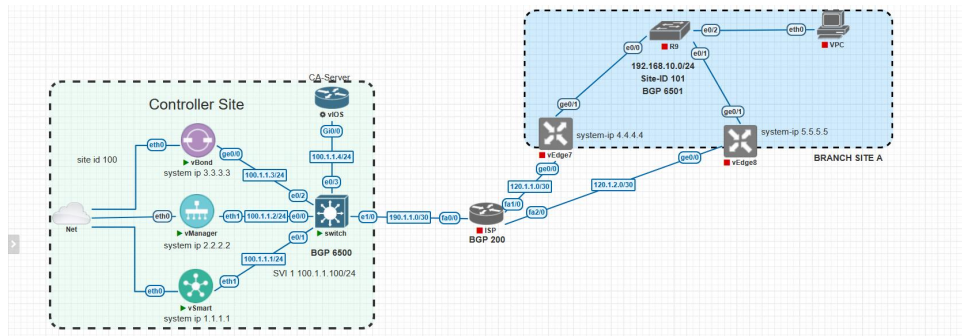


Step by step process to onboard Sdwan Devices (Controllers and Site Routers)

Step1

Onboard the controllers first (vbond, vmanage, vsmart)



Step 2

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

Vsmart System Configuration

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

Vmanage System Configuration

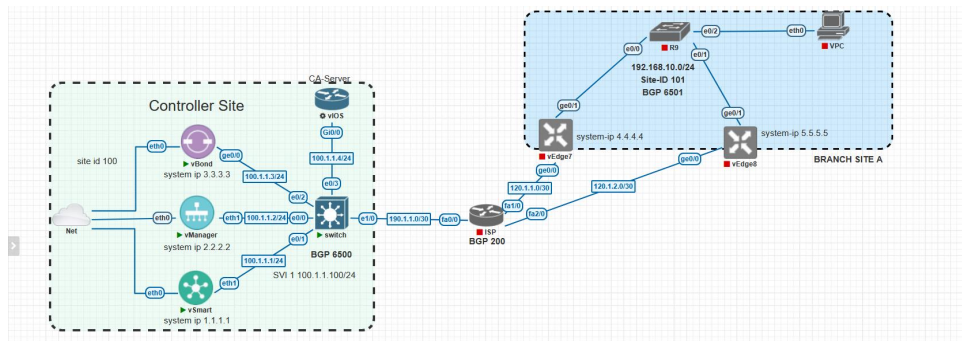
```
vmanage(config)# system
vmanage(config-system)# system-ip 2.2.2.2
vmanage(config-system)# organization-name cisco
vmanage(config-system)# vbond 100.1.1.3
vmanage(config-system)# site-id 100
vmanage(config-system)# clock timezone Africa/Accra
vmanage(config-system)# commit
Commit complete.
vmanage(config-system)#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

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 such as **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 100.1.1.1/24
vsmart(config-interface-eth1)# no shutdown
vsmart(config-interface-eth1)# tunnel-interface
vsmart(config-tunnel-interface)# allow-service sshd
vsmart(config-tunnel-interface)# allow-service netconf
vsmart(config-tunnel-interface)# commit
vsmart(config-tunnel-interface)#
```

Vmanager VPN 0 Configuration

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

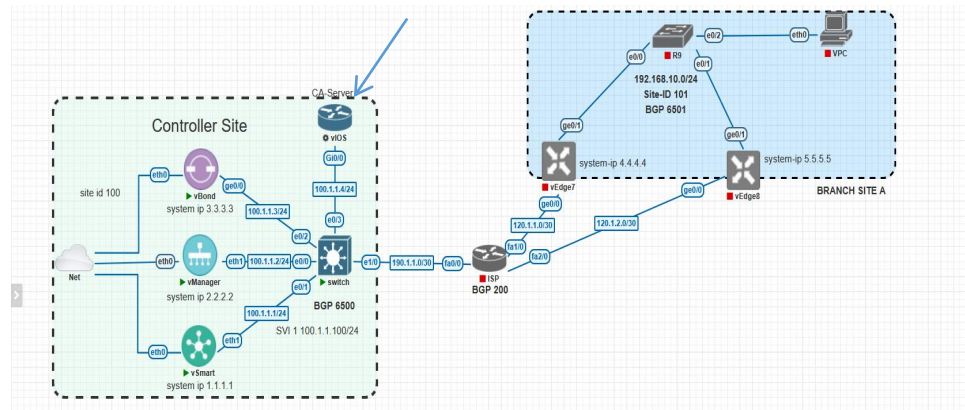
Configure the management vpn on the VManage. The management vpn by default is VPN 512. This vpn cannot be deleted.

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)#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 14141B180F0B787977
issuer-name cn=cisco.local
grant auto
hash sha256
database url flash:
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

```
vmanage(config)# do request download http://admin:cisco@100.1.1.4/ROOT.ca  
-2025-06-12 13:35:53-- http://admin:password@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  
personality vmanage  
sp-organization-name cisco  
organization-name cisco  
root-ca-chain-status Installed  
certificate-status Not-Installed  
certificate-validity Not Applicable  
certificate-not-valid-before Not Applicable
```

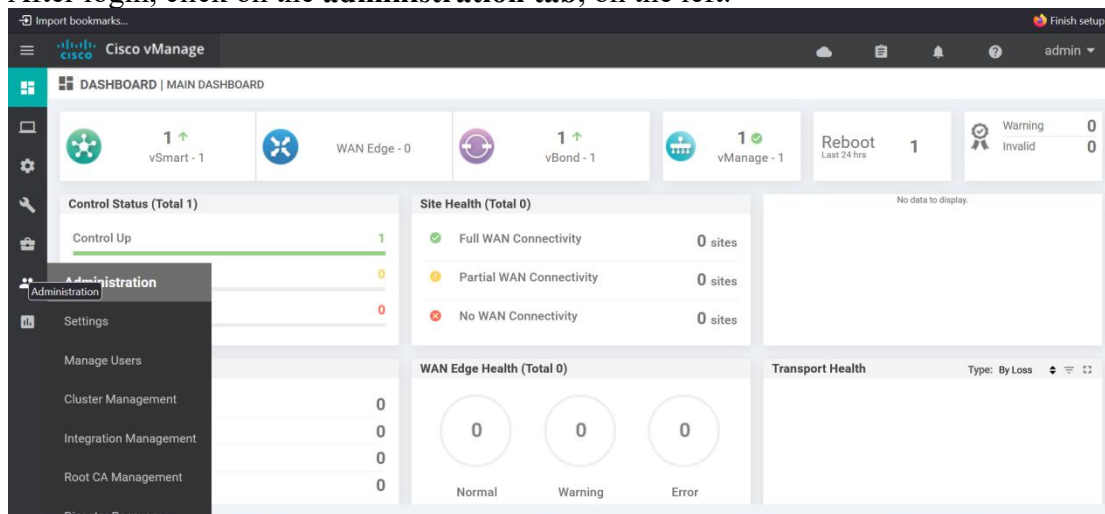
Step 9

Login into the GUI interface of VManage. 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.

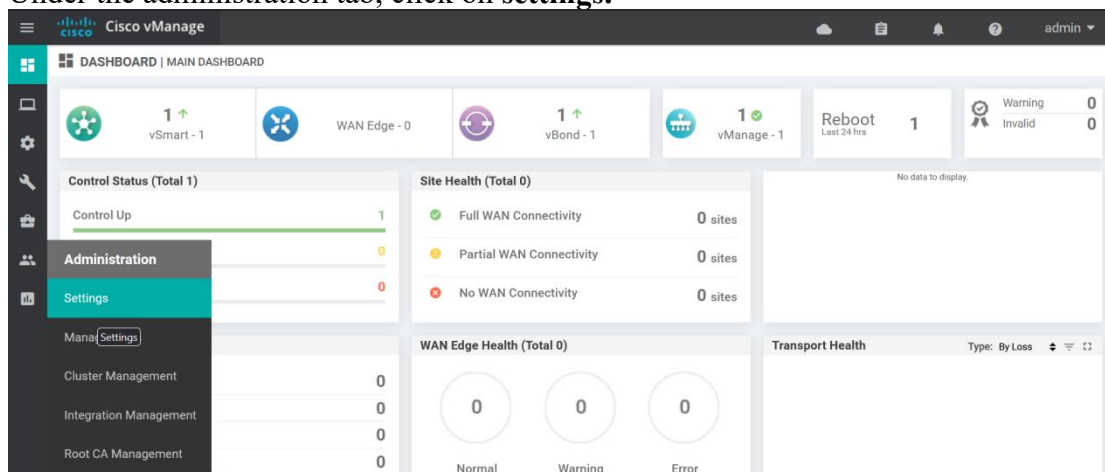
```
vmanage(config)# do show interface vpn 512
interface vpn 512, interface eth0 af-type ipv4
ip-address 192.168.13.187/24
if-admin-status Up
if-oper-status Up
encap-type null
port-type mgmt
hwaddr 50:08:87:00:3e:00
speed-mbps 1000
duplex full
uptime 0:01:59:05
rx-packets 5393
tx-packets 3488
vmanage(config)#
```

Step 10

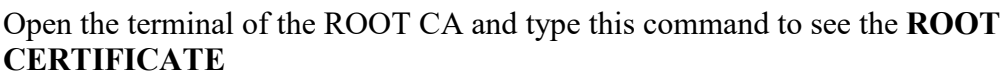
After login, click on the **administration** tab, on the left.



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

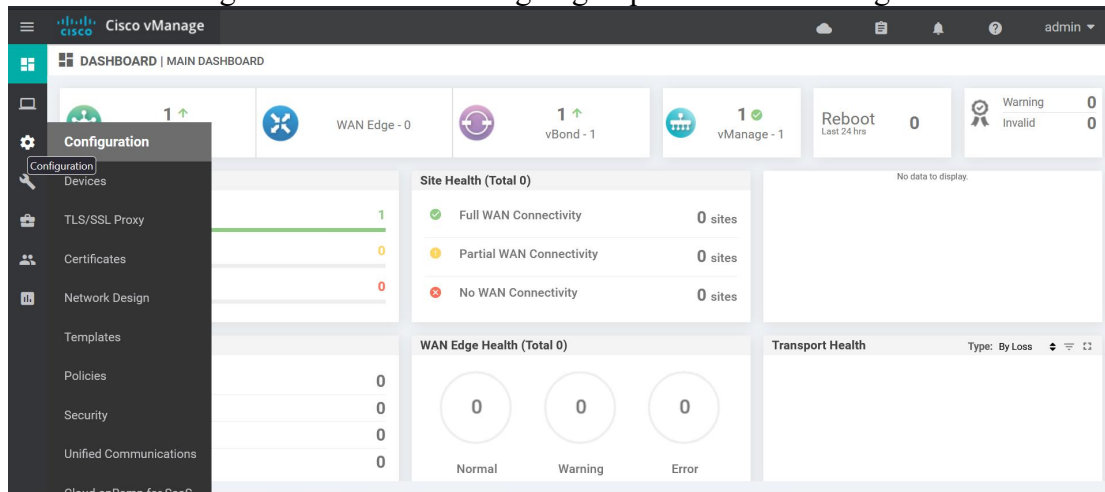


Click on **Controllers Certificate Authorization** section, and click on the “**Edit**” button on the right. Select the “**Enterprise Root Certificate**” option and paste the root certificate from the **ROOT CA Server** here and click on **Save**.

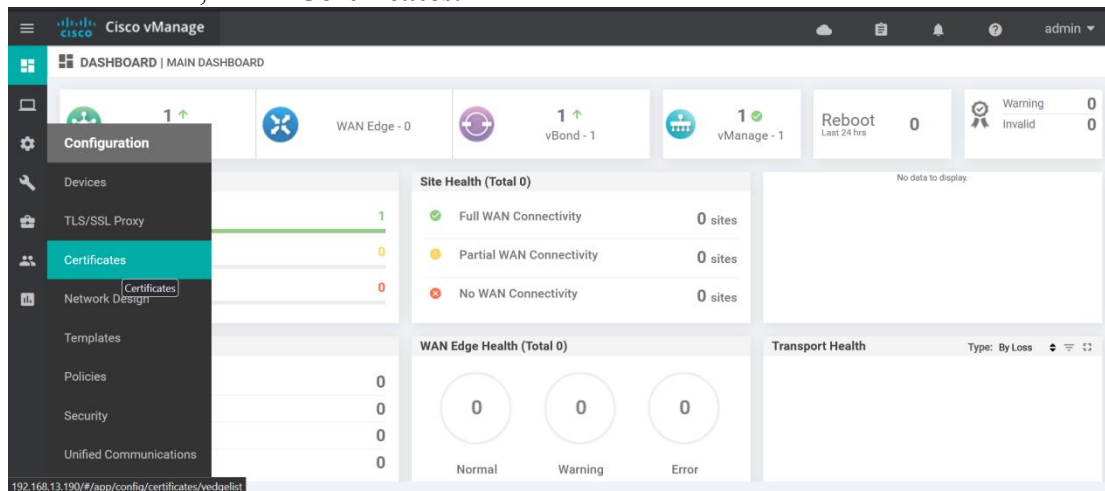
[illegible]

Step 12

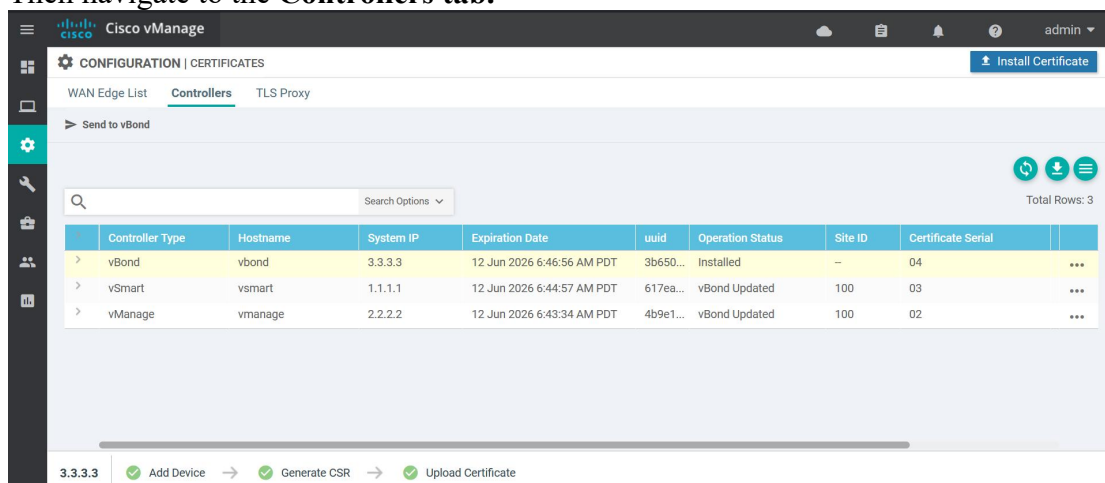
We will need to generate a certificate signing request for the vmanage.



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



Then navigate to the **Controllers** tab.



The screenshot shows the Cisco vManage interface for configuring certificates. The 'CONFIGURATION | CERTIFICATES' section is active, with the 'Controllers' tab selected. Below the tabs, there's a 'Send to vBond' button. A search bar is present above a table of controllers. The table has columns: Controller Type, Hostname, System IP, Expiration Date, uuid, Operation Status, Site ID, and Certificate. Three controllers are listed: vBond, vSmart, and vManage. A blue arrow points to the three-dot menu icon next to the vManage row, which has opened a context menu with the following options: View CSR, View Certificate, Generate CSR, Reset RSA, and Invalidate.

	Controller Type	Hostname	System IP	Expiration Date	uuid	Operation Status	Site ID	Certificate
>	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...	vBond Updated	100	02

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

Copy the CSR from the pop up window.

3.3.3.3 Add Device → Generate CSR → Upload Certificate

[illegible]

```
File Edit View Options Transfer Scripts Tools View Help
vManager vSmart vBond switch vIOS
ohXcb2qtV58qYf1PMHP1wGj2cnmsYRWAdow3Vg7F+G65BvX1k3u3SLqt14MofYF3
FYZJ2b2p82PmKRMd2FdcZC0e5-9YkV1J1FmNR3C0Dh0Xa4tF4MEZz1Ab
JkaKc2e5YNC1R0NqGRFRLdqweOq3e2ScXcb8GaxezoaQ5yYxtcUy4ZqQ1myLw5Dg
K106/85Nak3kmaesxgFulM/SwIDAQAQAb0dswOQYJKoZIhvcNAQOMSwMkJA3BgNV
HREMAjAAMBG0A1UddgQWBBTaoof1xyUfJmxbKcxzdaYMPZ5AjaNBgkqhkiG9wOg
AQAQACQgZAAQABAgQDABAgwB3-OnhVq4F7qbmS53Kf6kYdampy1c
KyJApe4YjnnYZa5N0s9cK7M6LkNmU49JKOYUdckFcgvvwv01l8kdcy5I0h10sh7
V1Rj326BxpGLT4Dxbnk9Cgn4v0EABNLKzYRCMicsvZwXcbjYvVUF21vhaqqQ3/gp
FkmwJg35pd88qkIdId0ic0HdLgnchFkxou4diEjK8VysZHMxkCzsaNs1Q3CW
FmW3741E11kVvabAB15Yvhw-Zort5vZy9nAG01BawCv1fak8yNmfrYv/JidjyPv
1u173CNHX1BAVSxduJHAAlp0xAG0YdcYxw
-----END CERTIFICATE REQUEST-----

%
-----BEGIN CERTIFICATE-----
MIIDqTCCAggAAgIBAgBTEBAnBgkqhkiG9wOBAQFADAAWRRQwEYDVQDEwtJAKNj
Fy582Nhhbdaefw0YnTAZMTmXNDABMDRwFw0YnJAZMTmXNDABMDRAMEHMQscWQY
VQGEZmVuzizETMBGAJUECMkQDABAgwB3-OnhVq4F7qbmS53Kf6kYdampy1c
JAMBGNVBASTBwNpc2N2MwQwEYDVQDEQWtwaXB0ZWxhEiMQZ2FMEEGA1UEAAMG
dm1lbmFmZS00Yj1jMTQxOS01ZTAwLm1rYnY1Y2MCI1nzF3YmQwMEOMUMtM152
AXB0ZWxhbmVudTE1MCAgZSg5d2J0GE2ARyTC3YwG9ydyB2aXB0ZWxhbmVudTC1
PwSIDQY3koZiJvbcNAQEBBQAGQgEAPdCCACoqgeBA1f8k13izYpdyG87TDG3J
fRS491xUM5fGSF1jzjYHtUHXNfrXAY3E00tq1N7e0L35E6NHW032dondh11/
0AR7wQvtVizj4X0YlduDSASE7K1zp426CF1mfqIV3G9qrB+fkmZHTB6SFuo3555F
Gevghart47H4d1Phep-qvZ5F7AS6ryYUk8dkgG9PflVnkmdwzj1ETHdn3Bc
QjNEvul13ixte34zcdwEAdf5Gk6-1B0bL3oGym6k2XumQdQUTJAKEx053B
3tknFwm/BmsKszmqumM6bFGOGAK1psvUQ4C1NOvweTwpN5JmrfacYHLC5v+cC
AwEAAANTMFEwDQVDR0TAQHBAUwAwEefZaF6gnvHSMGEADwBQDwBv0j12W01M
/7Hsk1Kf1b0Y1jadrngNVH04EFgQ0u8akH2pcc1B5Y121763w1BwGcy0YwG3Q2G1
PwSIDQgBQADgEAd000T7F08sp6YU7Majf8w9YHT3k1Q8FIINCEvduvCTY
gwXdcYc0Bic2rFpmkALE3C1kRaxogp0v1dHwvXku1U2BB2McZLAvo11V9TKd0Zw
Pu0-4fyCfKewdyxd71dx1ze+9iE1A1v+of35j1ewM5b3C/8ANHSjTTLr1Pr10M
r+Of41f8K1cY4d/3s3t3Yuz4v0GLN65X/c0CPBZb3LDnTCFYU1EUDh4eF5Ns
+CC9LcEdw0b05G/5T24ox+k110G0vC0gapi4BMZLQNCdC181wEXtzcZ1so5n
q1bKdQjY7DsFG0jns5Fnsa0AzmY9B7tsXodY/Ei5G
-----END CERTIFICATE-----

Router(Config)#
```

CONFIGURATION | CERTIFICATES

WAN Edge List Controllers TLS Proxy

Send to vBond

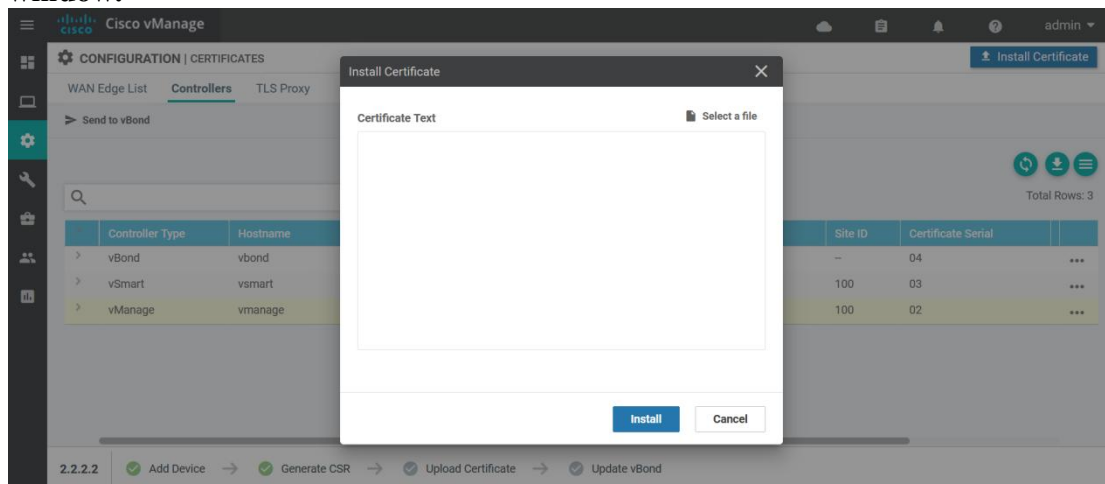
Search Options

Total Rows: 3

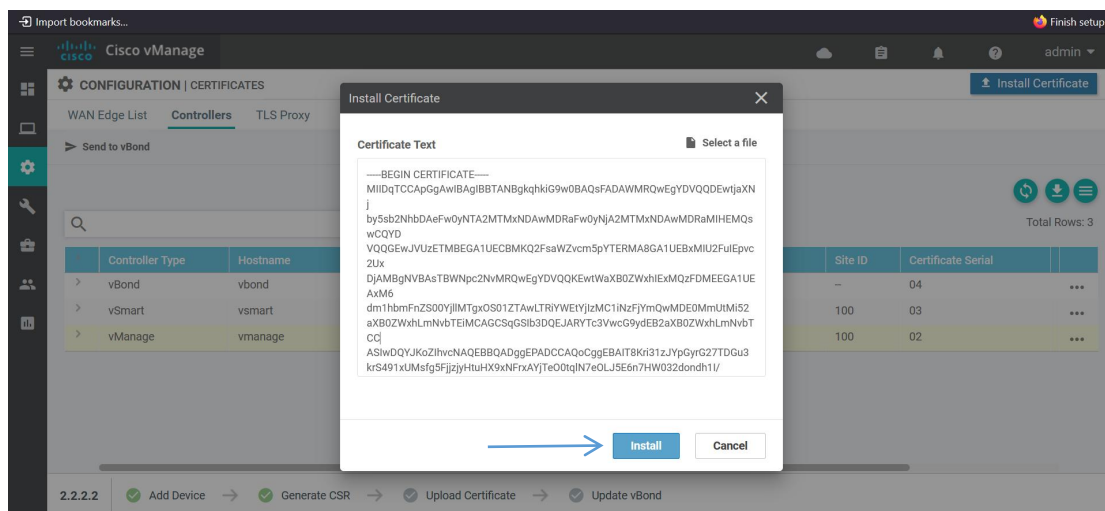
	Controller Type	Hostname	System IP	Expiration Date	uuid	Operation Status	Site ID	Certificate Serial	
>	vBond	vbond	3.3.3.3	12 Jun 2026 6:46:56 AM PDT	3b650...	Installed	-	04	...
>	vSmart	vsmart	1.1.1.1	12 Jun 2026 6:44:57 AM PDT	617ea...	vBond Updated	100	03	...
>	vManage	vmanage	2.2.2.2	12 Jun 2026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

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

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

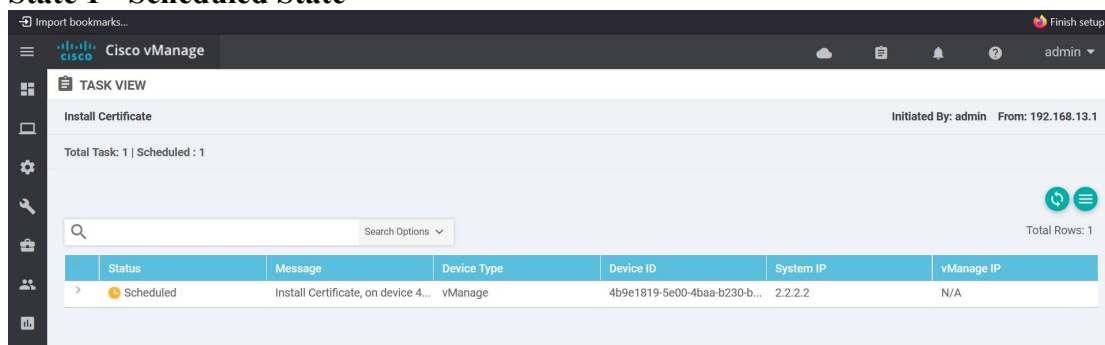


Click on the install button, Repeat this process for all the controllers and the Vedge devices



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

State 1 - Scheduled State



State 2 - In Progress State

The screenshot shows the Cisco vManage interface. The top navigation bar includes 'Cisco vManage' and a user profile 'admin'. The main section is titled 'TASK VIEW' and 'Install Certificate'. It indicates 'Total Task: 1 | In Progress : 1'. Below this is a table with columns: Status, Message, Device Type, Device ID, System IP, and vManage IP. The table contains one row with the status 'In progress' and the message 'Pushed serial list to vManage...'. The device type is 'vManage', the device ID is '4b9e1819-5e00-4baa-b230-b...', the system IP is '2.2.2.2', and the vManage IP is '2.2.2.2'. The interface also shows a search bar and 'Total Rows: 1'.

Status	Message	Device Type	Device ID	System IP	vManage IP
In progress	Pushed serial list to vManage...	vManage	4b9e1819-5e00-4baa-b230-b...	2.2.2.2	2.2.2.2

State 3 - Success State

The screenshot shows the Cisco vManage interface. The top navigation bar includes 'Cisco vManage' and a user profile 'admin'. The main section is titled 'TASK VIEW' and 'Install Certificate'. It indicates 'Total Task: 1 | Success : 1'. Below this is a table with columns: Status, Message, Device Type, Device ID, System IP, and vManage IP. The table contains one row with the status 'Success' and the message 'Successfully synced vEdge lis...'. The device type is 'vManage', the device ID is '4b9e1819-5e00-4baa-b230-b...', the system IP is '2.2.2.2', and the vManage IP is '2.2.2.2'. The interface also shows a search bar and 'Total Rows: 1'.

Status	Message	Device Type	Device ID	System IP	vManage IP
Success	Successfully synced vEdge lis...	vManage	4b9e1819-5e00-4baa-b230-b...	2.2.2.2	2.2.2.2

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".