

# Migration Guide

## DigiCert (Symantec) Certificate to Cisco PKI Certificate on Cisco SD-WAN Controllers

## Table of Contents

Goal of this Document .....	3
Pre-requisites .....	3
Migration Steps to Install Signed Cisco PKI Certificate to Controllers .....	4
Option1: Automated certificate signing through Cisco Systems .....	4
Key Considerations:.....	5
Step1: Verify Cisco Plug and Play (PnP) portal connectivity.....	5
Step 2: Configure Smart Account credentials .....	6
Step 2: Configure vManage certificate settings .....	7
Step 3: Generate certificate signing requests .....	7
Step 4: Sign and install certificate signing requests.....	8
Option 2: Manual certificate signing through Cisco Systems .....	10
Step 1: Configure vManage certificate settings .....	10
Step 2: Generate Certificate Signing Requests .....	11
Step 3: Submit and sign the certificate signing requests .....	12
Step 4: Install the signed certificates .....	14
Verification: .....	15
Additional Resources: .....	16

---

## Goal of this Document

The primary goal of the document is to provide technical guidance on the steps needed to successfully migrate DigiCert (Symantec) certificate to Cisco PKI certificate on the Cisco SD-WAN controllers solution. It includes automated and manual methods for obtaining signed controller certificates from Cisco Plug and Play portal.

This guide assumes that the vBond, vSmart and vManage controllers are already deployed with certificate provided by DigiCert (Symantec).

## Pre-requisites

- Recommended software version to migrate to Cisco PKI certificate are SD-WAN controllers and vEdge routers to run 19.2.3+ and XE SD-WAN routers to run 16.12+
- You will need a Smart Account and Virtual Account at <http://software.cisco.com> to use the automated or manual method. The Smart Account credentials should be configured in the vManage GUI under Administration>Settings>Smart Account Credentials
- It is important that the Virtual Account in the Cisco PnP portal has a controller profile defined, and the organization name in the profile must match the organization name in the vManage GUI
- To check if DigiCert is installed, go to configured settings on vManage dashboard under Administration – Settings. If Symantec Automated/manual option is chosen, then it indicates that DigiCert certificates are installed.
- Ensure that Cisco root certificates are loaded on the WAN Edge devices before converting to Cisco PKI else the WAN Edge devices will not come up onto the network
- For XE SD-WAN routers, verify using the command: `show sdwan certificate root-ca-cert | inc Cisco`

```
C8Kv_Router# show sdwan certificate root-ca-cert | inc Cisco
Issuer: OU=Arcturus, O=Cisco, CN=Internal Customer Root CA Subject: O=Cisco,
OU=Albireo, CN=Viptela SubCA Issuer: OU=Arcturus, O=Cisco, CN=Internal Customer
Root CA Subject: OU=Arcturus, O=Cisco, CN=Internal Customer Root CA
```

- For vEdge routers, verify using the command: show certificate root-ca-cert | inc Cisco

```
vEdge# show certificate root-ca-cert | inc Cisco
Issuer: OU=Arcturus, O=Cisco, CN=Internal Customer Root CA Subject: O=Cisco,
OU=Albireo, CN=Viptela SubCA Issuer: OU=Arcturus, O=Cisco, CN=Internal Customer
Root CA Subject: OU=Arcturus, O=Cisco, CN=Internal Customer Root CA
```

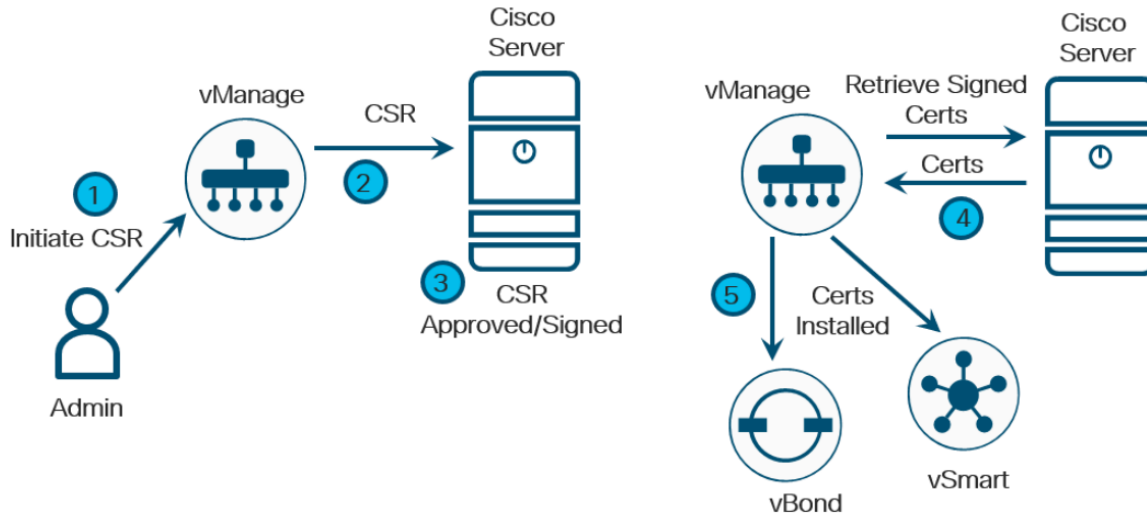
Note:

1. For Cisco XE SD-WAN and Viptela Edge (vEdge) routers (running 19.2 or higher), Cisco PKI root certificate are bundled in the software by default or distributed by the PnP or ZTP server when the WAN edge is automatically provisioned
2. Reach out to TAC support if there are any issues with migration or if Cisco SD-WAN controllers run on version below 19.2.3 to get support on upgrade/migration process

## Migration Steps to Install Signed Cisco PKI Certificate to Controllers

### Option1: Automated certificate signing through Cisco Systems

With this option, certificate signing requests are automatically sent to the Cisco PnP cloud service where the certificate is signed. The vManage then automatically retrieves the certificate and installs on itself and vBond, vSmart controllers as well.



### Key Considerations:

- Time taken to complete automated migration process (for vManage, vSmart & vBond controllers): ~ 15 minutes
- Control Connection expected to flap during certificate migration process
- vBond & vSmart controller downtime during migration: ~ 1 minute
- No service impact on WAN Edge routers

### Step1: Verify Cisco Plug and Play (PnP) portal connectivity

1. A DNS server needs to be configured to resolve the hostname `cloudsso.cisco.com` and subsequently `apx.cisco.com` and `swapi.cisco.com` using `ping` command.
2. To validate if vManage can reach the Cisco PnP server, go to the vManage CLI, type in `vshell`, then type `curl https://cloudsso.cisco.com`. You should see a message that the host is live.
3. Type in `curl https://apx.cisco.com` and you should get an html response from the server that the service unavailable. If the servers are not reachable, you should see "Failed to connect" messages. If they both succeed, then the automated process should work. Type in `exit` to end `vshell` mode.

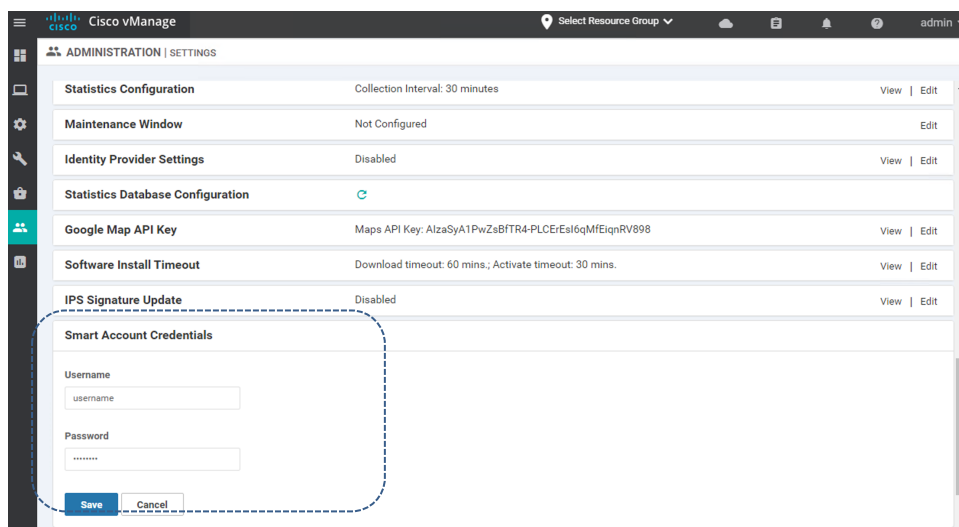
```
vmanage:~$ curl https://cloudsso.cisco.com
cloudsso is live
cloudsso2 is live
vmanage:~$ curl https://apx.cisco.com
<html><body><h1>503 Service Unavailable</h1>
No server is available to handle this request.
</body></html>
vmanage:~$
```

**Note:** Try curl -k “Cisco PnP Server URL” if you see SSL root certificate issue.

## Step 2: Configure Smart Account credentials

Before you can enable automatic signing of Cisco certificates, Smart Account credentials must be configured. h

1. On the vManage GUI, Go to Administration>Settings.
2. At the bottom of the page, go to the right of Smart Account Credentials and click Edit.
3. Enter the Username and Password that gives you access to your Smart Account information at <https://software.cisco.com>.

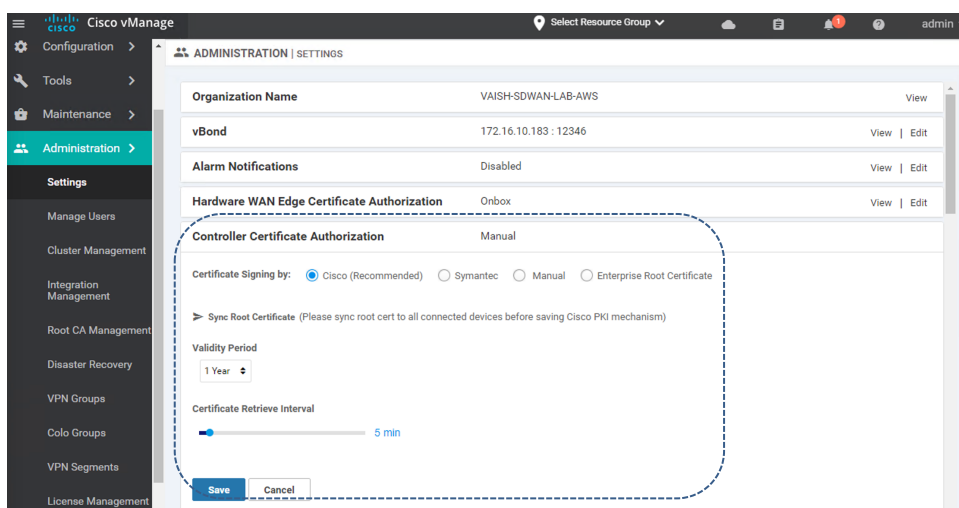


4. Click Save.

### Step 2: Configure vManage certificate settings

1. On the vManage Administration > Settings page, go to the right of Controller Certificate Authorization and click Edit.
2. Select Cisco Automated (Recommended). If you change the setting, you will get a popup window asking to confirm the Certificate Authorization change. Click Proceed.
3. Select the Validity Period. Minimum is 1 year and maximum is 2 years.
4. Set the Certificate Retrieve Interval. This is the interval the vManage will check on whether the signed certificates are available after the CSR has been submitted. The default is 60 minutes, so you may want to decrease this value. Minimum is 1 minute, and maximum is 60 minutes.

**Note:** Recommended minimum interval is 3-4 minutes for successful certificate retrieval.

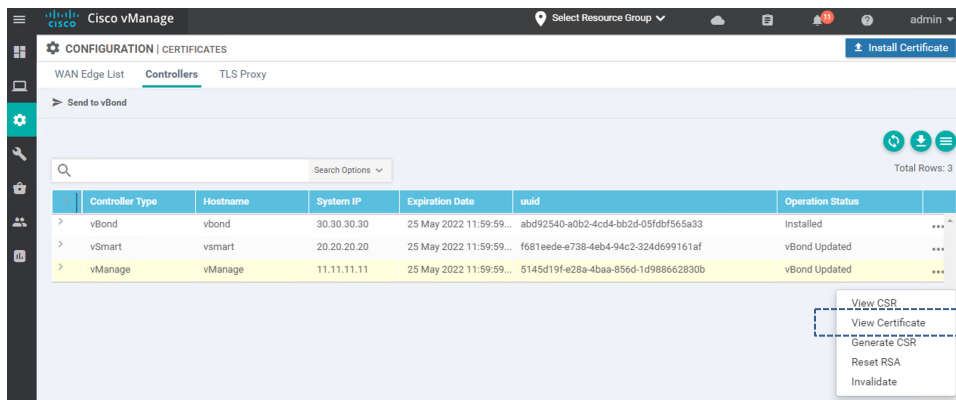


5. Click the Save button.

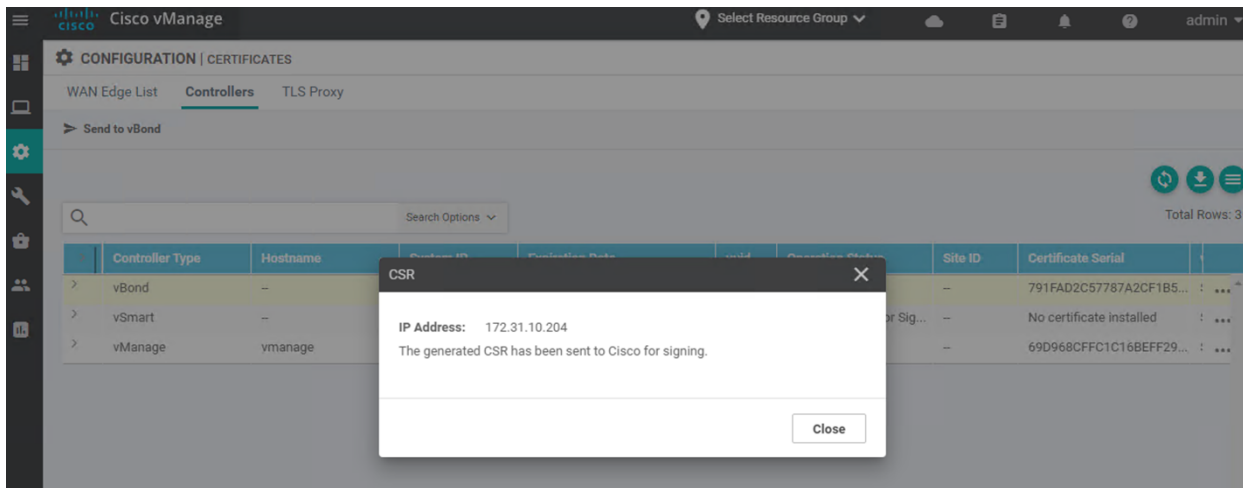
### Step 3: Generate certificate signing requests

Next, generate and submit certificate signing requests.

1. Navigate to Configuration > Certificates and click the Controllers tab
2. On the right side of vManage, click three dots (...) and select Generate CSR from the drop-down box.
3. A pop-up window states that the generated CSR has been sent to Cisco for signing. Click Close.



4. Repeat the process for the vSmart and vBond controllers.



#### Step 4: Sign and install certificate signing requests

The signing and installation of the Cisco certificates are completely automated. To view the status:

1. Go to <https://software.cisco.com> and login if prompted.
2. Click on Manage Devices under the Network Plug and Play section.



# Smart Licensing

Cisco Smart Licensing is a flexible licensing model that streamlines how you activate and manage software.

## For customers

### Existing account

Start by getting access to your company's existing Smart Account.

[Submit request >](#)

### New account

Don't have an account? Create one now.

[Create account >](#)

### Account administration

Update information and manage your users.

[Manage account >](#)

### Smart Software Manager

Convert classic to Smart Licenses.

[Manage licenses >](#)

### Network Plug and Play

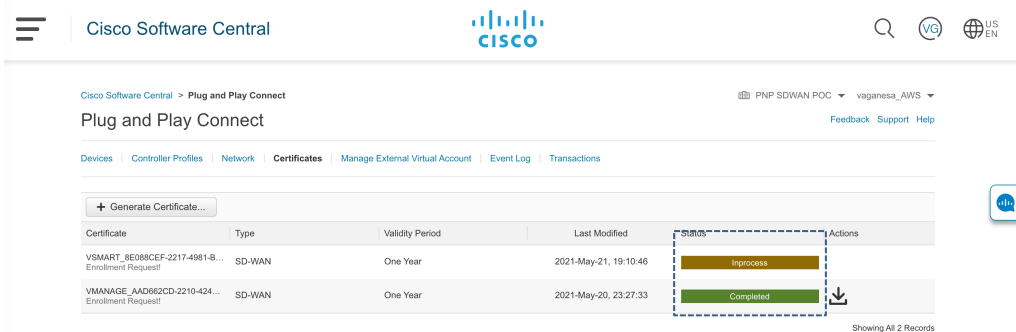
Automate device discovery and activation on-prem or from the cloud.

[Manage devices >](#)

3. Ensure the proper Virtual Account is chosen in the upper right-hand corner. This is the Virtual Account with the controller profile of the organization name used for the SD-WAN overlay.

## 4. Click Certificates

When a CSR is generated, you will see an enrollment request and the Status changes to In Process. When the request is signed, the Status changes to Completed.



The screenshot shows the Cisco Software Central interface. At the top, there is a navigation bar with the Cisco logo and a search icon. Below the navigation bar, the page title is "Cisco Software Central > Plug and Play Connect". The main content area is titled "Plug and Play Connect" and includes a "Generate Certificate..." button. Below this, there is a table with columns for Certificate, Type, Validity Period, Last Modified, Status, and Actions. The table contains two rows: one with "Inprocess" status and one with "Completed" status. A dashed blue box highlights the "Status" column for both rows.

Certificate	Type	Validity Period	Last Modified	Status	Actions
VSMART_BE089CEF-2217-4981-B... Enrollment Request	SD-WAN	One Year	2021-May-21, 19:10:46	Inprocess	
VMANAGE_AAD862CD-2210-424... Enrollment Request	SD-WAN	One Year	2021-May-20, 23:27:33	Completed	Download

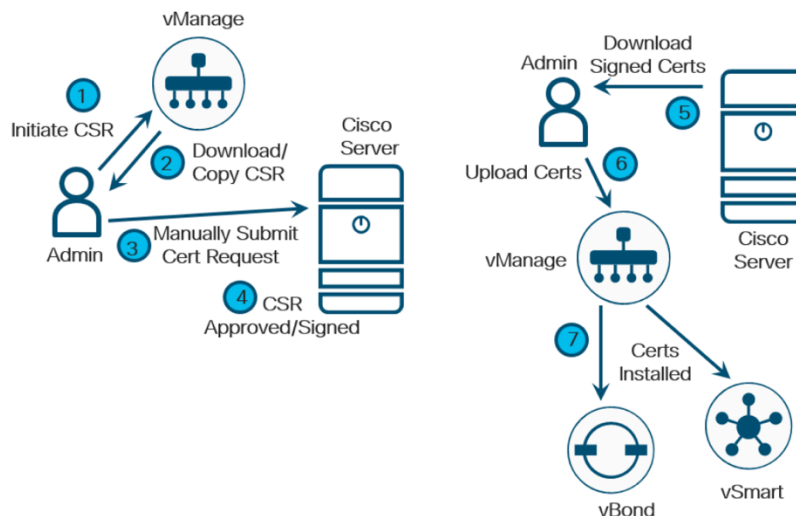
The vManage will automatically check at the configured interval for the signed certificates and install them.

Controller Type	Hostname ...	System IP	Expiration Date	uuid ...	Operation Status	Site ID	Certificate Serial
vBond	--	--	21 May 2022 7:11:40 ...	abd92...	Installed		153AE217170A211B0BF9...
vSmart	--	--	21 May 2022 7:00:47 ...	1f07f4...	vBond Updated		737CBCE0D0983922A9BE...
vManage	vmanage	5.5.5.5	20 May 2022 11:06:28...	67810...	vBond Updated		69D968CFFC1C16BEFF29...

172.31.10.137 | Add Device → Generate CSR → Waiting for Certificate

## Option 2: Manual certificate signing through Cisco Systems

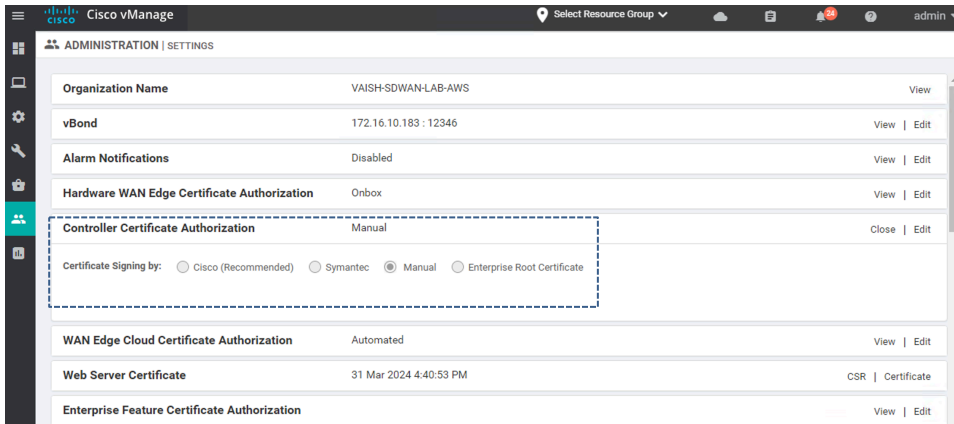
With this option, certificate signing requests are manually submitted by the administrator to the Cisco PnP portal, where the certificate is signed. The administrator can then download the resulting certificates from the PnP portal and manually install them in vManage.



### Step 1: Configure vManage certificate settings

1. On the vManage GUI, go to Administration>Settings
2. To the right of Controller Certificate Authorization, Click Edit

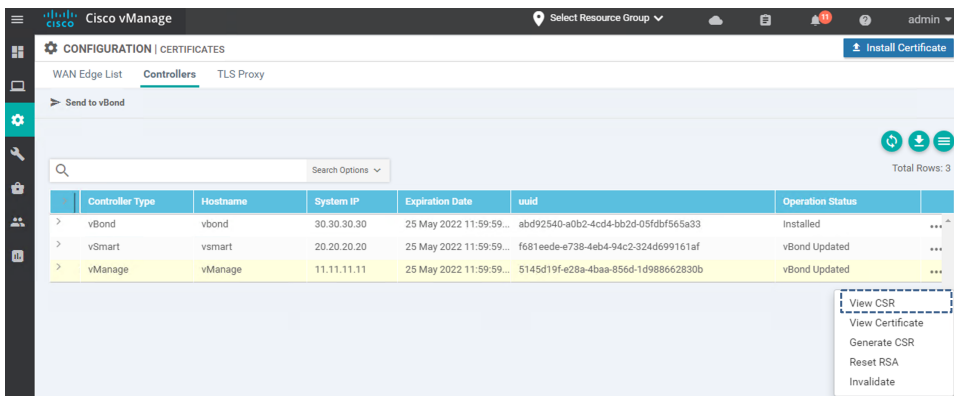
3. Select Manual if it is not already selected. If this is a change from the current configuration, you may get a pop-up window asking to confirm that you want to change the certificate authority which is used for authentication. Click Proceed



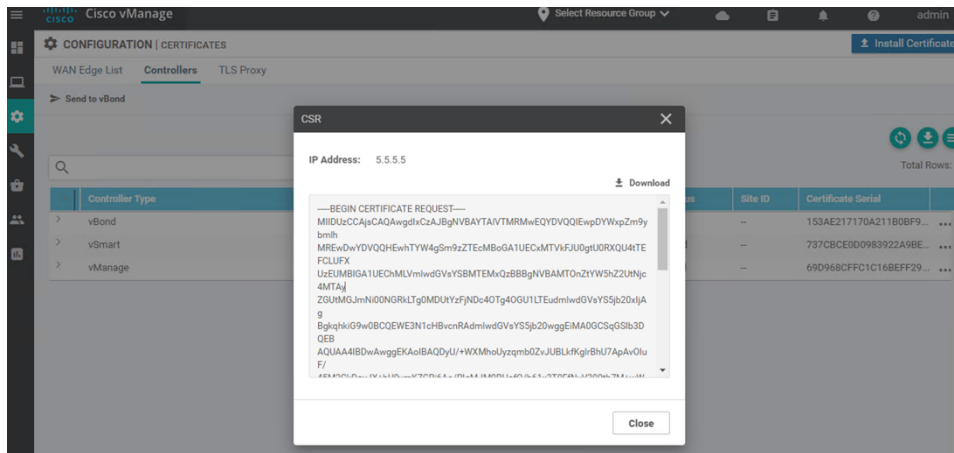
4. Click the Save button

## Step 2: Generate Certificate Signing Requests

1. Navigate to Configuration > Certificates and click the Controllers tab
2. On the right side of vManage, click three dots (...) and select Generate CSR from the drop-down box



3. A pop-up window appears with the certificate signing request. Copy the certificate signing request to submit for signing



4. Click Close. You can always view or download the CSR again by clicking three dots (...) to the right of the controller and selecting View CSR from the drop-down menu
5. Repeat the process for the vSmart and vBond controllers

### Step 3: Submit and sign the certificate signing requests

Next, the CSRs will be submitted to the Certificate Authority to be signed. This needs to be done for each controller.

1. Go to the Certificate portal at: <https://software.cisco.com> and login if prompted
2. Click Plug and Play Connect under the Network Plug and Play section
3. Ensure the correct Virtual Account is chosen in the upper right-hand corner. This is the Virtual Account with the controller profile of the organization name used for the SD-WAN overlay
4. Click Certificates
5. Click the Generate Certificate button. The Generate Certificate window is displayed
6. Next to Certificate Name, enter a name for the certificate (VMANAGE) 7. Next to Certificate Signing Request, paste the CSR copied from the vManage GUI. Be certain to include the “---BEGIN CERTIFICATE REQUEST---” and “---END CERTIFICATE REQUEST---” wording.

- Next to Validity Period, choose a timeframe for how long you want the certificate to be valid. Minimum is 1 month, and maximum is 2 years.
- Optionally, next to Description, type a description of the certificate (Certificate for vManage)
- Click the Next button

Plug and Play Connect [Feedback](#) [Support](#) [Help](#)

[Devices](#) | [Controller Profiles](#) | [Network](#) | **[Certificates](#)** | [Manage External Virtual Account](#) | [Event Log](#) | [Transactions](#)

---

Generate Certificate

STEP **1**

Identify Certificate

STEP **2**

Review & Submit

STEP **3**

Results

---

**Identify Certificate**  
Enter Certificate details and click Next to proceed to the next step

* Certificate Name	VMANAGE
* Certificate Signing Request	<pre>-----BEGIN CERTIFICATE REQUEST----- MIIDUzCCAIsCAQAwgdlxGzAJBgNVBAYTAiVTRMRwEQYDVOQIEwpDYWxpZm9ybmhl MREwDwYDVOQHewhTYW4gSm9zZTEcMBoGA1UECxMTVkfJUU0atU0RXQU4tTEFCLUFX UzEUMBIGA1UEChMLVmlwdGVsYSBMTEMxQzBBBqNVBAMTOnZiYW5hZm9yZm9yZm9y ZGUUMGJmNi00NGRkLTg0MDUyZjFjNDc4OTg4OGU1LTEudmlwdGVsYS5jb20xIAG BqkhhkiG9w0BCQEW3N1cHBvcnRAdmldGVsYS5jb20wggEIMA0GCsGSIb3DQEB AQUAA4IBDwAwggEKAoIBAQDyU/+WXMhoUyzamb0ZyJUBLkGlrBhUTApAvOluF/ 45M2CkDdyJX+bU9vmkZGRj6Ao/RigMJMORHafQ/b61x3T0FfnV309tb7M+wWApt Rv7+wtBH6olGGiww5oSkBWP9qSk+Ez6La0D++6CIKDUYTBAGw5BWHFJaCk+Lseh 1pGM8ZxWIKVSAztlSFTfcl.FITIKnGdQQQBdk2TLyxZbhEujElixSw2TM25H9Fp3 -----</pre>
* Validity Period	One Year
Type	SD-WAN
Description	Max characters not to exceed 255

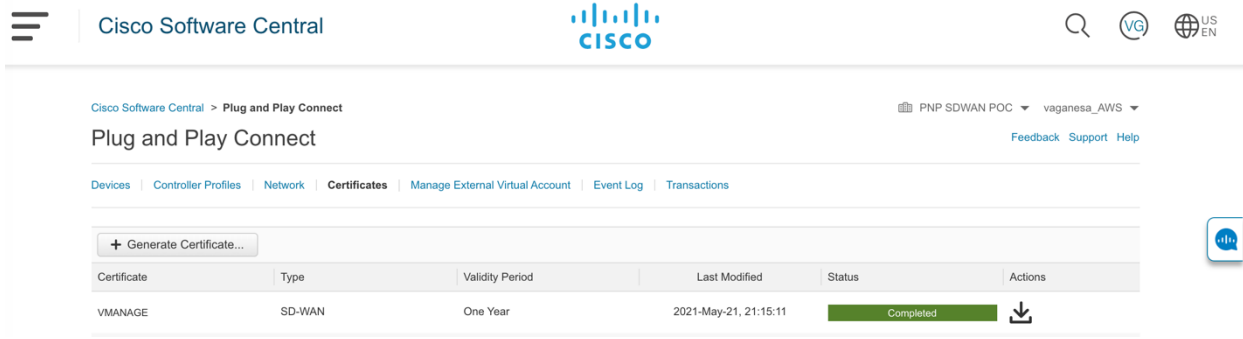
Cancel
Next

10. On the next screen, review and click Submit

11. A message will indicate that a certificate was successfully requested. Click Done

12. When the processing is complete, the status will show as Completed. Refresh the page if required

13. To the right under the Actions column, click the down arrow to download the certificate

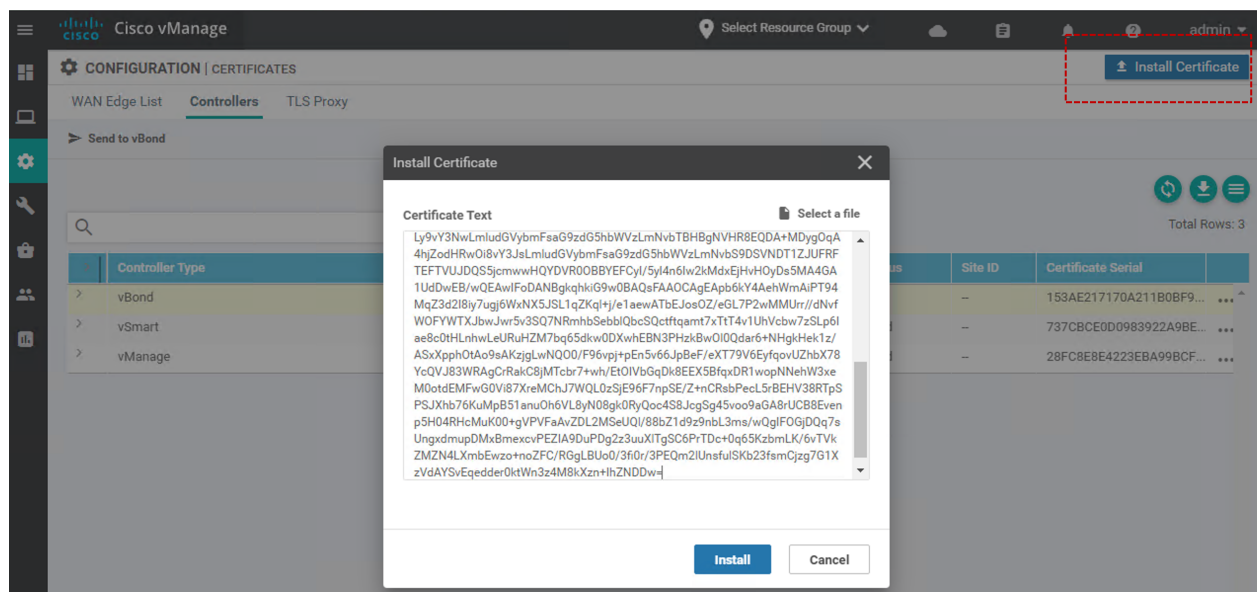


14.Repeat Step 3 for the vBond and vSmart controllers

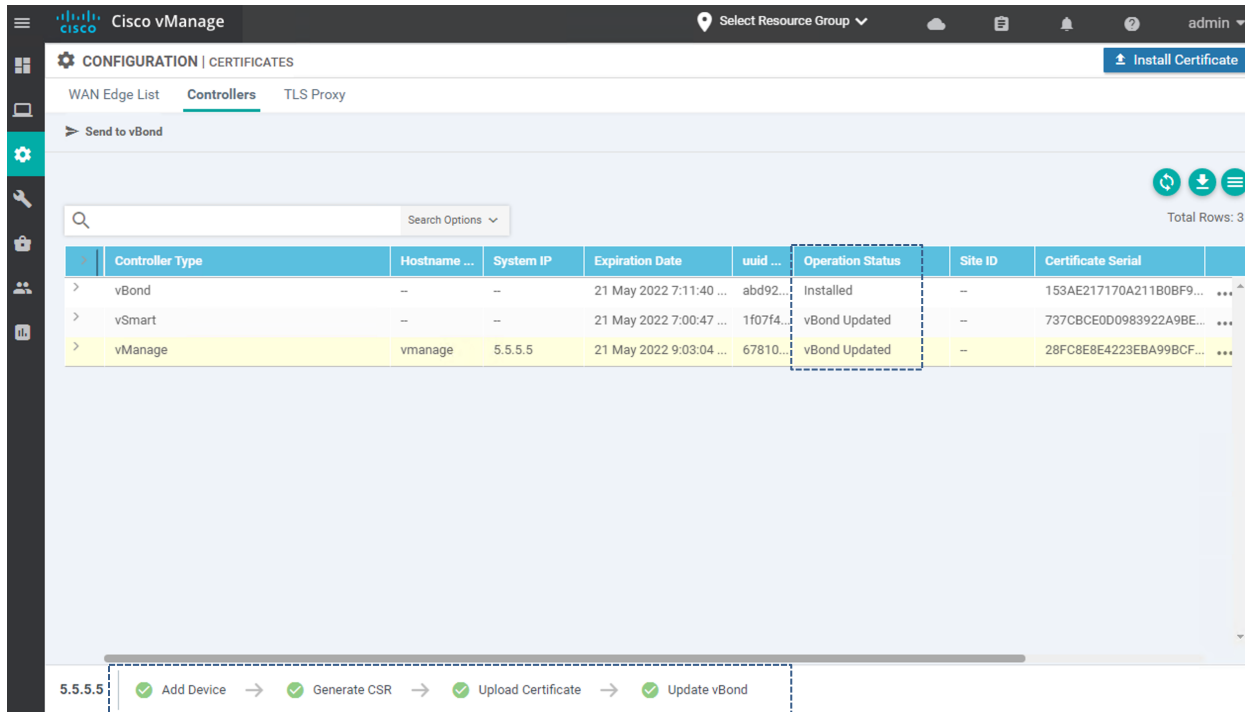
Step 4: Install the signed certificates

Signed certificates are downloaded directly from the Plug and Play Connect portal in the previous procedure. The resulting certificates are uploaded and installed manually in vManage.

1. Go to Configuration > Certificates and click the Controllers tab
2. In the top right of the screen, click the Install Certificate button. No specific controller needs to be selected. vManage applies them to the proper controller
3. Paste the contents of the certificate into the window or click Select a file and choose the certificate to upload. Note that vManage looks for a .pem file, but the certificate may have been downloaded with a .cer extension instead. The difference in extension names does not cause any issues



4. Click Install to get the certificate installed



5. Repeat the procedure for all the additional controllers

## Verification:

1. Go to the vManage dashboard. You should now see vSmart, vBond, and vManage icons with a green up arrow. This indicates that the control connections from the vManage to the other controllers are up. The Control Status box indicates the control connection of the vManage to the vSmart. Control connections cannot be completed without valid certificates. Any warnings or invalid certificates associated with control connections are also shown on the dashboard.
2. Go to Configuration > Certificates and click the Controllers tab. The Operation Status shows Installed for the vBond and vBond Updated for the remaining controller types
3. Other CLI commands to check certificate details on Cisco SD-WAN Controllers via SSH connection:
  - show control local-properties
  - show certificate validity
  - show certificate installed
  - show certificate root-ca-cert

**Note:** If you encounter any issues with certificate migration or if control plane/data plane restoration doesn't happen, please reach out to TAC support to create a service window.

---

## Additional Resources:

<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-controller-cert-deploy-guide.html>

### Americas Headquarters

Cisco Systems, Inc.  
San Jose, CA

### Asia Pacific Headquarters

Cisco Systems (USA) Pte. Ltd.  
Singapore

### Europe Headquarters

Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)