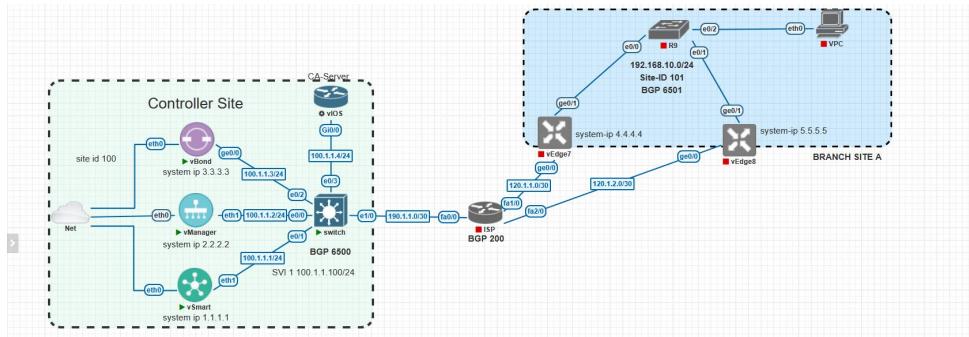


Step by step process to onboard Sdwan Devices (Controllers and Site Routers)

Step1

Onboard the controllers first (vbond, vmanage, vsmartrt)



Step 2

Get the system configuration done, stating the **Organizational name, site id , system-ip, clock time zone, vbond ip**.

Vsmartrt System Configuration

```
vsmartrt# conf t  
Entering configuration mode terminal  
vsmartrt(config)# system  
vsmartrt(config-system)# system-ip 1.1.1.1  
vsmartrt(config-system)# organization-name cisco  
vsmartrt(config-system)# vbond 100.1.1.3 BGP 6800  
vsmartrt(config-system)# site-id 100  
vsmartrt(config-system)# clock timezone Africa/Accra  
vsmartrt(config-system)# commit  
Commit complete.  
vsmartrt(config-system)#[
```

Vmanage System Configuration

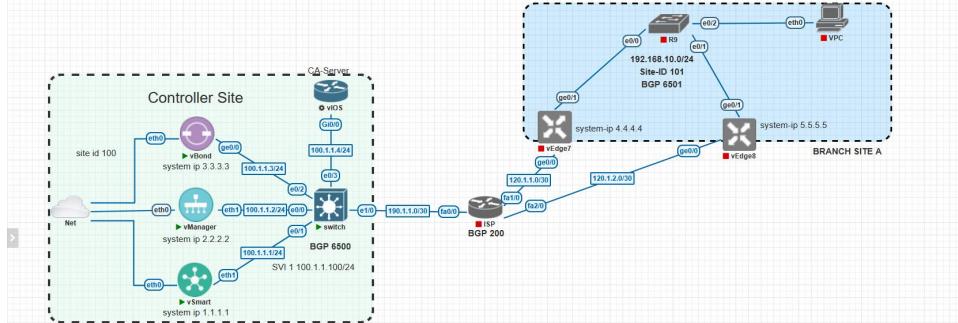
```
vmanage(config)# system  
vmanage(config-system)# system-ip 2.2.2.2  
vmanage(config-system)# organization-name cisco  
vmanage(config-system)# vbond local 100.1.1.3  
vmanage(config-system)# site-id 100  
vmanage(config-system)# clock timezone Africa/Accra  
vmanage(config-system)# commit  
Commit complete.  
vmanage(config-system)#[
```

Vbond System Configuration

```
vedge# conf t  
Entering configuration mode terminal  
vedge(config)# system  
vedge(config-system)# system-ip 3.3.3.3  
vedge(config-system)# organization-name cisco  
vedge(config-system)# vbond local 100.1.1.3  
vedge(config-system)# clock timezone Africa/Accra  
vedge(config-system)# host-name vbond  
vedge(config-system)# commit  
Commit complete.  
vbond(config-system)#[
```

Step 3

Configure the **transport side** for the controllers by enabling **VPN 0**. The transport side of this SDWAN topology are the physical interfaces connecting from the controllers to the ISP.



In order to get this done, ***we will first create a default static route to the ISP*** and then explicitly specify which physical interfaces we will need to be a part of the **transport vpn , VPN 0**.

VPN 0 cannot be deleted from any of the controllers, it is there by default. Enable services on each physical interfaces, by creating a tunnel that will allow services suchas **NetConf , sshd, and all others services**

Transport side configuration (VPN 0) will be done for all controllers in this topology.

Vsmart VPN 0 Configuration

```
vsmart(config)# vpn 0
vsmart(config-vpn-0)# ip route 0.0.0.0/0 100.1.1.100
vsmart(config-vpn-0)# int eth1
vsmart(config-interface-eth1)# ip add 100.1.1.2/24
vsmart(config-interface-eth1)# no shutdown
vsmart(config-interface-eth1)# tunnel-interface
vsmart(config-tunnel-interface)# allow-service all
vsmart(config-tunnel-interface)# allow-service sshd
vsmart(config-tunnel-interface)# allow-service netconf
vsmart(config-tunnel-interface)# commit
Commit complete.
vsmart(config-tunnel-interface)#

```

Vmanage VPN 0 Configuration

```
vmanage(config)# vpn 0
vmanage(config-vpn-0)# ip route 0.0.0.0/0 100.1.1.100
vmanage(config-vpn-0)# int eth1
vmanage(config-interface-eth1)# ip add 100.1.1.2/24
vmanage(config-interface-eth1)# no shutdown
vmanage(config-interface-eth1)# tunnel-interface
vmanage(config-tunnel-interface)# allow-service all
vmanage(config-tunnel-interface)# allow-service sshd
vmanage(config-tunnel-interface)# allow-service netconf
vmanage(config-tunnel-interface)# commit
Commit complete.
vmanage(config-tunnel-interface)#

```

VBond VPN 0 Configuration

```
vbond(config)# vpn 0
vbond(config-vpn-0)# ip route 0.0.0.0/0 100.1.1.100
vbond(config-vpn-0)# int ge0/0
vbond(config-interface-ge0/0)# ip add 100.1.1.3/24
vbond(config-interface-ge0/0)# no shutdown
vbond(config-interface-ge0/0)# tunnel-interface
vbond(config-tunnel-interface)# allow-service sshd
vbond(config-tunnel-interface)# allow-service netconf
vbond(config-tunnel-interface)# allow-service all
vbond(config-tunnel-interface)# commit

```

Step 4

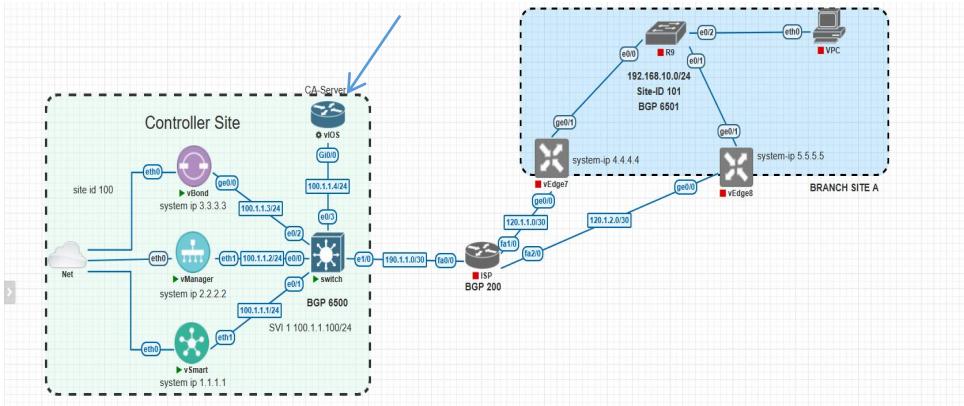
Configure the management vpn on the VManage. The management vpn by default is **VPN 512**. This vpn cannot be deleted.

Vmanage VPN 512 Configuration

```
vmanage(config)# vpn 512
vmanage(config-vpn-512)# int eth0
vmanage(config-interface-eth0)# ip dhcp-client
vmanage(config-interface-eth0)# no shutdown
vmanage(config-interface-eth0)# commit
```

Step 5

Create a **ROOT Certificate Authorization Server** on the VIOs Router



Enable **SSH** and **HTTP** services on the router we want to use as the **ROOT-CA**

SSH Configuration

```
ROOT_CA(config)#crypto key generate rsa label ROOT modulus 2048
% You already have RSA keys defined named ROOT.
% They will be replaced.
%
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
% Jun 12 13:55:18.921: %SSH-5-DISABLED: SSH 2.0 has been disabled
[OK] (elapsed time was 3 seconds)
ROOT_CA(config)#
%Jun 12 13:55:21.258: %SSH-5-ENABLED: SSH 2.0 has been enabled
ROOT_CA(config)#ip ssh version 2
ROOT_CA(config)#

```

HTTP Services Configuration

```
ROOT_CA(config)#
ROOT_CA(config)#
ROOT_CA(config)#
ROOT_CA(config)#
ROOT_CA(config)#
ROOT_CA(config)# ip http authentication local
ROOT_CA(config)# ip http server
ROOT_CA(config)# ip http path flash:
ROOT_CA(config)# username admin privilege 15 password cisco
ROOT_CA(config)#

```

Meaning of Each Command

#**ROOT_CA(config)# ip http authentication local**

Meaning:

This command tells the router to use the **local user database** for authenticating users who access the HTTP server (like when accessing the SCEP enrollment URL).

↙ Why it's needed:

When SCEP clients (like other routers) enroll via HTTP, they may need to provide a username and password. This ensures the credentials are checked against local usernames/passwords on the router.

```
#ROOT_CA(config)# ip http server
```

Meaning:

This **enables the HTTP server** on the router.

❖ **Why it's needed:**

This is required for the router to serve certificate enrollment pages or files (e.g., the ROOT_CA certificate or the SCEP service itself).

```
#ROOT_CA(config)# ip http path flash:
```

Meaning:

This sets the base directory (or path) for the HTTP server to serve files from the router's **Flash memory**.

❖ **Why it's needed:**

When a client requests a file like `http://<router-ip>/ROOT.ca`, the router looks in `flash:` to find and serve it.

```
#ROOT_CA(config)# username admin privilege 15 password cisco
```

Meaning:

This creates a **local user** named **admin** with:

Privilege level 15 (full admin access)

Password: `cisco`

❖ **Why it's needed:**

This is used for HTTP authentication (`ip http authentication local`), allowing the router to verify the client's username/password when accessing PKI enrollment or certificate files.

ROOT CA Configuration

```
ROOT_CA(config)#do sh run | sec crypto
crypto pki server ROOT
    database level complete
    database archive pkcs12 password 7 14141B180F0B7B7977
    issuer-name cn=cisco.local
    grant auto
    hash sha256
    database url flash:
                                         usernames/passwords on the router.

                                         ROOT_CA(config)# ip http server
```

Meaning of each command

#crypto pki server ROOT

This **creates and enters configuration mode** for a PKI Certificate Authority server named ROOT.

#database level complete

Specifies that the CA should **store full certificate information** in its database, not just minimal info.

❖ **Benefit:** Useful for tracking and revoking certificates later.

#database archive pkcs12 password cisco123

This tells the CA to **archive certificates and private keys** in **PKCS#12 format** (a secure binary format containing the cert + key), and:

password 7 ... sets the encrypted password used to protect the archive.

7 means the password is encrypted using Cisco's type 7 encoding.

Why: So certs/keys can be backed up securely (e.g., for disaster recovery).

#issuer-name cn=cisco.local

Sets the **Common Name (CN)** of the Certificate Authority's certificate to cisco.local.

❖ This becomes the **name of the root CA** in all certificates it issues.

```
#grant auto
```

Automatically **approves all certificate requests** without manual admin approval.

NB: Useful in lab or test environments, but in production, you'd typically **manually approve** requests.

```
#hash sha256
```

Specifies that the CA should use the **SHA-256 hashing algorithm** for certificate signatures (instead of older/less secure algorithms like SHA-1).

✓ Stronger and more secure hash.

```
#database url flash:
```

Tells the CA to **store its database files in the router's flash: memory**.

✓ Flash is non-volatile, so the data survives reboots.

Step 6

Uninstall the old root certificate on all controllers

```
vmanage(config)#  
vmanage(config)#  
vmanage(config)#  
vmanage(config)# do request root-cert-chain uninstall
```

Step 7

Download the root certificate from the Root CA on all controllers



The screenshot shows the vManage command-line interface (CLI) executing a 'do request download' command to retrieve a root certificate ('ROOT.ca') from a specific URL. The command output includes details about the connection, file length, and download progress. A network diagram at the bottom illustrates the path from the vManage controller to the external Root CA host (100.1.1.4).

```
vmanage(config)# do request download http://admin:cisco@100.1.1.4/ROOT.ca  
--2025-06-12 13:35:53-- http://admin:cisco@100.1.1.4/ROOT.ca  
Connecting to 100.1.1.4:80... connected.  
HTTP request sent, awaiting response... 401 Unauthorized  
Authentication selected: Basic realm="level_15 or view_access"  
Connecting to 100.1.1.4:80... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 1115 (1.1K)  
Saving to: 'ROOT.ca'  
  
ROOT.ca [100%] 1.09K --.+KB/s in 0s  
2025-06-12 13:35:53 (316 MB/s) - "ROOT.ca" saved [1115/1115]
```

Step 8

Install the new root certificate on all controllers

```
vmanage(config)# do request root-cert-chain install home/admin/ROOT.ca  
Uploading root-ca-cert-chain via VPN 0  
Copying ... /home/admin/ROOT.ca via VPN 0  
Installing the new root certificate chain Step 8  
Successfully installed the root certificate chain the new root certificate on all controllers  
vmanage(config)# do show control local-properties  
personalidentity  
sp-personality-name cisco  
organization-name cisco  
root-ca-chain-status Installed  
certificate-status Not-Installed  
certificate-validity Not Applicable  
certificate-not-valid-before Not Applicable
```

Step 9

Login into the GUI interface of VMManage. To do this, you need to retrieve the ip address assigned by the dhcp server on the **management vpn 512**. Use the command below. Copy this **ip address** in your web browser and press enter.

```
vmmanage (config)# do show interface vpn 512
interface vpn 512 interface eth0 af-type ipv4
ip-address 192.168.13.187/24
if-admin-status up
if-oper-status up
encap-type null
port-type mgmt
hwaddr 50:08:87:00:3e:00
speed-mbps 1000
duplex full
uptime 0:01:59:05
rx-packets 5395
tx-packets 3468
vmmanage (config)#

```

Step 10

After login, click on the **administration tab**, on the left.

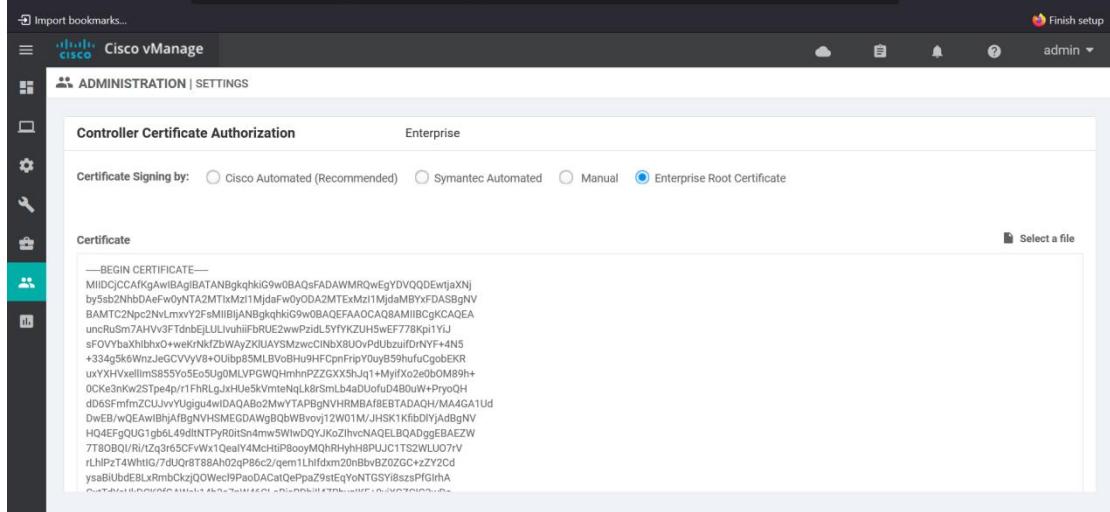
The screenshot shows the Cisco vManage Main Dashboard. On the left, there is a vertical navigation bar with several options: Import bookmarks..., Cisco vManage, DASHBOARD | MAIN DASHBOARD, Administration (which is highlighted in blue), Settings, Manage Users, Cluster Management, Integration Management, Root CA Management, and Disaster Recovery. The main dashboard area displays various status indicators: Control Status (Total 1), Site Health (Total 0), WAN Edge Health (Total 0), and Transport Health. The Control Status section shows 'Control Up' with 1 instance. The Site Health section shows 'Full WAN Connectivity' with 0 sites. The WAN Edge Health section shows 0 instances in Normal, Warning, and Error states. The Transport Health section has a dropdown menu set to 'By Loss'.

Under the administration tab, click on **settings**.

This screenshot is identical to the one above, but the 'Settings' option under the 'Administration' tab in the left sidebar is now highlighted in teal, indicating it is the active selection.

Step 11

Click on Controllers Certificate Authorization section, and click on the “Edit” button on the right. Select the “Enterprise Root Certificate” option and paste the root certificate from the **ROOT CA Server** here and click on **Save**.



The screenshot shows the Cisco vManage interface under the Administration settings. The 'Controller Certificate Authorization' section is displayed. The 'Enterprise' tab is selected. Under 'Certificate Signing by:', the 'Enterprise Root Certificate' option is checked. A large text area labeled 'Certificate' contains a long base64-encoded certificate string. A 'Select a file' button is visible at the top right of this area.

Open the terminal of the ROOT CA and type this command to see the **ROOT CERTIFICATE**

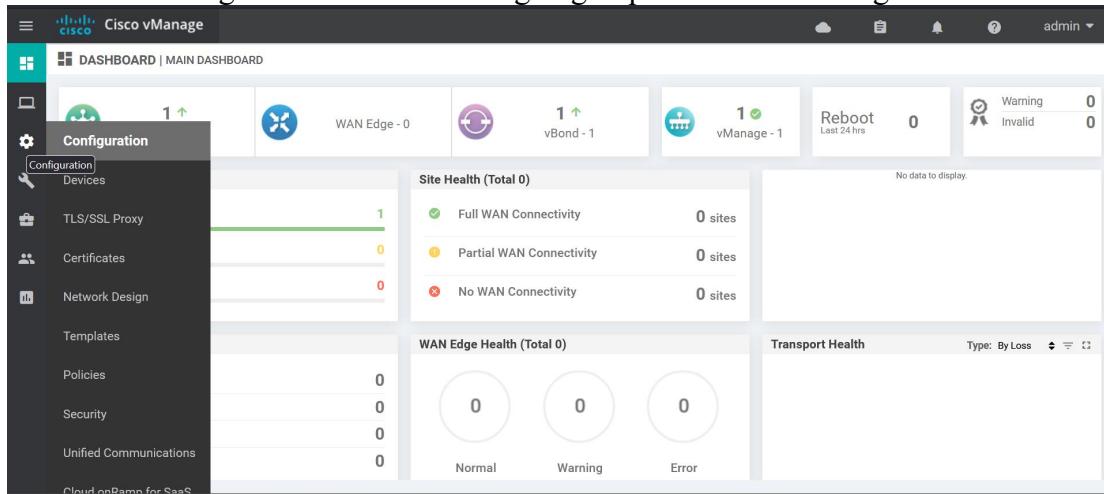
#crypto pki export ROOT pem terminal

```
ROOT_CA(config)#crypto pki export ROOT pem terminal
% The specified trustpoint is not enrolled (ROOT) of the ROOT CA and type this command
% Only export the CA certificate in PEM format.
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIDCzCAfkgwIBAgIBATANBgkqhkiG9w0BAQsFADAWMRQwEgYDVQQDEwtjaXNj
by5Sb2NhbAefw0yNTA2MTxMz1MjdaFwv0DA2MTExMz21MjdaBYFDASBgNV
BAMTC2Npc2NvLmxvY2FsmIIIBiJANBgkqhkiG9w0BAQEFAAOCAQ8AMIIlCgKCAQEA
uncRuSm7AHV3FTdnuEJULvhuiIbRUe2wwPzid5YFYKZUH5wEF778kp1Yj
sFOVYbaXhbxO+weKRNkZbWayZKUAYSMzwzClnBx8J0vPdUzziufhNYF+4N5
+334g5k6Wnz_leCVVvV8_0Ulb85MLBV0h4pHFpFnj0uPb9hfuFcgbEKR
uxXHVellim855yo5eo5ug0MLVPGW0hmhnPZGX5X5j1+MyfIx2e0bOM89h+
0CKe3nKw2STpe4p/1FRUgjxhJe5kVmteNqLk8SmI.b4aUoJu04b0uW+Pry0H
d6SFmfmzCUJvYUigui4wIDAQAB02MwYTAPBgNVRHMAfBEBTADAQH/MA4GA1ud
DwEB/wQEawIBhAfBgnVHSMEDAwgQbwvovoy12w01M/JHSK1kfbd0YjdgBgnV
HQ4EfgrQUG1gb6L49d1NTPyR0tsn4mSW1WDQYJkoZlhvcNAQELBQADggEBAEZw
7780BQz/R1/tzq3r65CFvw1QeaIY4MChtP8ooyMqrHyh8PUJC1TS2WL0U7FV
rlH1PzT4whrtzG//duQr8T8Ah02p86c2/qem1hifdxm20nbvBZ0ZGc-zZY2cd
ysaB1bd8LxRmbckzjqowec19PaodAcatoePpa29stEqv0NTGSY18szspFgIRhA
CxTdyaUdcK0FGAwak14b3a7nW46CL6bi5rdh1i14ZkhvqIKF=OjXGZC1G3wdo
v0gRhZ2eyq7LhfcnTHqtqe6mtiybckrdRpgDowS2i5H+GQxoYhBDw6nf7bzih
t7kdA1SNS1Jop0p1Rvbgs=
-----END CERTIFICATE-----
```

ROOT_CA(config)#

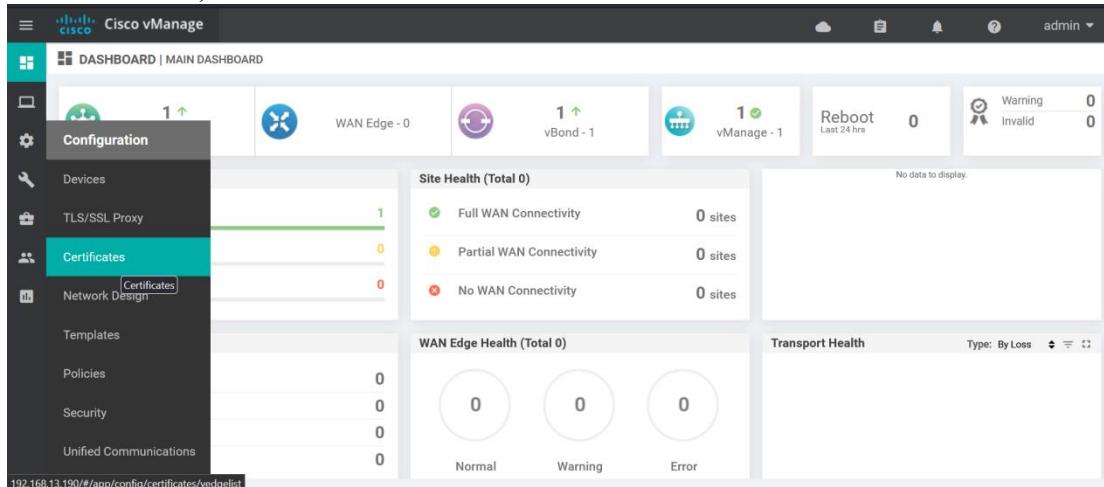
Step 12

We will need to generate a certificate signing request for the vmanage.



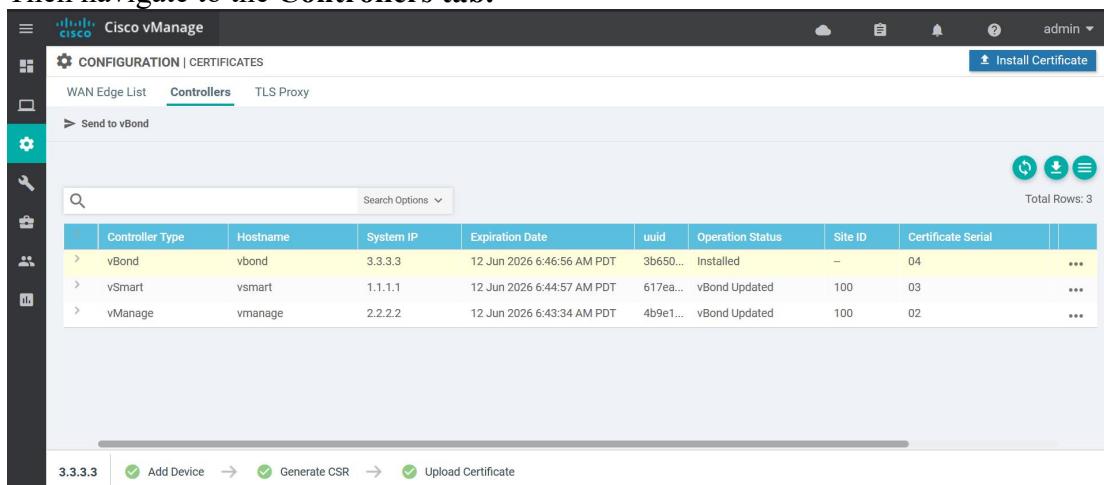
The screenshot shows the Cisco vManage main dashboard. On the left, a navigation menu under 'Configuration' has 'Certificates' selected. The dashboard displays various health metrics: Site Health (Total 0), WAN Edge Health (Total 0), and Transport Health. A status bar at the bottom indicates 'Cloud onPrem for SaaS'.

To do this, navigate to the menu on the left side of the panel, click on **Configuration** and under that , select **Certificates**.



The screenshot shows the Cisco vManage main dashboard. The 'Certificates' option in the 'Configuration' menu is highlighted. The dashboard displays Site Health (Total 0), WAN Edge Health (Total 0), and Transport Health. A status bar at the bottom indicates 'Cloud onPrem for SaaS'. The URL '192.168.13.190/#/app/config/certificates/vbondlist' is visible at the bottom left.

Then navigate to the **Controllers** tab.



The screenshot shows the 'CONFIGURATION | CERTIFICATES' page. The 'Controllers' tab is selected. It lists three controllers: vBond, vSmart, and vManage, along with their details like Hostname, System IP, Expiration Date, and Operation Status. At the bottom, there are buttons for 'Add Device', 'Generate CSR', and 'Upload Certificate'. The URL '3.3.3.3' is visible at the bottom left.

Click on the “three-dot” button on the right of the table and select “Generate CSR” from the drop-down menu.

The screenshot shows the Cisco vManage interface under the 'CONFIGURATION | CERTIFICATES' section, specifically the 'Controllers' tab. A table lists three controllers: vBond, vSmart, and vManage. The vManage row is highlighted in yellow. A context menu is open over the vManage row, with the 'Generate CSR' option highlighted. An arrow points from the text 'Select "Generate CSR"' to this menu item. Below the table, there are several green checkmark buttons for actions like 'Add Device', 'Generate CSR', 'Upload Certificate', and 'Update vBond'.

Copy the CSR from the pop-up window.

The screenshot shows the same Cisco vManage interface, but now the 'Generate CSR' button has been clicked, opening a modal dialog titled 'CSR'. The dialog displays the 'CSR' content for the IP address 2.2.2.2. The content starts with 'BEGIN CERTIFICATE REQUEST' and includes a long string of base64-encoded data. There is a 'Download' button at the top right of the dialog. The background table and other interface elements are visible behind the dialog.

Move to the CA_Server, type this command #do crypto pki server ROOT request pkcs10 terminal, then paste the CSR here, and press enter.

The screenshot shows a terminal session on a CA Server. The command '#do crypto pki server ROOT request pkcs10 terminal' has been entered. A large blue arrow points from the text 'Paste the CSR here' to the end of the command line where the CSR content is being pasted. The terminal also shows other configuration details and a table of certificates at the bottom.

The identity certificate will be generated, and copy what's under the **Granted Certificate** starting from, “Begin Certificate” to “End Certificate”.

Copy this Granted Certificate and head back to the GUI of the Vmanage, and click on the “Install Certificate Button”

The screenshot shows the Cisco vManage interface under the Configuration tab, specifically the Certificates section. The main content is a table listing three controllers: vBond, vSmart, and vManage. Each row includes columns for Controller Type, Hostname, System IP, Expiration Date, uuid, Operation Status, Site ID, and Certificate Serial. The vManage row is highlighted with a yellow background. At the top right of the table area, there is a blue button labeled "Install Certificate". A blue arrow points from the top right corner of the image towards this button.

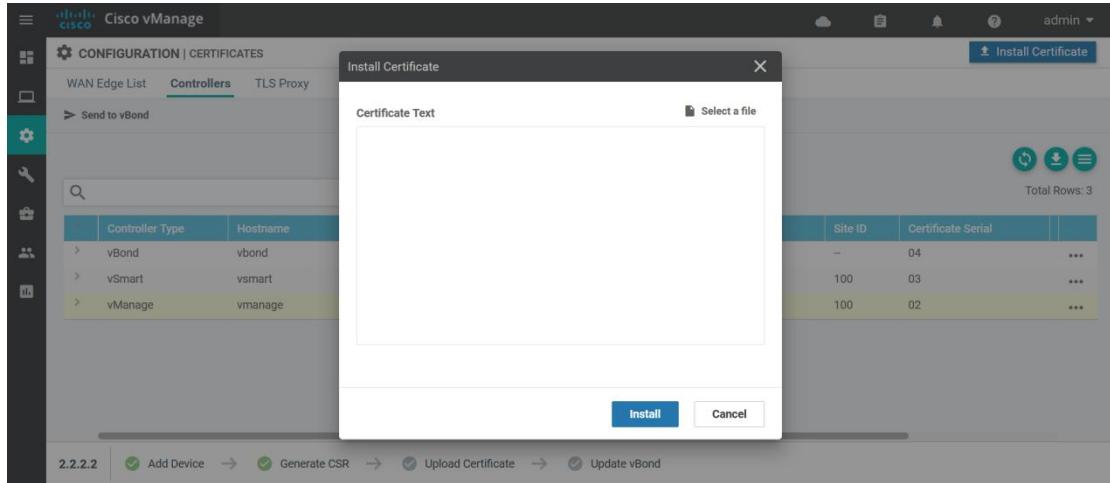
	Controller Type	Hostname	System IP	Expiration Date	uuid	Operation Status	Site ID	Certificate Serial	
>	vBond	vbond	3.3.3.3	12 Jun 2026 6:46:56 AM PDT	3b650...	Installed	—	04	***
>	vSmart	vsmart	1.1.1.1	12 Jun 2026 6:44:57 AM PDT	617ea...	vBond Updated	100	03	***
>	vManage	vmanage	2.2.2.2	12 Jun 2026 6:43:34 AM PDT	4b9e1...	CSR Generated	100	02	***

Total Rows: 3

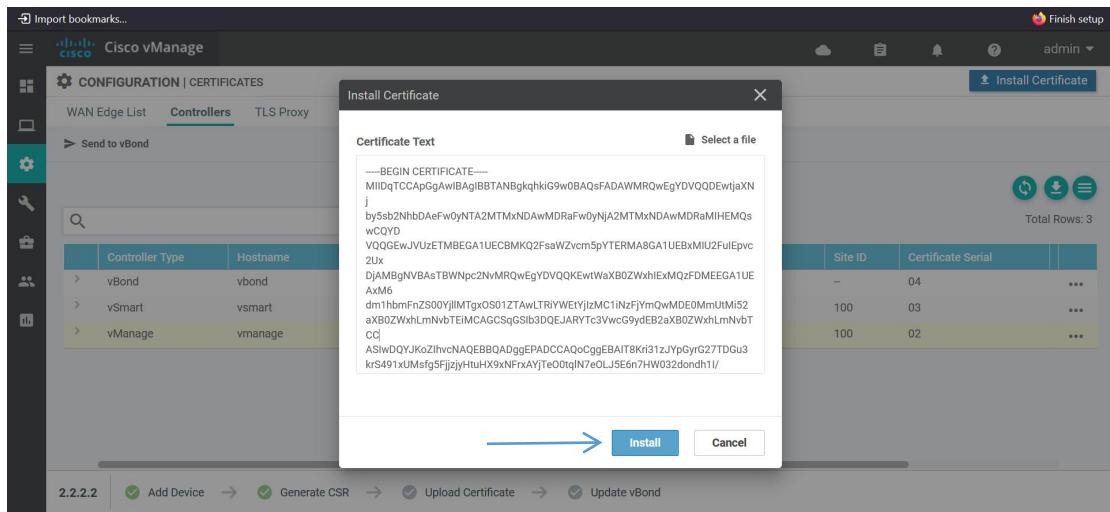
Bottom navigation bar:

- 2.2.2.2
- Add Device →
- Generate CSR →
- Upload Certificate →
- Update vBond

Paste the copied Generated Certificate (Identity certificate) here in the small window.



Click on the install button, Repeat this process for all the controllers and the Vedge devices



After clicking on the install button, the certificate will go through 3 different states, Scheduled , In Progress, Success State.

State 1 - Scheduled State

Status	Message	Device Type	Device ID	System IP	vManage IP
Scheduled	Install Certificate, on device 4...	vManage	4b9e1819-5e00-4baa-b230-ue...	2.2.2.2	N/A

State 2 - In Progress State

The screenshot shows the Cisco vManage interface with the title 'TASK VIEW'. A single task titled 'Install Certificate' is listed as 'In Progress'. The task details are: Status: In progress, Message: Pushed serial list to vManage..., Device Type: vManage, Device ID: 4b9e1819-5e00-4baa-b230-b..., System IP: 2.2.2.2, and vManage IP: 2.2.2.2. The task was initiated by admin from 192.168.13.1.

State 3 - Success State

The screenshot shows the Cisco vManage interface with the title 'TASK VIEW'. A single task titled 'Install Certificate' is listed as 'Success'. The task details are: Status: Success, Message: Successfully synced vEdge lis..., Device Type: vManage, Device ID: 4b9e1819-5e00-4baa-b230-b..., System IP: 2.2.2.2, and vManage IP: 2.2.2.2. The task was initiated by admin from 192.168.13.1.

Note : if you don't see the success state then you need to troubleshoot the entire topology, using the procedure below.

1. First check for reachability between controllers and the **ROOT CA Server**, by pinging from **VPN 0** to the destination ip address of the **ROOT CA Server**.
2. Check if the HTTP and SSH configurations were done appropriately on the **ROOT_CA Server**.
3. Check if **username**, **privilege** and **password** were configured on the **ROOT_CA Server**.
4. Make sure the pki server is m
5. Check each line of configuration under the #crypto pki server <ROOT_Servername>
6. Make sure the old root-cert-chain is uninstalled on all controllers.
7. Download the root-certificate from the **ROOT_CA** server on all controllers
8. Make sure the root-certificate is installed on all the controllers. To verify this use, the command, **#do show control local-properties. And check the root-ca-chain-status, you should see "installed".**