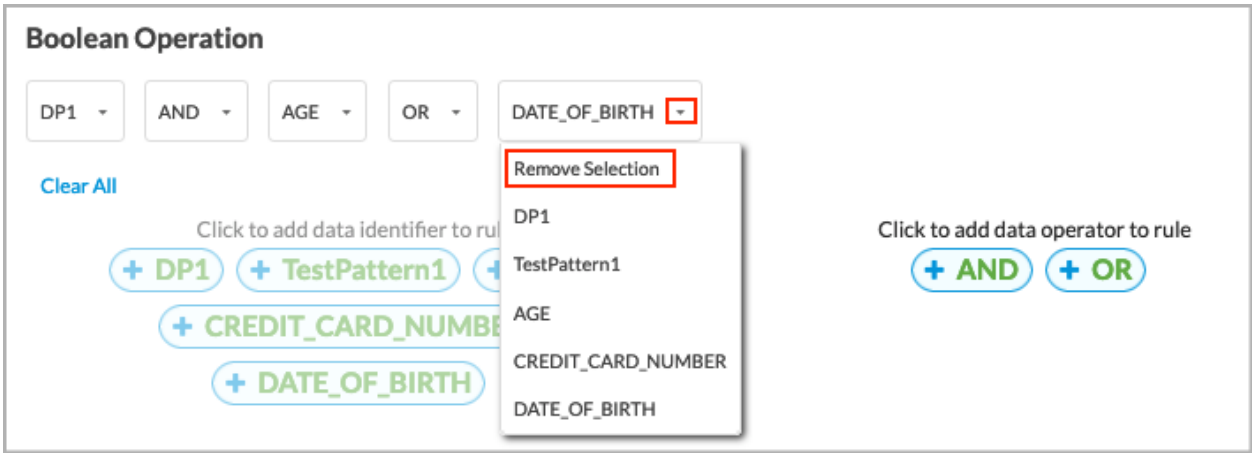
5. In Step 2, Action, you create a Boolean operation that defines how to match the selected data patterns. To do this, click a data pattern, click a Boolean operator, and then click a second data pattern to complete the Boolean operation. If a Boolean operation includes multiple data patterns, separate them a Boolean operator. The following example shows a Boolean operation created from the data patterns shown in the previous screenshot:



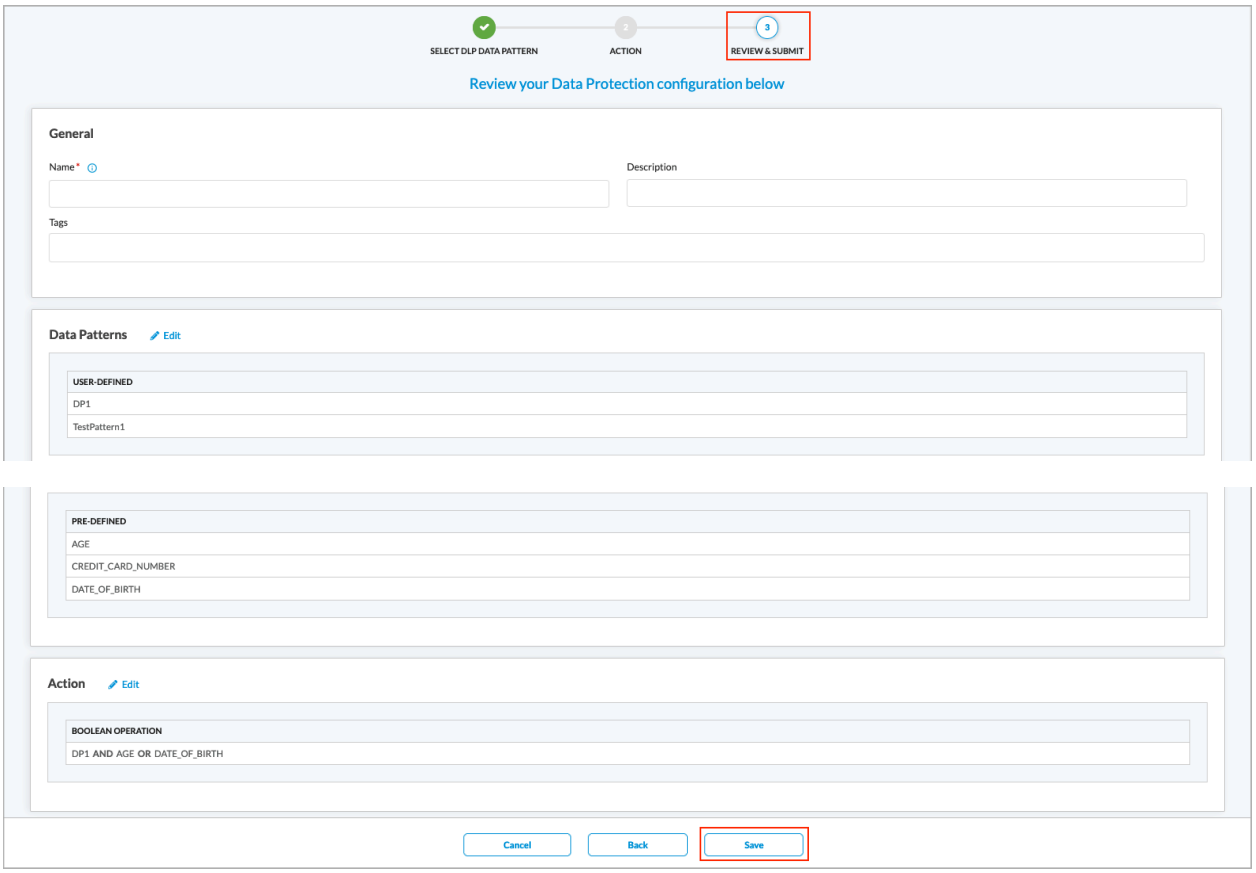
To replace one data pattern in the Boolean operation with another, click the down arrow next to the data pattern name, and then select a different one.

To change the Boolean operator, click the down arrow next to the operator name and then selecting a different one.

To remove the last element of a Boolean operation, click the down arrow, and then click Remove Selection.



6. Click Next.
7. In Step 3, Review and Submit, enter a name for the data protection profile and, optionally, a text description and one or more tags. A tag is an alphanumeric descriptor, with no white spaces or special characters, that you can use to search the objects.



8. Review the data protection profile entries.
9. To change any of the information, click the Edit icon in its section, and then make the required changes.
10. Click Save to create the data protection profile.

Configure DLP Rules

A DLP profile rule consists of the following components:

- Rule type—You can select one or more of the following rule types:
  - Context analysis—Scan data in the HTTP Context, such as HTTP Attachment, HTTP Body, and HTTP Header.
  - Document fingerprinting—Convert a standard form into a sensitive information type, which can then be used to define DLP policy rule. The DLP software examines files that have been fingerprinted and the directory path to these files to determine how similar a candidate file is to a previously fingerprinted file. The DLP software then computes a similarity threshold between the two files and compares the similarity threshold to the configured threshold. The configured threshold is the percentage of content that needs to be similar to the previously fingerprinted file stored in the folder path.
  - Exact data match (EDM)—Validate the match result of a custom or predefined data pattern against a user-provided data set. An exact data match rule can reduce false positives and can help to guarantee precise DLP for entries in the data set.
  - File DLP—Provide protection based on the configured file attributes.

    - Machine Learning—Uses models trained with predefined and custom data for image classification, source code detection, and document fingerprinting.
    - Optical character recognition (OCR)—Converts images to text and applies DLP policies on the converted text data.
- Protocol monitoring—DLP monitoring can scan the HTTP protocol.
- File-type filtering—You can configure data filters based on the file types.

The following table shows the applications supported by DLP and the whether upload and download are supported for each of the listed actions.

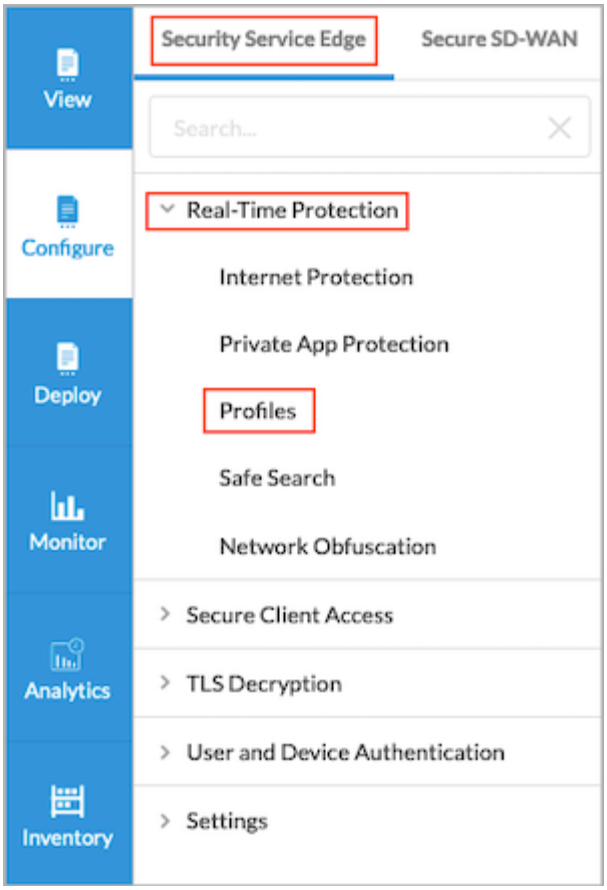
Application	Alert	Allow	Alert & Set Label	Allow & S
Box.com				
• Download	Supported	Supported	Supported	Supporte
• Upload	Supported	Supported	Supported	Supporte
Dropbox				
• Download	Supported	Supported	Supported	Supporte
• Upload	Supported	Supported	Not Supported	Not Supp
G-Drive				
• Download	Supported	Supported	Supported	Supporte
• Upload	Not Supported	Not Supported	Not Supported	Not Supp
Github				
• Download	Supported	Supported	Supported	Supporte
• Upload	Supported	Supported	Not Supported	Not Supp

Application	Alert	Allow	Alert & Set Label	Allow & S
Gmail				
• Download	Supported	Supported	Supported	Supporte
• Upload	Supported	Supported	Not Supported	Not Supp
Google Chat				
• Download	Supported	Supported	Supported	Supporte
• Upload	Supported	Supported	Not Supported	Not Supp
One Drive				
• Download	Supported	Supported	Supported	Supporte
• Upload	Supported	Supported	Supported	Supporte
Outlook				
• Download	Supported	Supported	Supported	Supporte
• Upload	Supported	Supported	Supported	Supporte
Salesforce				
• Download	Supported	Supported	Supported	Supporte
• Upload	Supported	Supported	Supported	Supporte
Slack				

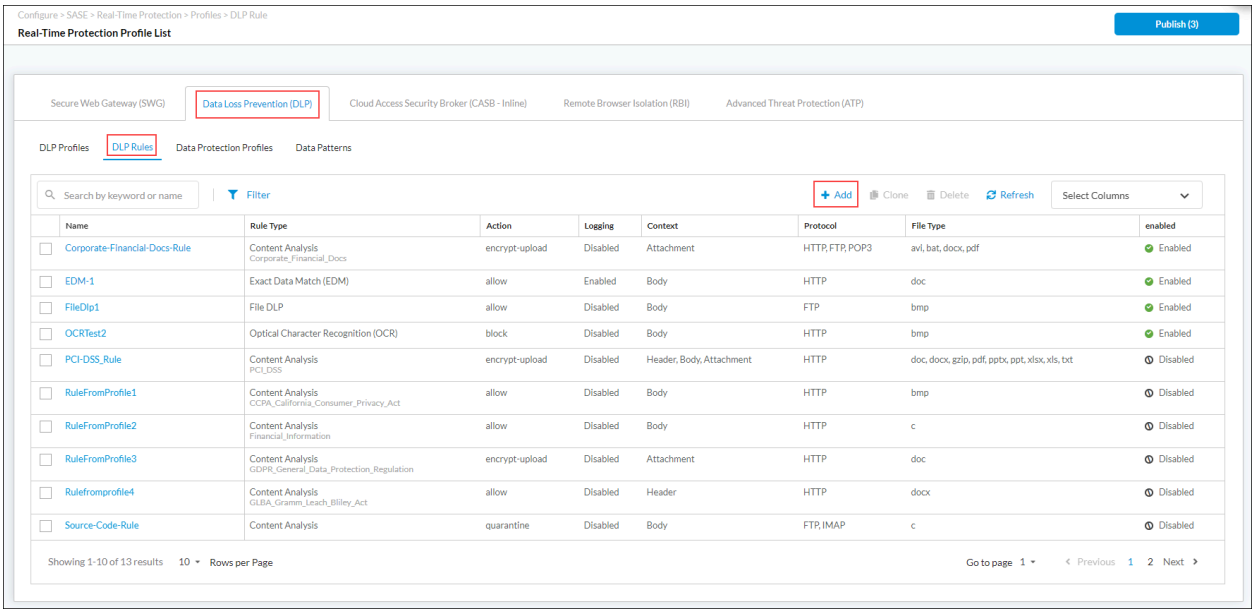
Application	Alert	Allow	Alert & Set Label	Allow & S
• Download	Supported	Supported	Supported	Supporte
• Upload	Supported	Supported	Not Supported	Not Supp
Teams				
• Download	Supported	Supported	Supported	Supporte
• Upload	Supported	Supported	Not Supported	Not Supp
Yahoo Mail				
• Download	Supported	Supported	Supported	Supporte
• Upload	Supported	Supported	Supported	Supporte

To configure rules to use in DLP profiles:

1. Go to Configure > Secure Services Edge > Real-Time Protection > Profiles.

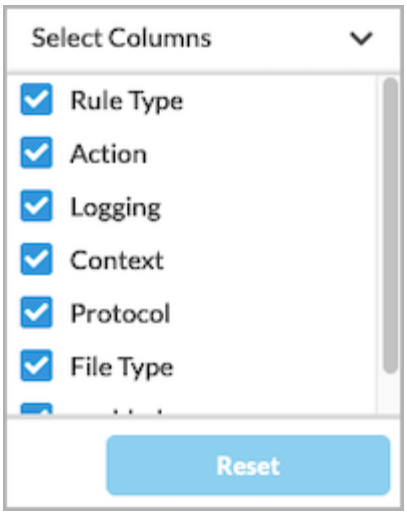


The following screen displays.

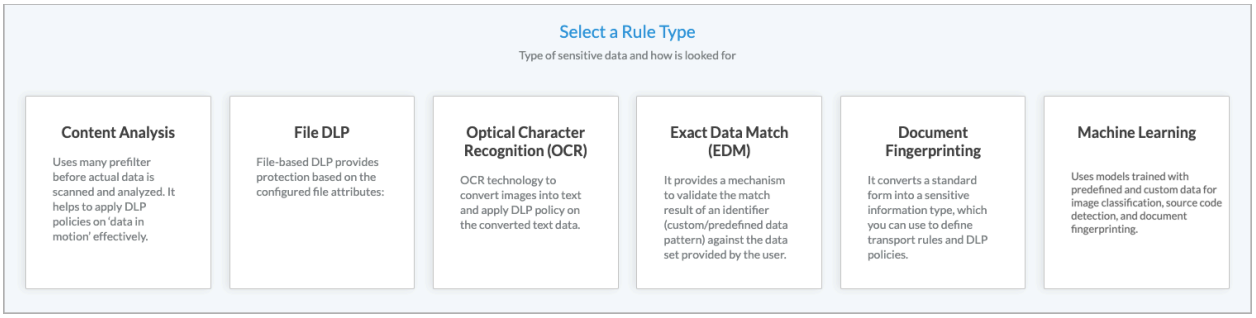


2. Select the Data Loss Prevention (DLP) tab, and then select the DLP Rules tab.

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



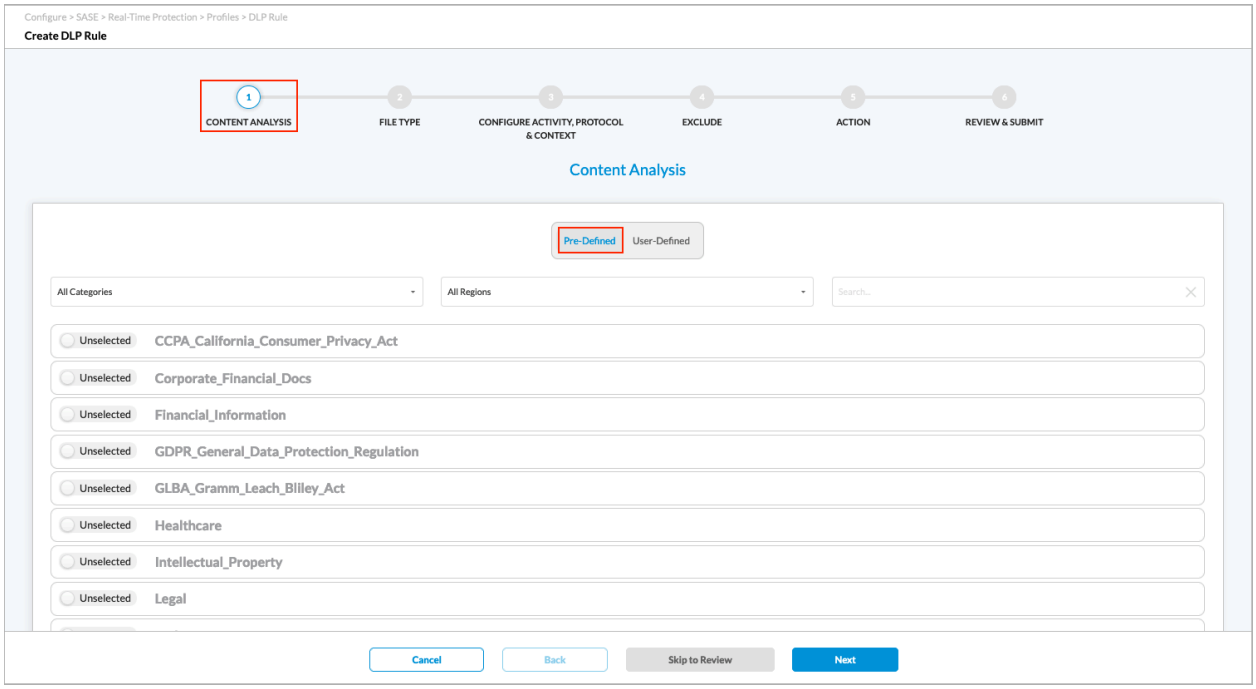
4. Click + Add to add a DLP rule. The Select a Rule Type screen displays. You can create Content Analysis, Exact Data Match (EDM), File DLP, Document Fingerprinting, Machine Learning, and Optical Character Recognition (OCR) rule types. The following sections describe how to configure the DLP file types.



5. **Configure a Content Analysis Rule**—To create a content analysis rule, click the Content Analysis box in the Select a Rule Type screen. The following screen displays, which lists all predefined data protection profiles by default. The pre-defined profiles are:

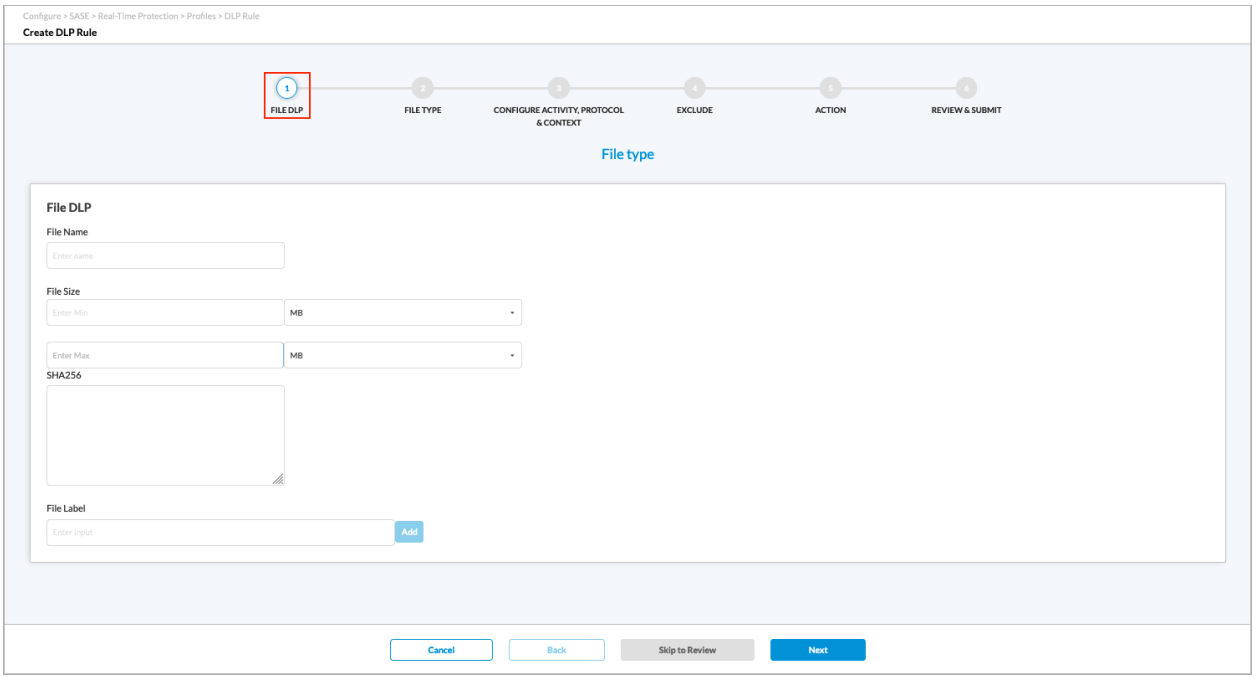
   - AUSTRALIA_FINANCIAL_DATA
   - CCPA_California_Consumer_Privacy_Act
   - Financial_Information
   - GDPR_General_Data_Protection_Regulation
   - GLBA_Gramm_Leach_Bliley_Act
   - PCI_DSS
   - SOCIAL_SECURITY_NUMBER_CONFIDENTIALITY_ACT2000
   - SOURCE_CODE_ACT
   - UK_ACCESS_TO_MEDICAL_REPORTS_Act1988
   - UK_FINANCIAL_DATA

- UK_PII
- US_DRIVERS_LICENSE_NUMBER_ALL_STATES
- US_FEDERAL_TRADE_COMISSION_RULES
- US_FINANCIAL_DATA
- US_HIPAA
- US_PATRIOTS_ACT
- US_PHI
- US_PII
- WESTERN_AUSTRALIA_HEALTH_SERVICES_ACT



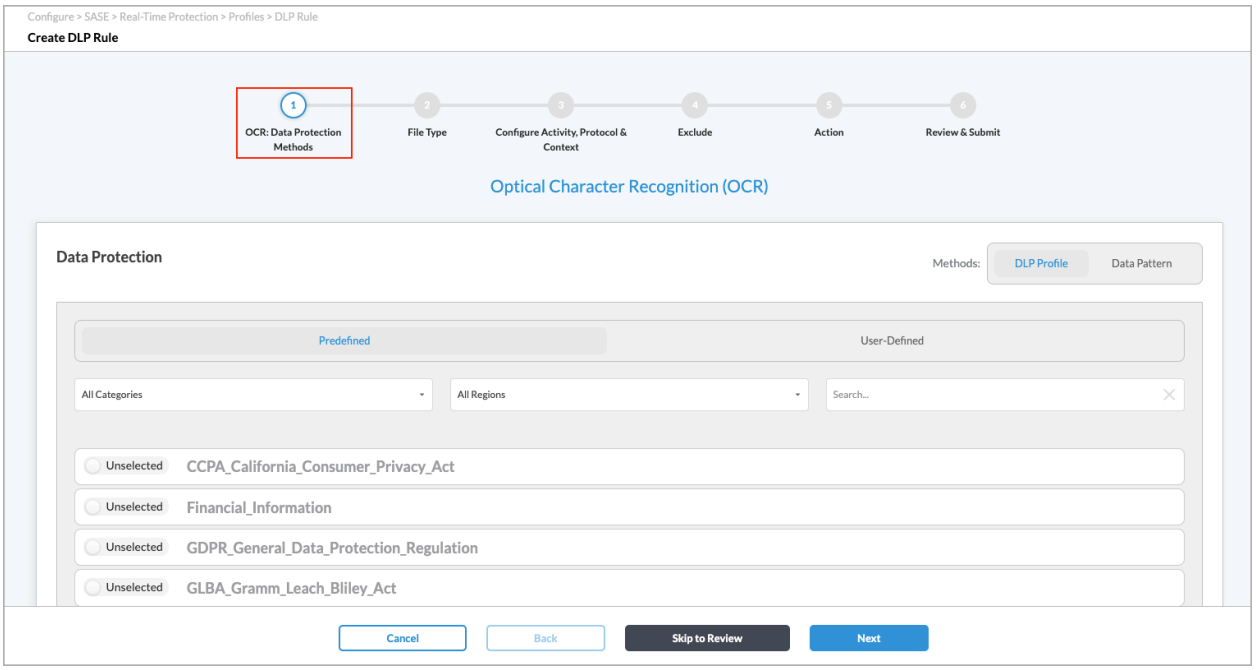
6. To view the custom data protection profiles, click User Defined.
7. To add the DLP rule for analysis, click one predefined or one user-defined data protection profile. You can select only one data protection profile, which can be either a predefined or a user-defined profile. To filter the data protection profiles by category, click All Categories. To filter the data protection profiles by region, click All Regions.

8. **Configure a File DLP Rule**—To create a file DLP rule, click File DLP in the Select a Rule Type screen. In the File DLP screen, enter information for the following fields.



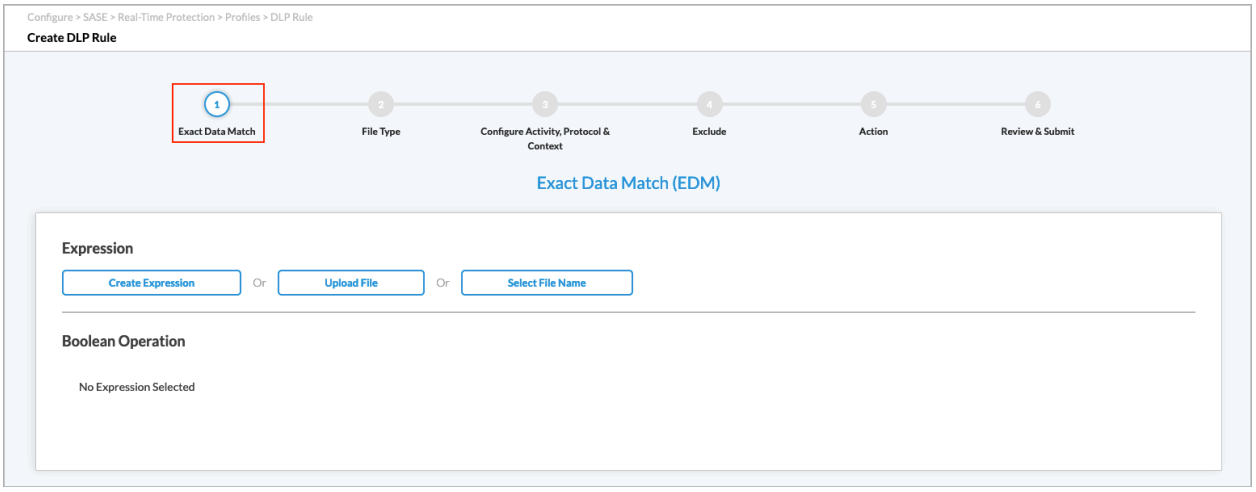
Field	Description
Filename	Enter a name for the file.
File Size (Group of Fields)	
◦ Enter Minimum	Enter the minimum size of the DLP file, and then select the size unit, either megabytes (MB), gigabytes (GB), kilobytes (KB), or bytes. The configured action is taken on all files that are smaller than the minimum size and that match the configured file type. If you set the minimum size to 0, the maximum DLP file size is used for the action.
◦ Enter Maximum	Enter the maximum size of the DLP file, and then select the size unit, either megabytes (MB), gigabytes (GB), kilobytes (KB), or bytes. The configured action is taken on all the files that are larger than the maximum size that match the configured file type.
SHA256	Enter the secure hash algorithm 256-bit (SHA256) value. To enter multiple SHA256 values, separate them by a new line.
File Label	Enter a file label, and then click Add.

9. **Configure an Optical Character Recognition Rule**—To create an optical character recognition (OCR) rule, click Optical Character Recognition in the Select a Rule Type screen. The following screen displays, which lists all predefined data protection profiles by default.

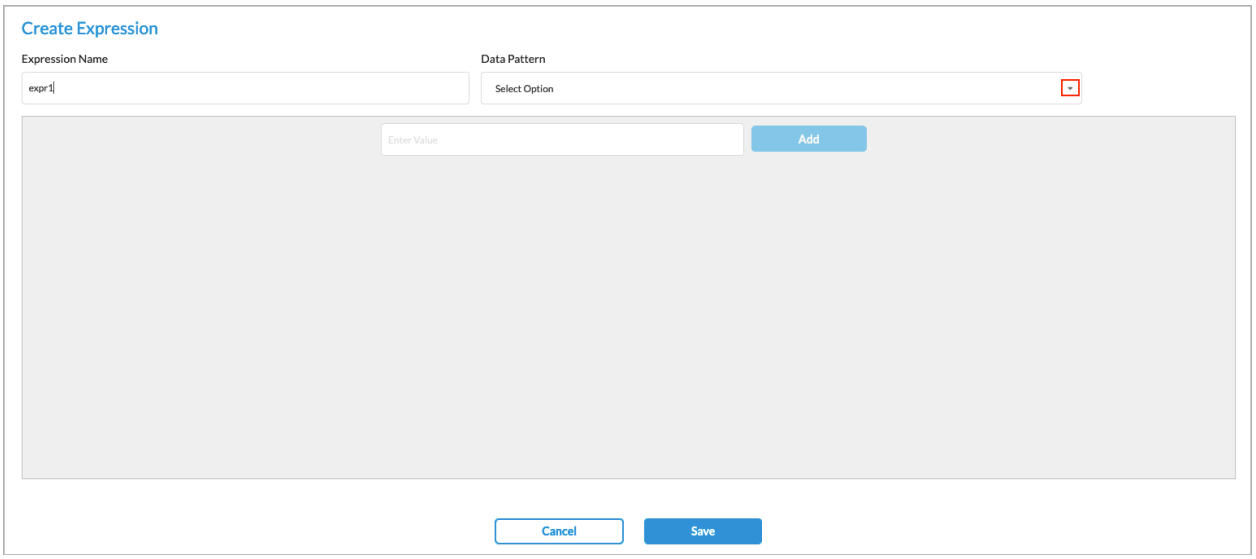


10. To view the custom data protection profiles, click User Defined.
11. To add the DLP rule for analysis, click one predefined or one user-defined data protection profile. You can select only one data protection profile, which can be either a predefined or a user-defined profile. To filter the data protection profiles by category, click All Categories. To filter the data protection profiles by region, click All Regions.

12. **Configure an Exact Data Match Rule**—To create an exact data match rule, click Exact Data Match (EDM) in the Select a Rule Type screen. The following screen displays.

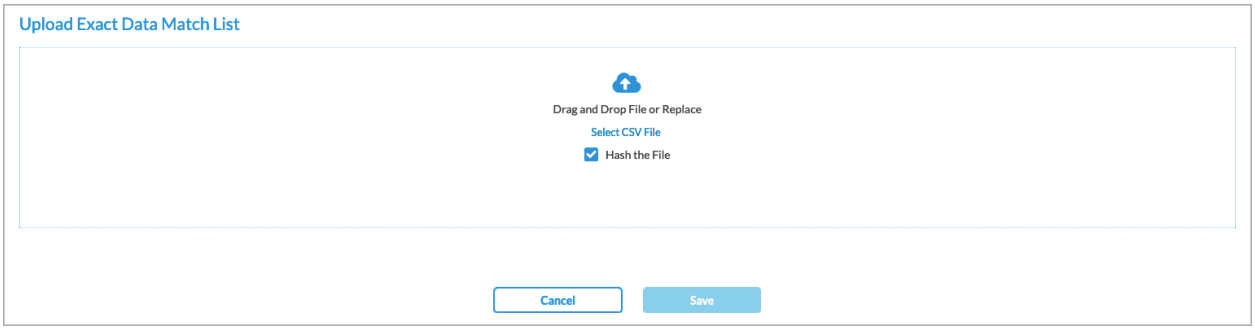


13. To create an expression, click Create Expression, and then enter information for the following fields.

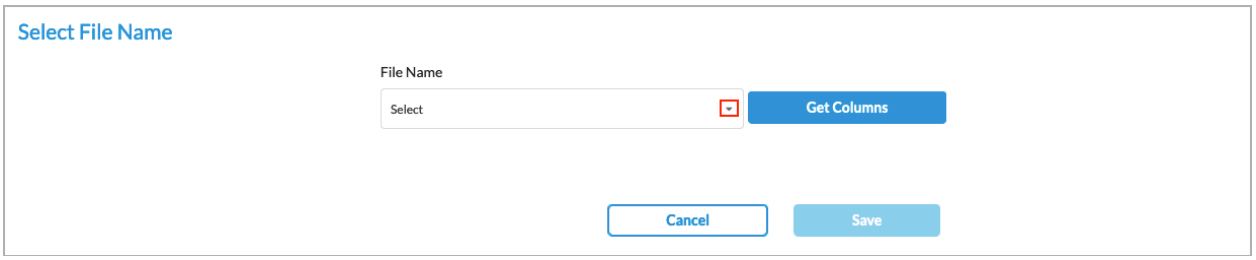


Field	Description
Name	Enter a name for the expression.
Data Pattern	Select a data pattern.
Enter Value	Enter a value for the expression, the click Add.

14. Click Save.
15. To upload a CSV file that contains a list of exact data matches, click Upload File.
    a. Drag and drop the CSV file into the window, or click Select CSV File to upload the file.
    b. To hash the CSV file, click Hash the File.
    c. Click Save.

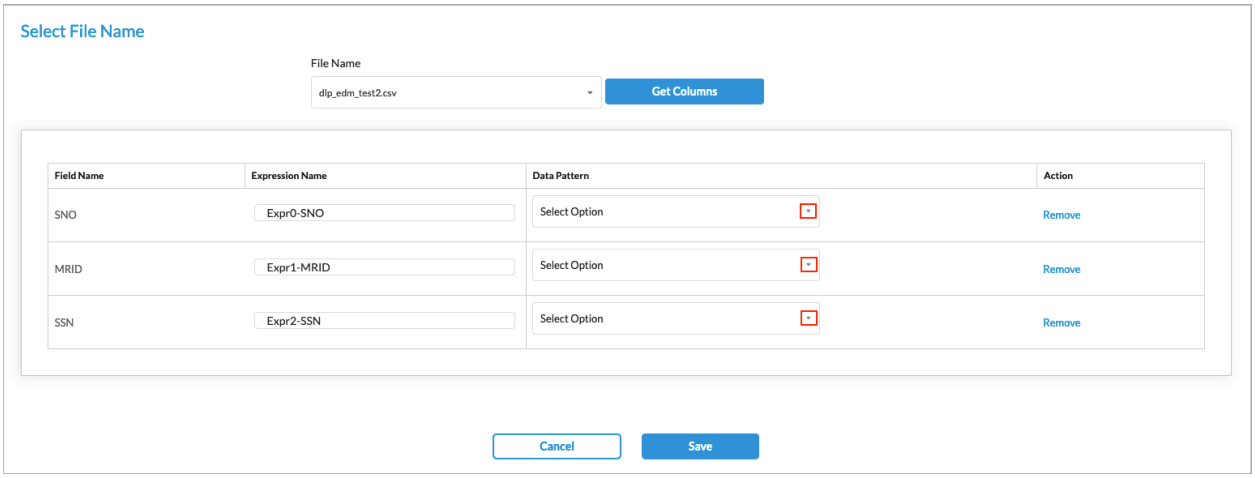


16. To select a filename, click Select File Name. The Select Filename screen displays.



i. In the Filename field, select a filename. Note that this list shows the names of CSV files that were previously uploaded. For information about uploading CSV files, see the Manage DLP Files and Folders, below.

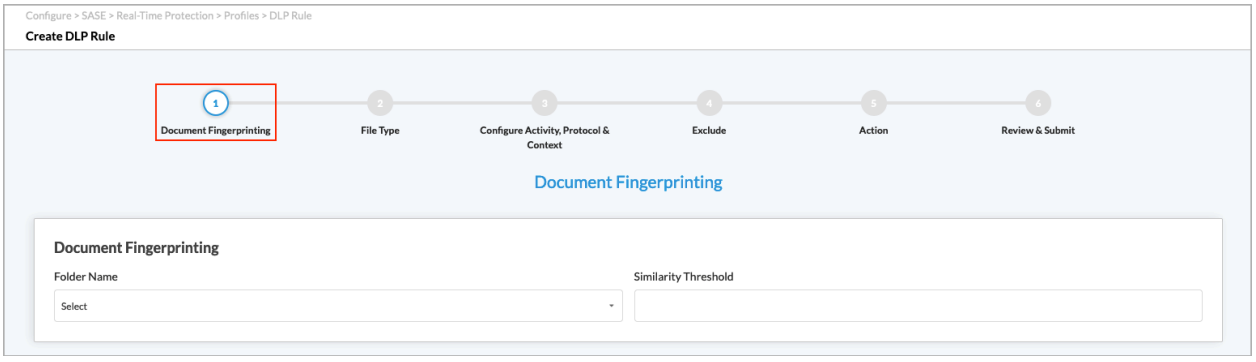
ii. Click Get Columns. The screen displays the columns for each field in the CSV file.



iii. In the Data Pattern column, select a data pattern to apply to each entry. Click Remove to remove an entry from the CSV file.

iv. Click Save.

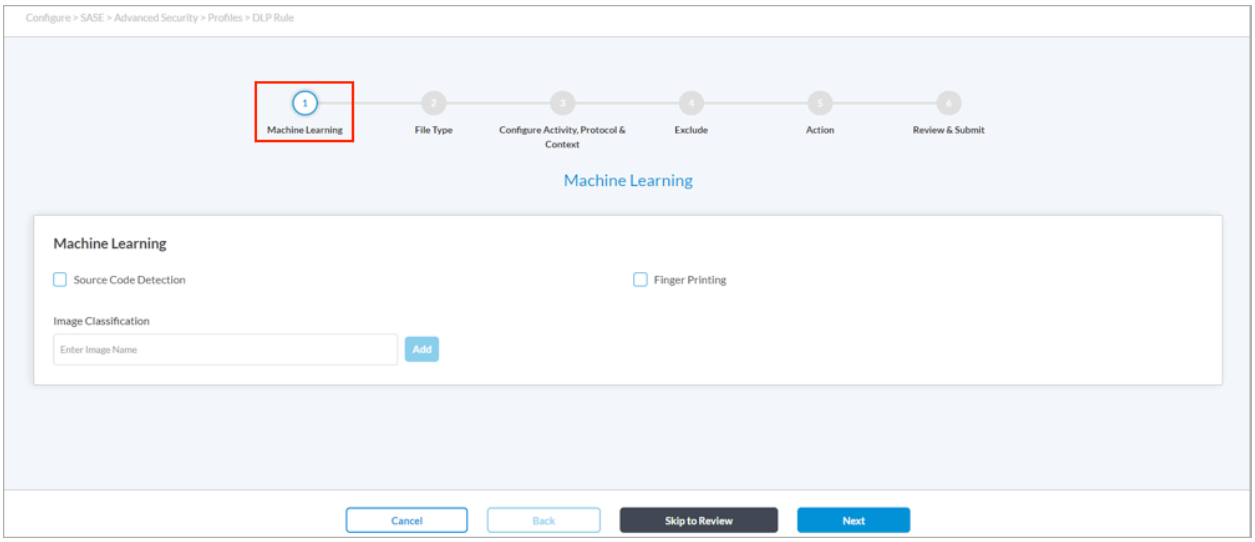
17. **Configure a Document Fingerprinting Rule**—To create a document fingerprinting rule, click the Document Fingerprinting in the Select a Rule Type screen, and then enter information for the following fields.



Field	Description
Folder Name	Select a folder.
Similarity Threshold	Enter the percentage of content that needs to be similar to the previously fingerprinted file stored in the folder path. *Range*: 1 through 100 *Default*: None

18. **Configure a Machine Learning Rule**—Versa's ML based classifiers augment automated identification of sensitive data. The following options are available:
    - Image Classification: Versa's cutting edge ML model classifies predefined images like Credit card, Debit card, social security number, driving license, passport etc.
      Besides the predefined images, Versa's ML model empowers user to train model with the proprietary images.
      The new trained model will detect proprietary and predefined images as well.
      The name or tag of the images can be configured in the 'Image classification' configuration.
    - Source code detection: It is very common to upload source code to generative AI model like chatGPT.
      Classical DLP needs a strong parser to detect different snippet of source code of each language.
      Versa's source detection model is trained with 15+ different type of source code like C, C++, perl, java, ruby, python etc.
      Any small snippet of source code is detected by Source code detection model.
    - Document fingerprint: Each organizations possess proprietary document types and templates, personalized forms etc.
      Versa's Document fingerprinting detection reads all the document empty template, form and store them in vector database.
      Any data filled in the given template or forms are detected by Document fingerprint classifier.

    To create a machine learning rule, click Machine Learning in the Select a Rule Type screen, and then enter information for the following fields.



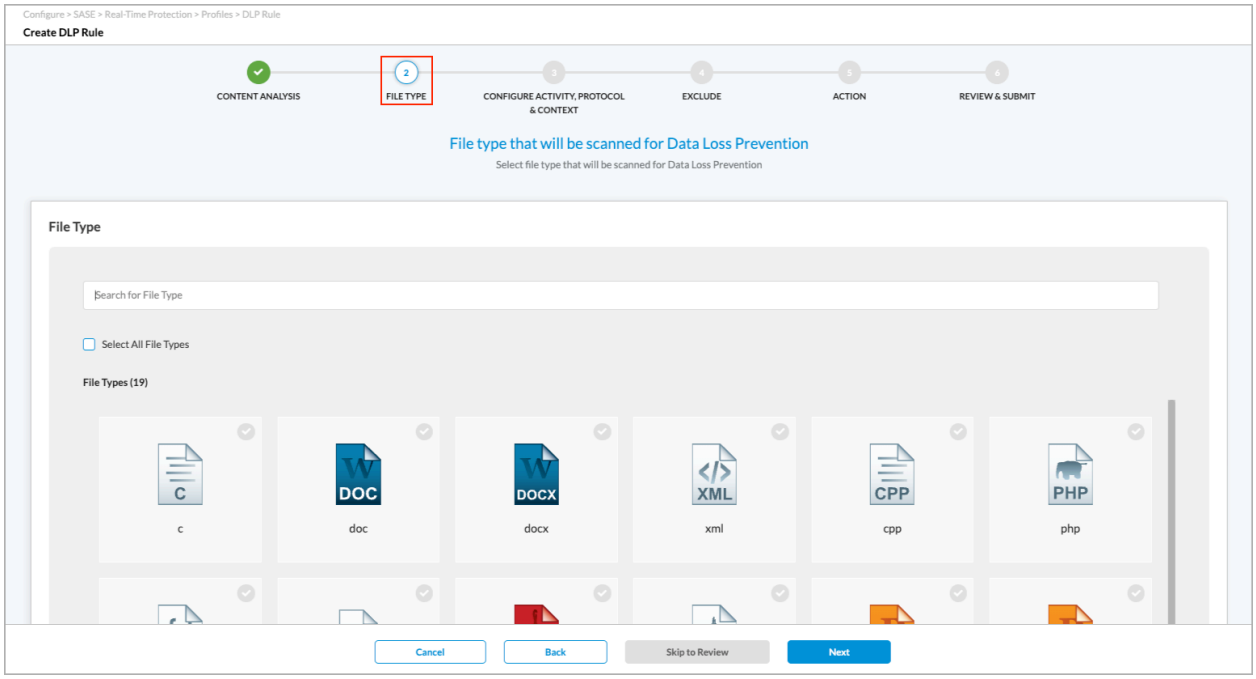
- Source Code Detection—Click to enable source-code detection.
- Finger Printing—Click to enable finger printing
- Image Classification—Enter the name of an image to classify.

19. Click Next to go to Step 2, File Type in the Create DLP Rule screen.
20. Select one or more file types to be analyzed. To search for specific file types, use the search box. To select all file types, click Select All File Types.

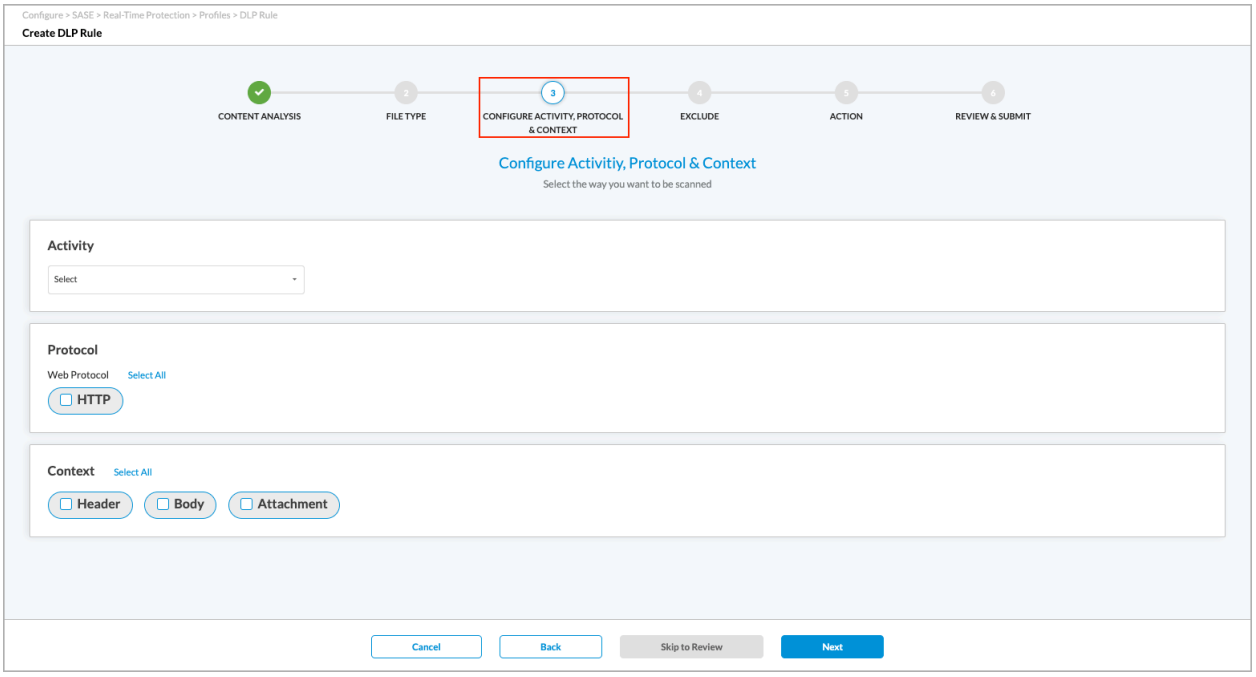
    Concerto supports the following file types:

    - c
    - class
    - cpp
    - doc
    - docx
    - html
    - msoffice
    - pdf
    - php
    - pl
    - ppt
    - pptx
    - rtf
    - sh
    - txt
    - xls
    - xlsx

- xml

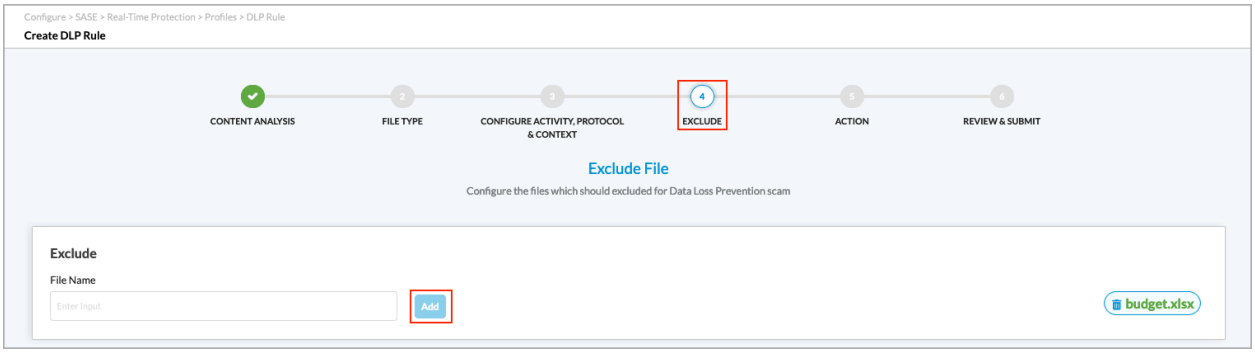


21. Click Next.
22. In Step 3 Configure Activity, Protocol, and Context, enter information for the following fields.



Field	Description
Activity	Select the direction of the traffic on which to apply the rule: ◦ Both—Apply the rule to both download and upload traffic. ◦ Download—Apply the rule when the client requests data from a server. ◦ Upload—Apply the rule when the client posts data to a server.
Protocol	Click the protocol to scan: ◦ Web Protocol ▪ HTTP
Context	Select one or more HTTP contexts of data to scan: ◦ Attachment—Data in an attachment ◦ Body—Data in the body ◦ Header—Data in the header of a packet

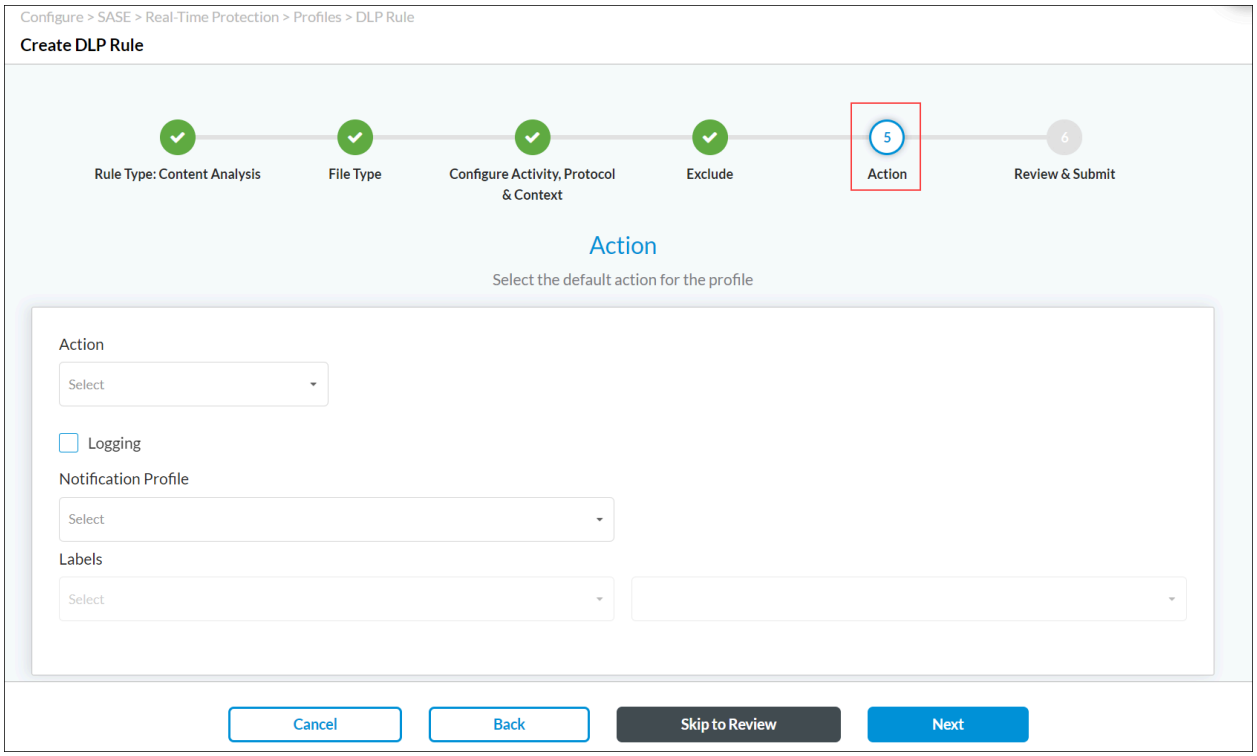
23. Click Next.
24. In Step 4, Exclude, in the Filename field, enter the names of a file to exclude, for example, budget.xlsx, and then click Add. The filename displays to the right of the Add button. You can exclude multiple files. To delete a filename from the list, click the Trash icon next to the filename.



25. Click Next.
26. In Step 5, Action, enter information for the following fields.

The following table shows the applications supported by DLP and whether file-name matching is supported for upload and download.

Applications	Download	Upload
Box	Supported	Supported
Dropbox	Supported	Not supported
Github	Supported	Supported
Gmail	Supported	Supported
Google Chat	Supported	Not supported
Google Docs	Supported	Not supported
Google Drive	Supported	Not supported
MS Teams (web)	Supported	Not supported
Office365	Supported	Not supported
OneDrive	Supported	Not supported
Salesforce	Supported	Supported
Service Now Developer Console	Supported	Supported
Sharepoint	Supported	Not supported
Slack	Supported	Supported
Yahoo Mail	Supported	Not supported



Updated: Wed, 23 Oct 2024 08:37:20 GMT

Field	Description
Action	Select an action to take if the traffic matches the rule: ◦ Alert—Allow traffic to pass and log it to Versa Analytics ◦ Allow—Allow traffic to pass without logging it to Versa Analytics ◦ Block—Drop the traffic without sending a notification to the client host that originated the traffic. ◦ Encrypt—Encrypt the traffic before sending it. ◦ Encrypt Upload—Encrypt the file and send it to the customer-provided cloud portal. To decrypt the file and view its contents, use a symmetric key. The session is rejected. ◦ Quarantine—Send the traffic to the customer-provided cloud portal without encrypting it. ◦ Redaction—If a rule match is detected in an editable, text-based file, change the content of the matched packet to random characters. Redaction is supported for exact data matches (EDMs) for file types .c, .html, .php, .sh, .txt, and .xml. ◦ Reject—Drop the traffic and send a notification to the client host indicating that the traffic was dropped.
Logging	Click to enable LEF logging to Analytics, which logs all actions to Versa Analytics, except fo actions that explicitly do not log. If you do not enable logging, no logging information is sent to Versa Analytics.
Notification Profile	Select a notification profile. To configure a notification profile, see Configure SASE User-Defined Objects.
Set Label	Click Set Label or Remove Label to set or remove a sensitivity label on a file before uploading or downloading it.
Enter Label	Enter the text of the label to be set or removed.

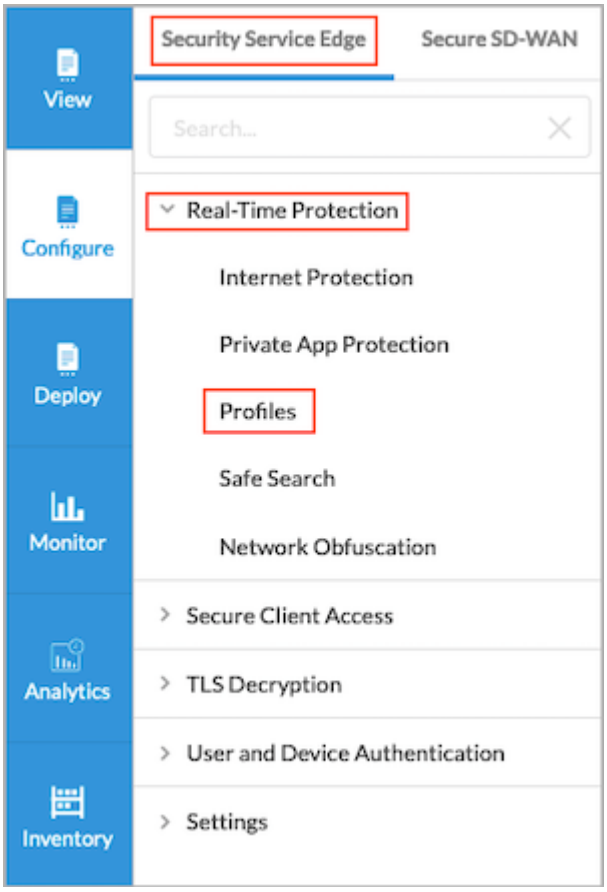
27. Click Next.
28. In Step 5, Review and Submit, review the configuration entries
29. To change any of the information, click the Edit icon and then make the required changes.
30. Click Save to create the DLP rule.

Configure DLP Profiles

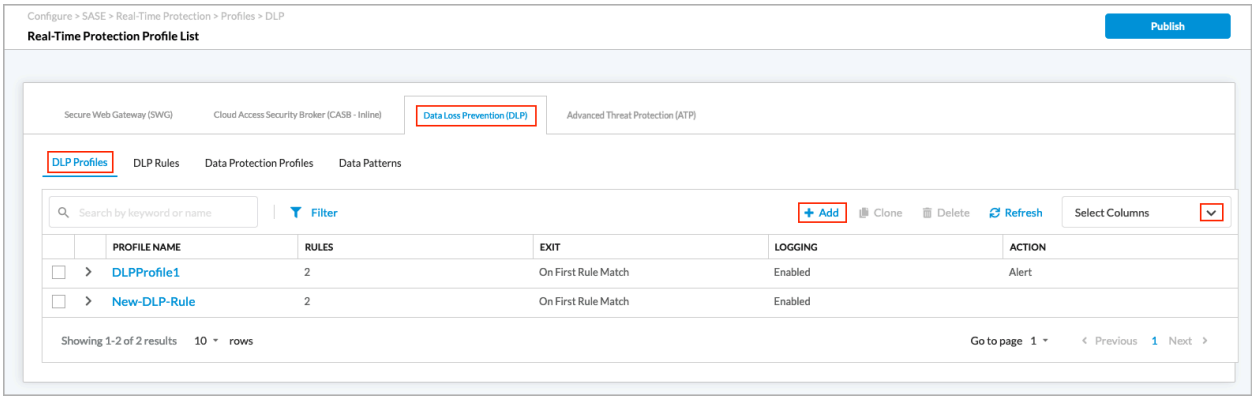
A DLP profile consists of one or more DLP rules.

To configure a DLP profile:

1. Go to Configure > Secure Services Edge > Real-Time Protection > Profiles.

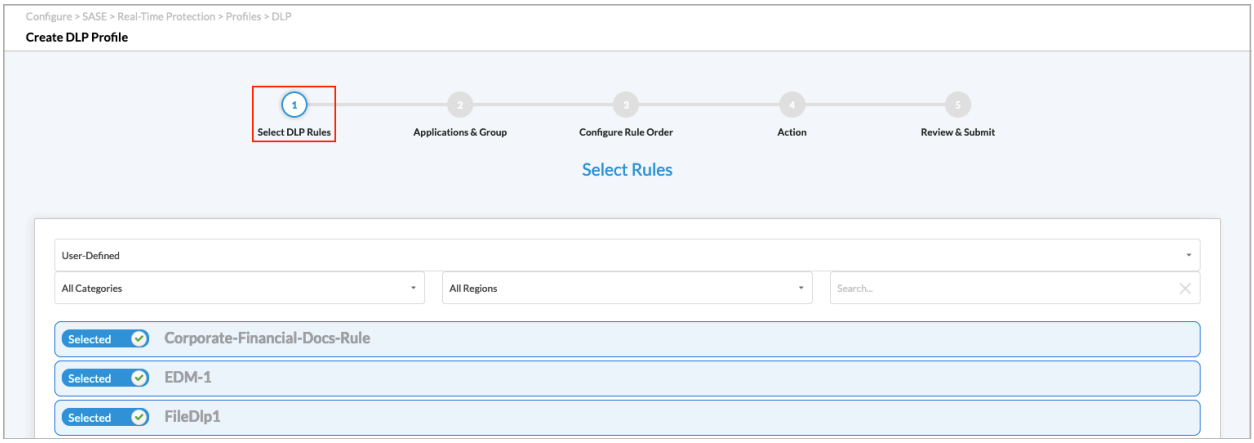


2. Select the Data Loss Prevention (DLP) tab. The following screen displays.



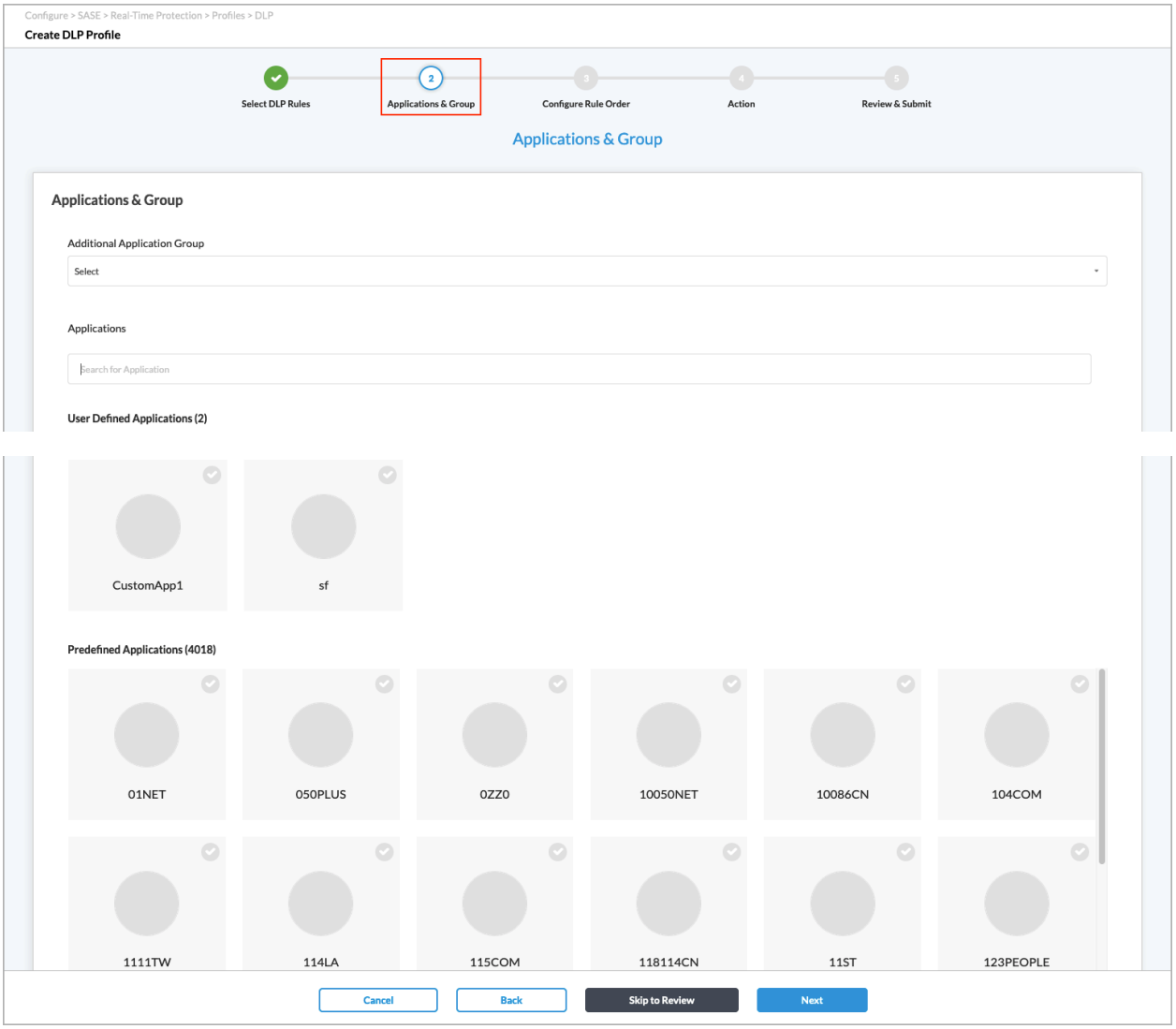
3. Select the DLP Profiles subtab.
4. To customize which columns display, click Select Columns down arrow and then click the columns to select or deselect the ones you want to display. Click Reset to return to the default column display settings.

5. Click the + Add icon to add a new DLP profile. The Create DLP Profile screen displays.



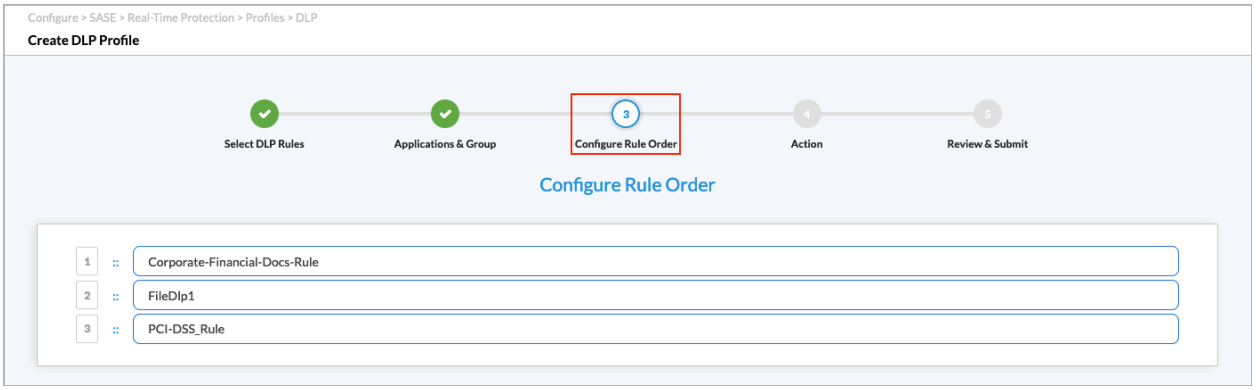
6. In Step 1, Select DLP Rules, select one or more DLP rules. To filter the types of rules that are displayed, use the User-Defined, All Categories, and All Regions boxes.

7. Click Next to go to Step 2, Applications & Group. Enter information for the following fields.

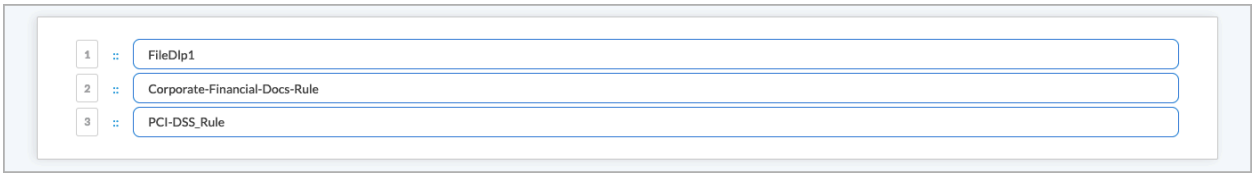


Field	Description
Additional Application Group	Select an additional application group. You can select only one group. Note that only user-defined application groups are listed.
Applications	Enter the name of an application to search for.
User Defined Applications	Select one or more user-defined applications.
Predefined Applications	Select one or more predefined applications.

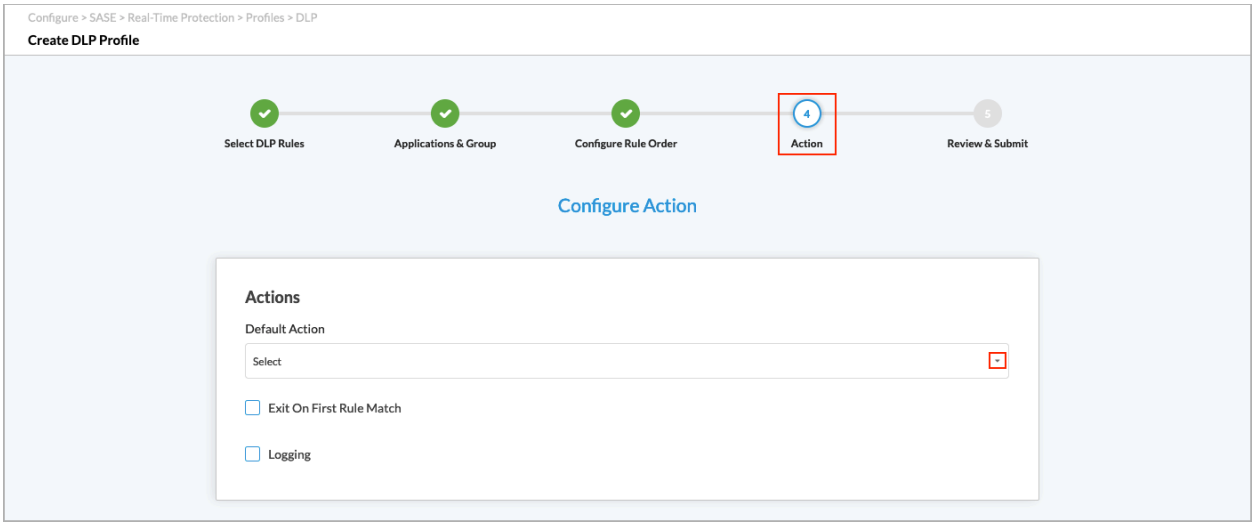
8. Click Next to go to Step 3, Configure Rule Order.



9. If you select two or more DLP rules in the Select DLP Rules screen, you can change the order in which the rules are processed by dragging and dropping the rules to the desired order. For example, the following screen shows that the rules have been reordered so that the FileDlp1 rule is processed first, followed by Corporate-Financial-Docs-Rule and then PCI-DSS_Rule.



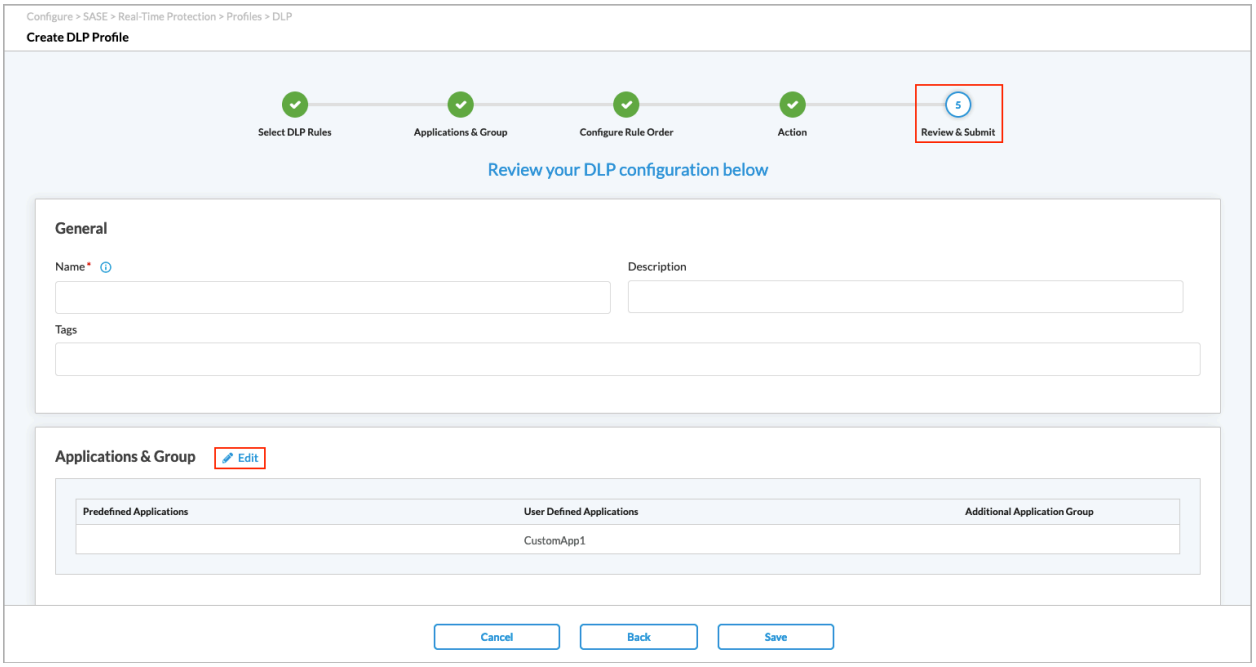
10. Click Next to go to Step 4, Action. Enter information for the following fields.



Field	Description
Default Action	Click the down arrow, and the select a default action. The default action is applied if none of the scanned data matches a rule.

Field	Description
	◦ Alert ◦ Allow ◦ Block ◦ Reject
Exit on First Rule Match	Click to exit rule processing after the first match occurs.
Logging	Enable logging of the DLP rules processing. All logs are sent to Versa Analytics.

11. Click Next.
12. In Step 5, Review & Submit. Enter a name for the DLP rule and, optionally, a description and one or more tags. A tag is an alphanumeric descriptor, with no white spaces or special characters, that you can use to search the rules.



13. Review the configuration.
14. To change any of the information, click the Edit icon and then make the changes.
15. After review, click Save to create the new DLP profile.

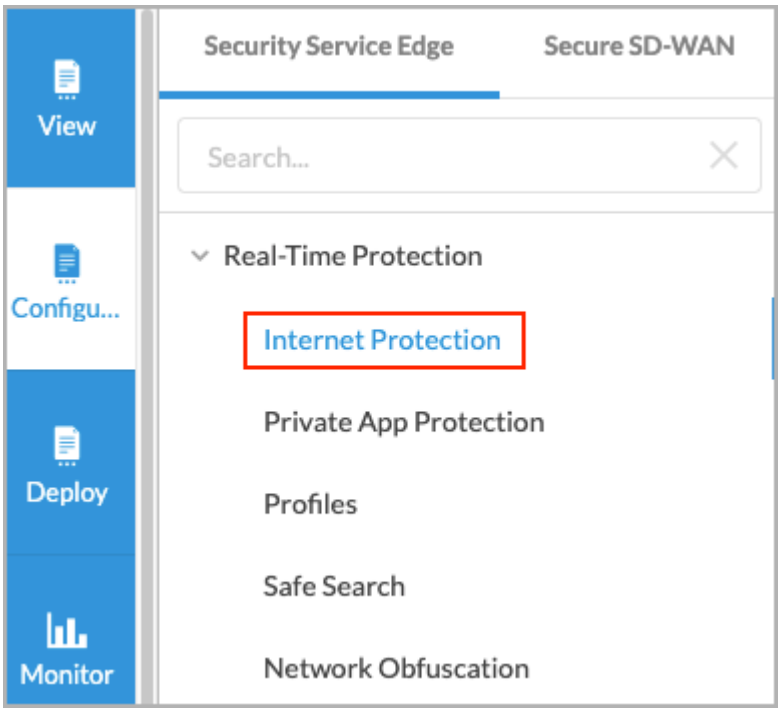
You can use the DLP profiles when you configure internet protection rules. For more information, see Configure SASE Internet Protection Rules.

Associate the DLP Profile with a SASE Internet Protection Rule

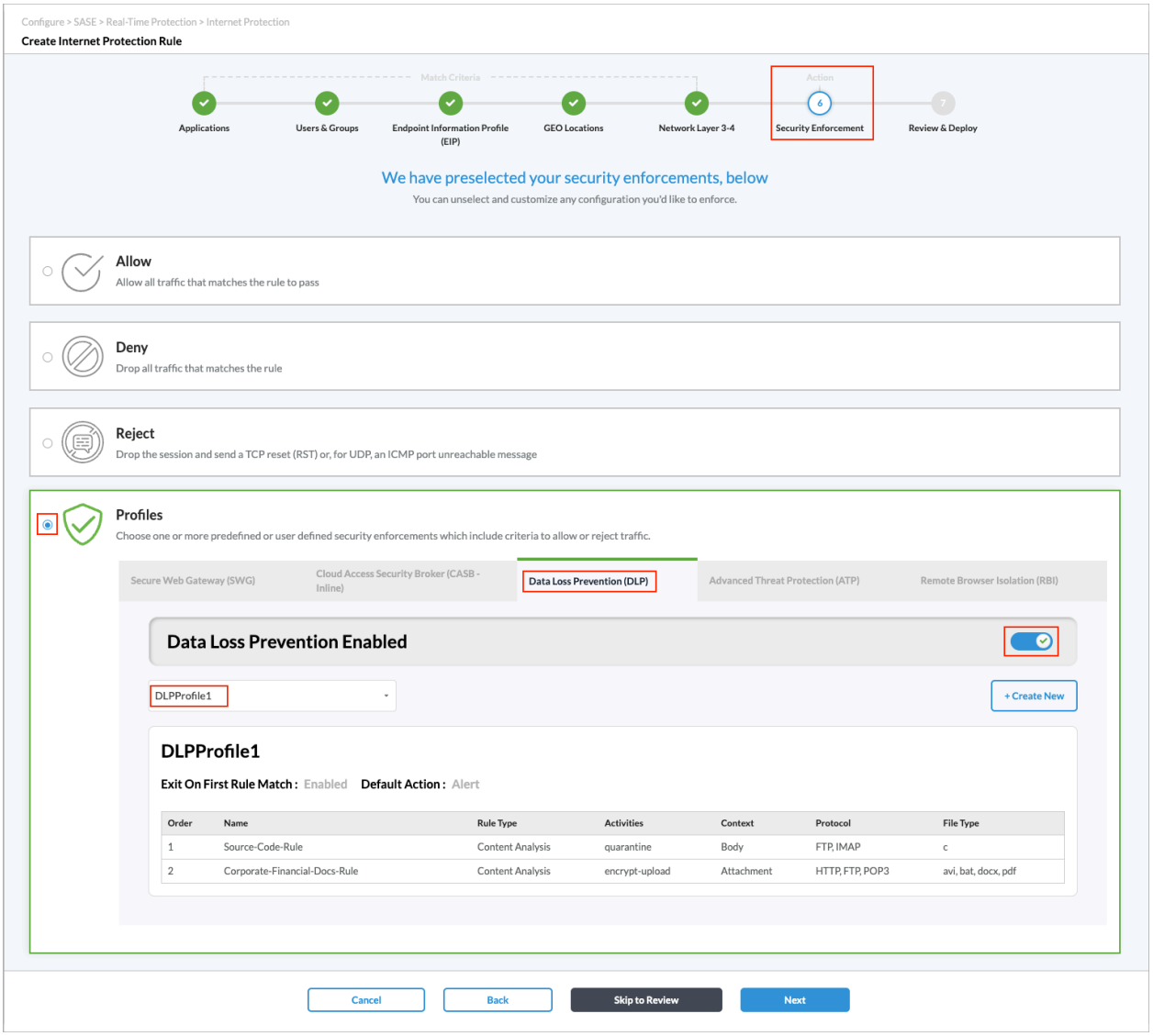
To oversee, track, and report all data transactions in the network and to scan all content that passes through an organization's ports and protocols to ensure data security in the organization, you can associate a DLP profile with a SASE internet protection rule. DLP provides a set of tools and processes for detecting and preventing data breaches, cyber exfiltration, and unwanted destruction of sensitive data. You use DLP to protect and secure an organization's data and to comply with regulations.

To associate a DLP profile with a SASE internet protection rule:

1. Go to Configure > Real-Time Protection > Internet Protection.



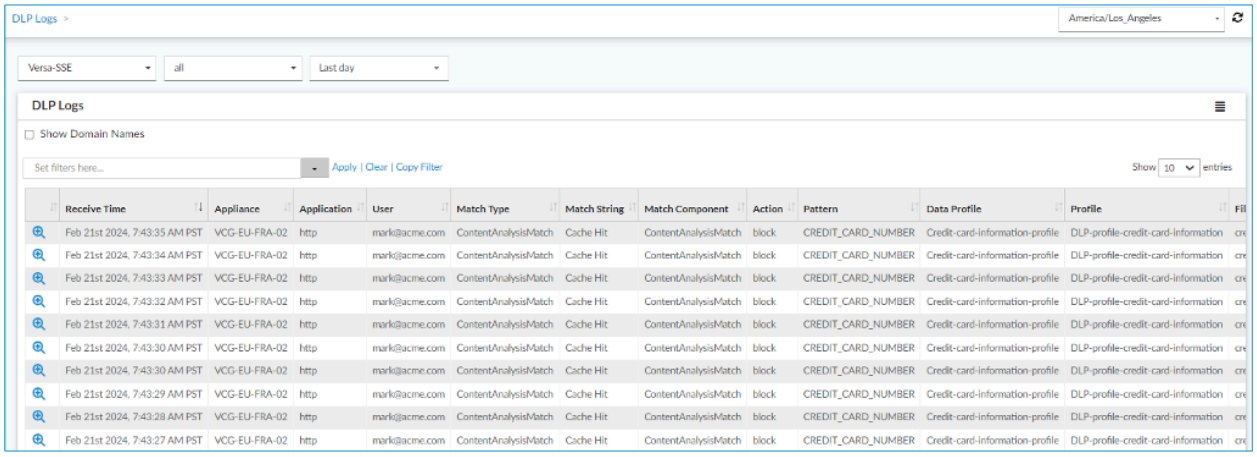
2. In the Internet Protection Rules List screen, click + Add to create a rule. The Create Internet Protection Rule screen displays. For more information, see Configure SASE Internet Protection Rules.
3. In the Security Enforcement screen, select Profiles, and then select the Data Loss Prevention (DLP) tab.



4. Click the slider bar to enable DLP.
5. Select a DLP profile from the drop-down list.
6. Click Next.
7. In the Review & Deploy, review your selections and make any needed updates.
8. Click Save.

Verification

To view the logs for DLP in the SASE portal, click Analytics in the left menu, and go to Logs > DLP.



Use Versa Analytics

To monitor Concerto and analyze Concerto information, you use Versa Analytics.

For more information on real-time monitoring of site-to-site tunnels, routes, and digital experience, see View Integrated Monitoring and Analytics.

For information about Versa Analytics, including dashboards and logs, see Versa Analytics.