
Use the Versa SASE Client Application

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

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.

The SASE client provides secure IKEv2 IPsec-based remote access VPN connectivity with enterprise-grade authentication, including the following:

- EAP-MSCHAPv2
- Two-factor authentication (2FA)
- One-time password (OTP) delivered through SMS or email
- Time-based one-time password (TOTP)

The SASE client supports the following OS versions:

- Android 6.0 and later
- iOS 13 and later
- Linux
 - Debian 10 (Buster) and later (equivalent to Ubuntu 18.04 and later)
 - Fedora 34 and later (equivalent to RHEL8 or CentOS8 and later)
- MacOS 10.14 and later
- Versa Operating System™ (VOS™) Releases 20.2.3 and later
- Versa Concerto Releases 11.3.1 and later
- Windows
 - Windows 11 (all versions)
 - Windows 10, 10.0.16299 and later
 - Windows 7 Professional Version 6.1.7601
 - Windows 8.1 Version 6.3 (OS Build 9600)
 - Windows Server 2016 Version 1607 (OS build 14393.693)
 - Windows Server 2019 Version 10.0.17763

- Windows Server 2012R2 6.3.9600

This article describes the SASE features and how to configure and use them. Before using the SASE client application, you must set up the Secure Access Service. See [Configure the Versa Secure Access Service](#). For more information about installing the SASE client, see [Configure Versa SASE Clients](#).

SASE Client Features

The following table describes the SASE client features available for Android (and ChromeOS), iOS, Linux, MacOS, and Windows clients, the SASE client application release in which the features are supported, and the corresponding VOS and Concerto software releases that support the feature.

Feature	Description	OS Support
Always-on connection	Allow preregistered or authorized clients to connect to the VSA gateway without user intervention.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.3.0 and later ◦ Concerto—Releases 11.3.1 and later ◦ iOS—Not supported ◦ Linux—Not supported ◦ MacOS—Releases 7.3.0 and later ◦ VOS—Releases 21.2.1 and later ◦ Windows—Releases 7.2.1 and later
Application-based split tunnel	Exclude or include traffic from specific Windows processes or applications in the tunnel.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.5.2 and later ◦ Concerto—Releases 11.3.1 and later ◦ iOS—Not supported ◦ Linux—Not supported ◦ MacOS—Not supported ◦ VOS—Releases 21.2.1 and later ◦ Windows—Releases 7.5.1 and later
Automatic configuration sync	Automatically synchronize configuration with the secure access portal at configured regular intervals while connecting to a gateway.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.4.3 and later ◦ Concerto—Not supported ◦ iOS—Releases 7.5.0 and later ◦ Linux—Releases 7.4.2 and later ◦ MacOS—Releases 7.3.0 and later ◦ VOS—Releases 22.1.3 and later

		<ul style="list-style-type: none"> ◦ Windows—Releases 7.5.1 and later
Autodisconnect	Automatically disconnect tunnel after the configured autodisconnect interval.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.5.6 and later ◦ Concerto—Not supported ◦ iOS—Not supported ◦ Linux—Not supported ◦ MacOS—Releases 7.6.0 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.8.1 and later
Automatic software update	Automatically check for software updates, and prompt users to update to the latest version when available.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Not supported ◦ Concerto—Releases 11.3.2 and later ◦ iOS—Releases 7.5.4 and later ◦ Linux—Not supported ◦ MacOS—Releases 7.6.0 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.8.1 and later
Best gateway selection	Select the best available gateway in a gateway group based on gateway proximity, gateway load, and network latency.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.4.3 and later ◦ Concerto—Releases 11.3.1 and later ◦ iOS—Releases 7.5.0 and later ◦ Linux—Releases 7.4.2 and later ◦ MacOS—Releases 7.3.0 and later

		<ul style="list-style-type: none"> ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.4.2 and later
Captive portal detection	Automatically detect captive portal in the internet path, and prompt users to restore internet connectivity using the captive portal page displayed automatically.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.3.0 and later ◦ Concerto—Not supported ◦ iOS—Releases 7.4.1 and later ◦ Linux—Releases 7.4.2 and later ◦ MacOS—Releases 7.3.0 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.4.2 and later
Certificate-based device authentication	Versa cloud gateway prompts SASE client to perform device authentication by presenting the device certificate.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Not supported ◦ Concerto—Not supported ◦ iOS—Releases 7.4.1 and later ◦ Linux—Not supported ◦ MacOS—Releases 7.6.0 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.8 and later
Connection to gateway group	Connect to the most optimal gateway from a group of gateways.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.4.3 and later ◦ Concerto—Releases 11.3.1 and later ◦ iOS—Releases 7.5.0 and later ◦ Linux—Releases 7.4.2 and later ◦ MacOS—Releases 7.3.0 and

		<p>later</p> <ul style="list-style-type: none"> ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.4.2 and later
Connect to specific gateway	Connect to a specific gateway from a list of gateways.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.3.0 and later ◦ Concerto—Releases 11.3.1 and later ◦ iOS—Releases 1.3.0 and later ◦ Linux—Releases 7.4.2 and later ◦ MacOS—Releases 7.2.0 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.2 and later
Custom logo	Customize the client screens with tenant-specific logo. Secure access portal provides the logo URL. Client downloads the logo from the configured URL and displays the custom logo instead of the default Versa Networks logo.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.4.3 and later ◦ Concerto—Releases 11.3.1 and later ◦ iOS—Releases 7.4.1 and later ◦ Linux—Not supported ◦ MacOS—Releases 7.3.0 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.4.6 and later
Disable restricted access imposed during Fail mode Close action	Disable restricted access. If the the Fail mode action is Close, client enforces restricted access by blocking all the traffic until the client establishes a tunnel to Versa cloud	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.5.1 and later ◦ Concerto—Releases 11.3.1 and

	gateway. In Restricted mode, traffic is allowed only to allowed (whitelisted) domains and IP address destinations.	<p>later</p> <ul style="list-style-type: none"> ◦ iOS—Not supported ◦ Linux—Not supported ◦ MacOS—Releases 7.3.0 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.5.7 and later
Domain-based split tunnel	Exclude or include traffic specific domains in the tunnel.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Not supported ◦ Concerto—Releases 11.3.1 and later ◦ iOS—Not supported ◦ Linux—Not supported ◦ MacOS—Not supported ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.5.1 and later
Endpoint information profile (EIP)	A Versa endpoint information profile (EIP) can classify endpoints based on multiple types of endpoint posture information. To protect the endpoints in an enterprise network, you can create EIP profiles, which define rules that allow the VOS SASE software to filter information from endpoint device traffic and then match information to enforce security policy.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Not supported ◦ Concerto—Releases 11.3.2 and later ◦ iOS—Not supported ◦ Linux—Not supported ◦ MacOS—Releases 7.6.0 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.7.0 and later
Fail Mode (Close/Open)	Configure fail mode:	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.4.5 and later

	<ul style="list-style-type: none"> • Fail-Open—Internet is accessible with or without a connection to a Versa Cloud Gateway (VCG). • Fail-Close—Internet is accessible only when a client is connected to a VCG. 	<ul style="list-style-type: none"> ◦ Concerto—Releases 11.3.1 and later ◦ iOS—Not supported ◦ Linux—Not supported ◦ MacOS—Releases 7.3.0 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.5.5 and later
FIPS compliance	Enable systemwide FIPS policy and allow only FIPS-supported ciphers for TLS and IPsec communication.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.5.1 and later ◦ Concerto—Not supported ◦ iOS—Not supported ◦ Linux—Not supported ◦ MacOS—Releases 7.5.4 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.4.7 and later
Hide gateways and list only gateway groups	Use the Display Gateway option during portal registration on a VOS device to display or hide gateways. If disabled, the Gateways drop-down list in the main client window displays only gateway groups and not gateways.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.5.6 and later ◦ Concerto—Releases 11.3.2 and later ◦ iOS—Releases 7.5.4 and later ◦ Linux—Not supported ◦ MacOS—Releases 7.5.0 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.8 and later

Maintenance mode notification	When a VCG is under maintenance, notify clients connected to that gateway and prompt users to connect to a different gateway.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.5.6 and later ◦ Concerto—Not supported ◦ iOS—Releases 7.5.4 and later ◦ Linux—Not supported ◦ MacOS—Releases 7.6.0 and later ◦ VOS—Releases 22.1.1 and later ◦ Windows—Releases 7.8 and later
Multifactor authentication (MFA) OTP TOTP Certificate	Client uses authentication factors such as OTP, TOTP, and x509 certificate in addition to LDAP, RADIUS, and SAML.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.5.4 and later ◦ Concerto—Releases 11.3.1 and later (MFA, OTP, TOTP) ◦ iOS—Releases 7.5.4 and later ◦ Linux—Not supported ◦ MacOS—Releases 7.6.0 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.6.0 and later
Option to disable IPv6	Instruct client to disable IPv6 on the device.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Not supported ◦ Concerto—Not supported ◦ iOS—Not supported ◦ Linux—Not supported ◦ MacOS—Not supported ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.5.8 and later

Password expiry due warning	Display password expiration notification message to remind users to reset the password.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.4.3 and later ◦ Concerto—Releases 11.3.2 and later ◦ iOS—Releases 7.4.1 and later ◦ Linux—Not supported ◦ MacOS—Releases 7.3.0 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.5.8 and later
Path SLA monitoring as per the configured path switchover profile.	Have client monitor the performance of all active paths to the connected Versa cloud gateway and switches to an alternate path if the SLA of the currently active path degrades while the other paths offer the required SLA.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Not supported ◦ Concerto—Not supported ◦ iOS—Not supported ◦ Linux—Not supported ◦ MacOS—Releases 7.5.0 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.6.0 and later
Periodic metric reporting	Periodically send metric information to the SASE portal.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.5.1 and later ◦ Concerto—Not supported ◦ iOS—Releases 7.5.0 and later ◦ Linux—Not supported ◦ MacOS—Releases 7.3.7 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.4.6 and later

Policy violation notification	Notify users when their activities violate the company's IT security policies	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.4.3 and later ◦ Concerto—Not supported ◦ iOS—Not supported ◦ Linux—Not supported ◦ MacOS—Releases 7.5.4 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.5.9 and later
Prefix-based split tunnel	Exclude or include traffic destined to specific prefixes in the tunnel.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.4.3 and later ◦ Concerto—Releases 11.3.1 and later ◦ iOS—Not supported ◦ Linux—Not supported ◦ MacOS—Not supported ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.5.1 and later
Pre-logon connectivity	Allow a SASE client to establish secure connection to an organization's network. Pre-logon authenticates a user on the client device and then establishes a secure connection to the organization's network.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.3.0 and later ◦ Concerto—Not supported ◦ iOS—Not supported ◦ Linux—Not supported ◦ MacOS—Not supported ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.2.5 and later

Register with DNS	Indicate the client to register the host with the DNS server.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Not supported ◦ Concerto—Releases 11.3.1 and later ◦ iOS—Not supported ◦ Linux—Not supported ◦ MacOS—Not supported ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.2.10 and later (CLI support)
Remember credentials	Remember user credentials.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.4.3 and later ◦ Concerto—Releases 11.3.1 and later ◦ iOS—Releases 7.4.1 and later ◦ Linux—Not supported ◦ MacOS—Releases 7.3.0 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.2.2 and later
Strict tunnel mode	Redirect all traffic through the tunnel. If disabled, specific traffic is routed through a tunnel and the rest is sent directly onto a WiFi or Ethernet interface. You can configure this feature from the secure access portal.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.4.3 and later ◦ Concerto—Releases 11.3.1 and later ◦ iOS—Not supported ◦ Linux—Not supported ◦ MacOS—Not supported ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.8 and later

Switch to optimal gateway	Use dynamic gateway selection to allow SASE clients to select the best gateways based on distance and availability. For more information, see Enable Performance-Based Dynamic Gateway Selection , below.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Not supported ◦ Concerto—Not supported ◦ iOS—Releases 7.5.0 and later ◦ Linux—Not supported ◦ MacOS—Releases 7.3.0 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.6.0 and later
Tamperproof protection	If enabled from the server side, you cannot uninstall the client, delete the client account, or delete any files from the installation directory. To disable, click the Tamper Protection toggle button in the Account Details window and then enter the tamper protection authentication key.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Not supported ◦ Concerto—Not supported ◦ iOS—Not supported ◦ Linux—Not supported ◦ MacOS—Not supported ◦ VOS—Releases 22.1.3 and later ◦ Windows—Releases 7.8 and later
Trusted network detection and tunnel bypass	<p>Have the client bypass establishing a tunnel to the Versa Cloud Gateway when a device is already connected to a trusted network segment.</p> <p>When you configure trusted network detection on a VOS device, the SASE client tries to reach the host by bypassing the tunnel. The following conditions must be true for the client to bypass establishing a tunnel to Versa Cloud Gateway:</p> <ul style="list-style-type: none"> ◦ The source IP address reported by the client in the HTTP query parameter for the private IP 	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.5.1 and later ◦ Concerto—Releases 11.3.1 and later ◦ iOS—Releases 7.5.2 and later ◦ Linux—Releases 7.4.2 and later ◦ MacOS—Releases 7.5.0 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—Release 7.4.2 and later

	<p>address must be same as the source IP address in the IP header of the received packet.</p> <ul style="list-style-type: none">◦ For trusted network detection, the captive portal must receive the login request through a tunnel interface such as a site-to-site IPSec, GRE, or SD-WAN tunnel and not through a WAN interface. For example, when a user connects from a location with a tunnel interface, this tunnel interface acts as the ingress interface. The request then reaches the captive portal virtual routing instance through a paired tunnel interface. In contrast, when a remote user connects from an untrusted network, the WAN interface on the gateway receives a login request, and then a captive portal that is associated with the routing instance of the WAN interface handles the request. <p>So, when gateway-assisted trusted network detection is enabled, when you try to connect using SASE Client, the client sends a request to the gateway to establish a VPN tunnel. The gateway then verifies if the client request is from an internal network. If it is, the server responds to client informing that it is in a trusted network and shares the time interval to send KeepAlive request.</p> <p>On receiving this information, the client applies the required configuration and sends periodic KeepAlive requests. The SASE client UI displays Trusted Network as the state to indicate that it is connected to a trusted network and that tunnel is bypassed. Trusted network</p>	
--	---	--

	<p>connection does not change any other functionality of the SASE client.</p> <p>While connected to a trusted network, the client monitors network changes on the device and attempts reconnection if the underlay changes or if the KeepAlive request fails. This restarts the connect cycle and the client sends a request to the gateway to establish connection.</p>	
Tunnel monitoring	<p>Monitor the health of the tunnel by checking the reachability of the configured hosts through the tunnel.</p>	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.5.1 and later ◦ Concerto—Releases 11.3.1 and later ◦ iOS—Releases 7.5.2 and later ◦ Linux—Not supported ◦ MacOS—Releases 7.3.7 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—Release 7.4.6 and later
User authentication	<p>Client supports authentication using LDAP, RADIUS, SAML, and local user certificate</p>	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.4.3 and later; local user certificate in Releases 7.5.4 and later ◦ Concerto—Releases 11.3.1 and later (SAML, LDAP, and local) ◦ iOS—Releases 7.5.4 and later ◦ Linux—Not supported ◦ MacOS—Releases 7.6.0 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—LADP, RADIUS, SAML, local in Releases 7.2.0

		and later; certificate in Releases 7.6.0 and later
WebSocket-based notification	Versa Cloud Gateway delivers various notifications to the client using the WebSocket connection established by the client.	<ul style="list-style-type: none"> ◦ Android and ChromeOS—Releases 7.5.2 and later ◦ Concerto—Not supported ◦ iOS—Releases 7.5.2 and later ◦ Linux—Not supported ◦ MacOS—Releases 7.5.0 and later ◦ VOS—Releases 22.1.3 and later ◦ Windows—Release 7.5.9 and later

Register with the VSA Portal

After you place an order for VSA, you receive an email that contains the following information:

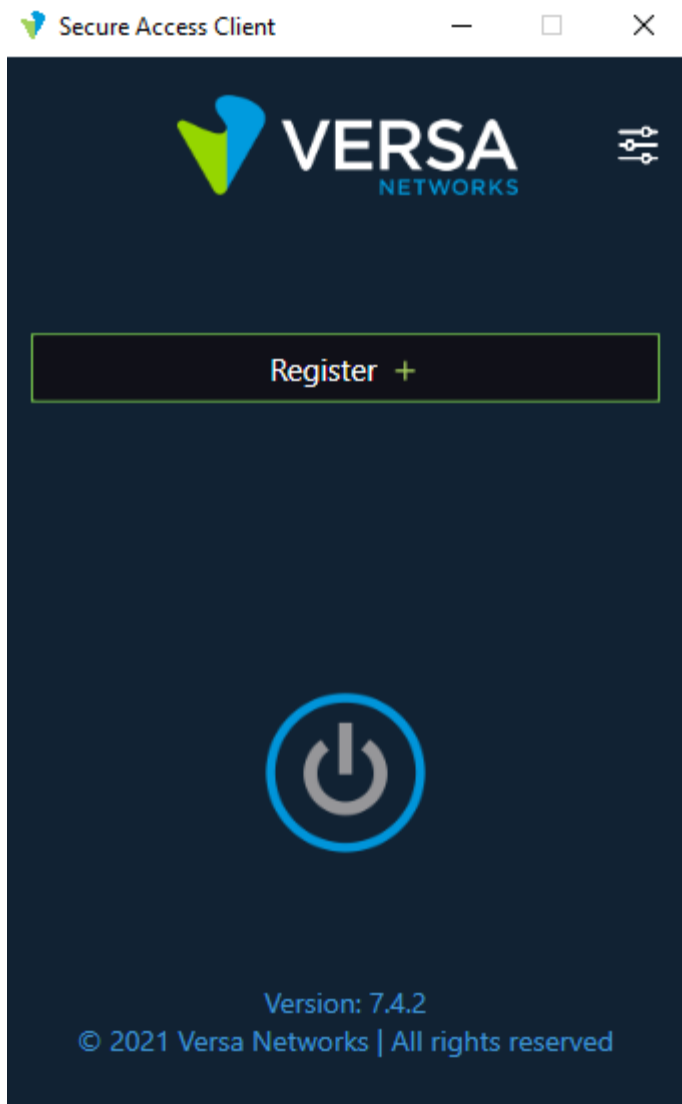
- Link to the registration portal's FQDN or IP address
- Your enterprise name
- Your user ID

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

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

To register with the VSA portal:


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



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

Secure Access Client

— □ ×

 **VERSA**
NETWORKS

Register

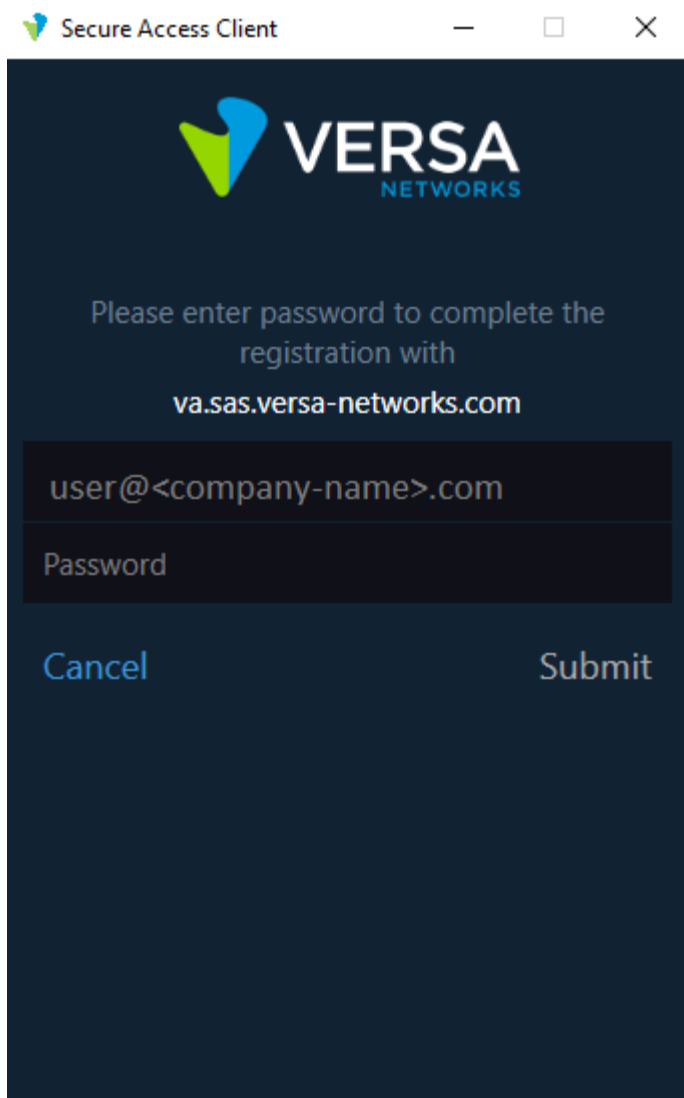
Portal FQDN

Enterprise Name

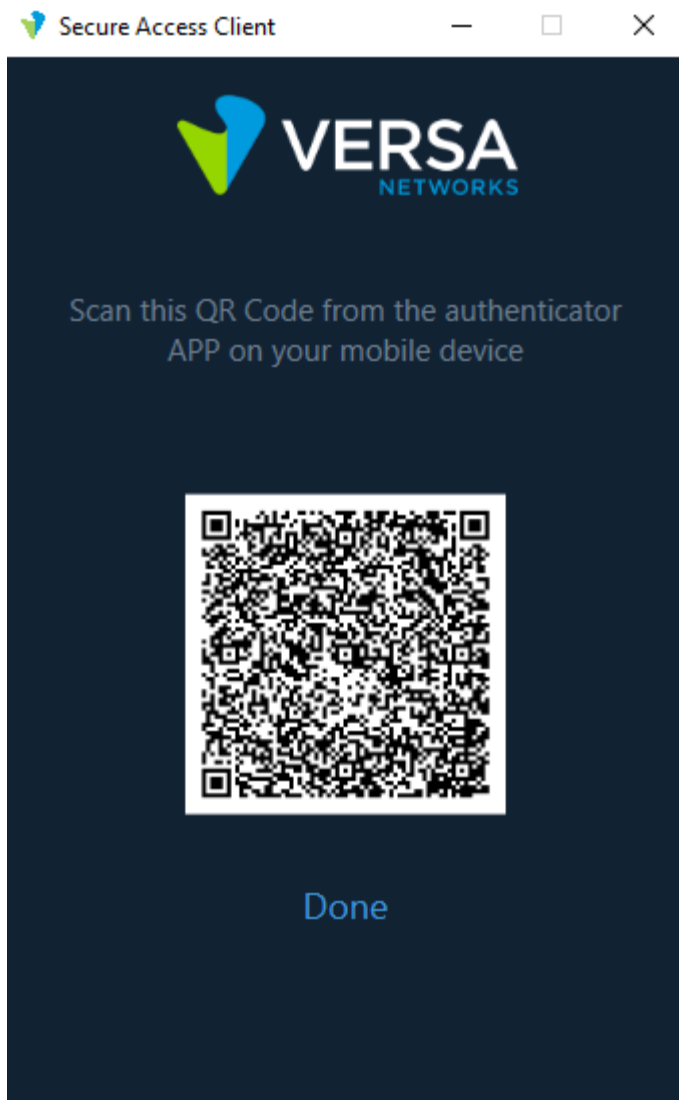
User ID

Cancel Submit

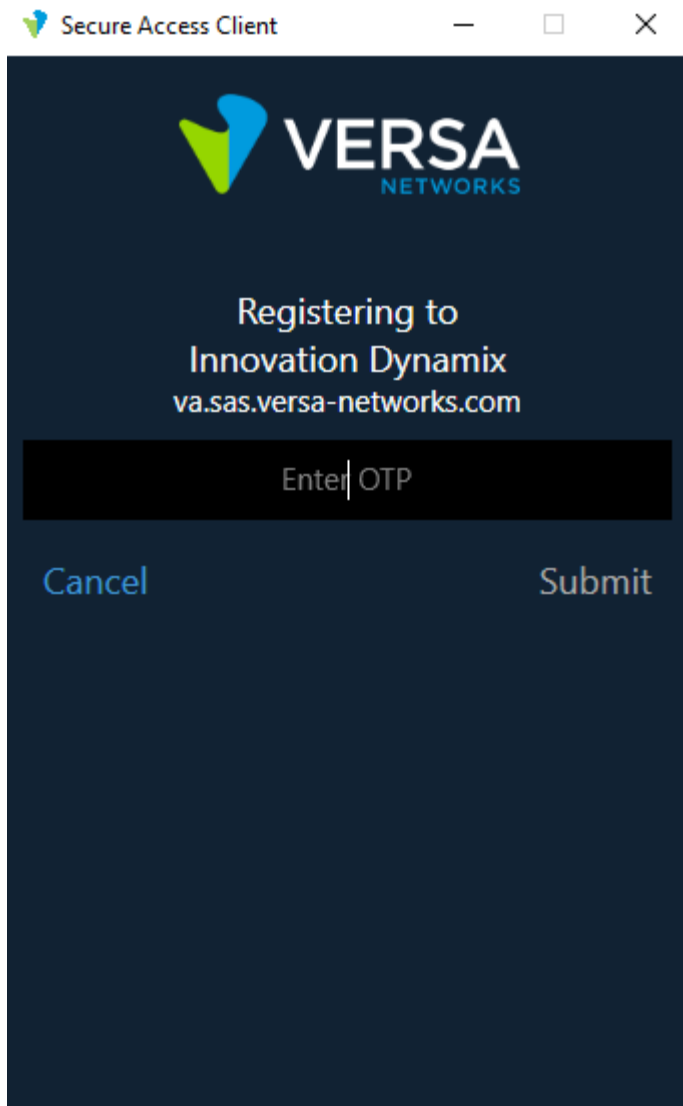
4. Enter the username and password that you received from the administrator, and then click Submit.



5. If authentication using two-factor authentication is required, enter the one-time password that you received in email or through a mobile message server, and click Submit. After the one-time password is validated, the registration process is complete.
6. (For Releases 21.2.1 and later.) 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 required, the client login page similar to the following displays:

Secure Access Client

<  **VERSA**
NETWORKS

 **VERSA**
NETWORKS  English ▼

Username

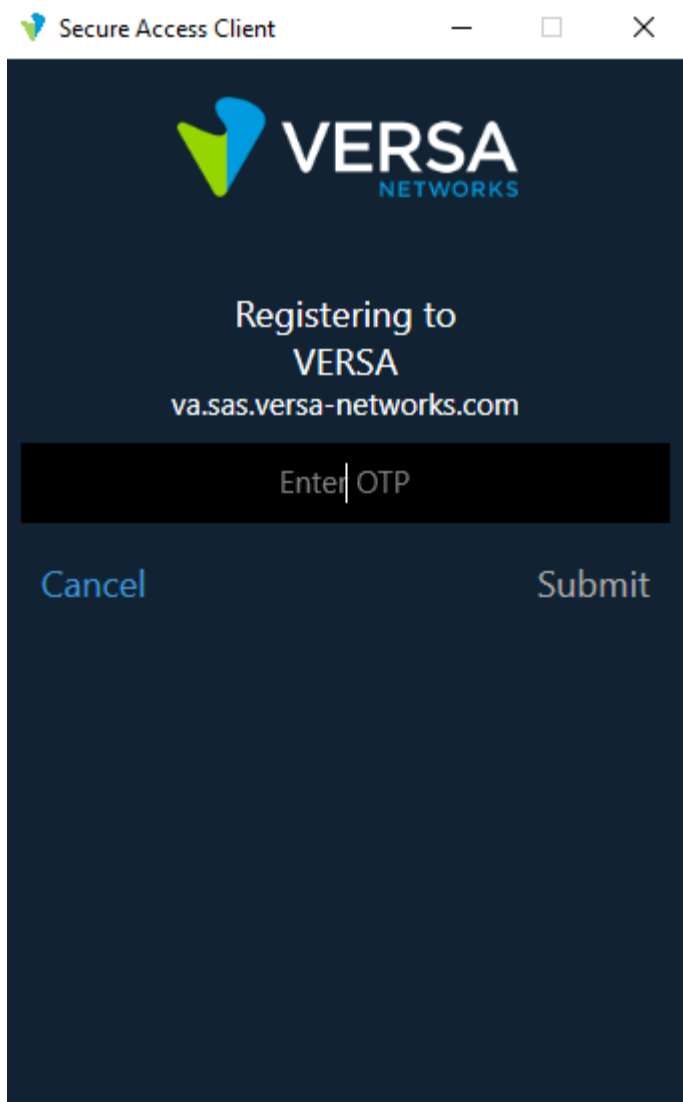
Password

☐ Remember me

[Forgot your password?](#)

LOGIN

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




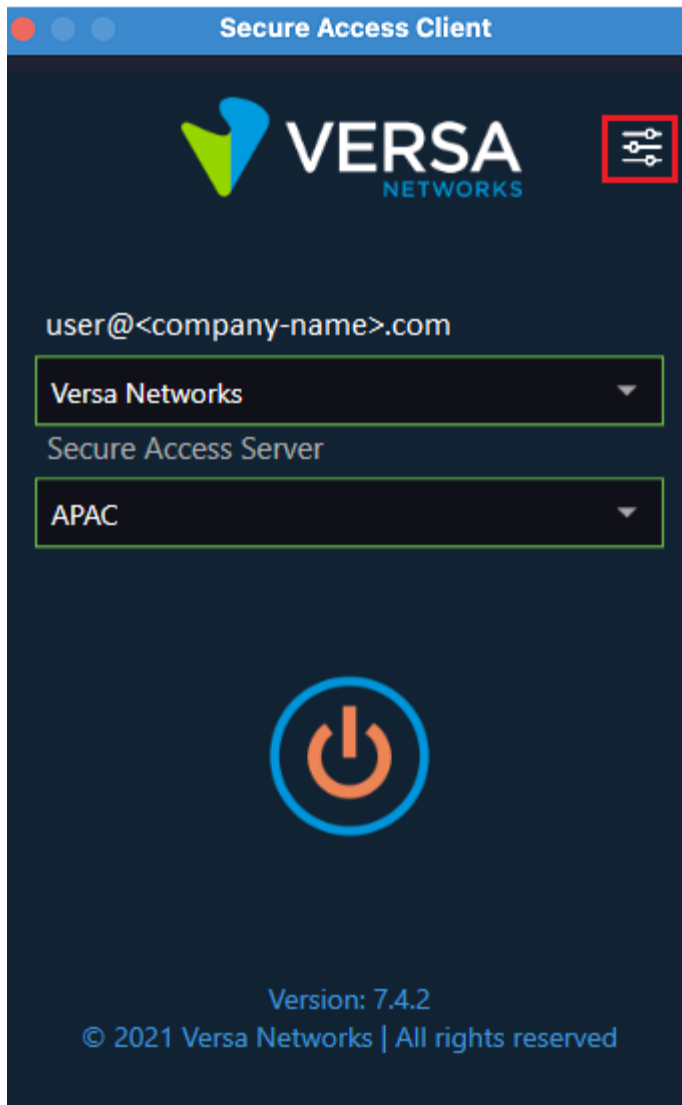
Add a New Connection to the Secure Access Gateway

For MacOS only.

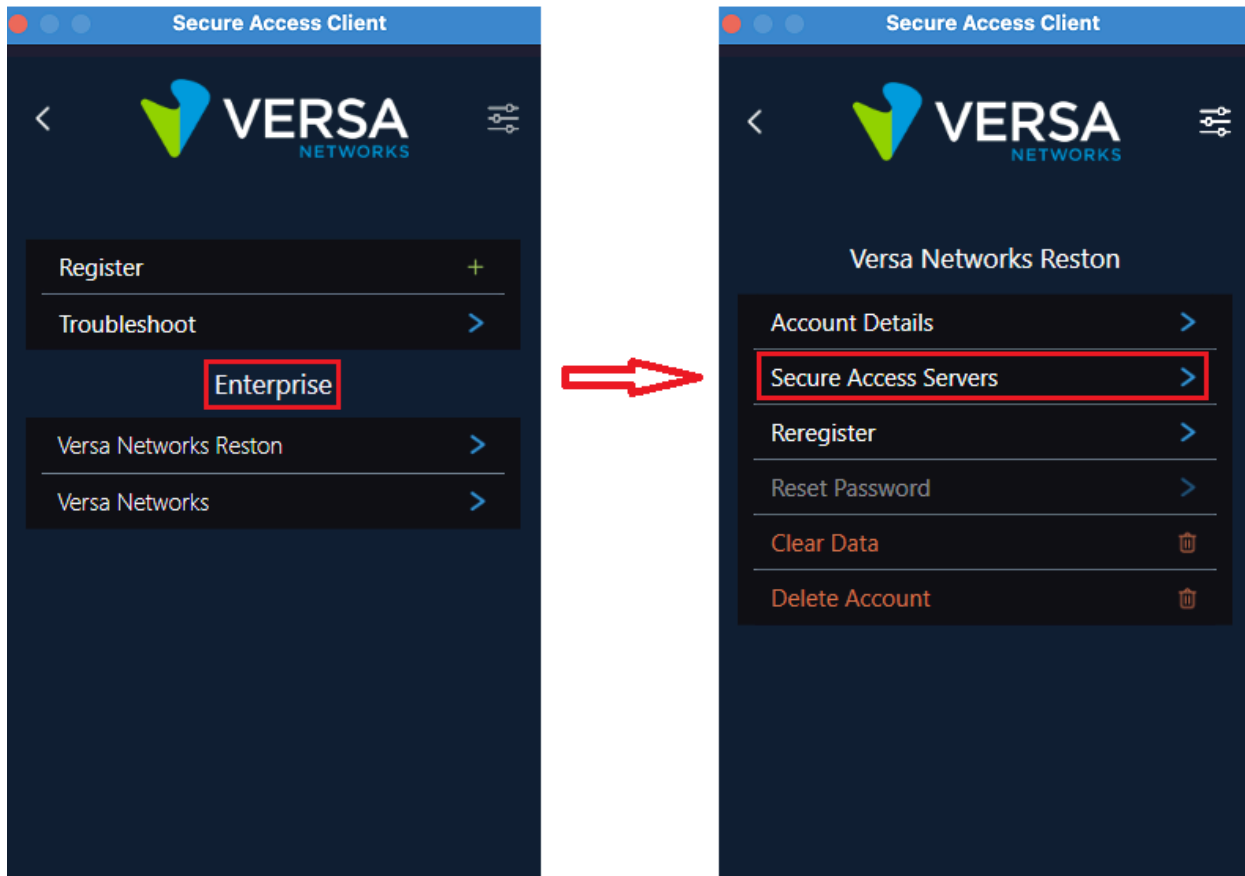
After you successfully register with the portal, the system automatically creates a secure access gateway connection profile. In MacOS, you can add new connections manually.

To add a new connection to the secure access gateway:

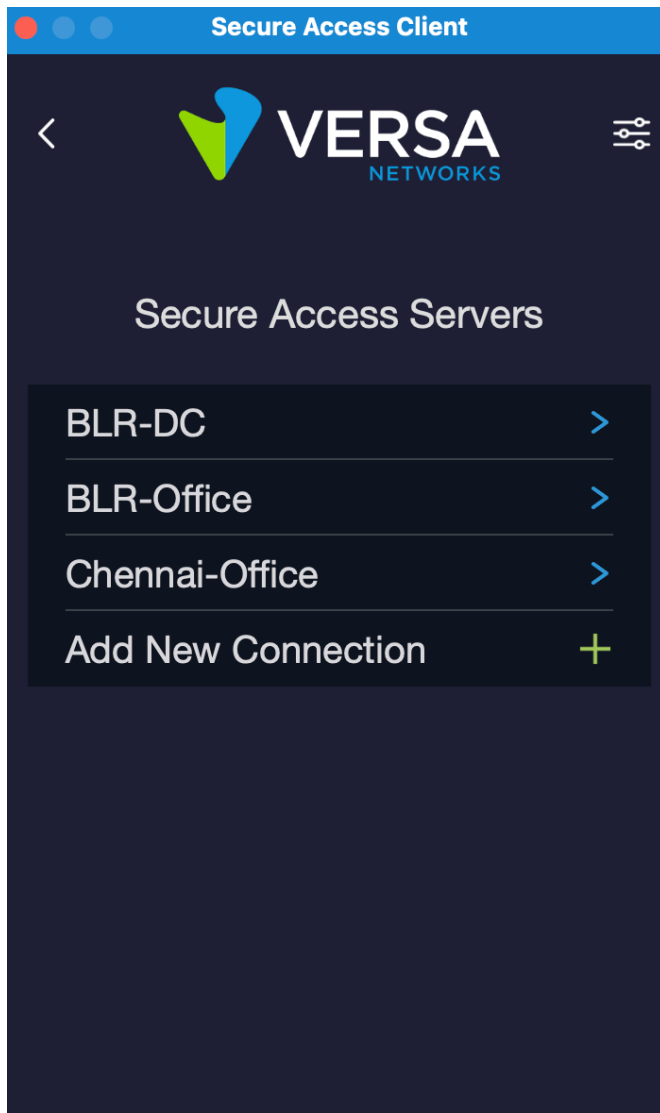
1. In the SASE client home screen, click the  Settings icon.



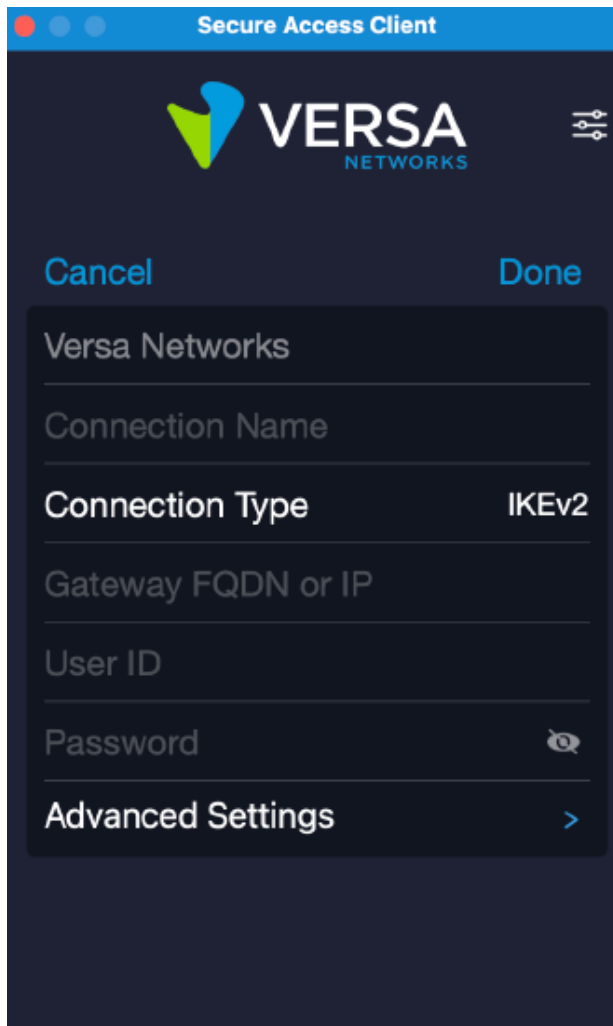
2. Click the enterprise name under Enterprise, and then click Secure Access Servers..



3. In the Secure Access Servers screen, click Add New Connection.



4. Enter the information for the new connection in the following fields.



Field	Description
Connection Name	Enter a name for the new connection.
Connection Type	Select the connection type.
Gateway FQDN or IP	Enter the FQDN or IP address of the gateway.
User ID	Enter the username or ID for the new user.
Password	Enter a password for the new user.
Remember Credentials	Toggle to remember the login credentials.
Advanced Settings	Click to enter advanced settings. For more information, see Configure Advanced Settings , below.


5. Click Done.

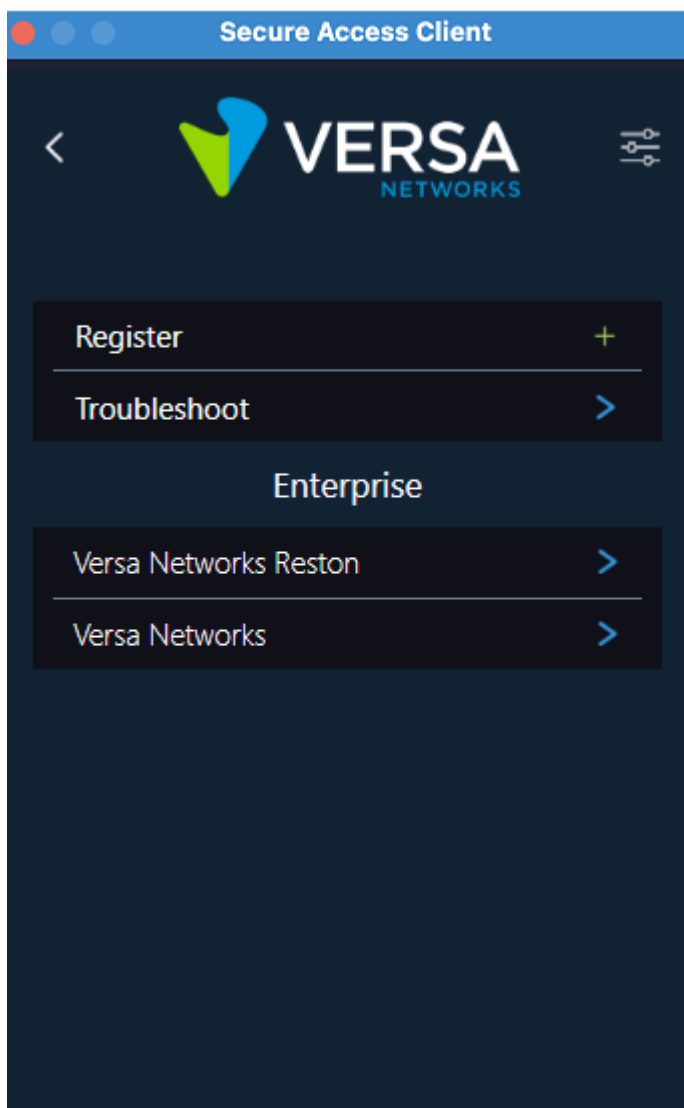
Configure Advanced Settings

Set IKE Phase 1 and Phase 2

For Android and MacOS only.

To set IKE Phase 1 and Phase 2 for MacOS devices:

1. In the SASE client home screen, click the  Settings icon.
2. In the Enterprise section, click the account for which to set IKE phase details.

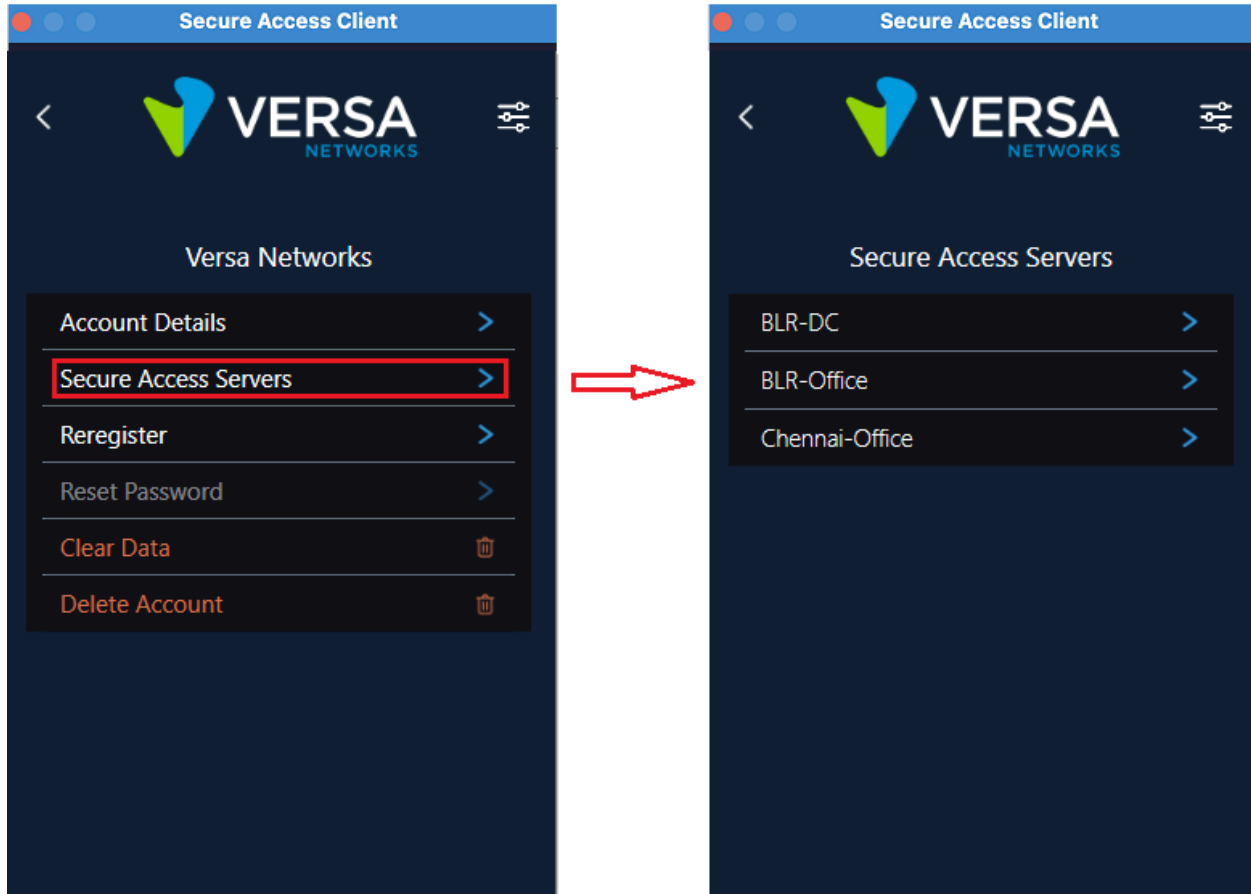


3. Click Secure Access Servers, and then click the secure access server for which to set IKE phase details.

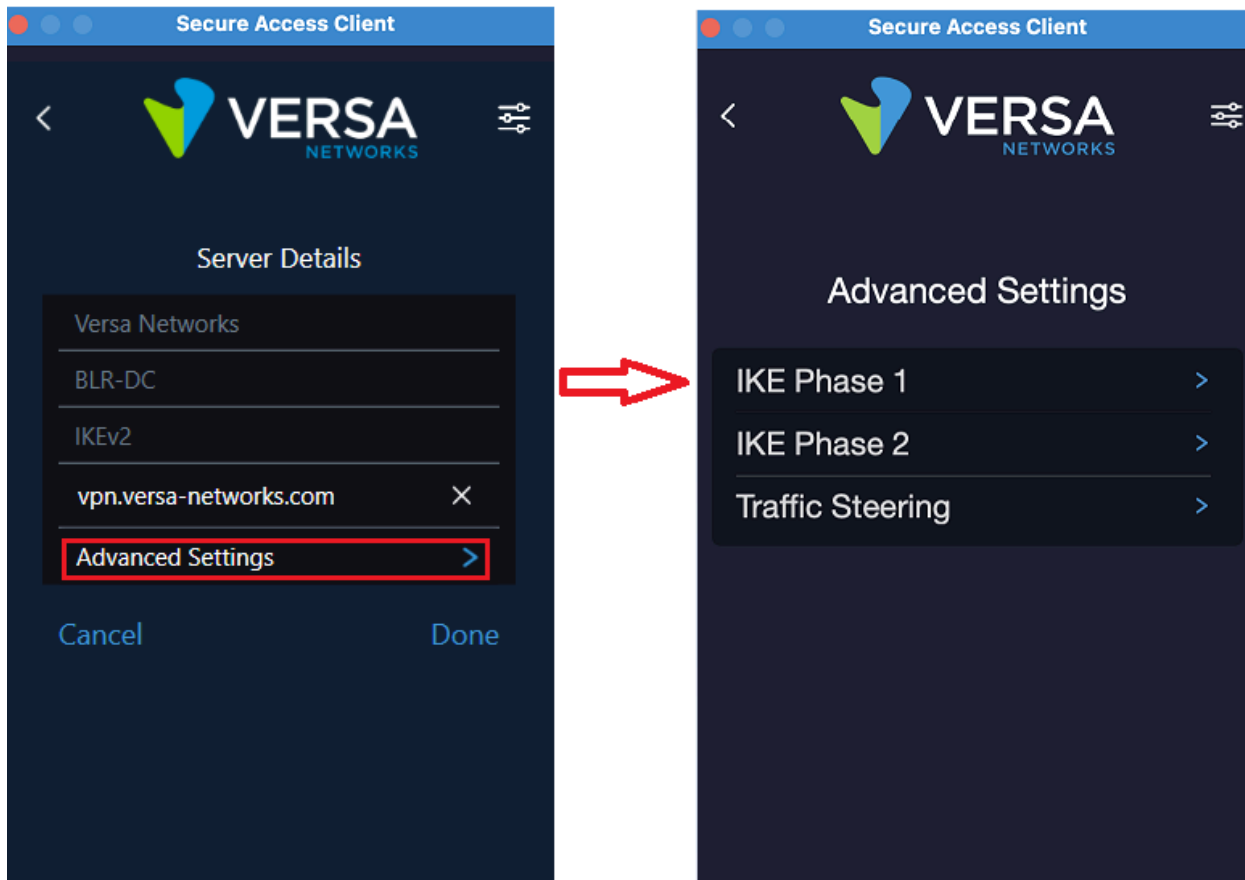
[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Director/Versa_SASE_Client/Use_the_V...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Director/Versa_SASE_Client/Use_the_V...)

Updated: Wed, 23 Oct 2024 08:43:16 GMT

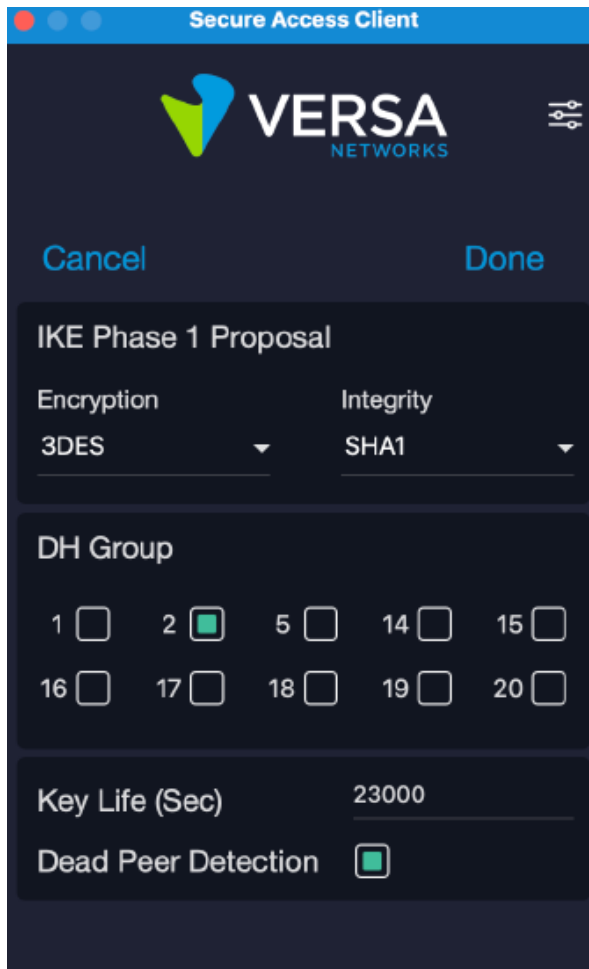
Copyright © 2024, Versa Networks, Inc.



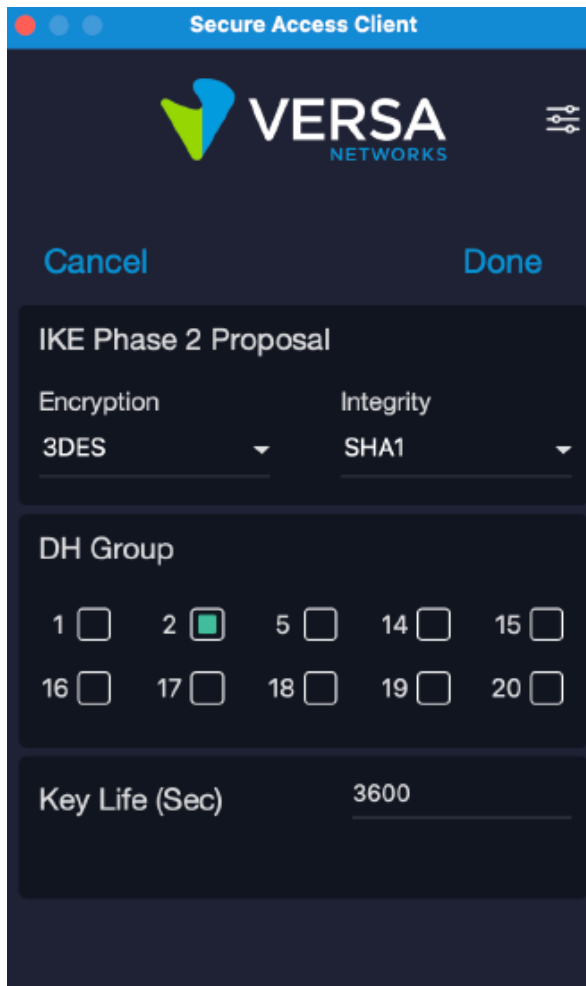
4. In the Server Details screen, click Advanced Settings, and then click IKE Phase 1.



5. Enter the required information, and then click Done.



6. In the Advanced Settings screen, click IKE Phase 2, and enter the required information.

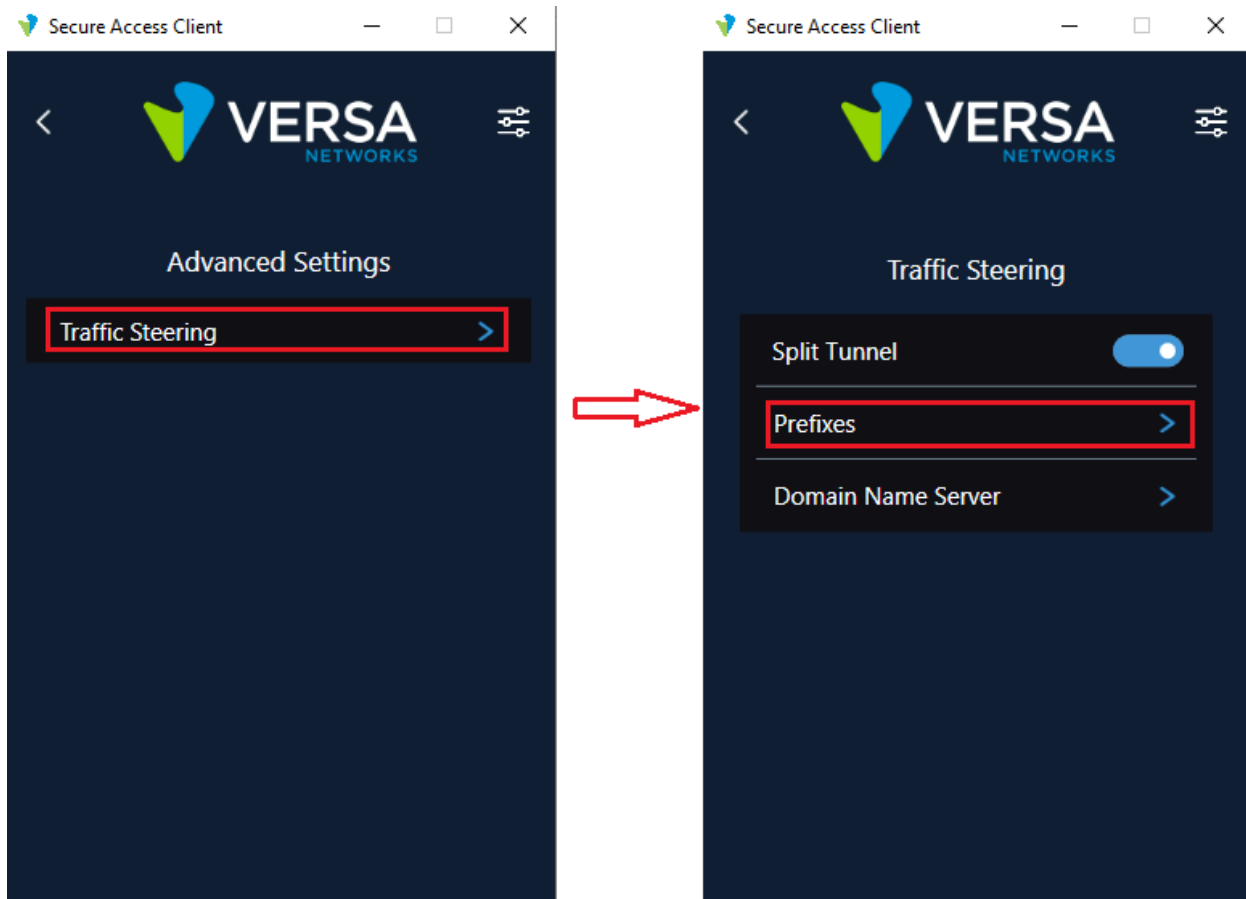


7. Click Done.

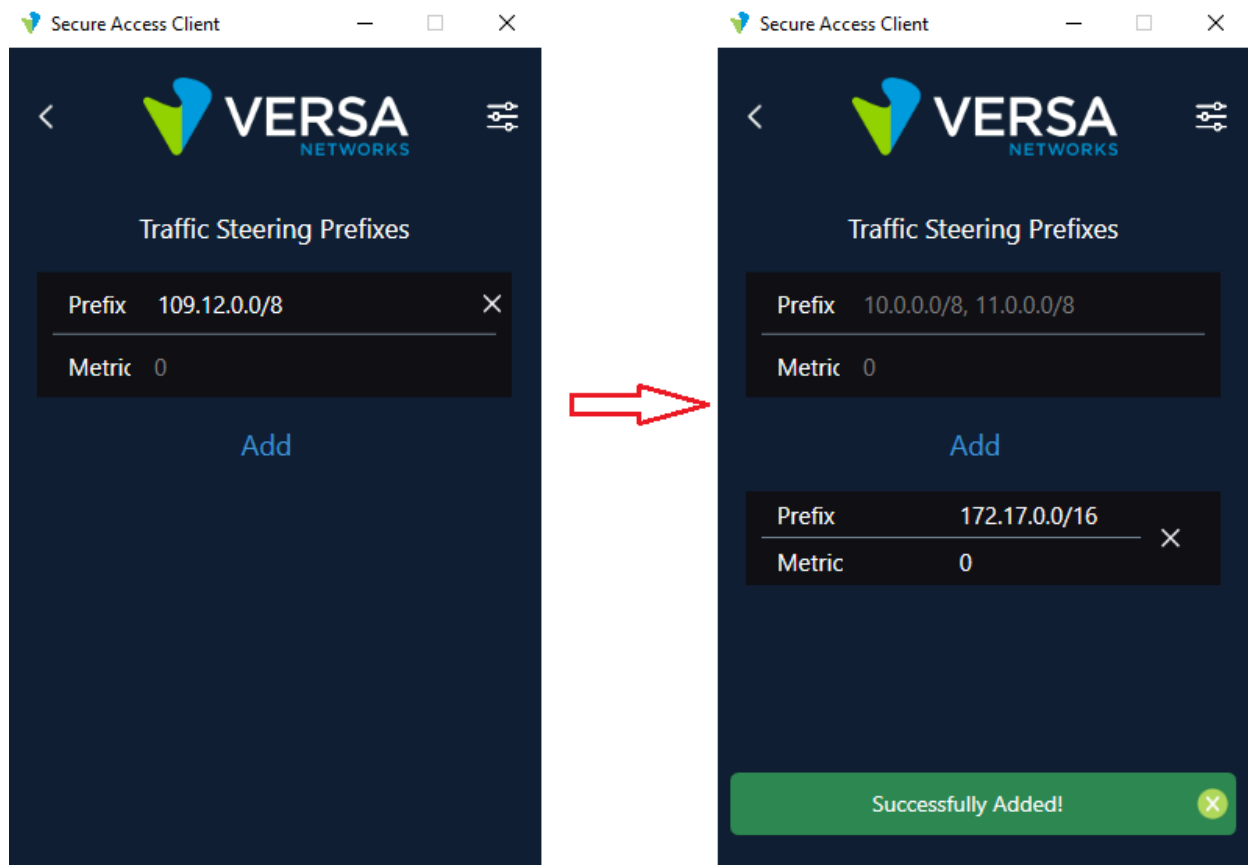
Set Prefixes and DNS Servers


To add prefixes:

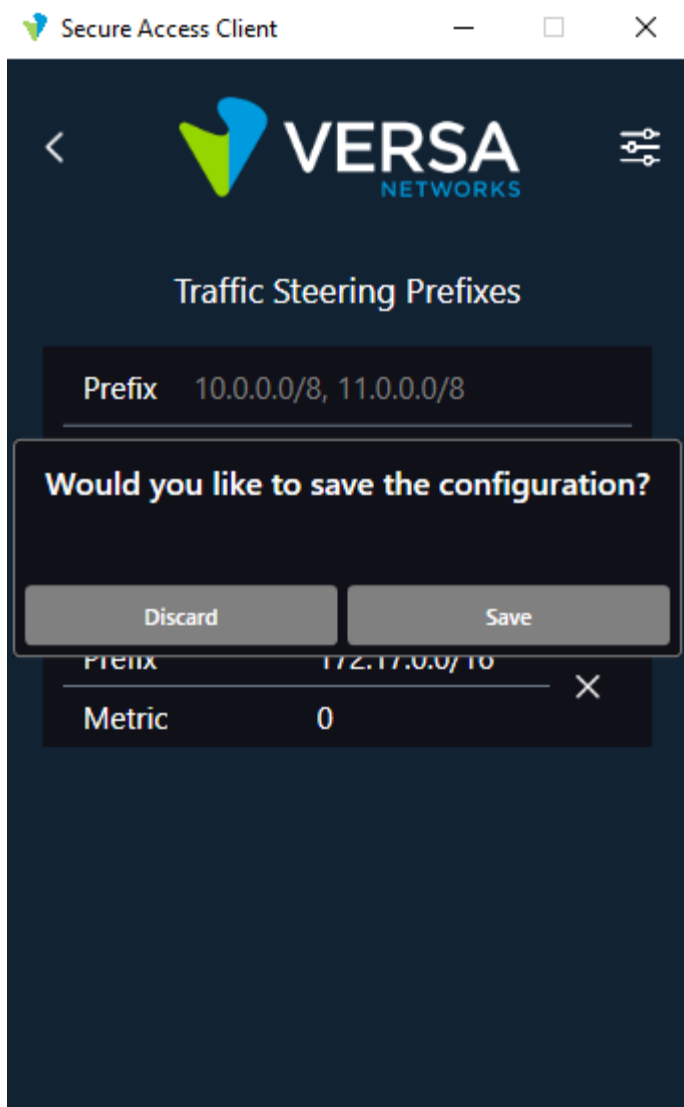
1. In the Advanced Settings screen, click Traffic Steering, and then in the Traffic Steering screen, click Prefixes.



2. In the Traffic Steering Prefixes screen, enter the prefix and metric values, and then click Add.



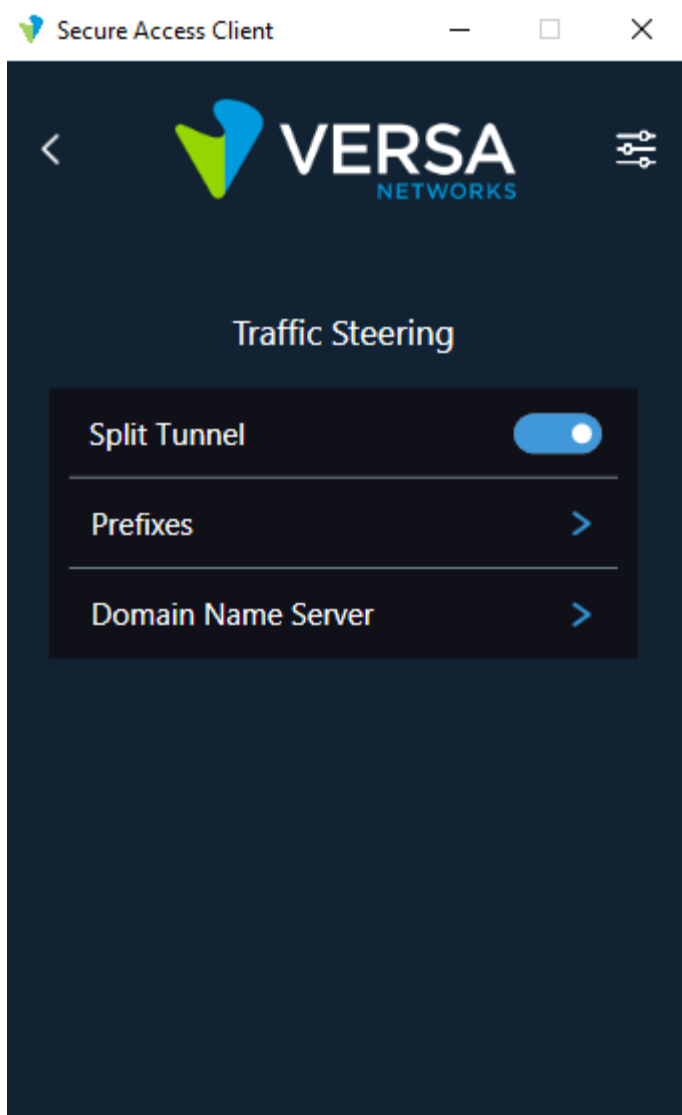
3. Click the  Back button, and save the configuration.



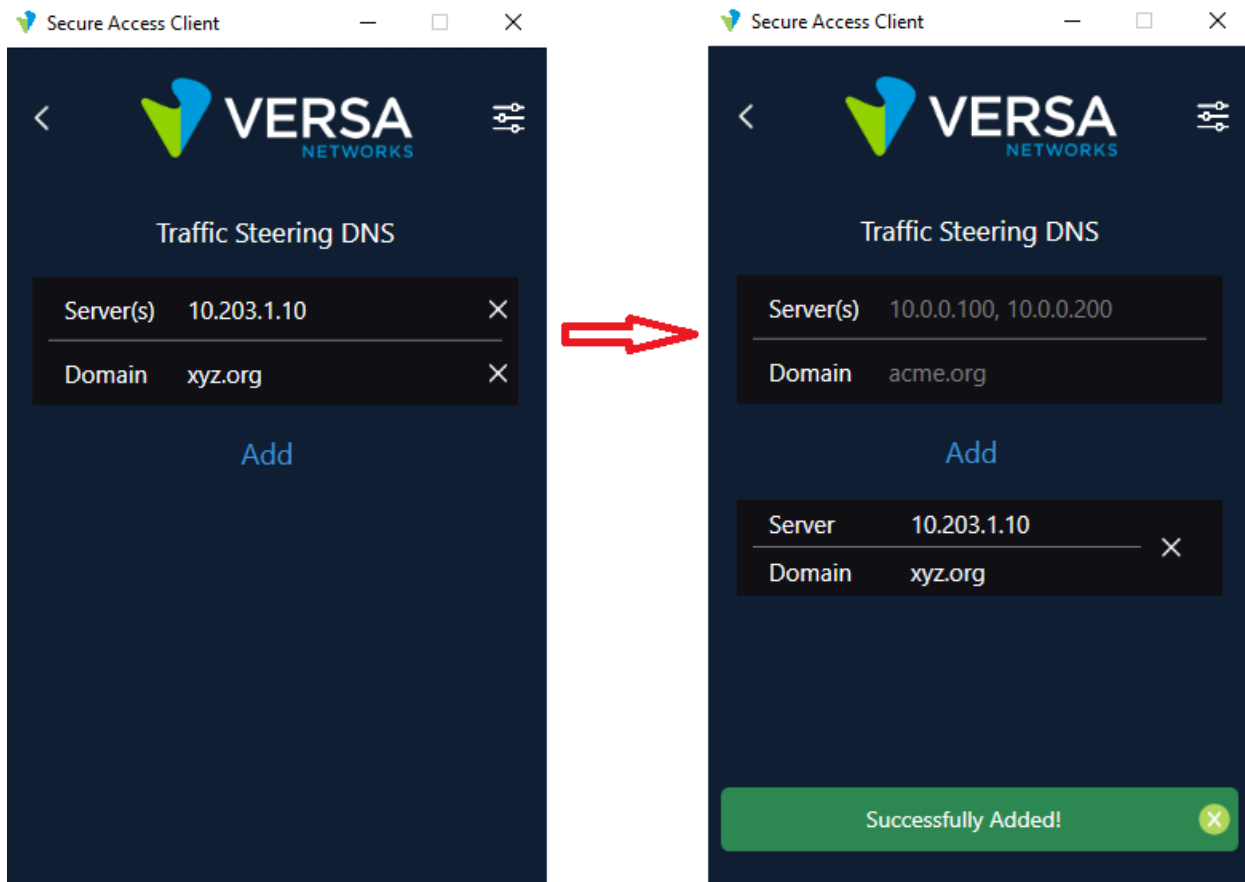
To add a DNS server:


Note that SASE Android client does not support split DNS.

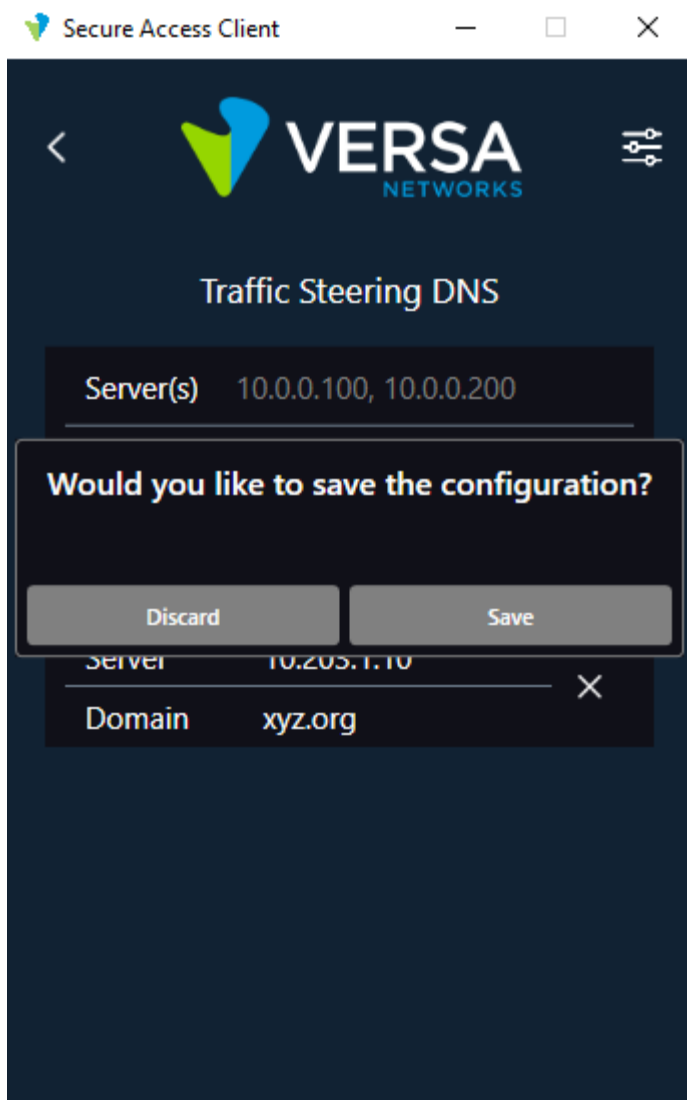
1. In the Traffic Steering screen, click Domain Name Server.



2. In the Traffic Steering DNS screen, enter the IP address of the DNS server and, optionally, the domain name, and click Add. Add additional DNS servers, as needed.



3. Click the  Back button, and save the configuration.

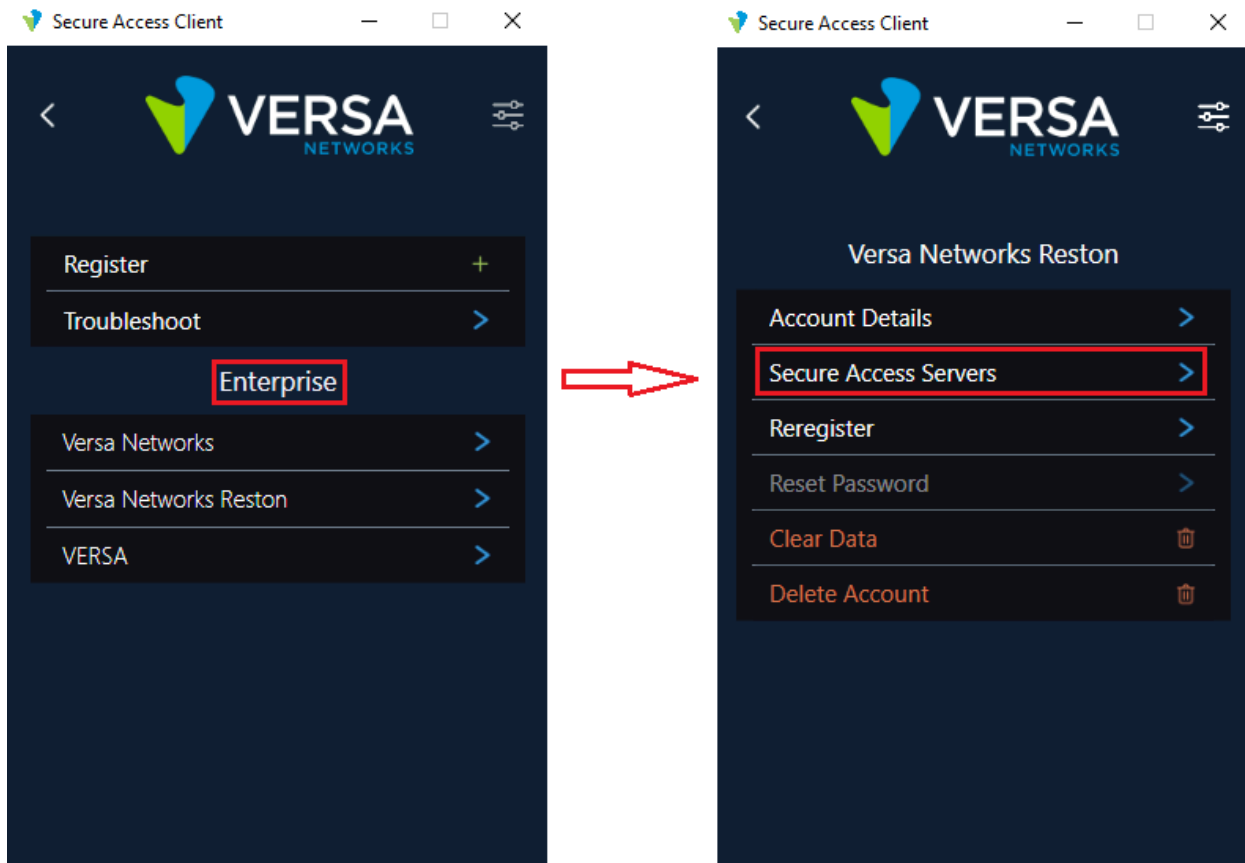


Edit a Connection

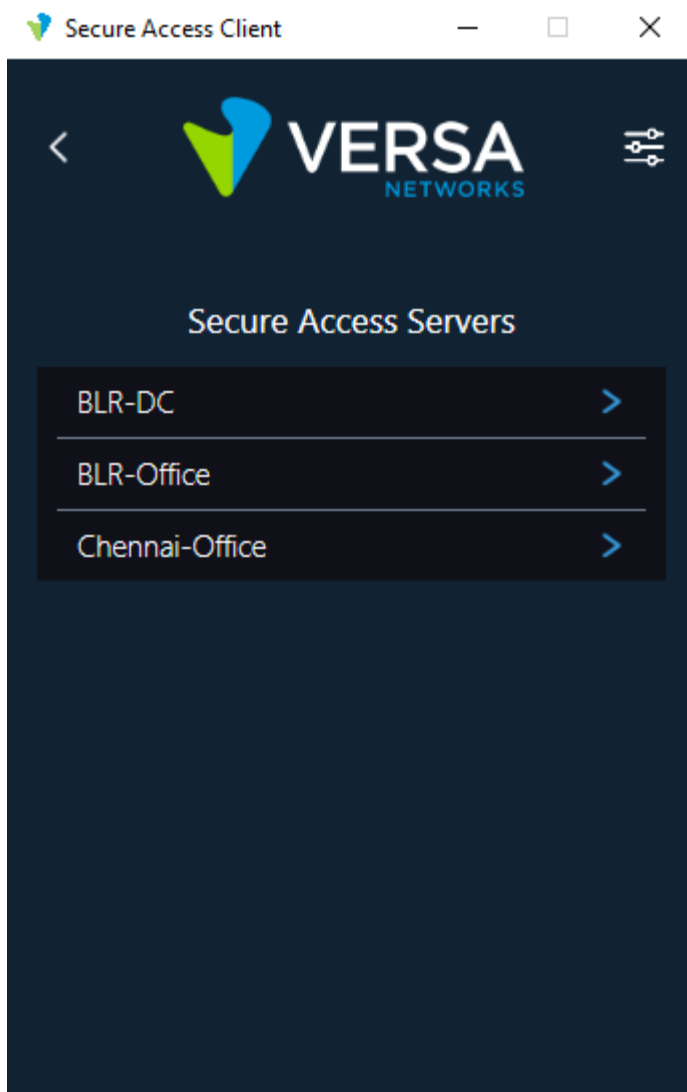
When you edit a connection to a secure access server, you can edit only the FQDN of the secure access server.

To edit a connection to the secure access server:

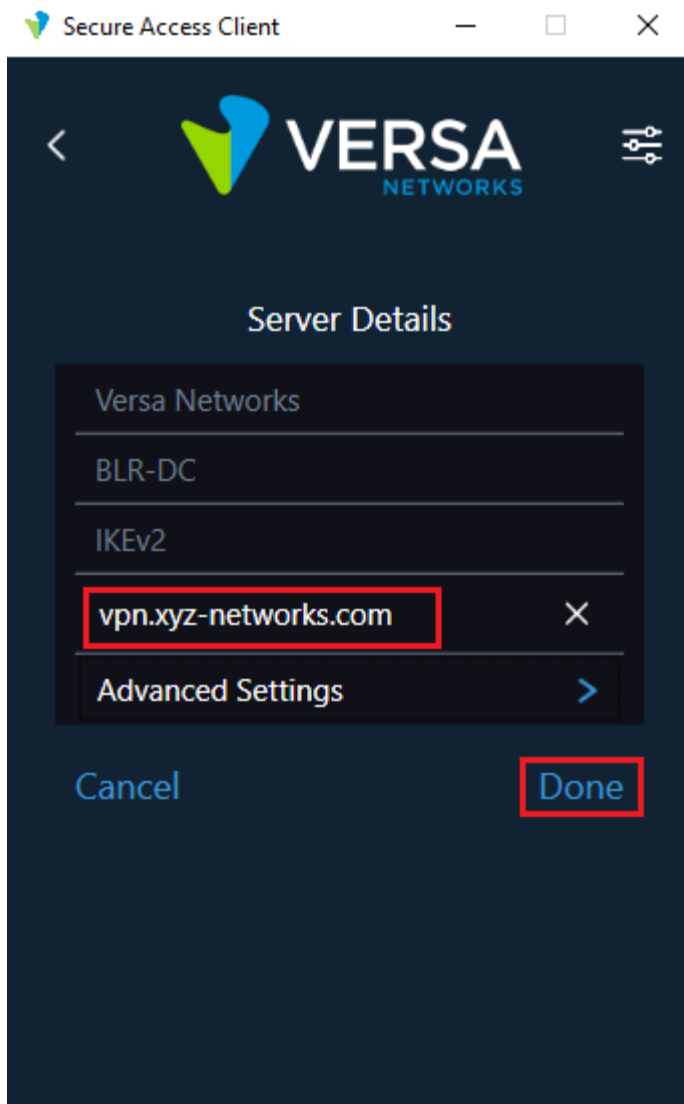
1. In the SASE client home screen, click the  Settings icon.
2. In the Enterprise section, click the enterprise name, and then click Secure Access Servers.



3. Click the secure access server connection to edit.




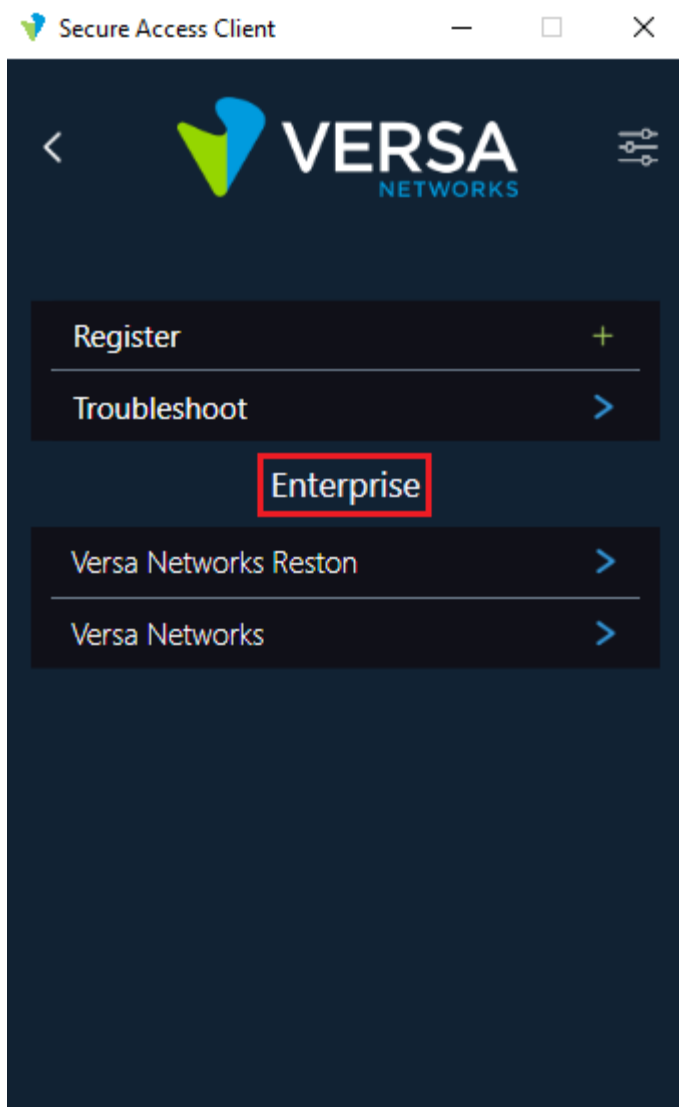
4. In the Server Details screen, edit the FQDN of the server. Other fields are disabled.



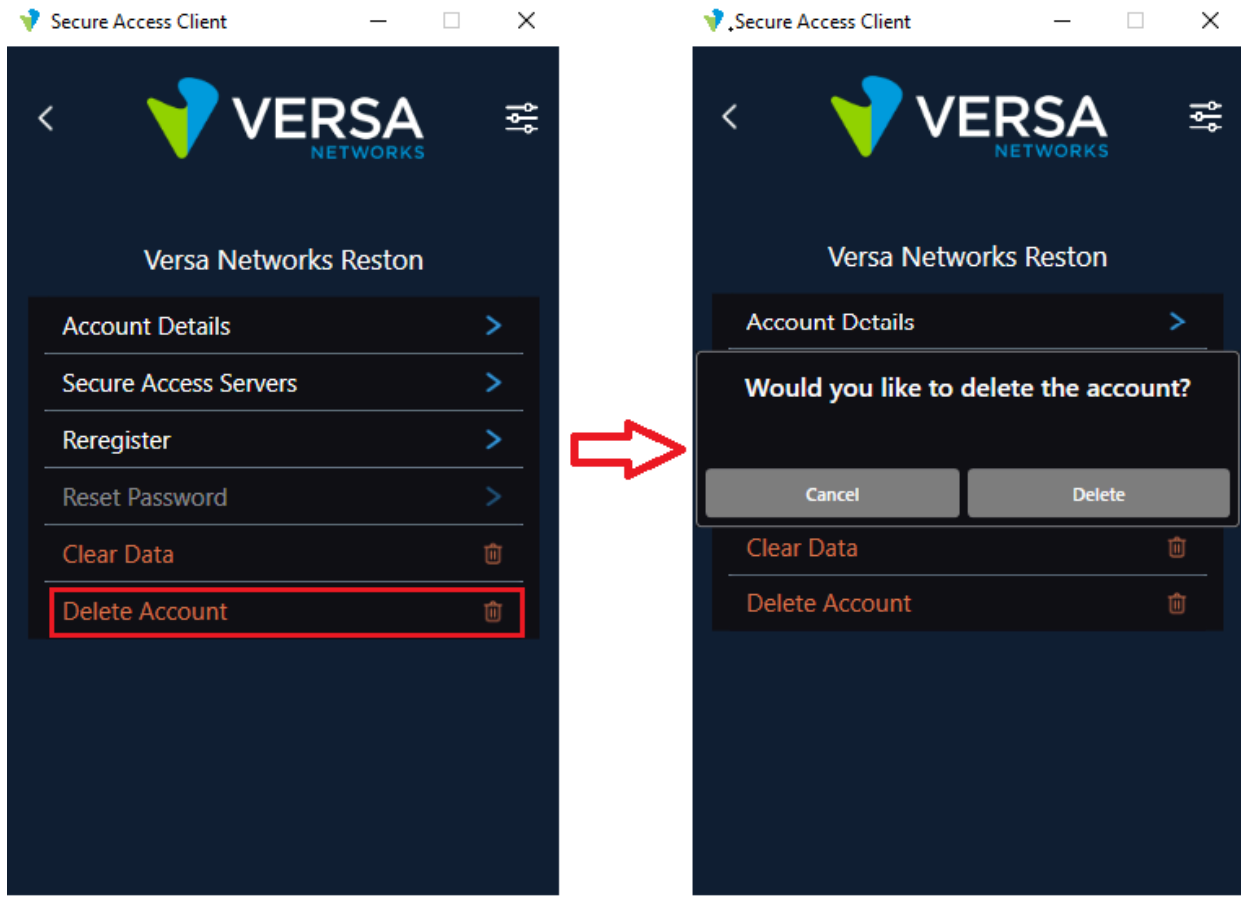
5. Click Done.

Delete an Enterprise Account

1. In the SASE client home screen, click the  Settings icon.
2. In the Enterprise section, click the enterprise name.

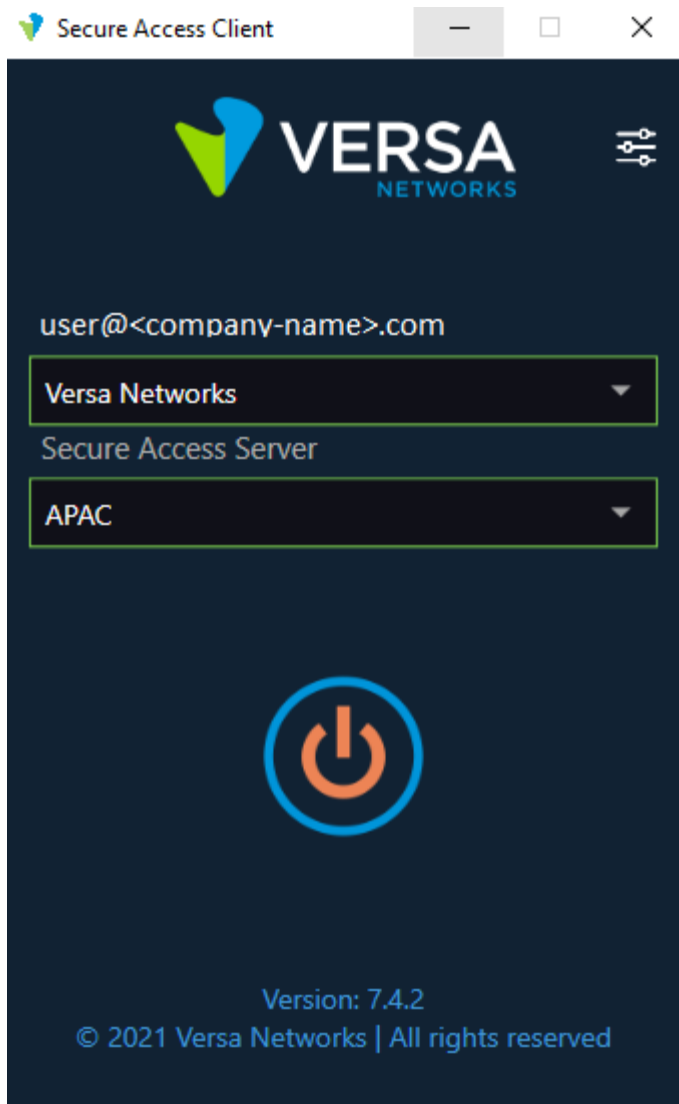


3. Click Delete Account. The connection is deleted, and the name of the connection is removed from the Secure Access Servers screen.

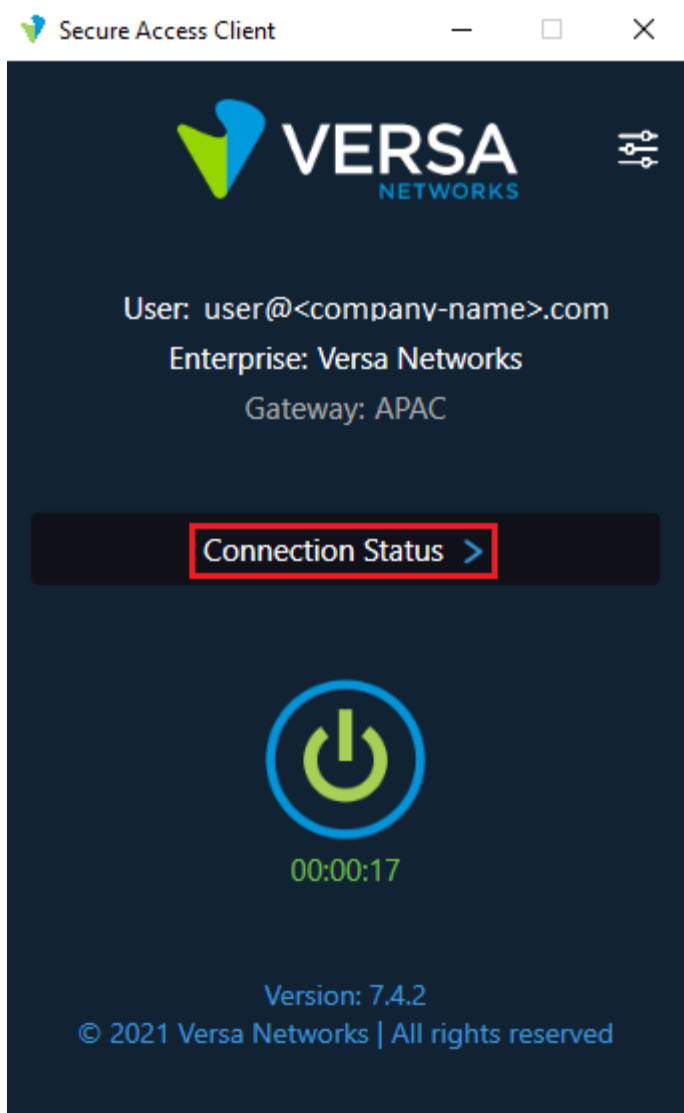



Display Connection Details

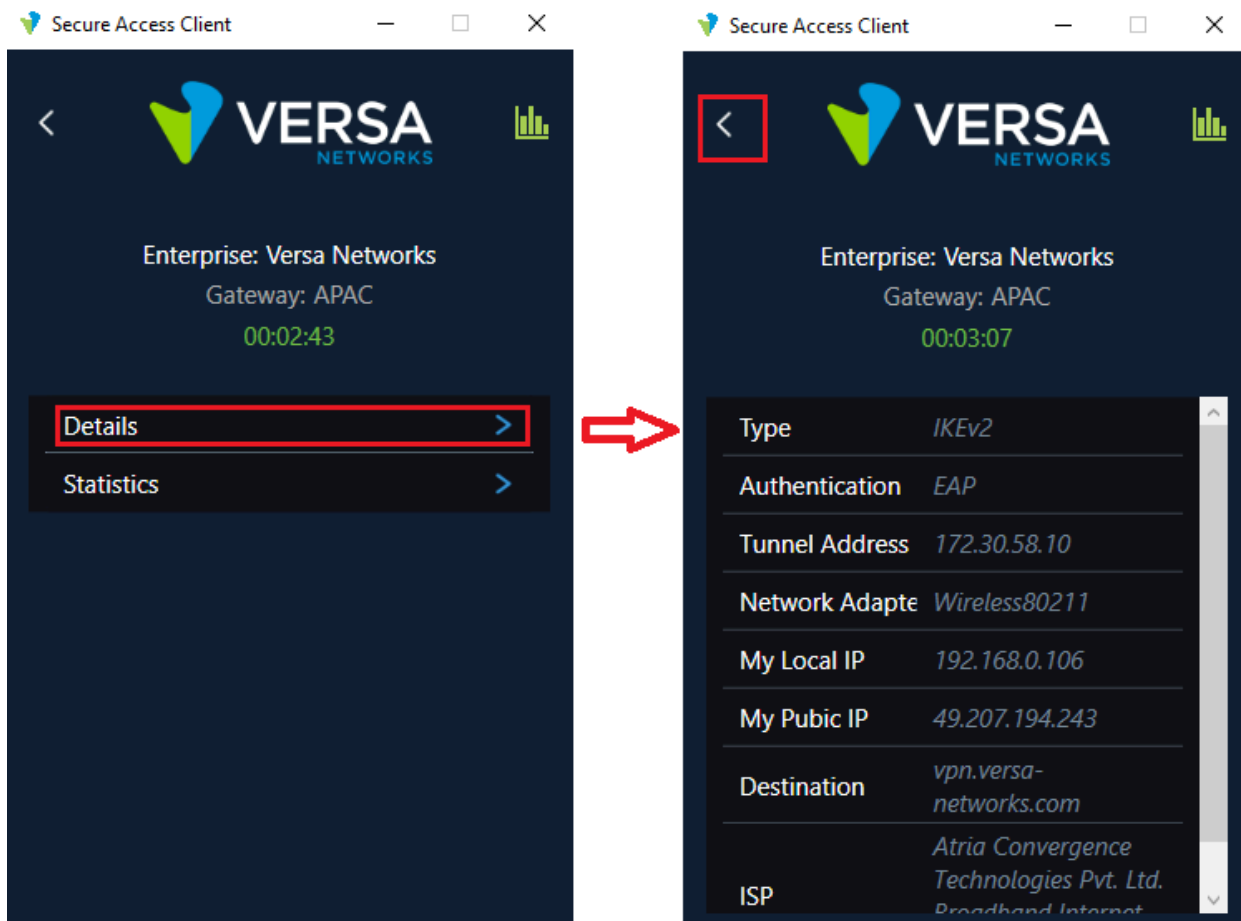
1. From the SASE client home screen, click the Power icon to connect to the server.




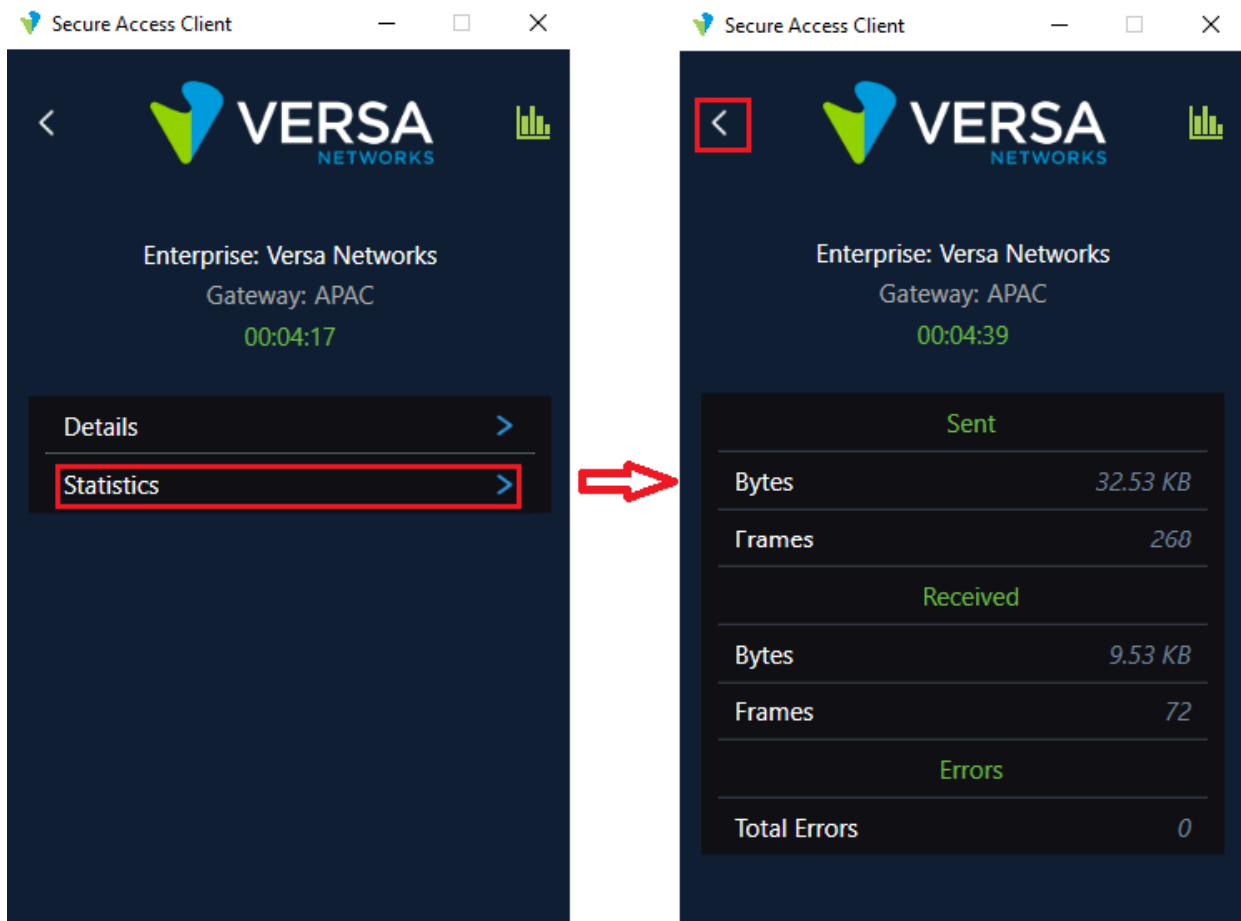
2. Click Connection Status to view configuration details about the server and to view statistics.



3. Click Details to display the server details. Click the Back  button to return to the previous screen.

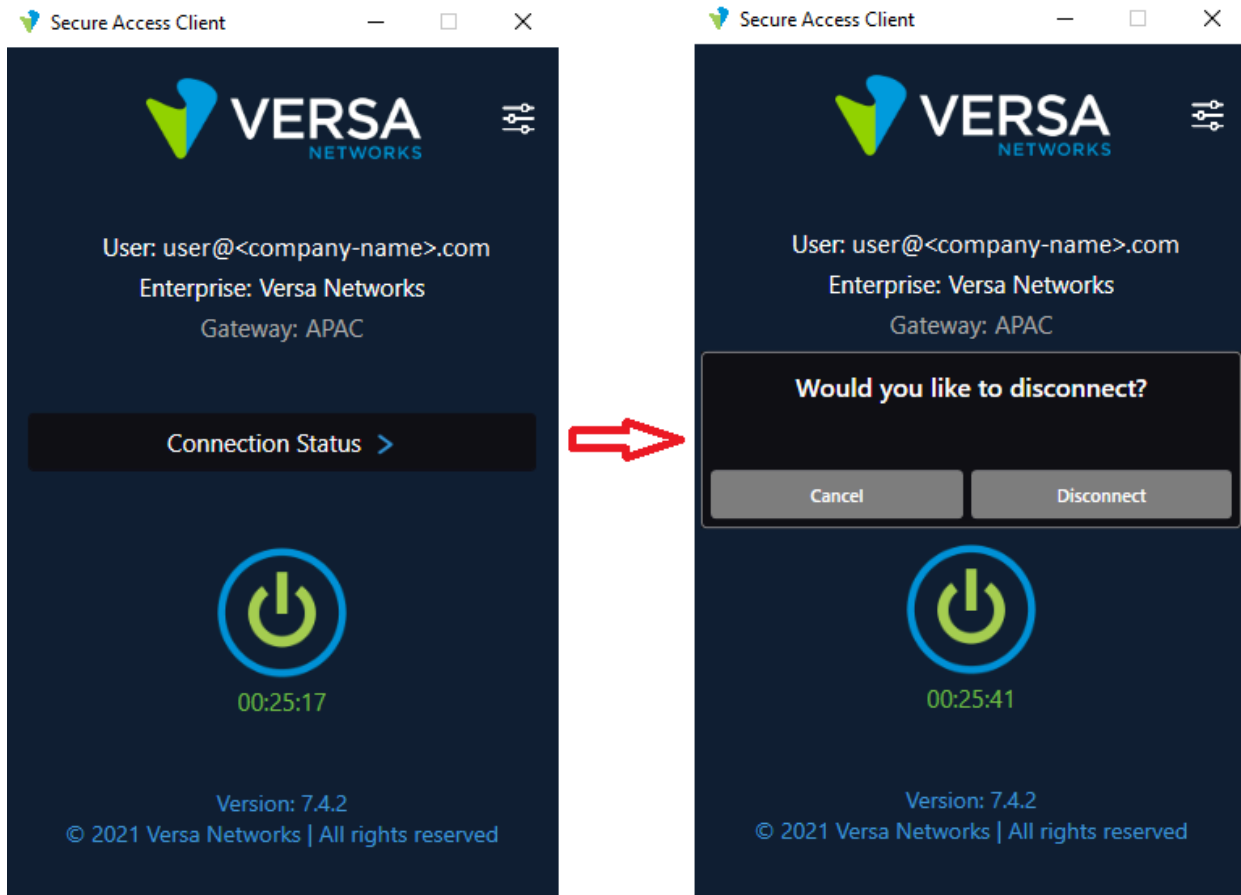


4. Click Statistics to view the server statistics. Click the  Back button to return to the previous screen.



Disconnect a SASE Client VPN Connection

1. Click the Power icon. A popup message displays asking whether you want to disconnect from the secure access server.



2. Click Disconnect to disconnect from the server and return to the client home screen.


Enable SASE Client Features

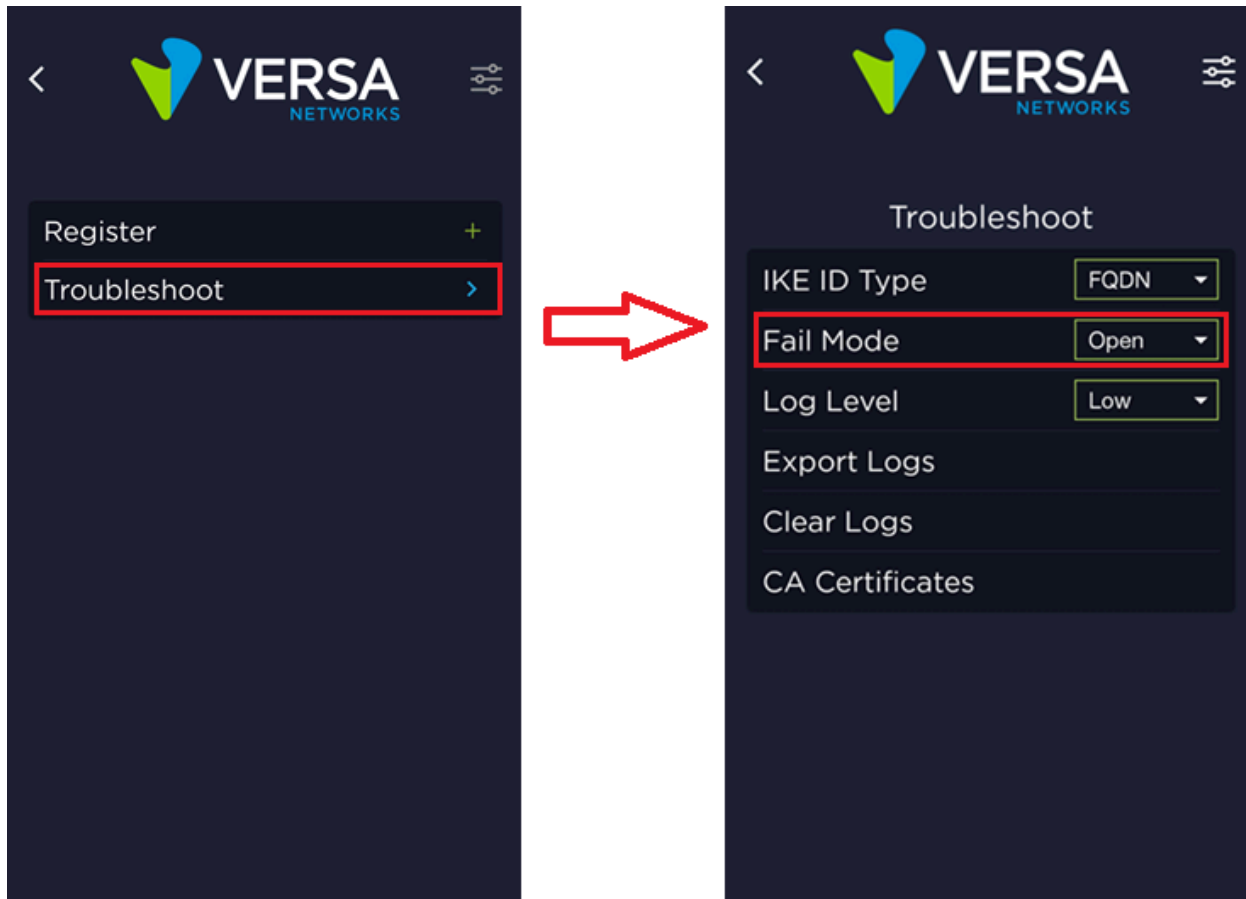
This section describes how to enable SASE client features from a Versa Director node and how to use the features.

Change Gateway Connection Fail Mode

For Android only.

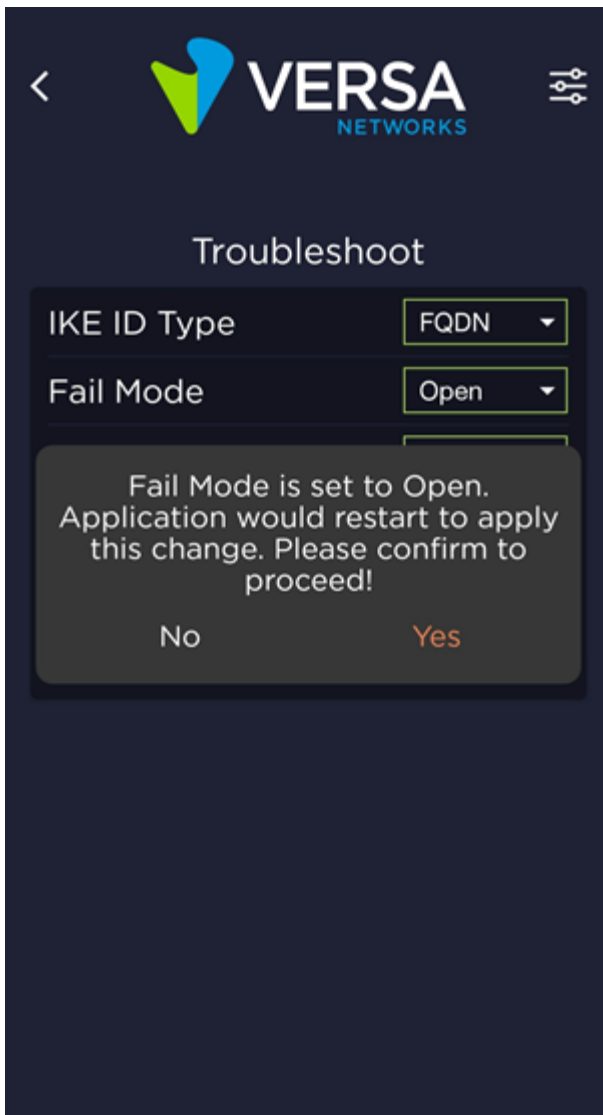
To select the action to perform when the SASE client fails to connect to a secure access gateway:

1. In the SASE client home screen, click the  Settings icon.
2. Click Troubleshoot. Then, in the Troubleshoot window, click Fail Mode.



3. Select one of the following options:

- Open (default)—If the SASE client cannot establish a connection to the gateway, the device bypasses the gateway and connects directly to internet. If the fail mode is Close and you select Open, the application restarts to apply the change. A confirmation message displays; click Yes to proceed.



- Close—If the client cannot establish a secure access connection to the gateway, all traffic is blocked and the application restarts to apply the change. A confirmation message displays; click Yes to proceed.

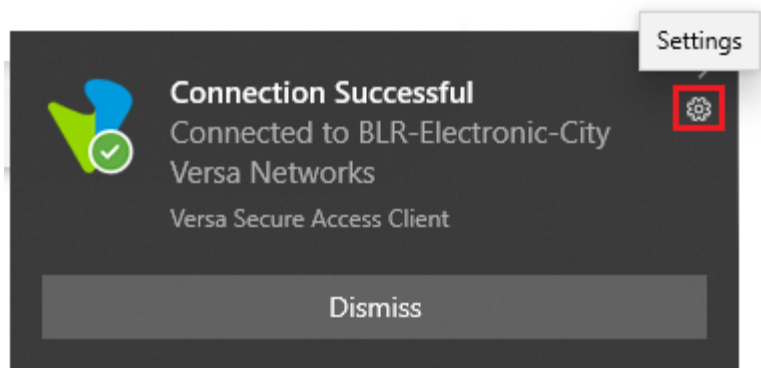


Change Notification Tray Settings

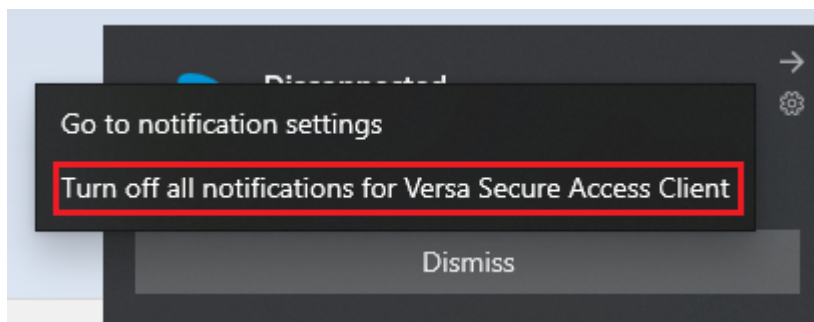
You can monitor the SASE client from the notification tray. You can turn off notifications from the SASE client and modify notification settings. Note that the steps below are for Windows OS only.

To turn off all notifications:

1. Click the Settings icon in the SASE client notification tray.

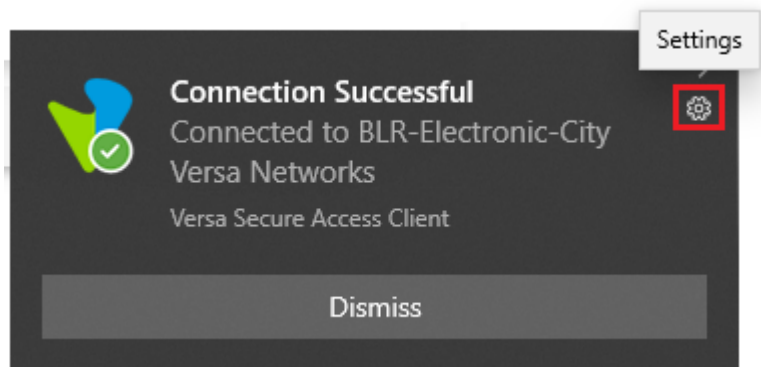


2. Click Turn Off All Notifications for Versa Secure Access Client.

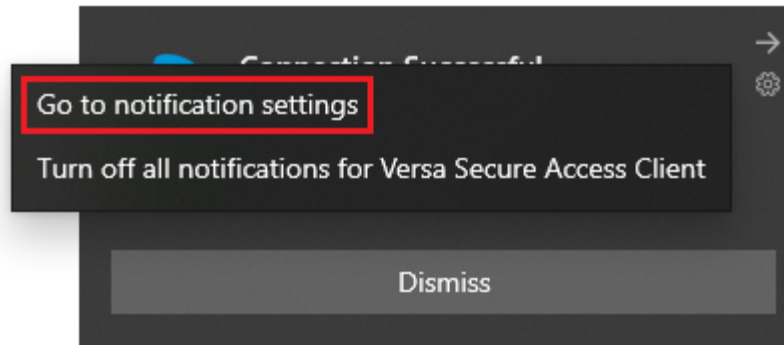


To edit notification settings:

1. Click the Settings icon in the SASE client notification tray.



2. Click Go To Notification Settings.



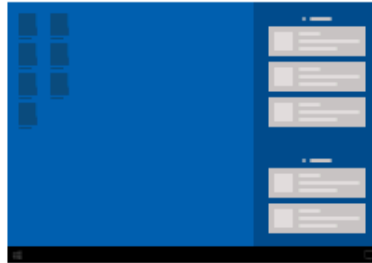
3. Change the settings as required on the Versa Secure Access Client Notification window.

Notifications

☒ On



☒ Show notification banners



☒ Show notifications in action center

Hide content when notifications are on lock screen

☐ Off

Play a sound when a notification arrives

☒ On

Number of notifications visible in action center

3

Priority of notifications in action center

☐ Top
Show at the top of action center

☐ High
Show above normal priority notifications in action center

☒ Normal
Show below high priority notifications in action center

Configure Pre-Logon

To configure pre-logon from a Versa Director node, see [Configure Pre-Logon for the Versa SASE Client](#). To view and execute pre-logon options using the CLI, see [Display and Execute Pre-Logon Options](#) below.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Director/Versa_SASE_Client/Use_the_V...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Director/Versa_SASE_Client/Use_the_V...)


Updated: Wed, 23 Oct 2024 08:43:16 GMT

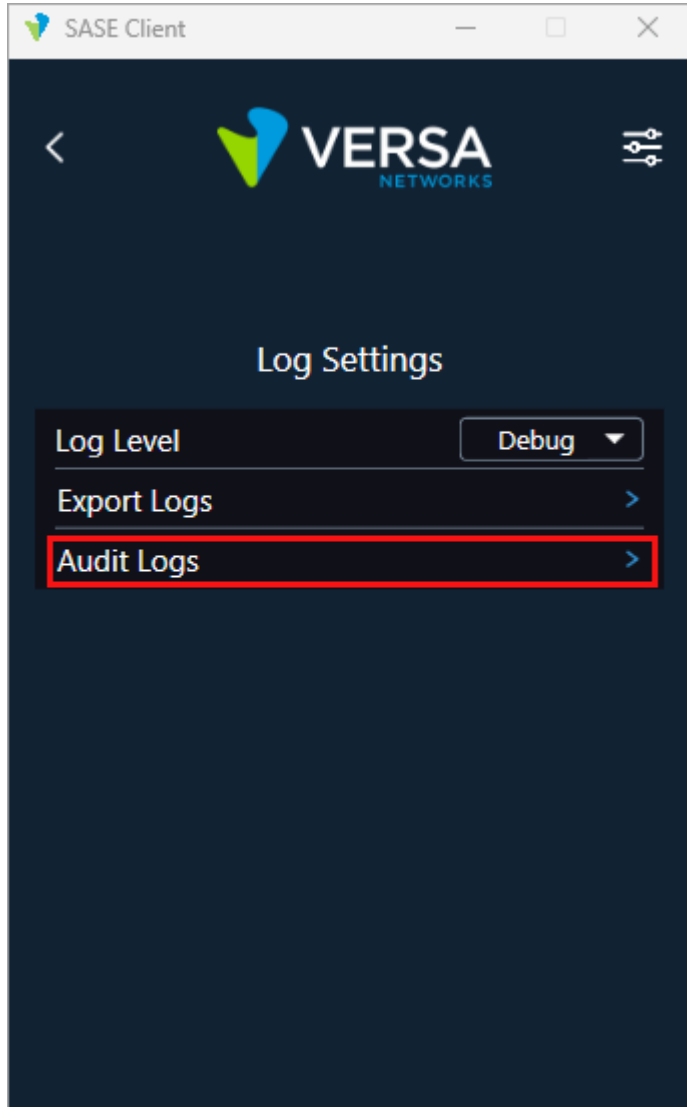
Copyright © 2024, Versa Networks, Inc.

Display Audit Logs

You display audit logs to view important client actions such as registration, VPN connection, and DEM collection status.

To display audit logs:

1. In the SASE client home screen, click the  Settings icon.
2. Click App Settings > Log Settings > Audit Logs.



The following screenshot shows a sample audit log:



Versa SASE Client Audit Logs

Level	Date and Time	Source	User	Description
Information	06-02-2024 16:27:23	EIP	NT AUTHORITY\SYSTEM	EIP data collection completed
Information	06-02-2024 16:27:12	DEM	NT AUTHORITY\SYSTEM	DEM collection completed
Information	06-02-2024 16:25:55	CLIENT	AzureAD\	VPN connection successful, Enterprise: , Profile:
Information	06-02-2024 16:25:34	CLIENT	AzureAD\	Register success. Enterprise:
Information	06-02-2024 16:23:00	SYSTRAY	AzureAD\	Auto Register Started.

Enable Always-On

To enable always-on connectivity, you enable always-on in a tenant's secure access gateway profile from the Versa Director node, and then you turn on always-on from the SASE client.

To enable always-on in a secure access gateway profile:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Templates > Device Templates in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Secure Access > Portal > Gateway Profiles in the left menu bar.
4. Click the + Add icon. The Add Profiles popup window displays.
5. Select the Client Controls tab.

Add Gateway Profiles ✕

General | IKE/IPsec | Client Controls | Traffic Steering | TLS | DTLS

Logo URL Change Password URL

☐ Add Custom Gateway
 ☒ **Edit Gateway**
☒ Display Gateway
 ☐ Multi-Tenancy
 ☒ Remember Credential
 ☐ Tamper Protection

☐ Register With DNS
 ☒ IP Stickiness
 ☐ Auto Update
 ☐ TWAMP
 ☒ IPv6
 ☐ Strict Tunnel Mode

☐ Auto Disconnect

Portal Lifetime(mins)
 Maximum Number of Gateway
 Password Expiry Warn Before
 Register DNS Suffix

Certificate Issuer
 Latency Bias
 Posture Check Interval(mins)
 Trusted Network Hostname

SLA Profile
 Tamper Protection Override Key
 Auto Disconnect Interval(mins)

Metric Reporting | Reconnect | Tunnel Monitoring | Always Connected | Cellular Network | PAC File | Data Exfiltration

☒ **Always Connected**

Disconnect

Disconnect Interval(secs)


Fail Mode

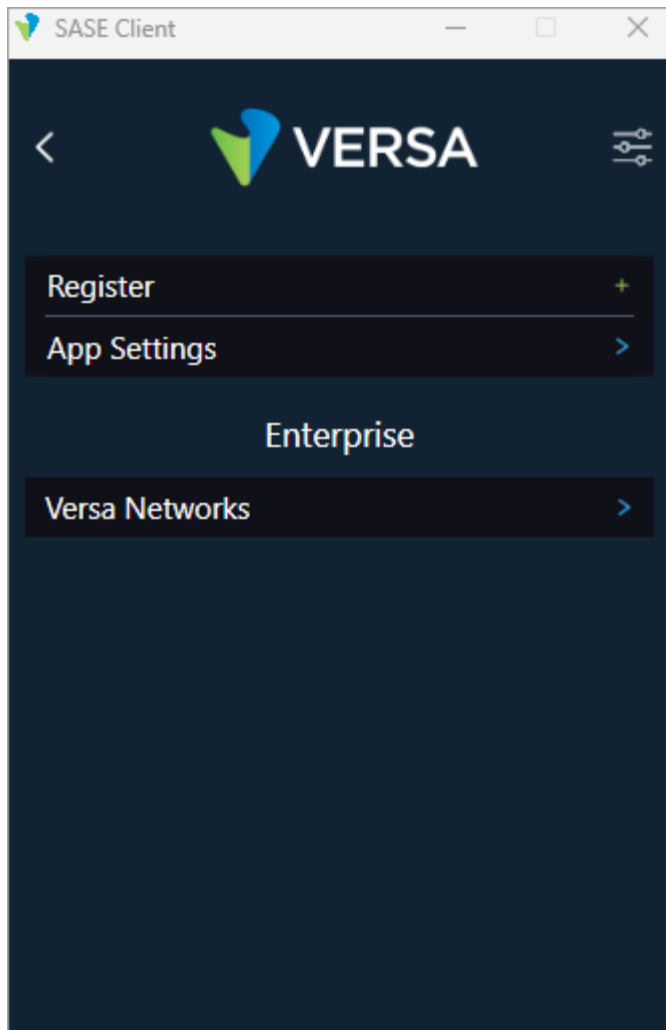
☒ **Override**

Override Interval(secs)

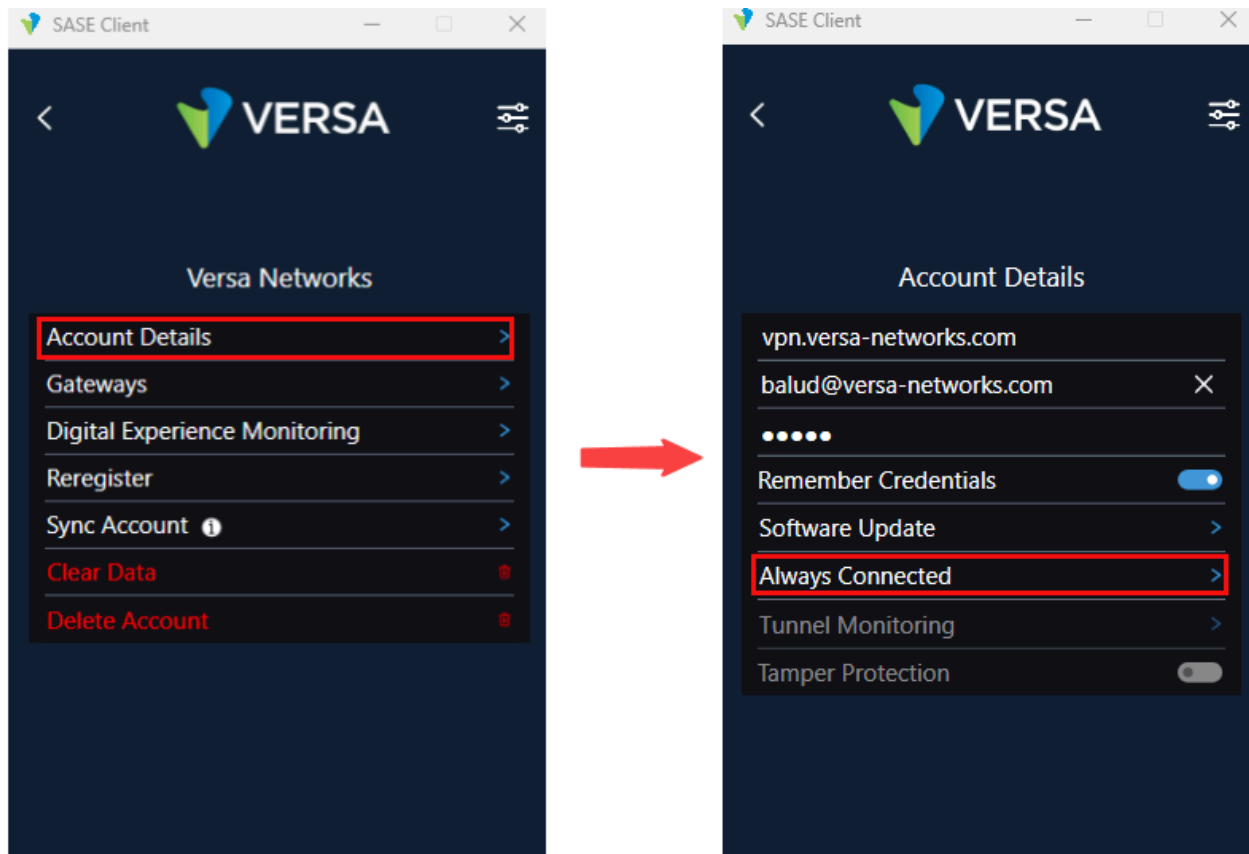
6. Click Edit Gateway to allow SASE client users to edit a gateway.
7. Select the Always Connected tab and click Always Connected so that the VPN connection for the secure access client is always on.
8. For information about configuring other fields in the Add Profiles popup window, see Configure Secure Access Gateway Profiles in [Configure the Versa Secure Access Service](#).
9. Click OK.

To enable always-on connectivity for the SASE client:

1. In the SASE client home screen, click the  Settings icon.
2. In the Enterprise section, click the account for which to enable an always-on connection.




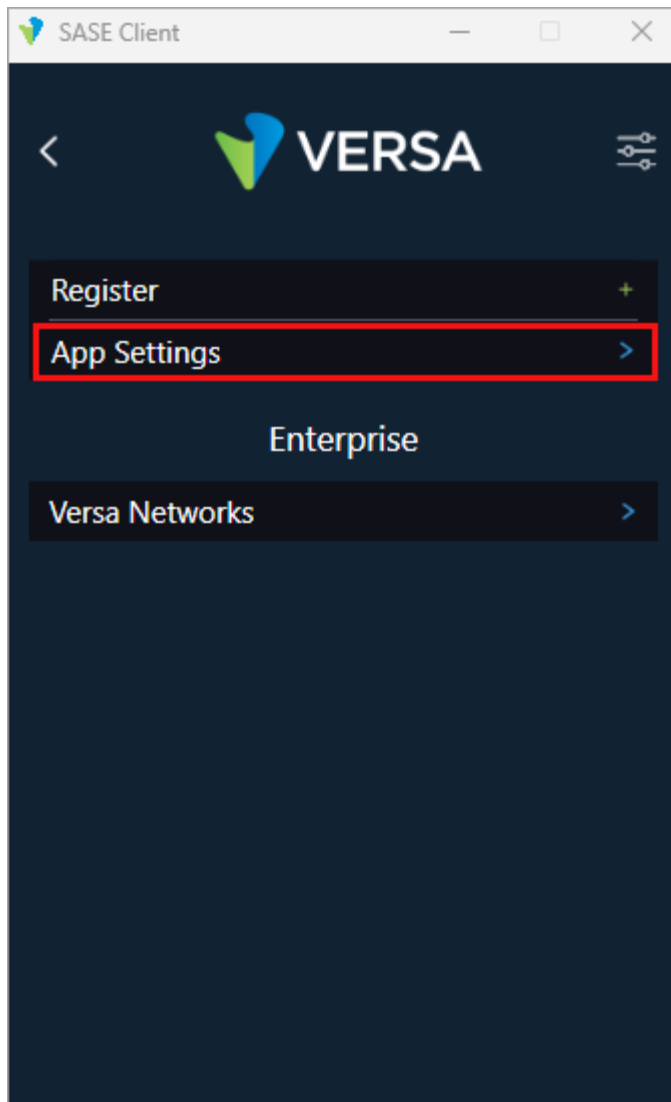
3. Click Account Details, and then click the Always On toggle button. When you enable always-on, the toggle button color changes from gray to blue. To disable always-on, click the toggle button a second time.



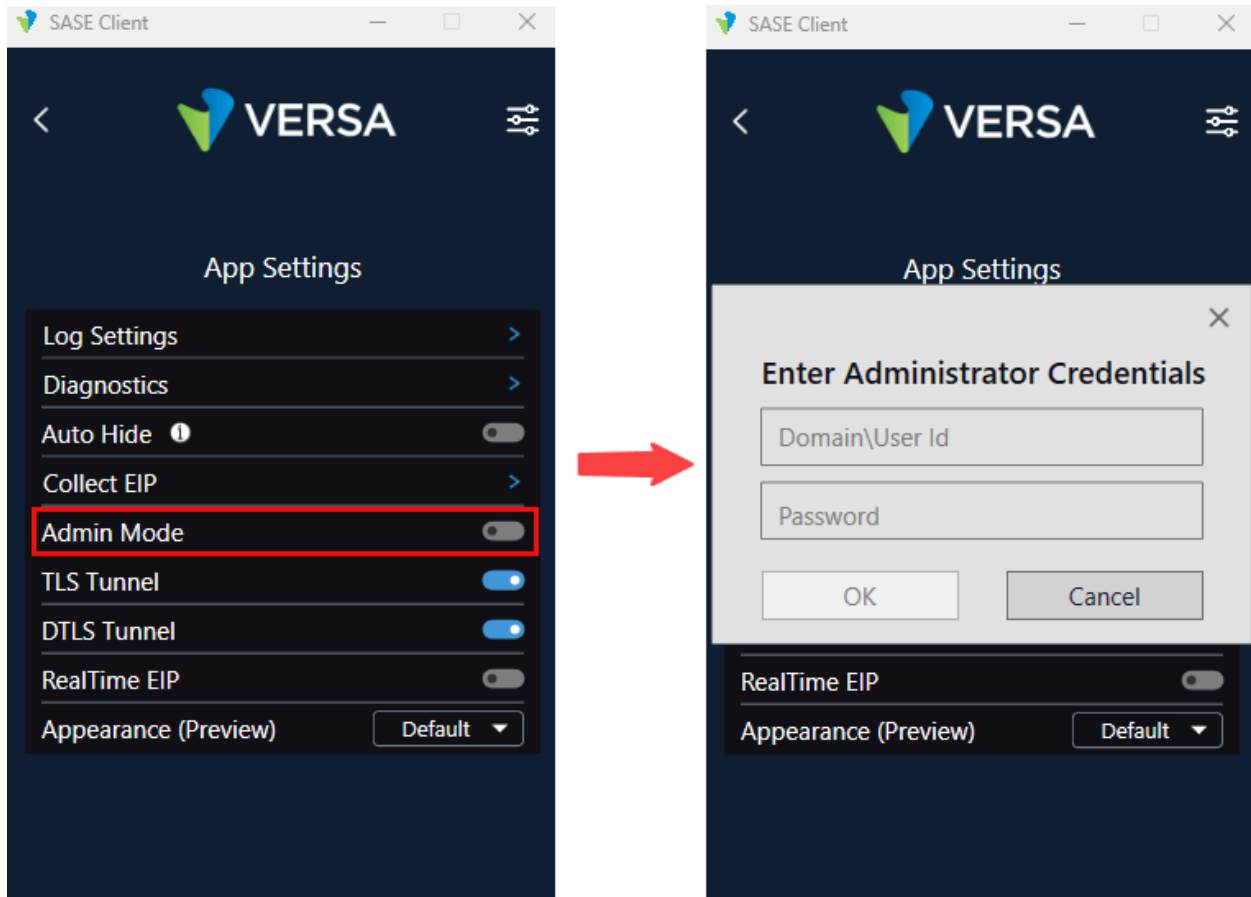
If always-on is not enabled for the secure access gateway profile, you can enable it from the SASE client if Edit Gateway is enabled for the gateway profile and if you have administrator privileges for your device. Note that always-on is the only feature not enabled in the portal that you can enable using administrator credentials.

To enable always-on connectivity from the SASE client:

1. In the SASE client home screen, click the  Settings icon.
2. Click App Settings.

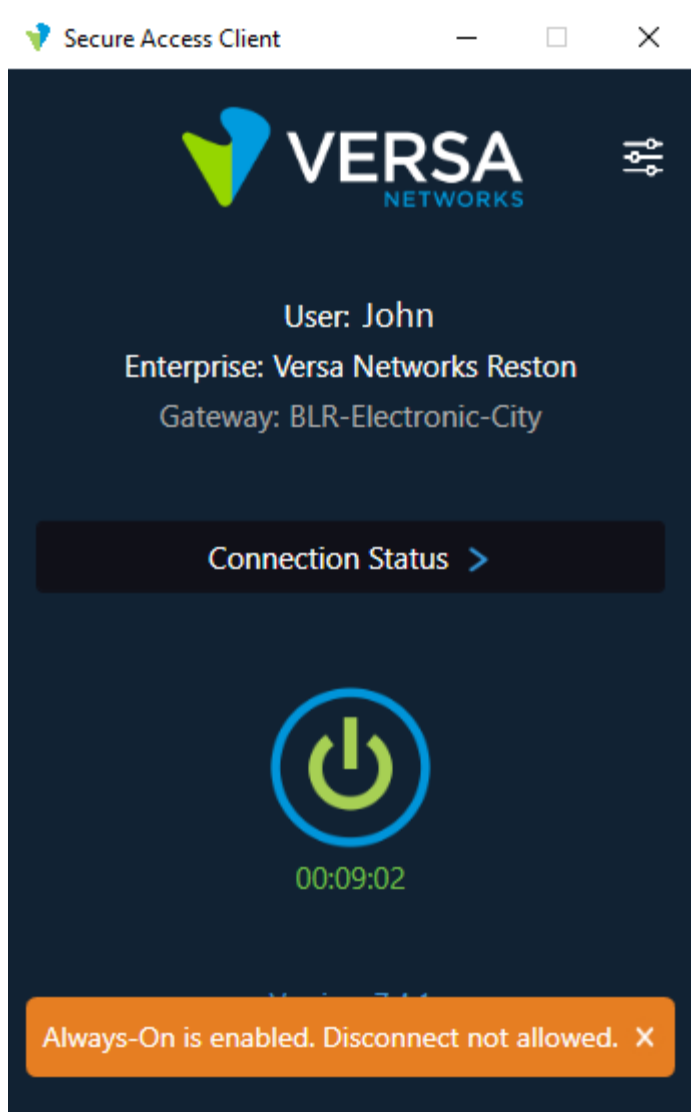


3. In the App Settings screen, click the Admin Mode toggle button, and then enter the administrator username and password.



4. Click OK.
5. Follow Steps 1 through 4 in the previous procedure to enable always-on connectivity for the client.

When always-on is enabled, if the user tries to disconnect the SASE client, a message is displayed that disconnection is not allowed. For example:



Enable an Application-Based Split Tunnel

You configure application-based split tunnels so that you can exclude certain application traffic from the tunnel so that the traffic can be sent directly to the destination from the end device. To enable application-based split tunnels, you configure a secure access gateway profile from the Versa Director node. If you enable split tunnel in the gateway profile associated with a SASE client, the Split Tunnel toggle button in the SASE client is enabled by default. Otherwise, the Split Tunnel toggle button in the client is disabled.

To enable split tunnel in a secure access gateway profile:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Templates > Device Templates in the horizontal menu bar.
 - c. Select an organization in the left menu bar.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Director/Versa_SASE_Client/Use_the_V...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Director/Versa_SASE_Client/Use_the_V...)

Updated: Wed, 23 Oct 2024 08:43:16 GMT

Copyright © 2024, Versa Networks, Inc.

- d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Secure Access > Portal > Gateway Profiles in the left menu bar.
4. Click the + Add icon. The Add Gateway Profiles popup window displays.
5. Select the Traffic Steering tab.


6. Click Split Tunnel to enable split tunneling.
7. Select the SASE client tab.

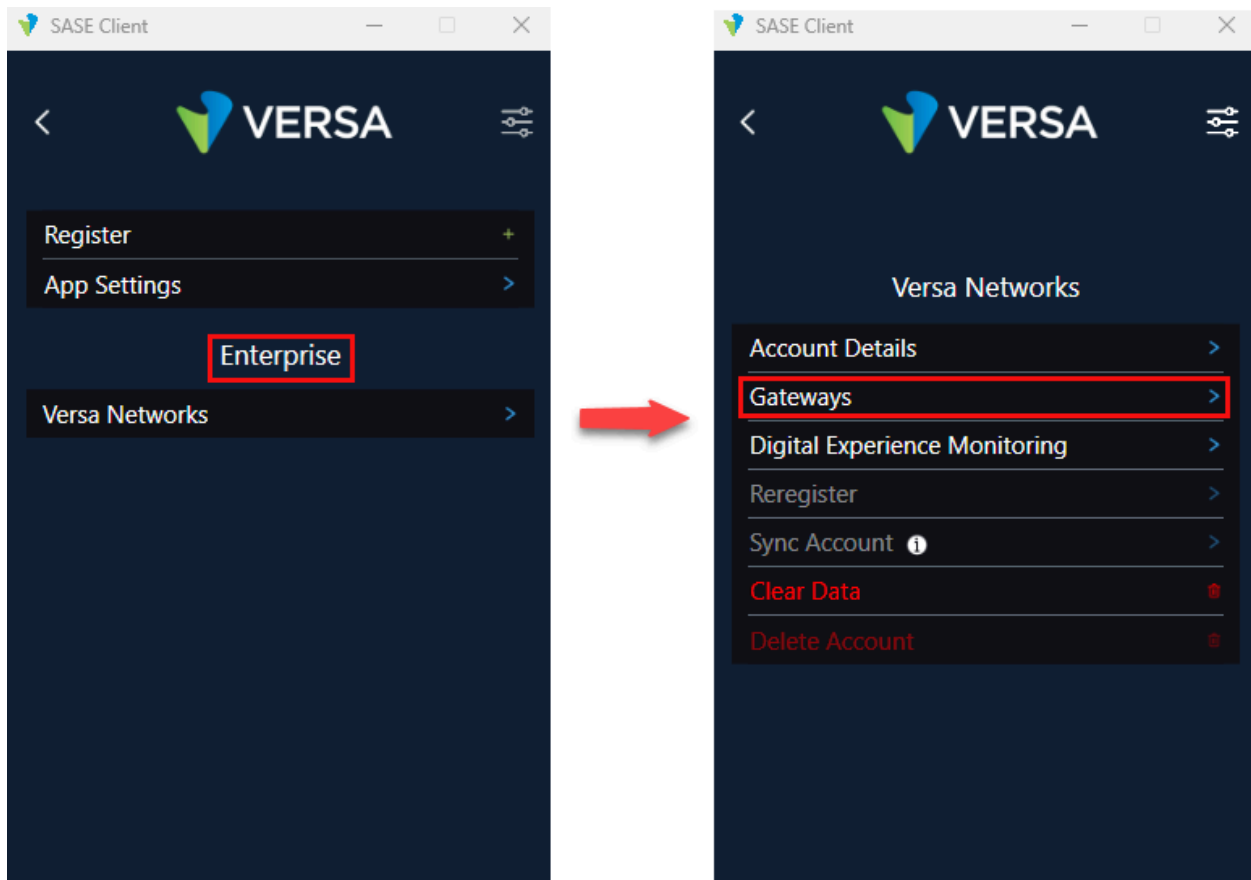
8. Select the applications and domains whose traffic you do or do not want to send to the client.
9. For information about configuring other fields on the Add Gateway Profiles popup window, see Configure Secure Access Gateway Profiles in [Configure the Versa Secure Access Service](#). Click OK.

Note that to enable or disable change split tunnel from the SASE client, you must enable split tunnel for the associated

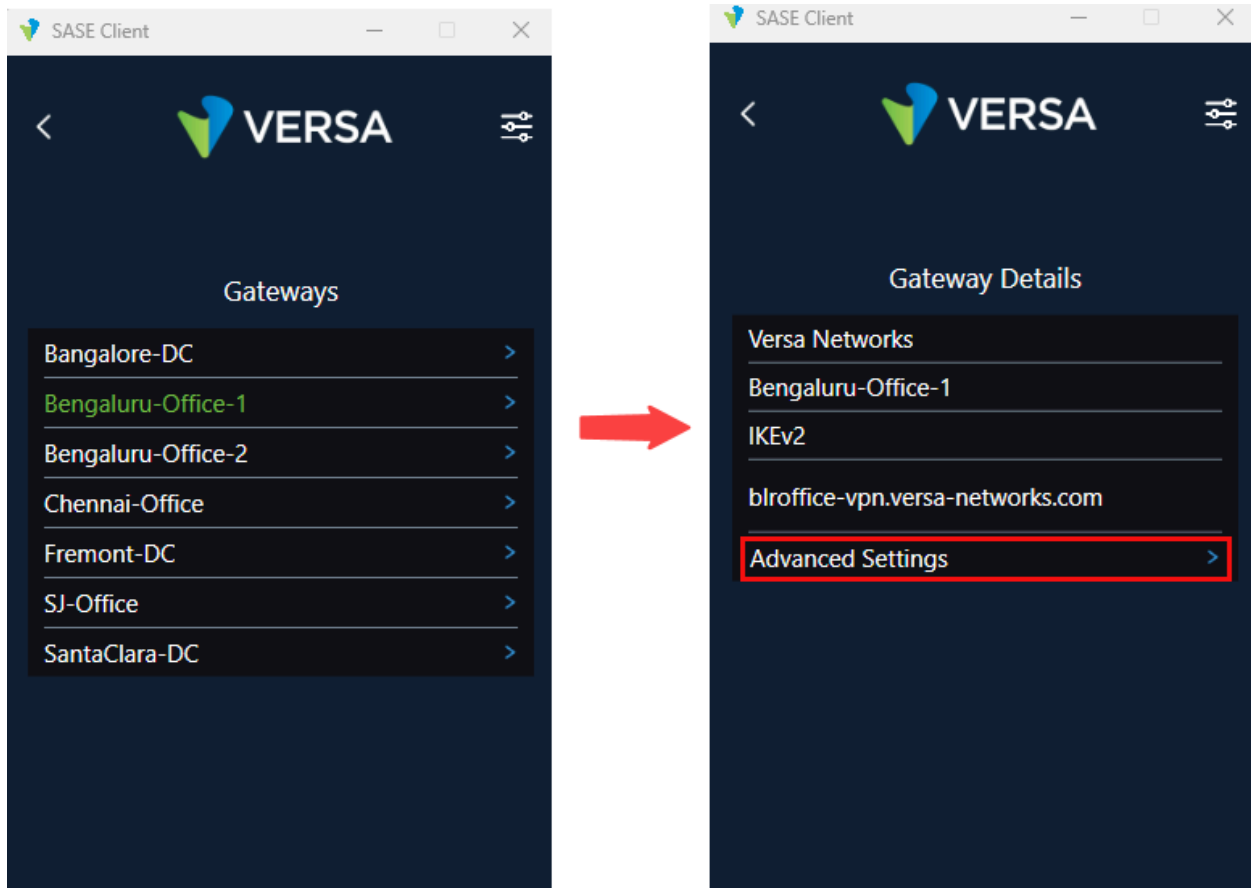
secure access profile. Otherwise, split tunnel is disabled for users on the SASE client.

To change the split tunnel setting from the SASE client:

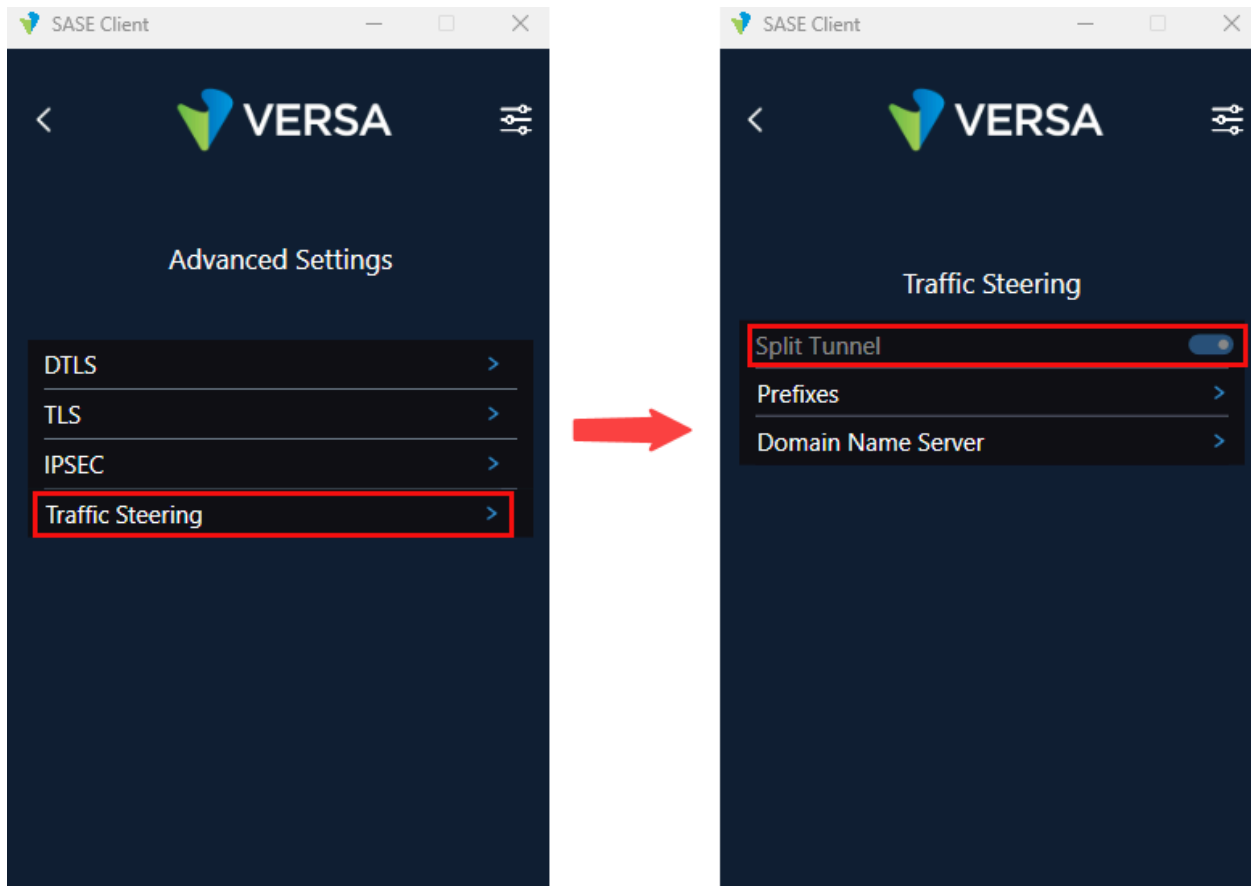
1. In the SASE client home screen, click the  Settings icon.
2. In the Enterprise section, click the account, and then click Gateways.




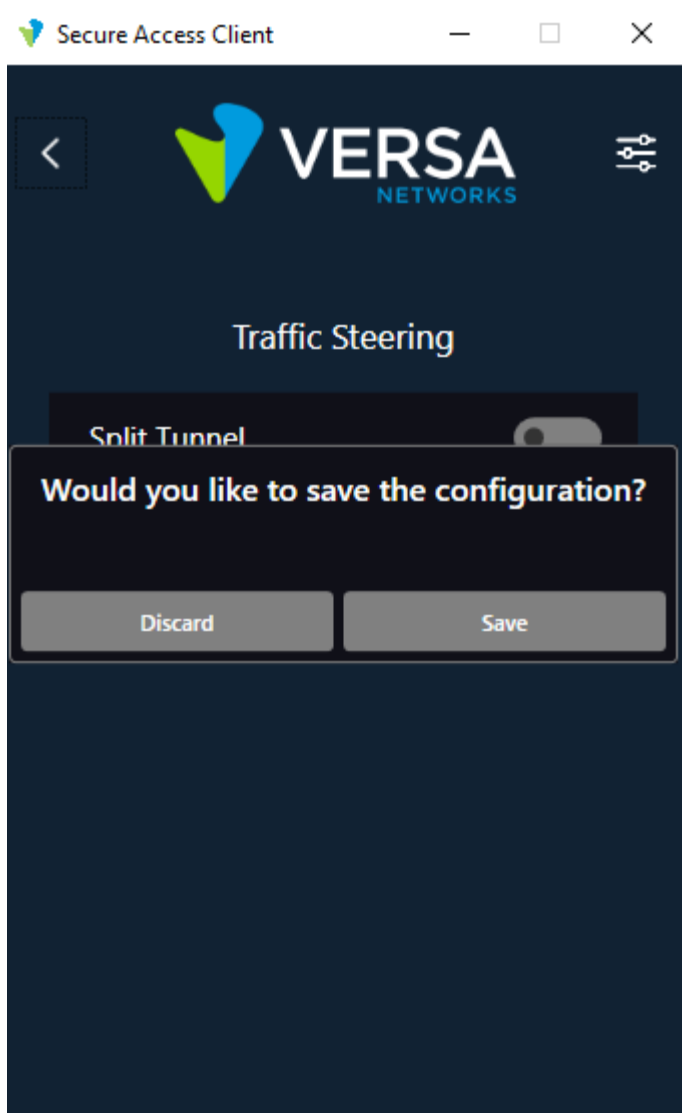
3. Click the gateway, and then in the Gateway Details screen, click Advance Settings.



4. In the Advanced Settings screen, click Traffic Steering, and then in the Traffic Steering screen, click the Split Tunnel toggle button. When you enable split tunnel, the toggle button color changes from gray to blue. To disable split tunnel, click the toggle button a second time.



5. Click the  Back button to save the changes.



Enable Authentication

VSA provides user and two-factor authentication.

For user authentication, you can use LDAP or SAML.

You enable LDAP authentication from a Versa Director node. For more information, see [Configure a Gateway To Use an LDAP Server for User Authentication](#).

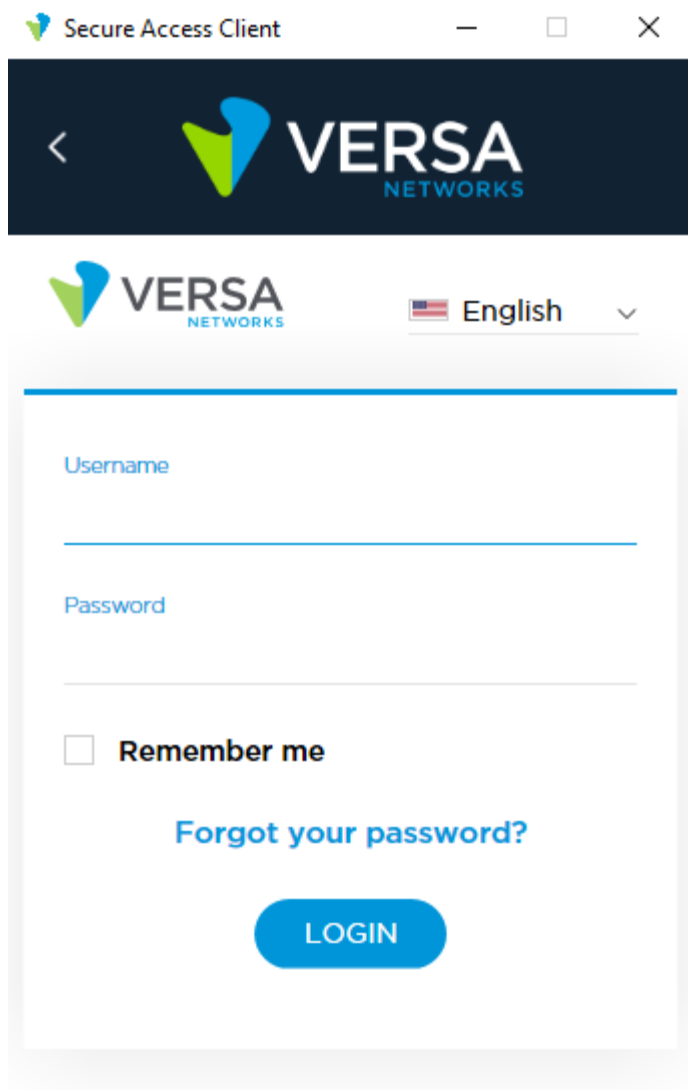
You enable SAML authentication from a Versa Director node. For more information, see [Enable SAML Authentication](#).

There are no SASE client settings for user authentication. For SAML authentication, the displayed client login page is similar to the following:

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Director/Versa_SASE_Client/Use_the_V...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Director/Versa_SASE_Client/Use_the_V...)

Updated: Wed, 23 Oct 2024 08:43:16 GMT

Copyright © 2024, Versa Networks, Inc.



For two-factor authentication, you can use SMS or email-based OTP or you can use TOTP.

To enable SMS or email-based OTP for client registration and login, see [Configure SMTP Server Settings](#) and [Configure an Authenticator Profile](#).

You enable TOTP from a Versa Director node. For more information, see [Enable Time-Based One-Time Password in Configure the Versa Secure Access Service](#).

There are no SASE client settings for two-factor authentication. For information about registering and logging in to the SASE client for SMS or email-based OTP and TOTP, see [Register with the Versa Secure Access Portal](#), above.

Enable Cookies

To enable cookies in the SASE client, you configure an authentication profile with caching mode enabled for cookies,

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Director/Versa_SASE_Client/Use_the_V...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Director/Versa_SASE_Client/Use_the_V...)

Updated: Wed, 23 Oct 2024 08:43:16 GMT

Copyright © 2024, Versa Networks, Inc.

and then you associate the authentication profile with the gateway and portal for the SASE client.

To configure an authentication profile with cookies enabled:

1. In Director view:
 - a. Select the Administration tab in the top menu bar.
 - b. Select Appliances in the left menu bar.
 - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Object and Connectors > Connectors > Users/Groups > Authentication Profiles in the left menu bar.
4. Click the + Add icon. The Add Authentication Profile window displays.

Add Authentication Profile

General Rules

Name *
VSA-Cookies-Auth-Profile

Description

Authentication Type
Active

VMS Profile
--Select--

Caching Mode
Cookie Based

Cookie Name

Cache Expiration (mins)
10

Cookie Expiration (mins)

Concurrent Login
1

Expiration Mode
--Select--

Default Authenticator
--Select--

Proactive-Reauth

Default Authentication Method *
Default Authentication Method Not Configured

LEF Profile
--Select--

Default Profile

OK Cancel


5. In the Name field, enter a name for the authentication profile (here, VSA-Cookies-Auth-Profile).
6. In the Authentication Type field, select Active.
7. To enable caching mode, click Local Database, or select a Kerberos, an LDAP, a SAML, or a certification authentication profile to use for cookie support. The screenshot above shows that Local Database is selected.
8. In the Caching Mode, select Cookie Based.
9. In the Expiration Mode field, do not select a value, because an expiration is not applicable for the SASE client.
10. For information about configuring other fields on the Add Authentication Profile popup window, see [Configure an Authentication Profile](#).
11. Click OK.

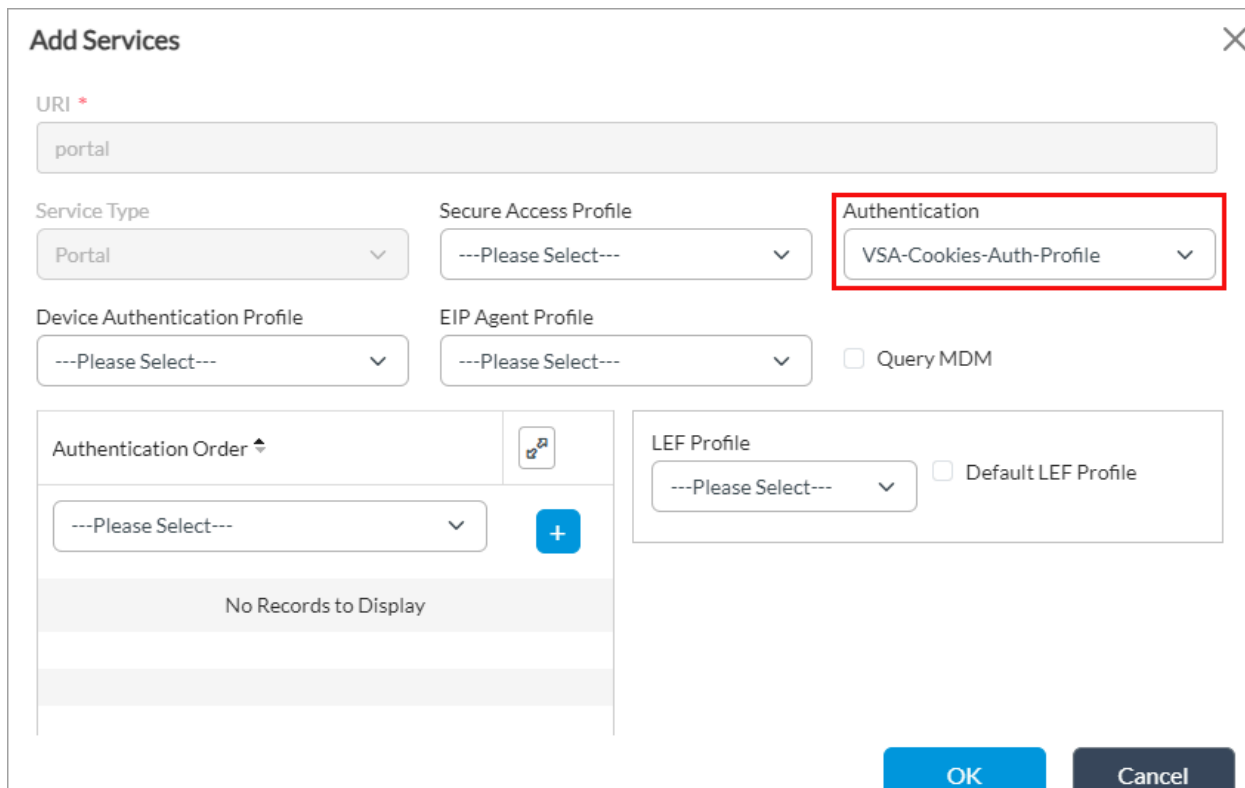
To associate the authentication profile with a VSA portal:

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Director/Versa_SASE_Client/Use_the_V...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Director/Versa_SASE_Client/Use_the_V...)

Updated: Wed, 23 Oct 2024 08:43:16 GMT

Copyright © 2024, Versa Networks, Inc.


1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Templates > Device Templates in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Secure Access > Portal > General in the left menu bar.
4. Click the  Edit icon. The Add Services popup window displays.

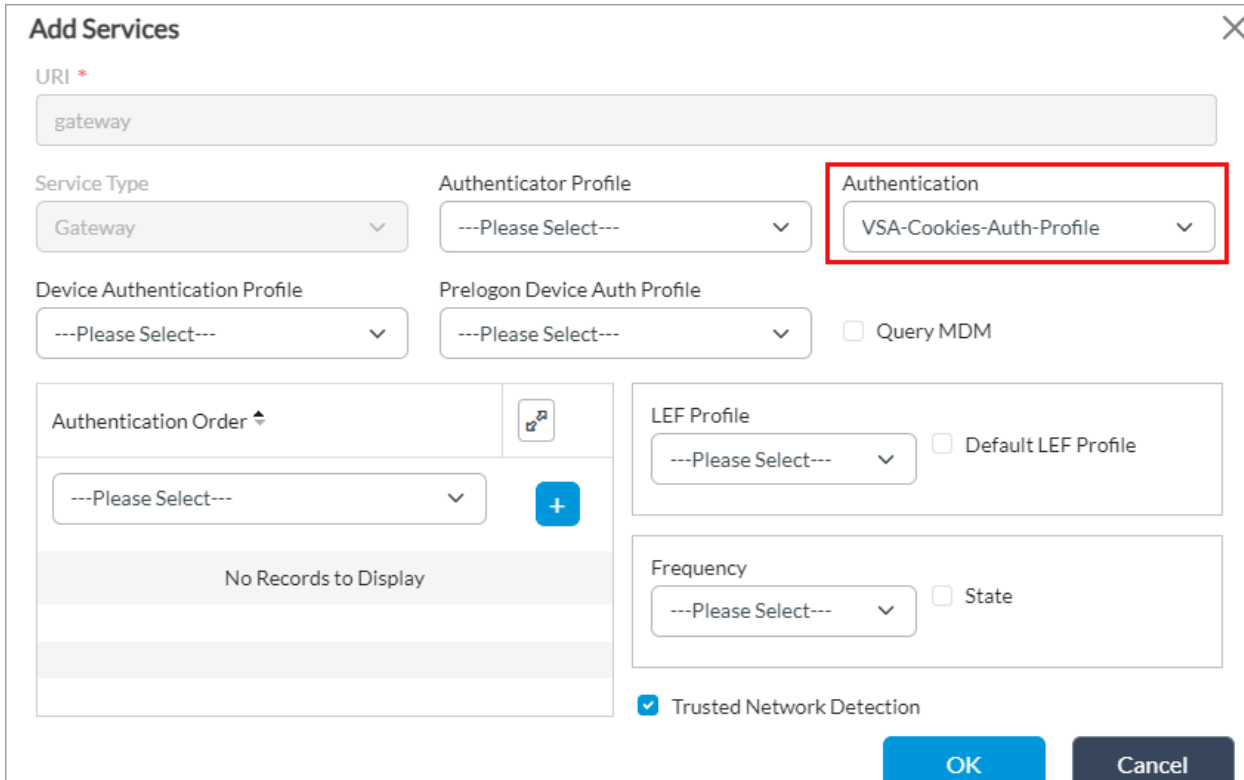


5. Select the authentication profile you configured in the steps above (here, VSA-Cookies-Auth-Profile) from the Authentication drop-down list.
6. For more information about configuring other fields in the Add Services popup window, see Add a Secure Access Portal in [Configure the Versa Secure Access Service](#).
7. Click OK.

To associate the authentication profile with a VSA gateway:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Templates > Device Templates in the horizontal menu bar.
 - c. Select an organization in the left menu bar.

- d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Secure Access > Gateway > General in the left menu bar.
4. Click the  Edit icon. The Add Services popup window displays.




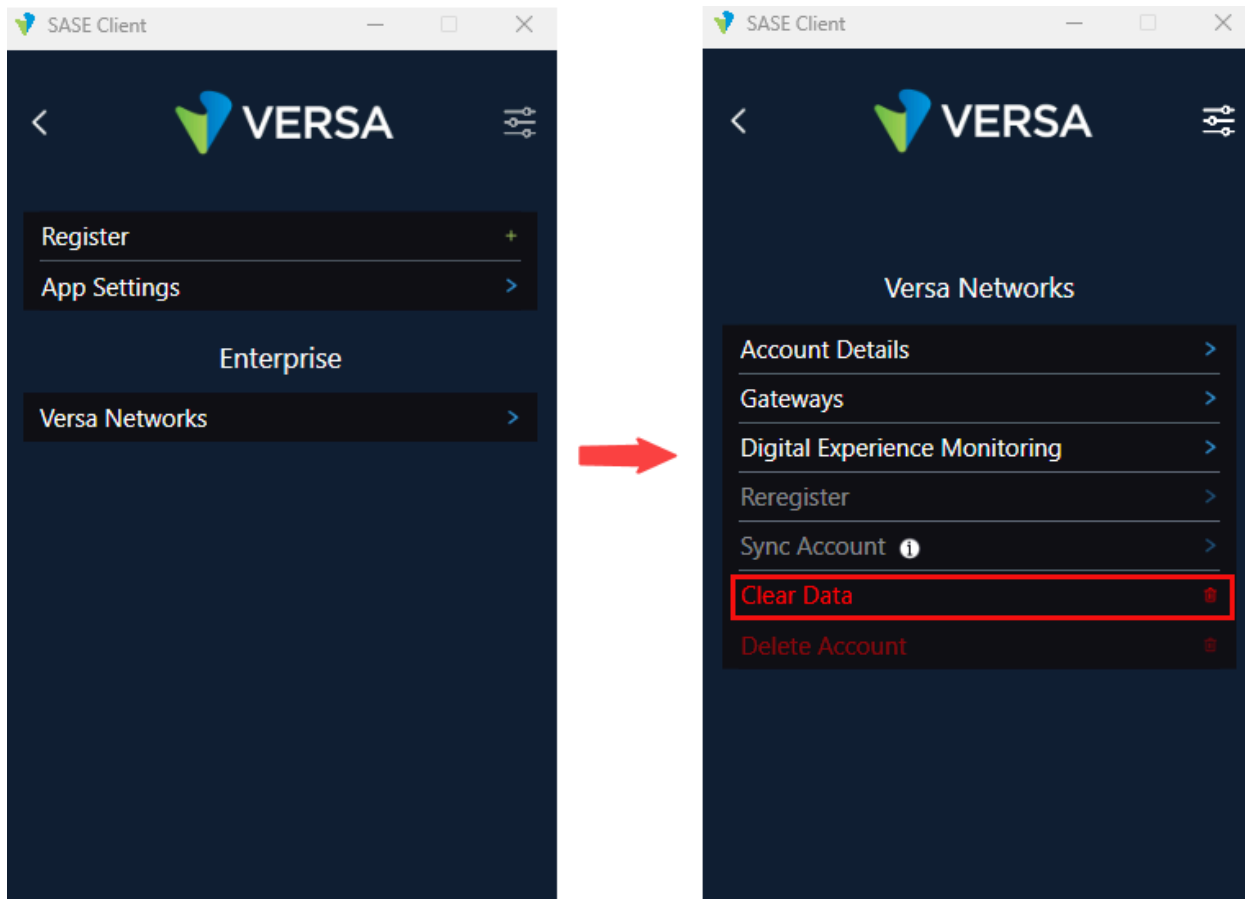
The screenshot shows the 'Add Services' dialog box. The 'URI' field contains 'gateway'. The 'Service Type' is set to 'Gateway'. The 'Authenticator Profile' is set to '---Please Select---'. The 'Authentication' dropdown is highlighted with a red box and shows 'VSA-Cookies-Auth-Profile'. The 'Device Authentication Profile' is set to '---Please Select---'. The 'Prelogon Device Auth Profile' is set to '---Please Select---'. There is a 'Query MDM' checkbox which is unchecked. The 'Authentication Order' section shows a dropdown set to '---Please Select---' and a '+' button. Below this is a message 'No Records to Display'. The 'LEF Profile' section shows a dropdown set to '---Please Select---' and a 'Default LEF Profile' checkbox which is unchecked. The 'Frequency' section shows a dropdown set to '---Please Select---' and a 'State' checkbox which is unchecked. At the bottom, there is a 'Trusted Network Detection' checkbox which is checked. The 'OK' and 'Cancel' buttons are at the bottom right.

5. In the Authentication field, select the authentication profile you configured above (here, VSA-Cookies-Auth-Profile).
6. For more information about configuring other fields in the Add Services popup window, see Configure a Secure Access Gateway in [Configure the Versa Secure Access Service](#).
7. Click OK.

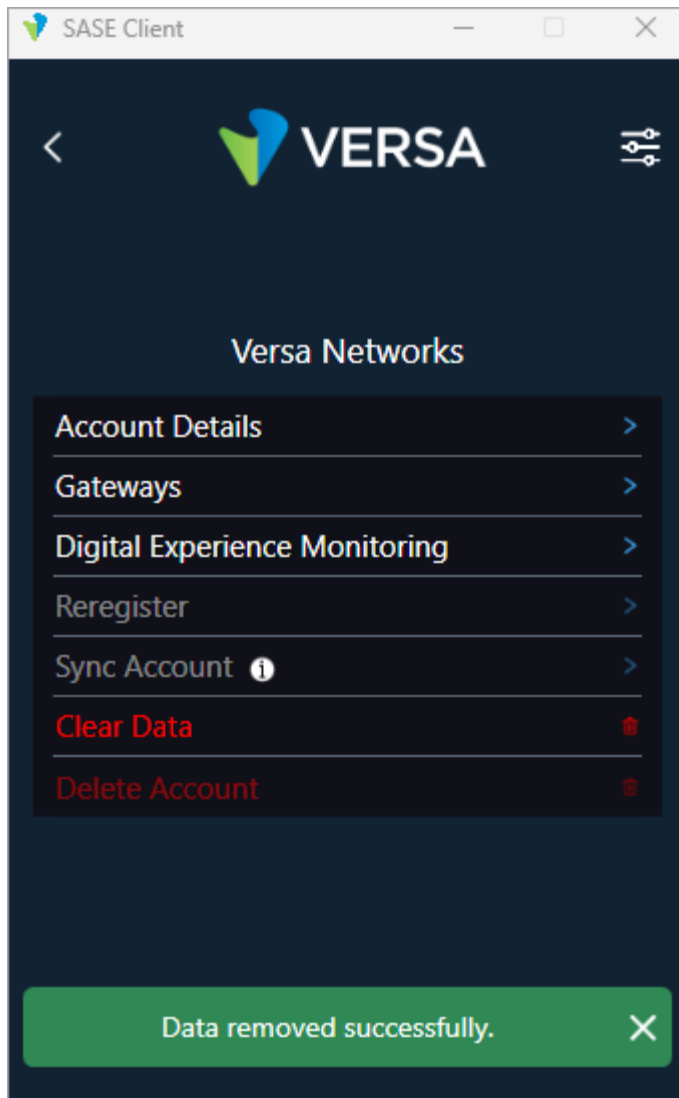
The SASE client has no fields that allow you to enable or disable cookies.

To clear stored cookies and data from the SASE client:

1. In the SASE client home screen, click the  Settings icon.
2. In the Enterprise section, click the account for which you want to clear stored cookies and data, and then Click Clear Data.



A message displays indicating that the data is cleared. For example:



Enable Performance-Based Dynamic Gateway Selection

Dynamic gateway selection allows SASE clients to select the best gateways based on distance and availability. You create groups of gateways that the client can use to choose the best gateway. When a user connects to a gateway group, the client selects the best available gateway. You add gateway groups from a Versa Director node and then associate gateways with gateway groups. For more information, see [Configure the Versa SASE Client To Select the Best Gateway](#).

To configure gateway groups from a Versa Director node:

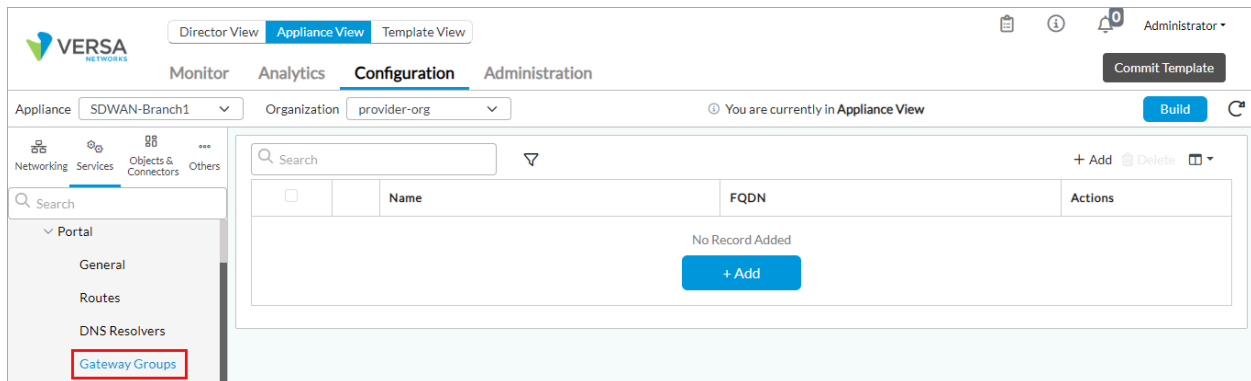
1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Templates > Device Templates in the horizontal menu bar.
 - c. Select an organization in the left menu bar.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Director/Versa_SASE_Client/Use_the_V...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Director/Versa_SASE_Client/Use_the_V...)

Updated: Wed, 23 Oct 2024 08:43:16 GMT

Copyright © 2024, Versa Networks, Inc.

- d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Secure Access > Portal > Gateway Groups in the left menu bar.



4. Click the + Add icon. The Add Gateway Groups popup window displays.

The screenshot shows a modal window titled 'Add Gateway Groups'. It has a close button (X) in the top right corner. The form contains three input fields: 'Name' with a red asterisk, 'Description', and 'FQDN' with a red asterisk. The 'Name' field contains the text 'APAC'. The 'FQDN' field contains the text 'apac.com'. At the bottom right, there are two buttons: 'OK' (blue) and 'Cancel' (dark grey).

5. Enter a name (here, APAC).
6. Optionally, enter a description.
7. Enter the FQDN for the server group.
8. Click OK.

To associate a gateway with a gateway group:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.

- b. Select Templates > Device Templates in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
 3. Select Services > Secure Access > Portal > Gateways in the left menu bar.
 4. Click the + Add icon. The Add Gateways popup window displays.

Add Gateways

General Traffic Steering IKE/IPsec TLS DTLS

Name * Description

☐ Allow Delete by App ☐ Display VPN Profile in OS ☐ Hot Standby

Hosts +

No Records to Display

Tunnel Order +

---Please Select---

No Records to Display

**Use drag and drop to change existing tunnel order*

Priority IPsec Profile ID CA Certificate Service Port

---Please Select---


443

Gateway Groups +

APAC

No Records to Display

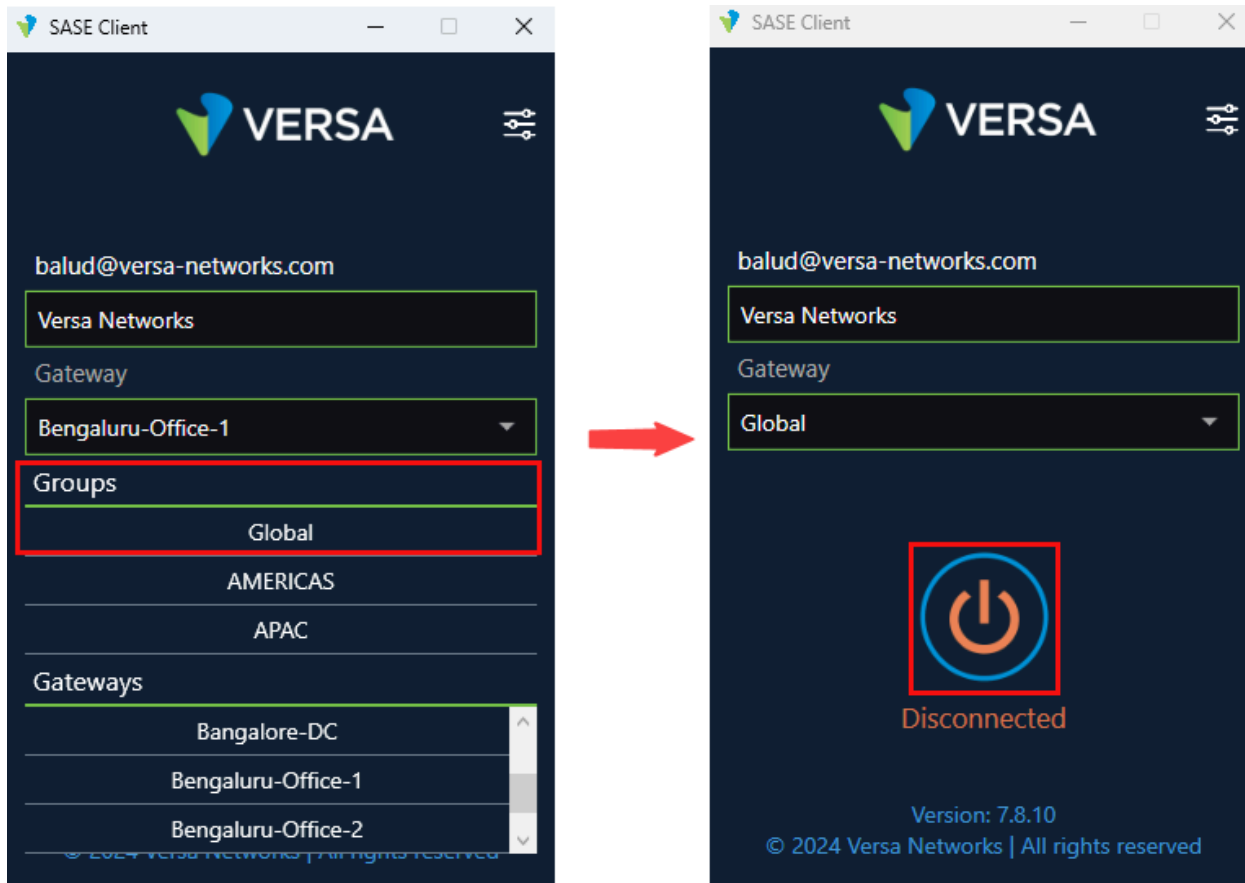
OK Cancel

5. Select the General tab.
6. In the Gateway Groups field, select the gateway group to associate with the gateway, and then click the  Add icon.
7. For information about configuring other fields on the Add Gateways popup window, see [Configure the Versa Secure Access Service](#).
8. Click OK.

Note that groups are displayed on the SASE client only if you configure gateway groups.

To select gateway groups from SASE client:

1. In the SASE client home screen, click the Gateway drop-down list, and then select the group to which you want to connect.




2. Click the Connect button.

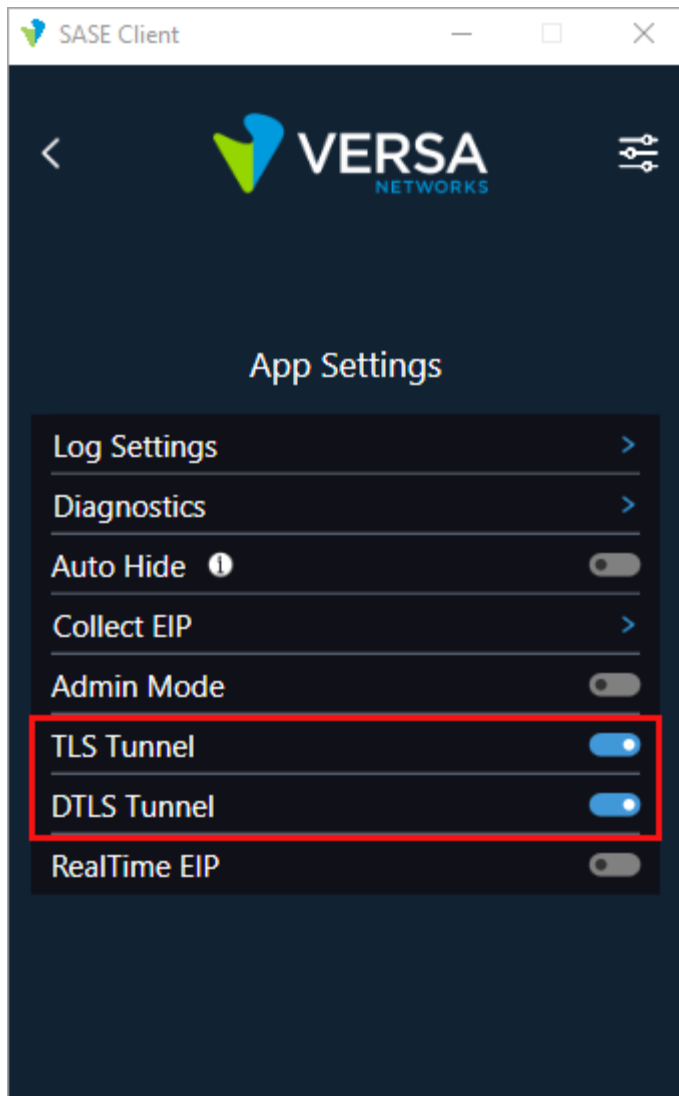
Enable TLS and DTLS Tunnels

For Windows only.

When you enable a TLS or DTLS tunnel, the client tries to establish a tunnel based on the tunnel type order it receives from the portal. If the first attempt fails, the client tries to connect to the next tunnel type in the configuration order. For more information about enabling TLS and DTLS tunnels using the CLI, see [Display and Execute Client Options](#).

To enable a TLS or DTLS tunnel:


1. In the SASE client home screen, click the  Settings icon.
2. Click App Settings.

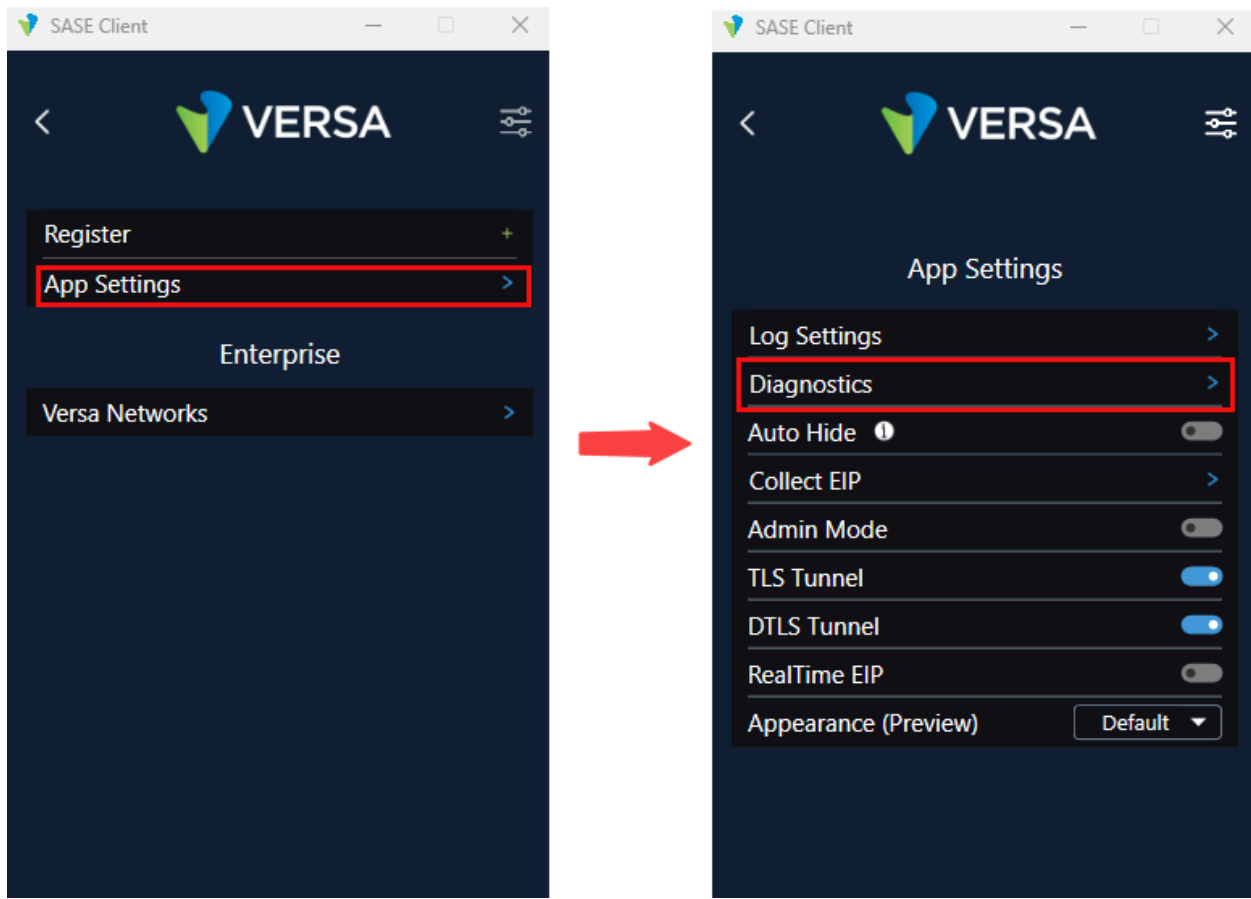


3. Click the TLS Tunnel or DTLS Tunnel toggle button to enable these features. By default, TLS and DTLS tunnels are disabled.

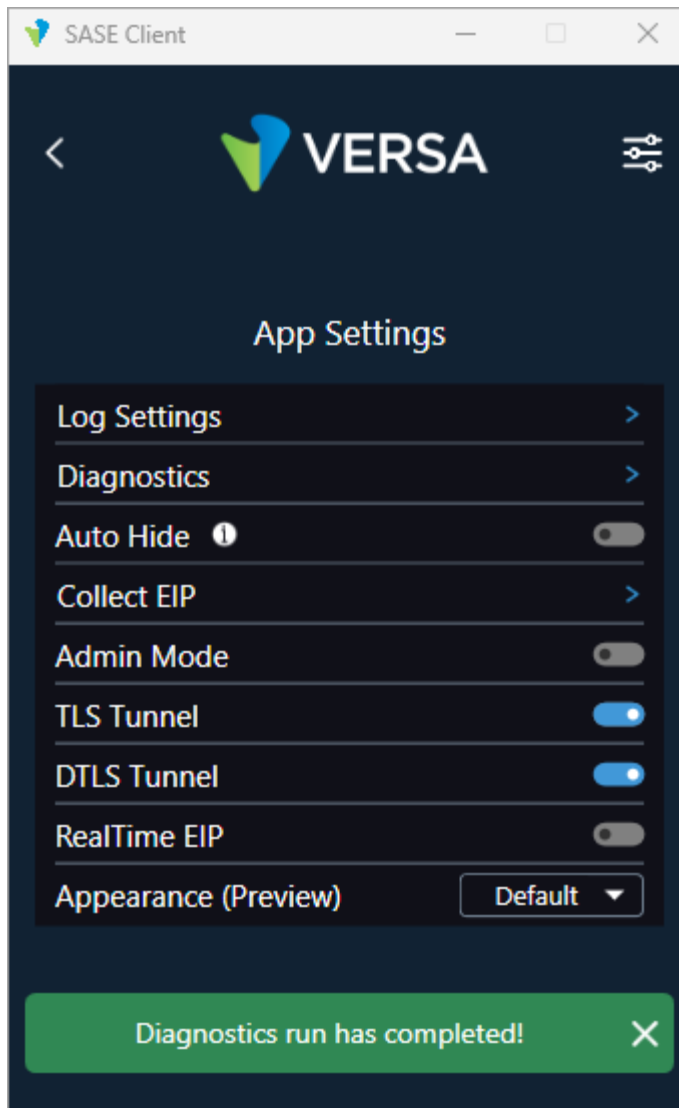
Perform Diagnostics and Export Logs

To perform diagnostics to automatically fix basic issues:

1. In the SASE client home screen, click the  Settings icon.
2. Click App Settings and then click Diagnostics.




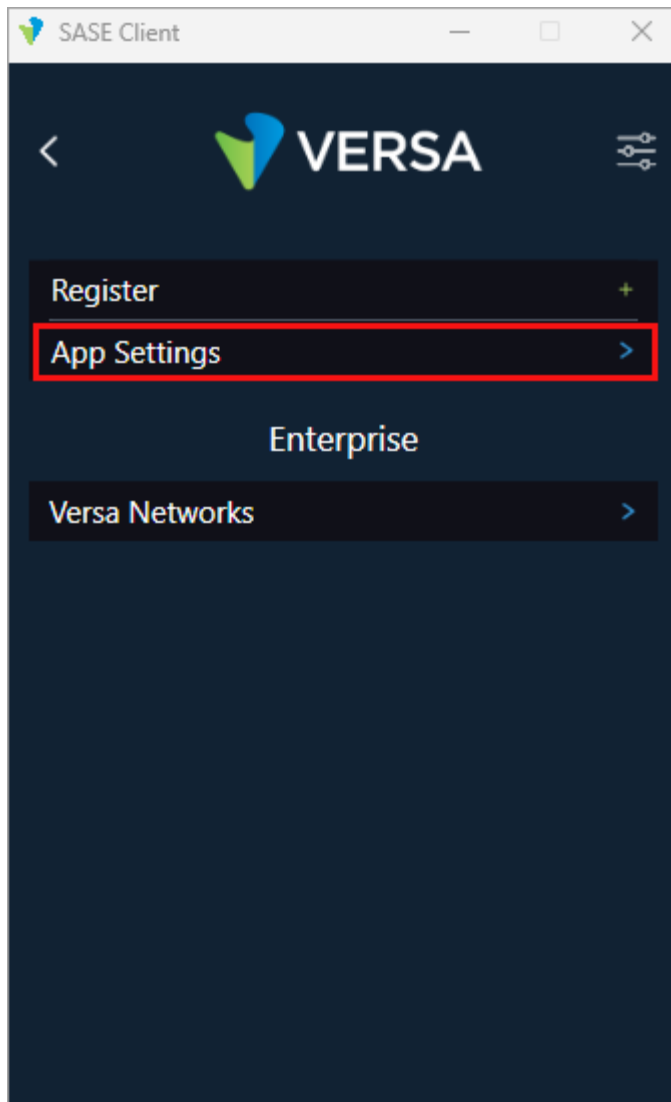
A message displays when the diagnostics complete. For example:



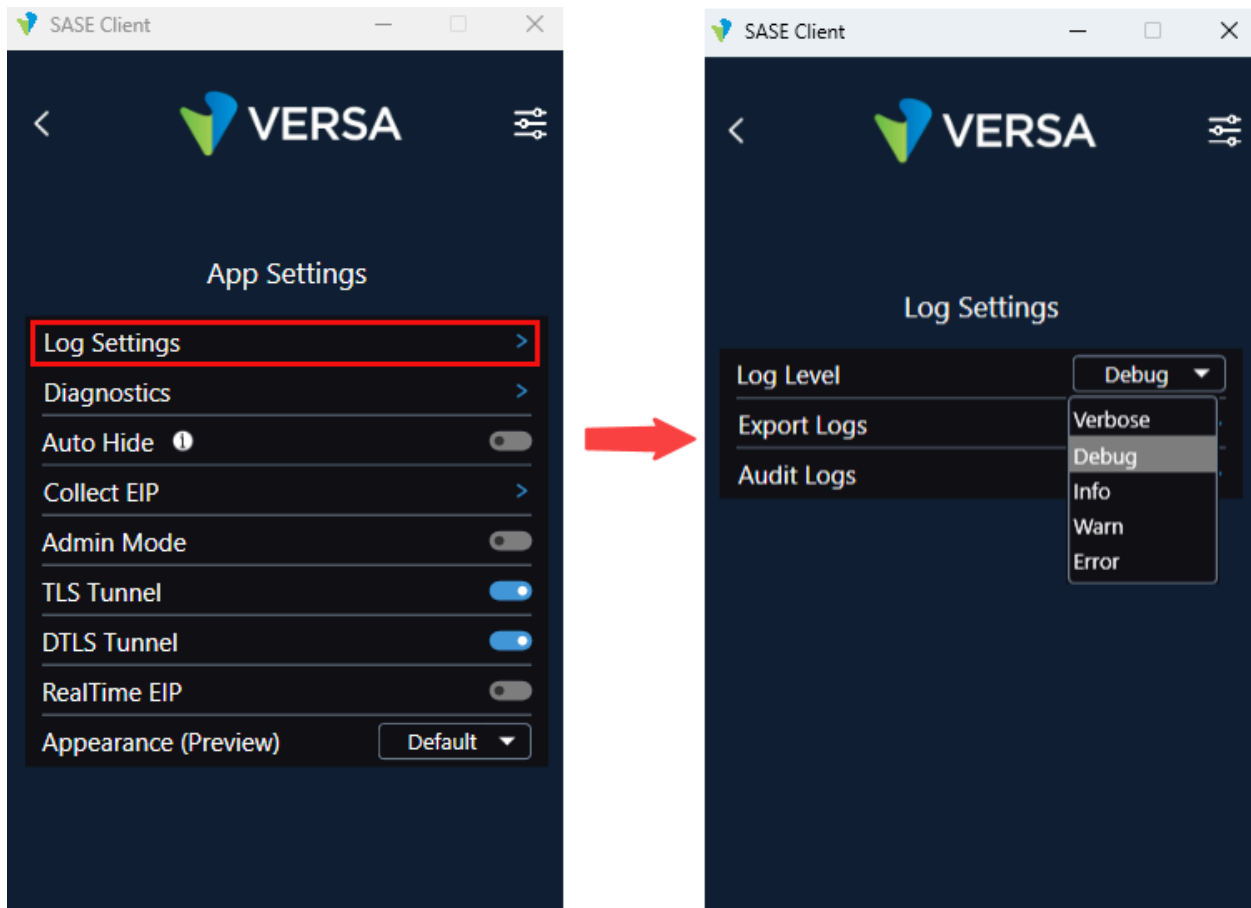
For issues that you cannot fix using Diagnostics, save the logs as a .zip file and share this file with Versa Networks Customer Support.

Before you save log files, select the severity of the logs to include:

1. In the SASE client home screen, click the  Settings icon.
2. Click App Settings.



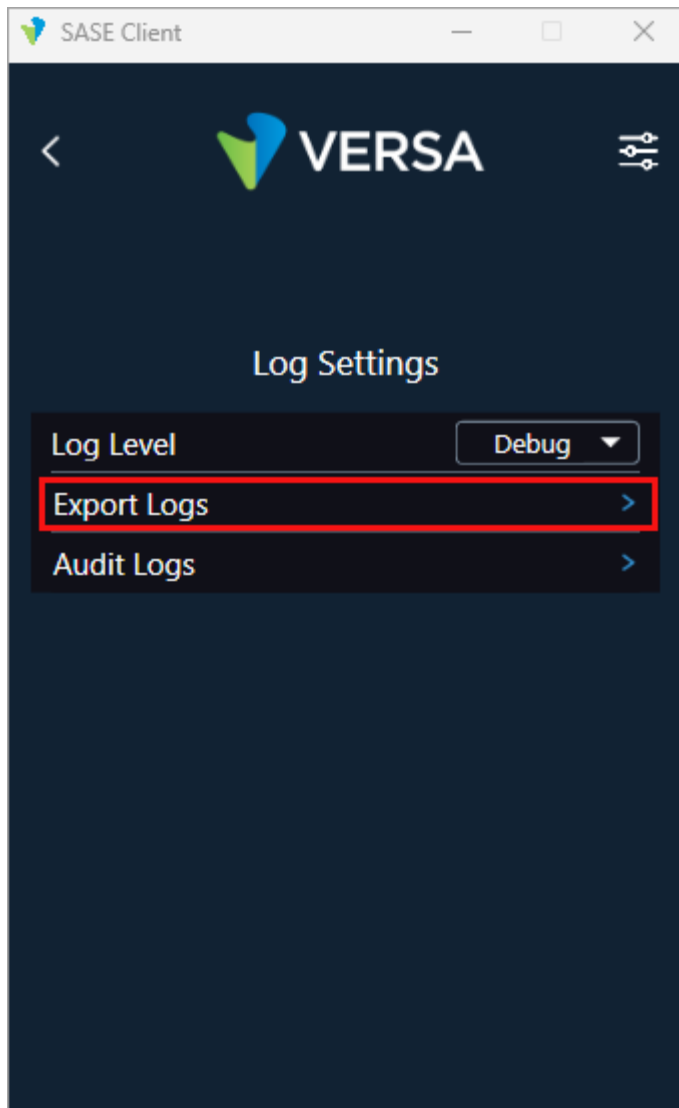
3. Click Log Settings.



4. In the Log Settings screen, click Log Level, and select a log severity level:
 - Debug—Log application debug-level information.
 - Error—Log error-level information.
 - Info (default)—Log informational-level information. This is the default.
 - Verbose—Log additional information during the interaction with the client user interface.
 - Warn—Log warning-level information.

To save log files:


1. In the App Settings screen, click Export Logs.

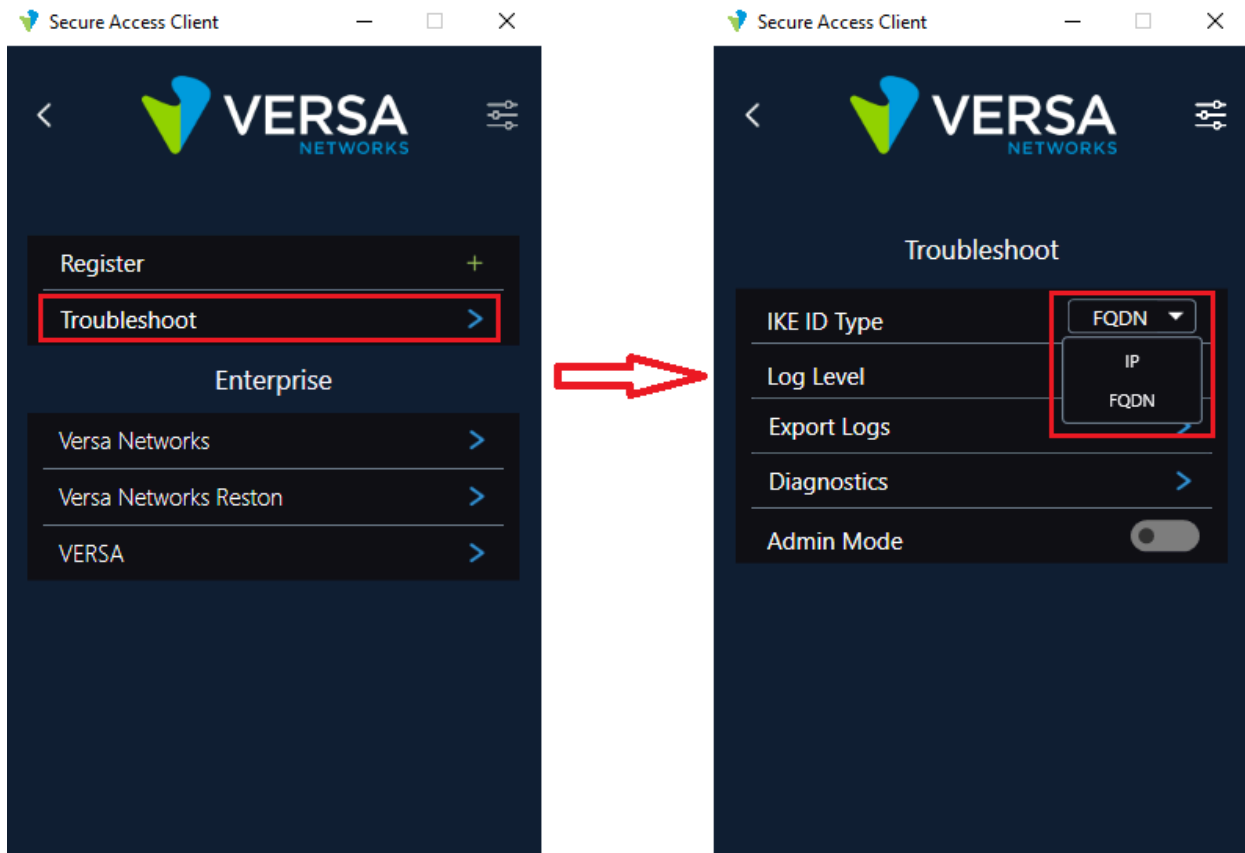


2. Select a folder and save the log file on your computer. The saved log file is in .zip format.

Select the IKE ID Type

For Releases 7.6.x and earlier.

1. In the SASE client home screen, click the  Settings icon.
2. Click Troubleshoot. Then, in the Troubleshoot window, click IKE ID Type and select IP or FQDN. The default is FQDN.



Support for IPsec Transforms and DH Groups

For Windows only.

Windows clients receive IPsec transform and Diffie-Hellman (DH) group values from the service-side configuration and map these values.

The following table describes the IPsec transform values that the client maps against the received configuration.

Configuration	Cipher Transform Constants	Encryption Methods	Integrity Check Method
esp-3des-md5	DES3	DES3	MD5
esp-3des-sha1	DES3	DES3	SHA1
esp-aes128-ctr-sha1 (Currently not supported)	—	—	—
esp-aes128-ctr-xcbc (Currently not supported)	—	—	—
esp-aes128-gcm	GCM AES128	AES128	—
esp-aes128-md5	AES128	AES128	MD5
esp-aes128-sha1	AES128	AES128	SHA1
esp-aes128-sha256	AES128	AES128	SHA256
esp-aes128-sha384	AES128	AES128	SHA384
esp-aes128-sha512	AES128	AES128	SHA384
esp-aes256-gcm	GCM AES256	AES256	—
esp-aes256-md5	AES256	AES256	MD5
esp-aes256-sha1	AES256	AES256	SHA1
esp-aes256-sha256	AES256	AES256	SHA256

esp-aes256-sha384	AES256	AES256	SHA384
esp-aes256-sha512	AES256	AES256	SHA384
esp-null-md5	None	None	MD5


The following table describes the DH group values that the client maps against the received configuration:

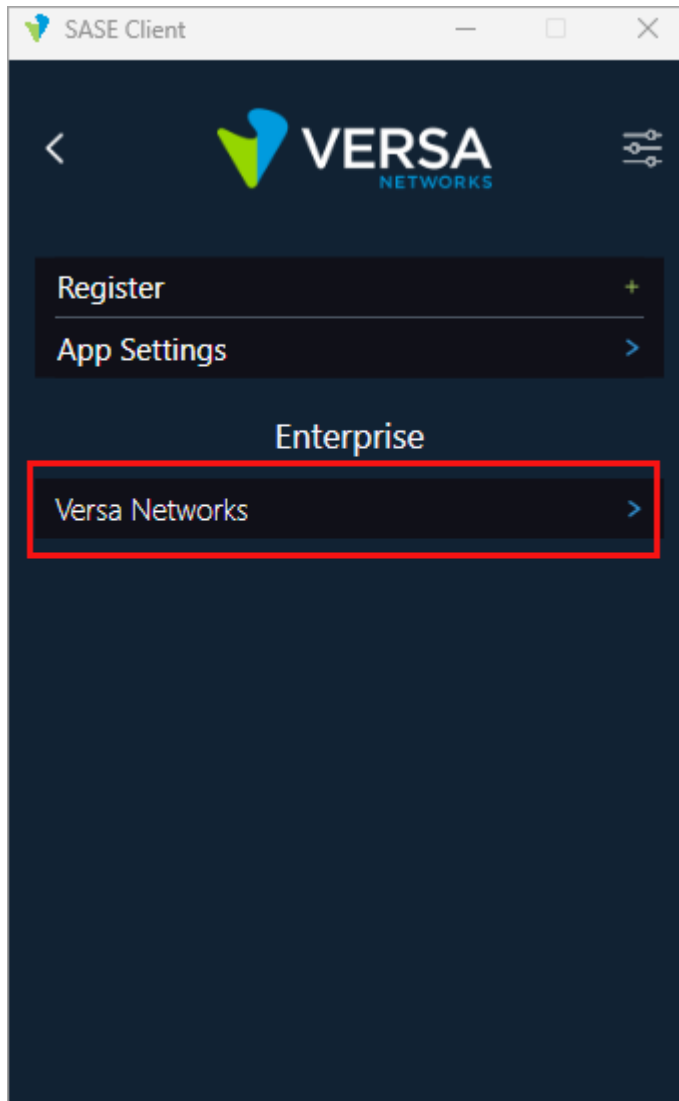
Configuration	PFS Group	DH Group
mod-none	None	None
Mod1	PFS1	Group1
Mod2	PFS2	Group2
Mod5	PFS2048	Group14
Mod14	PFS2048	Group14
Mod15	ECP256	ECP256
Mod16	ECP256	ECP256
Mod19	ECP256	ECP256
Mod20	ECP384	ECP386
Mod21 (Currently not supported)	—	—
Mod25 (Currently not supported)	—	—
Mod26 (Currently not supported)	—	—

Synchronize Account

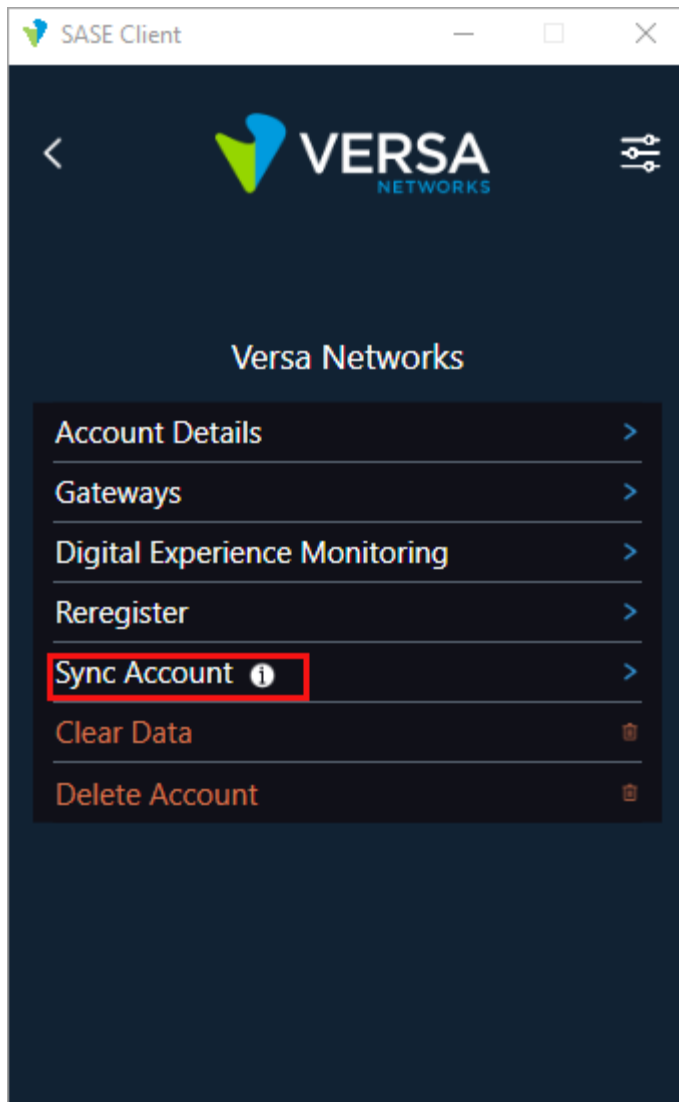
You can synchronize client configuration with the SASE portal, even if the client is not connected to the network. Note that you can perform this action only when the client is not connected to VPN.

To synchronize your client account:

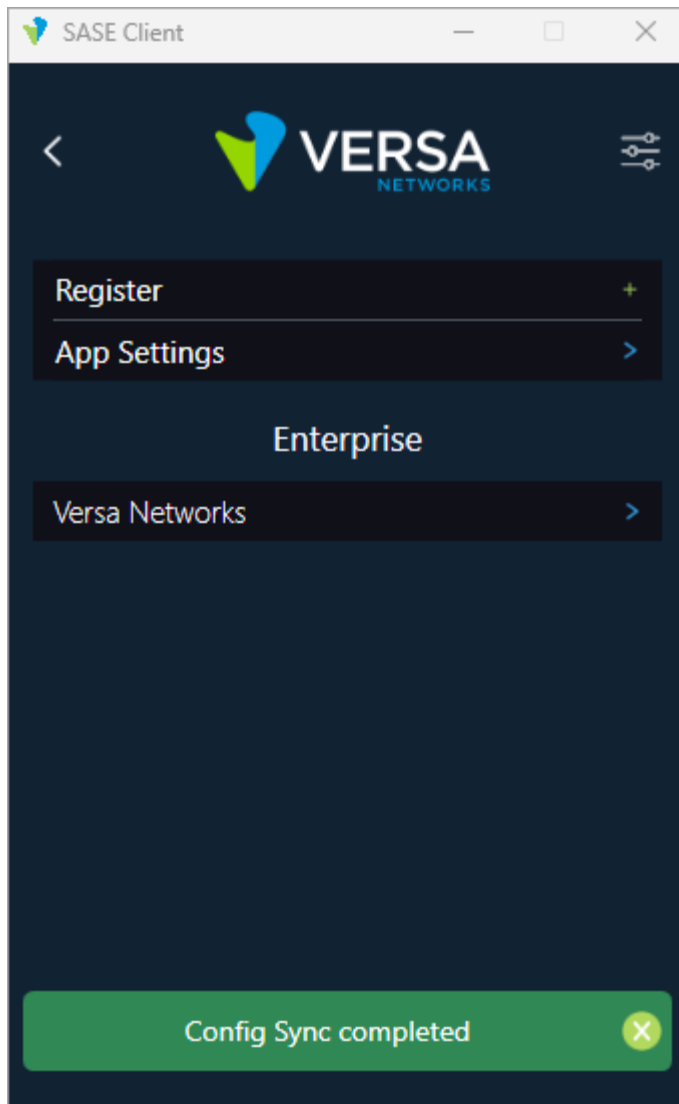
1. In the SASE client home screen, click the  Settings icon.
2. In the Enterprise section, click the account for which to synchronize the client configuration with the SASE portal.



3. In the Enterprise screen, click Sync Account.



If the synchronization is successful, the following message displays.



Use Host Information for Policy Enforcement

The SASE client automatically extracts the OS type, OS version, and antivirus software information of a user's device, a process that requires no settings on the gateway server (using a Versa Director node). If a user device is a managed device and has a certificate with device ID, the client tries to access the certificate issued by the issuer, extracts the CommonName (CN) of the certificate, and provides this as the device ID.

To set the certificate issuer from a Versa Director node:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Templates > Device Templates in the horizontal menu bar.
 - c. Select an organization in the left menu bar.

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Director/Versa_SASE_Client/Use_the_V...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Director/Versa_SASE_Client/Use_the_V...)

Updated: Wed, 23 Oct 2024 08:43:16 GMT

Copyright © 2024, Versa Networks, Inc.

- d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Secure Access > Portal > Gateway Profiles in the left menu bar.
4. Click the + Add icon. The Add Profiles popup window displays.
5. Select the Client Controls tab.

Add Gateway Profiles

General IKE/IPsec **Client Controls** Traffic Steering TLS DTLS

Logo URL

Change Password URL

☐ Add Custom Gateway
 ☐ Edit Gateway
 ☒ Display Gateway
 ☐ Multi-Tenancy
 ☒ Remember Credential
 ☐ Tamper Protection

☐ Register With DNS
 ☒ IP Stickiness
 ☐ Auto Update
 ☐ TWAMP
 ☒ IPv6
 ☐ Strict Tunnel Mode

☐ Auto Disconnect

Portal Lifetime(mins)
 Maximum Number of Gateway
 Password Expiry Warn Before
 Register DNS Suffix

Certificate Issuer
 Latency Bias
 Posture Check Interval(mins)
 Trusted Network Hostname

SLA Profile
 Tamper Protection Override Key
 Auto Disconnect Interval(mins)

OK Cancel

6. Enter the name of the certificate issuer.
7. For more information about configuring other fields in the Add Gateway Profiles popup window, see Configure Secure Access Gateway Profiles in [Configure the Versa Secure Access Service](#).
8. Click OK.


View CA Certificates

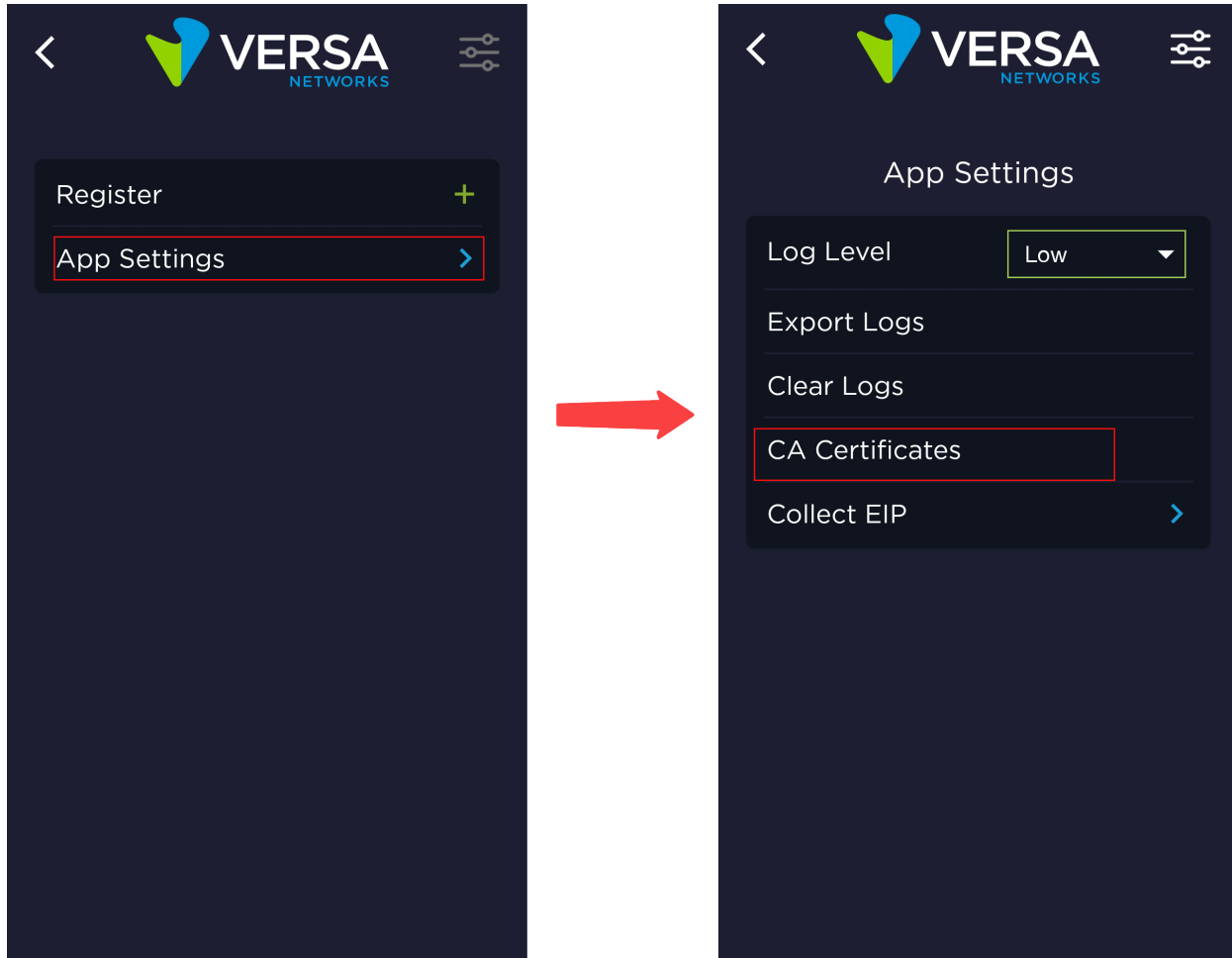
For Android only.

You can view the following type of CA certificates from the SASE client:

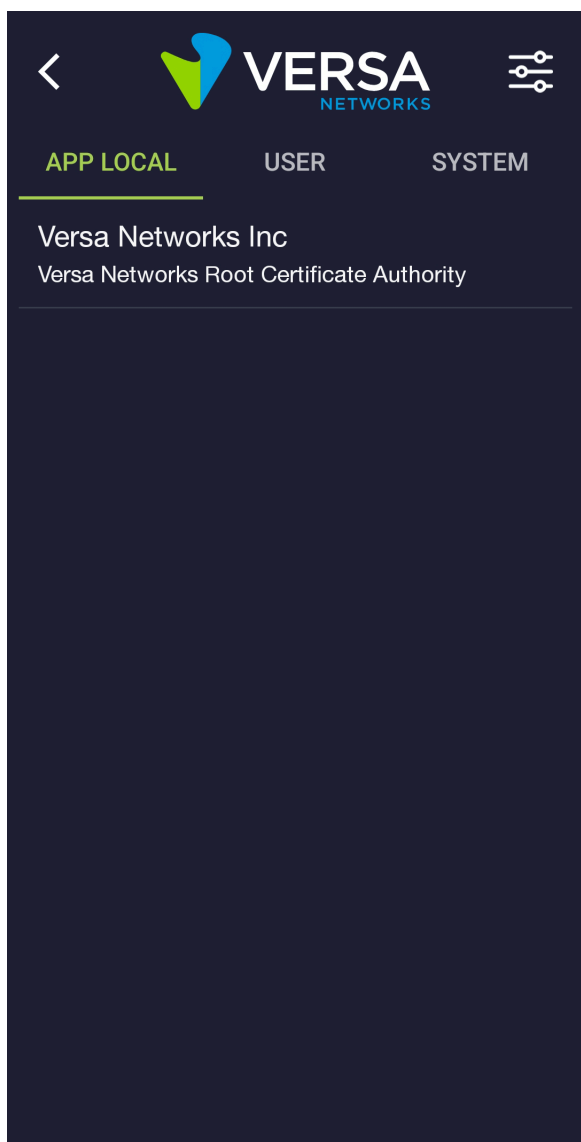
- CA certificate used by the Android OS—By default, Android devices use global CA certificates.
- The certificates that you have imported to your device—All global root CA certificates are stored in the Android system keystore. Some organizations have their own root CA certificates that users must import before they can securely access application URLs within their organization. On Android devices, you can import certificates that are stored in Android user keystore and that are used by all applications.
- Application-local certificates, which are dynamically imported in the following instances:
 - While synchronizing with an organization and fetching details of a gateway that has intermediate CA certificates, application-local certificates are imported to establish a tunnel successfully.
 - While accessing an API, the SASE client dynamically downloads intermediate CA certificates (from the the authority information access [AIA] URL of domain certificate). When the certificate is invalid, the client verifies the certificate chain and, if it is valid, allows the request.

To view CA certificates:

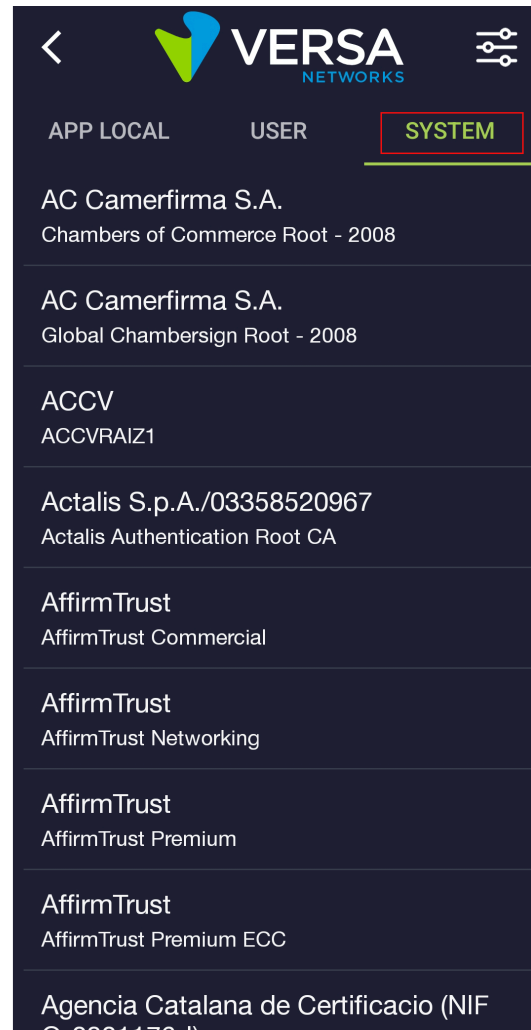
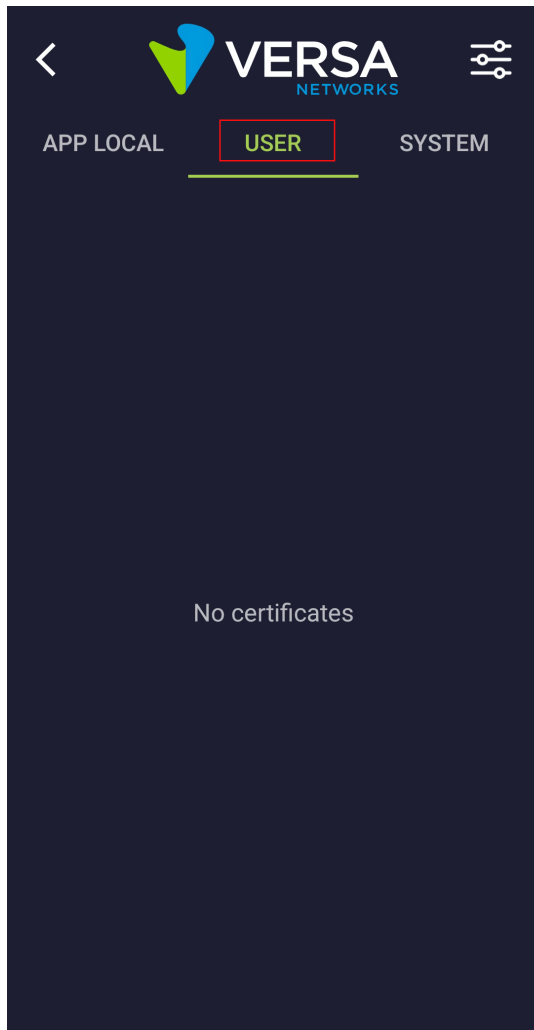
1. In the SASE client home screen, click the  Settings icon.
2. Click App Settings. Then, in the App Settings window, click CA Certificates.



The App Local tab displays:




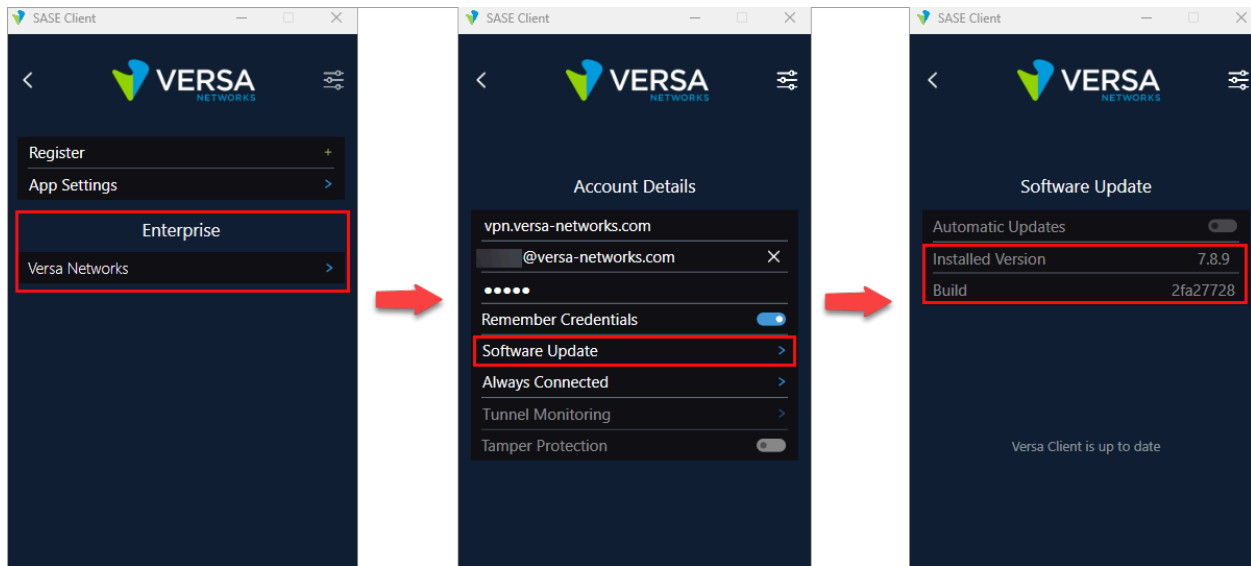
3. Click the User and System tabs to view the user and application-local certificates:



View Client Version and Build

To view the client software version and build:

1. In the SASE client home screen, click the  Settings icon.
2. Click Enterprise > Account Details > Software Update.



Enable SASE Client Features from the CLI (for Windows Clients)

On Windows clients, you can issue CLI commands from the SASE client's console to perform basic SASE client tasks and to troubleshoot SASE client issues.

To open the SASE client CLI console:

1. Open the Windows command prompt.
2. To start the SASE client CLI console, issue the following CLI commands:

```
C: cd C:\Program Files (x86)\Versa Secure Access
C:\Program Files (x86)\Versa Secure Access> VersaSecureAccessClientConsole.exe
```

For example:

```
C:\Program Files (x86)\Versa Secure Access> VersaSecureAccessClientConsole.exe
C:\Program Files (x86)\Versa Secure Access>VersaSecureAccessClientConsole.exe
263 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
Run: VersaSecureAccessClientConsole.exe global --help, to get help for global options
Run: VersaSecureAccessClientConsole.exe help, to check supported Options Verb
```

3. To display the VSA console CLI options, issue the following CLI command:

```
C:\Program Files (x86)\Versa Secure Access> VersaSecureAccessClientConsole.exe --help
VersaSecureAccessClientConsole 7.5.9.0

global    (Default Verb)
prelogon  Prelogon operations
client    Configure Client options
monitor   Monitor options
service   Configure Service options
```

help Display more information on a specific command.
version Display version information.

4. To display the SASE client software version, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe global --version  
VersaSecureAccessClientConsole 7.5.9.0
```

The following sections describe how to display and execute global, pre-logon, client, monitor, and service CLI options from the Windows SASE client console. The monitor and service CLI options are supported in Releases 7.5.8 and later.

Note that if a configuration is supported on the VSA server, the corresponding CLI option is displayed as [Deprecated]. If the server does not support pushing these configurations, the client continues to support deprecated CLI commands.

Display and Execute Global Options

To view all the global options, issue the following CLI command:

```
C:\Program Files (x86)\Versa Secure Access> VersaSecureAccessClientConsole.exe global --help
```

For example:

```
C:\Program Files (x86)\Versa Secure Access>VersaSecureAccessClientConsole.exe global --help  
VersaSecureAccessClientConsole 7.8.9.0  
  
--enable_split_dns      [Deprecated] Enable split DNS support  
--disable_split_dns     [Deprecated] Disable split DNS support  
--register_with_dns      [Deprecated] (true|false). Enable/Disable register with DNS  
--register_dns_suffix    [Deprecated] DNS Suffix to be used while registering with DNS. Used with  
                          --register_with_dns. Ignored if --register_with_dns is false  
--network_outage_timeout [Deprecated] Network outage timeout in seconds. (Range 30-3600)  
--uninstall_profiles    Remove all enterprise configurations  
--ip_stickiness          [Deprecated] (true|false). Enable/Disable IP stickiness  
--ip_stickiness_latency [Deprecated] Latency diff (in %) to be considered in comparison with best. This  
value is  
                          to be used along with ip_stickiness. Used with --ip_stickiness. Ignored if --ip_stickiness  
                          is false  
--http_timeout          Timeout for http calls. (Range 30-300)  
--disable_ipv6          Disable IPV6. You must restart your computer for these changes to take effect.  
--enable_sso            (true|false). Enable/Disable Single sign-on.  
--help                  Display this help screen.  
--version                Display version information.
```

--enable_split_dns

To enable split DNS support, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe global --enable_split_dns
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe global --enable_split_dns
324 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
401 [1] INFO Versa Secure Access (null) - Enable DNS Split tunnel
991 [1] INFO Versa Secure Access (null) - Success!
```

To disable split DNS support, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe global --disable_split_dns
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe global --disable_split_dns
291 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
330 [1] INFO Versa Secure Access (null) - Disable DNS Split tunnel
422 [1] INFO Versa Secure Access (null) - Success!
```

--register_with_dns

To register with a DNS server, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe global --register_with_dns true
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe global --register_with_dns true
386 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
615 [1] INFO Versa Secure Access (null) - Enable Register IP with DNS with Suffix
872 [1] INFO Versa Secure Access (null) - Success!
```

To unregister from a DNS server, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe global --register_with_dns false
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe global --register_with_dns false
563 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
628 [1] INFO Versa Secure Access (null) - Disable Register IP with DNS
```

--register_dns_suffix

To add the DNS suffix, issue the following CLI command. Note that you must issue this option with the **--register_with_dns true** option. If you issue the **--register_with_dns false** option, the **--register_dns_suffix** option is not accepted.

```
C:\VSA> VersaSecureAccessClientConsole.exe global --register_dns_suffix "domain-name" --
register_with_dns true
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe global --register_dns_suffix "abc.com" --register_
with_dns true
```

```
443 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
505 [1] INFO Versa Secure Access (null) - Enable Register IP with DNS with Suffix abc.com
624 [1] INFO Versa Secure Access (null) - Success!
```

--network_outage_timeout

To set the network outage time, in seconds, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe global --network_outage_timeout timeout
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe global --network_outage_timeout 10
367 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.4.1_24cd434d
467 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.4.1_24cd434d
467 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.4.1_24cd434d
526 [1] INFO Versa Secure Access (null) - Set Network Outage Timeout
526 [1] INFO Versa Secure Access (null) - Set Network Outage Timeout
676 [1] INFO Versa Secure Access (null) - Success!
676 [1] INFO Versa Secure Access (null) - Success!
```

--uninstall_profiles

Use this option to reset the client to the default (clean) installed state.

To uninstall registered profiles, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe global --uninstall_profiles
```

--ip_stickiness

IP stickiness stores the tunnel IP address provided by a connection and requests the same IP address for subsequent connections to the same gateway. When connecting to the best gateway with IP stickiness enabled, the client chooses the previously connected gateway, if it is available in the optimal gateway list and if that gateway's latency is within the permitted range compared to the best.

To enable IP stickiness, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe global --ip_stickiness true
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe global --ip_stickiness true
289 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
328 [1] INFO Versa Secure Access (null) - Set IP Stickiness
519 [1] INFO Versa Secure Access (null) - Success!
```

To disable IP stickiness, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe global --ip_stickiness false
```


For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe global --ip_stickiness false
291 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
331 [1] INFO Versa Secure Access (null) - Resets IP Stickiness
520 [1] INFO Versa Secure Access (null) - Success!
```

To customize the IP stickiness latency percentage difference compared against the best, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe global --ip_stickiness true --ip_stickiness_latency
latency
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe global --ip_stickiness true --ip_stickiness_latency 20
293 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
332 [1] INFO Versa Secure Access (null) - Set IP Stickiness
523 [1] INFO Versa Secure Access (null) - Success!
```

--http_timeout

To specify a timeout value for HTTP calls, issue the following CLI command. The value range is 30 through 300 seconds.

```
C:\VSA> VersaSecureAccessClientConsole.exe global --http_timeout 60
```

--disable_ipv6

To disable IPv6 support, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe global --disable_ipv6
```

--enable_sso

You can enable SSO when you register the client to the portal. By default, SSO is disabled, so the user is prompted to enter credentials during SAML-based registration and reregistration. When you enable SSO, the client attempts a browser-based SSO using the Windows login credentials and tries to avoid prompting users for credentials.

To enable single sign-on (SSO), issue the following CLI command:

```
VSA>VersaSecureAccessClientConsole.exe global --enable_sso true
```

To disable SSO, issue the following CLI command:

```
C:\VSA>VersaSecureAccessClientConsole.exe global --enable_sso false
```

Display and Execute Pre-Logon Options

To view the pre-logon options, issue the following CLI command:

```
C:\Program Files (x86)\Versa Secure Access> VersaSecureAccessClientConsole.exe prelogon --help
```

For example:

```
C:\Program Files (x86)\Versa Secure Access> VersaSecureAccessClientConsole.exe prelogon --help  
VersaSecureAccessClientConsole 7.8.0.0  
  
--prelogon_config          Prelogon configuration file path  
--trusted_root_ca_certificate Trusted root certificate for Secure Access Service  
--disconnect_prelogon      Disconnect prelogon connection  
--help                    Display this help screen.  
--version                 Display version information.
```

Note that to issue the pre-logon command options, you must have administrator privileges and you must be at the administrator command prompt. Also, save the pre-logon file (JSON) and CA certificate in your computer before you run the first two commands.

--prelogon_config

The pre-logon configuration option allows users to log in to the organization's VPN from a locked screen. For more information, see [Configure Pre-Logon for the Versa Secure Access Client](#).

To apply the pre-logon configuration, issue the following CLI command:

```
c:\VSA> VersaSecureAccessClientConsole.exe prelogon --prelogon_config json-filename
```

For example:

```
c:\VSA> VersaSecureAccessClientConsole.exe prelogon --prelogon_config C:\Pre-Logon\PreLogonConfig.json  
479 [1] INFO Versa Secure Access (null) - Starting application in prelogon_config mode. Version 7.4.1_24cd434d  
577 [1] DEBUG Versa Secure Access (null) - Prelogon configuration initiated  
578 [1] DEBUG Versa Secure Access (null) - Verifying and Applying Prelogon Configuration  
2092 [1] DEBUG Versa Secure Access (null) - Prelogon Configuration Applied Successfully!
```

--trusted_root_ca_certificate

Issue this command when the server uses private certificates and you want to add a root CA certificate. If the server uses trusted CA certificates, this command is optional.

To set the pre-logon configuration file path, issue the following CLI command:

```
c:\VSA> VersaSecureAccessClientConsole.exe prelogon --trusted_root_ca_certificate certificate-filename.cer
```

For example:

```
c:\VSA> VersaSecureAccessClientConsole.exe prelogon --trusted_root_ca_certificate C:\Certificate\
VersaIntermediateCertificateAuthority1.cer
278 [1] INFO Versa Secure Access (null) - Starting application in prelogon_config mode. Version 7.4.1_
24cd434d
417 [1] DEBUG Versa Secure Access (null) - Success!
```

--disconnect_prelogon

To disconnect the pre-logon VPN connection, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe prelogon --disconnect_prelogon
```

Display and Execute Client Options

To view the client options, issue the following CLI command:

```
C:\Program Files (x86)\Versa Secure Access> VersaSecureAccessClientConsole.exe client --help
```

For example:

```
C:\Program Files (x86)\Versa Secure Access> VersaSecureAccessClientConsole.exe client --help
VersaSecureAccessClientConsole 7.8.9.0

--display_default_logo           (true|false). Enable/Disable default logo
--hide_on_connect                (true|false). Enable/Disable hide on connect
--reconnect_interval             [Deprecated] Delay between subsequent auto reconnect attempts in
seconds (Range 1-10)
--allow_alwayson_disconnect      [Deprecated] (true|false). Enable/Disable disconnecting always on
profile
--alwayson_reconnect_delay       [Deprecated] When always on profile is disconnected, reconnect
will be attempted after specified
                                timeDelay in minutes. (Range 1-30)
--share_metrics_periodically     [Deprecated] (true|false). Enable/Disable sending periodic metrics
information
--post_metrics_interval         [Deprecated] Interval between posting metrics info in minutes. (Range
1-30)
--enable_fips_policy            (true|false). Enable/Disable FIPS algorithm policy
--enable_server_policy_alerts   (true|false). Enable/Disable CASB policy alerts from server
--set_default_portal_fqdn       Sets the default Portal FQDN for user registration. To reset, use --set_
default_portal_fqdn ""
--set_default_enterprise_name    Sets the default enterprise name for user registration. To reset, use
                                --set_default_enterprise_name ""
--set_default_username           Sets the default username to be prefilled during registration. To reset
use
                                --set_default_username ""
--restart_ipsec_service_on_disconnect (true|false) Restart system's IPsec policy agent service on user
disconnect
--prefer_ie_browser_engine       (true|false) Force using IE browser for SAML authentication
--sub_optimal_gateway_disconnect_delay Time delay to autodisconnect suboptimal gateway, in
```

seconds.

- enable_eip (true|false). Enable/Disable EIP (Default is true)
- enable_realtime_eip (true|false). Enable/Disable EIP (Default is false). Note: If enable_eip is set to false, it will disable real time as well
- auto_update_defer_limit Maximum allowed limit to defer software auto update (Range 1-5)
- auto_disconnect_interval Time interval to autodisconnect tunnel if user authentication fails, in minutes (Value >= 1 min)
- reset_auto_disconnect_interval Reset autodisconnect time interval. To reset, use --reset_auto_disconnect_interval ""
- auto_disconnect_reminder_time Reminder will be shown to user before the specified time about tunnel autodisconnect, in minutes (Value >= 1 minute)
- reset_auto_disconnect_reminder_time Reset autodisconnect reminder time. To reset, use --reset_auto_disconnect_reminder_time ""
- prefer_popout_browser (true|false) Application launches separate pop out browser for IDP authentication
- display_vpn_profile_in_os (true|false). Allows VPN profile to be listed in Windows network settings (Default is false) --logon_type Set the logon type to be used when AutoLogon flag is enabled. Possible values (1) - Email, (2) - Username
- auto_register_max_retry_count Maximum number of allowed autoregister attempts (Value >= 1)
- reset_auto_register_max_retry_count Reset autoregister retry count. To reset, use --reset_auto_register_max_retry_count ""
- prefer_gateway_assisted_tnd (true|false). When enabled, gateway assisted trusted network detection will be given priority over trusted host name check
- enable_tls_tunnel (true|false). When enabled, the client will attempt a TLS tunnel if configured in the gateway.
- enable_dtls_tunnel (true|false). When enabled, the client will attempt a DTLS tunnel if configured in the gateway.
- fetch_username_from_certificate To fetch username from personal certificate store e.g. To use --fetch_username_from_certificate true|false --cert_issuer <certificate issuer name> --username_field CN | SAN --san_match_regex

<regex>

- help Display this help screen.
- version Display version information.

--display_default_logo

To display the default logo in the SASE client interface, issue the following CLI command. Note that to issue the display and disable SASE client logo commands, you must have administrator privileges and you must be at the administrator command prompt.

```
c:\VSA> VersaSecureAccessClientConsole.exe client --display_default_logo true
```

For example:

```
c:\VSA> VersaSecureAccessClientConsole.exe client --display_default_logo true
276 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.4.1_24cd434d
311 [1] INFO Versa Secure Access (null) - Enable Display default logo
```

```
| 398 [1] INFO Versa Secure Access (null) - Success!
```

Disable the default logo:

```
| c:\VSA> VersaSecureAccessClientConsole.exe client --display_default_logo false
```

For example:

```
| c:\VSA> VersaSecureAccessClientConsole.exe client --display_default_logo false
302 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.4.1_24cd434d
336 [1] INFO Versa Secure Access (null) - Disable Display default logo
419 [1] INFO Versa Secure Access (null) - Success!
```

--hide_on_connect

Use the hide on connect option to automatically close the SASE client UI 10 seconds after a successful VPN connection. This command requires an administrator login.

To enable automatic closing of the SASE client, issue the following CLI command:

```
| C:\VSA> VersaSecureAccessClientConsole.exe client --hide_on_connect true
```

For example:

```
| C:\VSA>VersaSecureAccessClientConsole.exe client --hide_on_connect true
664 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.7_ce167b8e
714 [1] INFO Versa Secure Access (null) - Hide On Connect : True
```

To disable automatic closing of the SASE client UI, issue the following CLI command:

```
| C:\VSA> VersaSecureAccessClientConsole.exe client --hide_on_connect false
```

For example:

```
| C:\VSA>VersaSecureAccessClientConsole.exe client --hide_on_connect false
617 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.7_ce167b8e
662 [1] INFO Versa Secure Access (null) - Hide On Connect : False
```

--reconnect_interval

To configure the time between autoreconnection attempts, in seconds, issue the following CLI command. The range is 1 through 10 seconds.

```
| C:\VSA> VersaSecureAccessClientConsole.exe client --reconnect_interval seconds
```

For example:

```
| C:\VSA> VersaSecureAccessClientConsole.exe client --reconnect_interval 5
290 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
329 [1] INFO Versa Secure Access (null) - Set Auto Reconnect interval
495 [1] INFO Versa Secure Access (null) - Success!
```

--allow_alwayson_disconnect

To enable disconnection of always-on for a profile, issue the following CLI command. This command requires an administrator login.

```
| C:\VSA> VersaSecureAccessClientConsole.exe client --allow_alwayson_disconnect true
```

For example:

```
| C:\VSA> VersaSecureAccessClientConsole.exe client --allow_alwayson_disconnect true
327 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
368 [1] INFO Versa Secure Access (null) - Configure disconnect always on preference.
855 [1] INFO Versa Secure Access (null) - Success!
```

To disable disconnection of always-on for a profile, issue the following CLI command:

```
| C:\VSA> VersaSecureAccessClientConsole.exe client --allow_alwayson_disconnect false
```

For example:

```
| C:\VSA> VersaSecureAccessClientConsole.exe client --allow_alwayson_disconnect false
302 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
341 [1] INFO Versa Secure Access (null) - Configure disconnect always on preference.
591 [1] INFO Versa Secure Access (null) - Success!
```

--alwayson_reconnect_delay

Use this command to enter the time, in minutes, between reconnection attempts when always-on is disconnected for a profile. The range is 1 through 30 minutes.

To set the always-on reconnect delay, issue the following CLI command:

```
| C:\VSA> VersaSecureAccessClientConsole.exe client --alwayson_reconnect_delay minutes
```

For example:

```
| C:\VSA> VersaSecureAccessClientConsole.exe client --alwayson_reconnect_delay 10
326 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
371 [1] INFO Versa Secure Access (null) - Set AlwaysOn Delay Time
827 [1] INFO Versa Secure Access (null) - Success!
```

--share_metrics_periodically

To enable periodic metric sharing, issue the following CLI command. This command requires an administrator login.

```
| C:\VSA>VersaSecureAccessClientConsole.exe client --share_metrics_periodically true
```

For example:

```
| C:\VSA> VersaSecureAccessClientConsole.exe client --share_metrics_periodically true
```

```
300 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
341 [1] INFO Versa Secure Access (null) - Configure periodic metric share preference.
749 [1] INFO Versa Secure Access (null) - Success!
```

To disable periodic metric sharing, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --share_metrics_periodically false
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --share_metrics_periodically false
308 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
349 [1] INFO Versa Secure Access (null) - Configure periodic metric share preference.
761 [1] INFO Versa Secure Access (null) - Success!
```

--post_metrics_interval

Use this command to enter the time, in minutes, between posting metrics. The range is 1 through 30 minutes.

To set the interval for posting metrics, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --post_metrics_interval minutes
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --post_metrics_interval 5
316 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
358 [1] INFO Versa Secure Access (null) - Configure send metrics interval
748 [1] INFO Versa Secure Access (null) - Success!
```

--enable_fips_policy

To enable the Federal Information Processing Standards (FIPS) algorithm policy, issue the following CLI command. This command requires an administrator login.

```
C:\VSA> VersaSecureAccessClientConsole.exe client --enable_fips_policy true
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --enable_fips_policy true
358 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
398 [1] INFO Versa Secure Access (null) - Configure FIPS policy preference.
742 [1] INFO Versa Secure Access (null) - Success!
```

To disable the FIPS algorithm policy, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --enable_fips_policy false
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --enable_fips_policy false
360 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
```

```
400 [1] INFO Versa Secure Access (null) - Configure FIPS policy preference.
2815 [1] INFO Versa Secure Access (null) - Success!
```

--enable_server_policy_alerts

To enable Cloud Access Security Broker (CASB) policy alerts from server, issue the following CLI command. This command requires an administrator login.

```
C:\VSA> VersaSecureAccessClientConsole.exe client --enable_server_policy_alerts true
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --enable_server_policy_alerts true
320 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
359 [1] INFO Versa Secure Access (null) - Configuring server casb policy alerts display preference.
647 [1] INFO Versa Secure Access (null) - Success!
```

To disable CASB policy alerts from server:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --enable_server_policy_alerts false
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --enable_server_policy_alerts false
305 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
347 [1] INFO Versa Secure Access (null) - Configuring server casb policy alerts display preference.
538 [1] INFO Versa Secure Access (null) - Success!
```

--set_default_portal_fqdn

To set the default FQDN for user registration, issue the following CLI command. This command requires an administrator login.

```
C:\VSA> VersaSecureAccessClientConsole.exe client --set_default_portal_fqdn fqdn
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --set_default_portal_fqdn name.com
301 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.7_ce167b8e
341 [1] INFO Versa Secure Access (null) - Setting default portal FQDN: name.com
585 [1] INFO Versa Secure Access (null) - Successfully configured default portal FQDN!
```

To reset the default FQDN for user registration, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --set_default_portal_fqdn "fqdn"
```

--set_default_enterprise_name

To set the default enterprise name for user registration, issue the following CLI command. This command requires an administrator login.


```
C:\VSA> VersaSecureAccessClientConsole.exe client --set_default_enterprise_name "Versa Networks"
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --set_default_enterprise_name "Versa Networks"
718 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.7_d72e3e6f
796 [1] INFO Versa Secure Access (null) - Setting default Enterprise Name: Versa Networks
1031 [1] INFO Versa Secure Access (null) - Successfully configured default Enterprise Name!
```

--set_default_username

To set the default username for first time registration, issue the following CLI command. This command requires an administrator login.

```
C:\VSA> VersaSecureAccessClientConsole.exe client --set_default_username username
```

For example:

```
C:\VSA>VersaSecureAccessClientConsole.exe client --set_default_username martha
617 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.7_ce167b8e
661 [1] INFO Versa Secure Access (null) - Setting default Username: martha
1551 [1] INFO Versa Secure Access (null) - Successfully configured default Username for registration
```

--restart_ipsec_service_on_disconnect

To restart the IPsec policy agent service when a user disconnects, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --restart_ipsec_service_on_disconnect true
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --restart_ipsec_service_on_disconnect true
645 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.0_aa6f120a
686 [1] INFO Versa Secure Access (null) - Setting restart IPSec service on user disconnect to: True
1116 [1] INFO Versa Secure Access (null) - Successfully set IPSec service restart on user disconnect to: True!
```

To disable the restarting of the IPsec policy agent service when a user disconnects, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --restart_ipsec_service_on_disconnect false
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --restart_ipsec_service_on_disconnect false
648 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.0_aa6f120a
693 [1] INFO Versa Secure Access (null) - Setting restart IPSec service on user disconnect to: False
1104 [1] INFO Versa Secure Access (null) - Successfully set IPSec service restart on user disconnect to: False!
```

--prefer_ie_browser_engine

To use the Internet Explorer (IE) browser for SAML authentication, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --prefer_ie_browser_engine true
```

For example:

```
C:\VSA>VersaSecureAccessClientConsole.exe client --prefer_ie_browser_engine true
662 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.0_aa6f120a
710 [1] INFO Versa Secure Access (null) - Use IE Engine as preferred browser control: True
1099 [1] INFO Versa Secure Access (null) - Successfully set IE as preferred browser engine!
```

To disable use of the Internet Explorer browser for SAML authentication, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --prefer_ie_browser_engine false
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --prefer_ie_browser_engine false
657 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.0_aa6f120a
701 [1] INFO Versa Secure Access (null) - Use IE Engine as preferred browser control: False
1078 [1] INFO Versa Secure Access (null) - Successfully reset preferred browser engine to default value!
```

--sub_optimal_gateway_disconnect_delay

Use this command to configure the disconnect time for a non-optimal gateway. When connecting to a dynamic optimal gateway, the client establishes a new connection with a lower metric without disconnecting the old tunnel. The old, or non-optimal, tunnel automatically disconnects after 30 minutes. Automatic reconnection occurs only when the optimal gateway is disconnected.

To configure the sub-optimal gateway disconnect delay, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --sub_optimal_gateway_disconnect_delay
delay-time-in-seconds
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --sub_optimal_gateway_disconnect_delay 10
seconds
574 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.0_aa6f120a
617 [1] INFO Versa Secure Access (null) - Set sub-optimal gateway auto disconnect delay
855 [1] INFO Versa Secure Access (null) - Success!
```

--enable_eip

An endpoint information profile (EIP) can classify endpoints based on multiple types of endpoint posture information. To protect the endpoints in an enterprise network, you can create EIP profiles, which define rules that allow the VOS SASE software to filter information from endpoint device traffic and then match information to enforce security policy. Endpoint information ensures that remote hosts maintain and adhere to enterprise

security standards before they access the network resources. You can configure a notification that alerts users about the reason for access denial and another that allows users to access the installation program for the missing software. For more information, see [Configure Endpoint Information Profiles](#).

EIP is enabled by default for the SASE client. To disable EIP, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --enable_eip false
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --enable_eip false
575 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.0_aa6f120a
614 [1] INFO Versa Secure Access (null) - Turning OFF EIP feature.
887 [1] INFO Versa Secure Access (null) - Success!
887 [1] INFO Versa Secure Access (null) - Configure EIP collection preference.
925 [1] INFO Versa Secure Access (null) - Success!
```

To re-enable EIP, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --enable_eip true
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --enable_eip true
585 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.0_aa6f120a
666 [1] INFO Versa Secure Access (null) - Turning ON EIP feature.
933 [1] INFO Versa Secure Access (null) - Success!
933 [1] INFO Versa Secure Access (null) - Configure EIP collection preference.
986 [1] INFO Versa Secure Access (null) - Success!
```

--enable_realtime_eip

To enable real-time EIP, issue the following CLI command. Note that **--enable_realtime_eip** is disabled if you set **--enable_eip** to False. This command requires an administrator login.

```
C:\VSA> VersaSecureAccessClientConsole.exe client --enable_realtime_eip true
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --enable_realtime_eip true
682 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.7_ce167b8e
842 [1] INFO Versa Secure Access (null) - Turning ON EIP feature. DisableRealTimeEIPCollection.
1759 [1] INFO Versa Secure Access (null) - Success!
1761 [1] INFO Versa Secure Access (null) - Configure Realtime EIP collection preference.
1889 [1] DEBUG Versa Secure Access (null) - IsEIPSupported: True
```

--auto_update_defer_limit

Use this command to configure the maximum allowed limit, in days, to defer an automatic software update. The range is 1 through 5 days.

To set the auto update defer limit, issue the following CLI command. This command requires an administrator login.

```
C:\VSA> VersaSecureAccessClientConsole.exe client --auto_update_defer_limit 1 through 5
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --auto_update_defer_limit 3
575 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.0_aa6f120a
607 [1] INFO Versa Secure Access (null) - Set Auto Update defer limit
857 [1] INFO Versa Secure Access (null) - Success!
```

--auto_disconnect_interval

Use this command to configure the tunnel automatic disconnecter, in minutes. You configure this on the Versa Secure Access portal and then share the configuration with the SASE client during registration or reregistration. The value must be greater than or equal to 1. This command requires an administrator login.

```
C:\VSA> VersaSecureAccessClientConsole.exe client --auto_disconnect_interval
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --auto_disconnect_interval 2
628 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.7_ce167b8e
673 [1] INFO Versa Secure Access (null) - Set Auto Disconnect interval
1447 [1] INFO Versa Secure Access (null) - Success!
```

To reset the automatic disconnect interval, issue the following CLI command. This option is available for all registered enterprises. If you set the interval at the server and client CLI levels, the server configuration has preference.

```
C:\VSA> VersaSecureAccessClientConsole.exe client --reset_auto_disconnect_interval
```

--auto_disconnect_reminder_time

Use this option to configure the reminder time for automatic disconnection, in minutes. The value must be greater than or equal to 1. The default time is 15 minutes.

To configure the automatic disconnect reminder time, issue the following CLI command. This command requires an administrator login.

```
C:\VSA> VersaSecureAccessClientConsole.exe client --auto_disconnect_reminder_time time
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --auto_disconnect_reminder_time 20
582 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.7_ce167b8e
623 [1] INFO Versa Secure Access (null) - Set Auto Disconnect Reminder Time
917 [1] INFO Versa Secure Access (null) - Success!
```

To reset the automatic disconnect reminder time to the default value, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --reset_auto_disconnect_reminder_time
```

--prefer_popout_browser

To enable the display of a popup browser for SAML authentication, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --prefer_popout_browser true
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --auto_disconnect_reminder_time 20
582 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.7_ce167b8e
623 [1] INFO Versa Secure Access (null) - Set Auto Disconnect Reminder Time
917 [1] INFO Versa Secure Access (null) - Success!
```

To disable the display of a popup browser for SAML authentication, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --prefer_popout_browser false
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --prefer_popout_browser false
698 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.7_ce167b8e
745 [1] INFO Versa Secure Access (null) - Use pop out browser as preferred for web authentication: False
1205 [1] INFO Versa Secure Access (null) - Successfully reset pop out browser preference
```

--display_vpn_profile_in_os

To enable the listing of the VPN profile in the Windows network settings, issue the following CLI command. The default value is false. This command requires an administrator login.

```
C:\VSA> VersaSecureAccessClientConsole.exe client --display_vpn_profile_in_os true
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --display_vpn_profile_in_os true
578 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.7_ce167b8e
618 [1] INFO Versa Secure Access (null) - Display VPN Profile in OS : True
888 [1] INFO Versa Secure Access (null) - Successfully set "Display VPN Profile in OS" preference!
```

To disable the listing of the VPN profile in the Windows network settings, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --display_vpn_profile_in_os false
```

--auto_register_max_retry_count

Use this option to set the limit for the maximum number of attempts for automatic registration. The value must be greater than or equal to 1.

To set the maximum retry count, issue the following command. This command requires an administrator login.

```
C:\VSA> VersaSecureAccessClientConsole.exe client --auto_register_max_retry_count limit
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --auto_register_max_retry_count 5
614 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.7_ce167b8e
659 [1] INFO Versa Secure Access (null) - The requested operation requires elevation.
```

--reset_auto_register_max_retry_count

To reset the retry count for automatic registration, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --reset_auto_register_max_retry_count " "
```

--prefer_gateway_assisted_tnd

To prioritize gateway-assisted trusted network detection over trusted hostname-based network detection when both networks are configured, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --prefer_gateway_assisted_tnd true
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --prefer_gateway_assisted_tnd true
706 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.7_ce167b8e
751 [1] INFO Versa Secure Access (null) - Use gateway assisted trusted network detection: True
1212 [1] INFO Versa Secure Access (null) - Successfully set gateway assisted trusted network detection
method as preferred!
```

To disable this prioritization, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --prefer_gateway_assisted_tnd false
```

--enable_tls_tunnel and --enable_dtls_tunnel

By default, TLS and DTLS tunnels are disabled. When you enable TLS Tunnel or DTLS tunnel, the client tries to establish a tunnel based on the tunnel type order it receives from the portal. If the first attempt fails, the client tries to connect to the next tunnel type in the configuration order. If you have administrator privileges, you can enable or disable these tunnels using the CLI:

To enable TLS tunnel, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --enable_tls_tunnel true
```

To disable TLS tunnel, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --enable_tls_tunnel true
```

To enable DTLS tunnel, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --enable_dtls_tunnel true
```

To disable DTLS tunnel, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --enable_dtls_tunnel true
```

--fetch_username_from_certificate

To fetch username from personal certificate store, issue the following CLI command. For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe client --fetch_username_from_certificate true|false --  
cert_issuer  
certificate issuer name --username_field CN | SAN --san_match_regex regex
```

Display and Execute Monitor Options

To view the monitor options, issue the following CLI command:

```
C:\Program Files (x86)\Versa Secure Access> VersaSecureAccessClientConsole.exe monitor --help
```

For example:

```
C:\Program Files (x86)\Versa Secure Access> VersaSecureAccessClientConsole.exe monitor --help  
VersaSecureAccessClientConsole 7.8.0.0  
  
--tunnel_monitor          [Deprecated] (true|false). Enable/Disable tunnel monitoring  
--tunnel_monitor_interval [Deprecated] Tunnel monitor interval in seconds. (Range 10-600)  
--tunnel_monitor_retry_interval [Deprecated] Interval between each retry for tunnel monitoring in  
seconds. (Range 1-5)  
--tunnel_monitor_retry_count [Deprecated] Number of retry attempts before concluding the tunnel is  
down. (Range 1-5)  
--help                    Display this help screen.  
--version                  Display version information.
```

--tunnel_monitor

To enable tunnel monitoring, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe monitor --tunnel_monitor true
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe monitor --tunnel_monitor true  
296 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e  
343 [1] INFO Versa Secure Access (null) - Configure DNS monitoring.  
511 [1] INFO Versa Secure Access (null) - Success!
```

To disable tunnel monitoring, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe monitor --tunnel_monitor false
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe monitor --tunnel_monitor false
294 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
334 [1] INFO Versa Secure Access (null) - Configure DNS monitoring.
495 [1] INFO Versa Secure Access (null) - Success!
```

--tunnel_monitor_interval

To configure the tunnel monitoring interval, in seconds, issue the following CLI command. The range is 10 through 600 seconds.

```
C:\VSA> VersaSecureAccessClientConsole.exe monitor --tunnel_monitor_interval seconds
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe monitor --tunnel_monitor_interval 30
623 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
930 [1] INFO Versa Secure Access (null) - Configure tunnel monitoring interval
1525 [1] INFO Versa Secure Access (null) - Success!
```

--tunnel_monitor_retry_interval

Use this option to configure the interval, in seconds, between each try before concluding the tunnel is down. The range is 1 through 5 seconds.

To configure the tunnel monitor retry interval, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe monitor --tunnel_monitor_retry_interval seconds
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe monitor --tunnel_monitor_retry_interval 4
321 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
368 [1] INFO Versa Secure Access (null) - Configure DNS monitor retry interval.
716 [1] INFO Versa Secure Access (null) - Success!
```

--tunnel_monitor_retry_count

To configure the maximum number of retry attempts before concluding the tunnel is down, issue the following CLI command. The range is 1 through 5.

```
C:\VSA> VersaSecureAccessClientConsole.exe monitor --tunnel_monitor_retry_count retries
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe monitor --tunnel_monitor_retry_interval 4
321 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
368 [1] INFO Versa Secure Access (null) - Configure DNS monitor retry interval.
716 [1] INFO Versa Secure Access (null) - Success!
```

Display and Execute Service Options

To view the service options, issue the following CLI command:

```
C:\Program Files (x86)\Versa Secure Access> VersaSecureAccessClientConsole.exe service --help
```

For example:

```
C:\Program Files (x86)\Versa Secure Access>VersaSecureAccessClientConsole.exe service --help
VersaSecureAccessClientConsole 7.8.7.0

--enable_apptunnel          (true|false). Enable/Disable App tunnel driver
--fail_open_mode            [Deprecated] Set driver to fail open mode
--fail_close_mode          [Deprecated] Set driver to fail close mode
--restricted_access_fallback_duration [Deprecated] Duration in seconds for which Restricted Access will
be relaxed, when user disables Restricted Access. Restricted Access would be enabled back after
the duration completes (Range: 5 - 600)
--allow_domains             Allow domains/FQDNs in fail close mode. ex for domain: .versa-networks.
com, OR ".versa-networks.com .office365.com" ex for FQDN: test.versa-networks.com, OR
"test.versa-networks.com test.office365.com"
--reset_domains            Remove domains/FQDNs that were allowed in fail close mode. ex for
domain: ".versa-networks.com, OR ".versa-networks.com .office365.com" ex for FQDN:
test.versa-networks.com, OR "test.versa-networks.com test.office365.com"
--allow_ips                Allow IP(s) in fail close mode, ex: 10.0.0.1, OR "10.0.0.1 10.0.0.2"
--reset_ips                Remove IP(s) that was allowed in fail close mode. ex: 10.0.0.1, OR "10.0.0.1
10.0.0.2"
--strict_full_tunnel       (true|false) When connected to gateway in full tunnel mode, the traffic may
go through underlay if there are any routes through underlay interface. By setting the
the option to true, routes through underlay will not be effective; the traffic will
be sent through underlay only if they match any of excluded domain, excluded
application, excluded subnets or trusted subnets. When the option is set to false:
The routes will influence traffic through underlay or any other interface
--trusted_subnets         Trusted subnets to be excluded in case of full-tunnel and semi trusted
modeEx: 192.168.1.0/24 OR "192.168.1.0/24 192.168.2.0/24"
--reset_trusted_subnets   Reset the trusted subnets which are excluded in case of full-tunnel and
semi trusted modeEx: 192.168.1.0/24 OR "192.168.1.0/24 192.168.2.0/24"
--clean_dns_nrpt_rule      Clean all stale DNS NRPT rules
--exclude_subnets         Add one or more subnets to be excluded in case of full-tunnelEx: 192.168.
1.0/24 OR "192.168.1.0/24 192.168.2.0/24"
--reset_exclude_subnets   Remove one or more subnets which are excluded in case of full-
tunnelEx: 192.168.1.0/24 OR "192.168.1.0/24 192.168.2.0/24"
--apptunnel_bypass_application Command to add application(s) to Versa Client bypass list.The
traffic originated by these bypassed applications won't be processed by Versa client.Use this
```

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Director/Versa_SASE_Client/Use_the_V...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Director/Versa_SASE_Client/Use_the_V...)

Updated: Wed, 23 Oct 2024 08:43:16 GMT

Copyright © 2024, Versa Networks, Inc.

command to

Ex: red.exe OR " blue.exe black.exe"

--apptunnel_bypass_application_reset Command to clear the list of applications that were bypassed from Versa Client

--apptunnel_list_bypassed_applications Command to show the list of applications that were bypassed from Versa Client

--block_icmp_on_fail_close (true|false) Block ICMP Traffic in Fail-Close Mode

--Allow_Excluded_Application_traffic_on_fail_close (true|false) Allow Excluded Application Traffic in Fail-Close Mode

--exclude_service Allows TCP/UDP traffic to be excluded for the specified Port and IP when in full-tunnel.

Ex: Exclude based on Service and Ports: "TCP::1002" or "TCP::1002:1003:1004"

Exclude based on Service with Ports and IP: "TCP::1002|10.0.0.1, 10.0.0.2"

Exclude based on Service with Ports and IP Prefix: "TCP::1002|10.0.0.1/24" or "TCP::1002|10.0.0.1/24,10.0.0.2/24" or "TCP::1002|10.0.0.1/24,10.0.0.2/24:1003|10.0.0.3/24,10.0.0.4/24"

--reset_exclude_service Removes TCP/UDP traffic exclusions which were added using exclude_service command.

Ex: Remove exclusion based on Service and Ports: "TCP::1002" or "TCP::1002:1003:1004"

Remove exclusion based on Service with Ports and IP: "TCP::1002|10.0.0.1, 10.0.0.2"

Remove exclusion based on Service Ports and IP Prefix: "TCP::1002|10.0.0.1/24" or "TCP::1002|10.0.0.1/24,10.0.0.2/24" or "TCP::1002|10.0.0.1/24,10.0.0.2/24:1003|10.0.0.3/24,10.0.0.4/24"

--help Display this help screen.

--version Display version information.

--enable_apptunnel

Use this option to enable the application tunnel driver to enable application and domain-based traffic steering and fail-mode services. Note that to issue these commands, you must have administrator privileges and you must be at the administrator command prompt.

To enable the application tunnel driver for SASE client, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe monitor service --enable_apptunnel true
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --enable_apptunnel true
309 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
350 [1] INFO Versa Secure Access (null) - Enable App Tunnel Driver
859 [1] INFO Versa Secure Access (null) - Success!
```

To disable the application tunnel driver for SASE client, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe monitor service --enable_apptunnel false
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --enable_apptunnel false
277 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
315 [1] INFO Versa Secure Access (null) - Disable App Tunnel Driver
```

--fail_open_mode

To set the application tunnel driver to FAIL_OPEN mode for the client to allow all outgoing traffic when the client is not connected to a gateway, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --fail_open_mode
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --fail_open_mode
356 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
412 [1] INFO Versa Secure Access (null) - Setting apptunnel driver mode to FAIL_OPEN
803 [1] INFO Versa Secure Access (null) - Success!
```

--fail_close_mode

To set the application tunnel driver to FAIL_CLOSE mode for the client to block all outgoing traffic (except ICMP, allowed domains, and IP addresses) when the client is not connected to a gateway, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --fail_close_mode
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --fail_close_mode
279 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
316 [1] INFO Versa Secure Access (null) - Setting Apptunnel driver mode to FAIL_CLOSE
450 [1] INFO Versa Secure Access (null) - Success!
```

--restricted_access_fallback_duration

Use this option to configure the duration, in seconds, after which restricted access is enabled again. The range is 5 through 500 seconds. When a user enables restricted access, it is disabled for the specified amount of time and then re-enabled. Note that to issue this command, you must have administrator privileges and you must be at the administrator command prompt.

To configure the restricted access fallback duration, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --restricted_access_fallback_duration
seconds
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --restricted_access_fallback_duration 120
278 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
454 [1] INFO Versa Secure Access (null) - Success!
```

--allow_domains

Use this option to enable domain traffic in FAIL_CLOSE mode. You can specify the domains to be allowed if the tunnel is not connected and FAIL_CLOSE mode is enabled. Note that to issue the commands to enable or disable domains in FAIL_CLOSE mode, you must have administrator privileges and you must be at the administrator command prompt.

To allow domains in FAIL_CLOSE mode, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --allow_domains domain-name
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --allow_domains money.com
282 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
321 [1] INFO Versa Secure Access (null) - Registering domain money.com to whitelist
536 [1] INFO Versa Secure Access (null) - Restarting Services...
615 [1] INFO Versa Secure Access (null) - Success!
```

--reset_domains

To disable or remove domains that were allowed in FAIL_CLOSE mode, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --reset_domains domain-name
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe" service --reset_domains money.com
278 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
315 [1] INFO Versa Secure Access (null) - Unregistering domain money.com from whitelist
484 [1] INFO Versa Secure Access (null) - Restarting Services...
538 [1] INFO Versa Secure Access (null) - Success!
```

--allow_ips

Use this option to enable or allow IP addresses in FAIL_CLOSE mode. Note that to issue the commands to enable or disable IP addresses in fail close mode, you must have administrator privileges and you must be at the administrator command prompt.

To allow IP addresses in FAIL_CLOSE mode, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --allow_ips ip-address
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --allow_ips 10.10.10.10
279 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
317 [1] INFO Versa Secure Access (null) - Registering IP 10.10.10.10 to whitelist
514 [1] INFO Versa Secure Access (null) - Restarting Services...
567 [1] INFO Versa Secure Access (null) - Success!
```

--reset_ips

To disable or remove IP addresses that were allowed in FAIL_CLOSE mode, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --reset_ips ip-address
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe" service --reset_ips 10.10.10.10
281 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.5.9_6f38b04e
318 [1] INFO Versa Secure Access (null) - Unregistering IP 10.10.10.10 from whitelist
533 [1] INFO Versa Secure Access (null) - Restarting Services...
588 [1] INFO Versa Secure Access (null) - Success!
```

--strict_full_tunnel

Configure strict full tunnel (administrator mode). When the client connects to a gateway in full tunnel mode, the traffic may go through underlay if there are routes through underlay interface. If you enable strict full tunnel, routes through underlay are not effective, and traffic is sent through underlay only if they match any of excluded domain, excluded application, excluded subnets, or trusted subnets. When you disable strict full tunnel, routes influence traffic through underlay or any other interface.

To enable strict full tunnel, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --strict_full_tunnel true
```

For example:

```
C:\VSA>VersaSecureAccessClientConsole.exe service --strict_full_tunnel true
591 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.0_aa6f120a
630 [1] INFO Versa Secure Access (null) - Set strict full tunnel: True
907 [1] INFO Versa Secure Access (null) - Success!
```

To disable strict full tunnel, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --strict_full_tunnel false
```

For example:

```
C:\VSA>VersaSecureAccessClientConsole.exe service --strict_full_tunnel false
571 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.0_aa6f120a
609 [1] INFO Versa Secure Access (null) - Set strict full tunnel: False
852 [1] INFO Versa Secure Access (null) - Success!
```

--trusted_subnets

You can configure trusted subnets that bypass the tunnel. In semitrusted mode, the SASE client establishes a tunnel to the SASE gateway even when a trusted host is reachable without the tunnel. You can use semitrusted mode in deployments in which the site or branch CPE does not have a secure tunnel connection to the SASE gateway. The client establishes a tunnel to the gateway for all traffic expect for traffic to trusted subnets.

To configure trusted subnets, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --trusted_subnets subnet
```

For example:

```
C:\VSA>VersaSecureAccessClientConsole.exe service --trusted_subnets 192.168.1.0/24  
576 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.7_ce167b8e  
618 [1] INFO Versa Secure Access (null) - Registering trusted subnets 192.168.1.0/24  
891 [1] INFO Versa Secure Access (null) - Success!
```

To configure multiple trusted subnets, enclose the subnets in quotation marks; for example, "192.168.1.0/24 192.168.2.0/24".

--reset_trusted_subnets

To reset trusted subnets, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --reset_trusted_subnets subnet
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --reset_trusted_subnets 192.168.1.0/24  
532 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.2_6ab2577f  
569 [1] INFO Versa Secure Access (null) - Unregistering trusted subnets 192.168.1.0/24  
817 [1] INFO Versa Secure Access (null) - Success!
```

--clean_dns_nrpt_rule

To clear all stale DNS name resolution policy table (NRPT) rules, issue the following CLI command:

```
C:\VSA>VersaSecureAccessClientConsole.exe service --clean_dns_nrpt_rule
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --clean_dns_nrpt_rule  
652 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.0_aa6f120a  
695 [1] INFO Versa Secure Access (null) - Clear DNS NRPT Rules  
1513 [1] INFO Versa Secure Access (null) - Success!
```

--exclude_subnets

Use this option to exclude one or more subnets from a full tunnel. When you configure a full tunnel, all traffic redirects through the tunnel interface. When you exclude a subnet from a full tunnel, the subnet's traffic goes through the default underlay instead of over the tunnel.

To exclude subnets, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --exclude_subnets subnets
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --exclude_subnets 192.168.2.0/24
581 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.0_aa6f120a
620 [1] INFO Versa Secure Access (null) - Excluding subnets 192.168.2.0/24
984 [1] INFO Versa Secure Access (null) - Success!
```

--reset_exclude_subnets

To remove one or more subnets that have been excluded from a full tunnel, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --reset_exclude_subnets subnets
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --reset_exclude_subnets 192.168.2.0/24
546 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.2_6ab2577f
583 [1] INFO Versa Secure Access (null) - Reset excluded subnets 192.168.2.0/24
830 [1] INFO Versa Secure Access (null) - Success!
```

--apptunnel_bypass_application

Use this option to add applications to the bypass list of the SASE client so that the client does not process traffic that originates from the bypassed applications. For example, you can use red.exe, blue.exe, or black.exe to bypass these applications. Issuing this command requires admin login.

To add applications to the bypass list, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --apptunnel_bypass_application application-
name
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --apptunnel_bypass_application black.exe
709 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.7_ce167b8e
929 [1] DEBUG Versa Secure Access (null) - executable name: black.exe
1676 [1] INFO Versa Secure Access (null) - Success!
```

--apptunnel_bypass_application_reset

To clear or reset the bypass list of applications, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --apptunnel_bypass_application_reset
```

--apptunnel_list_bypassed_applications

To display applications that the client bypasses, issue the following CLI command. This command requires an administrator login.

```
C:\VSA> VersaSecureAccessClientConsole.exe service --apptunnel_list_bypassed_applications
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --apptunnel_list_bypassed_applications
613 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.7_ce167b8e
677 [1] INFO Versa Secure Access (null) - ByPass Application List
ByPass application: black.exe
ByPass application: red.exe
ByPass application: blue.exe
743 [1] INFO Versa Secure Access (null) - Success!
```

--block_icmp_on_fail_close

To allow ICMP traffic in FAIL_CLOSE mode, issue the following CLI command. This command requires an administrator login.

```
C:\VSA> VersaSecureAccessClientConsole.exe service --block_icmp_on_fail_close true
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --block_icmp_on_fail_close true
605 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.7_ce167b8e
656 [1] INFO Versa Secure Access (null) - Set Block ICMP in Fail Close Mode: True
1044 [1] INFO Versa Secure Access (null) - Success!
```

To disable ICMP traffic in FAIL_CLOSE mode, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --block_icmp_on_fail_close false
```

--Allow_Excluded_Application_traffic_on_fail_close

To allow DNS traffic for excluded applications in FAIL-CLOSE mode, issue the following CLI command. This command requires an administrator login.

```
C:\VSA> VersaSecureAccessClientConsole.exe service --Allow_Excluded_Application_traffic_on_fail_close true
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --Allow_Excluded_Application_traffic_on_fail_close true
624 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.7_ce167b8e
673 [1] INFO Versa Secure Access (null) - Set Allow Excluded Application Traffic in Fail Close Mode: True
994 [1] INFO Versa Secure Access (null) - Success!
```

To disable DNS traffic for excluded applications in FAIL_CLOSE mode, issue the following CLI command:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --Allow_Excluded_Application_traffic_on_fail_close false
```

--exclude_service

To exclude TCP/UDP traffic based on service, port number, and IP address when in full-tunnel mode, issue the following CLI command:


```
C:\VSA> Versa Secure Access>VersaSecureAccessClientConsole.exe service --exclude_service  
service-name
```

For example:

```
C:\VSA> VersaSecureAccessClientConsole.exe service --exclude_service TCP::1002  
624 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.8.7_ce167b8e  
1843 [1] INFO Versa Secure Access (null) - Exclude services is set: True
```

--reset_exclude_service

To remove or reset traffic exclusions, issue the following CLI command:

```
C:\VSA> Versa Secure Access>VersaSecureAccessClientConsole.exe service --reset_exclude_  
service service-name
```

For example:

```
C:\VSA> Versa Secure Access>VersaSecureAccessClientConsole.exe service --reset_exclude_  
service TCP::1002
```

Supported Software Information

VOS Releases 20.2.2 and later support all content described in this article, except:

- For Releases 21.2.1 and later, if TOTP authentication is required, a screen with a QR code displays; add support for Windows and MacOS clients.

SASE Client Releases 7.2.0 and later support all content described in this article.

Additional Information

[Configure Endpoint Information Profiles](#)

[Configure Pre-Login for the Versa Secure Access Client](#)

[Configure User and Group Policy](#)

[Configure the Versa SASE Client To Select the Best Gateway](#)

[Configure the Versa Secure Access Service](#)

[Configure Versa SASE Clients](#)

[Enable SAML Authentication](#)

[Troubleshoot the SASE Client](#)