

Enable SD-WAN Controllers Certificate Renewal via Manual Method

Contents

[Introduction](#)

[Available Methods](#)

[Requirements](#)

[Renewal Process](#)

[Cisco \(Recommended\)](#)

[Manual \(PnP\)](#)

[Common Problems](#)

[Time Mismatch](#)

[Not Able to Establish Connection](#)

Introduction

This document describes the steps to renew the SD-WAN certificate on the controllers through the Cisco or Manual method.

Available Methods

There are four different options available for the **Controller Certificate Authorization**.

- **Cisco (Recommended)** - Semi-automated process that uses the **Cisco Plug and play (PnP)** portal to sign the **CSR** generated by the vManage and automatically download and install them.
- **Manual** - Manual certificate sign through Cisco PnP.
- **Symantec** - Manual third-party certificate sign through Symantec/Digicert.
- **Enterprise Root Certificate** - Manual certificate sign through a private Root Certificate Authority (CA).

This document describes only the steps for the **Cisco (Recommended)** and **Manual** methods.

Caution: The certificates cover by this document are not related to the **Web Certificate** for vManage.

Requirements

- A PC/Laptop.
- A **Netadmin** account for the vManage GUI and for for each controller (vManage, vSmart, and vBond).
- Access to the **CA Server**.
- For **Cisco (recommended)** or **Manual**, a valid **account/password** for the PnP Portal.
- For **Cisco (recommended)**, the vManage must have internet access.
- All the Controllers need a valid NTP server and/or all of them need to have the correct date and time.

- Communication between the vBond and vSmart to the vManage.

Note: The certificate install in the vManage would not impact your control plane or data plane. For the certificate in the vSmart, the control connections can be affected. The control plane continue to work due to the OMP graceful timer. In order to perform a certificate change, you must schedule a maintenance window for the activity.

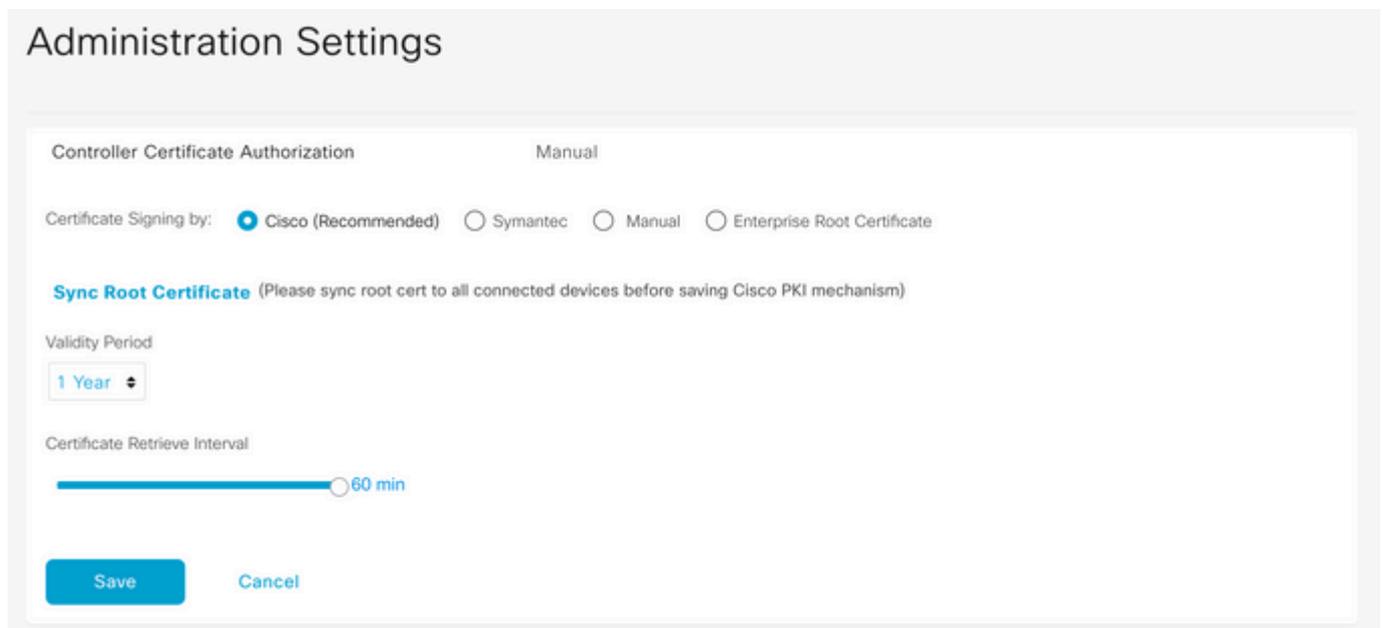
Renewal Process

This is a high-level procedure:

1. Identify the **Controller Certificate Authorization** option in use in the vManage GUI.
2. Generate a new **CSR** through the vManage GUI.
3. Create a new **Certificate**.
4. Download the **Certificate**.
5. Install the **Certificate**.

Cisco (Recommended)

1. Navigate to the **vManage > Administration > Settings > Certificate Authority Server**.
 - Verify the correct option is selected.
 - Select the duration of the certificate.



The screenshot shows the 'Administration Settings' page for 'Certificate Authority Server'. The 'Controller Certificate Authorization' is set to 'Manual'. Under 'Certificate Signing by', 'Cisco (Recommended)' is selected with a radio button. Below this, there is a 'Sync Root Certificate' section with a note: '(Please sync root cert to all connected devices before saving Cisco PKI mechanism)'. The 'Validity Period' is set to '1 Year' in a dropdown menu. The 'Certificate Retrieve Interval' is shown as a slider set to '60 min'. At the bottom, there are 'Save' and 'Cancel' buttons.

2. Scroll down to **Smart Account Credentials** and introduce valid **User/Password**. The credentials must have access to the Smart Account where the SD-WAN overlay is configured, as shown in the image.

Administration Settings

Smart Account Credentials

Username

egarcial@cisco.com

Password

.....

Save

Cancel

3. Navigate to **vManage > Configuration > Certificates > Controllers**.

- Select the ellipsis (...) on the controller (vBond, vSmart or vManage).
- Select **Generate CSR**.

WAN Edge List

Controllers

TLS Proxy

Send to vBond

Search

⊕	Operation Status	Controller Type	Hostname	System IP	Site ID	Certificate
⊕	CSR Generated	vBond	--	--	--	No certific
⊕	vBond Updated	vSmart	vSmart_206_egarcial	10.10.10.3	1	150FB2DD
⊕	vBond Updated	vManage	vmanage_206_egar...	10.10.10.1	1	70783C76

4. Five to twenty minutes is required for the process to finish.

Verify the installation was correct in the GUI **vManage > Configuration > Certificates > Controllers**.

WAN Edge List

Controllers

TLS Proxy

Send to vBond

Search

+	Controller Type	Hostname	System IP	Expiration Date	uuid	Oper
+	vBond	vBond_206_egarcial	10.10.10.2	25 Dec 2024 2:00:42 PM CST	96f5b...	Insta
+	vSmart	vSmart_206_egarcial	10.10.10.3	20 Dec 2024 3:18:21 PM CST	f0269...	vBon
+	vManage	vmanage_206_egar...	10.10.10.1	20 Dec 2024 3:01:02 PM CST	1f585...	vBon

Manual (PnP)

1. Navigate to the **vManage > Administration > Settings > Certificate Authority Server**

- Verify the correct option is selected.

2. Navigate to **vManage > Configuration > Certificates > Controllers**.

- Select the ellipsis (...) on the controller (vBond, vSmart or vManage).
- Select **Generate CSR**.
- Copy and save all the text in a temporarily file.

3. Access the PnP portal, select your SD-WAN overlay, and navigate to certificates, as shown in the image.



Plug and Play Connect

Devices | Controller Profiles | Network | **Certificates** | Manage External Virtual Account | Event Log | Transactions

<input type="checkbox"/>	<input type="text" value=""/>	<input type="text" value="Any"/>	<input type="checkbox"/>	<input type="text" value="VBOND-LAB-MX"/>
<input type="checkbox"/>	Profile Name	Controller Type	Default	Description
<input type="checkbox"/>	VBOND-LAB-MX	VBOND	<input checked="" type="checkbox"/>	VBOND-LAB-MX

4. In the **Certificates** section, click **Generate a new certificate** and enter all the information.

- On **Certificate Signing Request**, enter the **CSR** generated on step 2.

Plug and Play Connect

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	VBOND-2022-DEC
* Certificate Signing Request	ggEKAolBAQCk7hIAfeJB+u4PfLeru5adulhrGNeLWoNmPfQ47PEpSyJ8Aw466z+5 XX rHFZ2W8qrgu1i9f9c3eWQgQE4j4s6TNWqqhIWda8btVkkefo+4M6UW+hQbuJkk XX mFgeolVugR28pHq2yksVSaEKmy21ZGZcXsMMckcuHu0Tdx63/dsk68ZnDLJngexa XX iBw9Pmu3h7bvqE1UValzoAhaSMgft+OBAAEqTQ2G/EuWcGK2W0cVmOSh1V5+7j/ XX FE4VLW9j6dXIWehPqeJtcN+xk2/k25qQZmp/gGhp -----END CERTIFICATE REQUEST-----
* Validity Period	Two Years
Type	SD-WAN
Description	Max characters not to exceed 255

5. Click on **Submit** and **Done**.

Plug and Play Connect

[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

Review & Submit

Certificate Name	Type	Description
VBOND-2022-DEC	SD-WAN	--

[Cancel](#) [Back](#)

Plug and Play Connect

[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

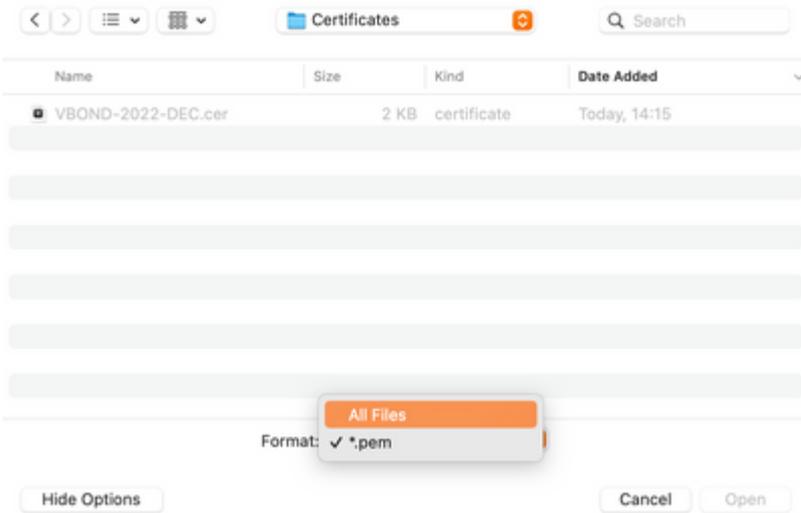
Attempted to generate 1 Certificate

✓ **Successfully requested for 1 Certificate !**
It may take a few minutes to process your request. Please check the request status on Certificates tab.

6. After few minutes, the certificate its ready to download.

- Download the certificate file
- Access the vManage GUI
- Select install certificate under **vManage > Certificate > Controllers.**
- Select the certificate in the pop window.

Note If you are not able see or select the certificate, ensure to choose **All files** under format option. If the format box is not visible, use a different web browser.



Install Certificate

Certificate Text Select a File

```
MIIFpzCCA4+gAwIBAgIUtbYIXWBzQ75WYFvDABMcURHTblowDQY
JKoZihvcNAQELBQAwoJEOmAwGA1UECgwFQ2lzY28xEDA0BgNVB
AsMB0FsYmlyZW8xZjAUBG9vBAMMDVZpcHRlbGEgU3ViQ0EwHhc
NMjIxMjI2MjAwMDQyWWhcNMjQxMjI1MjAwMDQyWjCBTELMAkGA1
UEBhMCMVVMxEzARBgNVBAGMCKNhbGlm3JuaWEeETAPBgNVBAC
MCFNhb3NIMRwwGgYDVQQKDBNDaXNjbyBTTeXN0ZW1zLCBjBj
mMuMRUwEwYDVQQLDAXTRC1XQU4tNzZMxMzMQTA/BgNVBAMM
OHZib25kLTk2ZjViNjVILTQ1MzctNDA5ZC05YTk2LWJiNDZmYjdiYzA
yYy0zLnZpcHRlbGEuY29tMlIBjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEApO4SAH3iQfruD3y3q7uWnblaxjXi1qDZj300OzxKUs
ifAMOOus
/uaEkIOxrjuMTrNiv9le0qwLZom4DUhrRxMQzNfh2kuwOVen3RUPshv
KF5yX0G3/8TqxxWdlvKuq4LtYvX
/XN3ljoEBOI+LOkzVqqoSfg2vG7VZJHn6PuDOIFvoUG7iZJK01B40y0
```

Install

Cancel

7. The certificate is now installed.

Install Certificate

Initi

Total Task: 1 | Success : 1

🔍 Search

+	Status	Message	Device Type	Device ID	System IP
+	✔ Success	Successfully synced vE...	vBond	96f5b65b-4537-409d...	--

Common Problems

Time Mismatch

Cisco Cloud hosted controllers have a NTP server configured.

If the NTP is not present due to a configuration change, the controllers can have different times and this can interfere with the certificate installation or CSR generation.

Ensure that the controllers have the same time.

Not Able to Establish Connection

The SD-WAN controllers must be reachable via the interface configured under VPN0.

Verify that there is Layer 3 and Layer 4 communication.

We can check the logs of the controller via console for more details about the problem.