Configure Certificate-Based Authentication for SASE Clients

For supported software information, click here.

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

Before You Begin

Before you configure certificate-based authentication for the SASE client:

- Generate the root certificate authority (CA) key and CA certificate.
- Create the client certificate file.
- Generate the key and CSR for the client.
- Generate the client certificate signed by a CA.
- Convert the .crt file to a Personal Information Exchange (.pfx) file for the client certificate.
- Import the client certificate to the client device.
- Upload the root CA chain certificate to the device (this CA certificate validates the SASE client certificate).

Generate the CA Key, CA Certificate, and Client Certificate

This section describes how to generate a CA key, CA certificate, and SASE client certificate using OpenSSL on any Linux system. You can create a certificate, get it signed by a CA, and then use it on a Director node. For more information, see Create and Manage Certificates.

You can skip the following steps if you have already generated CA and SASE client certificates or if you use other methods to generate certificates, you can skip this section.

To generate a CA key, CA certificate, and SASE client certificate:

1. Generate the root CA key:

```
openssl genrsa -aes256 -out root-ca.key 4096
```

2. Generate the CA certificate using the root CA key:

   ```
   openssl req -new -x509 -sha256 -days 3650 -key root-ca.key -out root-ca-cert.pem
   ```

3. Create the cert.conf file with the following values. In the sample configuration here, commonName is alice-cert, which is same as the user name:

   ```
   cat cert.conf

   #authorityKeyIdentifier = keyid,issuer:always
   distinguished_name = req_distinguished_name
   req_extensions      = v3_req
   x509_extensions = usr_cert

   prompt = no

   [ req_distinguished_name ]
   countryName = US
   stateOrProvinceName = VA
   localityName = Reston
   organizationName = Versa Networks
   commonName = alice-cert

   [ v3_req ]
   extendedKeyUsage = clientAuth, emailProtection
   basicConstraints = CA:FALSE
   keyUsage = critical, digitalSignature, keyEncipherment
   [ usr_cert ]
   basicConstraints = CA:FALSE
   nsCertType = client, email
   nsComment = "OpenSSL Generated Client Certificate"
   keyUsage = critical, digitalSignature, keyEncipherment
   extendedKeyUsage = clientAuth, emailProtection
   subjectKeyIdentifier = hash
   authorityKeyIdentifier = keyid,issuer
   ```

4. Generate a certificate signing request (CSR) for the client certificate:

   ```
   openssl req -out Client.csr -newkey rsa:2048 -nodes -keyout Client-Cert.key -config cert.conf -extensions 'v3_req'
   ```

5. Generate the client certificate signed by the CA:

   ```
   openssl x509 -req -in Client.csr -CA root-ca-cert.pem -CAkey root-ca.key -out Client-Cert.crt -CAcreateserial -days 730 -sha256 -extfile cert.conf -extensions 'usr_cert'
   ```

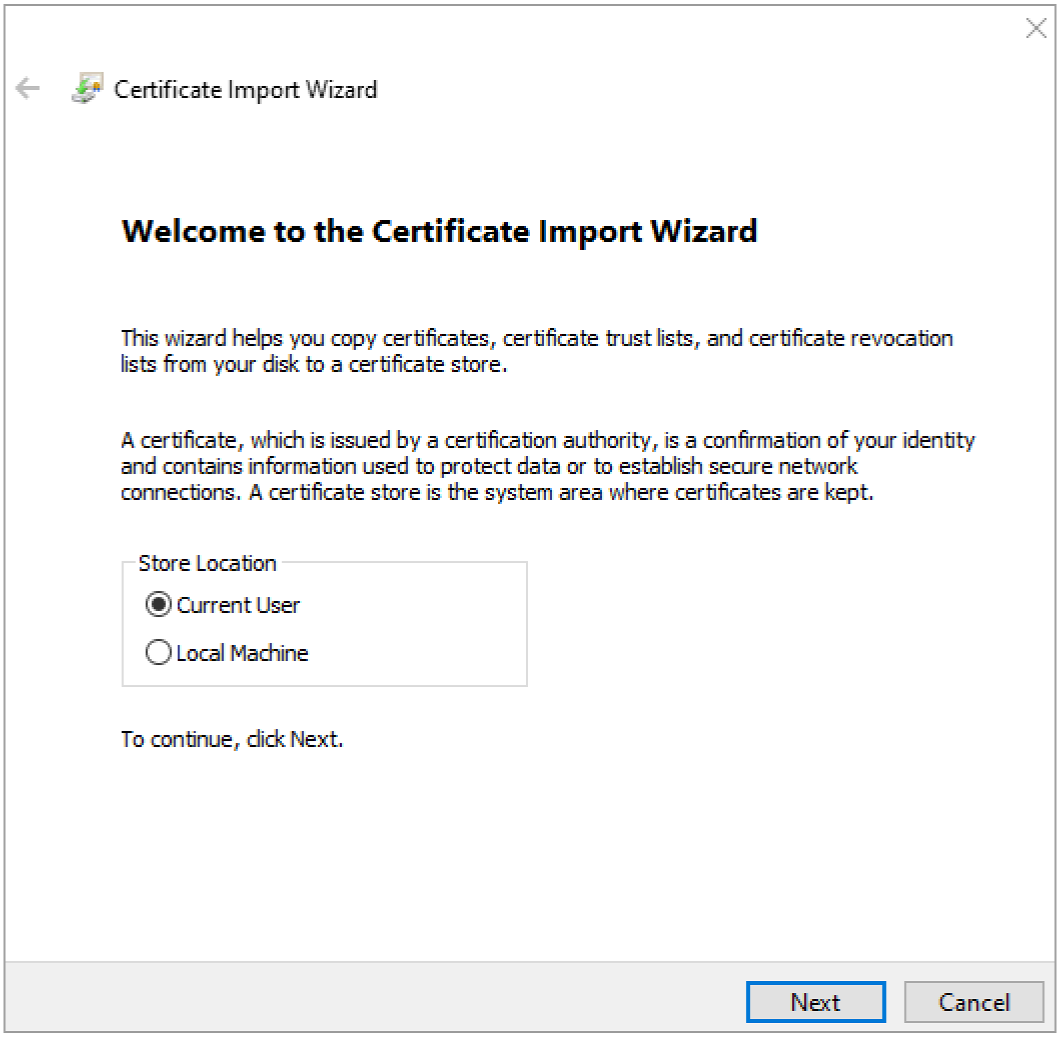
6. Convert the .crt file to a .pfx file. Here, we use the name AliceClient-Cert.pfx:

   ```
   openssl pkcs12 -inkey Client-Cert.key -in Client-Cert.crt -export -out AliceClient-Cert.pfx -passin pass:versa123 -passout pass:versa123
   ```

Import the Client Certificate to a Windows OS Client Device

To import the client certificate that you created in Generate the CA Key, CA Certificate, and Client Certificate, above, to a client device that is running Windows OS:

1. Navigate to where you saved the client certificate, and then double-click it. The Certificate Import Wizard displays.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

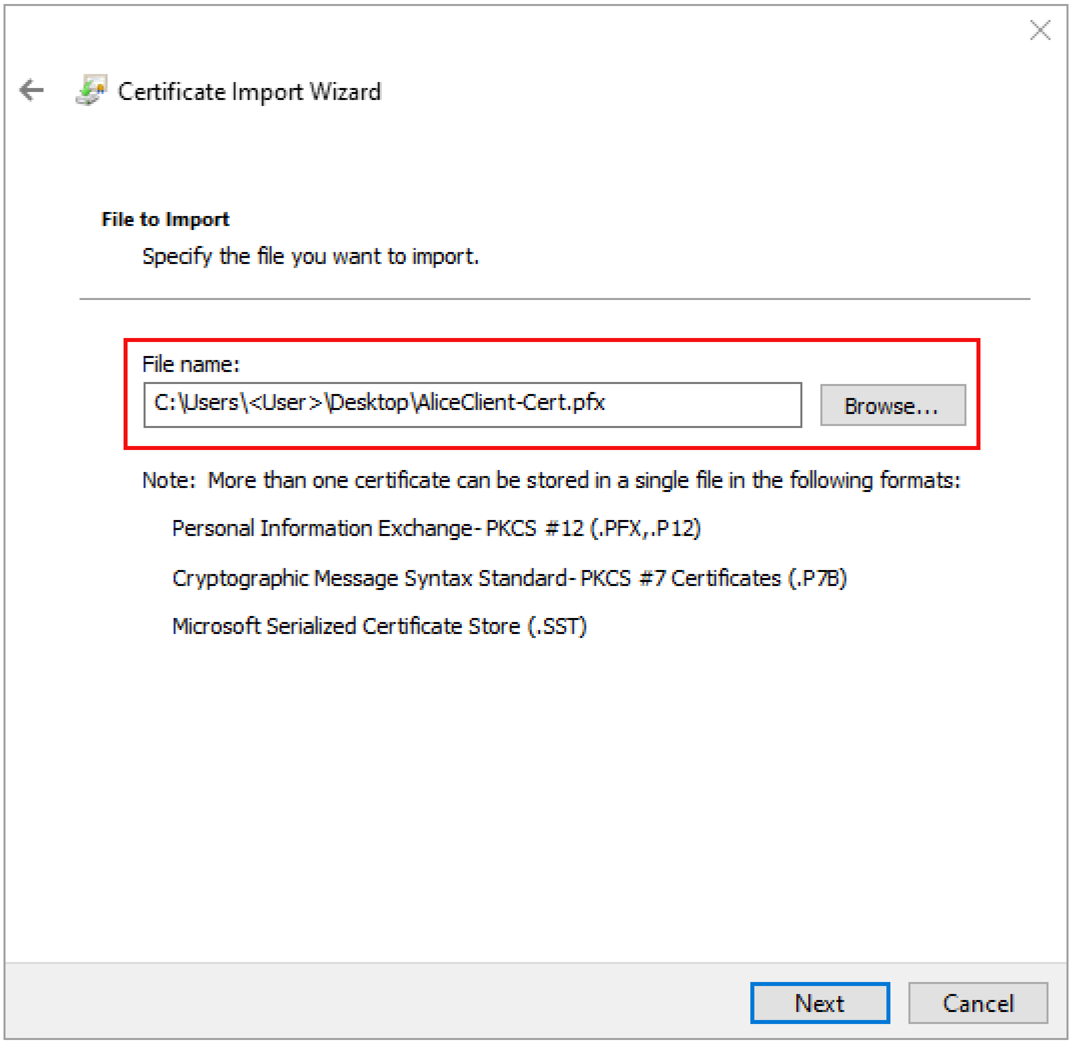
Store Location

● Current User

○ Local Machine

To continue, click Next.

2. For certificate-based user authentication, select Current User, or for device authentication, select Local Machine. Here, we select Current User.
3. Click Next.
4. In the File to Import window, click the Browse button, and then select the client certificate file.


Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Users\<User>\Desktop\AliceClient-Cert.pfx

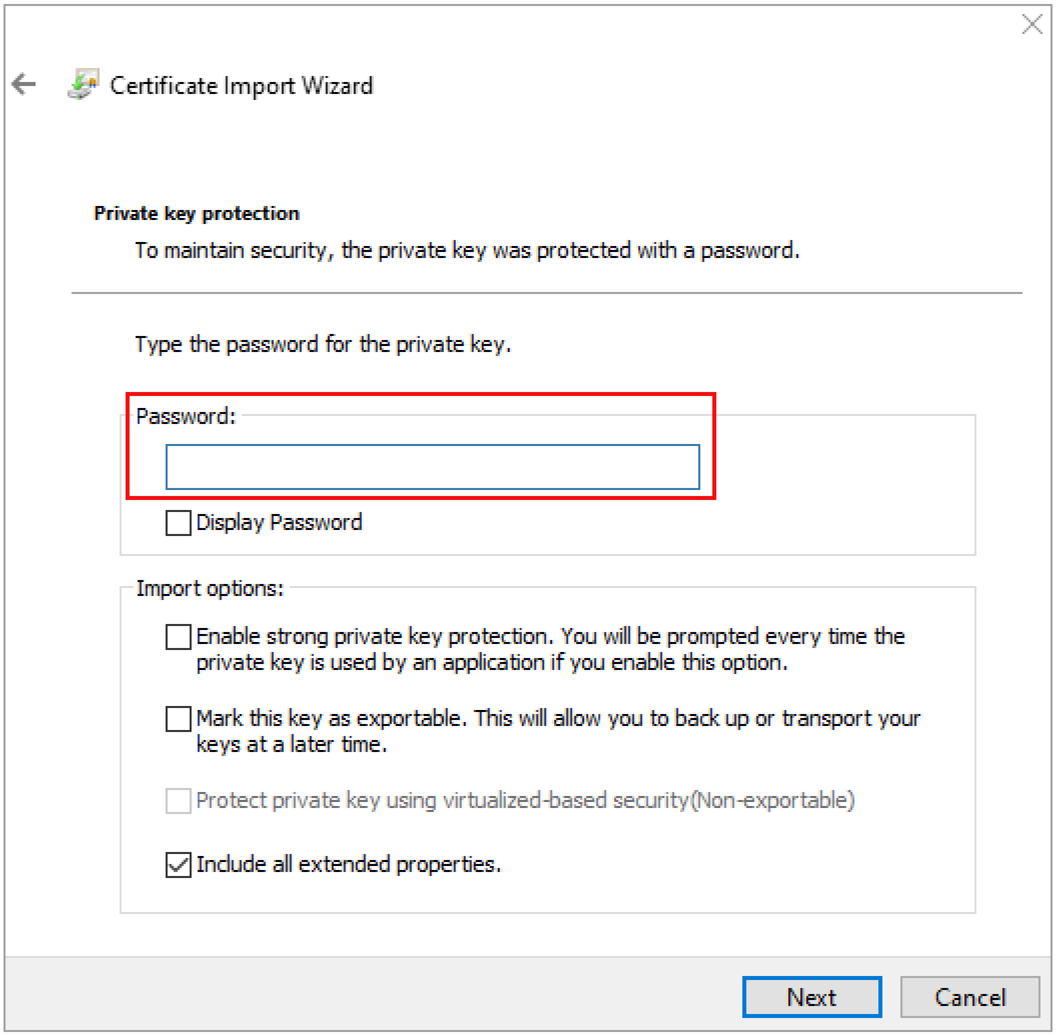
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

5. Click Next. If the file is password-protected, the Private Key Protection screen displays.



Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

□ Display Password

Import options:

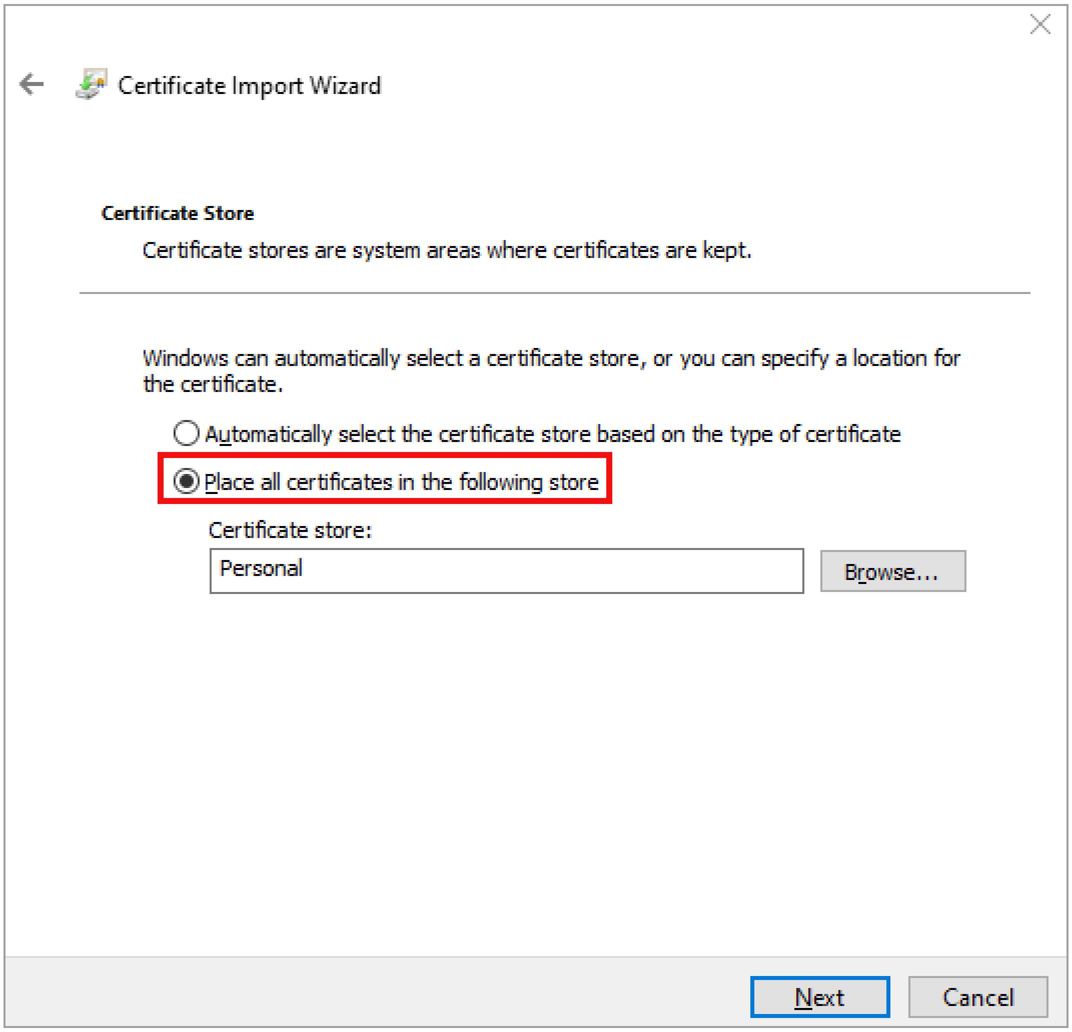
□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

□ Protect private key using virtualized-based security(Non-exportable)

☑ Include all extended properties.

6. In the password field, enter the name of the password file, and then click Next. The Certificate Store window displays.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

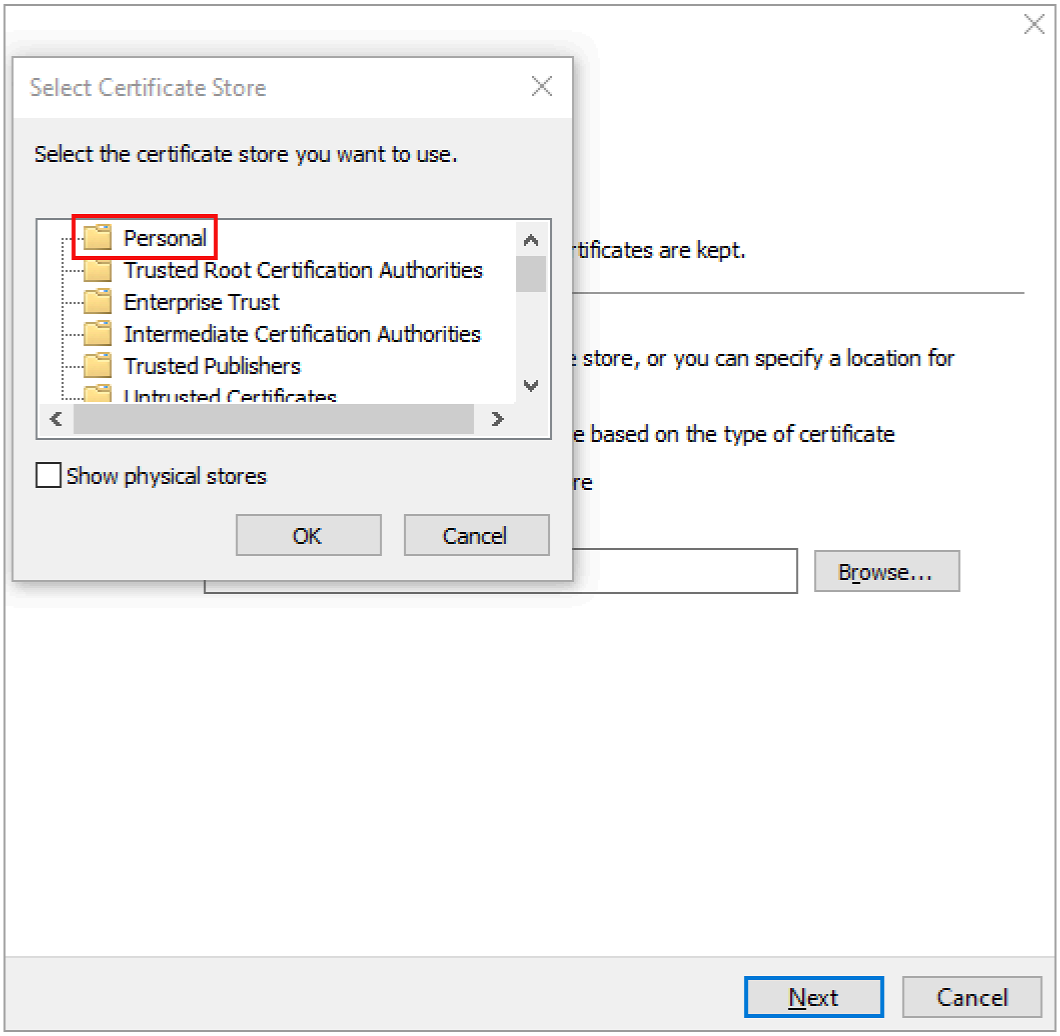
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Personal

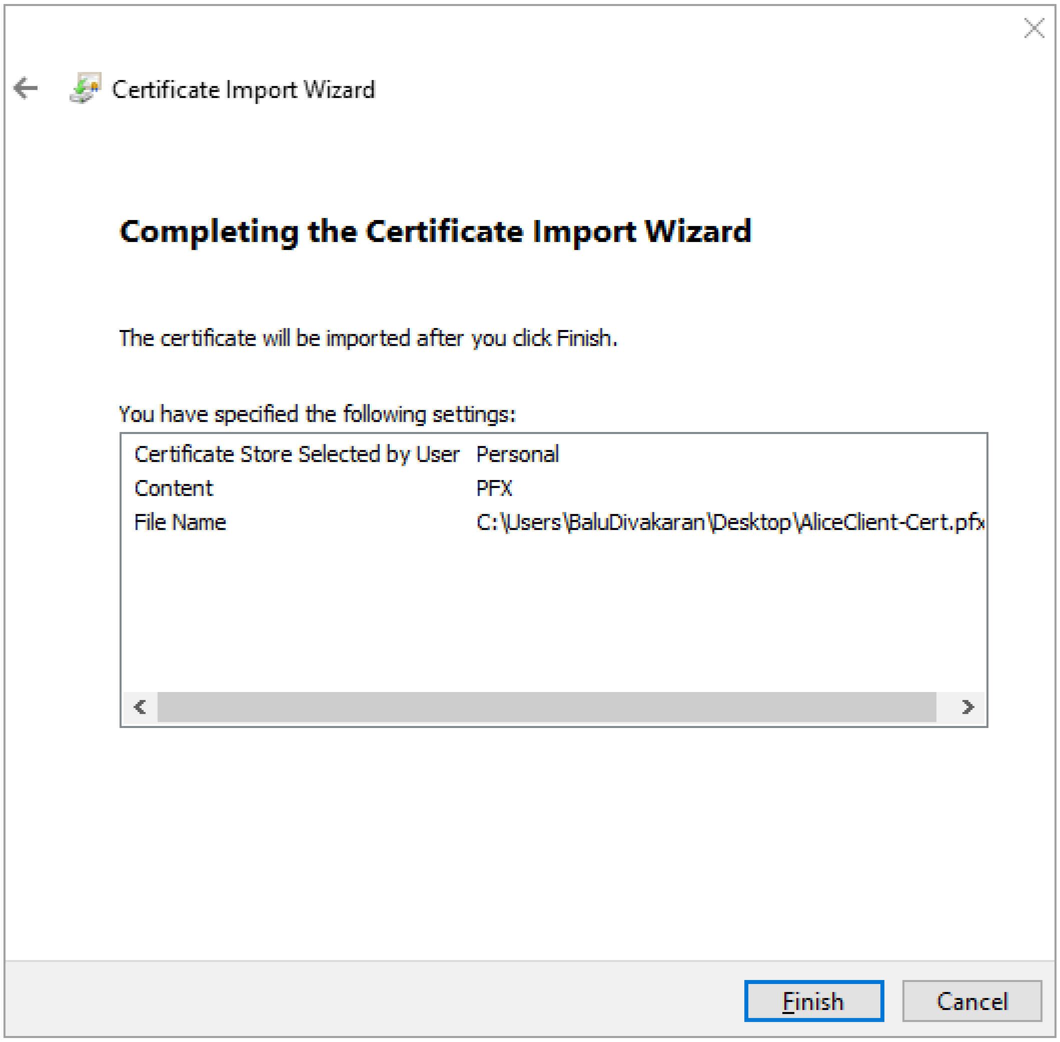
7. Select Place all Certificates in the Following Store option, and then click Browse. The Select Certificate Store popup window displays.


Select Certificate Store

Select the certificate store you want to use.

Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
☐ Show physical stores
OK
Cancel
rtificates are kept.
e store, or you can specify a location for
e based on the type of certificate
re
Browse...
Next
Cancel

8. Select Personal, and then click OK.
9. Click Next. The Completing the Certificate Import Wizard window displays.



Certificate Import Wizard

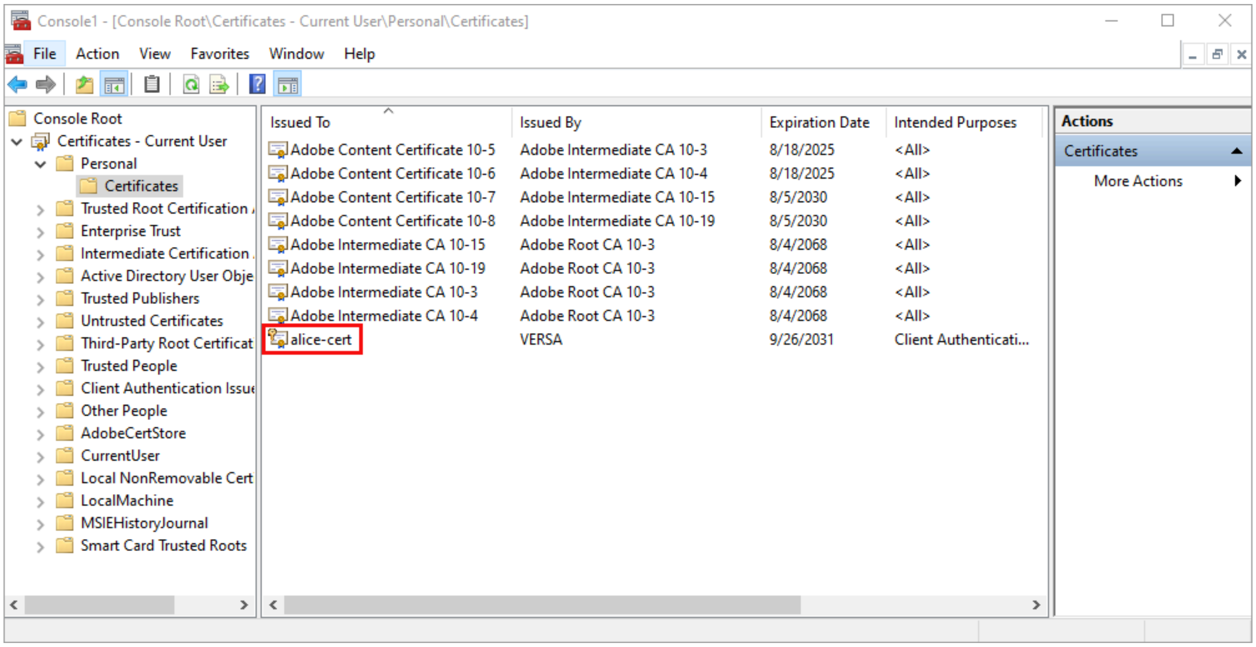
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Personal
Content	PFX
File Name	C:\Users\BaluDivakaran\Desktop\AliceClient-Cert.pfx

10. Click Finish to import the certificate. The certificate displays under Personal > Certificates.



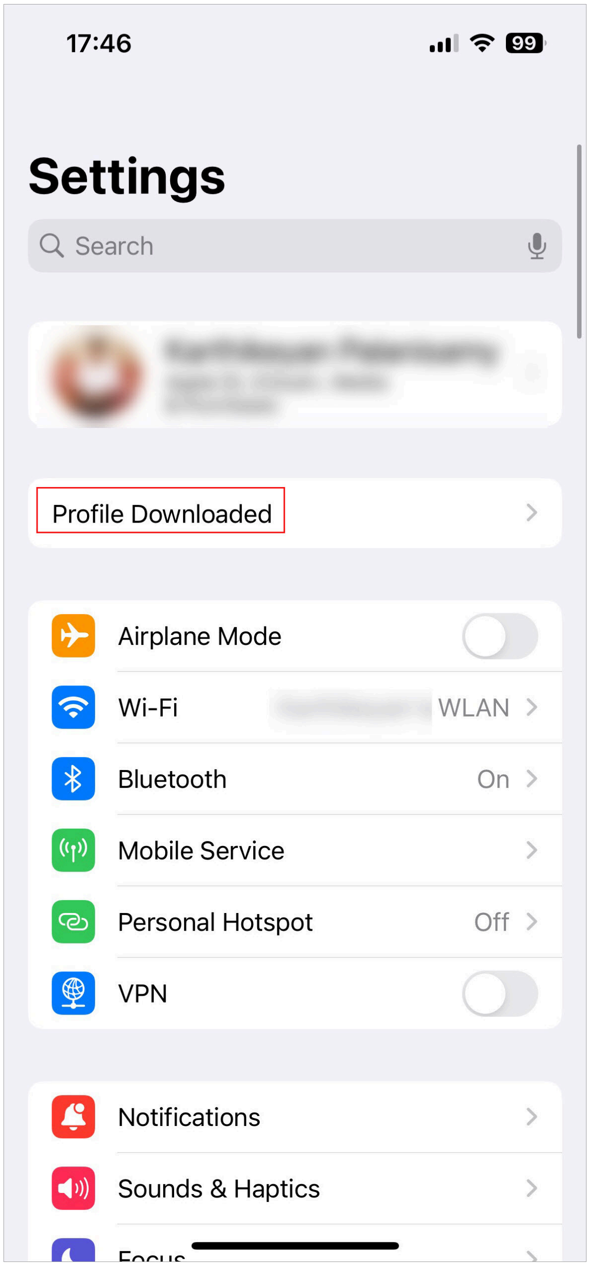
Issued To	Issued By	Expiration Date	Intended Purposes
Adobe Content Certificate 10-5	Adobe Intermediate CA 10-3	8/18/2025	<All>
Adobe Content Certificate 10-6	Adobe Intermediate CA 10-4	8/18/2025	<All>
Adobe Content Certificate 10-7	Adobe Intermediate CA 10-15	8/5/2030	<All>
Adobe Content Certificate 10-8	Adobe Intermediate CA 10-19	8/5/2030	<All>
Adobe Intermediate CA 10-15	Adobe Root CA 10-3	8/4/2068	<All>
Adobe Intermediate CA 10-19	Adobe Root CA 10-3	8/4/2068	<All>
Adobe Intermediate CA 10-3	Adobe Root CA 10-3	8/4/2068	<All>
Adobe Intermediate CA 10-4	Adobe Root CA 10-3	8/4/2068	<All>
alice-cert	VERSA	9/26/2031	Client Authenticati...

Import the Client Certificate to an iOS Client Device

Before you import the client certificate that you created in Generate the CA Key, CA Certificate, and Client Certificate, above, on an iOS device, you must download it from your email or from the appropriate server.

To import the client certificate to a client device that is running iOS:

1. To view the downloaded client certificate on your device, go to Settings > Profile Downloaded.



17:46

99

Settings

Search

[redacted]

Profile Downloaded

Airplane Mode

Wi-Fi [redacted] WLAN

Bluetooth On

Mobile Service

Personal Hotspot Off

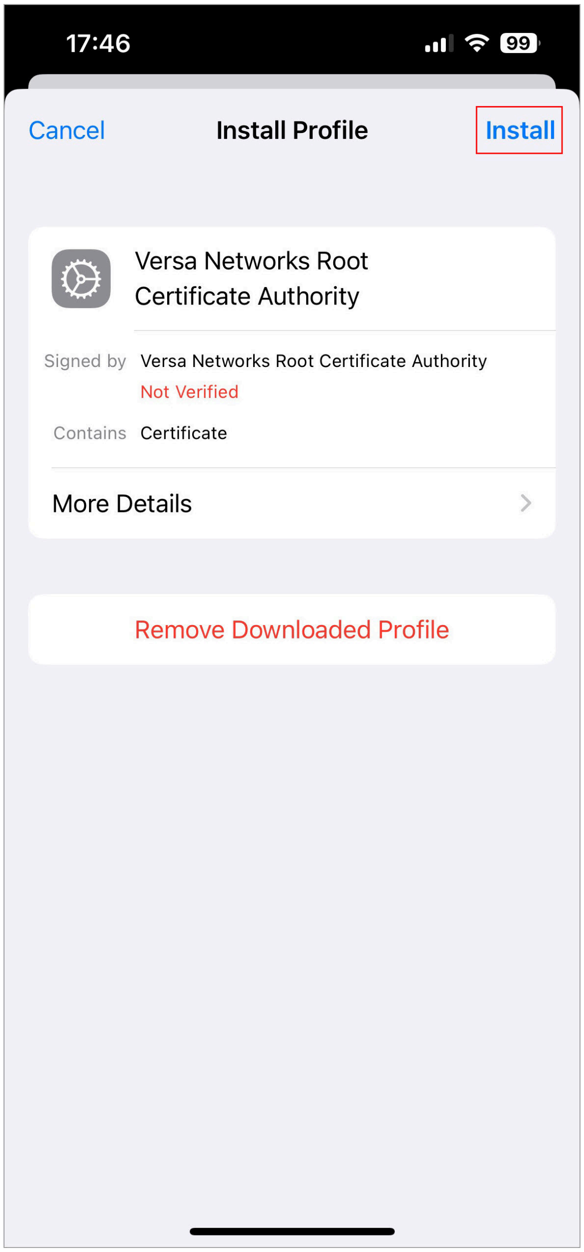
VPN

Notifications

Sounds & Haptics

Focus

2. To install the certificate on your device, click Profile Downloaded. The Install Profile window displays the client certificate.

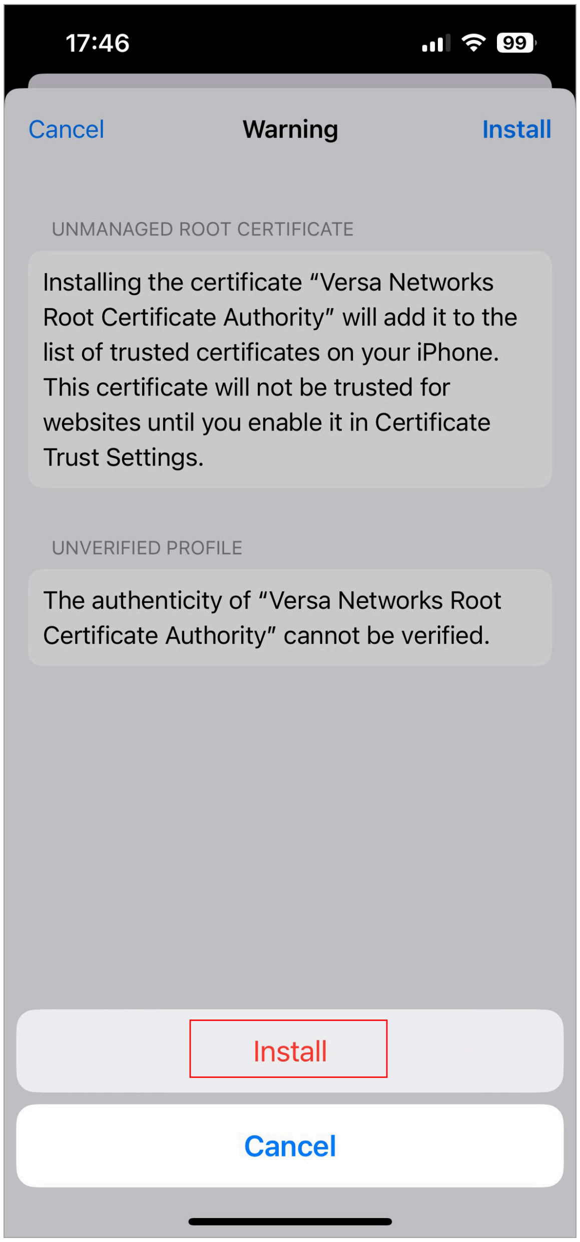


Versa Networks Root Certificate Authority

Signed by Versa Networks Root Certificate Authority
Not Verified

Contains Certificate

3. Click Install. The following message displays.



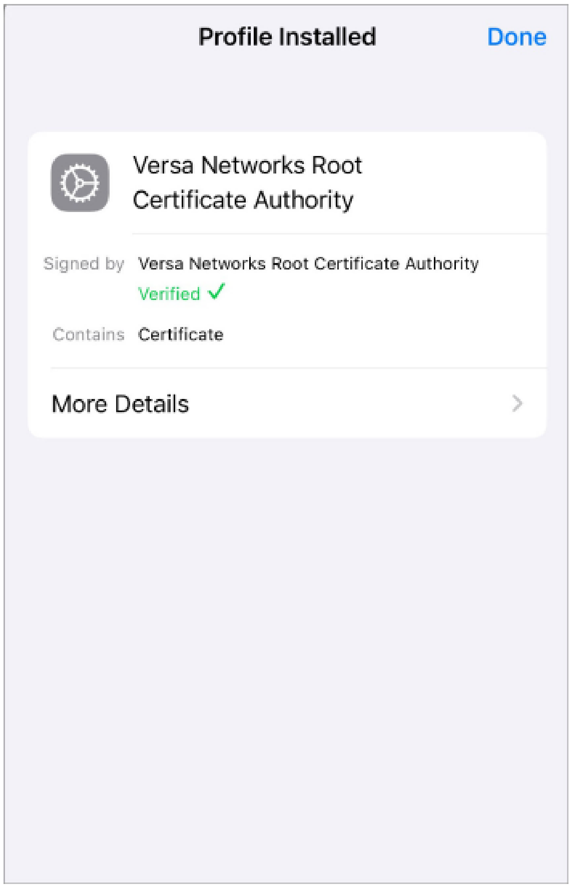
UNMANAGED ROOT CERTIFICATE

Installing the certificate “Versa Networks Root Certificate Authority” will add it to the list of trusted certificates on your iPhone. This certificate will not be trusted for websites until you enable it in Certificate Trust Settings.

UNVERIFIED PROFILE

The authenticity of “Versa Networks Root Certificate Authority” cannot be verified.

4. Click Install. The installed certificate displays.



Profile Installed

Done

Versa Networks Root Certificate Authority

Signed by Versa Networks Root Certificate Authority

Verified ✓

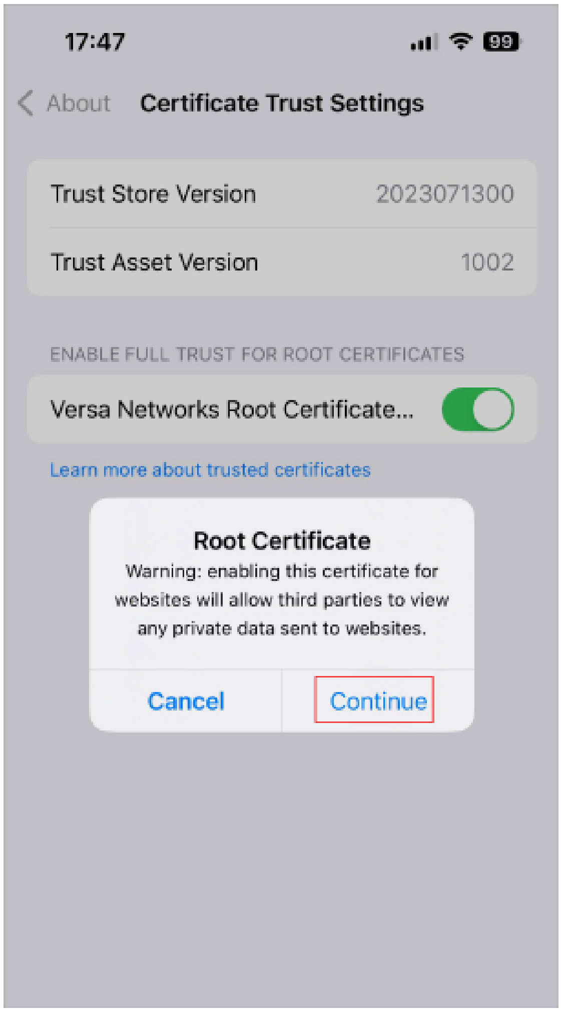
Contains Certificate

More Details

5. Click Done.

After you import the client certificate, you must trust the certificate so that the registration does not fail. To trust the certificate:

1. Click General > About > Certificate Trust Settings. The Certificate Trust Settings window displays.



17:47

About Certificate Trust Settings

Trust Store Version 2023071300

Trust Asset Version 1002

ENABLE FULL TRUST FOR ROOT CERTIFICATES

Versa Networks Root Certificate...

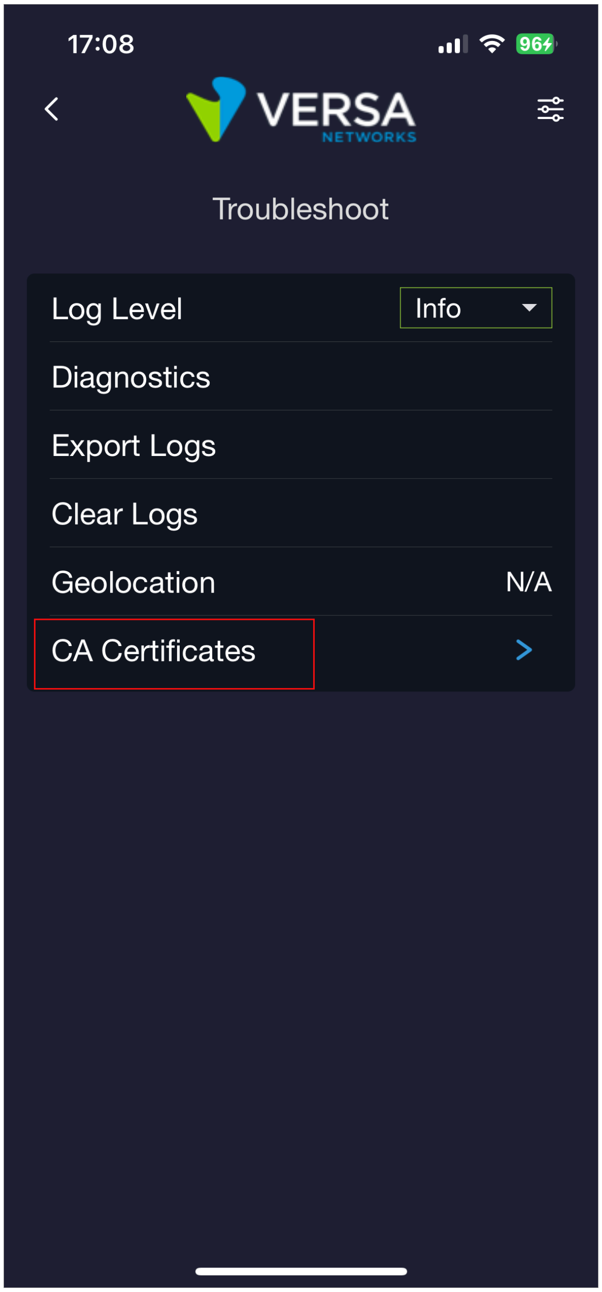
Learn more about trusted certificates

Root Certificate

Warning: enabling this certificate for websites will allow third parties to view any private data sent to websites.

2. In the Enable Full Trust for Root Certificates field, click the toggle for the Versa SASE client certificate, and then click Continue.

To view the client certificate from the SASE client, select Troubleshoot > CA Certificates.



For information about importing the client certificate on a MacOS device, see Import the CA Certificate.

Upload the CA Certificate to the Device

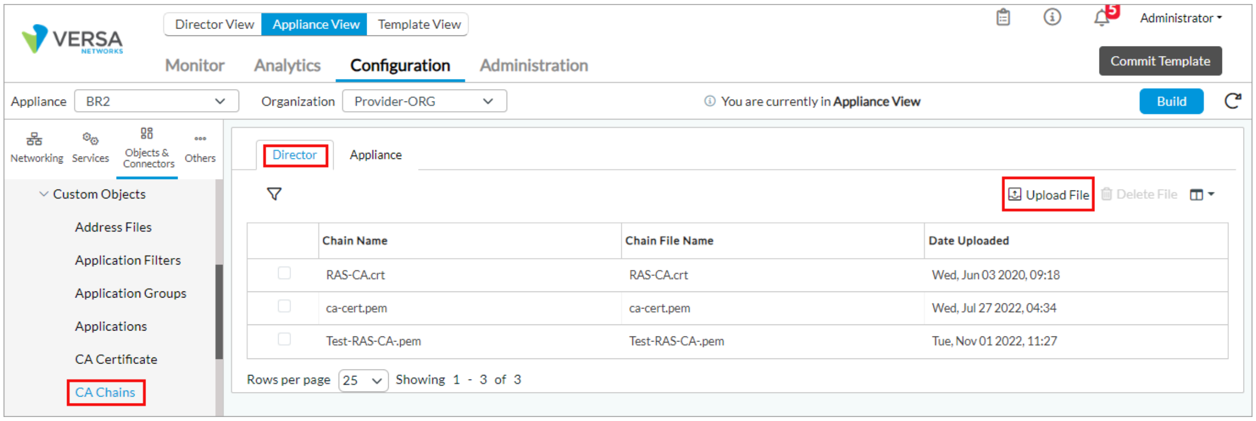
To upload the root CA certificate to the device:

1. In the Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Devices > Devices in the horizontal menu bar.

c. Select an organization in the left menu bar.

d. Select a Controller or Versa Operating System^{TM} (VOS^{TM}) device in the dashboard. The view changes to Appliance view.

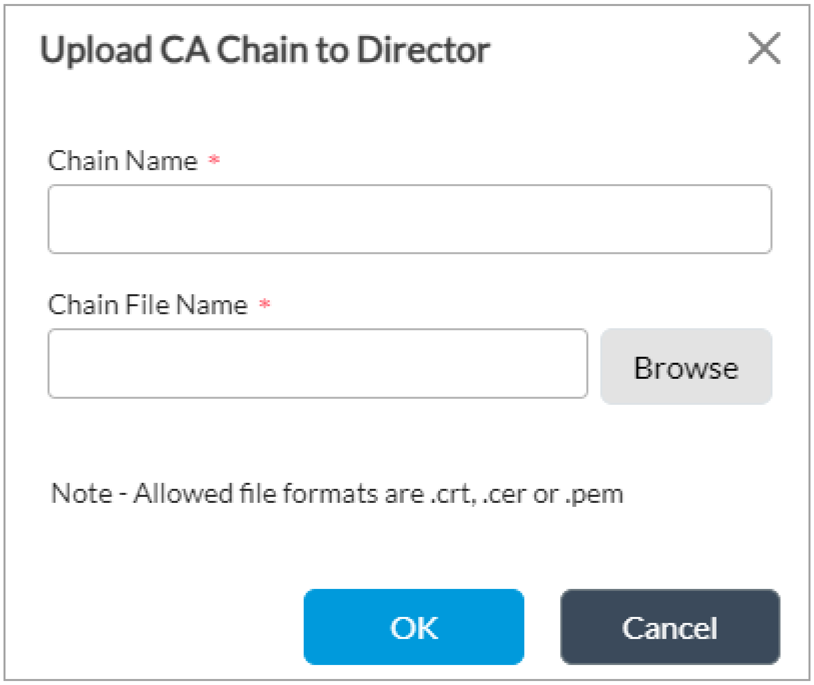
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Objects > Custom Objects > CA Chains in the left menu bar.



	Chain Name	Chain File Name	Date Uploaded
□	RAS-CA.crt	RAS-CA.crt	Wed, Jun 03 2020, 09:18
□	ca-cert.pem	ca-cert.pem	Wed, Jul 27 2022, 04:34
□	Test-RAS-CA-.pem	Test-RAS-CA-.pem	Tue, Nov 01 2022, 11:27

Rows per page 25 Showing 1 - 3 of 3

4. Select the Director tab, and then click Upload File to upload the .crt file. The Upload CA Chain to Director popup window displays.

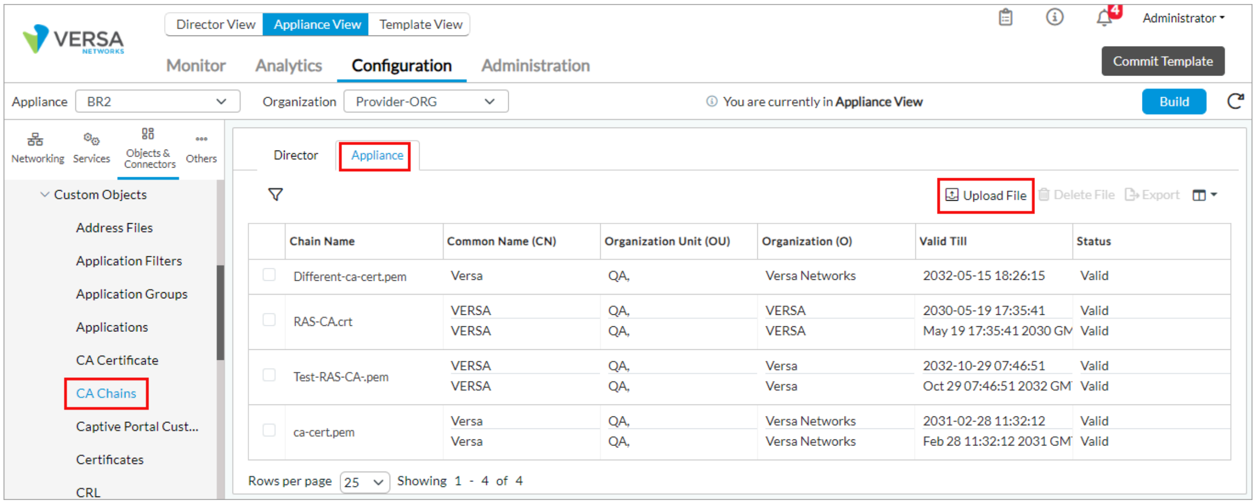

Upload CA Chain to Director

Chain Name *

Chain File Name *

Note - Allowed file formats are .crt, .cer or .pem

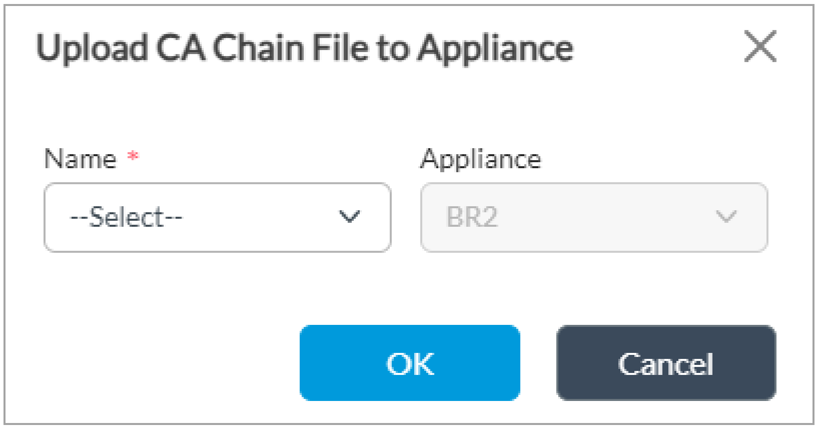
5. In the Chain Name field, enter a name for the chain.
6. In the Chain Filename field, enter the name of the chain file to upload, or click Browse to select the file to upload to the Director node.
7. Click OK to upload the file.
8. Select the Appliance tab.



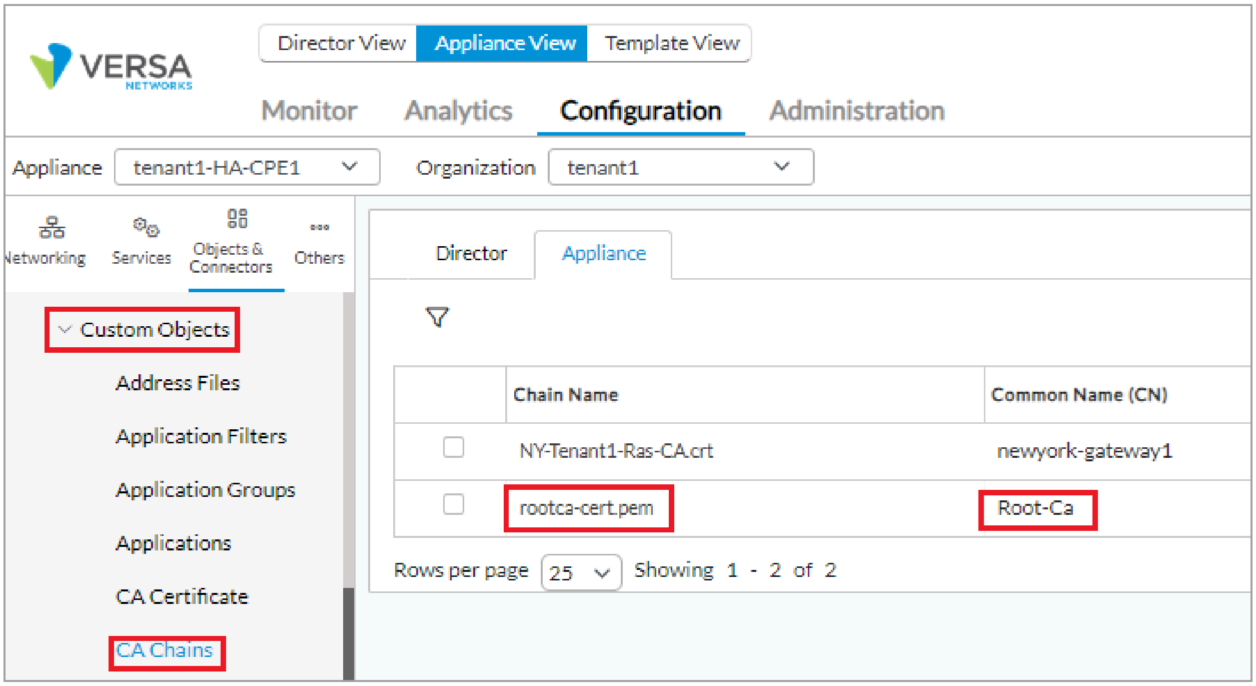
	Chain Name	Common Name (CN)	Organization Unit (OU)	Organization (O)	Valid Till	Status
□	Different-ca-cert.pem	Versa	QA,	Versa Networks	2032-05-15 18:26:15	Valid
□	RAS-CA.crt	VERSA VERSA	QA, QA,	VERSA VERSA	2030-05-19 17:35:41 May 19 17:35:41 2030 GM	Valid Valid
□	Test-RAS-CA-.pem	VERSA VERSA	QA, QA,	Versa Versa	2032-10-29 07:46:51 Oct 29 07:46:51 2032 GM	Valid Valid
□	ca-cert.pem	Versa Versa	QA, QA,	Versa Networks Versa Networks	2031-02-28 11:32:12 Feb 28 11:32:12 2031 GM	Valid Valid

Rows per page 25 Showing 1 - 4 of 4

9. Click Upload File. The Upload CA Chain File to Appliance popup window displays.



10. In the name field, select the name of the CA chain file (here, rootca-cert.pem) to upload to the VOS device.
11. Click OK to upload the file to the VOS device. The CA chain file displays on the Appliance tab.



Appliance: tenant1-HA-CPE1
Organization: tenant1

	Chain Name	Common Name (CN)
□	NY-Tenant1-Ras-CA.crt	newyork-gateway1
□	rootca-cert.pem	Root-Ca

Rows per page 25 Showing 1 - 2 of 2

Configure Certificate-Based User Authentication

To configure certificate-based user authentication, you do the following:

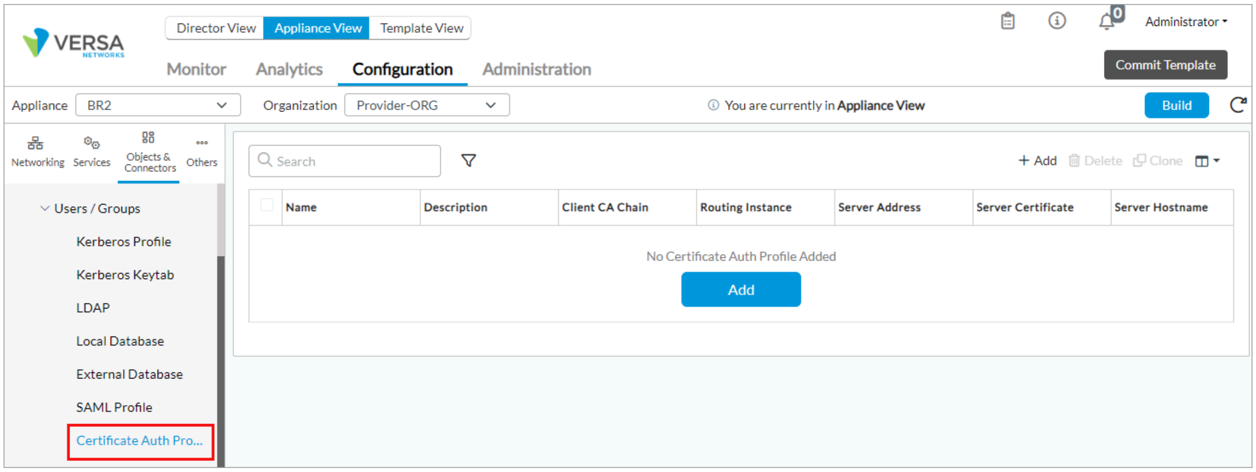
- Configure a certificate authentication profile.
- Configure an authentication method for the certificate authentication profile.
- Associate the authentication method with the authentication profile.
- Associate the authentication profile with a secure access portal and secure access gateway.
- Modify the organization limit to add the certificate service host name under domain names.

Configure a Certificate Authentication Profile

You configure a certificate authentication profile and use it in an authentication profile.

To configure a certificate authentication profile:

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 pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Object and Connectors > Connectors > Users/Groups > Certificate Authentication Profile in the left menu bar.



Appliance: BR2

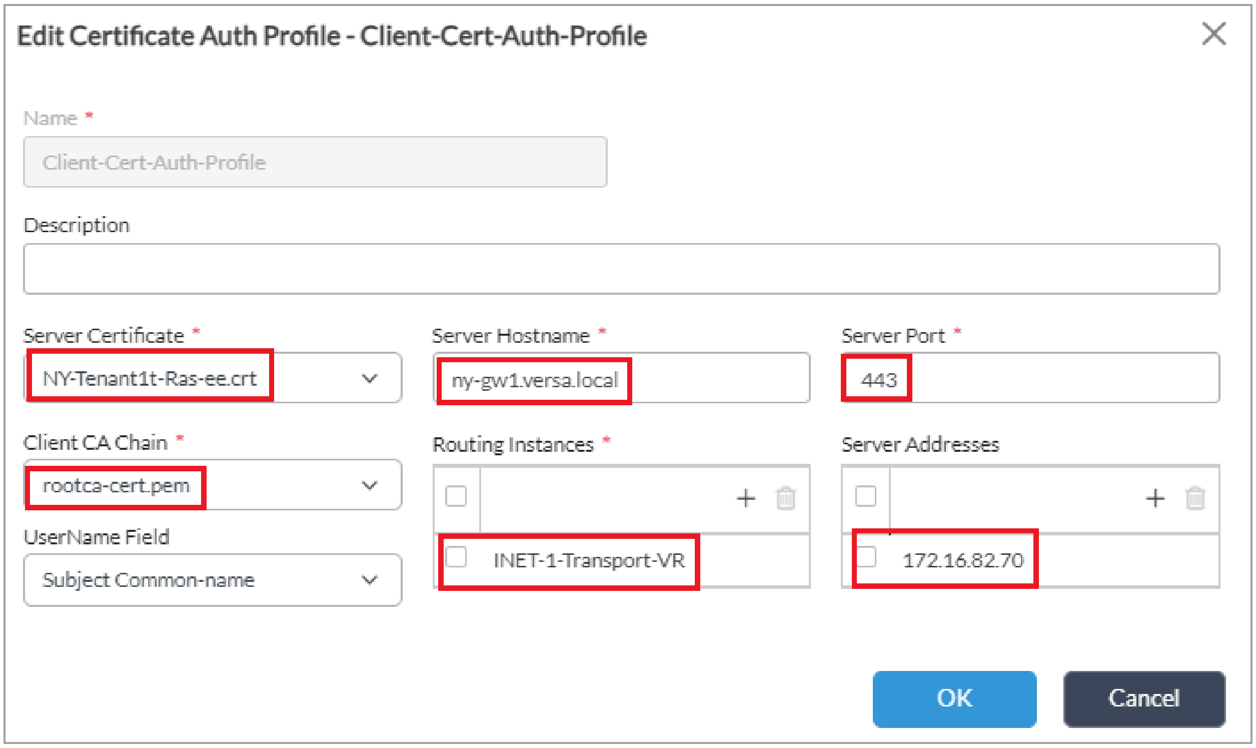
Organization: Provider-ORG

You are currently in **Appliance View**

Name	Description	Client CA Chain	Routing Instance	Server Address	Server Certificate	Server Hostname

No Certificate Auth Profile Added

4. Click Add. In the Add/Edit Certificate Authentication Profile popup window, enter information for the following fields.



Edit Certificate Auth Profile - Client-Cert-Auth-Profile

Name *: Client-Cert-Auth-Profile

Description:

Server Certificate *: NY-Tenant1t-Ras-ee.crt

Server Hostname *: ny-gw1.versa.local

Server Port *: 443

Client CA Chain *: rootca-cert.pem

Routing Instances *: INET-1-Transport-VR

Server Addresses: 172.16.82.70

UserName Field: Subject Common-name

Field	**Description**
Name (Required)	Enter a name for the certificate authentication profile.
Description	Enter a description for the certificate authentication profile.
Server Certificate (Required)	Select the server certificate for certificate authentication.
Server Hostname (Required)	Enter a hostname to start certificate authentication service. Ensure that this fully qualified domain name (FQDN) is different from the FQDN of the SASE gateway.
Server Port (Required)	Enter the port number to start certificate authentication service. You can enter 443 or any other private port number.
Client CA Chain (Required)	Select the root CA chain that you uploaded in Upload the CA Certificate to the Device to authenticate the client certificate.
Routing Instances (Required)	Click the + Add icon and select the routing instance to reach the certificate authentication server.
Server Addresses	Enter the WAN-VR IP address to start certificate authentication service.
Username Field	Select the field that the VOS software uses to validate a name match in the client certificate: ◦ Alternative-name Email ◦ Subject Alternative-name Principal Name ◦ Subject Common-nameSubject

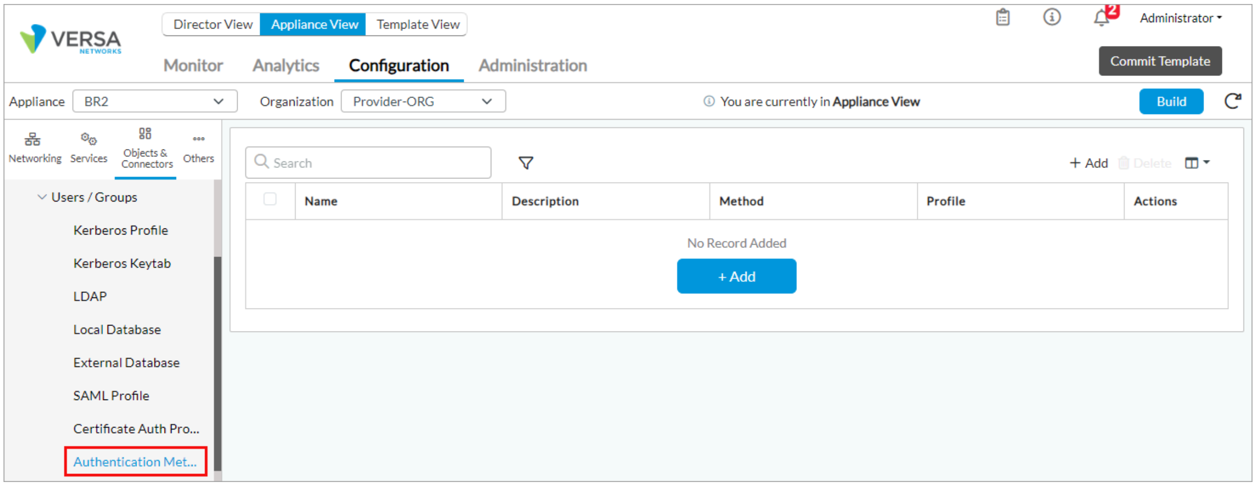
5. For more information about the other fields in the Add/Edit Certificate Authentication Profile popup window, see Configure a Certificate Authentication Profile in Configure User and Group Policy.
6. Click OK.

Configure an Authentication Method for Certificate Authentication Profile

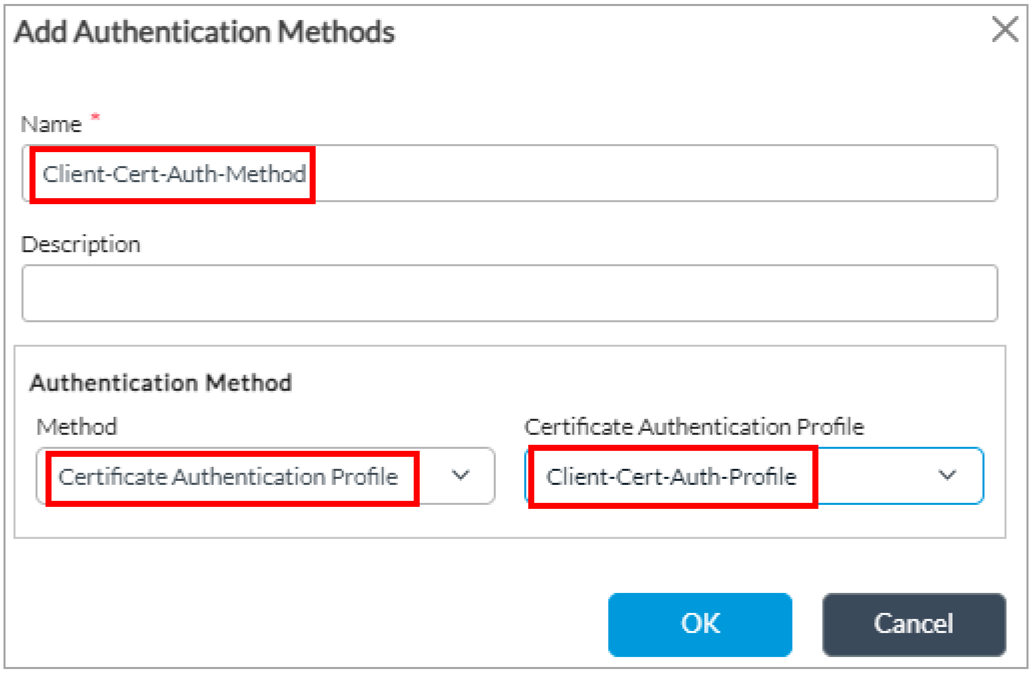
To configure an authentication method for the certificate authentication profile you configured in Configure a Certificate

Authentication Profile, above:

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 Methods in the left menu bar.



4. Click Add. The Add Authentication Methods popup window displays.



Name * Client-Cert-Auth-Method

Description

Authentication Method

Method: Certificate Authentication Profile

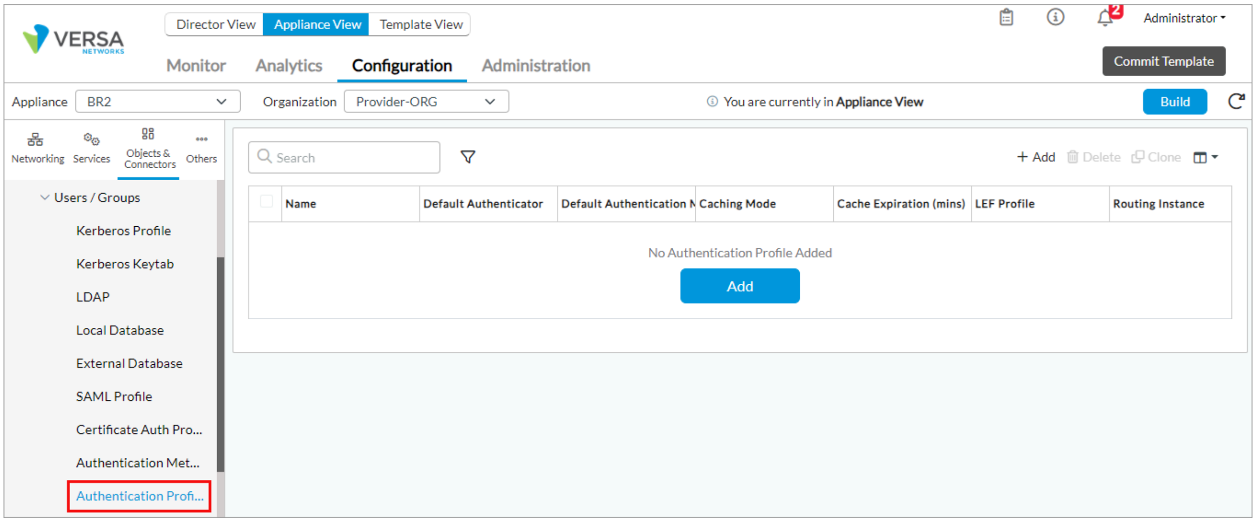
Certificate Authentication Profile: Client-Cert-Auth-Profile

5. Enter a name for the authentication method.
6. Under Authentication Method, select Certificate Authentication Profile in the Method field.

7. In the Certificate Authentication Profile field, select the profile (here, Client-Cert-Auth-Profile) that you created in Configure a Certificate Authentication Profile, above.
8. Click OK.

Associate the Authentication Method with the Authentication Profile

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 Objects & Connectors > Connectors > Users/Groups > Authentication Profiles in the left menu bar.



Appliance BR2

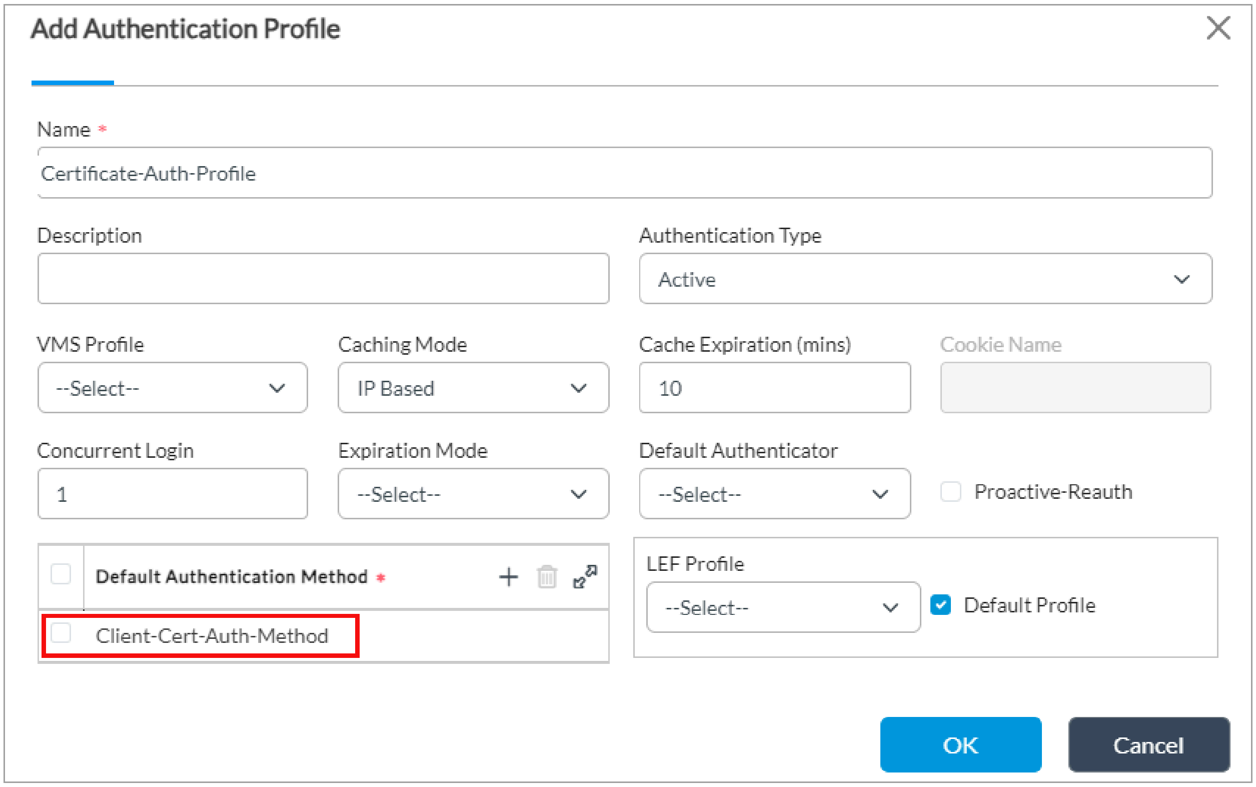
Organization Provider-ORG

You are currently in Appliance View

Name	Default Authenticator	Default Authentication M	Caching Mode	Cache Expiration (mins)	LEF Profile	Routing Instance

No Authentication Profile Added

4. Click Add. The Add Authentication Profiles popup window displays.



Add Authentication Profile

Name *: Certificate-Auth-Profile

Description:

Authentication Type: Active

VMS Profile: --Select--

Caching Mode: IP Based

Cache Expiration (mins): 10

Cookie Name:

Concurrent Login: 1

Expiration Mode: --Select--

Default Authenticator: --Select--

□ Proactive-Reauth

□	Default Authentication Method *
□	Client-Cert-Auth-Method

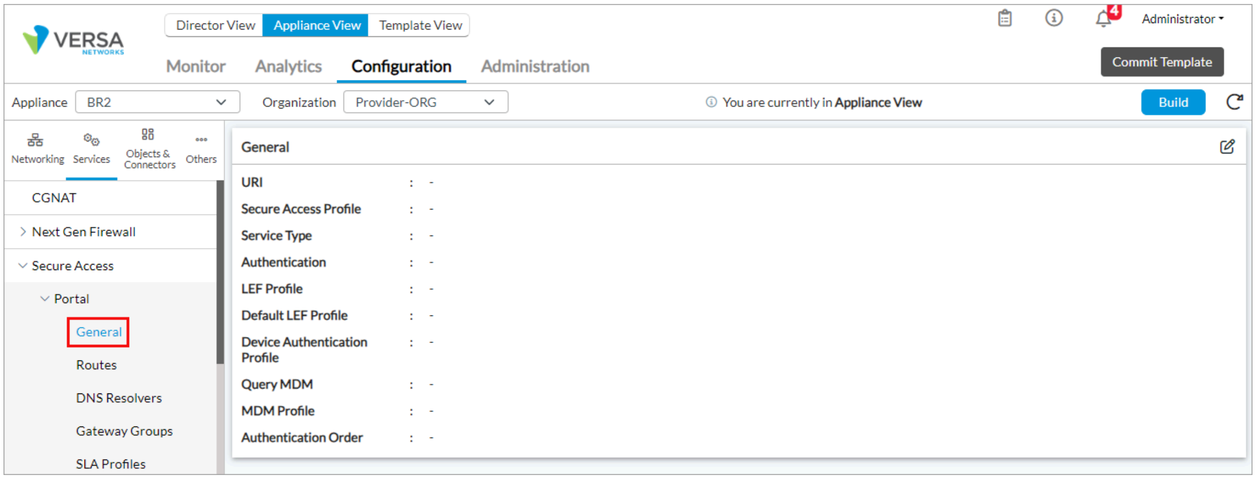
LEF Profile: --Select--

☑ Default Profile

5. Enter a name for the authentication profile.
6. In the Default Authentication Method field, click + and then select the authentication method (here, Client-Cert-Auth-Method) that you added in Associate the Certification Authentication Profile with the Authentication Method, above.
7. For information about configuring other parameters, see Configure an Authentication Profile in Configure User and Group Policy.
8. Click OK.

Associate the Authentication Profile with the Secure Access Portal

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.

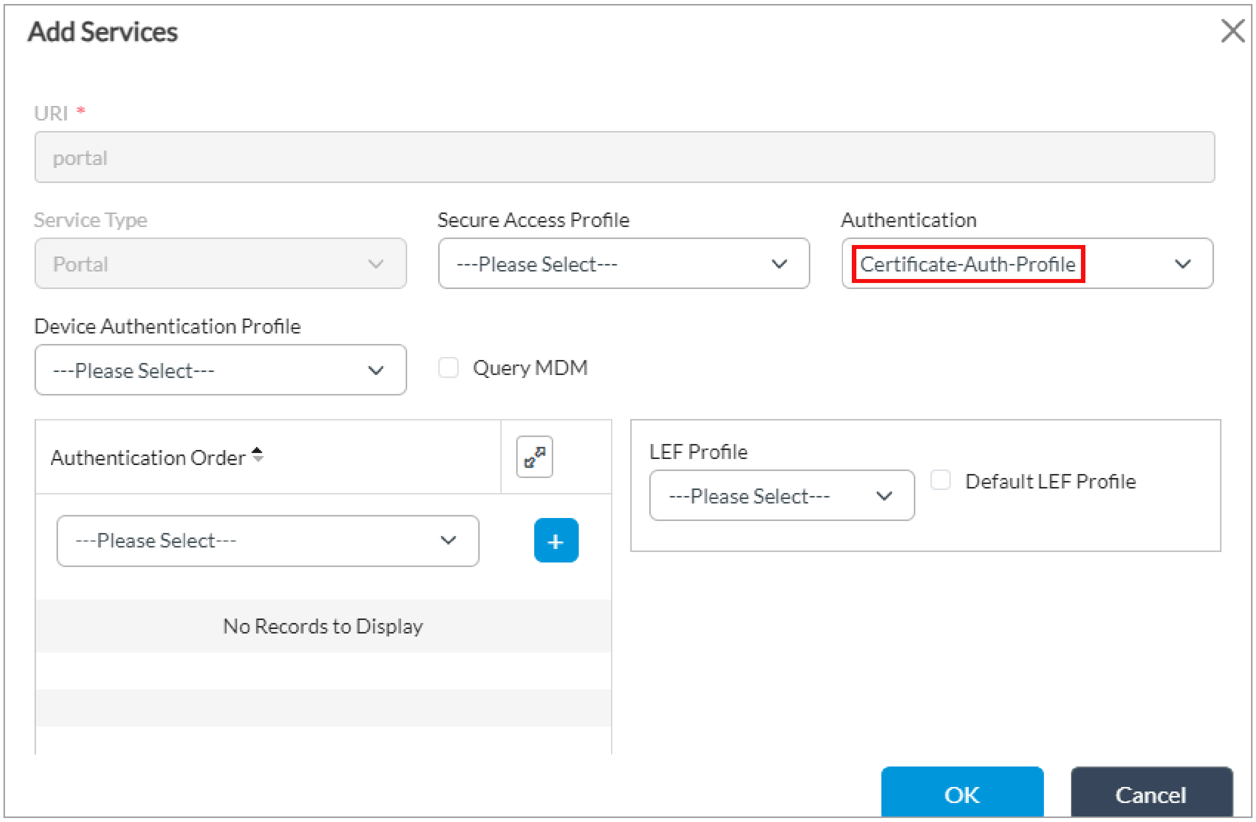


Appliance: BR2
Organization: Provider-ORG
You are currently in **Appliance View**

General

URI	: -
Secure Access Profile	: -
Service Type	: -
Authentication	: -
LEF Profile	: -
Default LEF Profile	: -
Device Authentication Profile	: -
Query MDM	: -
MDM Profile	: -
Authentication Order	: -

4. Click the ✎ Edit icon. The Add Services popup window displays.



Add Services

URI *: portal

Service Type: Portal

Secure Access Profile: ---Please Select---

Authentication: Certificate-Auth-Profile

Device Authentication Profile: ---Please Select---

□ Query MDM

Authentication Order: ---Please Select---

No Records to Display

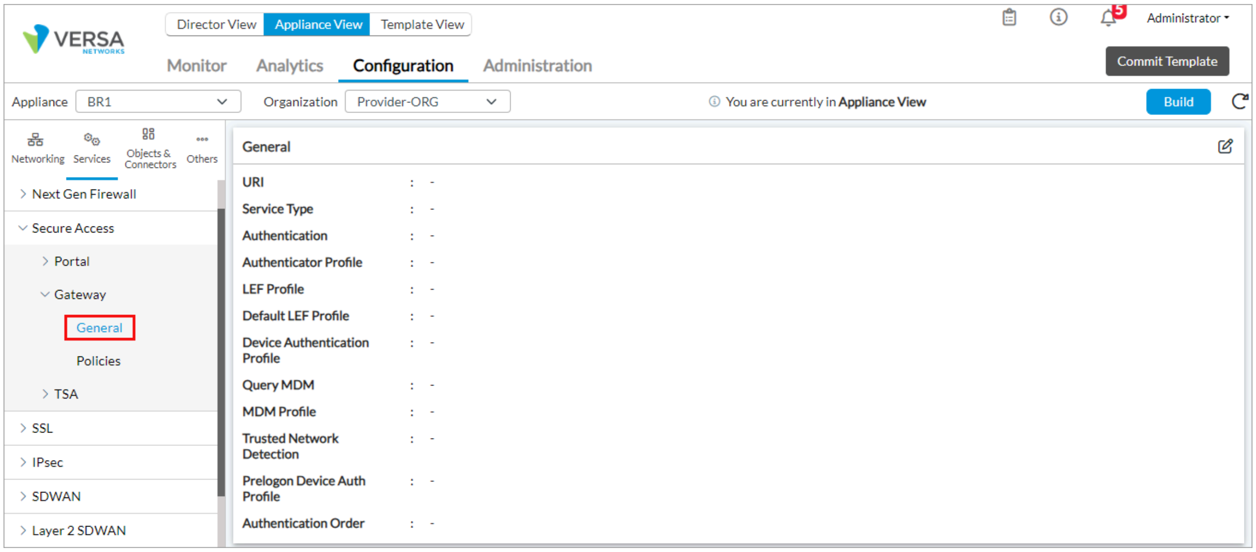
LEF Profile: ---Please Select---

□ Default LEF Profile

5. In the Authentication field, select the certificate authentication profile (here, Client-Cert-Auth-Profile) that you added in Configure a Certificate Authentication Profile, above.
6. For information about configuring other parameters, see Configure a Secure Access Gateway in Configure the Versa Secure Access Service.
7. Click OK.

Associate the Authentication Profile with the Secure Access Gateway

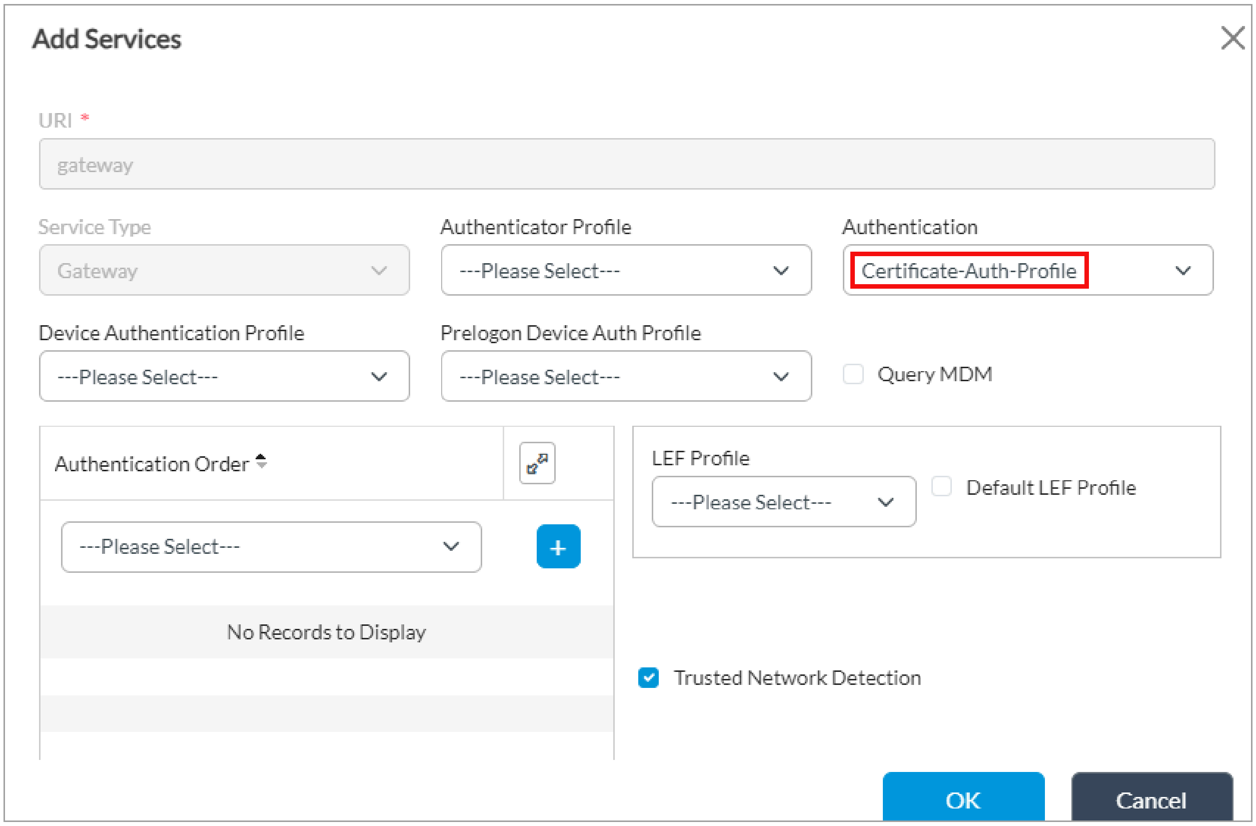
1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left menu bar.
   d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Secure Access > Gateway > General in the left menu bar.



General

URI : -
Service Type : -
Authentication : -
Authenticator Profile : -
LEF Profile : -
Default LEF Profile : -
Device Authentication Profile : -
Query MDM : -
MDM Profile : -
Trusted Network Detection : -
Prelogon Device Auth Profile : -
Authentication Order : -

4. Click the ✎ Edit icon. The Add Services popup window displays.



Add Services

URI * gateway

Service Type: Gateway

Authenticator Profile: ---Please Select---

Authentication: Certificate-Auth-Profile

Device Authentication Profile: ---Please Select---

Prelogon Device Auth Profile: ---Please Select---

□ Query MDM

Authentication Order: ---Please Select---

No Records to Display

LEF Profile: ---Please Select---

□ Default LEF Profile

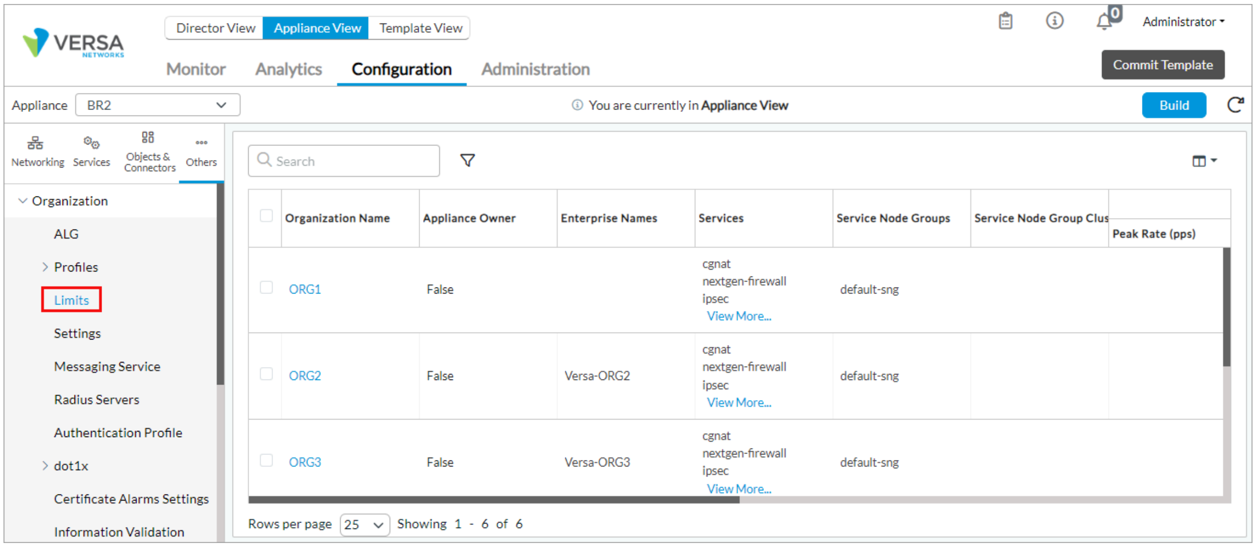
☑ Trusted Network Detection

5. In the Authentication field, select the certificate authentication profile (here, Client-Cert-Auth-Profile) that you added in Configure a Certificate Authentication Profile above.
6. For information about configuring other parameters, see Configure a Secure Access Portal in Configure the Versa Secure Access Service.
7. Click OK.

Modify the Organization Limit to Associate the Server Hostname with the Domain Name

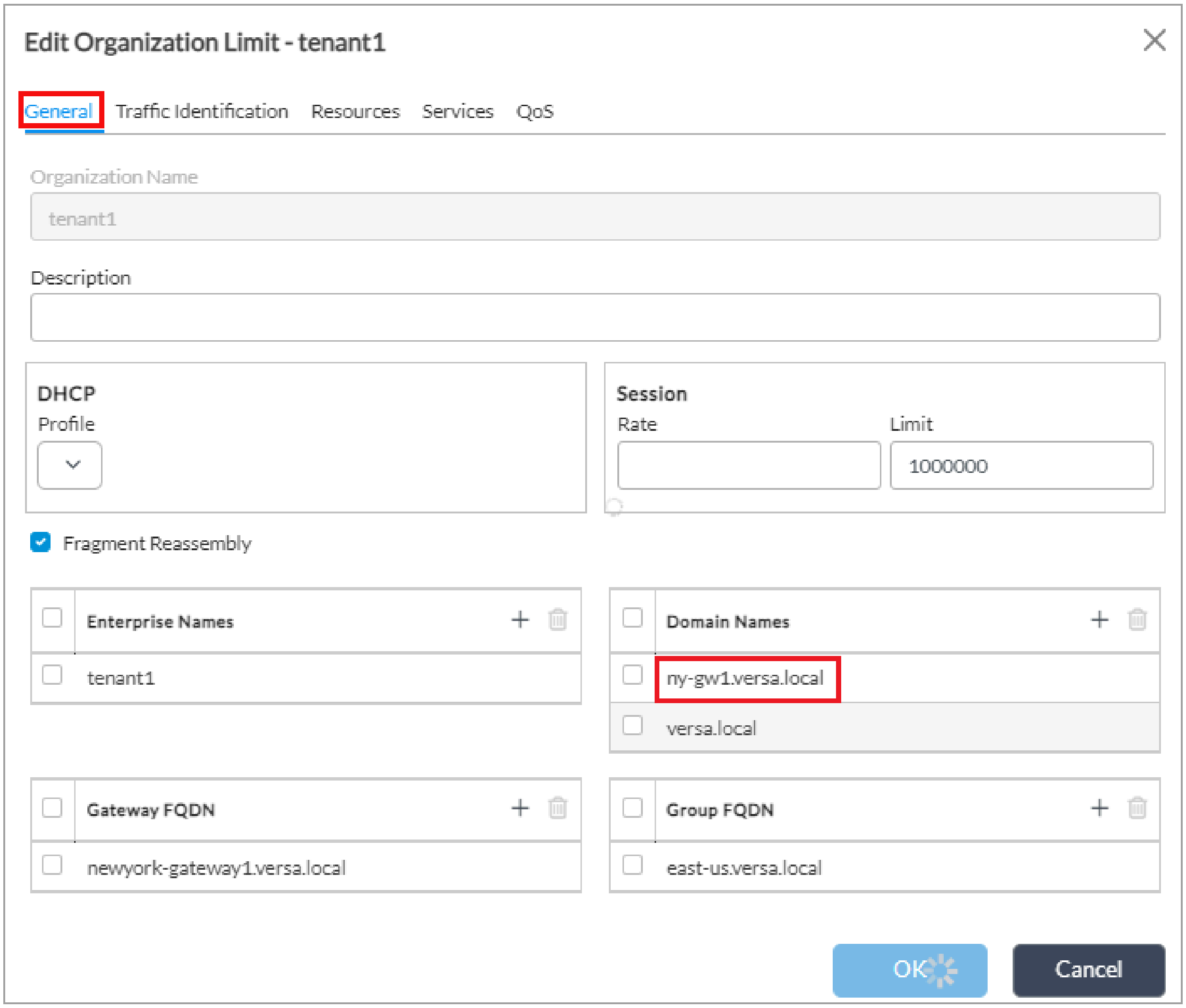
To modify organization (tenant) limits:

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.
    d. Select an organization.
2. Select the Configuration tab in the top menu bar.
3. Select Others > Organization > Limits in the left menu bar. The main pane displays the organizations associated with the Controller node.



Organization Name	Appliance Owner	Enterprise Names	Services	Service Node Groups	Service Node Group Clus	Peak Rate (pps)
ORG1	False		cgnat nextgen-firewall ipsec View More...	default-sng		
ORG2	False	Versa-ORG2	cgnat nextgen-firewall ipsec View More...	default-sng		
ORG3	False	Versa-ORG3	cgnat nextgen-firewall ipsec View More...	default-sng		

4. Select the General tab.



Organization Name: tenant1

Description:

DHCP

Profile:

Session

Rate:

Limit: 1000000

☑ Fragment Reassembly

□	Enterprise Names
□	tenant1

□	Domain Names
□	ny-gw1.versa.local
□	versa.local

□	Gateway FQDN
□	newyork-gateway1.versa.local

□	Group FQDN
□	east-us.versa.local

5. In the Domain Names field, click + and then select the host (here, ny-gw1.versa.local) that you added in the Server Hostname field in Configure a Certificate Authentication Profile, above.
6. For information about configuring other parameters, see Configure Organization Limits.
7. Click OK.

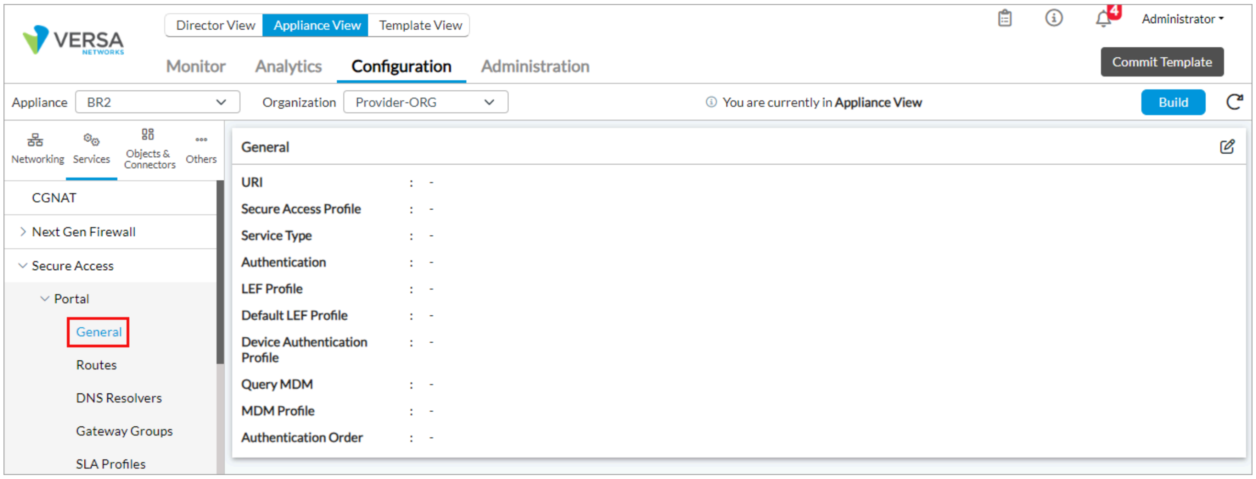
Configure Certificate-Based Device Authentication

To configure certificate-based device authentication, you do the following:

- Create a certificate authentication profile. For more information, see Configure a Certificate Authentication Profile, above.
- Modify the organization limit to add a certificate service hostname under domain names. For more information, see Modify the Organization Limit to Associate the Server Hostname with the Domain Name, above.
- Associate a certificate authentication profile with the secure access portal and with the secure access gateway.

Associate Certificate Authentication Profile with Secure Access Portal

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.

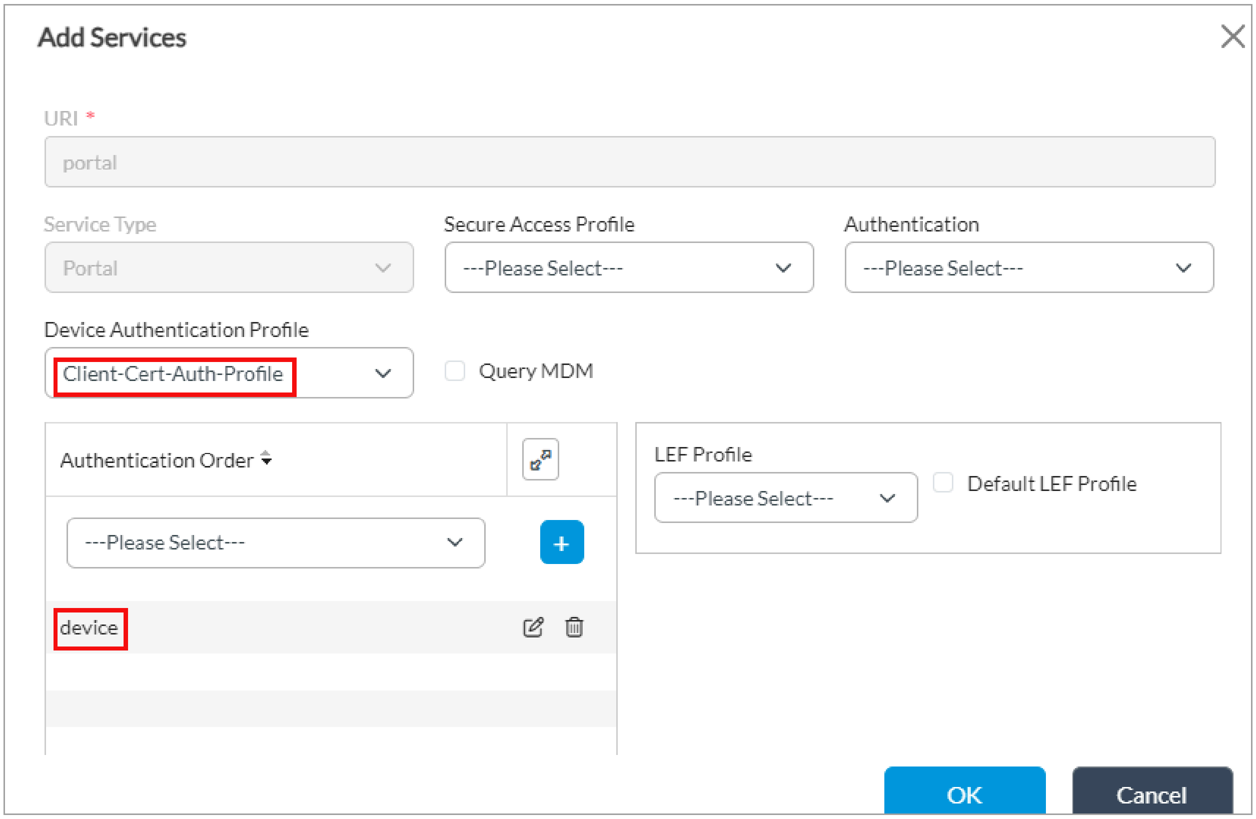


Appliance: BR2
Organization: Provider-ORG
You are currently in **Appliance View**

General

URI	:	-
Secure Access Profile	:	-
Service Type	:	-
Authentication	:	-
LEF Profile	:	-
Default LEF Profile	:	-
Device Authentication Profile	:	-
Query MDM	:	-
MDM Profile	:	-
Authentication Order	:	-

4. Click the ✎ Edit icon. The Add Services popup window displays.



Add Services

URI *

portal

Service Type: Portal

Secure Access Profile: ---Please Select---

Authentication: ---Please Select---

Device Authentication Profile: Client-Cert-Auth-Profile

□ Query MDM

Authentication Order

---Please Select---

device

LEF Profile: ---Please Select---

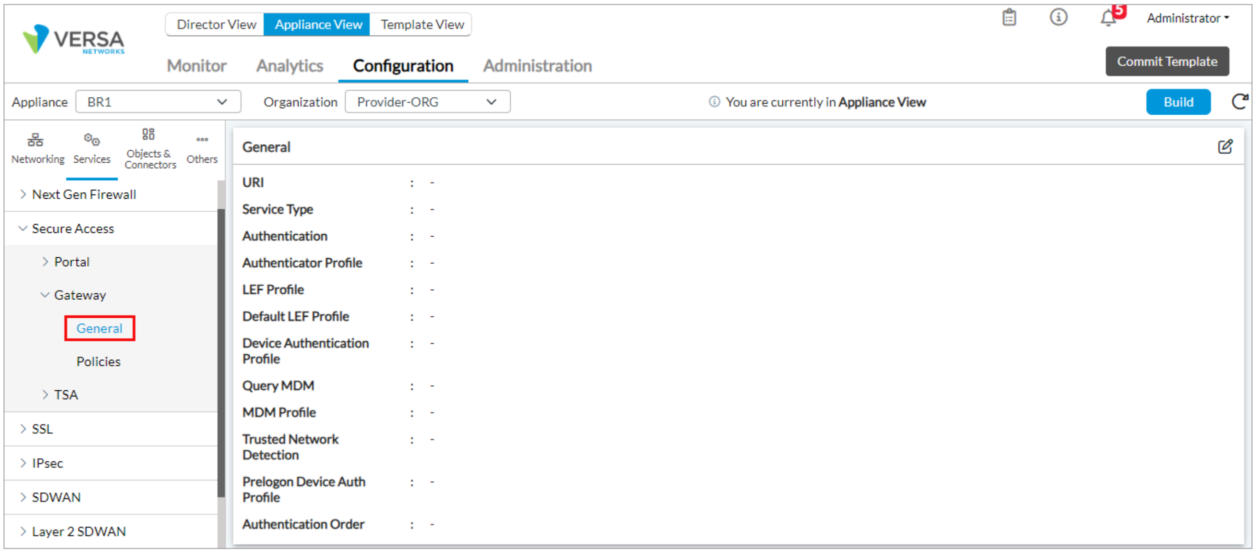
□ Default LEF Profile

5. In the Device Authentication Profile field, select the certificate authentication profile (here, Client-Cert-Auth-Profile) that you added in Configure a Certificate Authentication Profile, above.

6. In the Authentication Order field, select Device Authentication, and then click the + Add icon. The device option displays. Versa SASE supports multifactor authentication, so to authenticate users, also select User Authentication.
7. For information about configuring other parameters, see Configure a Secure Access Gateway in Configure the Versa Secure Access Service.
8. Click OK.

Associate the Certificate Authentication Profile with the Secure Access Gateway

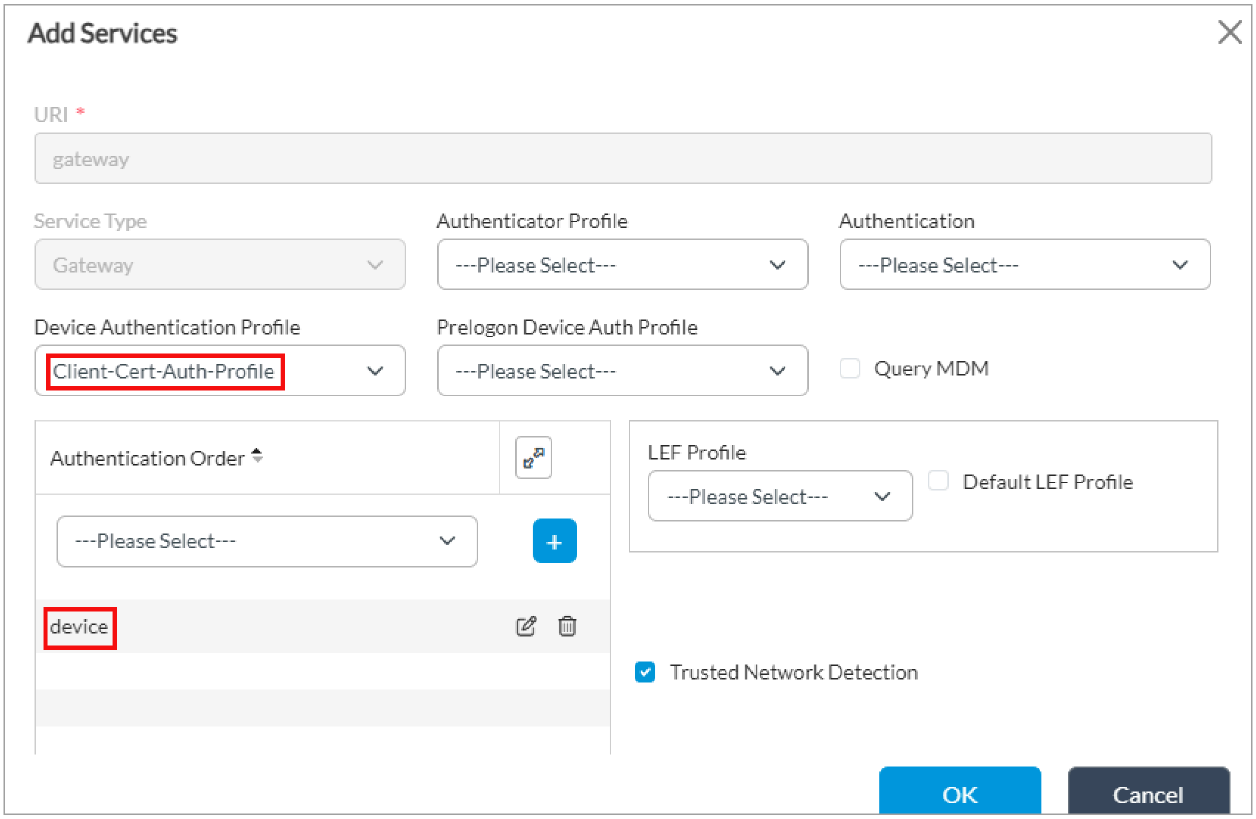
1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Templates > Device Templates in the horizontal menu bar.
   c. Select an organization in the left menu bar.
   d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Secure Access > Gateway > General in the left menu bar.



General

URI	:	-
Service Type	:	-
Authentication	:	-
Authenticator Profile	:	-
LEF Profile	:	-
Default LEF Profile	:	-
Device Authentication Profile	:	-
Query MDM	:	-
MDM Profile	:	-
Trusted Network Detection	:	-
Prelogon Device Auth Profile	:	-
Authentication Order	:	-

4. Click the ✎ Edit icon. The Add Services popup window displays.



Add Services

URI *
gateway

Service Type
Gateway

Authenticator Profile
---Please Select---

Authentication
---Please Select---

Device Authentication Profile
Client-Cert-Auth-Profile

Prelogon Device Auth Profile
---Please Select---

□ Query MDM

Authentication Order
---Please Select---
device

LEF Profile
---Please Select---

□ Default LEF Profile

☑ Trusted Network Detection

5. In the Device Authentication Profile field, select the certificate authentication profile (here, Client-Cert-Auth-Profile) that you added in Configure a Certificate Authentication Profile, above.

6. In the Authentication Order field, select Device Authentication, and then click the + Add icon. The device option displays. Versa SASE supports multifactor authentication, so to authenticate users, also select User

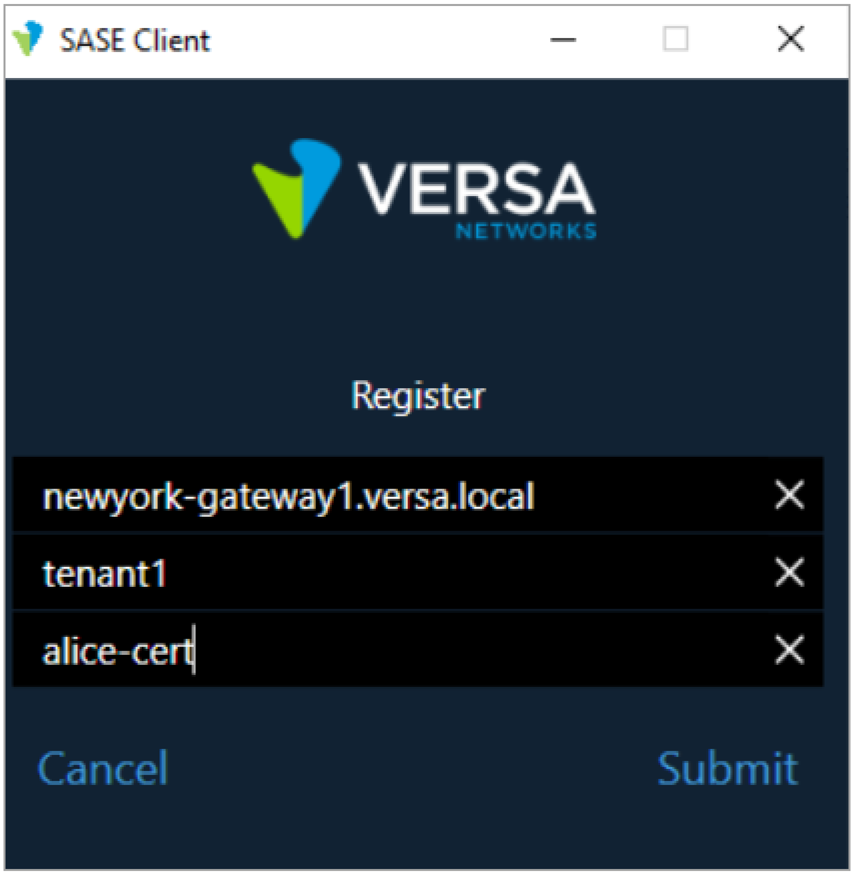
Authentication.

7. For information about configuring other parameters, see Configure a Secure Access Portal in Configure the Versa Secure Access Service.
8. Click OK.

Verify SASE Client Registration and Gateway Connectivity

To verify certificate-based authentication after you configure certificate-based device and user authentication for the SASE client:

1. Download the Versa SASE client. For more information, see Configure Versa SASE Clients.
2. Click Register in the Versa SASE Client home screen. The Register screen displays.

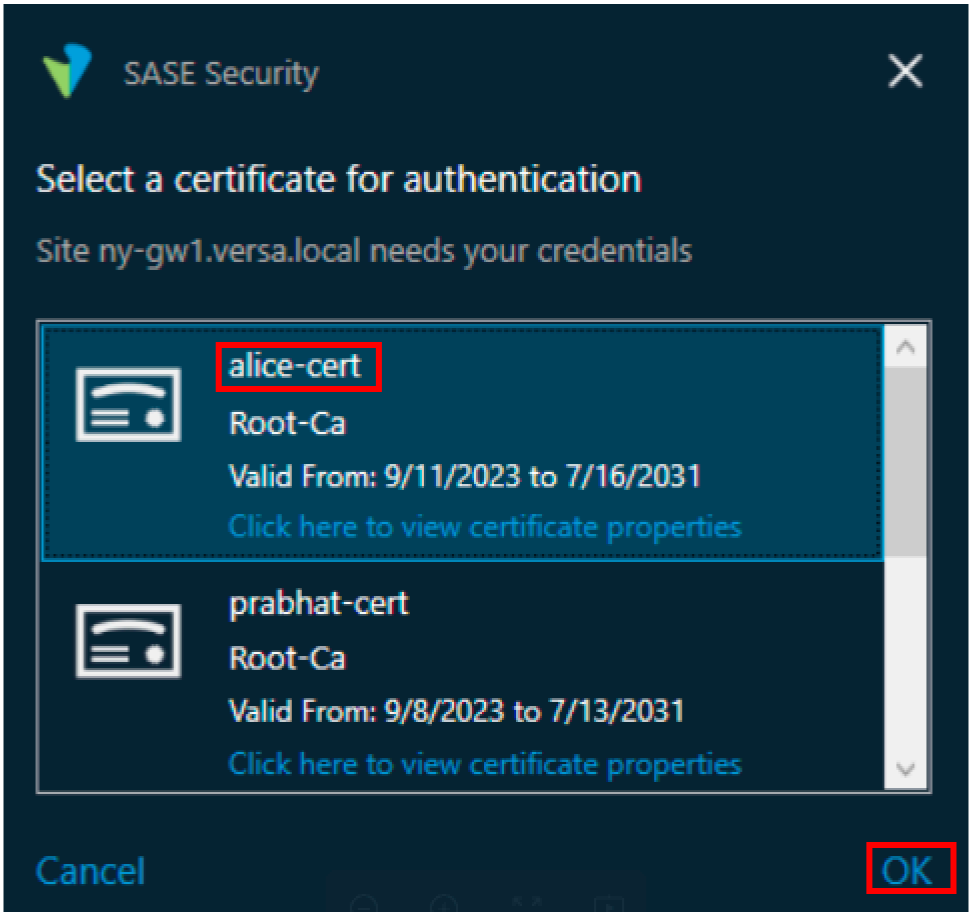


newyork-gateway1.versa.local

tenant1

alice-cert

3. Enter the gateway FQDN, tenant name, and username.
4. If there are multiple certificates on the device, the SASE Security window displays all of them. Select the appropriate certificate (here, alice-cert), and then click OK. If there is only one certificate, the SASE client automatically selects that certificate, and the following window does not display.



SASE Security

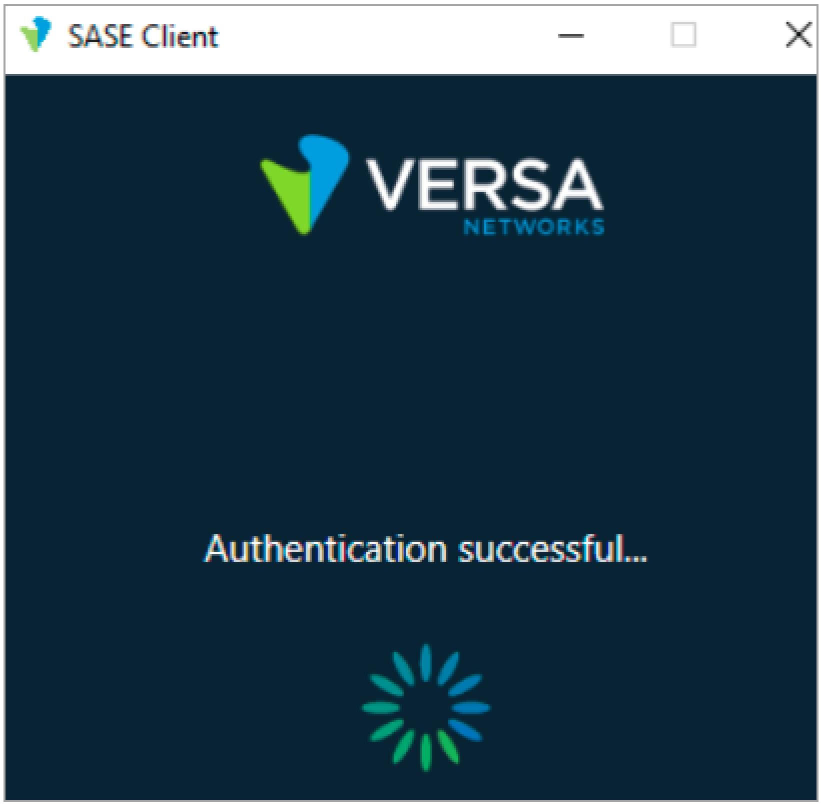
Select a certificate for authentication

Site ny-gw1.versa.local needs your credentials

alice-cert
Root-Ca
Valid From: 9/11/2023 to 7/16/2031
Click here to view certificate properties

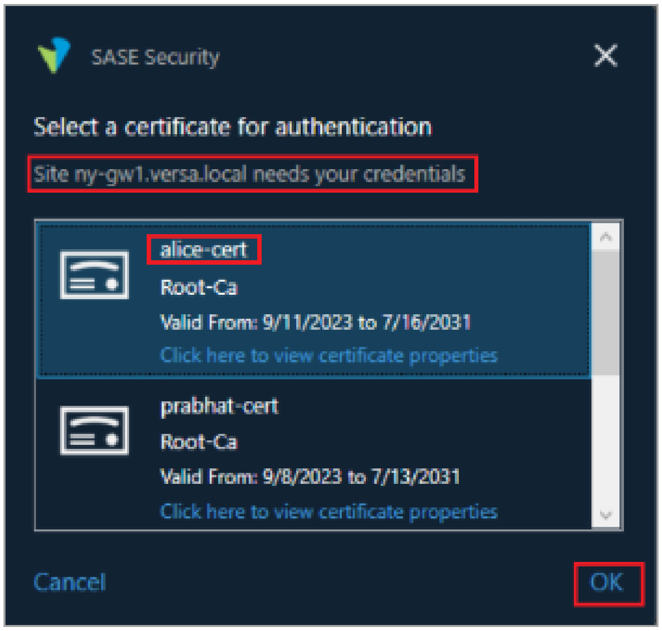
prabhat-cert
Root-Ca
Valid From: 9/8/2023 to 7/13/2031
Click here to view certificate properties

5. If authentication is successful, the following window displays.



Authentication successful...

6. After you register the SASE client, select the gateway or group FQDN to log in. If certificate-based authentication is configured on the VOS SASE gateway, the Select a Certificate for Authentication popup window displays.



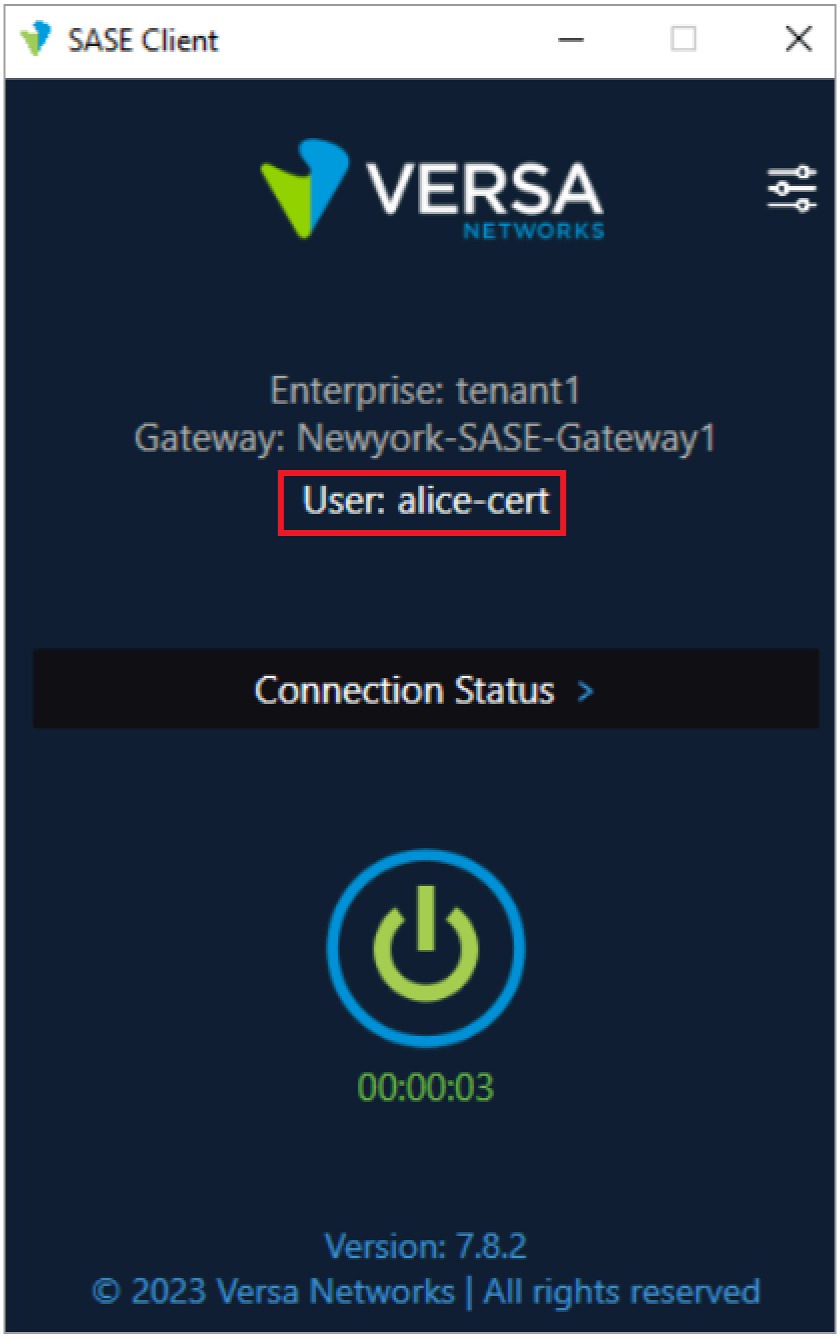
Select a certificate for authentication

Site ny-gw1.versa.local needs your credentials

alice-cert
Root-Ca
Valid From: 9/11/2023 to 7/16/2031
Click here to view certificate properties

prabhat-cert
Root-Ca
Valid From: 9/8/2023 to 7/13/2031
Click here to view certificate properties

7. Select the certificate (here, alice-cert) that you want to use for the device or user authentication, and then click OK. The connection status window displays on successful connection.



Enterprise: tenant1
Gateway: Newyork-SASE-Gateway1
User: alice-cert

Supported Software Information

Releases 22.1.1 and later support all content described in this article.

Additional Information

Configure User and Group Policy
Configure Versa SASE Clients
Configure the Versa Secure Access Service
Create and Manage Certificates
Use the Versa SASE Client Application