

Configure CA Certificates, Key File, and CA Chains

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


A certificate authority (CA) is a trusted entity that issues electronic documents. The CA certificate verifies a digital entity's identity on the internet. The electronic documents, which are called digital certificates, are an essential part of secure communication.

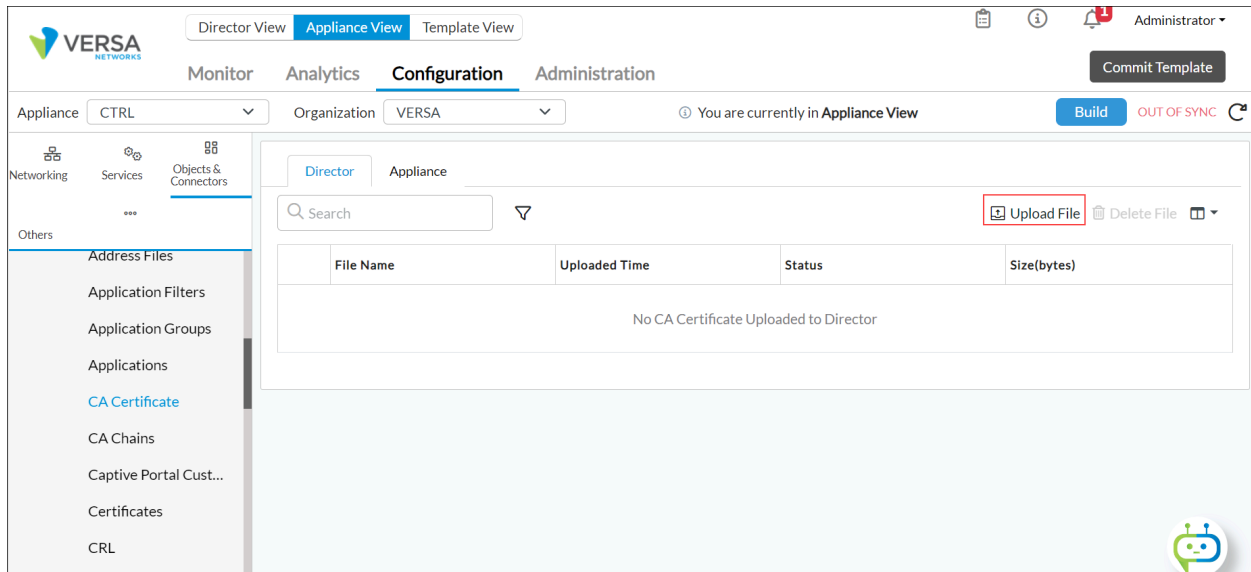
A private key is required to access secured traffic using a certificate. To secure the traffic on a Versa Operating System™ (VOS™) device, you can use either a self-signed CA certificate or a trusted CA certificate.

A certificate chain is an ordered list of certificates, containing an SSL/TLS certificate and CA certificates, that allow the receiver to verify that the sender and all CA's are trustworthy.

This article describes how to upload a CA certificate, a private key file, and a CA chain first to the Director node and then to a VOS device.

Upload a CA Certificate

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 a 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 Certificate in the left menu bar.
4. In the Director tab, click the  Upload File icon to upload a CA certificate file to the Director node.



5. In the Upload CA Certificate to Director popup window, enter information for the following fields.

Upload CA Certificate to Director

File Name *

Browse

CA Chain

▼

Note :

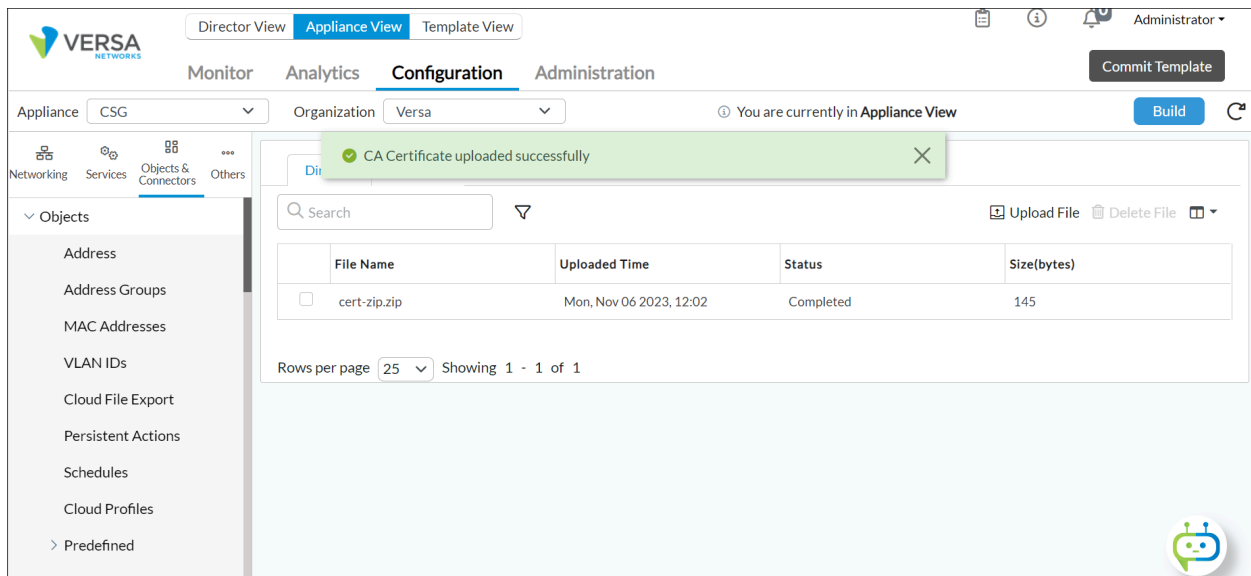
- The file to be uploaded need to be in .zip format. They will consist of 2 files a key and a certificate. The key file needs to have .key extension there is no restriction on the extension of the certificate file.
- CA Chain is Mandatory for 22.1 devices and above


OK

Cancel

Field	Description
File Name (Required)	Click Browse, and then select the CA certificate file to upload to the Director node.
CA Chain	For devices running Releases 22.1.1 and later, select the CA chain.

- Click OK to upload the file to the Director node.



- Select the Appliance tab.
- Click the  Upload File icon to upload a CA certificate file to the selected VOS device.
- In the Upload CA Certificate to Appliance popup window, enter information for the following fields.

Upload CA Certificate to Appliance

✕

File Name *

cert-zip.zip

▼

Appliance

CSG

▼

CA Chain

Intermediate

▼

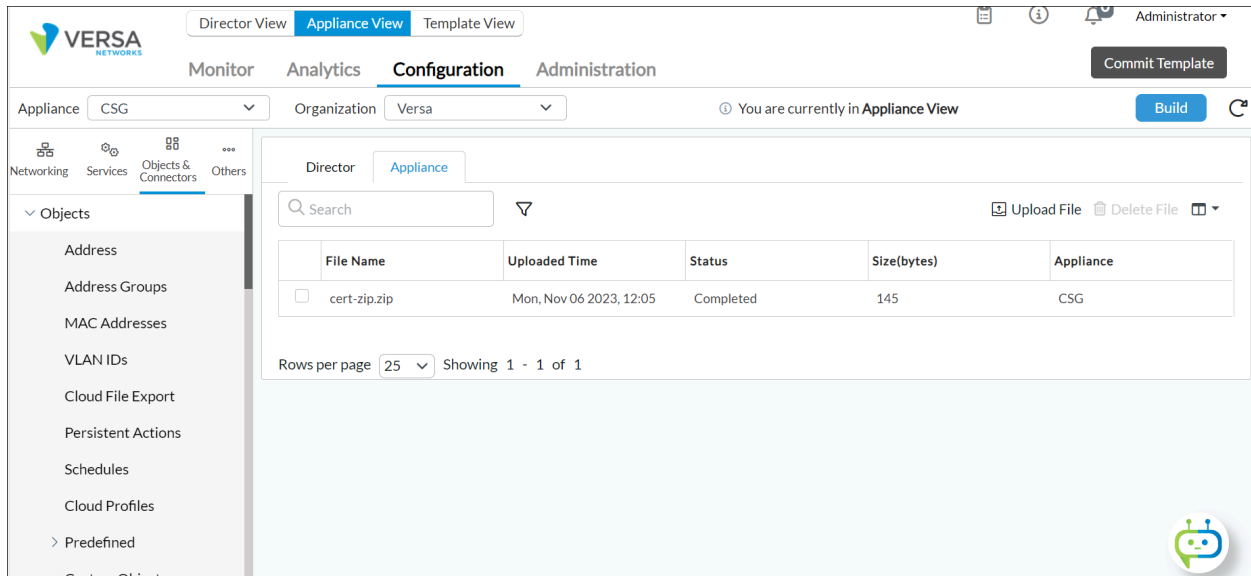
Note - CA Chain is Mandatory for 22.1 devices and above

OK

Cancel

Field	Description
File Name (Required)	Select the CA certificate file to upload to the VOS device.
Appliance	Select the VOS device to upload the CA certificate file.
CA Chain	For devices running Releases 22.1.1 and later, select the CA chain for the devices.


- Click OK to upload the file to the VOS device.



For information about creating a CA certificate, see [Create a CA Certificate](#).

Upload a Private Key

For Releases 22.1.3 and later.

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 a Controller or VOS 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 > Keys in the left menu bar.
4. In the Director tab, click the  Upload File icon to upload the private key file to the Director node.
5. In the Upload Key File to Director popup window, enter information for the following fields.

Upload Key File to Director

Key Name *

Pass Phrase

Key File Name *


Field	Description
Key Name (Required)	Enter a name for the key file.
Passphrase	Enter a passphrase.
Key Filename (Required)	Click the Browse button, and then select the key file to upload to the Director node.

- Click OK to upload the file.

The screenshot shows the Versa Networks Appliance View interface. The top navigation bar includes tabs for Director View, Appliance View (selected), and Template View. Below this, there are tabs for Monitor, Analytics, Configuration (selected), and Administration. The left sidebar shows a tree view with categories like Networking, Services, Objects & Connectors, and Others. Under Objects & Connectors, the 'Keys' option is selected. The main content area displays a table with the following data:

	Key Name	Key File Name	Date Uploaded
<input type="checkbox"/>	gcp_srv_acc_priv_key	gcp_srv_acc_priv_key.key	Sat, Oct 07 2023, 01:05
<input type="checkbox"/>	versa-staging	versa-staging.key	Tue, Oct 10 2023, 02:40

Below the table, it shows 'Rows per page' set to 25 and 'Showing 1 - 2 of 2'. There are also buttons for 'Upload File', 'Delete File', and a refresh icon.

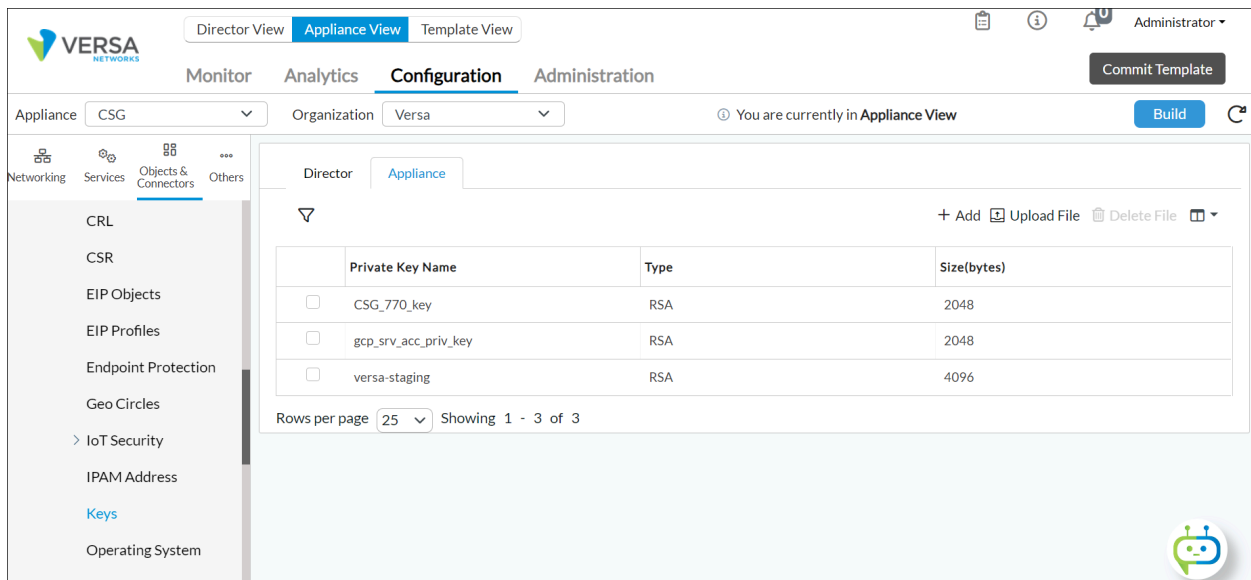
7. Select the Appliance tab.
8. Click the  Upload File icon to upload a key file to the selected VOS device.
9. In the Upload Key File to Appliance popup window, enter information for the following fields.

The screenshot shows a popup window titled 'Upload Key File to Appliance'. It contains the following fields and buttons:

- Name ***: A dropdown menu with 'versa-staging' selected.
- Appliance**: A dropdown menu with 'CSG' selected.
- Pass Phrase**: A text input field.
- OK**: A blue button.
- Cancel**: A dark blue button.


Field	Description
Name (Required)	Select the key file to upload to the VOS device.
Appliance	Select the VOS device to upload the key file.
Passphrase	Enter a passphrase.

10. Click OK to upload the file to the VOS device.



For information about creating a private key, see [Create a Private Key for a CA Certificate](#).

Upload a CA Chain

- In the Director view:
 - Select the Configuration tab in the top menu bar.
 - Select Devices > Devices in the horizontal menu bar.
 - Select a Controller or VOS device in the dashboard. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Objects & Connectors > Objects > Custom Objects > CA Chains in the left menu bar.
- Click the  Upload icon to upload the CA chain file. The file must be in .crt, .cer, or .pem format.

Upload CA Chain to Director

✕

Chain Name *

Chain File Name *

Browse

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

OK

Cancel

Field	Description
Chain Name (Required)	Enter a name for the CA chain.
Chain Filename (Required)	Click Browse to select the chain file to upload to the Director node. The chain file must be in .cer, .crt, or .pem format.

- Click OK to upload the file.

Director View | **Appliance View** | Template View

Monitor | Analytics | **Configuration** | Administration

Appliance: CSG | Organization: Versa | You are currently in Appliance View

Networking | Services | **Objects & Connectors** | Others


Address Files
Application Filters
Application Groups
Applications
CA Certificate
CA Chains
Captive Portal Cust...
Certificates
CRL
CSR
FID Objects

Director | Appliance

Upload File | Delete File

	Chain Name	Chain File Name	Date Uploaded
<input type="checkbox"/>	Intermediate	Intermediate.crt	Mon, Oct 09 2023, 18:26
<input type="checkbox"/>	SD-GCP	SD-GCP.crt	Tue, Oct 10 2023, 02:37
<input type="checkbox"/>	versa-branch-staging	versa-branch-staging.chain.crt	Tue, Oct 10 2023, 02:43

Rows per page: 25 | Showing 1 - 3 of 3

6. Select the Appliance tab.
7. Click the  Upload File icon, and then select the name of the CA chain file to upload to the VOS device.

Upload CA Chain File to Appliance

Name *

versa-branch-staging

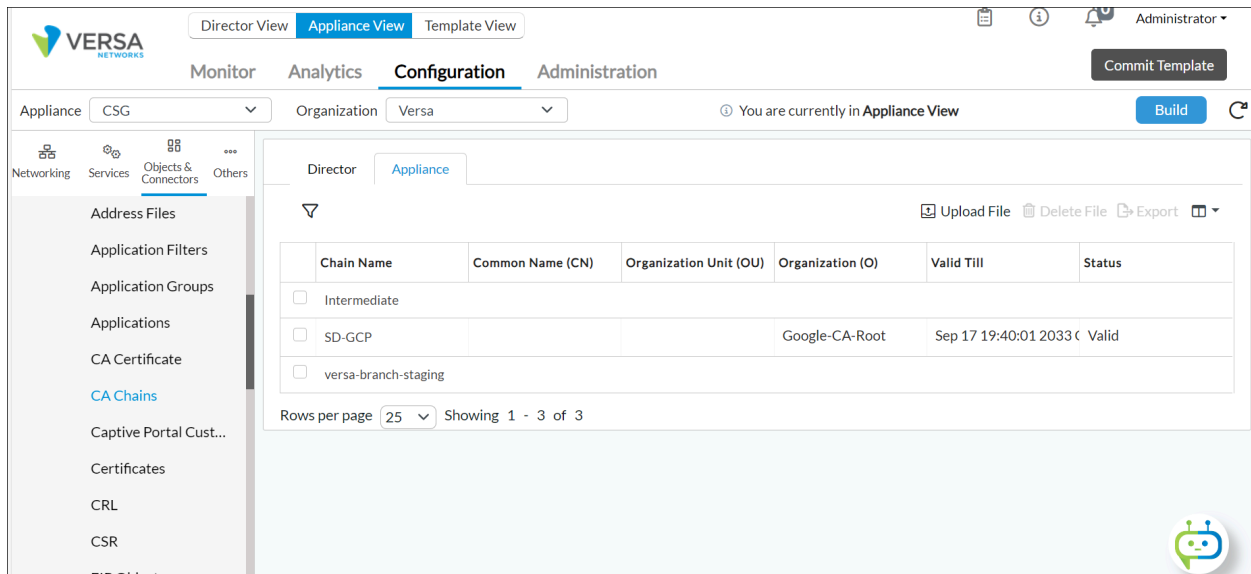
Appliance

CSG

OK

Cancel

8. Click OK to upload the file to the VOS device.



Apply CA Certificates, Private Key, and CA Chains

After you configure a CA certificate, private key, and CA chain, you associate them with a VPN profile so that the certificate and chain can be used:

1. In Director view:
 1. Select the Configuration tab in the top menu bar.
 2. Select Devices > Devices in the horizontal menu bar.
 3. Select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > IPsec > VPN Profiles in the left menu bar.
4. Click the + Add icon to create a VPN profile. The Add IPsec VPN window displays.

Director View **Appliance View** Template View

Monitor Analytics **Configuration** Administration

Appliance CSG Organization Versa You are currently in Appliance View

Networking Services Objects & Connectors Others

CGNAT

> Next Gen Firewall

> IPsec

VPN Profiles

Branch SDWAN Profile

> SDWAN

> Layer 2 SDWAN

Web Proxy

Captive Portal

Search + Add Delete Clone

VPN Profile	VPN Type	Local IP/Interface/Hostn	Peer IP/FQDN/Hostname	Auth Type	Local Auth Info
<input type="checkbox"/> Controller-1-Profile	branch-sdwan	tvi-0/2.0	10.0.11.1	psk	id-type = email key = cun5DBX4Zrks+j... id-string = CSG@Versa...
<input type="checkbox"/> Controller-2-Profile	branch-sdwan	tvi-0/2.0	10.0.11.5	certificate	cert-name = CSG_770_... ca-chain = SD-GCP cert-domain = tenant

Rows per page 25 Showing 1 - 2 of 2

5. In the Add IPsec VPN popup window, select the IKE tab, and then enter information for the following fields.

Add IPsec VPN

General
IKE
IPsec

Version
v2

Fragment Size
576

DPD Timeout (secs)
30

Auth Domain

Revocation Check
None

Rekey Time
Seconds
28800

Transform & DH Group
Multiple Transforms
Single Transform

Hash Algorithm
+

Encryption Algorithm
+

DH Group
+

Hash Algorithm Not Configured
Encryption Algorithm Not Configured
DH Group Not Configured

Local Auth
Authentication Type *
Certificate Domain
Certificate Name *
CA Chain *

Certificate
Tenant
--Select--
--Select--

Provider Org
--Select--

Peer Auth
Authentication Type *
CA Chain *

Certificate

OK
Cancel

Field	Description
Local Authentication (Group of Fields)	
◦ Authentication Type (Required)	Select Certificate
◦ Certificate Domain	Select Tenant

Field	Description
◦ Certificate Name (Required)	Select the name of the certificate that you uploaded to the Director and VOS devices.
◦ CA Chain (Required)	Select the CA chain that you uploaded to the Director and VOS devices.
Peer Authentication (Group of Fields)	
◦ Authentication Type (Required)	Select Certificate.
◦ CA Chain (Required)	Select the CA chain that you uploaded to the Director and VOS devices.

6. For information about configuring other parameters, see [Configure IPsec VPN Profiles](#).
7. Click OK.

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Releases 22.1.3 adds support for uploading private key file to Director and VOS devices.

Additional Information

[Configure Certificate Servers](#)

[Configure IPsec VPN Profiles](#)

[Configure User and Group Policy](#)

[Manage Files and Folders](#)

[Troubleshoot Analytics Access and Certificate Issues](#)