Table of Contents

About This Guide ......................................................................................................................... 4
Introduction ........................................................................................................................................ 6
About The Solution ............................................................................................................................. 6
Define ................................................................................................................................................ 9
Audience ............................................................................................................................................ 9
Overview .......................................................................................................................................... 9
Design ............................................................................................................................................... 10
Certificates ........................................................................................................................................ 10
Choosing a Method ............................................................................................................................ 12
Control Plane Whitelisting ............................................................................................................... 13
Controller Whitelist .......................................................................................................................... 13
WAN Edge Authorized Serial Whitelist .............................................................................................. 14
Prerequisites: ..................................................................................................................................... 15
Certificates .......................................................................................................................................... 15
Whitelist ........................................................................................................................................... 16
Deploy .............................................................................................................................................. 17
Architecture ....................................................................................................................................... 17
Example Topology ............................................................................................................................. 17
Process 1: Deploying Controller Certificates ..................................................................................... 17
Overview ........................................................................................................................................... 17
Procedure 1: Verify and configure the organization name ............................................................... 18
Procedure 2: Ensure that NETCONF and SSH are allowed on the controller VPN 0 interface .... 18
Option 1: Automated third-party certificate signing through Symantec/Digicert .............................. 19
Procedure 1: Verify Symantec server reachability .......................................................................... 19
Procedure 2: Configure vManage certificate settings ...................................................................... 19
Procedure 3: Generate certificate signing requests ......................................................................... 20
Procedure 4: Sign and install certificate signing requests ................................................................. 21
Option 2: Manual third-party certificate signing through Symantec/Digicert .................................... 21
Procedure 1: Configure vManage certificate settings ...................................................................... 22
Procedure 2: Generate Certificate Signing Requests ....................................................................... 22
Procedure 3: Submit the certificate signing requests ....................................................................... 23
Procedure 4: Sign certificate signing requests ................................................................................ 24
Procedure 5: Install the signed certificates .................................................................................... 24
Option 3: Automated certificate signing through Cisco Systems .................................................... 25
Procedure 1: Verify Cisco server reachability ................................................................................ 25
Procedure 2: Configure Smart Account credentials ....................................................................... 25
Appendix C: Plug and Play (PnP) Connect Portal

Appendix B

Operate

Procedure 3: Add WAN Edge devices to the portal ................................................. 26
Procedure 4: Create the Root CA ............................................................................. 28
Procedure 2: Set up the Root Certificate Authority ....................................................... 29
Procedure 1: Retrieve the authorized WAN Edge serial number file from the PnP Connect Portal ................................................................. 31
Procedure 4: Install the signed certificates ................................................................. 32
Procedure 5: Manual certificate signing through Cisco Systems .................................. 33
Procedure 1: Configure vManage certificate settings .................................................. 34
Procedure 2: Generate certificate signing requests ....................................................... 35
Procedure 3: Submit and sign the certificate signing requests ...................................... 37
Procedure 4: Install the signed certificates ................................................................. 38
Procedure 2: Deploying the WAN Edge Authorized Serial Whitelist .......................... 39
Option 1: Manual upload ......................................................................................... 40
Procedure 1: Retrieve the root certificate from your CA server .................................. 41
Procedure 1: Configure vManage certificate settings and install the root certificate chain ........................................................................................................ 42
Procedure 2: Generate certificate signing requests ....................................................... 43
Procedure 3: Submit and sign the certificate signing requests ...................................... 44
Procedure 4: Install the signed certificates ................................................................. 45
Process 2: Deploying the WAN Edge Authorized Serial Whitelist .......................... 46
Option 1: Manual upload ......................................................................................... 47
Procedure 1: Retrieve the authorized WAN Edge serial number file from the PnP Connect Portal ................................................................. 49
Procedure 2: Load the authorized WAN Edge serial number file manually .................. 50
Option 2: Automatically sync to the PnP Connect portal from vManage .................... 52
Operate ..................................................................................................................... 53
Controller certificate status ......................................................................................... 54
WAN Edge Device Certificate Status ......................................................................... 55
Invalidate a controller certificate .................................................................................. 56
Renew controller certificates ....................................................................................... 57
Manual Loading of Root Certificates (WAN Edge Routers) ...................................... 58
Migration to Cisco PKI Certificates .......................................................................... 60
Appendix A—Hardware and software used for validation ........................................... 61
Appendix B—Windows OpenSSL Certificate Authority (CA) ...................................... 62
Procedure 1: Install OpenSSL .................................................................................. 63
Procedure 2: Set up the Root Certificate Authority ................................................... 64
Procedure 3: Set up the Subordinate Certificate Authority (Sub CA) ......................... 65
Procedure 4: Create the Root CA certificate chain ....................................................... 66
Appendix C: Plug and Play (PnP) Connect Portal ......................................................... 67
Procedure 1: Log into the PnP Connect portal ......................................................... 68
Procedure 2: Configure the controller file ................................................................. 69
Procedure 3: Add WAN Edge devices to the portal ................................................... 70
About this guide ........................................................................................................ 71


About This Guide

This document provides technical guidance on the steps needed to successfully install certificates on the Cisco SD-WAN controllers or in a Cisco-hosted or provider-hosted cloud solution. It includes different methods for obtaining signed controller certificates and how to configure and load the serial authorization whitelist file. The certificate renewal process is also covered.

This guide assumes that the controllers are already deployed and integrated into vManage. See the Cisco SD-WAN Design Guide for background information.

This document contains five major sections:

- The Introduction section discusses background information on the solution.
• The **Define** section defines the audience and gives an overview of the deployment guide.
• The **Design** section discusses the solution components, design aspects, and any prerequisites.
• The **Deploy** section provides information about various configurations and best practices.
• The **Operate** section shows how to manage different aspects of the solution.
There are three distinct types of controllers within the Cisco SD-WAN solution, each responsible for either the orchestration plane, the management plane, or the control plane.

- **Orchestration Plane**: the vBond controller, or vBond orchestrator, is part of the orchestration plane. It authenticates and authorizes devices onto the network and distributes the list of vSmart controllers and vManage to all the WAN Edge routers.

- **Management Plane**: the vManage server is the controller that makes up the management plane. It is a single pane of glass for Day 0, Day 1, and Day 2 operations. It provides centralized provisioning, troubleshooting, and monitoring for the solution.

- **Control Plane**: the vSmart controller is part of the control plane. It disseminates control plane information between routers, implements control plane policies, and distributes data plane policies to the routers.

**Control Connections**

The Cisco SD-WAN vManage and vSmart controllers and the WAN Edge devices initially contact and authenticate to the vBond orchestrator and then subsequently establish and maintain DTLS/TLS connections with other vManage and vSmart controllers. The controllers maintain persistent connections to the vBond as well as the other controllers, while WAN Edge devices drop this connection to the vBond and maintain connections with the vManage and vSmart controllers.

**Whitelist Model**

All WAN Edge devices and controllers mutually authenticate each other using a whitelist model, where the devices have to be authorized before being allowed access onto the network.
There are two authorized whitelists that are distributed by vManage, one for the controllers and one for WAN Edge devices.

- Controller whitelist: The controller whitelist is a result of the administrator adding the controllers manually into the vManage user interface. This list can be distributed from the vManage to all of the controllers and subsequently, from the vBond to the vSmart controllers.

- Whitelist for WAN Edge devices: The digitally-signed, authorized whitelist file for the WAN Edge devices can be retrieved from the Plug and Play Connect portal at http://software.cisco.com. After the whitelist is uploaded or synced to vManage, it is distributed by vManage to all of the controllers.

**Figure 2 WAN Edge and Controllers Whitelist**

Controller Identity

Controller identity is provided by a Symantec/Digicert or Cisco-signed certificate, or alternatively, an Enterprise CA certificate. Each controller in the network must have a certificate signed and installed. In addition, root certificates for the corresponding CA must also be installed for each controller before the controller certificates can be installed. Some root certificates are pre-loaded or automatically installed, and others must be installed by an administrator.

Identity for WAN Edge routers, with the exception of the ASR1002-X, is provided by a root certificate that is pre-loaded in hardware. This root certificate may either be pre-loaded in manufacturing, loaded manually, distributed automatically by vManage, or installed during the PnP or ZTP automatic provisioning process. The identity for Cisco ASR-1002Xs, cloud vEdge routers, ISRv routers, and CSR1000v routers is provided by vManage, which can operate as a CA to generate and install certificates for these devices.

Authentication/Authorization of SD-WAN devices

When the controllers authenticate each other and WAN Edge devices, they generally:

1. Validate the trust for the certificate root Certificate Authority (CA).
2. Compare the organization name of the received certificate OU against the locally configured one.
3. Compare the certificate serial numbers against the authorized whitelist distributed from vManage.

Note: When authenticating the vBond, the vBond certificate serial number is not compared to the authorized whitelist.
When WAN Edge devices authenticate to the controllers, they:

1. Validate the trust for the certificate root Certificate Authority (CA).

2. Compare the organization name of the received certificate OU against the locally configured one.

After authentication and authorization succeeds, a persistent DTLS/TLS connection is established.

The following diagram shows how a vSmart controller authenticates with a vManage server.

**Figure 3 Authentication between a vSmart controller and vManage server**
Define

Audience

This document is for anyone interested in installing and/or renewing Cisco SD-WAN controller certificates, either for production or lab purposes. In addition, it also provides information to create and download or synchronize the serial authorization whitelist file to vManage for authorizing devices on the SD-WAN overlay.

Overview

The following is an overview of the deployment guide:

— Design
  o Certificates
  o Control Plane Whitelisting
    • Controller Whitelist
    • WAN Edge Authorized Serial Whitelist
  o Prerequisites

— Deploy
  o Deploying Controller Certificates
    • Option 1: Automated Third-Party Certificate Signing Through Symantec/Digicert
    • Option 2: Manual Third-Party Certificate Signing Through Symantec/Digicert
    • Option 3: Automated Certificate Signing Through Cisco Systems
    • Option 4: Manual Certificate Signing Through Cisco Systems
    • Option 5: Enterprise Root Certificate Authority (CA)
  o Deploying the WAN Edge Authorized Serial Whitelist
    • Manual Upload
    • Automatically Sync to the PnP Connect Portal from vManage

— Operate
  o Controller Certificate Status
  o WAN Edge Device Certificate Status
  o Invalidate a Controller Certificate
  o Renew Controller Certificates
  o Manual Loading of Root Certificates (WAN Edge Routers)
  o Migration to Cisco PKI Certificates
Certificates

Before controllers can be operational in an SD-WAN overlay network, each controller must have both a root certificate plus a controller certificate that is signed and installed. Root certificates come pre-installed on the controller except when using an Enterprise CA, and in that case, a root certificate needs to be installed before controller certificates can be installed. In the case of controller certificates, a Certificate Signing Request (CSR) is generated for each controller, either when the controller is added to vManage, or initiated by an administrator through the vManage GUI. Each CSR is then submitted and signed and then the signed certificate is retrieved and installed on the respective controller.

There are several different ways to accomplish the controller certificate signing and installation process:

1. **Automated third-party certificate signing through Symantec/Digicert**: With this option, a Certificate Signing Request (CSR) is generated for each controller and it is automatically sent to the Symantec/Digicert server. A Cisco Technical Assistance Center (TAC) case needs to be opened to complete the signing process. After the certificate is signed, vManage automatically retrieves each signed certificate and installs it on the respective controller. Note that the root certificate is installed by default on each controller.

   ![Figure 4 Automated certificate signing using Symantec/Digicert](image)

2. **Manual third-party certificate signing through Symantec/Digicert**: With this option, a CSR is generated for each controller and is copied or downloaded locally. A separate certificate request for each controller is made manually through the Symantec/Digicert web portal using the CSR generated in the previous step. A Cisco TAC case needs to be opened to complete the signing process. Once signed, the signed certificates are delivered to the administrator, typically through email. The administrator uploads each certificate to vManage and vManage then installs it on the respective controller. Note that the root certificate is installed by default on each controller.

   ![Figure 5 Manual certificate signing using Symantec/Digicert](image)
3. **Automated Cisco PKI certificate signing (recommended):** This option requires vManage version 19.1 at a minimum and is very similar to the automated Symantec/Digicert option except that the certificates are signed by the Cisco PKI certificate server and a Cisco TAC case does not need to be opened to complete the signing process. A CSR is generated for each controller and is automatically sent to the Cisco PKI certificate server. After the signing is complete, the vManage automatically retrieves each signed certificate and installs it on the respective controller. Note that the root certificate is installed by default on each controller.

![Diagram of Automated certificate signing using Cisco PKI](image)

Figure 6 Automated certificate signing using Cisco PKI

4. **Manual Cisco PKI certificate signing:** This option requires vManage version 19.1 and is very similar to the manual Symantec/Digicert option except that the certificates are signed by the Cisco PKI certificate server and a Cisco TAC case does not need to be opened to complete the signing process. A CSR is generated for each controller and is copied or downloaded locally. A separate certificate request for each controller is made manually through the **Plug and Play Connect > Certificates** portal at [https://software.cisco.com](https://software.cisco.com), using the CSR generated in the previous step. After the signing is complete, the certificates can be downloaded by the administrator and each certificate is then uploaded to vManage. vManage installs each certificate on the respective controller. Note that the root certificate is installed by default on each controller.
5. **Enterprise Root Certificate Authority (CA):** Customers can use their own CA servers to sign controller certificates. This method is similar to the manual Cisco PKI certificate signing method as automatic enrollment using Simple Certificate Enrollment Protocol (SCEP) to an Enterprise CA is not supported. In addition, as a first step, the Enterprise CA root certificate is installed on vManage, which can automatically distribute the root certificate to the other controllers. Once a root certificate is installed, a CSR is generated for each controller and is either copied or downloaded locally. Separate certificate requests are made for each controller to the Enterprise Root CA, submitting the CSR generated in the previous step. Once signed, the generated certificates can be uploaded to vManage by the administrator. vManage will install each certificate on the respective controller.

Figure 8 Manual certificate signing using Enterprise CA

Choosing a Method

The recommended method is the automated Cisco PKI certificate signing method (option 3), which is supported starting from vManage version 19.1 (version 19.2 or higher is recommended). This method simplifies the process as it requires a single step, which is CSR generation initiated from an administrator. If vManage has no Internet access, the manual Cisco PKI method can be used instead (option 4). Note that when using the Cisco PKI method, you need to ensure that the WAN
Edge devices have a Cisco root certificate installed. If this certificate is not loaded, authentication will fail and the WAN Edge device will not be able to brought up onto the overlay. The easiest way to accomplish this for an existing SD-WAN network is through a Symantec/Digicert to Cisco PKI certificate migration. See the Operate section for details. For new deployments already on Cisco PKI certificates, Cisco root certificates can be loaded manually or obtained through automated provisioning (PnP/ZTP) if these certificates are not preinstalled.

If you are running a vManage version less than 19.1 or you are trying to integrate into an overlay already using Symantec/Digicert certificates, then the recommendation is to use the automated Symantec/Digicert method (option 1), or if there is no Internet access for vManage, use the manual Symactec/Digicert method instead (option 2). Note that Symantec/Digicert root certificates come preinstalled on most WAN Edge devices in manufacturing so in most cases, you should not need any extra intervention when deploying.

The Enterprise CA is an option for those who require it (option 5). This option requires the Enterprise root certificate to be installed on WAN Edge devices, either manually or through automated provisioning (PnP/ZTP).

**Control Plane Whitelisting**

All WAN Edge devices and controllers need to be known and authorized before allowing access to the network. This is accomplished through two authorized whitelists that are distributed through vManage - one for the controllers and one for WAN Edge devices.

**Controller Whitelist**

When the controllers are authenticated to each other, part of the check is to ensure that the certificate serial number of the controller they are trying to authenticate with is listed in the authorized whitelist that is distributed from vManage. Only the vBond controller is not checked against the authorized list, but controller devices are configured with the vBond IP address or domain name and it is the first controller they authenticate to. This list, which includes the certificate serial numbers of each controller, is automatically created and sent to the controllers when controller devices are added into the vManage GUI. The list is also distributed by the vBond as connections are established.

---

**Figure 9 Controller Whitelisting**
WAN Edge Authorized Serial Whitelist

When the controllers authenticate to the WAN Edge routers, part of the check is for the controllers to ensure the certificate serial number of the WAN Edge router they are trying to authenticate with is listed in the WAN Edge Authorized Serial Whitelist that is distributed from vManage. This list, which includes the certificate serial numbers of each WAN Edge device can be retrieved from the Plug and Play (PnP) Connect portal at [http://software.cisco.com](http://software.cisco.com). The WAN Edge routers are associated with a Smart Account (SA) and Virtual Account (VA) at the time of ordering. The device information is automatically transferred to the PnP portal. In addition, the list can be modified by the administrator for any devices not already listed. The administrator can have vManage synchronize to the portal to retrieve this information, or the administrator can download the list manually and upload it to vManage.

**Figure 10  WAN Edge Authorized Serial Whitelist Upload Process**

![Diagram showing the process of uploading the whitelist](image-url)
Prerequisites:

Certificates

Prerequisites for the certificate installation process will depend on which method you use. Some general prerequisites that apply to all methods:

• Before a Certificate Signing Request can be generated, the organization name needs to be defined in the vManage GUI under Administration>Settings>Organization Name. The organization name is included in the certificate and is checked during the controller authentication process.

• If no DTLS/TLS connections are up yet between the controllers, ensure that both NETCONF and SSH are allowed on the VPN 0 tunnel interface and that the appropriate ports are open on any firewalls between controllers, or certificate installation may fail. vManage uses NETCONF (TCP 830) to communicate to the controllers, so communication will be unencrypted if there is no DTLS/TLS connection yet formed between them. vManage cannot generate CSRs for the other controllers without TCP port 830 open. In addition, SSH (TCP 22) also needs to be permitted because SCP (which uses SSH) is used to load certificates on the controllers.

There are additional prerequisites that need to be considered depending on the method:

Symantec/Digicert

• Any certificate installation involving Symantec/Digicert requires a Cisco TAC case to be opened to complete the signing request, regardless of whether you choose the automated or manual process.

• For the automated process, vManage must be able to reach the Symantec/Digicert certificate server. The vManage will need a DNS server configured on the Command Line Interface (CLI) in VPN 0 to resolve the domain name, certmanager-webservers.websecurity.symantec.com (which is associated with CNAME certmanager.blu.websecurity.symauth.net). The vManage will need to reach this website on port 443.

Cisco PKI

• This method requires vManage version 19.1 or higher (version 19.2 or higher is recommended).

• You will need a Smart Account and Virtual Account at http://software.cisco.com to use the automated or manual method. You can manually generate certificates at http://software.cisco.com in the PnP Connect portal under the Certificates tab. It is important that the Virtual Account has a controller profile defined, and the organization name in the profile must match the organization name in the vManage GUI. For the automated method, the Smart Account credentials should be configured in the vManage GUI under Administration>Settings>Smart Account Credentials.

• When using the automated method, vManage needs to reach the Cisco certificate server. The vManage will need a DNS server configured on the CLI in VPN 0 to resolve first the domain name, cloudsso.cisco.com, followed by the domain name, apx.cisco.com. The vManage reaches both of these sites on TCP port 443.

• For an existing SD-WAN network, 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 existing SD-WAN networks running Symantec/Digicert certificates, you can do this automatically through vManage by upgrading to vManage 19.1 or higher and then migrating to Cisco PKI (For more information, see the Operate section). You can also load them manually or through automated provisioning (PnP/ZTP).
Enterprise CA

- For the other certificate methods, the root CA chain is already pre-installed on the controllers. Before generating requests and installing signed certificates, the Enterprise Root CA method requires that a full root CA chain certificate gets installed on all of the controllers.

  Note: If you are on version prior to vManage 18.3, the root CA chain certificate needs to be installed manually through CLI on each controller.

- Ensure that enterprise root certificates are loaded on the WAN Edge devices, either manually or through automated provisioning (PnP/ZTP).

Whitelist

The controller whitelist is generated and distributed automatically when controllers are added by the administrator into vManage, so just the WAN Edge Authorized Serial Whitelist is covered in the remaining section. Prerequisites for installing the WAN Edge Authorized Serial Whitelist include the following:

- A Smart Account and Virtual Account at [http://software.cisco.com](http://software.cisco.com) is required in order to use either the automated or manual method.

- A controller profile needs to be created in the PnP portal. This may or may not already be done for you. If it is not present, you will be required to create one. Using the controller profile you can download the whitelist, also called the provisioning file.

- When using the automated method, vManage needs to reach the PnP cloud service. The vManage will need a DNS server configured on the CLI in VPN 0 to resolve first the domain name, cloudsso.cisco.com, followed by the domain name, apx.cisco.com. The vManage reaches both of these sites on port 443.

- If you are using the automated method, configure the Smart account credentials. This can be initially configured in the vManage GUI by going to Configuration>Devices and under the WAN Edge List tab, click Sync Smart Account.

Note: You can upload and sync multiple lists to vManage, and the duplicates should be removed. This could be needed if you have an older vEdge authorized serial list that did not get moved to the PnP portal.
Deploy

Architecture

Example Topology

The following example topology is used in this deployment guide, although there are many different options available. The example topology consists of one vManage, vBond, and vSmart. All controllers are configured with a public IP address and all controllers have access to the internet.

Process 1: Deploying Controller Certificates

Technical tip: Note that the CA/Browser (CAB) Forum has taken progressive steps and dropped the Maximum Certificate Lifetime to 825 days (27 months) in 2018. This means that the certificate validity can only be set to one or two years when generating CSRs and submitting certificate requests.

Overview

Installing certificates involve various steps and are covered in detail later in this section. The summary of steps are as follows::

1. **Prerequisites**: Ensure that NETCONF and SSH are allowed on the controller interface tunnels if DTLS/TLS connections are not established yet. Configure the organization name in the vManage GUI, and depending on the method, validate your server connectivity, configure Smart Account credentials, and/or ensure a DNS server is configured in vManage for VPN 0.

2. **Configure vManage certificate settings**: Set the certificate method in the vManage GUI under Administration>Settings>Controller Certificate Authorization.
3. **Install the full root CA certificate chain**: This needs to be done only for the Enterprise CA method, as for the other methods, the root certificate is already pre-installed.

4. **Generate certificate signing requests**: Generate certificate signing requests for each controller using the vManage GUI by navigating to the **Controllers** tab under **Configuration>Certificates**.

5. **Submit certificate signing requests**: This may be done automatically or manually, depending on the method.

6. **Sign certificate signing requests**: Depending on the method, this may be done automatically, or it may require a Cisco TAC case to be opened to complete the signing and approval process.

7. **Receive the signed certificates**: This may be done automatically by vManage, or can be manually downloaded.

8. **Install the signed certificates**: The signed certificates are installed on the controllers, either automatically or manually, depending on the method.

The following describes the detailed steps needed to deploy controller certificates.

**Procedure 1: Verify and configure the organization name**

The organization name must be configured in the vManage GUI before certificate signing requests can be made. This may have been automatically configured and synchronized from the vManage CLI during setup, or may have been configured earlier in the controller deployment process.

1. In the vManage GUI, go to **Administration>Settings**. Next to **Organization Name** verify the settings. If the organization name needs to be configured, click **Edit**. Type in the **Organization Name** (**ENB-Solutions – 21615**, for example), then type the name again to confirm. The name is case-sensitive and must match exactly, including any characters.

![Organization Name](image)

**Procedure 2: Ensure that NETCONF and SSH are allowed on the controller VPN 0 interface**

Both NETCONF and SSH must be permitted on the VPN 0 interface tunnels on the vBond and vSmart controllers for certificate installation. If there are no tunnels configured on the controllers, then all protocols will be permitted. If tunnels are configured on the VPN 0 interface, then verify that NETCONF and SSH are both allowed:

1. **SSH or console to the vBond controller**

2. Issue a **show running-config**. If NETCONF or SSH are not both allowed as a service, configure them to be allowed:

   ```
   config terminal
   interface ge0/0
   tunnel-interface
   allow-service sshd
   allow-service netconf
   commit-and-quit
   ```
Option 1: Automated third-party certificate signing through Symantec/Digicert

With this option, certificate signing requests get automatically sent to the Symantec signing server, where the certificate is signed. The vManage then automatically retrieves the certificate and installs it. A DNS server must be configured to resolve the hostname, certmanager-webservers.websecurity.symantec.com (which is associated with CNAME certmanager.blu.websecurity.symauth.net). The vManage needs to reach the server on TCP port 443. Note that a Cisco TAC case needs to be opened to complete the signing and install process.

Procedure 1: Verify Symantec server reachability

1. Ensure that a DNS server is defined for VPN 0 on vManage via SSH or console:

```plaintext
config terminal
vpn 0
dns 208.67.222.222 primary
commit and-quit
```

2. To validate if vManage can reach the Symantec server, go to the vManage CLI, type in `vshell`, then type `curl https://certmanager.websecurity.symantec.com/mcelp/enroll/index?jur_hash=f422d7ceb508a24e32ea7de4f78d37f8`.
   If it succeeds, then the automated process should work. Type in `exit` to exit vshell mode. This domain name is also associated with CNAME certmanager.blu.websecurity.symauth.net.

Procedure 2: 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 **Symantec Automated** 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. Fill in the **First Name** and **Last Name**, the user’s **Email** address, and a **Validity Period** for how long the certificates should be valid. Select 1 or 2 years. If you select 3 years, you may get an error when generating a CSR that there is an invalid validity period.

5. To configure a **Challenge Phrase** (for certificate renewal or revocation), click the **Edit Challenge Phrase** checkbox and enter and confirm a challenge phrase.

6. Set the **Certificate Retrieve Interval** (60 min). This is the interval the vManage will check on whether the signed certificates are available after the CSR has been submitted. You may want to decrease this value, as you could be waiting up to an hour after the certificate is signed before it is automatically installed.

7. Click the **Save** button.
Procedure 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 ... and select Generate CSR from the drop-down box.

3. A pop-up window states that the generated CSR has been sent to Symantec for signing.
4. Repeat the process for the vSmart and vBond controllers.

**Procedure 4: Sign and install certificate signing requests**

Open a Cisco TAC case to have the certificates signed and released. To open a Cisco TAC case:

1. Go to [https://mycase.cloudapps.cisco.com/case](https://mycase.cloudapps.cisco.com/case)
2. Choose *Open New Case* and click the *Open Case* button.
3. Enter in the appropriate entitlement info. Select *Next*.
4. Enter in the case details. In the *Description*, ask for the certificate signing requests submitted to be signed and released. Be certain to provide the organization name associated with the SD-WAN overlay.
5. Click on *Manually Select a Technology*. Search for and select *Software Defined Wide Area Networking (SDWAN)*. Select the appropriate area and sub-area (*SD-WAN Cloud Infra (Certificates - Activation/renewals, Analytics, Zprov)*).
6. Under *Problem Area*, select *Installation>Licensing*, then click *Select*.
7. Fill out any contact information and preferences.
8. Click *Submit*.

Once the certificates are approved, the vManage will check at the time interval selected and install them automatically.

---

**Option 2: Manual third-party certificate signing through Symantec/Digicert**

With this option, certificate signing requests are manually submitted by the administrator to the Symantec signing server. A Cisco TAC case is opened in order to complete the signing process. The signed certificates are emailed to the administrator and the administrator installs them in vManage.
Procedure 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 Symantec 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.

   Technical tip: Note that starting in vManage version 19.1, this option is named Manual.

4. Click the Save button.

Procedure 2: 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 ... and select Generate CSR from the drop-down box.
3. A pop-up window appears with the certificate signing request. Download or copy the certificate signing request so it can be submitted for signing.
4. Click Close. You can always view or download the CSR again by clicking ... 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.
Procedure 3: Submit the certificate signing requests

The next step is to submit the CSRs to the Certificate Authority to be signed. This needs to be done for each controller.

1. Go to the Certificate portal at:
   https://certmanager.websecurity.symantec.com/mcelp/enroll/index?jur_hash=f422d7ceb508a24e32ea7de4f78d37f8

2. Under Get a new certificate, ensure Standard Intranet SSL is selected and click Go.

3. Fill in your First Name, Last Name, and Email Address.

4. Under Server platform, choose Apache (or any).

5. Under Certificate Signing Request (CSR), Paste or upload the CSR that was generated in Procedure 2.

6. (Optional) Under Subject Alternative Names (SANs), enter any fully-qualified domain names. This allows you to specify additional hostnames for a single SSL certificate. The default Common Name (CN) for the server is vmanage-[uuid].viptela.com. The CN (along with any Subject Alternative Names) represents the server name protected by the SSL certificate.

   Note that this field must be in domain name format, and you cannot specify a domain name that does not match the organization domain name in the certificate (viptela.com).

7. Under Certificate Signature Algorithm, keep the default (SHA-256 with RSA and SHA-1 root)

8. Under How many servers will use this certificate?, keep the default number of Server Licenses at 1.

9. The Validity Period defaults to 1 Year, and you cannot modify this setting.

10. Under Challenge Phrase, enter and re-enter a password. This is used to renew or revoke your certificate.

11. Click Get Certificate.

12. Click the Back button and repeat Procedure 3 for the vBond and vSmart controllers.
Procedure 4: Sign certificate signing requests

1. Open a Cisco TAC case to have the certificates signed and released. To open a TAC case:
   
   2. Go to https://mycase.cloudapps.cisco.com/case
   
   3. Click Open New Case and click the Open Case button.
   
   4. Enter in the appropriate entitlement info. Click Next.
   
   5. Enter in the case details. In the Description, ask for the certificate signing requests submitted to be signed and released. Be certain that your email address is provided, along with the organization name associated with the SD-WAN overlay.
   
   6. Click on Manually Select a Technology. Search for and select Software Defined Wide Area Networking (SDWAN). Select the appropriate area and sub-area (SD-WAN Cloud Infra (Certificates-Activation/renewals, Analytics, Zprov)).
   
   7. Under Problem Area, select Installation>Licensing, then click Select.
   
   8. Fill out any contact information and preferences.
   
   9. Click Submit.

Procedure 5: Install the signed certificates

Signed certificates typically arrive in email in the form of an attachment. Certificates can either be saved from email and uploaded to vManage, or they can be copied and pasted in.

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. Click Install.
   
   4. Repeat the procedure for the additional controllers.
Option 3: 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 it. A DNS server needs to be configured to resolve the hostname, cloudssso.cisco.com and subsequently, apx.cisco.com. The vManage needs to reach both servers on TCP port 443.

Note that this option requires vManage version 19.1 or higher (19.2 or higher is recommended) and also requires that Smart Account credentials are configured before this certificate option can be configured.

Procedure 1: Verify Cisco server reachability

1. Ensure that a DNS server is defined for VPN 0 on vManage via SSH or console:
   ```
   config terminal
   vpn 0
   dns 208.67.222.222 primary
   commit and-quit
   ```

2. To validate if vManage can reach the Cisco PnP server, go to the vManage CLI, type in vshell, then type “curl https://cloudssso.cisco.com”. You should see a message that the host is live. 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 exit vshell mode.

   ![Example output of the curl command](image)

Procedure 2: Configure Smart Account credentials

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

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.
Procedure 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. Select 1 or 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.

5. Click the Save button.

Procedure 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 ... 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.

Procedure 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](https://software.cisco.com) and login if prompted.

2. Click **Plug and Play Connect** under the **Network Plug and Play** section.

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

Option 4: Manual certificate signing through Cisco Systems

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

Note that this option requires vManage version 19.1 or higher (19.2 or higher is recommended).

Procedure 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.

Procedure 2: 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 ... 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 ... 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.

Procedure 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.

8. Next to Validity Period, choose a timeframe for how long you want the certificate to be valid (One Year).
9. Optionally, next to Description, type a description of the certificate (Certificate for vManage).

10. Click the Next button.

11. On the next screen, review and click Submit.

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

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

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

15. Repeat Procedure 3 for the vBond and vSmart controllers.

**Procedure 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.

*Technical tip:* In the 19.1.0 version of vManage, vManage expects to see uploaded certificates in PEM format, which uses a plain-text header (BEGIN CERTIFICATE) and footer (END CERTIFICATE), but the PnP Connect portal
deploy does not generate the certificates with the BEGIN CERTIFICATE and END CERTIFICATE text. If you install the certificate into vManage without adding the header and footer, you may get an error similar to: System organization [ENB-Solutions – 21615] does not match cert subject’s OU [ ]. To correct this, manually insert “-----BEGIN CERTIFICATE-----” [carriage return] at the beginning of the file, and [carriage return] “-----END CERTIFICATE-----” at the end of the file, save it, then upload this certificate to vManage. Starting in version 19.2, the certificate can be installed without adding delimiters.

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.

5. Repeat the procedure for all the additional controllers.

Option 5: Enterprise Root Certificate Authority (CA)

With this option, an Enterprise-existing CA infrastructure can be leveraged. Certificate signing requests get manually submitted by the administrator to the Enterprise CA, where the certificates are signed. The administrator then receives the resulting certificates and manually installs them in vManage. Note that this option requires a full root certificate chain to be loaded in vManage which is automatically distributed to the other controllers when the vManage certificate setting type is configured to be Enterprise Root Certificate.

Technical tip: The automatic distribution of the root certificate to the other controllers is supported starting in 18.3 vManage code. Before that, the root certificates needed to be installed manually on each controller.

In lab testing, there are some options to create your own CAs. Some examples include Linux-based XCA, TinyCA, or OpenSSL (which is part of all Linux distributions) or Windows (where you can install an Ubuntu shell or OpenSSL).

Some tips to keep in mind when you are using an Enterprise CA:
• When you are generating a root certificate, the organization name—does not need to match the organization name that you use for the SD-WAN overlay.

• Once you have the PKI server configured, you can use it to sign the certificates for the controllers. When you generate the CSR from the vManage server, the organization unit name of the CSR will match the organization name of the SD-WAN overlay. When you perform the signing, it is important that the PKI server does not overwrite the populated fields of the CSR. So accept what is defined in the CSR and confirm issuing of the certificate.

• If you are using subordinate servers, be certain to export, and then import the full root CA chain into vManage, which includes both the root and the subordinate, or intermediate, certificates.

In this deployment, OpenSSL installed on Windows 10 was used. See Appendix B for the setup information.

Procedure 1: Retrieve the root certificate from your CA server

1. In this example, the root CA and sub CA were created using OpenSSL and the steps are shown in Appendix B. The resulting CA root chain certificate was created and named root-ca-chain.pem.

Procedure 1: Configure vManage certificate settings and install the root certificate chain

1. On the vManage GUI, go to Administration>Settings.

2. To the right of Controller Certificate Authorization, Click Edit.

3. Select Enterprise Root Certificate 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. Copy and paste the root certificate chain file (root-ca-chain.pem) into the Certificate box, 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 different extension depending on how it was saved and named on download. The certificate should be in PEM format, which means that each certificate in the file begins with the text “-----BEGIN CERTIFICATE-----” and ends with the text “-----END CERTIFICATE-----”.

5. Click the box next to Set CSR Properties.
6. The **Organization Unit** is already populated (**ENB-Solutions – 21615**, in this example) since this was previously defined under **Administration>Settings>Organization Name**. Fill in the **Domain Name** (**cisco.com**), **Organization** (**ENB**), **City** (**RTP**), **State** (**NC**), **Email** (**username@cisco.com**), **Country Code** (**US**), and **Validity** (2 Years).

7. Click the **Import & Save** button.

After the root certificate is imported, vManage installs the root certificates on the remaining controllers.

To verify root certificate installation, you can issue a **show certificate root-ca-cert | include Subject** on the CLI of the controller.

```
vsmart# show certificate root-ca-cert | include Subject:
Subject: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at https://www.verisign.com/rpa
Subject: C=US, CN=74e2c6b3-6200-4ed7-b695-3c20389aaf8b, O=Vintela
Subject: C=US, ST=NC, L=RTP, O=Cisco Systems Inc, OU=ENB Solutions, CN=enb-subcal.cisco.com
Subject: C=US, ST=NC, L=RTP, O=Cisco Systems Inc, OU=ENB Solutions, CN=enb-cal.cisco.com
```

Note: If you add a new controller to vManage after the root certificate has been distributed by vManage, the root certificate will be distributed to the new controller automatically.
If you are running vManage code prior to 18.3, the root certificate chain needs to be installed manually on all of the controllers.

Technical tip: It is not recommended to install root certificates manually in vManage versions 18.3 and above.

**Procedure 2: Generate certificate signing requests**

Next, generate and submit certificate signing requests.

1. On the vManage GUI, navigate to **Configuration>Certificates** and click the **Controllers** tab

2. On the right side of vManage, click … and select **Generate CSR** from the drop-down box.

3. A pop-up window appears with the certificate signing request. Download or copy the certificate signing request so it can be submitted for signing. In this example, the CSR is downloaded and moved to the C:\OpenSSL-Win64\bin folder so it can be submitted easily to the CA.

   Technical tip: Note that the downloaded file may be automatically downloaded as undefined.csr, so you may want to change the name of the downloaded file before submitting the CSR to the CA.

4. Click **Close**. You can always view or download the CSR again by clicking … 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.

**Procedure 3: Submit and sign the certificate signing requests**

1. Next, the CSRs are submitted to the Certificate Authority to be signed. This needs to be done for each controller. Each CSR is submitted and signed for a validity period of two years. Each resulting certificate has a unique serial number. The resulting certificates are **vmanage.crt**, **vsmart.crt**, and **vbond.crt**. If you are using default path settings for OpenSSL, the certificates will be created in the \bin folder, which in this example is C:\OpenSSL-Win64\bin.

   OpenSSL> x509 -req -days 730 -in vmanage.csr -CA subca.crt -CAkey subca.key -set_serial 02 -out vmanage.crt
   
   Open SSH> x509 -req -days 730 -in vsmart.csr -CA subca.crt -CAkey subca.key -set_serial 03 -out vsmart.crt
   
   OpenSSL> x509 -req -days 730 -in vbond.csr -CA subca.crt -CAkey subca.key -set_serial 04 -out vbond.crt
Procedure 4: Install the signed certificates

Certificate files can be uploaded to vManage, or they can be copied and pasted in.

1. In vManage, 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. Copy and paste or upload the resulting certificate from the previous procedure.
4. Click Install.
5. Repeat the procedure for the additional controllers.

Process 2: Deploying the WAN Edge Authorized Serial Whitelist

In order for the WAN Edge devices to come up and be active in the overlay, you must have a valid authorized serial number file uploaded to vManage. This authorized serial number file lists the serial and chassis numbers for all the WAN Edge routers allowed in the network. The vManage sends this file to the controllers, and only devices that match serial numbers on this list will be validated and authenticated successfully by the controllers.
The legacy authorized serial number files for vEdge routers were once located at the Cisco SD-WAN support website, but these files are now migrated to the Plug and Play (PnP) Connect portal. The authorized serial number file on the PnP Connect portal also contains IOS XE SD-WAN router information. See Appendix C for information on how to create a controller profile or add any WAN Edge devices to the portal if needed before downloading or syncing the authorized serial number file. Note that you can upload multiple authorized serial number files to vManage and the duplicates should be filtered.

There are two ways to load the WAN Edge Authorized Serial Whitelist in vManage, either by manually uploading the serial file or automatically syncing the file.

**Option 1: Manual upload**

The following section details how to retrieve the WAN Edge authorized serial whitelist and how to upload it manually to vManage.

**Procedure 1: Retrieve the authorized WAN Edge serial number file from the PnP Connect Portal**

1. Navigate to [https://software.cisco.com](https://software.cisco.com).
2. Under the **Network Plug and Play** section, click **Plug and Play Connect**.
3. Click on **Controller Profiles**.
4. Select the Smart Account and Virtual Account in the upper right-hand corner that contains the Controller profile which references the proper Cisco SD-WAN overlay Organization Name (**ENB-SOLUTIONS-VBOND**, in this example).
5. Next to the correct controller profile (**ENB-SOLUTIONS-VBOND**), click on the **Provisioning File** text.

![Provisioning File](image)

6. In the pop-up window, select the controller versions from the drop-down box. Choose **18.3 and newer**. Click **Download** and save the file to your computer. It is saved as **serialFile.viptela** by default.

![Download File](image)
Procedure 2: Load the authorized WAN Edge serial number file manually

1. In the vManage GUI, go to **Configuration>Devices** in the left pane, or alternatively, expand the left pane by selecting the three horizontal bars in the top left corner of the GUI, then select **Configuration>Devices**. Ensure the **WAN Edge List** tab is selected.

2. Select the **Upload WAN Edge List** button. A pop-up window appears. Select **Choose File**. Browse and select the serial number file (serialFile.viptela by default). Select **Open**.

3. Now that the file is selected, select the check box in order to validate the list and send it to the controllers. Select the **Upload** button. If you select the check box, this will put all the devices on the list into a valid state, which means they are authorized on the network and can be brought up at any time to start forwarding traffic. If you do not select **Validate**, then all the devices show the status as invalid, and you have to individually change them to valid if you want to bring them up on the network and participate in the overlay.

4. Select **OK** in the confirmation box that appears.

5. A pop-up window appears to inform you that the list uploaded successfully and informs you of the number of WAN Edge routers that were uploaded successfully. Select **OK**. A page will indicate that the list has been successfully pushed out to the vBond and vSmart controllers.
6. If you did not select the check box to validate the uploaded list to send to the controllers, you can go to Configuration>Certificates, ensure the WAN Edge List tab is selected, and select the Send to Controllers button in the top left section of the screen. This will distribute the list of WAN Edge routers to all of the controllers. A page will indicate that the list has been successfully pushed out to the vBond and vSmart controllers. All devices are in an invalid state.

Option 2: Automatically sync to the PnP Connect portal from vManage

Starting from version 18.3, vManage has a Sync Smart Account option, which allows vManage to automatically connect to the PnP Connect portal and download the authorized WAN Edge serial number file.

1. In the vManage GUI, go to Configuration>Devices, and ensure the WAN Edge List tab is selected.

2. Click on Sync Smart Account and a window pops up which prompts you for your Username and Password.

3. Enter your username and password for the https://software.cisco.com website. The checkbox which validates the uploaded list is selected by default. Note that the list still needs to be distributed to the other controllers once synced with vManage even if the checkbox was selected.

4. Click Sync. vManage connects to the Cisco servers and the authorized list is downloaded. Status should indicate Success.
5. Go to **Configuration>Certificates** in vManage to view the uploaded list. The devices should all be in a valid state.

6. Click the **Send to Controllers** button in the top left corner of the GUI in order for all of the controllers to be updated with the valid WAN Edge list. Once completed, the operation should indicate success.
Controller certificate status

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.

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.

Select Tools>SSH Terminal to establish a SSH connection to a device from vManage. Select the device on the left (vsmart) and login with the proper credentials. You can now execute the following commands to check certificate details:

- show control local-properties
- show certificate validity
- show certificate installed
- show certificate root-ca-cert
WAN Edge Device Certificate Status

There are three different states of a WAN Edge certificate:

- **Valid (shown in green):** The certificate is valid and the WAN Edge router can fully participate and forward traffic in the SD-WAN overlay network.

- **Staging (shown in yellow):** The certificate is in staging state and the WAN Edge router can form control connections with the controllers, but it cannot join the overlay and forward traffic until it is in a valid state. More specifically, each WAN Edge router becomes an OMP peer with the vSmart controllers, but no OMP routes will be sent nor will any local routes be redistributed into OMP.

- **Invalid (shown in red):** The certificate is not valid and the WAN Edge router will be barred from forming control connections.

**Technical tip:** When you manually load or sync the WAN authorization serial whitelist, you have the option to validate the list before you complete the upload or sync. If you select validate, all devices will be in the **Valid** state when the list is loaded. If you do not select validate, all devices will be in the **Invalid** state when the list is loaded, and you will need to manually validate each one as the invalid devices cannot form control connections with the controllers.

To check the certificate status:

1. On the vManage GUI, navigate to **Configuration>Certificates**. Ensure the **WAN Edge List** tab is selected. In the **Validate** column you can view the current status of the certificate.

To change the certificate status:

1. From the **Configuration>Certificates>WAN Edge List** page, next to the targeted WAN Edge router, select the desired status (**Staging** for example).

2. A pop-up window will ask if you to confirm. Click **OK**.
3. The **Send to Controllers** text in the top left of the page will be marked in red, indicating that the controllers need to be updated with the modified list. Click **Send to Controllers**.

The updated whitelist is sent to all of the controllers.

To check the WAN Edge authorized serial white list on the controllers, you can execute a `show orchestrator valid-edges` command on the vBond, or a `show control valid-edges` on the vSmart or vManage.

<table>
<thead>
<tr>
<th>CHASSIS NUMBER</th>
<th>SERIAL NUMBER</th>
<th>VALIDITY</th>
<th>ORG</th>
</tr>
</thead>
<tbody>
<tr>
<td>11OG403180391</td>
<td>10007556</td>
<td>valid</td>
<td>ENB-Solutions - 21615</td>
</tr>
<tr>
<td>ISR4351/K9-FDO205108CB</td>
<td>1373974</td>
<td>staging</td>
<td>ENB-Solutions - 21615</td>
</tr>
</tbody>
</table>

Note that when a device certificate is set to **invalid**, the device is removed from the authorized whitelist. Only devices in valid and staging status appear on the whitelist. Control connections are deleted to the invalid devices once the whitelist is updated and distributed to all of the controllers.

When a device’s certificate has been set to invalid and tries to connect to the vBond, you might see the following information on the vBond (partial output):

```
vbond# show orchestrator connections-history
[edited]
```
The command lists a legend for the error codes, and the error code CRTVERFL means the vBond failed to verify the peer certificate. If you run a `show orchestrator valid-vedges` command on the vBond, you can see if the specific WAN Edge device is in the authorized serial file whitelist that was distributed to the controllers.

**Invalidate a controller certificate**

To invalidate a controller certificate:

1. In the vManage GUI, go to **Configuration>Certificates** and click the **Controllers** tab.
2. To the far right of the controller you want to invalidate, click … and choose **Invalidate**.
3. Select OK to confirm the action.
4. The device is removed from vManage and the controller whitelist is updated with the device removed. A `show orchestrator valid-vsmarts` on the vBond (or a `show control valid-vsmarts` from a vSmart or vManage) displays the controller whitelist, that consists of the vSmart and vManage controllers.

The following screenshot shows the controller list before and after a vSmart invalidation:
Renew controller certificates

The controller certificates must be renewed before the expiration date. If a valid certificate is not present in the controller, the control connections will be disabled.

Several months in advance, vManage will indicate on the vManage Dashboard that there are certificate warnings indicating that certificates will expire. The Configuration>Certificates>Controllers tab will indicate the certificate expiration dates marked in yellow or red.
When the Cisco Viptela SDWAN controller certificates are renewed and installed, the control plane will flap briefly, however, there is no impact to the data plane. Although the certificate installation takes only a few minutes, it is recommended to change certificates using a maintenance window time of 1 hour.

If the controllers are Cisco-managed/cloud-hosted, a Cisco TAC case should be opened to initiate the renewal process. The Technical Assistance Center will engage with CloudOps, and the change is coordinated.

For on-premise controllers or Enterprise CA-based certificates, the renewal process is owned by the customer or SP. The renewal process is the same procedure as the initial deployment of certificates. CSRs are first generated, then signed and received, and then installed. Here is an example of a renewal using the automated Symantec/Digicert method:

1. On the vManage GUI, go to Administration>Settings and next to Controller Certificate Authorization, click Edit.
2. Review the settings for accuracy, then click Save.
3. Go to Configuration>Certificates and click the Controllers tab.
4. To the far right of the vManage controller, select ... and select Generate CSR from the drop-down box. Repeat for each controller.
5. Open a Cisco TAC case to get approval and the vManage automatically retrieves and installs the signed certificates. [https://mycase.cloudapps.cisco.com/case](https://mycase.cloudapps.cisco.com/case)

When transitioning, devices with the new certificates installed will lose connections to the devices with the old certificate. Connections are re-initiated. Once renewed certificates are installed on all controllers, connections will come up fully. Data traffic will continue to run and should not be affected.

---

**Manual Loading of Root Certificates (WAN Edge Routers)**

In the event that root certificates (either Enterprise Root certificates or Cisco Root certificates) need to be manually installed in a WAN Edge router, use the following procedures:
WAN Edge Enterprise Root Certificate

To install an individual Enterprise Root Certificate, which will be installed as the current root certificate chain, do the following.

Note that the root certificate should be pre-loaded onto a server reachable from the WAN Edge router in PEM format.

vEdge router

1. Either copy the PEM-formatted certificate file into the router or paste the certificate into a file.
   a. To copy, use the download command. The file will be installed by default in the /home/admin folder if you are logged in as admin.

   ```
   br3-wel# request download vpn 512 ftp://admin:clsco123@192.168.254.51/ent-root-ca-chain.pem
   => 'ent-root-ca-chain.pem'
   Connecting to 192.168.254.51:21... connected.
   Logging in as admin ... Logged in!
   ==> SYST ... done.  ==> PWD ... done.
   ==> TYPE I ... done.  ==> CWD not needed.
   ==> SIZE ent-root-ca-chain.pem ... 3992
   ==> PASV ... done.  ==> RETR ent-root-ca-chain.pem ... done.
   Length: 3992 (3.9K) (unauthoritative)
   ```

   ```
   ent-root-ca-chain.pem
   100%[======================================] 3.90K
   --.-KB/s in 0s
   ```

   2019-08-07 16:19:40 (68.4 MB/s) - 'ent-root-ca-chain.pem' saved [3992]

   To paste directly into a file:
   a. Enter vshell mode.
   b. Type in "vi" with the name of the file. In this case, vi ent-root-ca-chain.pem.
   c. Type "i", then paste in the certificate (PEM format).
   d. Type ":", then "wq" to save and quit.
   e. Exit out of vshell mode by typing "exit".

2. Install the certificate into the root certificate store by typing request root-cert-chain install <path/certname>.

   ```
   br3-wel# request root-cert-chain install /home/admin/ent-root-ca-chain.pem
   Uploading root-ca-cert-chain via VPN 0
   Copying ... /home/admin/ent-root-ca-chain.pem via VPN 0
   Updating the root certificate chain.
   ```
Successfully installed the root certificate chain

3. To verify, issue show certificate root-ca-cert.

```
br3-wel# show certificate root-ca-cert | inc ENB

Issuer: C=US, ST=NC, L=RTP, O=Cisco Systems Inc, OU=ENB Solutions, CN=enb-cal.cisco.com
Subject: C=US, ST=NC, L=RTP, O=Cisco Systems Inc, OU=ENB Solutions, CN=enb-subca1.cisco.com

Issuer: C=US, ST=NC, L=RTP, O=Cisco Systems Inc, OU=ENB Solutions, CN=enb-cal.cisco.com
Subject: C=US, ST=NC, L=RTP, O=Cisco Systems Inc, OU=ENB Solutions, CN=enb-cal.cisco.com
```

Cisco IOS XE SD-WAN router

The process is similar for the Cisco IOS XE SD-WAN routers.

1. Copy the PEM-formatted certificate file into the router.

```
br2-wel# copy ftp://admin:c1sco123@192.168.254.51/ent-root-ca-chain.pem bootflash: vrf Mgmt-intf
Accessing ftp://*:*@192.168.254.51/ent-root-ca-chain.pem...!
[OK - 3992/4096 bytes]
```

3992 bytes copied in 0.027 secs (147852 bytes/sec)

2. Install the certificate into the root certificate store by typing request platform sdwan root-cert-chain install <path/certname>.

```
br2-wel# request platform software sdwan root-cert-chain install bootflash:ent-root-ca-chain.pem
Uploading root-ca-cert-chain via VPN 0
Copying ... /bootflash/ent-root-ca-chain.pem via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
```

Technical tip: Note that when you try to verify whether a particular root certificate is installed, the show sdwan certificate root-ca-cert command only returns one certificate.

WAN Edge Cisco PKI Root Certificate

This process is identical to the Enterprise Root Certificate deployment in the previous operation.

When you install it, you can verify it on a vEdge router using the show certificate root-ca-cert command.

```
br5-wel# 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

If you do not have a copy of the Cisco root certificates, you can install the entire root certificate chain instead. See the next section for instructions.

WAN Edge Root Certificate Chain

In this section, the entire root certificate chain can be exported from a controller and imported into a WAN Edge router.

1. From a controller, export the root certificate chain to an external server.

   vbond# request upload vpn 512 ftp://admin:c1sco123@192.168.254.51/root-cert-chain.crt master_root.crt
   
   master_root.crt

ENB_vBond_West# vshell
ENB_vBond_West:~$ cp /usr/share/viptela/root-ca.crt /home/admin/root-ca.crt
ENB_vBond_West:~$ exit
exit

vbond# request upload vpn 512 ftp://admin:c1sco123@192.168.254.51/root-ca.crt
root-ca.crt

vEdge router

1. Uninstall the previous root certificate chain.

   br3-we1# request root-cert-chain uninstall
   Successfully uninstalled the root certificate chain

2. Copy the PEM-formatted certificate file into the router.

   a. To copy, use the request download command. The file will be installed by default in the /home/admin folder if you are logged in as admin.

      br3-we1# request download vpn 512 ftp://admin:c1sco123@192.168.254.51/root-ca.crt
      ==> 'root-ca.crt'
      Connecting to 192.168.254.51:21... connected.
      Logging in as admin ... Logged in!
      ==> SYST ... done.  ==> PWD ... done.
      ==> TYPE I ... done.  ==> CWD not needed.
      ==> SIZE root-ca.crt ... 42492
      ==> PASV ... done.  ==> RETR root-ca.crt ... done.
      Length: 42492 (41K) (unauthoritative)
      root-ca.crt 100%[============================================>]
      41.50K --.-KB/s in 0.001s

      2019-08-07 20:01:28 (34.8 MB/s) - 'root-ca.crt' saved [42492]
3. Install the certificate into the root certificate store by typing `request root-cert-chain install <path/certname>`.

   br3-wel# request root-cert-chain install /home/admin/root-ca.crt
   Uploading root-ca-cert-chain via VPN 0
   Copying ... /home/admin/root-ca.crt via VPN 0
   Installing the new root certificate chain
   Successfully installed the root certificate chain

4. To verify, issue `show certificate root-ca-cert`

   br3-wel# 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: O=Arcturus, O=Cisco, CN=Internal Customer Root CA

Cisco IOS XE SD-WAN router

The process is similar for the Cisco IOS XE SD-WAN routers.

1. Uninstall the previous root certificate chain.

   br2-wel# request platform software sdwan root-cert-chain uninstall
   Successfully uninstalled the root certificate chain

2. Copy the PEM-formatted certificate file into the router.

   br2-wel# copy ftp://admin:cisco123@192.168.254.51/root-ca.crt bootflash: vrf Mgmt-intf
   Destination filename [root-ca.crt]?
   Accessing ftp://*:*@192.168.254.51/root-ca.crt...!
   [OK - 42492/4096 bytes]

   42492 bytes copied in 0.051 secs (833176 bytes/sec)

3. Install the certificate into the root certificate store by typing `request platform sdwan root-cert-chain install <path/certname>`.

   br2-wel# request platform software sdwan root-cert-chain install bootflash:root-ca.crt
   Uploading root-ca-cert-chain via VPN 0
   Copying ... /bootflash/root-ca.crt via VPN 0
   Successfully installed the root certificate chain

Migration to Cisco PKI Certificates

To have a seamless migration to Cisco PKI certificates, it is imperative that all WAN Edge devices have the Cisco PKI root certificate chain installed before the migration to Cisco PKI. If a device is missing the certificate and Cisco PKI certificates are
installed on the controllers, the WAN Edge device will be unable to connect to the SD-WAN overlay and the certificate chain will need to be manually installed. Alternatively, the Cisco PKI root certificate can be distributed by the PnP or ZTP server when the WAN Edge is automatically provisioned. For vEdge routers, the Cisco root certificate is bundled in the software, so the vEdge routers could be manually upgraded to 19.1 or higher as an alternative.

In vManage version 19.1, vManage will distribute the root certificate chain to all WAN Edge devices, so it is important that all WAN Edge devices are authenticated and connected into the overlay when vManage is upgraded to 19.1.

For an existing SD-WAN network, the best way to migrate to Cisco PKI certificates from Symantec/Digicert:

1. Ensure that all WAN Edge routers have connections to the controllers.
2. Upgrade the controller complex to 19.1, first the vManage, followed by the vBond, then followed by the vSmart controllers.
3. Verify that the Cisco root certificate has been installed on the WAN Edge devices. For vEdge routers, issue the show certificate root-ca-cert | inc Cisco command.

   
   br3-wel# 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: O=Arcturus, O=Cisco, CN=Internal Customer Root CA

   If you go to vshell mode on a controller, you can verify the file length of the root-ca.crt file:

   
   ENB_vBond_West# vshell
   ENB_vBond_West:~$ ls -l /usr/share/viptela/root-ca.crt
   -rwxr-xr-x 1 root root 42492 Aug  6 20:33 /usr/share/viptela/root-ca.crt
   ENB_vBond_West:~$ exit
   exit
   
   For Cisco IOS XE SD-WAN routers, the show sdwan certificate root-ca-cert command may only show one certificate. You can look at the timestamp to see if the root-ca.crt was updated around the time of the vManage upgrade. You can also compare the file size of root-ca.crt to the size of the root-ca.crt file on a controller to see if they match.

   
   br2-wel# show bootflash: | inc sdwan/usr/share/viptela/root-ca.crt
   
   1366 42492 Aug 07 2019 20:09:22.000000000 +00:00
   /bootflash/sdwan/usr/share/viptela/root-ca.crt
   
   4. Once you verify the root certificate has been distributed to the WAN Edge routers, the migration to Cisco PKI certificates can be performed. See Option 3: Automated certificate signing through Cisco Systems or Option 4: Manual certificate signing through Cisco Systems in the Deploying Certificates section.
This guide was validated using the following hardware and software.

<table>
<thead>
<tr>
<th>Functional area</th>
<th>Product</th>
<th>Software version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco SD-WAN controllers</td>
<td>Cisco vManage, Cisco vSmart, and Cisco vBond controllers</td>
<td>18.4.1</td>
</tr>
<tr>
<td>Server</td>
<td>Hypervisor/vSphere client</td>
<td>VMware ESXi, 6.7.0, 10302608/version 6.7.0.20000</td>
</tr>
</tbody>
</table>
Appendix B—Windows OpenSSL Certificate Authority (CA)

The following shows an example of how to set up a Windows OpenSSL CA, along with a subordinate CA. Due to some error codes in the later versions, version 1.0.2s 64-bit is used in this deployment.

Procedure 1: Install OpenSSL


2. Run the installer. In this example, the program was installed in C:\OpenSSL-Win64

3. Start the OpenSSL application. Go to C:\OpenSSL-Win64\bin, right-click openssl.exe and choose Run as administrator.

A command window with the OpenSSL prompt opens up.

4. Optionally, you can customize the OpenSSL configuration file (openssl.cfg) and specify the local CA folder structure, default validity in days, policy, etc. By default, created keys and certificates will appear in C:/OpenSSL-Win6/bin.

Procedure 2: Set up the Root Certificate Authority

1. Generate a 4096-bit RSA key for the root CA and store it in the ca.key file.

   OpenSSL> genrsa -out ca.key 4096
Appendix B—Windows OpenSSL Certificate Authority (CA)

2. Create the self-signed root CA certificate `ca.crt` to provide identity for the root CA. Specify the validity of the root certificate for 5 years (1825 days).

   OpenSSL> req -new -x509 -days 1825 -key ca.key -out ca.crt

3. Enter in the fields for the root certificate. Note that Organization Name does not need to match the SD-WAN overlay organization name. In this example, the following fields are used:

   • Country Name: US
   • State or Province Name: NC
   • Locality Name: RTP
   • Organization Name: Cisco Systems Inc
   • Organizational Unit Name: ENB Solutions
   • Common Name: enb-ca1.cisco.com
   • Email Address: [blank]

Procedure 3: Set up the Subordinate Certificate Authority (Sub CA)

6. Generate a 4096-bit RSA key for the sub CA and store it in the `subca.key` file.

   OpenSSL> genrsa -out subca.key 4096

7. Generate the sub CA certificate request, which will be submitted to the root CA for signing.

   OpenSSL> req -new -x509 -days 1825 -key subca.key -out subca.crt

8. Enter in the fields for the sub CA CSR. Note that Organization Name does not need to match the SD-WAN overlay organization name. In this example, the following fields are used:

   • Country Name: US
   • State or Province Name: NC
Appendix B—Windows OpenSSL Certificate Authority (CA)

- Locality Name: RTP
- Organization Name: Cisco Systems Inc
- Organizational Unit Name: ENB Solutions
- Common Name: enb-subca1.cisco.com
- Email Address: [blank]
- A challenge password: cisco123
- An optional company name: [blank]

9. Submit the sub CA CSR for signing. Set the validity period for 3 years (1095 days). The resulting certificate will be named subca.crt.

OpenSSL> x509 -req -days 1095 -in subca.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out subca.crt

Procedure 4: Create the Root CA certificate chain

In the above procedures, the root CA certificate and the sub CA certificate were created. VManage needs the full root CA certificate loaded, which includes the root CA certificate and any intermediate certificates. The intermediate certificates should come first in the file, followed by the root CA certificate. To create the file, you can use the type command at the Windows cmd prompt.

C:\OpenSSL-Win64\bin>cat subca.crt ca.crt > root-ca-chain.pem
C:\OpenSSL-Win64\bin\>type subca.crt ca.crt > root-ca-chain.pem

subca.crt

ca.crt

C:\OpenSSL-Win64\bin>
Appendix C: Plug and Play (PnP) Connect Portal

The PnP portal is located at [http://software.cisco.com](http://software.cisco.com). At this website, you can download software, manage devices through the PnP Connect portal, and manage licenses. Licenses can be managed with the traditional method or through Smart accounts. Smart accounts are required in order to use smart licensing and they provide a central location where you can manage Cisco licenses across the entire organization. After you set up a Smart Account, you have the flexibility to create sub accounts (virtual accounts) to help manage your licenses for departments, areas, or locations within your organization. A virtual account is like a file folder, where you can add multiple virtual accounts based on your business functions. A Smart Account and Virtual Account is required in order to create a controller profile on the PnP Connect portal.

For additional information on Smart Accounts and Smart Licensing:

[https://cisco.com/go/smartaccounts](https://cisco.com/go/smartaccounts)
[https://cisco.com/go/smartlicensing](https://cisco.com/go/smartlicensing)

The Plug and Play Connect portal ([https://software.cisco.com/#pnp-devices](https://software.cisco.com/#pnp-devices)) contains a list of devices and allows you to do multiple things. You can:

1. Enable automatic network provisioning of the IOS XE SD-WAN routers. A controller profile is created within the portal which defines your vBond and organization name information. On bootup, the IOS XE SD-WAN router looks for devicehelper.cisco.com, which directs the router to the PnP portal. The PnP portal checks the serial number of the router and pushes key parameters to it, such as vBond IP address and organization name. From there, the router contacts the vBond orchestrator and controller connectivity is initiated from there. The PnP portal information is used to populate the Zero-Touch Provisioning (ZTP) servers so the vEdge routers can be enabled for automatic network provisioning.

2. Through the controller profile, you can create a serial authorization file for the WAN Edge hardware that you can load into vManage manually. Alternatively, you can allow vManage to sync to the PnP account to download the serial authorization information without manual intervention. Without the serial authorization file, the WAN Edge routers cannot join the overlay network.

3. Transfer devices between Smart Accounts and Virtual Accounts

4. Submit CSRs and receive Cisco PKI certificates for controller certificates as an alternative to Symantec/Digicert certificates. This can be done automatically by vManage or manually.

If you have a Cisco cloud-hosted controller deployment, the controller profile should already be created in the PnP portal. Also, WAN Edge devices that are ordered through Cisco Commerce Workspace (CCW) with a Smart account and Virtual account associated with them should be automatically pushed to the PnP portal.

For on-premise controller deployments, a controller profile can be created manually and WAN Edge devices that are not already in the PnP portal can also be added manually.

This section can show you how to:

- Create a controller profile if one hasn’t already been created
- Add WAN Edge devices to the portal and associate them with a controller profile


Procedure 1: Log into the PnP Connect portal

1. Navigate to [https://software.cisco.com](https://software.cisco.com).
2. In the Network Plug and Play section, click **Plug and Play Connect**. The **Plug and Play Connect** dialog box opens.

3. Within the **Plug and Play Connect** portal, find your Virtual Account linked to the Smart Account on the top right.

If you have not already created the controller profile, do so now. If you have a Cisco-hosted controller model, the information pertaining to your vBond controller should be pre-populated within the controller profiles and you can skip procedure 2.

**Procedure 2: Configure the controller file**

1. Click the **Controller Profiles** tab located directly beneath the **Plug and Play Connect** title and to the right of the **Devices** tab.

2. Click **Add Profile**. The **Add Controller Profile** dialog box opens with **Step 1 Profile Type** highlighted.

3. In the **Controller Type** drop-down, select **vBond**.

4. Click **Next**. **Step 2 Profile Settings** is highlighted and the profile setting fields displayed.
5. In the **Profile Name** field, enter a name for the controller profile you are creating (**ENB-SOLUTIONS-VBOND** in the example).

6. In the **Description** field, enter a description of the profile you are creating (**vBond for ENB SOLUTIONS**). This field is optional.

7. In the **Default Profile** drop-down box, select **Yes** if no other controller profile exists. Regardless of the setting, each WAN Edge that gets added to the PnP Connect portal needs to have a profile associated with it.

8. In the Multi-tenancy box, select **No** if you are using vManage in single tenancy mode, select **Yes** if you are using vManage in Multi-tenancy mode.

9. In the **Organization Name** field, enter the organization name (**ENB-Solutions – 21615** in this example). You can find the organization name in the vManage GUI under the **Administration > Settings** screen.

10. In the **Primary Controller** drop down box, select **Domain Name** or **IPv4** and fill out the vBond hostname or IP address. In the example, select **Host Name** from the drop-down box, and type in the vBond hostname (**vbond-21615.cisco.net** in this example) in the text box. In the textbox to the right, keep the vBond port number at the default (or update it if you have configured a different vBond port number in your network).

11. **Click Next.**

12. Review the options you just configured. If this is a single tenant vManage, then the **SP Organization Name** will be blank. Select **Submit** if they are correct, else go back to correct any settings.

13. The window indicates that the profile was successfully created. Select **Done**.

**Procedure 3: Add WAN Edge devices to the portal**

You can manually add WAN Edge devices that have not already been added to the portal through the Cisco Commerce Workspace process.

To add IOS XE devices to the PnP portal, you need to know the Serial Number, the Base PID (Product Identifier), and the Certificate Serial number. This information is available within the **show crypto pki certificates CISCO_IDEVID_SUDI** command issued on CLI mode in IOS XE code. For the purposes of PnP, the Chassis Serial Number and SUDI certificate (Secure Unique Device Identification) is bound to the Smart account to enable authentication and easy provisioning of the IOS XE device. Note that you need to be on at least 3.14.0s software or higher in order to be able to run this command for the ISR4k.

```plaintext
ISR4351#show crypto pki certificates CISCO_IDEVID_SUDI
```
Certificate

Status: Available
Certificate Serial Number (hex): 01373974
Certificate Usage: General Purpose
Issuer:
  cn=ACT2 SUDI CA
  o=Cisco
Subject:
Name: ISR4351/K9
Serial Number: PID:ISR4351/K9 SN:FDO205108CB

If you have already converted to the SD-WAN image then use the command, show sdwan certificate installed instead.

Router#show sdwan certificate installed
Board-id certificate
-----------------------------
Certificate:

Data:
  Version: 3 (0x2)
  Serial Number: 20396404 (0x1373974)
Signature Algorithm: sha256WithRSAEncryption
  Issuer: O=Cisco, CN=ACT2 SUDI CA
Validity
  Not Before: Dec 16 01:53:51 2016 GMT
  Not After : Dec 16 01:53:51 2026 GMT
Subject: serialNumber=PID:ISR4351/K9 SN:FDO205108CB, O=Cisco,

Alternatively, you can use show sdwan certificate serial:

Router#show sdwan certificate serial
Chassis number: ISR4351/K9-FDO205108CB  Board ID serial number: 01373974

For vEdge routers, you need the serial number and PID of the device in order to add the device to the portal. If this isn't already known, the information can be retrieved using the show hardware inventory CLI command.

2. Under the Network Plug and Play section, click Plug and Play Connect.
3. Ensure the correct Smart and Virtual account is chosen in the top right corner.
4. The **Devices** tab should be selected by default. Select **Add Devices**.

5. The first step is to identify how the device information will be entered, either manually or through a .csv file. Click the **Download Sample CSV** text to use if you select the .csv import method. Select the radio button next to **Enter Device info manually** and click **Next**.

6. Click on the **Identify Device** button. A popup-window will prompt for the **Serial Number** and **Base PID**, a **Controller Profile** to associate the device with, and a **Description**.

7. Enter the **Serial Number** (FDO205108CB), and the **Base PID** (ISR4351/K9) of the device. Once you select the **Base PID** textbox, enter values to search on, press enter and then select the PID that matches your device. Once a PID is selected, additional fields will appear. Enter the **Certificate Serial Number** (1373974) and choose the **Controller Profile** (ENB-SOLUTIONS-VBOND) to associate with the device when using PnP. Enter an optional **Description** (BR1-WE1) and click **Save**.

Note that the certificate serial number is in hex format with no preceding 0x.
8. Select **Next**. Review the device information. Click the **Back** button if information for the device needs to be modified.

9. Click **Submit**. The page will indicate that it successfully added 1 device.

10. Select **Done** to refresh the page. By default, an IOS XE SD-WAN device will be in **Pending (Redirection)** status and marked yellow, and a vEdge device will be in **Pending for publish** status and marked yellow. Once PnP occurs with an IOS XE SD-WAN device, the device will be in **Redirect Successful** status and marked green. Once the vEdge information is synced to the ZTP server, the device will be in **Provisioned** status and marked green.

11. Repeat steps to add any additional devices.
ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unified Computing System (Cisco UCS), Cisco UCS B-Series Blade Servers, Cisco UCS C-Series Rack Servers, Cisco UCS S-Series Storage Servers, Cisco UCS Manager, Cisco UCS Management Software, Cisco Unified Fabric, Cisco Application Centric Infrastructure, Cisco Nexus 9000 Series, Cisco Nexus 7000 Series. Cisco Prime Data Center Network Manager, Cisco NX-OS Software, Cisco MDS Series, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, LightStream, Linksy, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0809R)

© 2019 Cisco Systems, Inc. All rights reserved.

Feedback & Discussion

For comments and suggestions about our guides, please join the discussion on Cisco Community.