Configure SD-WAN Certificates

For supported software information, click here.

A certificate authority (CA) is a trusted third-party organization that issues electronic documents, called digital certificates. A CA certificate is a small data file issued by a CA that verifies a digital entity's identity on the internet and indicates that the website is secured using an encrypted connection. CA certificates are an essential part of secure communication.

Versa Networks provides a set of self-signed trusted certificates that enable secure data transfer between web servers and the clients using secure socket layer (SSL) encryption. You can also add additional certificates, such as certificates for LDAP and IPsec tunnels.

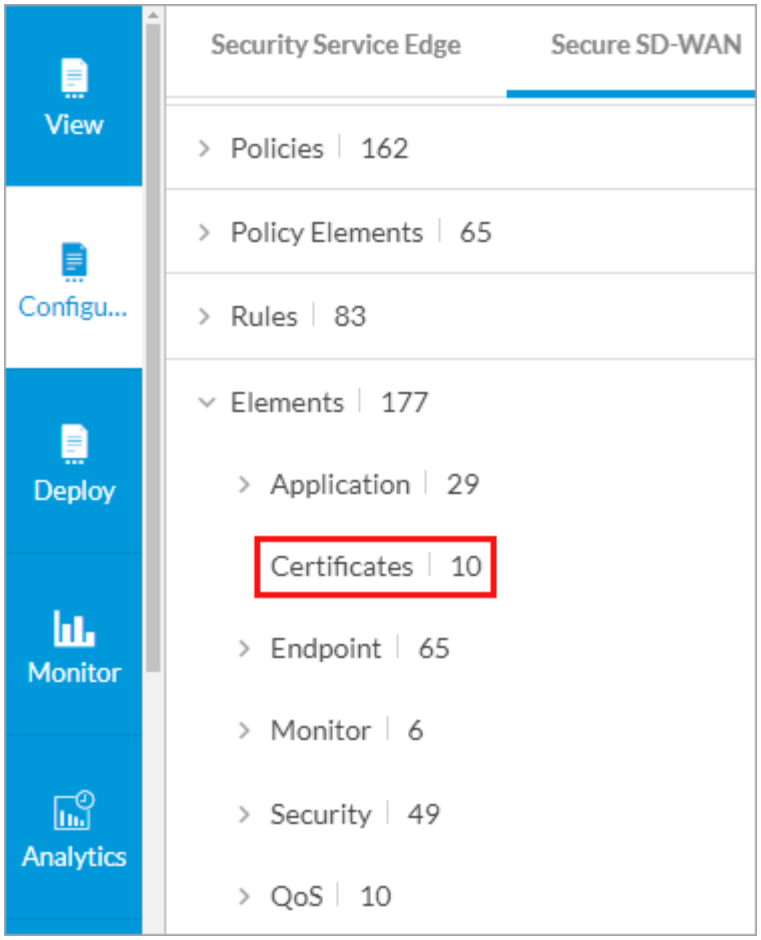
A CA chain is an ordered list of the CA certificates for all trustworthy intermediate and end devices in a communications chain.

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.

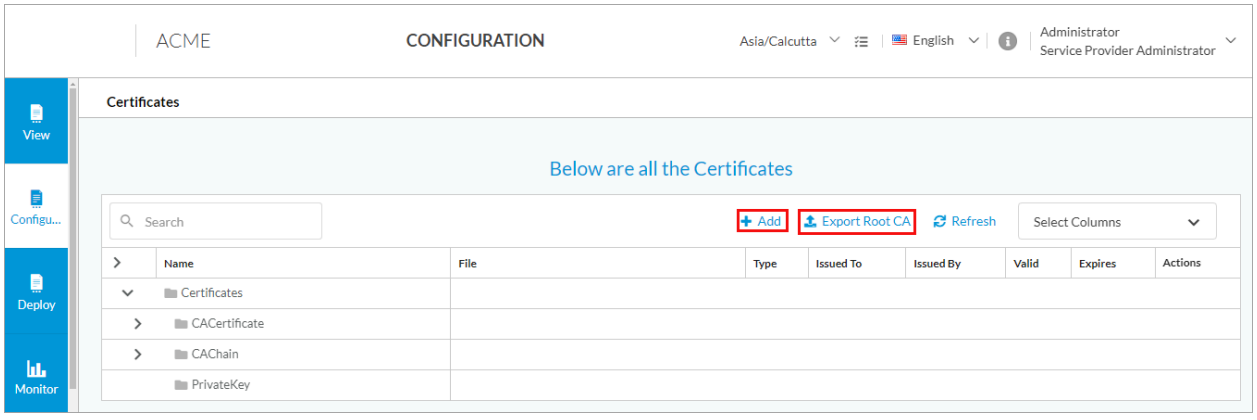
This article describes how to upload a CA certificate, a CA chain, and a private key file to the Concerto node.

To configure certificates and a private key file:

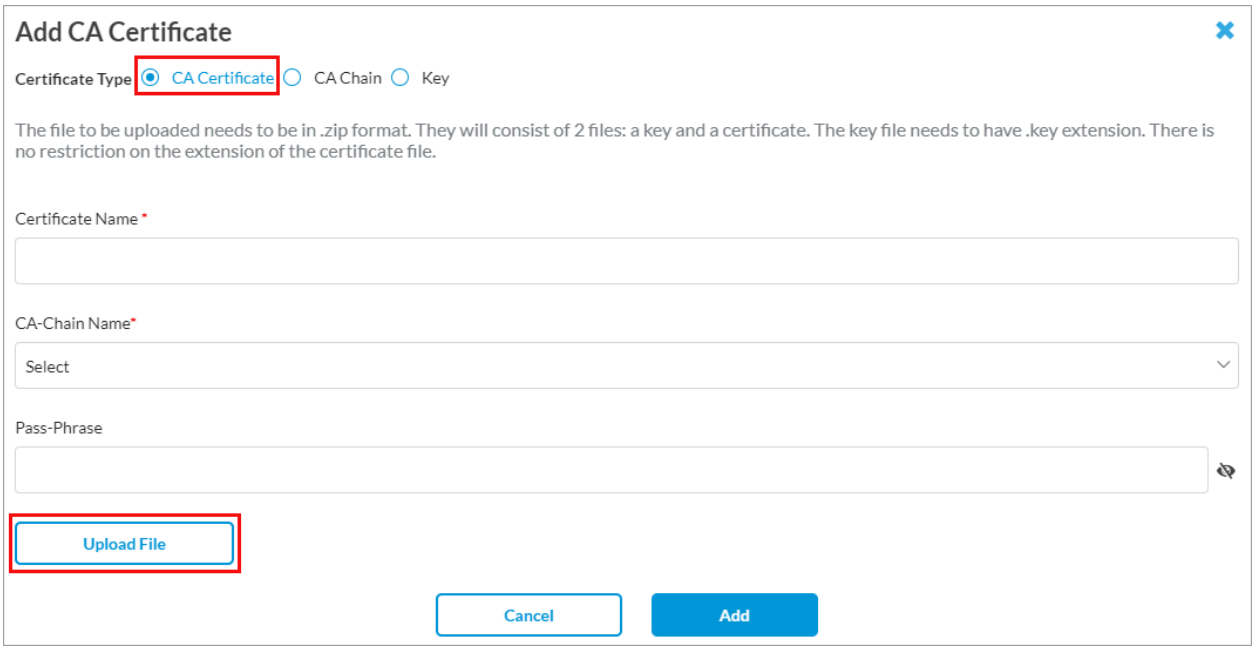
1. Go to Configure > Secure SD-WAN > Profile Elements > Elements > Certificates.



The Certificates screen displays all currently available certificates, including the default Versa Cert certificate, which is supplied by Versa Networks, and the Versa CA Chain.



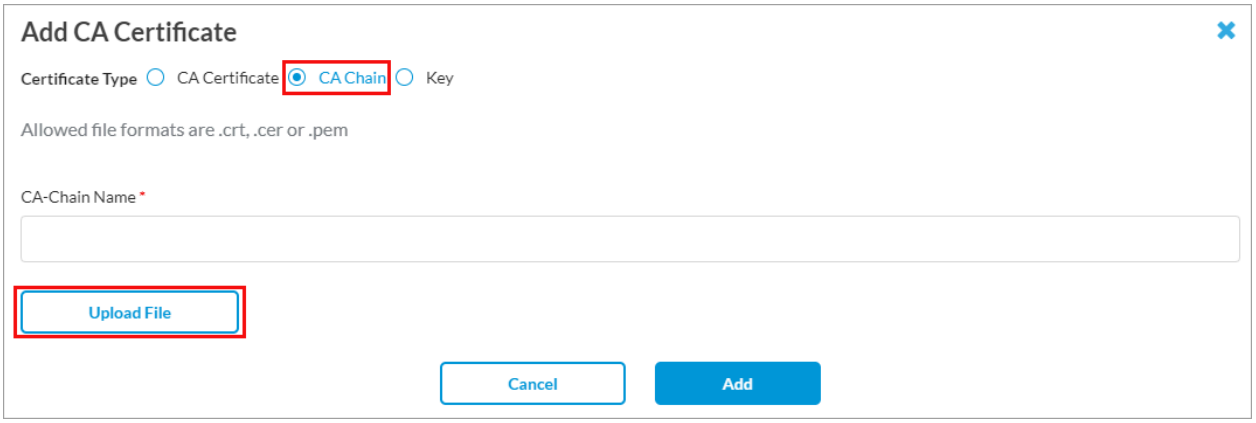
2. Click + Add to add certificates. The Add CA Certificate popup window displays.



3. To add a CA certificate, click CA Certificate, and then enter information for the following fields.

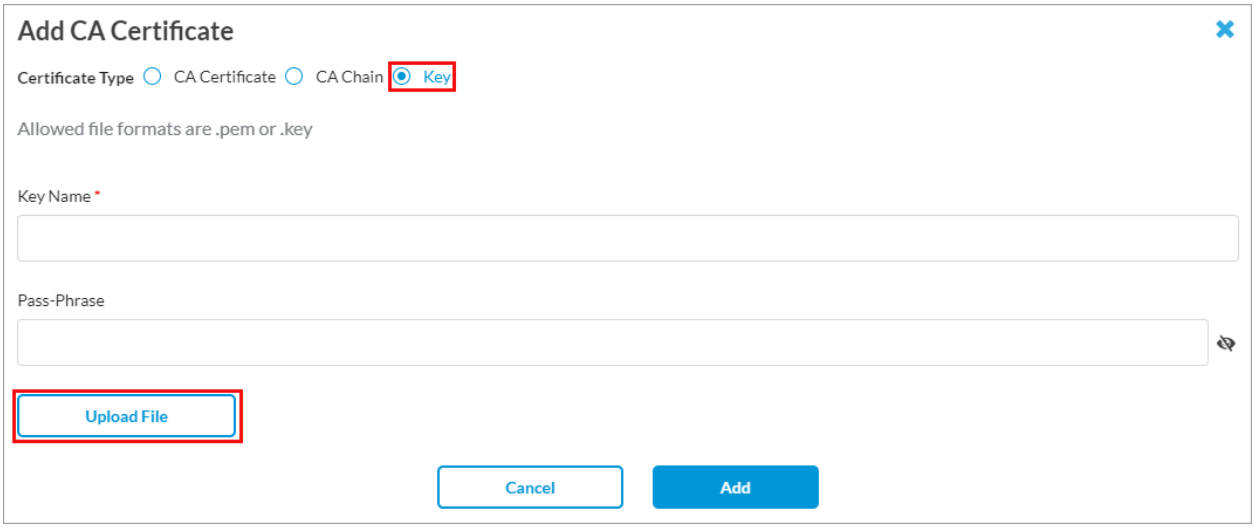
Field	Description
Certificate Name (Required)	Enter a name for the certificate.
CA Chain (Required)	Select the CA chain.
Passphrase	Enter a passphrase.
Upload File	Click to upload the CA certificate file. The file must be in .zip format.
Add	Click to add the new certificate.

4. To add a CA Chain certificate, click CA Chain, and then enter information for the following fields.



Field	Description
CA Chain Name (Required)	Enter a name for the CA chain.
Upload File	Click to upload the CA chain certificate file. The file must be in .cer, .crt, or .pem format.
Add	Click to add the new certificate.

5. To add a private key file, click Key, and then enter information for the following fields.



Field	Description
Key Name (Required)	Enter a name for the key file.
Passphrase	Enter a passphrase.
Upload File	Click to upload the private key file. The file must in be

Field	Description
	.pem or .key format.
Add	Click to add the new certificate.

Supported Software Information

Releases 12.1.1 and later support all content described in this article.

Additional Information

Configure SASE Certificates