Configure SASE 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 verifies a digital entity's identity on the internet. 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.

You can onboard and manage the certificates needed by a tenant. You use these certificates when you configure profiles and rules.

There are two types of certificates:

- CA certificate—A small data file issued by a CA that contains information that indicates that the website is secured using an encrypted connection.
- CA chain—An ordered list of the CA certificates for all trustworthy intermediate and end devices in a communications chain.

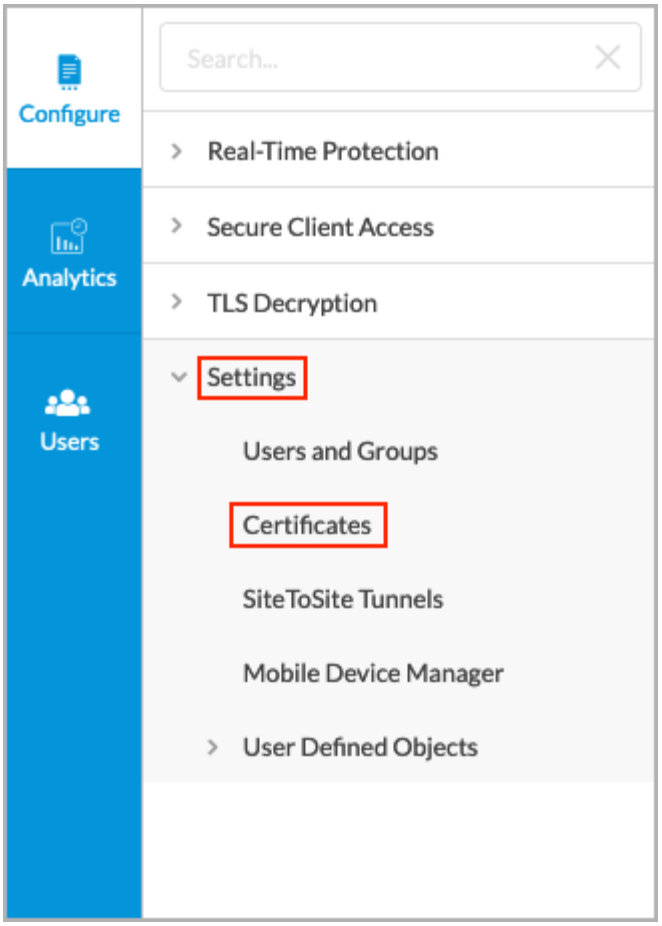
Note: You must configure the SASE rules, profiles, and settings in the following order:

1. Configure users and groups first, and then publish them to the gateway. For more information, see Configure Users and Device Authentication.
2. Configure site-to-site tunnels. For more information, see Configure SASE Site-to-Site Tunnels.
3. Configure secure client access profiles and rules. For more information, see Configure SASE Secure Client Access Rules.

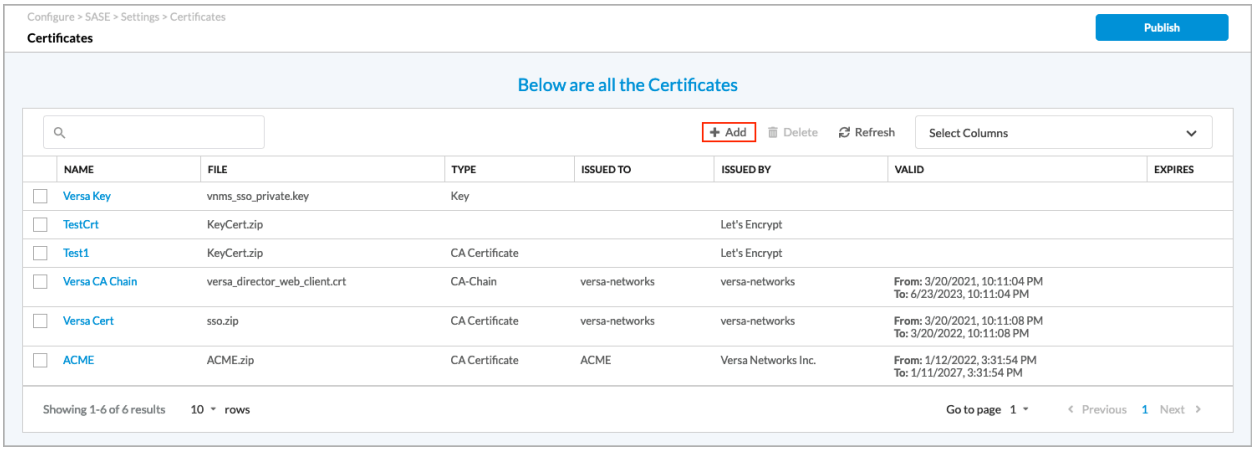
You do not need to configure the remaining SASE rules, profiles, and settings in any particular order.

To configure certificates:

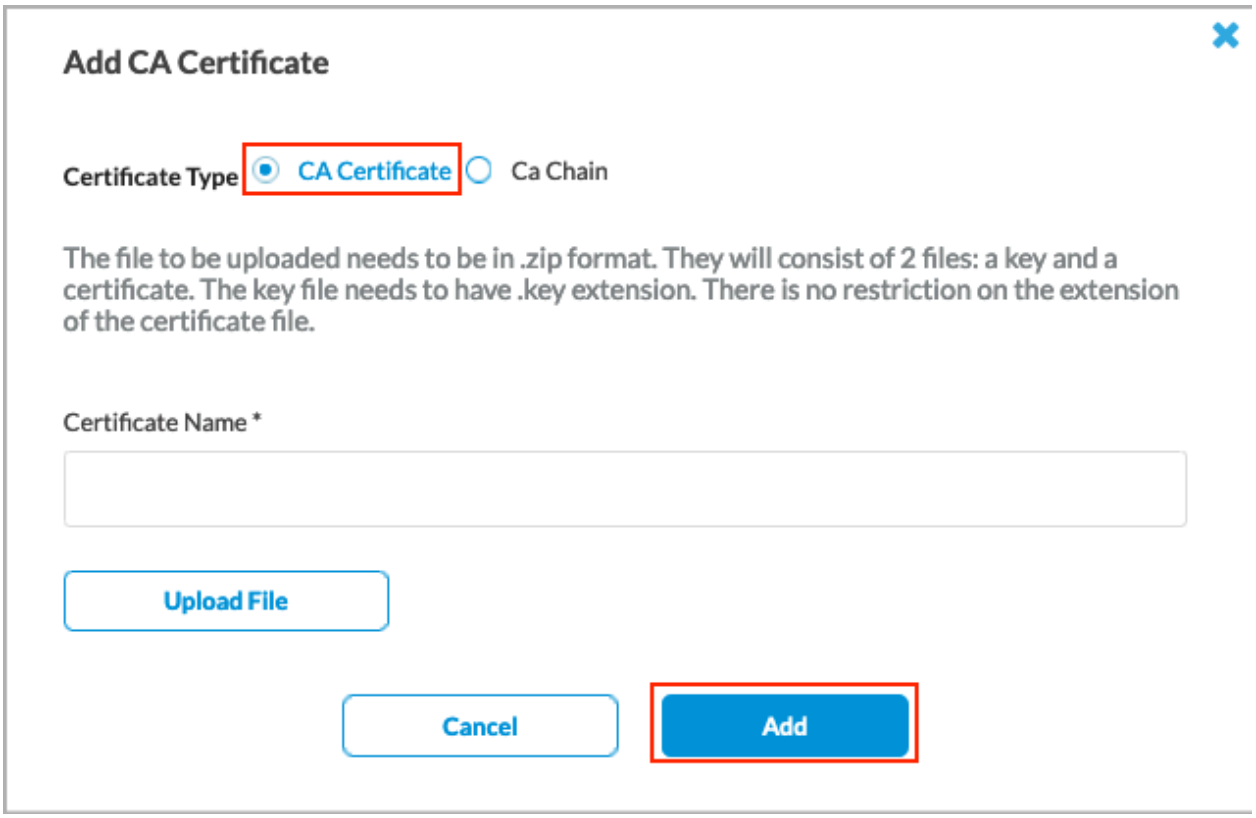
1. Go to Configure > Settings > Certificates.



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



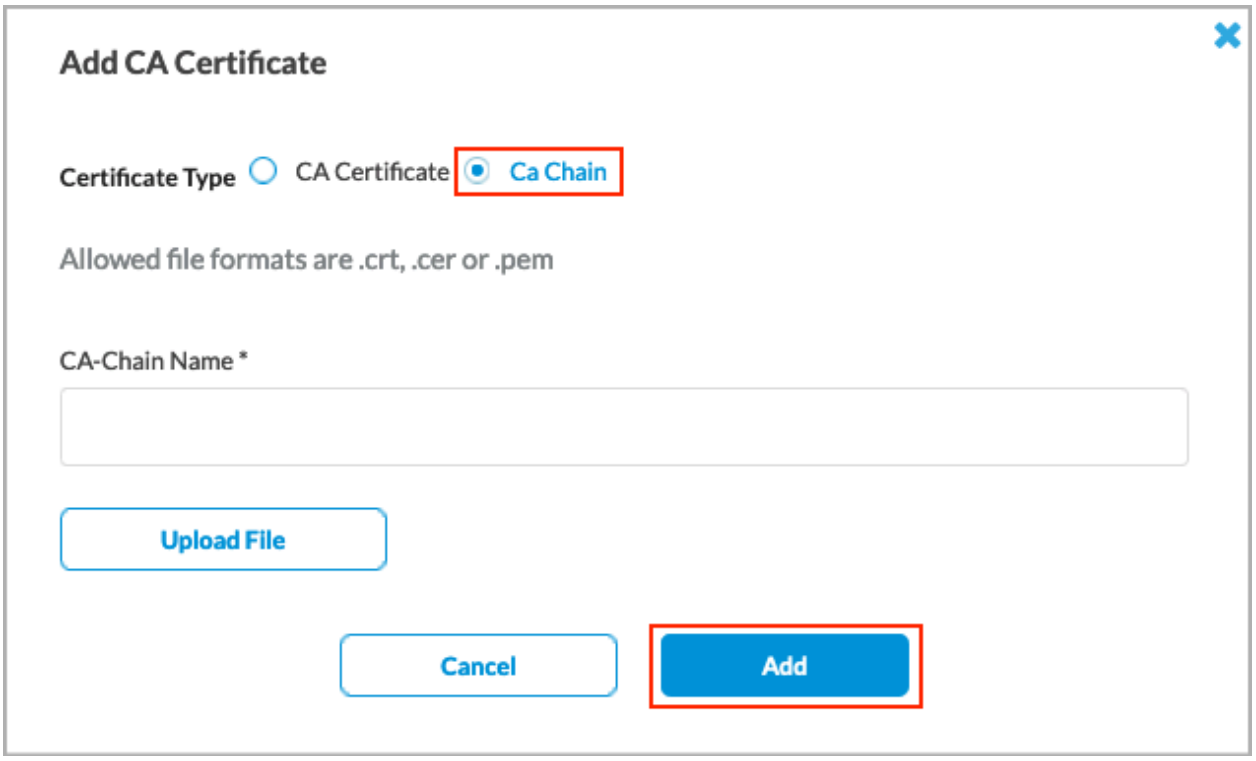
2. Click + Add to add certificates. The Add CA Certificate popup window displays.



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

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

Supported Software Information

Releases 11.1.1 and later support all content described in this article.

Additional Information

Configure SASE Secure Client Access Rules
Configure SASE Site-to-Site Tunnels
Configure Users and Device Authentication