Troubleshoot the SASE Client

For supported software information, click here.

This article describes some of the error messages that an end user might see when using the Versa SASE client and the reasons that the errors might occur. However, it does not cover all the issues that might be caused by the underlying operating system, because there can be various conditions that differ for each operating system and platform.

This article also describes a few cases when the VSA service might become unavailable so that an MSP can appropriately assign these issues to the Versa Networks Managed Services NOC team.

The article describes errors from an end customer perspective. It is not applicable if you are using VSA or Versa SASE services from the cloud, and it assumes that the MSP has no access to any troubleshooting on the VSA or SASE gateways that are managed by the Versa Managed Services team.

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

Flow of SASE Client Connectivity

To understand the SASE client error messages, you must understand the normal flow of events when an end user connects to an enterprise using the SASE client.

The following steps describe these events:

1. End user downloads the SASE client software using the link provided by Versa Networks.
2. End user installs the SASE client on the client device by following instructions provided.
3. During the installation, a Versa root authority certificate is pushed to the client and installed in the user's certificate trust store. For this to occur, the user must have administrative privileges on the client.
4. Client registers using the following information provided by the enterprise's IT administrator: the FQDN of the registrar portal FQDN, the name of the enterprise as configured on the gateways, and the user credentials.
5. When the registration successfully authenticates the user, the portal pushes a set of Versa SASE profiles based on the username, user group, device, and posture to the client. The SASE profiles determine the connection type, the selection of the gateways to which the client can connect, the encryption standards to use, the traffic-steering policies, and other parameters. The connection to the gateway can be manual or automatic depending on the policies.
6. When the connection successfully establishes, the client uses the IP address assigned to it.

7. End user can then use the SASE client to access their corporate internal network, and to access general public networks and applications. Access depends on the policies that the gateway pushes to the end user's device.

8. If the end user wants to disconnect from the private network, they can click Disconnect, if the option is available. If Always On is enabled on the end user's device, you cannot disconnect the client.

SASE client Error Message Categories

There are eight categories of SASE client errors. The initial owner of each error category is the end user, the customer IT department, or Versa Networks. The following are the SASE client error categories organized by who is responsible for addressing the error condition:

- End user or the customer IT department
    - Authentication errors
    - Configuration errors
    - Internet connectivity errors
    - Network access errors
    - Operating system errors
- Versa Networks
    - Client application errors
    - Gateway connectivity errors
    - Unknown errors

Error Messages Reported on the SASE client

This section describes the error messages reported on the SASE client. This section lists the error messages in an order as described Flow of SASE Client Connectivity above.

Error Message: **Your attention is needed to restore internet**
Error Message: **You are not connected to the internet. Please check your connection.**

Description	There is no Internet connection for the client device to reach the registrar portal or the cloud gateway.
Error type	Internet connectivity
Responsible party	End user, customer IT team
Possible reasons	- The device does not have Internet connection. - Interface failed because of operating system issues. - Wireless network is down.

	• Internet router is up, but that are internet connection issues from the internet service provider (ISP).
Next steps	• Work with customer IT team to ensure that the details provided on the client are valid and correct. • If the details are correct, create a support ticket with Versa Networks to debug the issue further.

Error Message: **Account creation failed! Please try again later**

Description	Registration with the cloud gateway failed.
Error type	Internet connectivity
Responsible party	End user, customer IT team
Possible reasons	• Registration information provided for the client are incorrect. • Registration portal rejected the registration process.
Next steps	• Work with customer's IT team to ensure that the details provided on the client are valid and correct. • If the details are correct, create a support ticket with Versa Networks to debug the issue further.

Error Message: **Please enter all the fields to add a connection! Cancel otherwise**

Description	Not all registration values are provided.
Error type	Configuration
Responsible party	End user, customer IT team
Possible reasons	• Not all the values required for registration have been provided on the SASE client.

Next steps	• Work with customer's IT team to obtain and enter all necessary details provided on the Versa client.

Error Message: Change password failed! Please enter correct OTP and then resubmit

Description	Procedure to change the password has failed because the OTP entered is incorrect.
Error type	Authentication
Responsible party	End user
Possible reasons	• User did not provide correct the OTP values during the password change procedure. • The OTP expired, as the user took longer than the expiry time to enter the password during password change.
Next steps	• Initiate the password reset process again on the client agent to obtain a new OTP and use the new OTP to reset the password.

Error Message: Passwords don't match! Please use same password and then submit

Description	During the password reset process, the user is prompted twice to enter the new password. The two passwords do not match.
Error type	Authentication
Responsible party	End user
Possible reasons	• User entered the passwords incorrectly.
Next steps	• Initiate the password reset option again, and enter the details correctly.

Error Message: **Authentication failed! Please check Username and Password, and then resubmit**

Description	The credentials provided for user authentication are incorrect.
Error type	Authentication
Responsible party	End user, customer IT team, Versa Networks
Possible reasons	• User did not provide the correct username/password combination for registration or for the connection process. • The IT Administrator did not enter the correct details on the identity provider (IdP).
Next steps	• End user should try again with correct credentials. • If the failure is not resolved, work with the customer's IT team to verify the credentials and, if necessary, to reset the credentials on the IdP. • If the failure is still not resolved, contact the Versa Networks Managed Services NOC to debug the client issues.

Error Message: **OTP verification failed! Please enter correct OTP and then resubmit**

Description	User has not entered the correct one-time password (OTP) during the multifactor authentication (MFA) authentication process
Error type	Authentication
Responsible party	End user
Possible reasons	• User did not provide the correct OTP. • The OTP has expired.
Next steps	• Initiate the credential validation again to obtain a new OTP, and then resubmit.

Error Message: **Password has expired! Please use your new password**

Description	User password has expired.
Error type	Authentication
Responsible party	End user, customer IT team
Possible reasons	• User password expired as the result of the password expiration policy on the IdP.
Next steps	• Initiate the password reset process. • Try to connect again after the password has been reset.

Error Message: **Failed to register! Please try after some time**

Description	The user was not able to connect to the registrar portal to register the device.
Error type	Gateway connectivity
Responsible party	Customer IT team, Versa Networks
Possible reasons	• Operating system issues occurred while running the SASE client software. • The Versa client is having issues reaching the Versa Networks gateway. • There may be configuration issues with the Versa networks gateway.
Next steps	• End user must work with the customer IT team to ensure that there is no issue with the operating system. • Create a support ticket with the Versa Managed Services NOC team to debug the issue further.

Error Message: **Failed to connect! Please try after some time**

Description	The user was not able to connect to the registrar portal

	to register the device.
Error type	Gateway connectivity
Responsible party	Customer IT team, Versa Networks
Possible reasons	• Operating system issues occurred while running the SASE client software. • The Versa client is having issues reaching the Versa Networks gateway. • There may be configuration issues with the Versa networks gateway.
Next steps	• End user should work with the customer IT team to ensure that there is no issue with the operating system. • Create a support ticket with the Versa Managed Services NOC team to debug the issue further.

Error Message: **Failed to connect! Please restore your Internet connection and try again**

Description	Client is not able to access Internet to reach the Versa Cloud Gateway (VCG).
Error type	Internet connectivity
Responsible party	Customer IT team
Possible reasons	• Failure to reach the internet.
Next steps	• End user should work with the customer IT team to restore Internet connectivity on the user device.

Error Message: **Permission Denied or Config Error! Please allow VPN configuration to connect**

Description	The profile pushed during the registration process failed. The user did not allow the configuration to be saved on the device. This is error message usually seen on MacOS.

Error type	Configuration
Responsible party	End user
Possible reasons	• On MacOS, the user should accept the configuration profile that is pushed by the registrar portal during the registration process. If the profile is not accepted, the client is unable to use the profile to connect to the VCG.
Next steps	• End user should accept or allow the configuration that was pushed, and then retry connection to the VCG.

Error Message: Tunnel network identified! Tunnel bypassed

Description	Client does not trust the cloud gateway and hence is bypassing the tunnel.
Error type	Gateway connectivity
Responsible party	Versa Networks
Possible reasons	• The certificate on the gateway has expired or has some issues. • The Certificate Authority (CA) on the user device does not recognize the certificate presented by the gateway.
Next steps	• Create a support ticket with the Versa Managed Services NOC team to debug the issue further.

Error Message: Service Restart Failed! Please retry after some time

Description	On MacOS, internal services restart after the initial configuration has failed.
Error type	Operating system
Responsible party	Versa Networks

Possible reasons	• Possible issues with MacOS. • Possible issues with Versa client on MacOS.
Next steps	• Create a support ticket with the Versa Managed Services NOC team to debug the issue further.

Error Message: **Failed to connect! System would reconnect in 60 seconds**

Description	The Versa Client is not able to connect to the VCG even though it has detected that the gateway is reachable.
Error type	Gateway connectivity
Responsible party	End user, Versa Networks
Possible reasons	• Possible internet congestion-related issues at the user device. • Possible internet congestion or reliable connection issues at the VCG.
Next steps	• Wait some amount time for the internet at the user device to get more reliable. • Create a support ticket with the Versa Managed Services NOC team to debug the issue further.

Error Message: **Unknown Error Occurred**

Description	The Versa client is not able to connect, but the error is an unexpected one.
Error type	Unknown
Responsible party	Customer IT team, Versa Networks
Possible reasons	• Possible issues with the 0perating system or Versa client.

Next steps	• Create a support ticket with the Versa Managed Services NOC team to debug the issue further.

Error Message: Failed to Reconnect. Please try connect manually.

Description	Graceful restart from the client has failed, and manual intervention or attention required.
Error type	Gateway connectivity
Responsible party	Customer IT team, Versa Networks
Possible reasons	• The client tries to reconnect automatically to the VCG when a connection fails, but is unable to reconnect.
Next steps	• Create a support ticket with the Versa Managed Services NOC team to debug the issue further.

Error Message: Check DNS settings OR choose different server and connect

Description	DNS resolution to the preferred VCG has failed.
Error type	Internet connectivity
Responsible party	Customer IT team, Versa Networks
Possible reasons	• Client is unable to connect to the VCG because the FQDN of the gateway cannot be resolved to an IP address, possibly because the DNS server is not reachable from the client. • The gateway is down and has not responded.
Next steps	• Customer IT team should resolve DNS settings for the client device. • Choose an alternate gateway from the drop-down list, and use it while the customer IT team is resolving the DNS settings.

	• Choose alternate DNS servers on the client device.
	• Create a support ticket with the Versa Managed Services NOC team to debug the issue further.

Error Message: Check DNS settings OR use alternate FQDN for registration

Description	DNS resolution to the Versa registration has failed.
Error type	Internet connectivity
Responsible party	Customer IT team, Versa Networks
Possible reasons	• Client is unable to resolve the DNS address, possibly because the DNS server is not reachable.
Next steps	• Customer IT team should resolve DNS settings for the client device. • Choose an alternate registrar portal from the drop-down list, and use it while the customer IT team is resolving the DNS settings. • Choose alternate DNS servers on the client device. • Create a support ticket with the Versa Managed Services NOC team to debug the issue further.

Error Message: Failed to connect to gateway group! Please try connecting to a specific gateway

Description	The Versa client chooses a best gateway from a group of gateways available for the user to connect to. While connecting to this gateway group, the Versa client is unable to connect to any available best gateway.
Error type	Gateway connectivity
Responsible party	Customer IT team, Versa Networks
Possible reasons	• Connectivity issues at the client. • All gateways are down. • Enterprise subscription has expired.

Next steps	• Create a support ticket with Versa Networks to determine whether some of the gateways are down and, if so, to determine alternative gateways to use. • If the subscription has expired, renew the subscription to the Versa service.

Error Message: Authentication failed. Disconnected from *enterprise-name*

Description	A reauthentication request from the server has failed, and the user has been disconnected from the enterprise network.
Error type	Authentication
Responsible party	End user
Possible reasons	• When the authentication server requests the user to reauthenticate for continuous security, the user did not complete the authentication process within specified time. Hence, for security reasons, the Versa client terminates the end user's connection to the gateway.
Next steps	• End user should connect to the gateway again and provide authentication credentials to connect again to their enterprise network.

Error Message: Record not found for VPN Profile *gateway-name*
Error Message: Profile not found

Description	Information the gateway that was chosen to connect is not found..
Error type	Configuration
Responsible party	End user, customer IT team, Versa Networks
Possible reasons	• Possible corruption of the configuration on the Versa Client because of operating system issues. • Possible deletion of the configuration on the Versa

	client.
	• Registration of the client did not happen correctly.
Next steps	• End user should reregister with the registration portal. • If the end user registration does not fix the issue, the customer IT team should collect debug logs and provide them to Versa Managed Service NOC team • Create a support ticket with the Versa Managed Services NOC team to debug the issue further.

Error Message: **Failed to connect. Unable to communicate to Versa Service. Please retry again**

Description	Issue with the Versa client software on a Windows machine.
Error type	Operating system
Responsible party	Customer IT team, Versa Networks
Possible reasons	• The Windows WCF service that the Versa client uses has malfunctioned. • New security software installed on the Windows machine has blocked the service from running.
Next steps	• Restart the Windows WCF service on the client device. • Restart Windows. • Create a support ticket with the Versa Managed Services NOC team to debug the issue further.

Error Message: **Failed to save configuration**

Description	Error while saving user changes made to the VPN profiles on the Versa client.
Error type	Client application, operating system
Responsible party	Customer IT team, Versa Networks

Possible reasons	• User privilege issues in the operating system. • Versa client misbehavior.
Next steps	• Customer IT team should confirm whether end user has appropriate privileges to make changes on the device. • Restart the Versa client software. • Create a support ticket with the Versa Managed Services NOC team to debug the issue further.

Error Message: **Failed to fetch the secure access servers**

Description	Error while trying to read the server details from the configuration file.
Error type	Client application, operating system
Responsible party	End user, Versa Networks
Possible reasons	• Operating system misbehavior. • Versa client misbehavior.
Next steps	• Restart the Versa client software. • Restart the device • Create a support ticket with the Versa Managed Services NOC team to debug the issue further.

Error Message: **Authentication failed! User forbidden.**

Description	During the OTP verification process, a Forbidden error was received from the server.
Error type	Authentication
Responsible party	Customer IT team
Possible reasons	• User account issues.

	• IdP is misconfigured.
Next steps	• Customer IT team to verify the user account.

Error Message: Captive Portal Detected! Your attention is needed to restore Internet.

Description	A captive portal has been detected at the customer location, possibly at a public or hotel internet location.
Error type	Internet connectivity
Responsible party	Customer IT team
Possible reasons	• User is at a location where they need to accept certain conditions before they are provided with access to the internet.
Next steps	• User must accept captive portal terms and conditions or provide a password to access the internet at the location.

Error Message: enterprise-name is already Registered

Description	User is trying to register with an enterprise name with which they have already registered.
Error type	Configuration
Responsible party	End user, customer IT team
Possible reasons	• User is trying to register with an enterprise name with which they have already registered.
Next steps	• User to obtain a different enterprise name from the customer IT team to use to register with.

Other Issues

This section describes how to handle other issues that the user might experience on the SASE client.

Issue: I am able to connect to the gateway, but I am not able to access anything on the network.

Description	The user is able to connect to any of the Versa VCGs but cannot access their private network or their applications.
Error type	Network access
Responsible party	End user, customer IT team
Possible reasons	• IPsec tunnel from the VCG to the customer network is down. • Remote application or network is down. • Internet on the gateway to connect to the customer data center is down.
Next steps	• User to work with customer IT team to resolve connectivity issue.

Issue: I am able to connect to the gateway, but I am not able to access the internet.

Description	The user is able to connect to any of the Versa VCGs but cannot access the internet using the customer network.
Error type	Network access
Responsible party	End user, customer IT team
Possible reasons	• IPsec tunnel from the VCG to the customer network is down. • Remote application or network is down. • Internet on the gateway to connect to the customer data center is down.
Next steps	• User to work with customer IT team to resolve connectivity issue.

Issue: **I am able to connect to the gateway, but able to access only a few private networks or applications.**

Description	The user is able to connect to any of the Versa VCGs and is able to access only some parts of the private network, but not others.
Error type	Network access
Responsible party	End user, customer IT team
Possible reasons	• IPsec tunnel from the VCG to the customer network is down. • Remote application or network is down. • Internet on the gateway to connect to the customer data center is down.
Next steps	• User to work with customer IT team to resolve connectivity issue.

Issue: **I am not able to connect to one of the gateways in the gateway list on the client.**

Description	The user is able to select and connect with only some of the VCGs in the list of gateways in the Versa client software, but is unable to connect with others.
Error type	Gateway connectivity
Responsible party	Versa Networks
Possible reasons	• IPsec tunnel from the VCG to the customer network is down. • Remote application or network is down. • Internet on the gateway to connect to the customer data center is down.
Next steps	Create a support ticket with the Versa Managed Services NOC team to debug the issue further.

Debug the SASE client

Perform Diagnostics

To automatically fix basic issues on the Versa Client, perform the diagnostics procedure:

1. In the SASE client home screen, click the Settings icon.
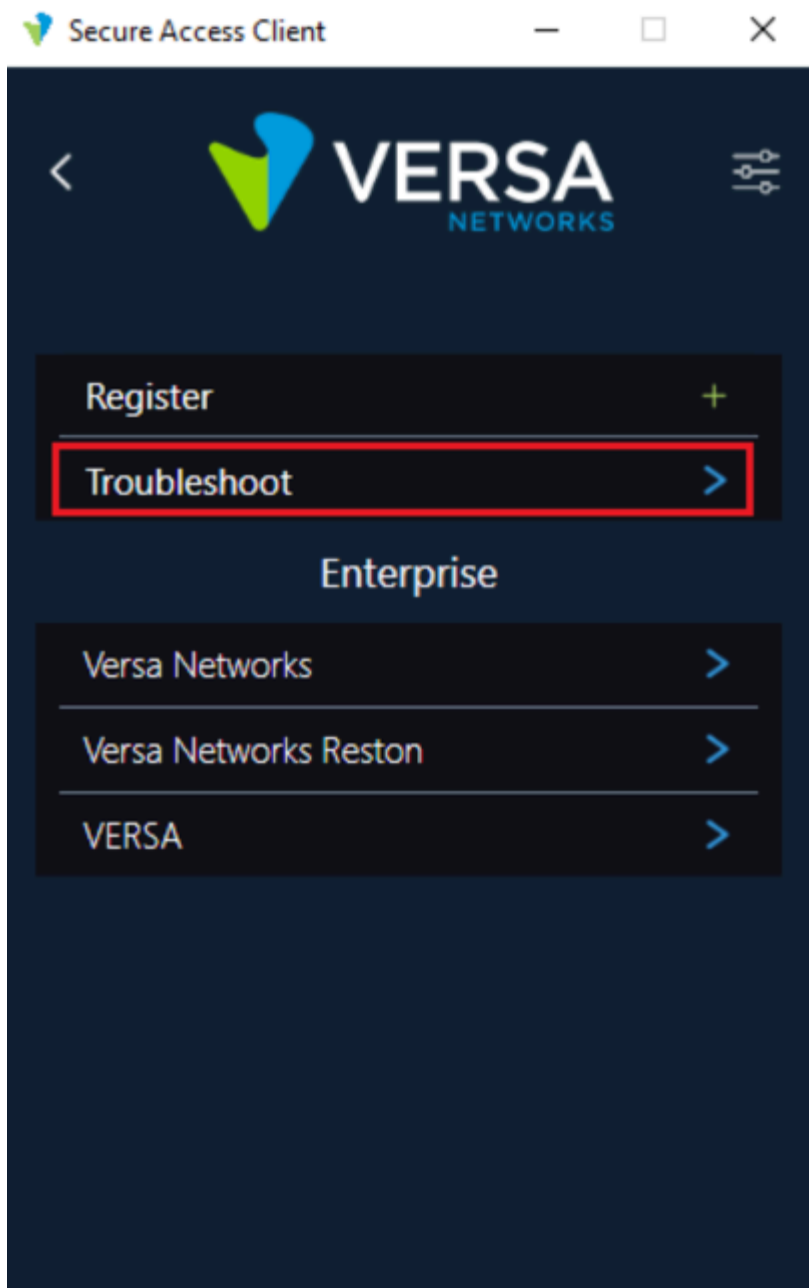2. Click Troubleshoot, and then click Diagnostics.
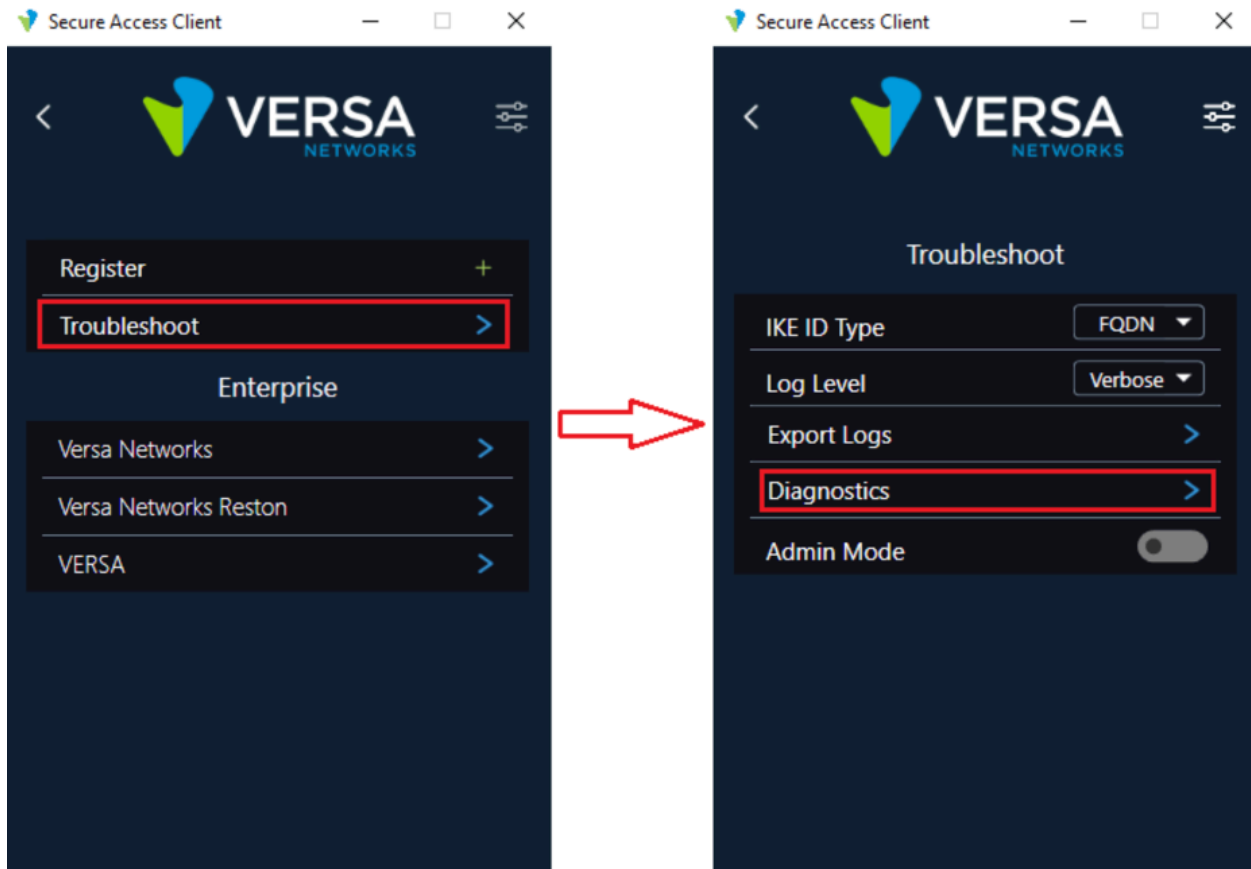
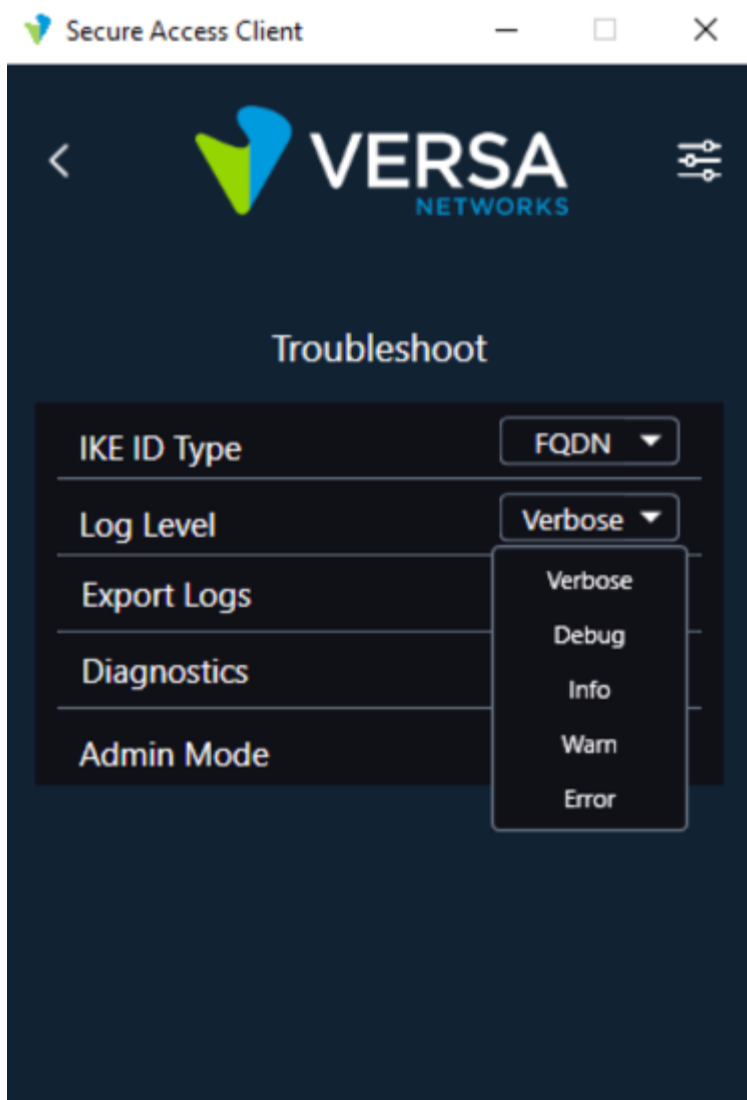3. When the diagnostics complete, a message displays.

Collect Complete Debug Logs

To collect a complete set of debug logs to help the Versa Managed Services NOG team debug issues on the Versa client and the operating system:

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

3. Click Log Level.

4. Select a log severity level:
   ◦ Debug—Log application debug-level information.
   ◦ Error—Log error-level information.
   ◦ Info—Log informational-level information. This is the default.
   ◦ Verbose—Log additional information during the interaction with the client user interface.
   ◦ Warm—Log warming-level information.
5. To save the logs as a .zip file, click Export Logs.
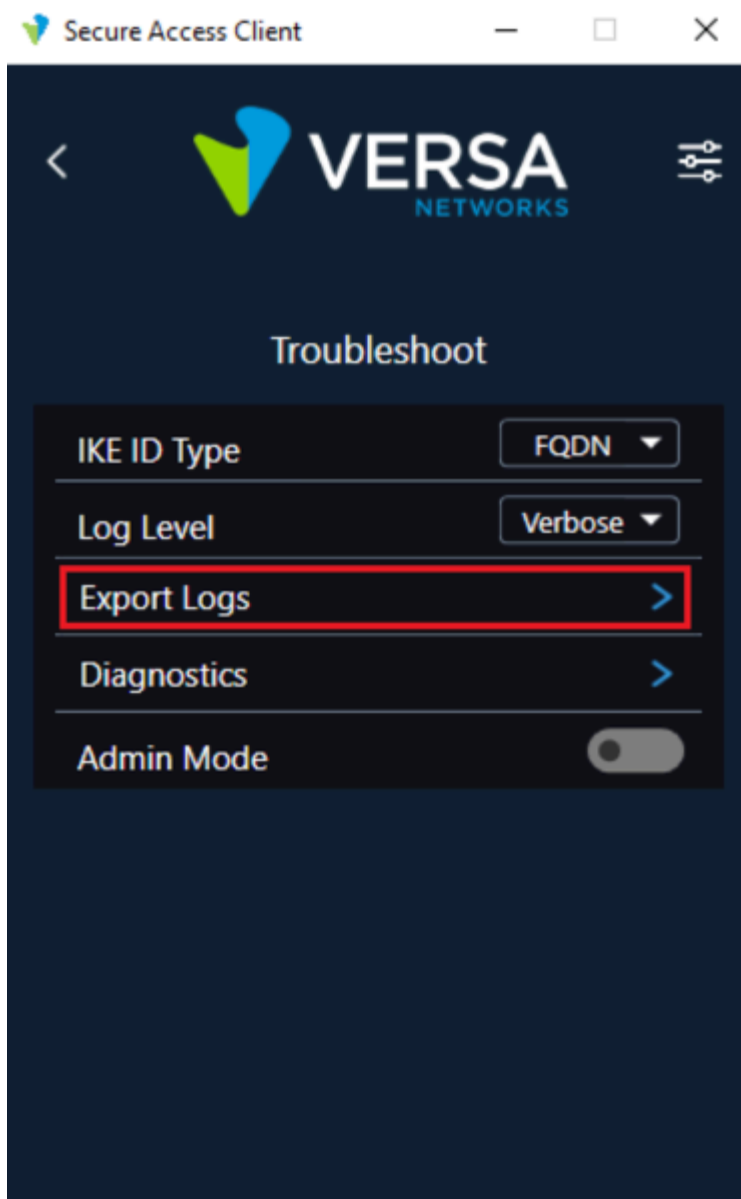
6. Share the .zip file with the Versa Managed Services NOC team.

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

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. Start the SASE client CLI console:

> **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**
>
> 387 [1] INFO Versa Secure Access (null) - Starting application in console mode. Version 7.4.1_24cd434d
> Run: VersaSecureAccessClientConsole.exe global --help, to get help for global options
> Run: VersaSecureAccessClientConsole.exe help, to check supported Options Verb
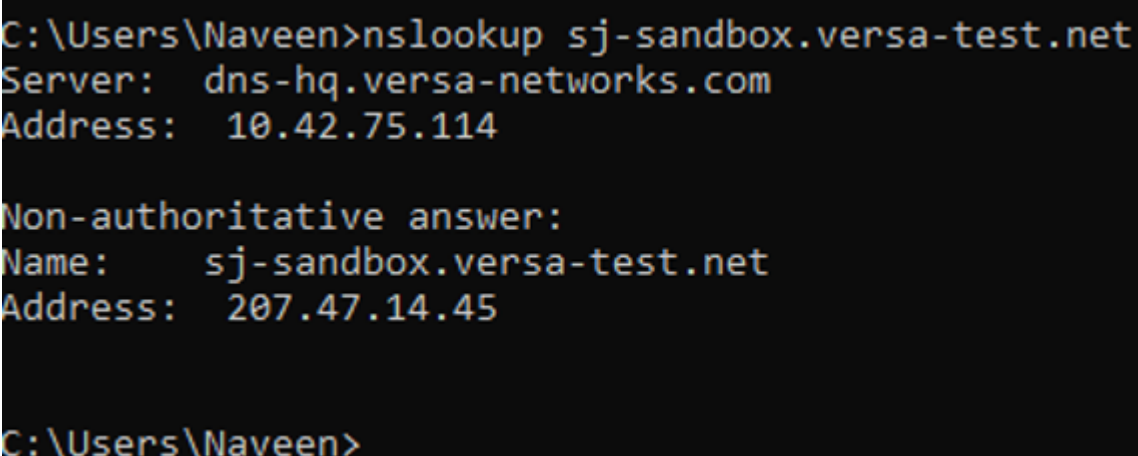
3. Display the VSA console CLI options:

> C:\Program Files (x86)\Versa Secure Access> **VersaSecureAccessClientConsole.exe --help**
> VersaSecureAccessClientConsole 7.4.1.0
> Copyright c 2020
> global   (Default Verb)
> prelogon   Prelogon operations
> client   Configure Client options
> help   Display more information on a specific command.
> version   Display version information.

4. Display the SASE client software version:

> C:\Program Files (x86)\Versa Secure Access> **VersaSecureAccessClientConsole.exe global --version**
> VersaSecureAccessClientConsole 7.4.1.

Verify the FQDN Used for Portal Registration

To verify that that FQDN used for portal registration resolves to the correct SASE portal WAN IP address, issue an **nslookup** or **ping** command for the FQDN that you use used for registration from your computer or laptop. The FQDN must resolve to the SASE portal WAN IP address. For example:

```
C:\Users\Naveen>nslookup sj-sandbox.versa-test.net
Server:   dns-hq.versa-networks.com
Address:  10.42.75.114

Non-authoritative answer:
Name:    sj-sandbox.versa-test.net
Address:  207.47.14.45


C:\Users\Naveen>
```

Verify that HTTP and HTTPS Packets Are Allowed

To verify that HTTP and HTTPS packets destined to the SASE portal are allowed, check that your computer or laptop is set to allow HTTP and HTTPS packets to the VCG and registration portal. Make sure that the firewall on computer or laptop is not set to block HTTP and HTTPS packets bidirectionally.

To troubleshoot firewall issues on your computer or laptop, see the documentation from computer OS provider.

Supported Software Information

VOS Releases 20.2.3 and later support all content described in this article.

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

Additional Information

[Configure Versa SASE Clients](#)
[Use the Versa SASE Client Application](#)