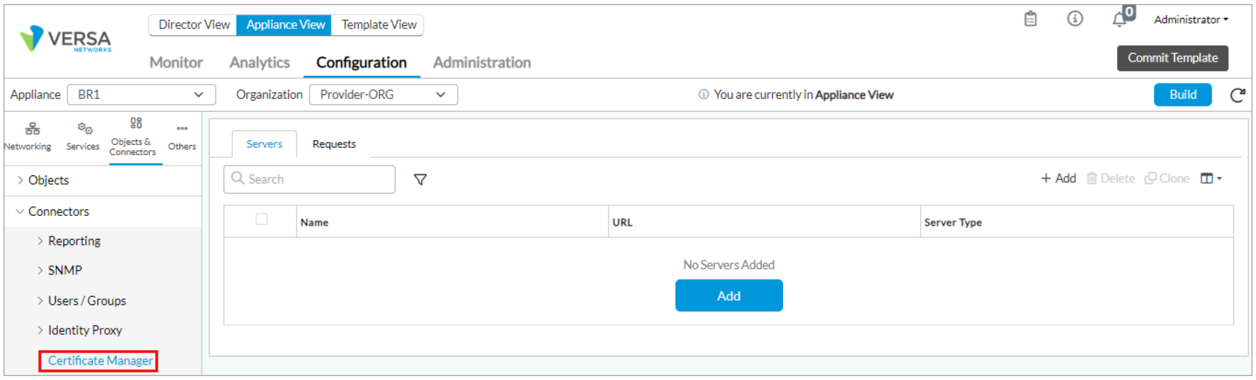
Configure Certificate Servers

For supported software information, click here.

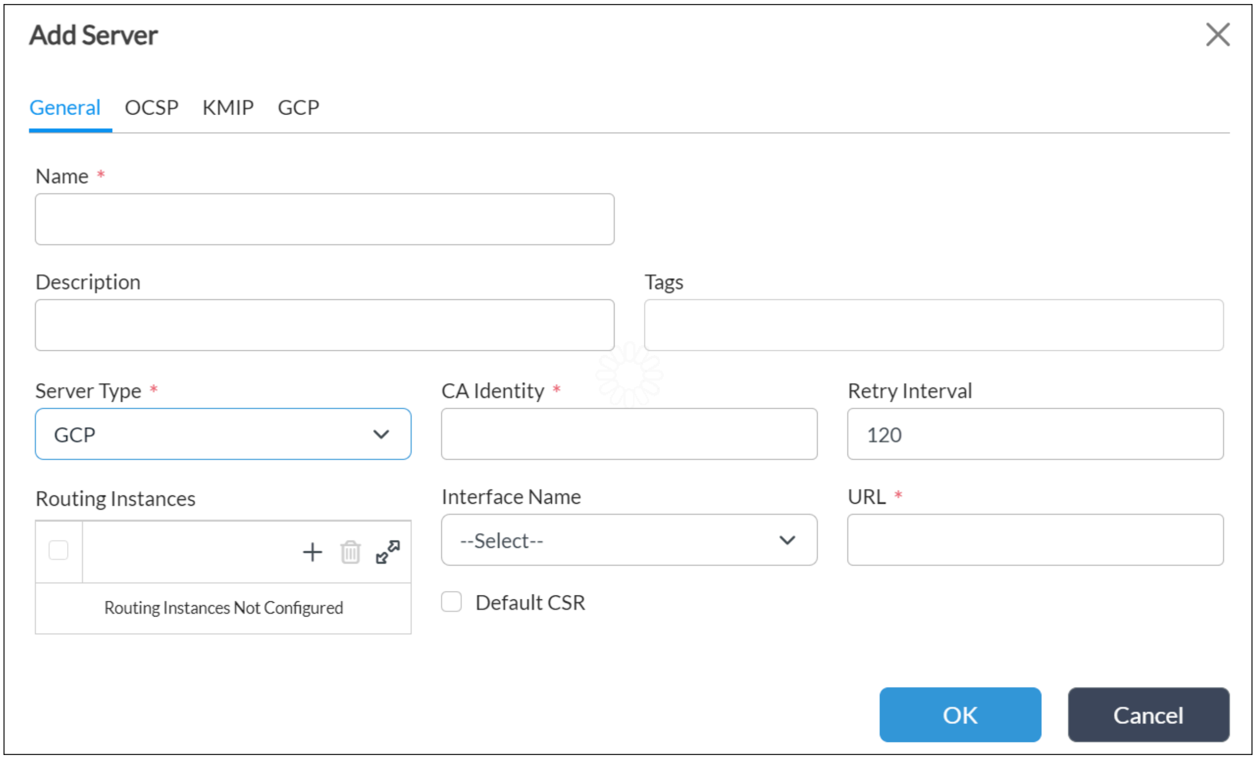
To configure a Versa Operating System^{TM} (VOS^{TM}) device to use certificates, you configure a server that hosts the certificates. When the branch or Controller device requires a certificate, it sends a certificate request to the server.

To configure a certificate server:

1. In 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 device in 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.



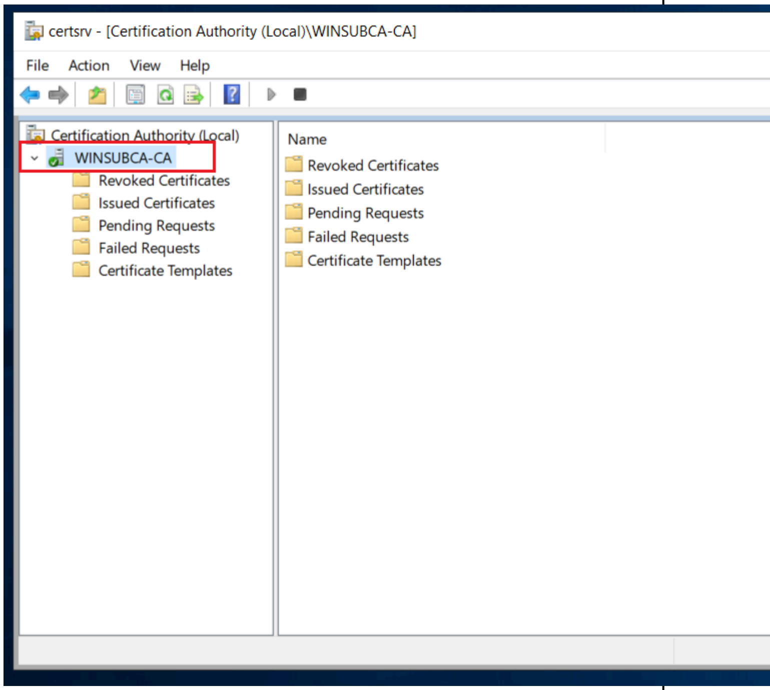
4. Select the Servers tab in the horizontal menu bar, and then click + Add. In the Add Server popup window, select the General tab, and then enter information for the following fields. For Releases 21.2.3 and earlier, the General and OCSP fields are displayed on a single window.

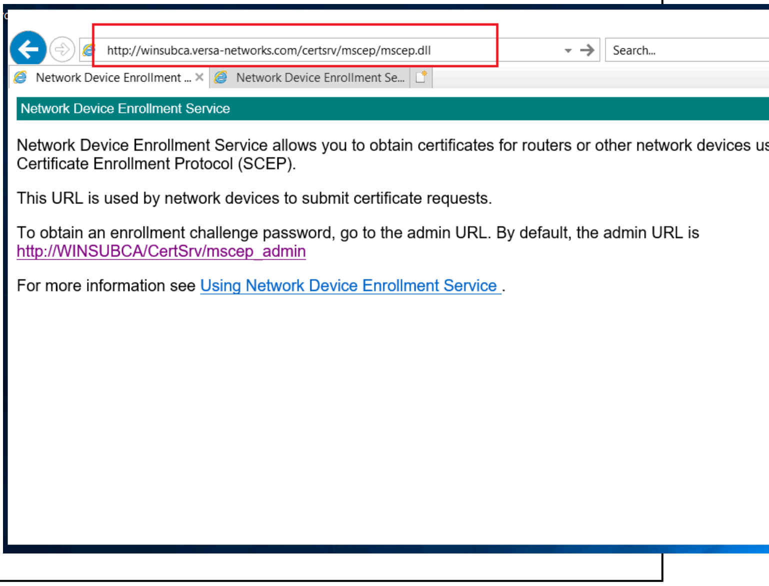


Server Type * GCP

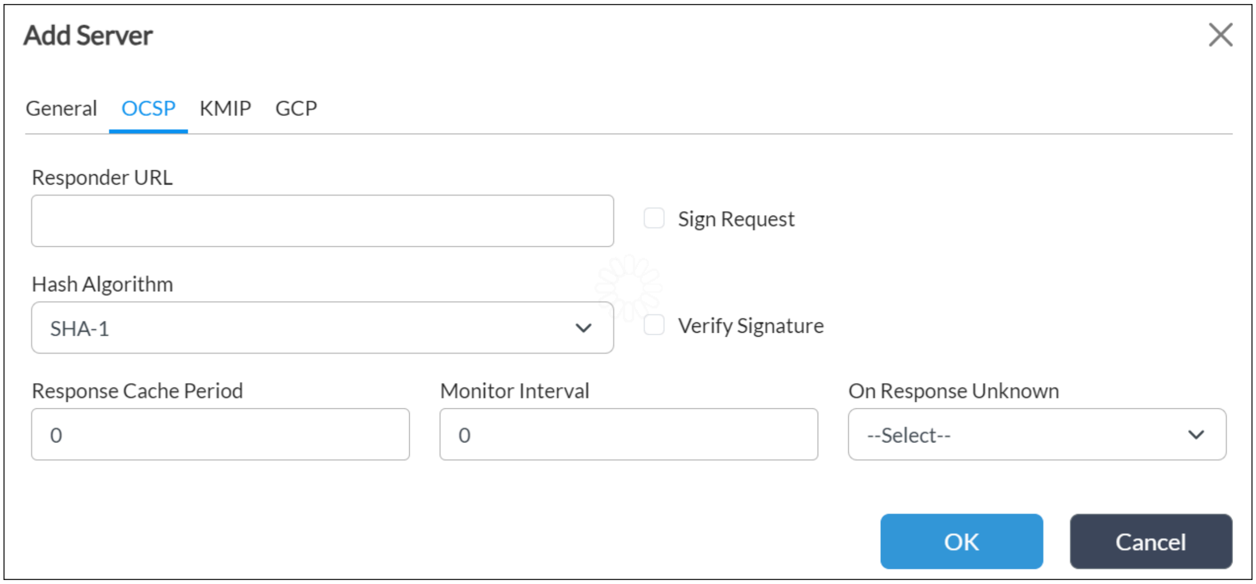
Retry Interval 120

Field	Description
Name (Required)	Enter a name for the certificate server.
Description	Enter a text description for the certificate server.
Tags	Enter tags to identify the certificate server. A tag is an alphanumeric text descriptor with no spaces or special characters that you use to search for multiple certificate servers.
Server Type (Required)	Select the type of certificate authority (CA) server: ◦ ACME—(For Releases 22.1.3 and later.) Automatic Certificate Management Environment ◦ CMP—Select if the CA server is using the Certificate Management Protocol for enrollment. ◦ GCP—(For Releases 22.1.3 and later.) Select if the CA server uses Google Cloud Platform for enrollment. ◦ SCEP—Select if the CA server is using the Simple Certificate Enrollment Protocol.

Field	Description
CA Identity (Required)	Enter the name of the CA server: ◦ For the server type CMP, enter CN=*CA-name* ◦ (For Releases 22.1.3 and later.) For the server type GCP, enter GCP-CA ◦ For the server type SCEP, enter *CA-name*. The following screenshot shows an example entry for a Microsoft CA server in which the CA identity is WINSUBCA-CA.  certsrv - [Certification Authority (Local)\WINSUBCA-CA] File Action View Help Certification Authority (Local) WINSUBCA-CA Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates Name Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates
Retry Interval	Enter the interval, in seconds, at which a branch or a Controller device retries to retrieve the certificate.
Routing Instance	Select the routing instance to use to reach the certificate server. If you select the eth0 (management) interface, you do not need to select a routing instance.
Interface Name	Select the interface to use to communicate with the certificate server.
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

Field	Description
	additional certificate-signing request options.
URL (Required)	Enter the URL of the CA server enrollment service. This is the URL to which CA certificate and enrollment requests are sent. The following figure shows the URL for an SCEP server type with the Microsoft Network Device Enrollment Service (NDES; SCEP and NDES are available for Releases 20.2.1 and later).  Search... Network Device Enrollment ... Network Device Enrollment Se... http://winsubca.versa-networks.com/certsrv/mscep/mscep.dll Network Device Enrollment Service Network Device Enrollment Service allows you to obtain certificates for routers or other network devices us Certificate Enrollment Protocol (SCEP). This URL is used by network devices to submit certificate requests. To obtain an enrollment challenge password, go to the admin URL. By default, the admin URL is http://WINSUBCA/CertSrv/mscep_admin For more information see Using Network Device Enrollment Service .

5. Select the OCSP tab, and then enter information for the following fields.



Add Server

Responder URL

□ Sign Request

Hash Algorithm: SHA-1

□ Verify Signature

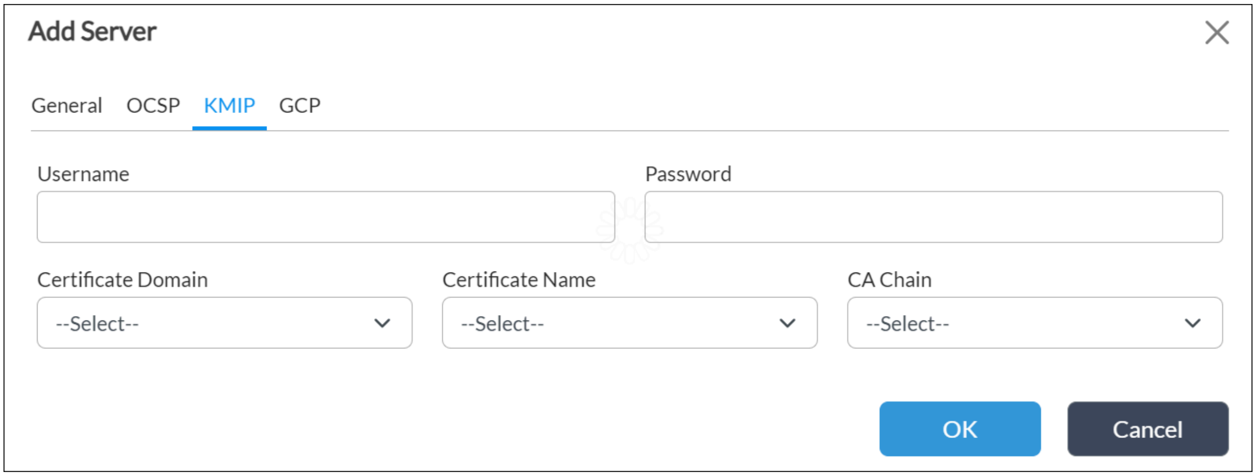
Response Cache Period: 0

Monitor Interval: 0

On Response Unknown: --Select--

Field	Description
Responder URL	Enter the URL of the OCSP responder. The OCSP responder reports the status of a certificate.
Sign Request	Click to have the OCSP responder verify the signature before responding to certificate requests.
Hash Algorithm	Select the hash algorithm to use when preparing the OCSP request.
Verify Signature	Click to have the VOS device verify the signature of OCSP responder.
Response Cache Period	Enter how long, in hours, to cache OCSP responses. *Range*: 0 through 168 hours *Default*: 0 (no cache is created)
Monitor Interval	Enter the time interval at which to verify the validity of the certificate status. *Range*: 0 through 1440 minutes *Default*: 0 (monitoring is disabled)
On Response Unknown	(For Releases 22.1.3 and later.) Select the action to take on the IPsec tunnel when an unknown response is received from the OCSP responder: ◦ Tunnel Down—Bring the IPsec tunnel down. ◦ Tunnel Up—Bring the IPsec tunnel up.

6. (For Releases 22.1.1 and later.) Select the KMIP tab, and then enter information for the following fields. You configure Key Management Interoperability Protocol (KMIP) information for the certificate server to use to interface with a key management server (KMS) using KMIP to perform key management and cryptographic operations such as generation of a symmetric key and an asymmetric key-pair. For more information, see Configure a KMIP Client.



Add Server

General OCSP KMIP GCP

Username

Password

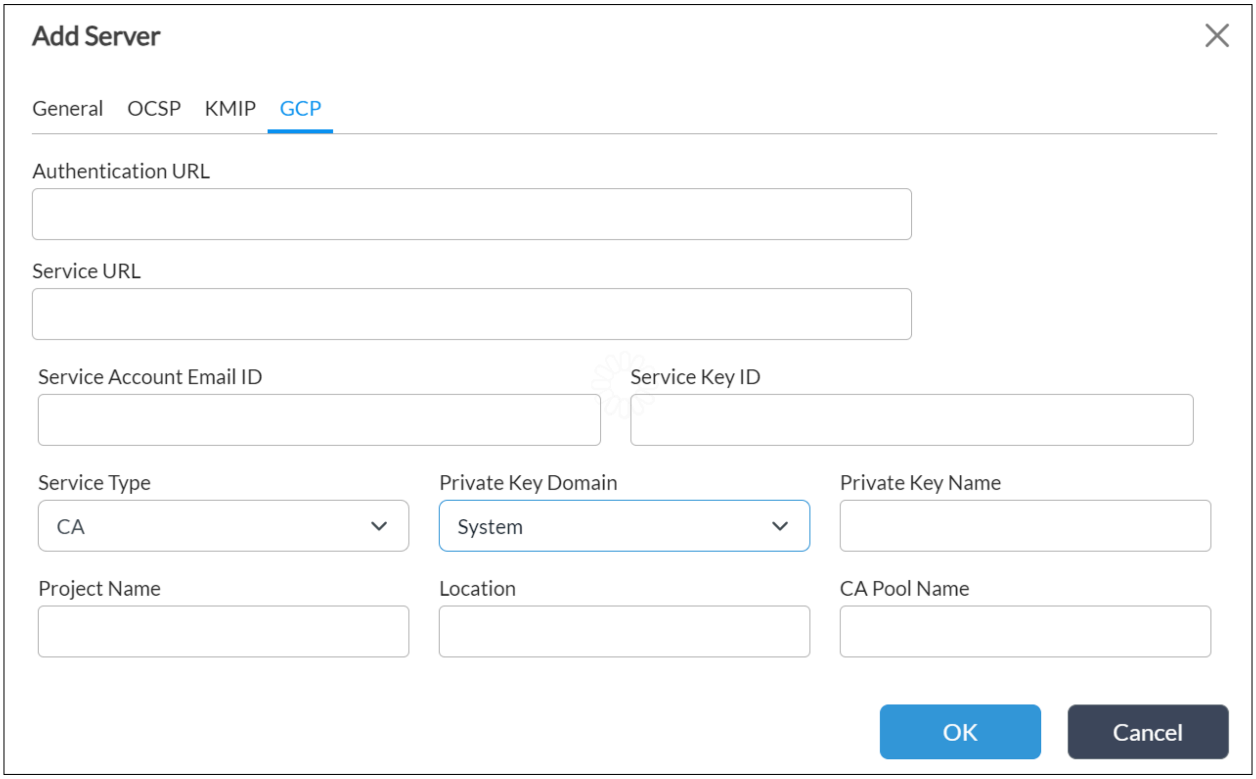
Certificate Domain: --Select--

Certificate Name: --Select--

CA Chain: --Select--

Field	**Description**
Username	Enter the username of the KMS administrator to use to authenticate KMIP requests from the VOS KMIP client.
Password	Enter the KMS administrator password to useto authenticate KMIP request from the VOS KMIP client.
Certificate Domain	Select the KMS client certificate location: ◦ System ◦ Tenant
Certificate Name	Select the certificate to use to establish HTTPS or TLS connection from the VOS KMIP client to the KMS.
CA Chain	Select the CA chain name to use to establish HTTPS or TLS connection from the VOS KMIP client to the KMS.

7. (For Releases 22.1.3 and later.) Select the GCP tab, and then enter information for the following fields.



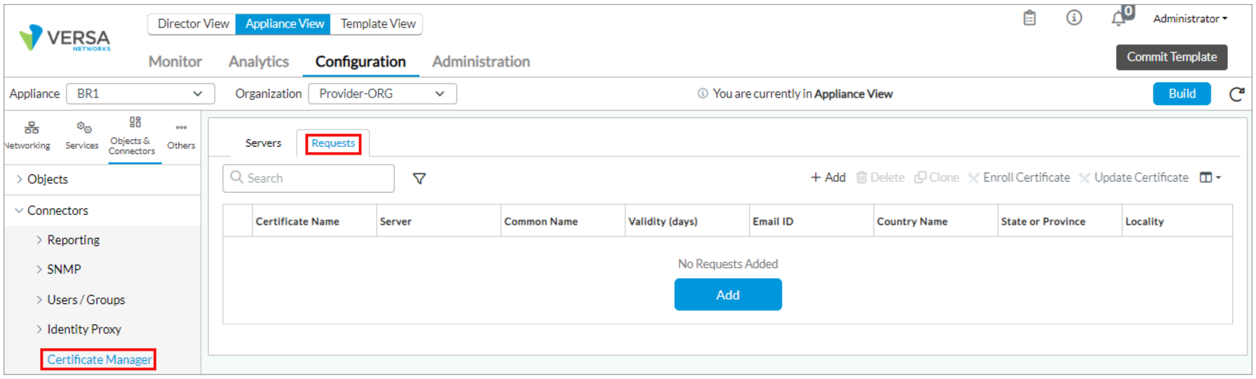
Service Type: CA

Private Key Domain: System

Field	Description
Authentication URL	Enter the URL for the GCP Open Authorization (OAuth) 2.0 server's web serv before enrolling. Use the token_uri value from the JSON file downloaded durin
Service URL	Enter the URL https://privateca.googleapis.com/v1.
Service Account Email ID	Enter the client email ID that is associated with the service account.
Service Key ID	Enter the private key ID that is associated with the service account.
Service Type	Select CA.
Private Key Domain	Select Tenant.
Private Key Name	Enter the name of the GCP service account private key filename.
Project Name	Enter the project_id value that is associated with the service account.
Location	Enter the location of the CA pool.
CA Pool Name	Enter the name of the CA pool.

8. Click OK.

9. Select the Requests tab in the horizontal menu bar.



Appliance: BR1

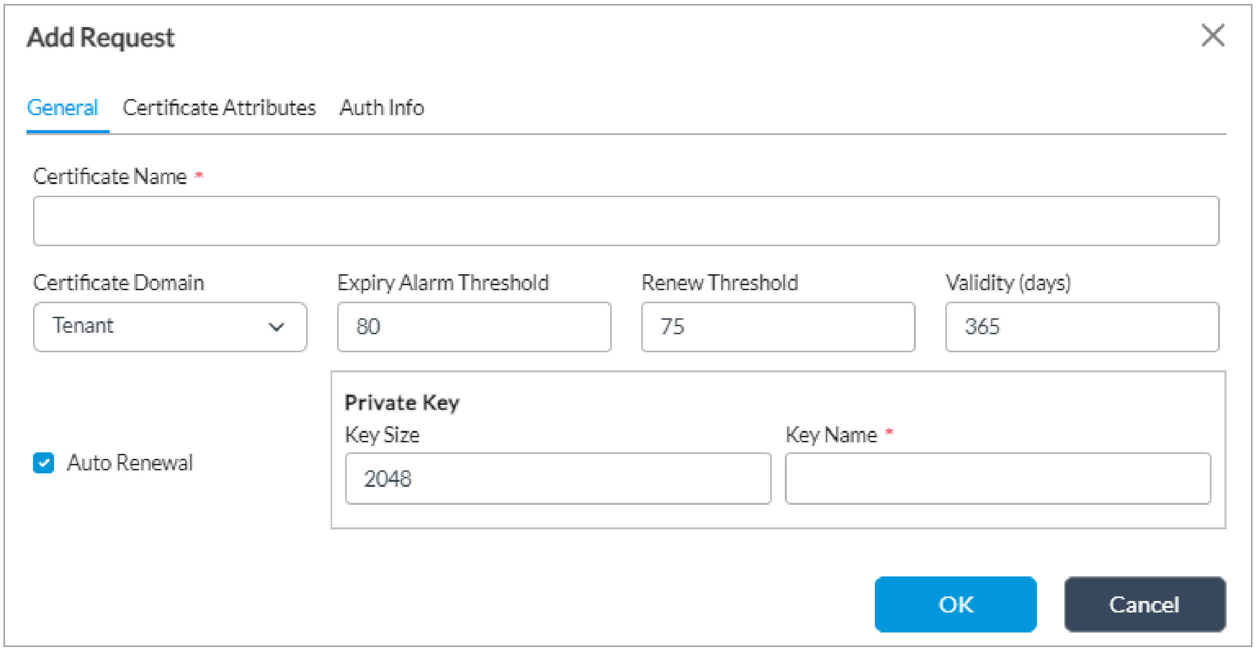
Organization: Provider-ORG

You are currently in Appliance View

Certificate Name	Server	Common Name	Validity (days)	Email ID	Country Name	State or Province	Locality

No Requests Added

10. Click + Add to add a request. 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.



Certificate Name *

Certificate Domain: Tenant

Expiry Alarm Threshold: 80

Renew Threshold: 75

Validity (days): 365

☑ Auto Renewal

Private Key

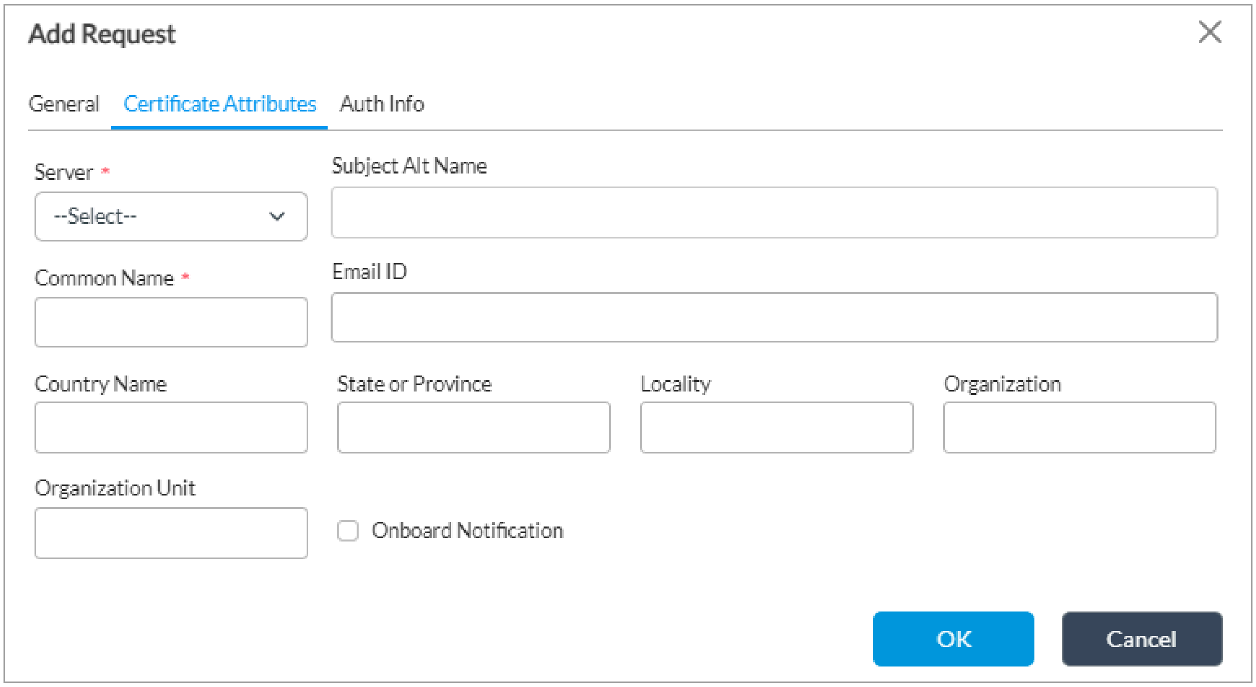
Key Size: 2048

Key Name *

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.

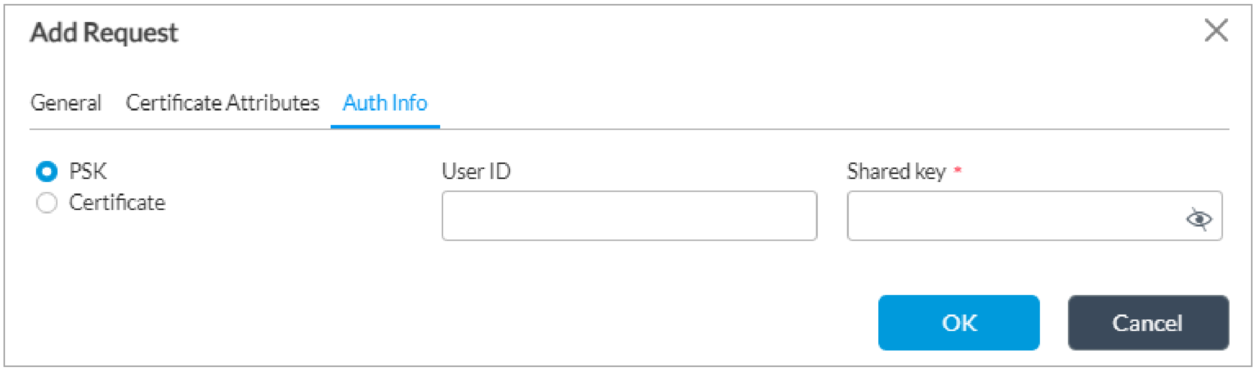
Field	Description
	Range: 50 through 99 percent *Default:* 80 percent
Renew Threshold	(For Releases 22.1.3 and later.) Enter the certificate renewal threshold value, which is a percentage of the certificate validity time. *Range:* 50 through 99 percent *Default:* 75 percent
Validity	Enter the number 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.

11. Select the Certificate Attributes tab, and then enter information for the following fields.

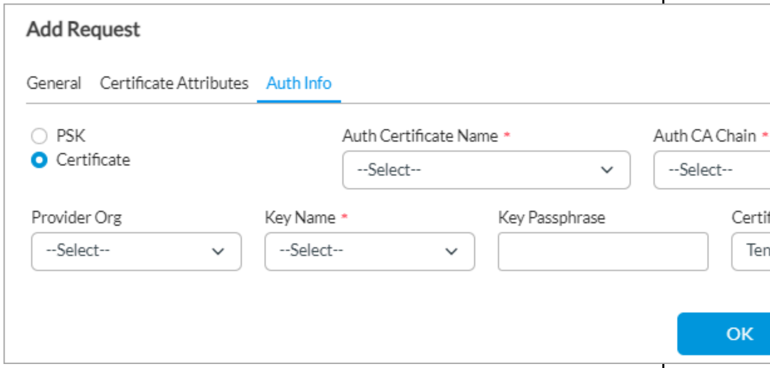

Add Request
General
Certificate Attributes
Auth Info
Server *
--Select--
Subject Alt Name
Common Name *
Email ID
Country Name
State or Province
Locality
Organization
Organization Unit
□ Onboard Notification
OK
Cancel

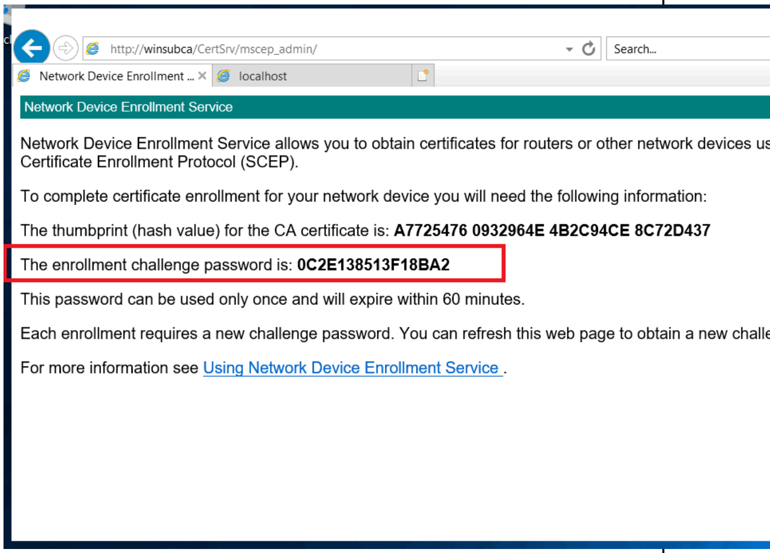
Field	Description
Server (Required)	Select the name of the certificate server.
Subject Alternate Name	(For Releases 22.1.3 and later.) Enter the DNS hostname. You can specify it as a domain name, a wildcard, or an IP address.
Common Name (Required)	Enter the name of the certificate server. This name is also an identity, which you must also configure in the CA server. Both the names should match. Only then does the CA server issue the certificate.
Email ID	Enter the email address of the user who downloads the certificate. This email address must be registered in the CA server.
Country Name	Enter the country in which the VOS device is deployed.
State or Province	Enter the state or province in which the VOS device is deployed.
Locality	Enter the location where the VOS device is deployed.
Organization	Enter the name of the organization associated with the certificate.
Organizational Unit	Enter the name of the organizational unit associated with the certificate.
Onboard Notification	(For Releases 22.1.3 and later.) Click to send a notification when the certificate is issued and loaded onto the VOS device.

12. Select the Authentication Information tab, and then enter information for the following fields.



Add Request

Field	Description
Mode	Select the type of authentication to use
◦ PSK	Click to use a preshared key.
◦ Certificate	Click to use a certificate. The following fields then display:  Add Request General Certificate Attributes Auth Info ○ PSK ● Certificate Auth Certificate Name * --Select-- Auth CA Chain * --Select-- Provider Org --Select-- Key Name * --Select-- Key Passphrase Certi Ten OK
User ID	If you select PSK authentication, enter the user identifier.
Shared Key	If you select PSK authentication, enter the password that to use in enrollment requests. The CA server's enrollment service uses this password to authenticate client enrollment requests. For example, if you use Microsoft NDES (available for Releases 20.2.1 and later), the password can be retrieved as shown in the following sample screenshot:

	 http://winsubca/CertSrv/mscep_admin/ Search... Network Device Enrollment ... localhost Network Device Enrollment Service Network Device Enrollment Service allows you to obtain certificates for routers or other network devices us Certificate Enrollment Protocol (SCEP). To complete certificate enrollment for your network device you will need the following information: The thumbprint (hash value) for the CA certificate is: **A7725476 0932964E 4B2C94CE 8C72D437** The enrollment challenge password is: **0C2E138513F18BA2** This password can be used only once and will expire within 60 minutes. Each enrollment requires a new challenge password. You can refresh this web page to obtain a new challe For more information see Using Network Device Enrollment Service .
Authentication Certificate Name	If you select certification authentication, select the certificate.
Authentication CA Chain	If you select certification authentication, select the CA chain.
Provider Organization	If you select certification authentication, select the provider organization to which the certificate applies.
Key Name	If you select certification authentication, select the name of the key.
Key Passphrase	If you select certification authentication and a key name, enter the password to use with the key.
Certificate Domain	If you select certification authentication, select the domain to which the certificate applies.

13. Click OK. The main pane displays the certificate request.

Supported Software Information

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

- Release 20.2.1 adds support for Microsoft NDES and SCEP network access control.
- Release 22.1.1 adds support for KMIP.
- Release 22.1.3 adds support for Google Cloud Platform; adds support for the Default CSR, On Response Unknown and ACME in Server Type field in the Add Server popup window and the Expiry Alarm Threshold, Renew

Threshold, Subject Alternate Name, and Onboard Notification fields in the Add Request popup window.

Additional Information

Configure a Branch SD-WAN Profile
Configure CA Certificates and CA Chains