Configure Certificates for IPsec

For supported software information, click here.

Certificates are used to set up a secure communication channel between a branch and a Controller node. When a branch or Controller node needs to communicate with each other, it sends a request for a certificate to the certificate authority. The certificate authority issues certificates.

A branch requires two types of certificates:

- Staging
- Post-staging

Configure Staging Certificates

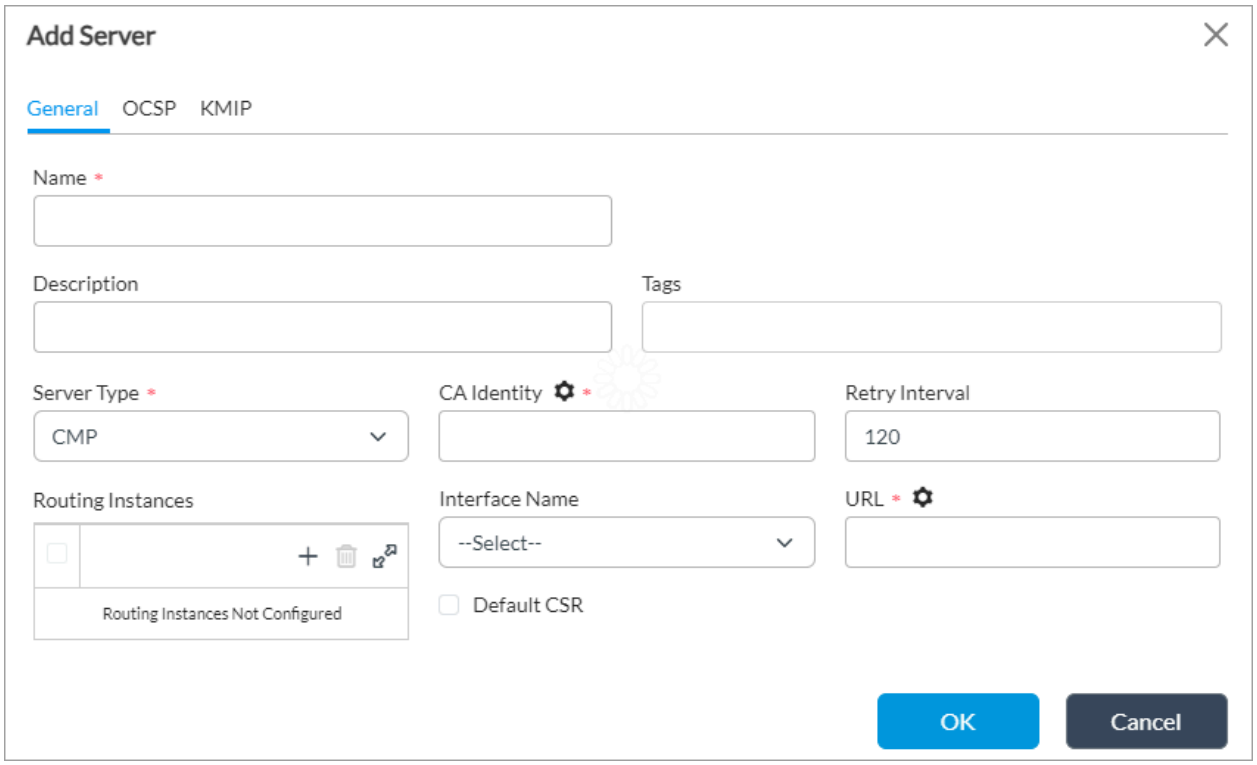
Certificates are issued by a certificate authority (CA). To configure a certificate, you need to configure the server that hosts the certificate. The branch or controller that requires a certificate sends a certificate request to the server.

To configure a staging certificate, you do the following:

- Configure a certificate server.
- Configure a certificate request.

Configure a Certificate Server

1. In the 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 staging template on the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Connectors > Certificate Manager in the left menu bar.
4. Select the Servers tab, and then click the + Add icon. In the Add Server popup window, select the General tab, and then enter information for the following fields. In Releases 21.2.3 and earlier, the General, Certificate Attributes, Authorization Information fields are displayed in a single window.



Updated: Wed, 23 Oct 2024 08:11:29 GMT

Field	Description
Name (Required)	Enter a name for the server.
Description	Enter a text description for the server.
Tags	Enter a keyword or phrase that allows you to filter the server names. A tag is an alphanumeric text descriptor with no white spaces or special characters that you can use to names. You can specify multiple tags.
Server Type (Required)	Select CMP.
CA Identity	Enter the name of the certificate authority.
Retry Interval	Enter the interval at which a branch or Controller node can try again to retrieve the certificate, in seconds.
Routing Instance	Select the routing instance that the branch or controller node uses to communicate with the server.
Interface Name	Select the interface to use for communication with the server.
URL	Enter the URL of the server hosting the certificate authority.
Default CSR	(For Releases 22.1.3 and later.) Click to have the server generate a certificate signing request (CSR) that contains the device ID as the common name. If you select this option, you do not need to configure additional certificate-signing request options.

5. For information about configuring other parameters and tabs, see Configure Certificate Servers.
6. Click OK.

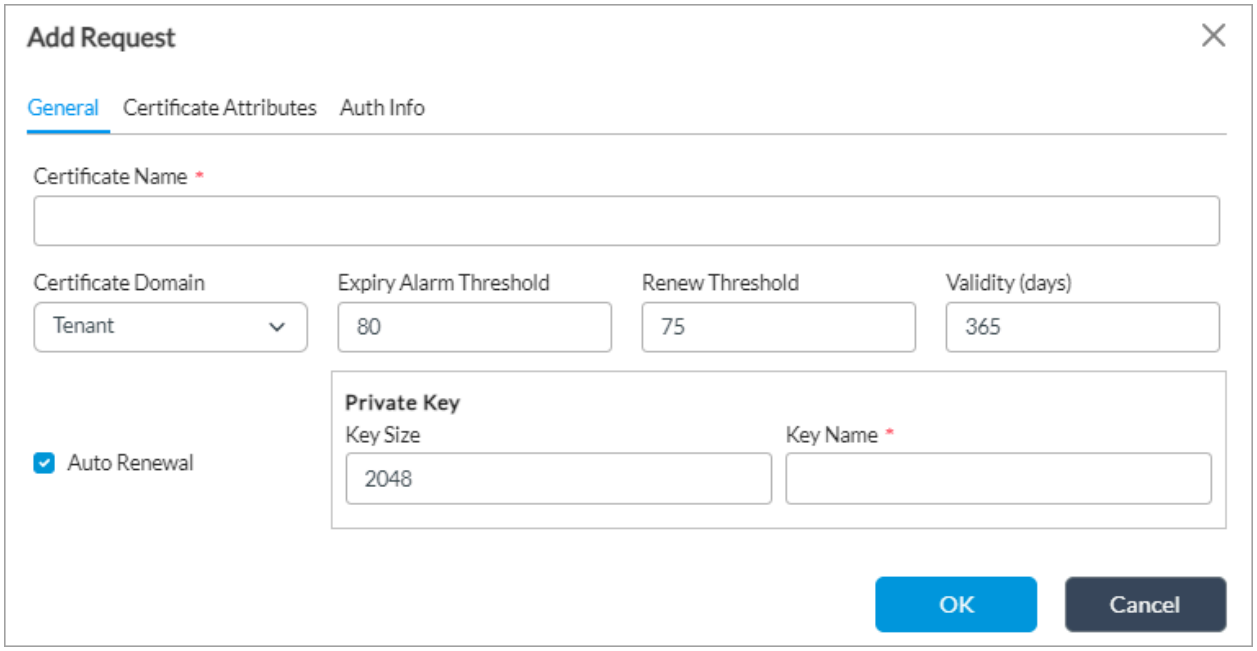
To delete an existing server, select the checkbox next to the server and click in the top right corner.

To filter the configuration screen table information, click the Filter Records icon.

Configure a Certificate Request

1. In the 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 staging template on the main pane. The view changes to Appliance view.

2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors > Connectors > Certificate Manager in the left menu bar.
4. Select the Requests tab, and then click the + Add icon. In the Add Request popup window, select the General tab, and then enter information for the following fields. In Releases 21.2.3 and earlier, the General, Certificate Attributes, Authorization Information fields are displayed in a single window.



Field	Description
Certificate Name (Required)	Enter a name for the branch certificate.
Certificate Domain	Select the domain to which the certificate applies.
Expiry Alarm Threshold	(For Releases 22.1.3 and later.) Enter the certificate expiration alarm threshold value, which is a percentage of the certificate validity time. *Range:* 50 through 99 percent *Default:* 80 percent
Renew Threshold	(For Releases 22.1.3 and later.) Enter the certificate renewal threshold value, which is a percentage of the certificate validity time. *Range:* 50 through 99 percent *Default:* 75 percent
Validity	Enter the number of days for which the certificate is valid. *Default*: 365 days
Autorenewal	Click to renew the request automatically.
Private Key (Group of Fields)	
◦ Key Size	Enter the size of the key to generate. The standard size is 1024 MB. *Default*: 2048 bytes
◦ Key Name (Required)	Enter the name of the key to generate.

5. For information about configuring other parameters and tabs, see Configure Certificate Servers.
6. Click OK.

Configure Post-Staging Certificates

You can use the same certificate configured for a staging template of a branch for the post-staging phase. You repeat the steps listed in the previous section, selecting the post-staging template instead of the staging template for the branch.

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

Configure Certificate Servers