

Configure a Common Certificate Authority

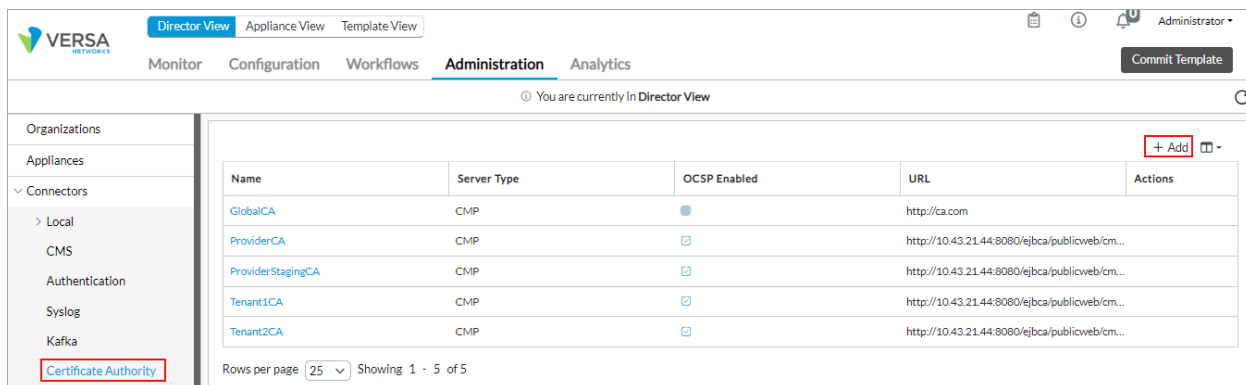
 For supported software information, click [here](#).

On Versa Operating System™ (VOS™) devices, you can create a global certificate authority (CA) that is common and not associated with any organization. You can use this CA when you create provider or customer organizations and Controller nodes that use cryptographic public key infrastructure (PKI) for CPE authentication. After you configure a common CA, you can configure the WAN and LAN interfaces to connect to the CA server in template workflows.

When you deploy a Controller node in a Controller workflow, the CA that you specify in the provider organization, and for any of its subordinate organizations, is pushed to the Controller node. For organizations and subordinate organizations in a Controller workflow, you must also specify a CSR, which is also pushed to the Controller node.

To configure a common CA:

1. Select the Administration tab in the top menu bar.
2. Select Connectors > Certificate Authority in the left menu bar.



Name	Server Type	OCSP Enabled	URL	Actions
GlobalCA	CMP	<input type="checkbox"/>	http://ca.com	
ProviderCA	CMP	<input checked="" type="checkbox"/>	http://10.43.21.44:8080/ejbca/publicweb/cm...	
ProviderStagingCA	CMP	<input checked="" type="checkbox"/>	http://10.43.21.44:8080/ejbca/publicweb/cm...	
Tenant1CA	CMP	<input checked="" type="checkbox"/>	http://10.43.21.44:8080/ejbca/publicweb/cm...	
Tenant2CA	CMP	<input checked="" type="checkbox"/>	http://10.43.21.44:8080/ejbca/publicweb/cm...	

Rows per page: 25 Showing 1 - 5 of 5

3. Click the + Add icon. The Certificate Authority popup window displays.

Certificate Authority

General

OCSP

Name *

URL *

CA Identity *

Retry Interval(seconds)

Server Type *

---Please Select---

OK

Cancel

4. Select the General tab, and enter information for the following fields.

Field	Description
Name (Required)	Enter a name for the certificate server.
URL (Required)	Enter the URL of the CA server enrollment service. This is the URL to which CA certificate and enrollment requests are sent.
Retry Interval	Enter the interval, in seconds, at which an organization or a Controller node retries to retrieve the certificate.
Server Type	<p>Select the type of certificate authority (CA) server:</p> <ul style="list-style-type: none"> ◦ ACME—Automatic Certificate Management Environment ◦ CMP—Select if the CA server is using the Certificate Management Protocol for enrollment. ◦ SCEP—Select if the CA server is using the Simple Certificate Enrollment Protocol.

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

Certificate Authority

General

OCSP

☒ OCSP Enabled

Responder URL *

Hash Algorithm

Response Cache Period(hours)

Monitor Interval (mins)

☐ Sign Request

☐ Verify Signature

Action on Response Unknown

Please Select---

OK

Cancel

Field	Description
OCSP Enabled	Click to enable Online Certificate Status Protocol (OCSP) usage.
Responder URL	Enter the URL of the OCSP responder. The OCSP responder reports the status of a certificate.
Hash Algorithm	Select the hash algorithm to use when preparing the OCSP request.
Response Cache Period	Enter how long, in hours, to cache OCSP responses. <i>Range:</i> 0 through 168 hours <i>Default:</i> 0 (no cache is created)
Monitor Interval	Enter the time interval at which to verify the validity of the certificate status. <i>Range:</i> 0 through 1440 minutes <i>Default:</i> 0 (monitoring is disabled)
Sign Request	Click to have the OCSP responder verify the signature before responding to certificate requests.
Verify Signature	Click to have the VOS device verify the signature of OCSP responder.
Action on Response Unknown	Select the action to take on the IPsec tunnel when an unknown response is received from the OCSP responder: <ul style="list-style-type: none"> ◦ Tunnel Down—Bring the IPsec tunnel down. ◦ Tunnel Up—Bring the IPsec tunnel up.

6. Click OK.

Supported Software Information

Releases 22.1 and later support all content described in this article.

Additional Information

[Configure Basic Features](#)

[Configure Certificate Servers](#)

[Create and Manage Certificates](#)