Cisco SD-WAN: WAN Edge Onboarding

Prescriptive Deployment Guide

January, 2020

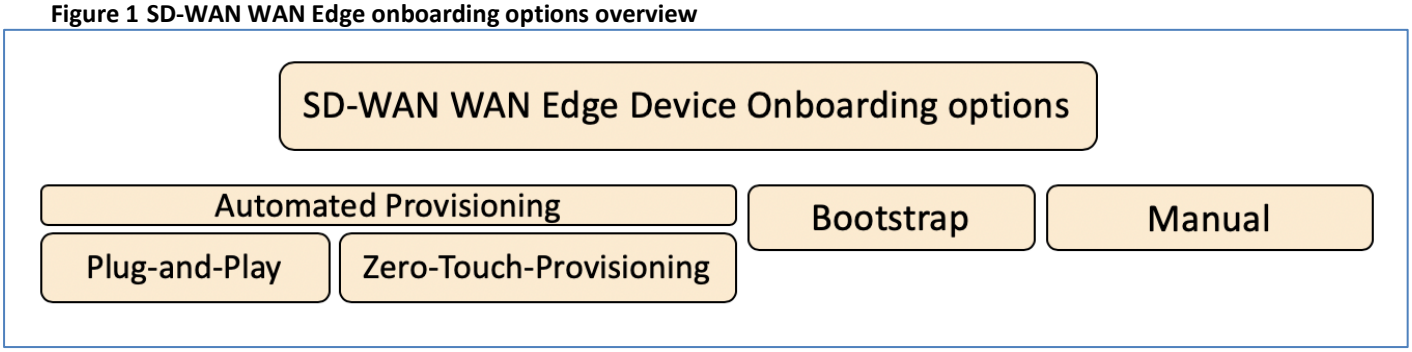
Table of Contents

Introduction

About the guide

This guide is intended to provide design and deployment guidance to onboard Cisco SD-WAN WAN Edge devices into the enterprise SD-WAN Infrastructure. The guide focuses on the step-by-step procedures to configure each of the onboarding options available, along with the use cases specific to WAN Edge deployment using default pre-installed certificates or enterprise root-ca certificates. The physical or virtual WAN Edge onboard options include manual, bootstrap or the automated deployment process, which is referred to as Zero Touch Provisioning (ZTP) for vEdge devices and Plug-and-Play (PnP) for IOS XE SD-WAN devices.

Figure 1 SD-WAN WAN Edge onboarding options overview



This prescriptive deployment guide focuses on how to deploy a Cisco WAN Edge device within a branch environment. In this guide, SD-WAN controllers are deployed in the cloud and WAN Edge routers are deployed either at remote sites or at the datacenter and are connected to two WAN transports, Internet and MPLS. This guide covers SD-WAN deployment using multiple certificate use cases – Symantec/DigiCert, Cisco PKI or Enterprise CA certificates.

Although this deployment guide is about onboarding Cisco SD-WAN WAN Edge devices. It is presumed that

- Cisco SD-WAN Controllers (vManage, vBond, and vSmart) are already deployed with valid certificates.
- Cisco WAN Edge has reachability to the vBond orchestrator and other SD-WAN controllers which are reachable via public IP addresses across the WAN transport(s).

For more information on SD-WAN controller design and deployment, please refer to the Cisco SD-WAN Design guide and the Cisco SD-WAN End-to-End Deployment guide.

This document contains four major sections:

The **Define** section provides a high-level overview of the SD-WAN architecture and components, WAN Edge devices and options available to onboard for a physical or virtual WAN Edge router.

The **Design** section provides detailed discussion on the design considerations and prerequisites needed for each of the onboarding options to build a secure SD-WAN enterprise infrastructure.

The **Deploy** section discusses step-by-step procedures to onboard a Cisco SD-WAN WAN Edge device in the SD-WAN network. It walks through the best practices and gotchas to consider during the WAN Edge onboarding process.

The **Operate** section briefly discusses how to monitor and troubleshoot the onboarding issues, if necessary, in the SD-WAN environment.

Refer to Appendix A for details on the platform and software versions used to build this document.

Audience

The audience for this document includes network design engineers and network operations personnel who have deployed the Cisco SD-WAN controllers and are looking for the best viable option to onboard the WAN Edge devices in their respective network environment.

Define

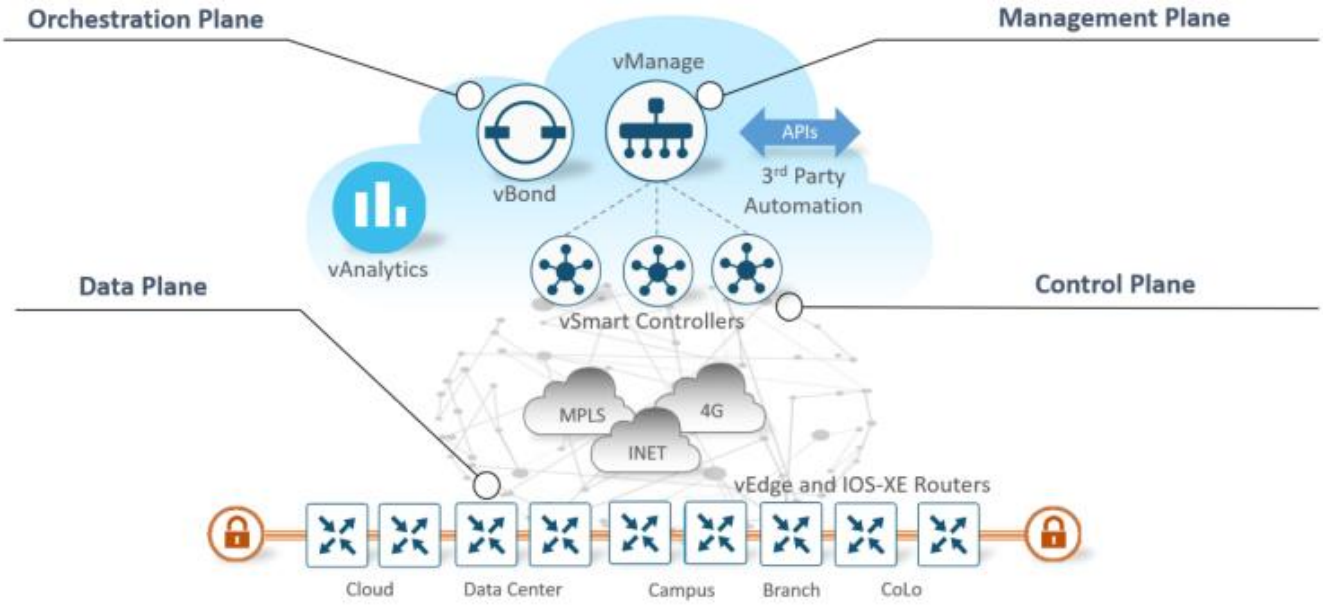
About the solution

The Cisco SD-WAN solution is an enterprise-grade SD-WAN architecture overlay that enables digital and cloud transformation for enterprise. The solution fully integrates routing, security, centralized policy and orchestration into large-scale networks and addresses the problems and challenges of common WAN deployments.

The Cisco SD-WAN solution is comprised of separate orchestration, management, control and data plane.

- **Orchestration plane** assists in securely onboarding the SD-WAN WAN Edge routers into the SD-WAN overlay. The vBond controller, or orchestrator, authenticates and authorizes the SD-WAN components onto the network. The vBond orchestrator takes an added responsibility to distribute the list of vSmart and vManage controller information to the WAN Edge routers.
- **Management plane** is responsible for central configuration and monitoring. The vManage controller is the centralized network management system that provides a single pane of glass GUI interface to easily deploy, configure, monitor and troubleshoot all Cisco SD-WAN components in the network.
- **Control plane** builds and maintains the network topology and make decisions on the traffic flows. The vSmart controller disseminates control plane information between WAN Edge devices, implements control plane policies and distributes data plane policies to network devices for enforcement.
- **Data plane** is responsible for forwarding packets based on decisions from the control plane. WAN Edge physical or virtual devices provide secure data-plane connectivity between the sites in the same SD-WAN overlay network. WAN Edge devices are responsible for establishing secure connections for traffic forwarding, for security, encryption, Quality of Service (QoS) enforcement and more.

Figure 2 Cisco SD-WAN solution components



In this solution, we focus on building secure data plane connections, which involves onboarding physical or virtual WAN Edge devices and establishing secure control connections across all the SD-WAN components in the network environment.

Secure onboarding of the SD-WAN WAN Edge physical or virtual device always requires the device to be identified, trusted and white-listed in the same overlay network. Mutual authentication needs to happen across all the SD-WAN components before establishing secure control connections between SD-WAN components in the same overlay network.

Identity, Trust and Whitelist

Identity of the WAN Edge device is uniquely identified by the chassis ID and certificate serial number. Depending on the WAN Edge router, certificates are provided in different ways:

- Hardware-based vEdge device certificate is stored in the on-board Tamper Proof Module (TPM) chip installed during manufacturing.
- Hardware-based Cisco IOS-XE SD-WAN device certificate is stored in the on-board SUDI chip installed during manufacturing.
- Virtual platform or Cisco IOS-XE SD-WAN devices do not have root certificates (such as the ASR1002-X platform) preinstalled on the device. For these devices, a One-Time Password (OTP) is provided by vManage to authenticate the device with the SD-WAN controllers.

Trust of the WAN Edge devices is done using the root chain certificates that are pre-loaded in manufacturing, loaded manually, distributed automatically by vManage, or installed during the PnP or ZTP automated deployment provisioning process.

The Cisco SD-WAN solution uses a whitelist model, which means that the WAN Edge devices that are allowed to join the SD-WAN overlay network need to be known by all the SD-WAN controllers beforehand. This is done by adding the WAN Edge devices in the Plug-and-Play connect portal (PnP). The added WAN Edge devices are attached to the vBond controller profile contained in the PnP portal (associated with the SD-WAN overlay organization-name) to create a provisioning file. This file is imported into the SD-WAN vManage controller, which then automatically shares the device whitelist with the rest of SD-WAN controllers (vBond and vSmart). The provisioning file containing the device whitelist can also be synced directly from the plug-and-play connect portal to Manage via a secure SSL connection through REST APIs.

Note: The Cisco SD-WAN components (vManage, vBond and vSmart controllers and WAN Edge devices) should all be configured with the same organization-name to join the same SD-WAN overlay network.

WAN Edge onboarding process

Upon bootup, the WAN Edge device contacts the vBond orchestrator to establish a secure transient DTLS control connection. The vBond information can be either configured manually via CLI on the WAN Edge device, using an IP address or resolvable domain-name FQDN, or can be obtained automatically through the PnP or ZTP process.

The SD-WAN controllers (vBond, vManage and vSmart) and WAN Edge devices need to mutually authenticate and trust each other before establishing the secure control connections. When the SD-WAN controllers authenticate each other and WAN Edge devices, they:

- Validate the root of trust for the certificate root CA.
- Compare the organization name of the received certificate OU against the locally configured.
- Compare the certificate serial number against the authorized whitelist.

When the WAN Edge devices authenticate the controllers, they:

- Validate the root of trust for the certificate root CA.
- Compare the organization name of the received certificate OU against the locally configured.

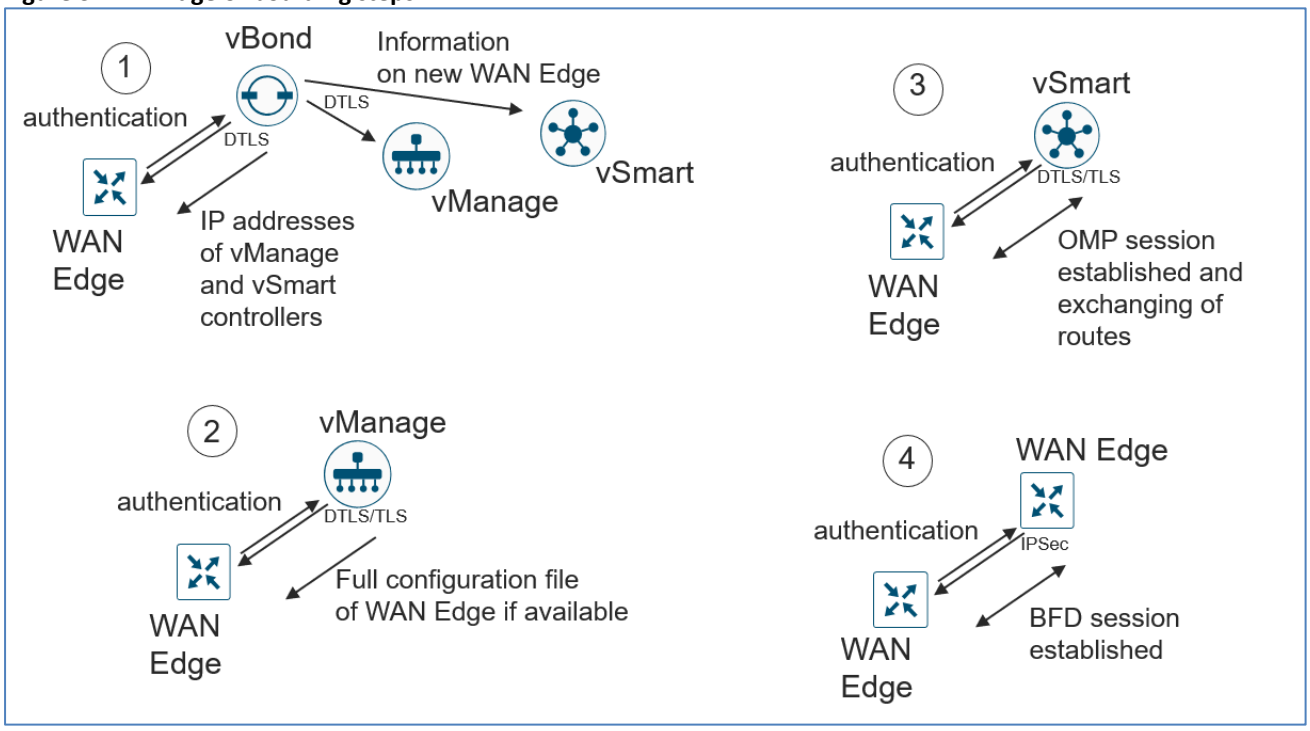
The vBond orchestrator upon successful authentication establishes a secure transient DTLS control connection and then shares vManage and vSmart controller IP addresses. At this time, the vBond orchestrator will inform the other SD-WAN controllers (vManage and vSmart) to expect a control connection request from the WAN Edge device.

The WAN Edge device, upon learning the vManage information, initiates a control connection to the vManage server. Following successful authentication, a separate secure persistent DTLS/TLS connection is established and vManage, based on the device template attached to the WAN Edge device, provisions the configuration using the NETCONF protocol.

The WAN Edge device also establishes a parallel secure persistent DTLS/TLS control connection to the vSmart controller. The WAN Edge device establishes OMP adjacencies and shares local route information with the vSmart controller. The vSmart controller based on the defined policies, calculates and disseminates the route, security and policy information to all WAN Edge devices using OMP updates. Overlay Management Protocol (OMP) is responsible for establishing and maintaining the overlay control plane.

Cisco WAN Edge devices upon receiving route information, establish BFD sessions across all WAN transports to every other WAN Edge device that is part of the overlay network.

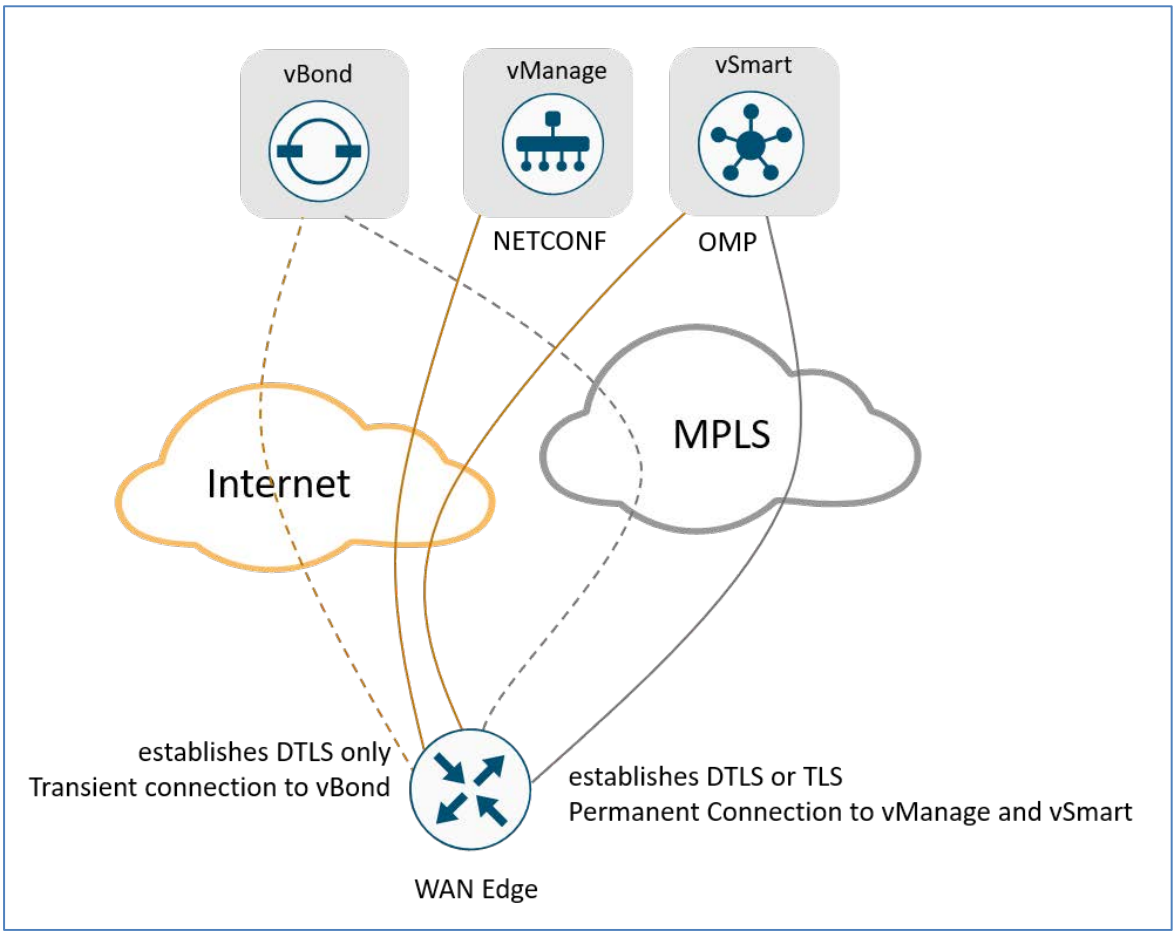
Figure 3 WAN Edge onboarding steps



Default behavior of the SD-WAN WAN Edge device is to establish:

- Secure transient DTLS control connection to vBond across all available WAN transports only during the onboarding process.
- Secure permanent DTLS/TLS control connections to vSmart across all available WAN transports and to vManage across a single WAN transport.
- Secure BFD sessions between WAN Edge devices which are part of the same overlay network across all available WAN transports.

Figure 4 WAN Edge control connections to different SD-WAN controllers



Cisco SD-WAN WAN Edge device

Cisco SD-WAN WAN Edge devices can be broadly categorized based on the software powering the device into two software categories,

Cisco IOS-XE SD-WAN software:

- Physical Platform: ASR 1000, ISR 1000, ISR 4000 series router models (with exception of ISR1100-4G/6G)
- Virtual Platform: CSR 1000v, ISRv series router models

Viptela OS software:

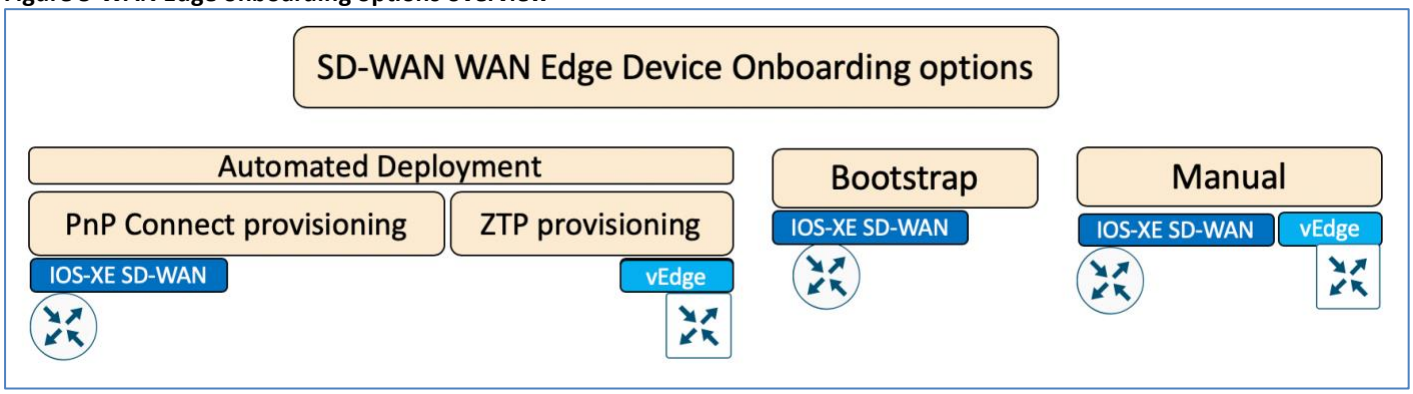
- Physical Platform: vEdge 100b/100m, vEdge 1000, vEdge 2000, vEdge 5000, ISR1100-4G/6G router models
- Virtual Platform: vEdge cloud router models

Design

WAN Edge Onboarding options

There are several options available to securely onboard SD-WAN Edge devices.

Figure 5 WAN Edge onboarding options overview



Supported WAN Edge Devices

Depending on the software running on the network device, IOS-XE SD-WAN or vEdge software, the below tables list the supported WAN Edge onboarding options.

Table 1 IOS-XE SD-WAN WAN Edge onboarding options

Platform	Plug-and-Play (PnP)	Bootstrap	Manual
ASR1K	✓	✓	✓
ASR1002-X	×	✓	×
ISR4K	✓	✓	✓
ISR1K	✓	✓	✓

Table 2 vEdge WAN Edge onboarding options

Platform	Zero-Touch Provisioning (ZTP)	Manual
vEdge 100	✓	✓
vEdge 1000	✓	✓
vEdge 2000	✓	✓
vEdge 5000	✓	✓
vEdge Cloud	×	✓

Automated Deployment

Automated deployment automates the true day-zero experience of securely onboarding and deploying the WAN Edge device, with default-shipped factory settings, into the SD-WAN network. Automated deployment discovers the vBond IP address dynamically using,

- the Plug-and-Play process for the IOS-XE WAN Edge physical platform
- the Zero-Touch provisioning process for the vEdge physical platform

The following outlines the primary requirements in order to use this onboarding option:

- The WAN Edge device is connected to a WAN transport that can provide a dynamic IP address, default-gateway and DNS information.
- The WAN Edge device can resolve 'devicehelper.cisco.com' for the Plug-and-Play connect server for IOS-XE SD-WAN physical devices and 'ztp.viptela.com' for the ZTP server for vEdge physical devices.
- In vManage, a device configuration must be built and attached to the WAN Edge device to successfully onboard the device. Refer to '**Appendix G - SD-WAN Device Template**' for the feature and device template used in this guide.

Plug-and-Play process:

The day-zero automated Plug-and-Play (PnP) process provides a simple, secure procedure to discover, install and provision the Cisco IOS-XE SD-WAN Edge device to join the SD-WAN overlay network.

An overview of all the steps involved during the Plug-and-Play onboarding process is explained below:

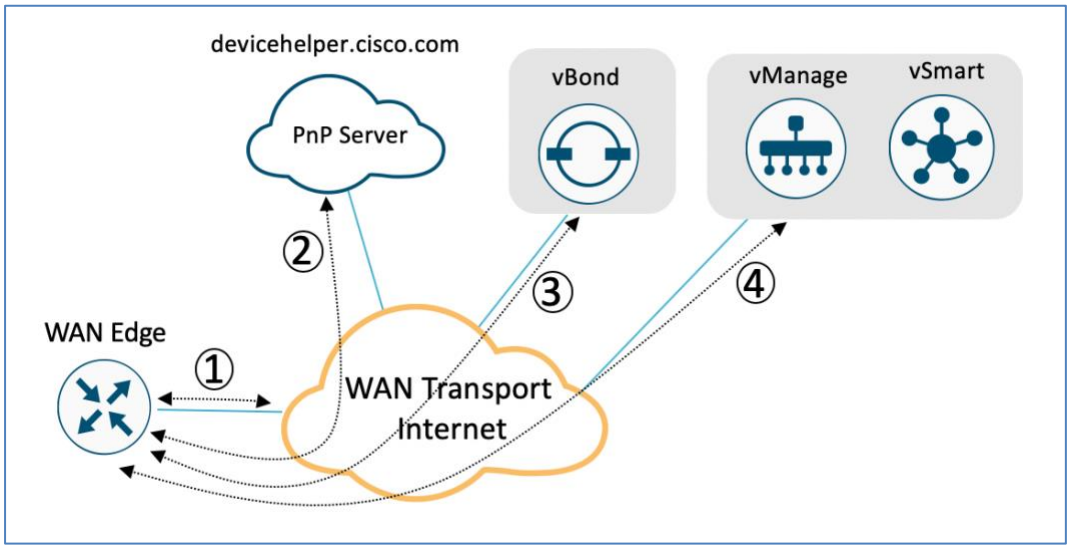
1. The Cisco WAN Edge device on boot up, obtains IP address, default gateway and DNS information via DHCP on the supported device's PnP interface that is connected to the WAN transport (typically Internet).
2. The Cisco WAN Edge device attempts to reach the Cisco-hosted Plug-and-Play (PnP) connect server. The router attempts to resolve the name of the PnP server at devicehelper.cisco.com and uses an HTTPS connection to gather information about the enterprise SD-WAN vBond orchestrator, including the organization-name.

Technical Tip: For an SD-WAN deployment using enterprise root-ca certificates, the WAN Edge device receives the root certificates, along with the vBond and organization name information from the PnP Connect portal.

3. The WAN Edge device authenticates with the vBond orchestrator using its chassis/serial number and root-certificate. Following successful authentication, the vBond orchestrator provides the device with the vManage and vSmart controller information.
4. The WAN Edge device initiates and establishes secure connections with the vManage and vSmart controllers and downloads the configuration using NETCONF from vManage and joins the SD-WAN overlay network.

The figure below provides an overview of the steps involved, in the Plug-and-Play onboarding process.

Figure 6 Cisco IOS-XE WAN Edge onboarding – PnP process



The table below lists the platform along with the interfaces that support the Plug-and-Play (PnP) onboarding process:

Table 3 IOS XE SD-WAN WAN Edge platform support list

Platform	Plug-and-Play	Interface
ASR1K	✓	GigabitEthernet (routed interface)
ASR1002-X	✕	NA
ISR1K	✓	GigabitEthernet (routed interface) Cellular
ISR4K	✓	GigabitEthernet (routed interface) Cellular

Note: PnP is supported on all routed GigabitEthernet interfaces with the exception of the Management interface and GigabitEthernet0. PnP is not supported on switched interfaces.

Zero-Touch Provisioning process:

The day-zero automated ZTP process provides a simple, secure procedure to discover, install and provision vEdge devices to join the SD-WAN overlay network.

The Zero-Touch-Provisioning server maintains the authorized WAN Edge device list and vBond information that device registers to join the SD-WAN overlay network. The Cisco cloud-based ZTP server can be utilized, or in an air-gapped network, an on-premise ZTP server can be deployed in the datacenter with the requirement that the vEdge platform should resolve ztp.viptela.com to reach the ZTP server upon connection to the WAN transport.

An overview of all the steps involved during the ZTP onboarding process is explained below:

1. The vEdge device upon boot up, obtains an IP address, default gateway IP and DNS information through DHCP on the supported device's ZTP interface connected to the WAN-transport, typically Internet.
2. The vEdge device attempts to reach the ZTP server. The router attempts to resolve the name of the ZTP server at ztp.viptela.com and uses an HTTPS connection to gather information about the enterprise SD-WAN vBond orchestrator along with the organization name.

Technical Tip: For WAN Edge devices using enterprise root-ca certificate, the device is installed with an enterprise root certificate to successfully authenticate and join the enterprise SD-WAN network. The ZTP server can send the enterprise root certificates along with the organization name and vBond information automatically.

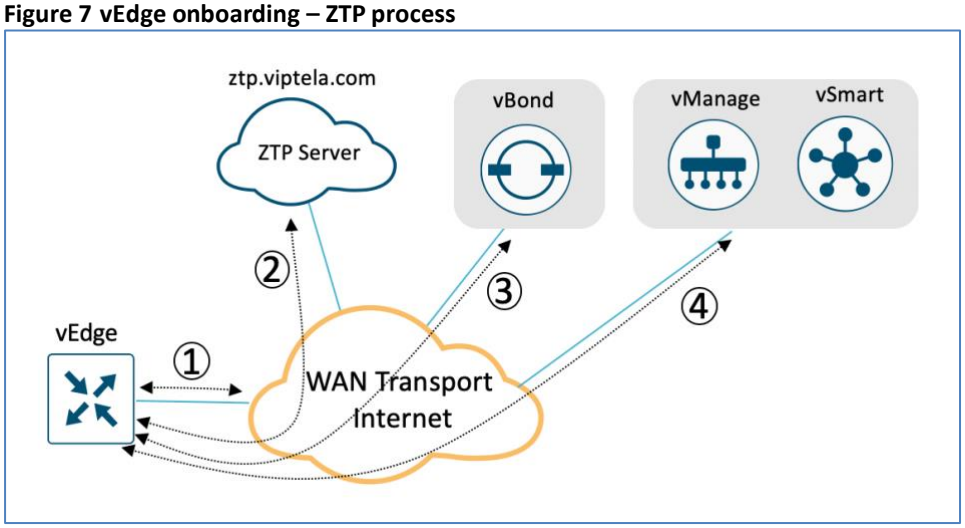
3. The vEdge router authenticates to the vBond orchestrator using its chassis/serial number and root-certificate. Following successful authentication, the vBond orchestrator provides the vEdge router with vManage and vSmart controller information.

4. vEdge device then establishes secure connections with the vManage and vSmart, and downloads the configuration using NETCONF from vManage and joins the SD-WAN overlay network.

   Note, vEdge devices can be updated to the desired software version as a part of automated onboarding process.

The figure below provides an overview of the steps involved, as discussed above, in the ZTP onboarding process.

Figure 7 vEdge onboarding – ZTP process



The table below lists the platform along with the interfaces that support the ZTP onboarding process:

Table 4 vEdge platform, interface support list

Platform	ZTP	Interface
vEdge 100, 100b	✓	ge0/4
vEdge 100m, 100wm	✓	ge0/4 Cellular0
vEdge 1000	✓	ge0/0
vEdge 2000	✓	ge2/0
vEdge 5000	✓	ge0/0 (first port on the first available network slot)
vEdge cloud	✕	NA

Bootstrap Deployment

An alternative option to onboard the IOS-XE SD-WAN WAN Edge device is to use the bootstrap option.

The intent behind using this option is to provide the factory-shipped default configured WAN Edge device the configuration needed to securely onboard, when a customer is unable to leverage the automated discovery option.

Note, that this option is available only for IOS-XE SD-WAN WAN Edge platforms and not for vEdge devices.

This onboarding option can be leveraged in deployments where,

- The WAN Edge device has a connection to the WAN transport that cannot provide a dynamic IP Address, typically MPLS or private WAN transport.
- The WAN Edge device is deployed in an air-gapped environment, where the device cannot reach the cloud-hosted Plug-and-Play (PnP) connect server.
- The WAN Edge device is connected to the WAN transport with a non-PnP supported interface, or with an interface requiring additional configuration for connectivity, such as PPoE or a subinterface, for example.

Leveraging bootstrap deployment requires the device template configuration to be built and attached to the WAN Edge device in vManage, after which the configuration file is built and shared with the WAN Edge device. The configuration file can be shared with the WAN Edge device either by copying the configuration to the device's internal bootflash or by copying the file to a bootable USB, which is connected and available on the WAN Edge device on bootup. Note, the configuration file has to have a specific filename for the device to load during the device bootup process.

An overview of all the steps involved during the bootstrap onboarding process is explained below:

1. The WAN Edge device upon bootup initiates the Plug-and-Play (PnP) process. The PnP process first searches the device bootflash for the configuration file, which is a specific filename based on the platform. If the configuration file is unavailable, the PnP process continues to search for a bootable USB connected to the device (if available). If a file is available, the device loads the entire configuration and aborts the Plug-and-Play process.

   The following table list out the platforms that support the bootstrap method, along with the configuration filename to be used.

Table 5 Bootstrap WAN Edge platform support list with filename that need to be leveraged

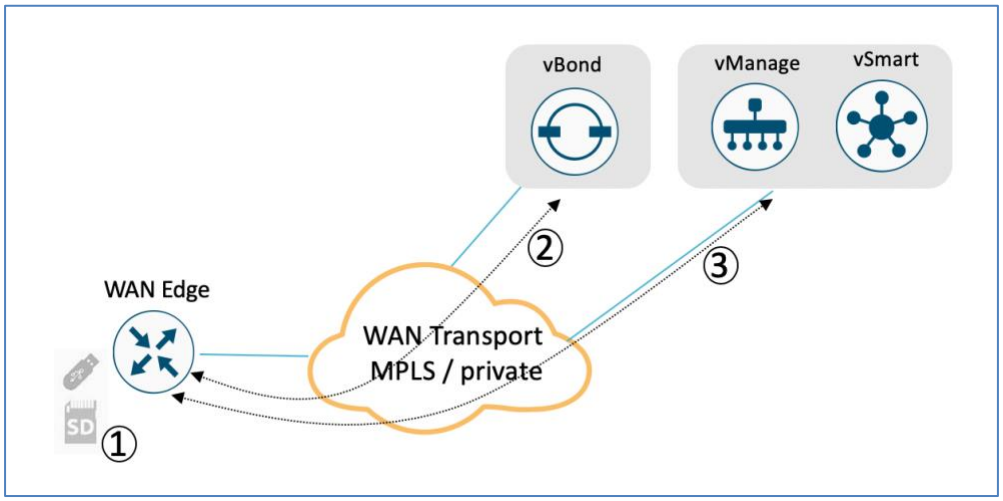
Platform	Bootstrap	Configuration filename
ASR1K	✓	ciscosdwan.cfg
ISR1K	✓	
ISR4K	✓	
ASR1002-X	✓	ciscosdwan_cloud_init.cfg

2. The WAN Edge device learns the vBond and organization name from the system template embedded in the configuration and initiates a secure control connection to the vBond orchestrator. Upon successful authentication by the vBond controller, the WAN Edge device receives information regarding the vManage and vSmart controllers.
3. The WAN Edge device establishes secure connections with vManage and vSmart and downloads the entire configuration using NETCONF from the vManage and joins the SD-WAN overlay network.

Technical Tip: For WAN Edge devices using enterprise root-ca certificates, the device is installed with the root certificates manually before it initiates a connection with the vBond orchestrator. In the bootstrap onboarding method, the enterprise root-certificate is copied along with the configuration to the WAN Edge device and installed to successfully onboard the device.

The figure below shows an overview of the steps involved in the bootstrap onboarding process.

Figure 8 Cisco IOS-XE SD-WAN onboarding – Bootstrap process



Technical Tip: The WAN Edge ASR1002-X does not have a trusted root certificate preinstalled on the chassis that is required to authenticate the device. For such devices, a One-Time-Password (OTP) is leveraged to authenticate the device. The OTP is auto-generated by vManage upon adding the WAN Edge in the SD-WAN controller authorized device whitelist. The bootstrap configuration generated for the device contains the OTP in the cloud-config section of the file. Upon successful authentication, vManage generates and pushes the root certificate that will be used going forward. The bootstrap method is the only option available to onboard the ASR 1002-X platform into the SD-WAN network.

Manual Deployment

Alternatively, the WAN Edge devices can be manually configured using the console port on the hardware platform or using the KVM/ ESXi console connection for the virtual device. When using this option, configure the device with a bare minimum configuration that is needed for the device to reach the vBond SD-WAN controller. Upon device authentication and authorization by the vBond orchestrator, and subsequently, the vManage and vSmart controllers, the WAN Edge device makes a permanent control connection with the vManage and vSmart controllers.

The vManage feature template and device template can be leveraged to fully configure the WAN Edge device. On establishing a control connection with vManage, the configured device template is pushed to the WAN Edge device.

Note, that a device template attached in vManage is not required for WAN Edge devices to establish control connections to the controllers, as long as the bare minimum CLI configuration is configured. The device template may be attached at a later time. To successfully onboard the WAN Edge, the minimum basic configuration contains,

- System properties with system-ip, site-id, organization-name and vBond information.
- Transport VPN (VPN 0) interface with IP address, route and tunnel configuration.

System Properties

Some system properties are basic parameters that are required for the WAN Edge device to get onboarded into the SD-WAN overlay network. System properties include:

- Hostname (optional): unique name defined for the WAN Edge device. The name is prepended to the device's user prompt.
- System-ip: system-ip is a unique physical identity assigned to the WAN Edge device, independent of any interface address. Similar to a router-id, this address need not be advertised.
- Site-id: system site-id identifies the physical location within the Cisco SD-WAN overlay network such as branch, datacenter or campus. WAN Edge devices in the same location are configured with the same site-id and by default, WAN Edge devices with the same site-id will not establish IPSec tunnel connections between them.

Technical Tip: Careful consideration should be taken when choosing system-ip and site-id as this gives a logical scheme to the network and specifically site-id can be leveraged to define policy influencing the geo-location. Refer to the SD-WAN Design Guide for guidance on how to organize these values.

- Organization-name: system organization-name is a unique name specified for the overlay network. All SD-WAN components (vManage, vBond, vSmart and WAN Edge devices) have to match the organization name to be authenticated and become a part of the same SD-WAN overlay network.
- vBond: system vBond is the SD-WAN orchestrator for the overlay network. A WAN Edge device first reaches out to vBond to authenticate before initiating control connections to any SD-WAN controllers (vManage or vSmart). vBond configuration includes either an IP address or a resolvable FQDN domain-name of the vBond interface IP address in the transport VPN, VPN 0.

Technical Tip: Note that, for certificate authentication to succeed, network time should be synced between WAN Edge routers and the controllers. Configure NTP to ensure time is synced across network devices.

Transport VPN

VPN 0 is the transport VPN that connects the WAN Edge to the WAN transport and creates control plane and data plane connections. The WAN Edge device can connect to multiple WAN transport(s) on different interfaces on the same VPN 0 transport segment. At least one interface needs to be configured to initially reach the SD-WAN controllers for onboarding.

Each interface in the transport VPN, VPN 0, should include:

- Interface IP address and subnet mask on the WAN transport VPN 0 Interface.
- Tunnel connection to establish secure control connections to the SD-WAN controller components. Tunnel configuration should include:
    - Color, that identifies the individual WAN transport on the WAN Edge.
    - Encapsulation, that determines the encapsulation type of the tunnel. By default, none is set. IPSec, which performs encryption, or GRE must be explicitly set.
- Dynamic routing or default route to provide reachability to the SD-WAN controllers.

Management VPN (optional)

VPN 512 is the network management VPN and is reserved for out-of-band management traffic. Configure the VPN 512 interface with:

- Interface IP address and subnet mask
- Dynamic routing or default route to provide reachability for out-of-band management.

Manual Onboarding Process

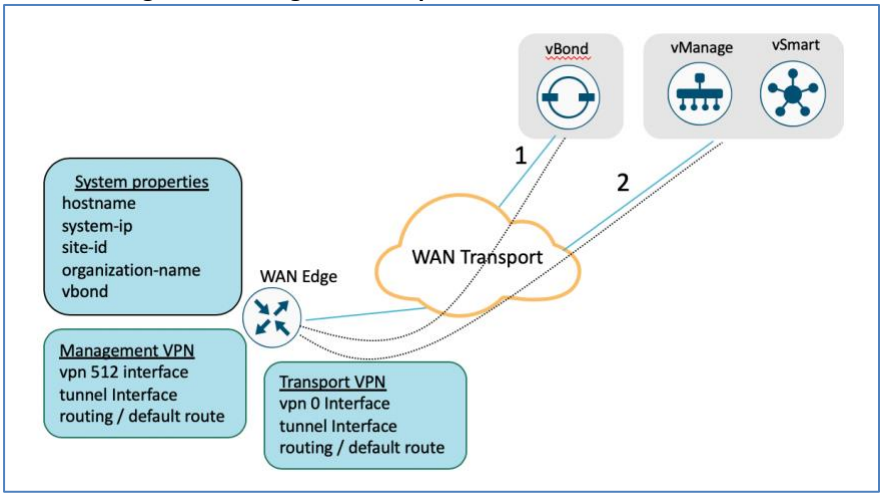
An overview of all the steps involved during the manual onboarding process is explained below:

1. The WAN Edge device learns the vBond and organization name from the configuration and initiates a secure control connection to the vBond orchestrator. Upon successful authentication by the vBond controller, the WAN Edge device receives information regarding the vManage and vSmart controllers.
2. The WAN Edge device establishes secure connections with vManage and vSmart and, downloads the entire configuration if present using NETCONF from the vManage and joins the SD-WAN overlay network.

Technical Tip: For WAN Edge devices using enterprise root-ca certificates, the WAN Edge device needs to be installed with root certificates manually before initiating the connection to vBond orchestrator. To successfully onboard the WAN Edge device, copy and install the enterprise root-certificate into the device.

The figure below shows an overview of the steps involved in the manual onboarding process.

Figure 9 WAN Edge onboarding – Manual process



Staging

WAN Edge devices can be staged through the certificate status, controlled from vManage. Certificates for devices can be placed in staging state before deployment. During staging state, WAN Edge devices can only establish secure control connections with the SD-WAN controllers. No data plane connections are created. Hence, the vSmart controller establishes a secure connection with the WAN Edge device and learns routes from the staged device but does not advertise learned routes to any other WAN Edge devices in the network. Also, the vSmart will not send any routes or data policies to the staged WAN Edge device.

The WAN Edge device in the staged state can be leveraged to prepare the device, which may involve upgrading software and configuring the device, before fully integrating it into the SD-WAN overlay network by changing the certificate status from **Staging** to **Valid** from the vManage GUI.

WAN Edge Certificate Status

The WAN Edge device certificate, in vManage, can be configured to be in one of the below states:

- Invalid – In this state, the WAN Edge device is not authorized to join the SD-WAN controllers and the overlay network. The device does not form control plane or data plane connections to any of the SD-WAN components.
- Staging – In this state, the WAN Edge device establishes secure control plane connections to the SD-WAN controllers (vBond, vManage, and vSmart) only. It is important to note that no data plane connections are established with other WAN Edge devices in the overlay network.
- Valid – In this state, the WAN Edge device is fully onboarded onto the SD-WAN network. The device establishes secure control plane connections with the controllers and secure data plane connections with all the other WAN Edge routers in the SD-WAN overlay network.

Zero-Trust Model

The Cisco SD-WAN solution is a Zero-Trust model. Trusting a WAN Edge device involves two important components, the WAN device whitelist and the root certificate. In addition, in order to be authorized on the network, the device certificate must be in a valid state.

WAN Edge Device Whitelisting

WAN Edge devices have to be known and authorized by all the SD-WAN controllers before allowing the device onto the network. Authorizing the device can be done by,

- Adding the device in Plug-and-Play connect portal and associating it with the vBond controller profile.
- Synchronizing the device list to vManage or manually downloading and importing the provisioning file to vManage.

Technical Tip: WAN Edge network devices can be added automatically and associated with the vBond profile in the Plug-and-Play connect portal by assigning the smart account and virtual account details while ordering at Cisco Commerce. For more information, refer to **Appendix D – Cisco Plug-and-Play connect**.

Root Certificate

Physical WAN Edge devices have either a Symantec/DigiCert or Cisco PKI root certificate pre-installed during the device manufacturing.

Alternatively, customers also have the flexibility of installing enterprise root CA certificates. In this case, the enterprise root-certificate must be installed to successfully authenticate and onboard the device.

The ASR1002-X and virtual WAN Edge devices do not have root certificates preinstalled. Authenticating these device requires the use of a one-time-password generated by vManage. Upon successful authentication of the device by the vManage SD-WAN controller, the vManage installs root certificates on the device.

Network Firewall Requirements

For deployments with WAN Edge devices behind a firewall, make certain the appropriate ports are opened for the SD-WAN components to securely establish connections.

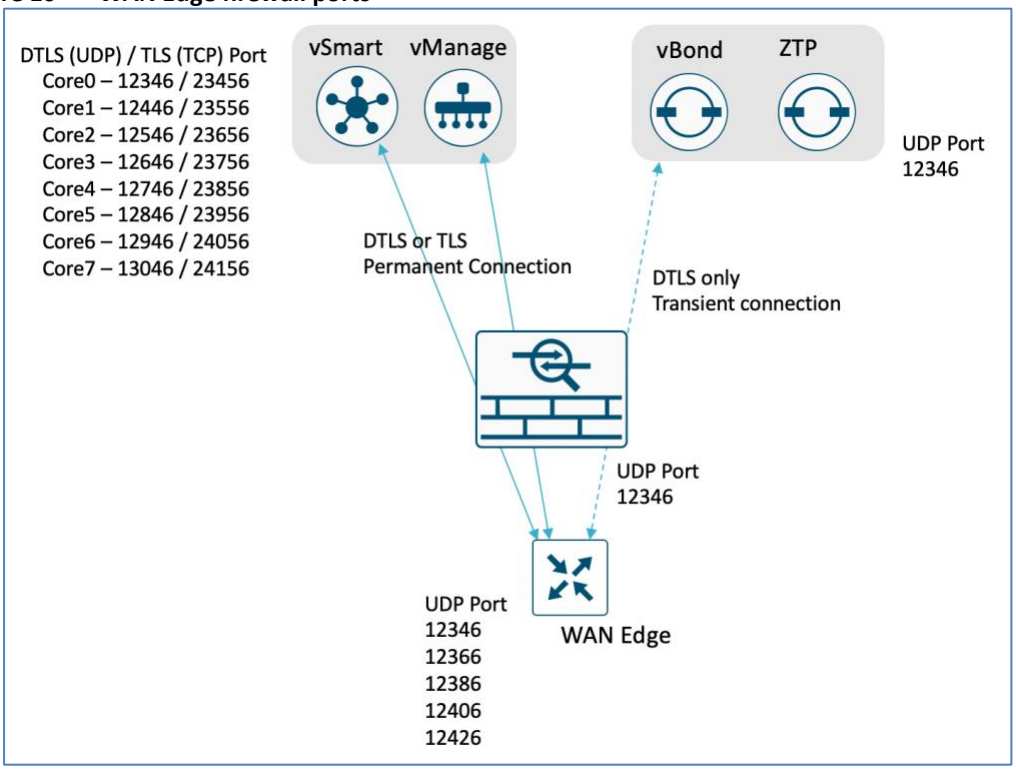
- By default, all the SD-WAN components attempt to use DTLS, UDP base port 12346 to establish connections.
- In scenarios where the WAN Edge device is not able to establish control connections with the SD-WAN controllers using the default base port or when multiple WAN Edge devices are placed behind a NAT device, the WAN Edge device can port hop through 5 base ports after attempting on each port longer and longer between each connection attempt. Port hopping is done sequentially on ports 12346, 12366, 12386, 12406, 12426 before returning to port 12346. Port hopping is turned on by default on the WAN Edge device.
- A port-offset can be configured to uniquely identify each WAN Edge device placed behind a NAT device and to prevent attempts from using the same base ports. A port offset is a number from 0 to 19, 0 being the default. If a port-offset is configured, the default base port is incremented with the port-offset value and then subsequent ports are incremented by 20. For example, in a deployment with a port-offset value set to 1, then the WAN Edge initiates the connection with port 12347 (12346+1) and then subsequently port hopping is done sequentially on ports 12347, 12367, 12387, 12407, 12427 before returning to port 12347.
- The WAN Edge device uses the same base ports to establish data plane connections, such as IPsec connections and BFD sessions, with other WAN Edge devices in the overlay network.
- The vBond orchestrator always uses DTLS, UDP source port 12346, to establish control connections with the SD-WAN components. This default port can be changed with a configuration change, however.

- By default, the vManage and vSmart controllers run on virtual machines, each running up to eight cores. Each core uses DTLS and is allocated a separate base port for control connections, which is UDP on ports 12346, 12446, 12546, 12646, 12746, 12846, 12946, and 13046 by default. Port offsets can also be configured on the controllers if needed, so any port offset from 1 to 19 would increment the base port by the offset number. The WAN Edge device is hashed to one of these ports to form a control connection.

- Cisco SD-WAN can be deployed using TLS connections, instead of the default DTLS. In such scenarios, the vManage and vSmart controllers will use TCP base ports 23456, 23556, 23656, 23756, 23856, 23956, 24056, and 24156. The WAN Edge device uses random TCP source ports to establish connections.

The following diagram illustrates the base port numbers used for control connections by the WAN Edge routers and the SD-WAN controllers. Be certain to account for any offset port numbers in use.

Figure 10 WAN Edge firewall ports



Technical Tip: On the vEdge devices, the CLI commands, **show control local properties** and **show control connections** shows source and destination ports respectively in use for connections to the controllers. On the IOS XE SD-WAN devices, the equivalent CLI commands are **show sdwan control local properties** and **show sdwan control connections**.

Deploy

The deployment section is organized to cover the prerequisites, followed by the onboarding options and onboarding verification.

Process 1: Prerequisites for WAN Edge Onboarding

The below checklist showcases the prerequisites that are needed before proceeding with the WAN Edge onboarding process.

Procedure 1: Prerequisites for all Onboarding Options

Verify and validate the onboarding prerequisites that apply to all onboarding options.

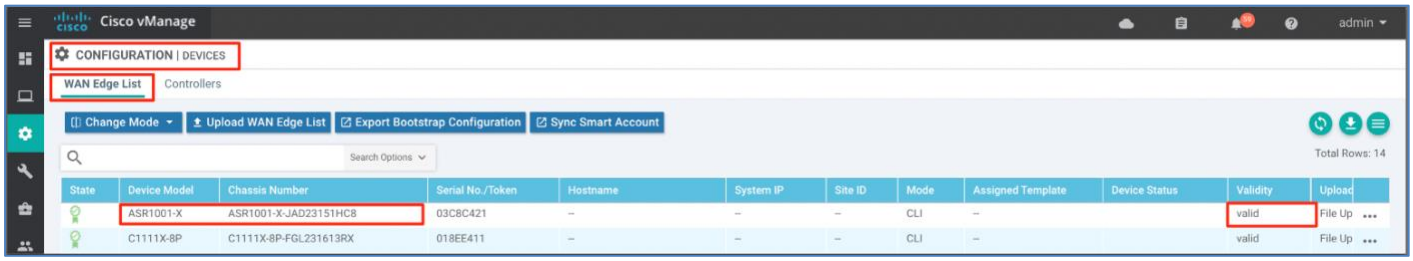
- Make sure the WAN Edge device has reachability to the vBond orchestrator, vManage and vSmart controllers.
- The authorized WAN Edge device whitelist must be uploaded to all SD-WAN controllers. This can be achieved by adding and associating the WAN edge devices with a vBond controller profile in the Plug and Play portal (PnP). The whitelist provision file can be downloaded from the PnP portal and uploaded to the vManage NMS or synchronized to the vManage via the **Sync Smart Account** option. vManage later distributes this whitelist to the additional controllers.

  Technical Tip: Software WAN Edge devices deployed in virtual environment do not have chassis or serial number. For such devices, PnP server generates a unique serial number when the software device is added in the PnP portal.

  For more information, refer to '**Appendix D — Cisco Plug-and-Play Connect**' to add the WAN Edge devices in the Plug-and-Play portal and '**Appendix E — WAN Edge whitelist Authorization File'** to upload or sync the whitelist authorization file to vManage.

- The WAN Edge device must be in **valid or staging** certificate state.

  In vManage, navigate to **Configuration** > **Devices** > **WAN Edge List**, identify the WAN Edge device and under the **Validity** column, verify the device is in either **valid** or **staging** state.



  Technical Tip: A WAN Edge device within staging state will establish only control connections with the SD-WAN controllers. No data plane connections are established across WAN Edge devices. To fully onboard the device, the device state must be moved from staging to valid. In vManage under **Configuration** > **Certificates > WAN Edge List,** select the WAN Edge device(s) and change the state to **valid** under the **Validity** column and click **Send to Controllers**.

- The WAN Edge device must be running SD-WAN software. For details on how to migrate from an IOS-XE code to IOS XE SD-WAN code, refer to **'Appendix H – Upgrading software to SD-WAN IOS-XE Software**'.

Procedure 2: Additional Prerequisites for Onboarding vEdge Devices using the ZTP Process

Verify and validate the additional onboarding prerequisites that apply to the ZTP process.

- The factory default vEdge router should be able to resolve the FQDN ztp.viptela.com and reach the ZTP server.
- The WAN Edge must be factory defaulted before onboarding using bootstrap option

Technical Tip: vEdge device can be factory defaulted if needed using the CLI command on the device **request software reset.**

- If using the **Cisco cloud-based ZTP server**, ensure the vEdge devices are entered in the PnP Connect portal and associated to the vBond controller profile at http://software.cisco.com. Devices entered in the PnP Connect portal are pushed out to the ZTP cloud server. If you are using enterprise root certificates and you want certificates pushed out during the ZTP process, ensure that the root CA certificate chain is uploaded to the PnP vBond controller profile, which is also pushed out to the ZTP cloud server.

  Refer to '**Appendix D — Cisco Plug-and-Play Connect**' to create vBond controller profile, add enterprise root certificates and procedure to associate the profile to WAN Edge.

- If using an **on-premise ZTP server**, the ZTP server should have entries of all the authorized vEdge devices with its vBond controller information, organization-name and optionally, enterprise root-ca certificates, before onboarding the device using the Zero-Touch-Provisioning process.

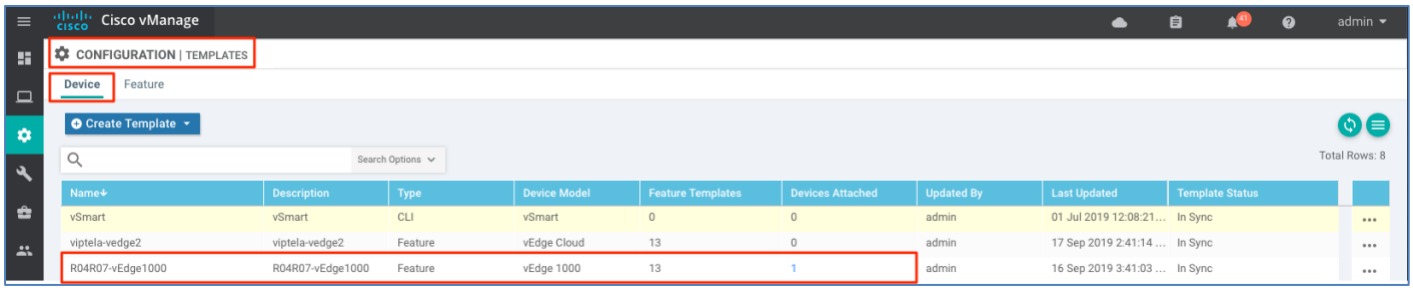
```
ZTP-Server# show ztp entries

                                                                                    ROOT
                      SERIAL                                  VBOND  ORGANIZATION   CERT
INDEX  CHASSIS NUMBER NUMBER    VALIDITY  VBOND IP            PORT   NAME           PATH
-------------------------------------------------------------------------------------------
5      11OG621194126J 1001F4FA  valid     10.4.246.71         12346  ENB-Solutions  default
```

  If you are using enterprise root certificates and you want certificates pushed out during the ZTP process, copy the certificate to the ZTP server and provide the path information in the ZTP entry device list. The vBond IP address and organization name along with the enterprise root-ca certificate is pushed and installed on the vEdge device during the ZTP device onboarding process. Refer to '**Appendix F – Zero Touch Provisioning Server**' to install and configure an on-premise ZTP server.

```
ZTP-Server# show ztp entries

                      SERIAL                                  VBOND  ORGANIZATION
INDEX  CHASSIS NUMBER NUMBER    VALIDITY  VBOND IP            PORT   NAME           ROOT CERT PATH
-------------------------------------------------------------------------------------------------
4      11OG621194126J 1001F4FA  valid     10.4.246.71         12346  ENB-Solutions  /home/admin/root-ca-chain.pem
```

- The WAN Edge configuration should be built and associated to the device in vManage NMS. Refer to **'Appendix G - SD-WAN Device Template**' for the feature and device templates used in this guide. For additional detailed information refer to the Cisco SD-WAN End-to-End Deployment Guide.

  In vManage, navigate to **Configuration > Templates** > **Device** and verify a device template is created and attached to the WAN Edge router. In this example, a device template is attached to vEdge1000 platform.

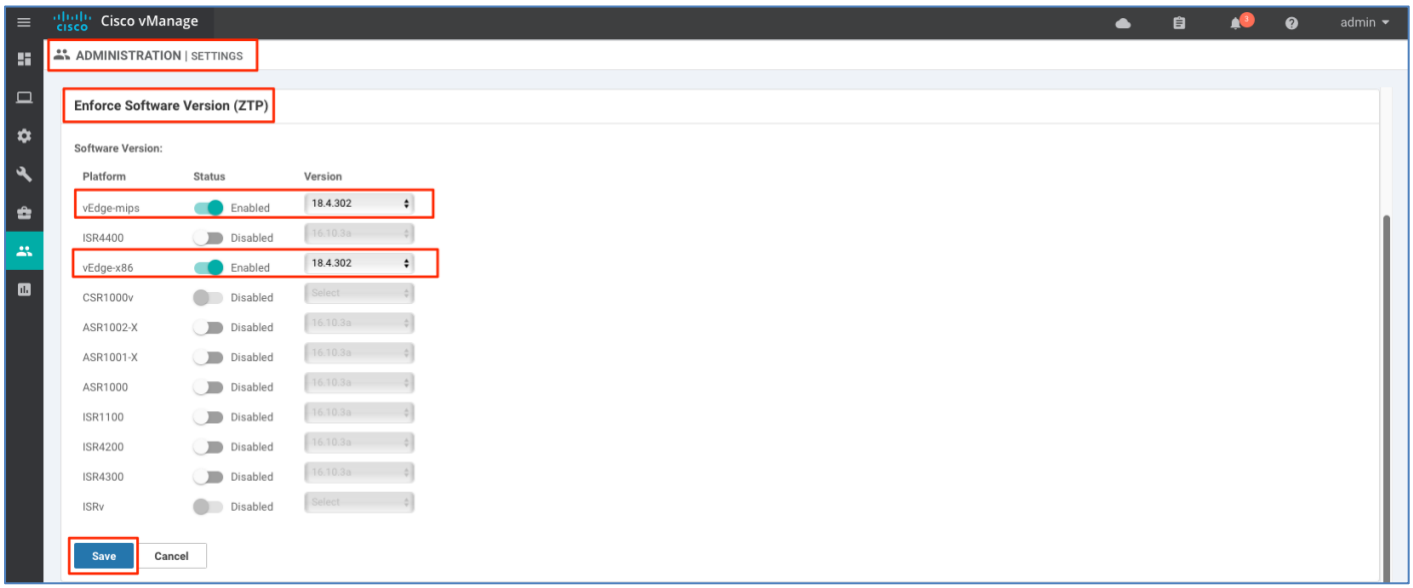


- The software version of a vEdge devices can be upgraded during the ZTP onboarding process. To perform the upgrade, upload the software in vManage and ensure the appropriate version is enabled for the platform in the vManage.

Refer to **'Appendix B — Upgrading software on SD-WAN'** for the procedure to load the software image to vManage.

In vManage, navigate to **Administration** > **Settings**. Next to **Enforce Software Version (ZTP)**, click **View** in the far right to verify the selected **Software Version** for each platform, along with the **Status.** To set the proper software version for the platform, click **Edit**, slide the **Status** bar to enable and choose the **Version** from the drop-down option and click **Save**.

Note: vEdge-x86 platform refers to vEdge Cloud device and for all physical vEdge devices choose vEdge-mips.



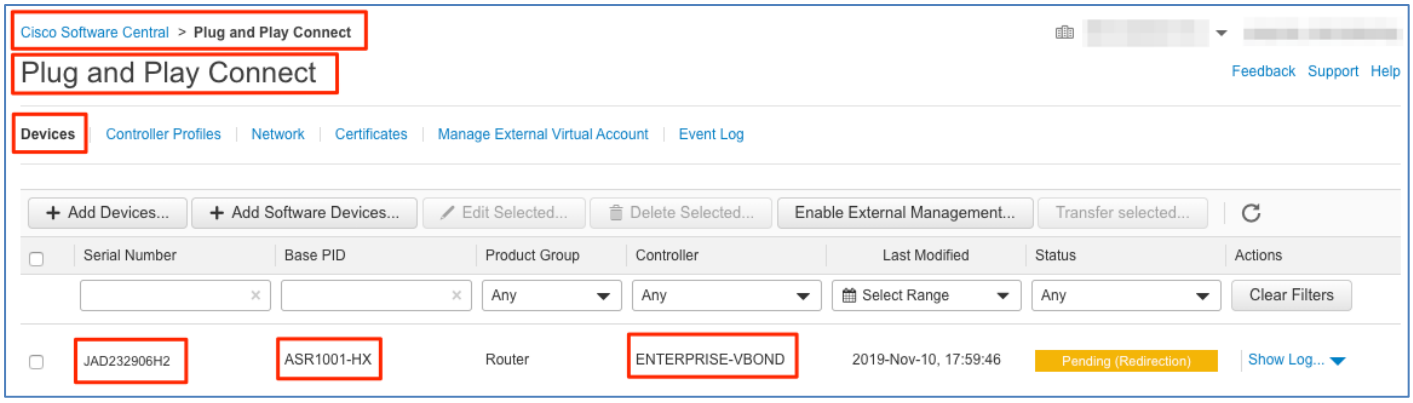
Procedure 3: Additional Prerequisites for onboarding IOS-XE SD-WAN WAN Edge devices using PnP process

- The factory default WAN Edge router should be able to resolve FQDN devicehelper.cisco.com and reach the Cisco cloud-hosted Plug-and-Play Connect server to retrieve the vBond controller information, organization-name and enterprise root-ca certificates (if using enterprise root-ca certificates).
- The WAN Edge must be factory defaulted before onboarding using bootstrap option.

Technical Tip: IOS-XE SD-WAN devices can be factory defaulted if needed using the CLI command on the device **request platform software sdwan software reset**

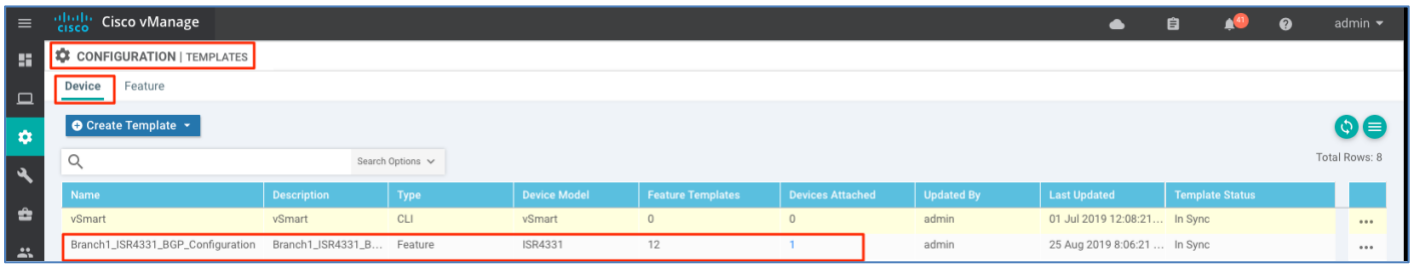
- The Cisco PnP Connect server at http://software.cisco.com must have the IOS-XE SD-WAN WAN Edge added and the device associated with the VBOND controller profile.

Navigate to **Cisco Software Central > Network Plug and Play > Plug and Play Connect > Devices**, verify the device is available with **Controller** Profile associated to it.



- The WAN Edge configuration should be built and associated to the device in vManage NMS. Refer to **'Appendix G - SD-WAN Device Template'** for the feature and device templates used in this guide. For additional detailed information refer to the Cisco SD-WAN End-to-End Deployment Guide.

  In vManage, navigate to **Configuration > Templates > Device** and verify a device template is created and attached to the WAN Edge router. In this example, a device template is attached to ISR4331 platform.



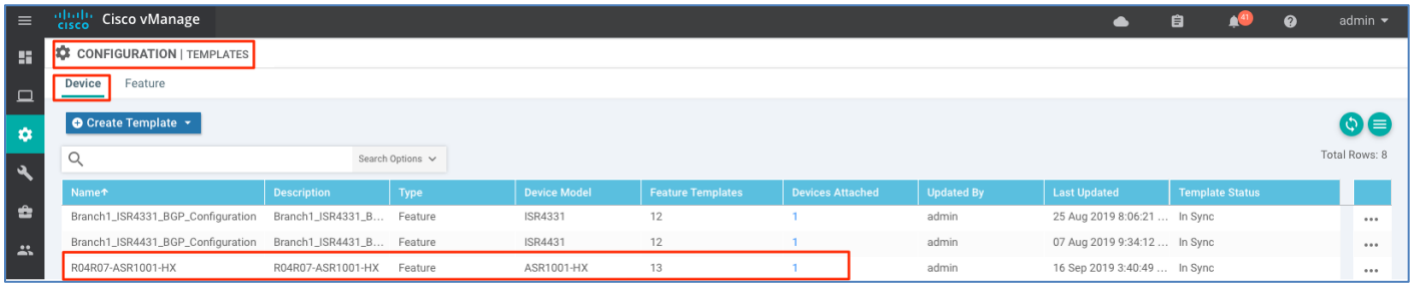
Procedure 4: Additional prerequisites for onboarding IOS-XE SD-WAN WAN Edge devices using bootstrap process

- The WAN Edge must be factory defaulted before onboarding using bootstrap option.

  Technical Tip: IOS-XE SD-WAN devices can be factory defaulted if needed using the CLI command on the device **request platform software sdwan software reset**.

- The WAN Edge configuration should be built and associated to the device in vManage NMS. Refer to **'Appendix G - SD-WAN Device Template'** for the feature and device templates used in this guide. For additional detailed information refer to the Cisco SD-WAN End-to-End Deployment Guide.

  In vManage, navigate to **Configuration > Templates > Device** and verify a device template is created and attached to the WAN Edge router. In this example, a device template is attached to ASR1001-HX platform.



Process 2: Onboarding vEdge devices

Cisco vEdge devices can be onboarded using one of the following onboarding options.

Zero-Touch-Provisioning: A day-zero automated ZTP process provides a simple, secure procedure to discover, install and provision vEdge devices to join the SD-WAN overlay network.

Manual Configuration: Onboard vEdge devices using manual configuration via console port or by using the KVM/ ESXi console connection.

Supported vEdge platforms include:

Table 6 vEdge WAN Edge onboarding options

Platform	Zero-Touch Provisioning	Manual
vEdge 100	✓	✓

vEdge 1000	✓	✓
vEdge 2000	✓	✓
vEdge 5000	✓	✓
vEdge cloud	✕	✓

Option 1: Automated deployment for vEdge device: Zero-Touch-Provisioning

In this option, the vEdge platform is initially onboarded into the SD-WAN overlay network via ZTP, followed by a code upgrade which is also optionally performed as a part of the ZTP process. Note, the factory-default WAN Edge device has the ZTP supported interface pre-configured with the '**ip dhcp-client**' command. Hence, the device dynamically procures an IP address and registers itself with the SD-WAN controllers.

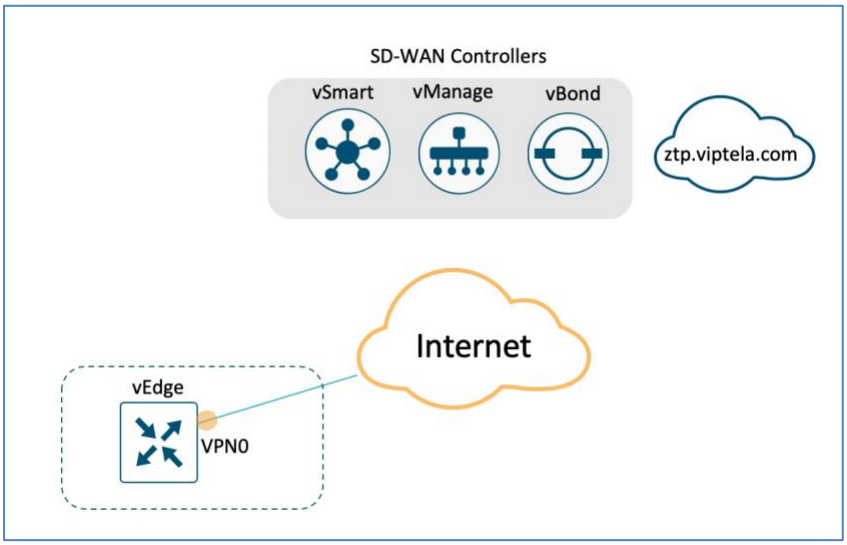
The following table lists the ZTP supported interfaces that can be leveraged to onboard devices with Zero-Touch Provisioning.

Table 7 vEdge platform - supported ZTP Interfaces

Platform	ZTP	Interface
vEdge 100, 100b	✓	ge0/4
vEdge 100m, 100wm	✓	ge0/4 Cellular0
vEdge 1000	✓	ge0/0
vEdge 2000	✓	ge2/0
vEdge 5000	✓	ge 0/0* *first port on the first available network slot

Procedure 1: Onboarding vEdge device using Zero-Touch-Provisioning

Step 1 Connect the ZTP-supported vEdge device interface to the WAN transport (typically Internet).



Step 2 Power on the vEdge router.

- Upon bootup, the device dynamically obtains ip-address, default-gateway, and DNS information through the DHCP process from the upstream WAN transport device.
- The vEdge device makes a DNS request to resolve ztp.viptela.com to the ZTP server.
- The vEdge device reaches the ZTP server and presents its chassis and serial number in order to authenticate with the server.
- Post authentication, the ZTP server provides information about the vBond orchestrator, organization-name and root certificates.

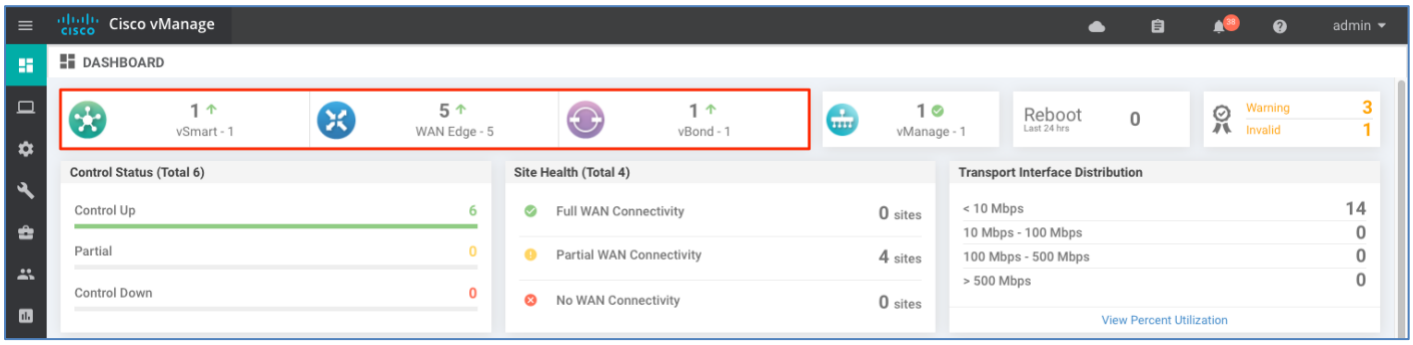
Technical Tip: For deployments using enterprise root-ca certificates, the device downloads the enterprise root CA certificate, , along with the vBond IP address/DNS and organization-name. This information is used by the vEdge WAN device to initiate control connections to the vBond controller.

- The vEdge device, on receiving the details from the ZTP server, tears down the control connection and initiates a transient connection to the vBond orchestrator.
- Following authentication with the vBond orchestrator, the vEdge device is provided with vManage and vSmart information to register and establish a secure connection.
- The device then attempts to establish a secure control connection with the vManage NMS. It is important to note that the device has no configuration and to build the connection, it uses 0.0.0.0 as the system-ip to bring up the initial control connection with the vManage.
- Post authentication, vManage responds to the vEdge with the device's System IP address and forces the device to re-authenticate using the shared system-ip information.
- The WAN Edge device then re-initiates control connections to all the SD-WAN controllers (vBond, vManage and vSmart controller) using the configured system-ip IP address in order to join the SD-WAN overlay network.
- If '**Enforce Software Version (ZTP)**' is enabled in vManage **Administration>Settings** with the version selected for the platform, the software is downloaded, and the device is upgraded.
- Upon loading the selected software version and re-authenticating with the SD-WAN controller, the vEdge device joins the SD-WAN overlay network.

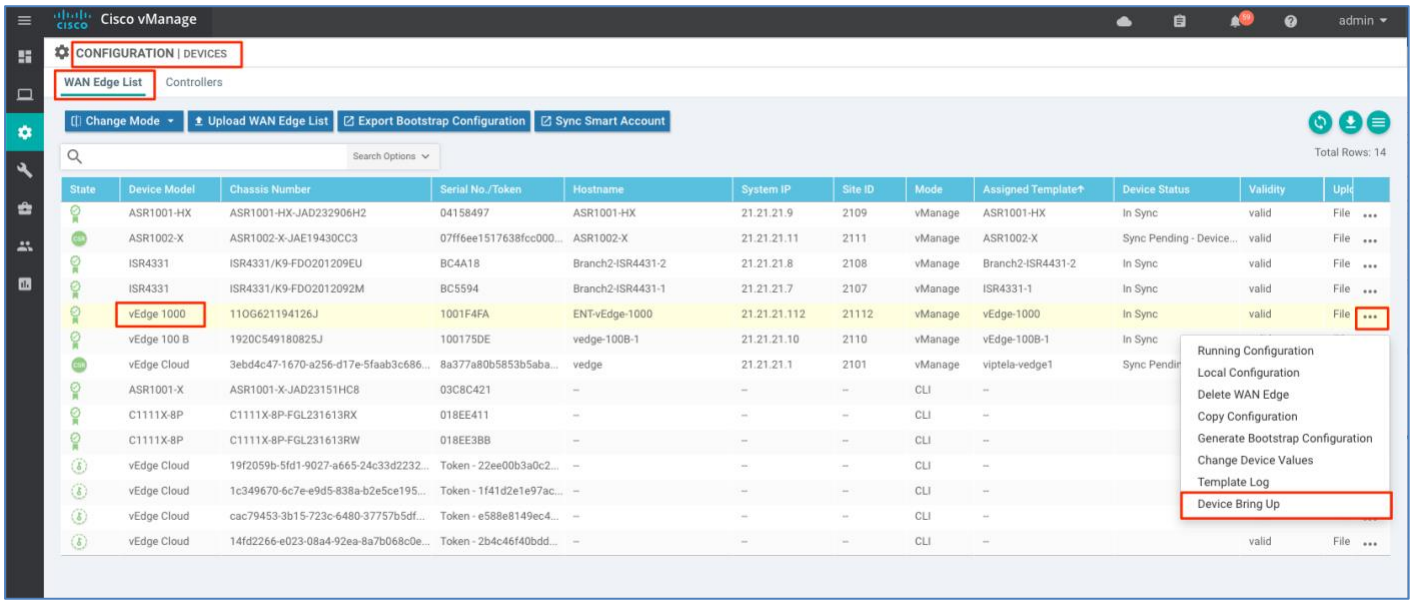
Procedure 2: Verify the onboarded vEdge devices using vManage NMS

Step 1 Verify the WAN Edge device is successfully onboarded via ZTP.

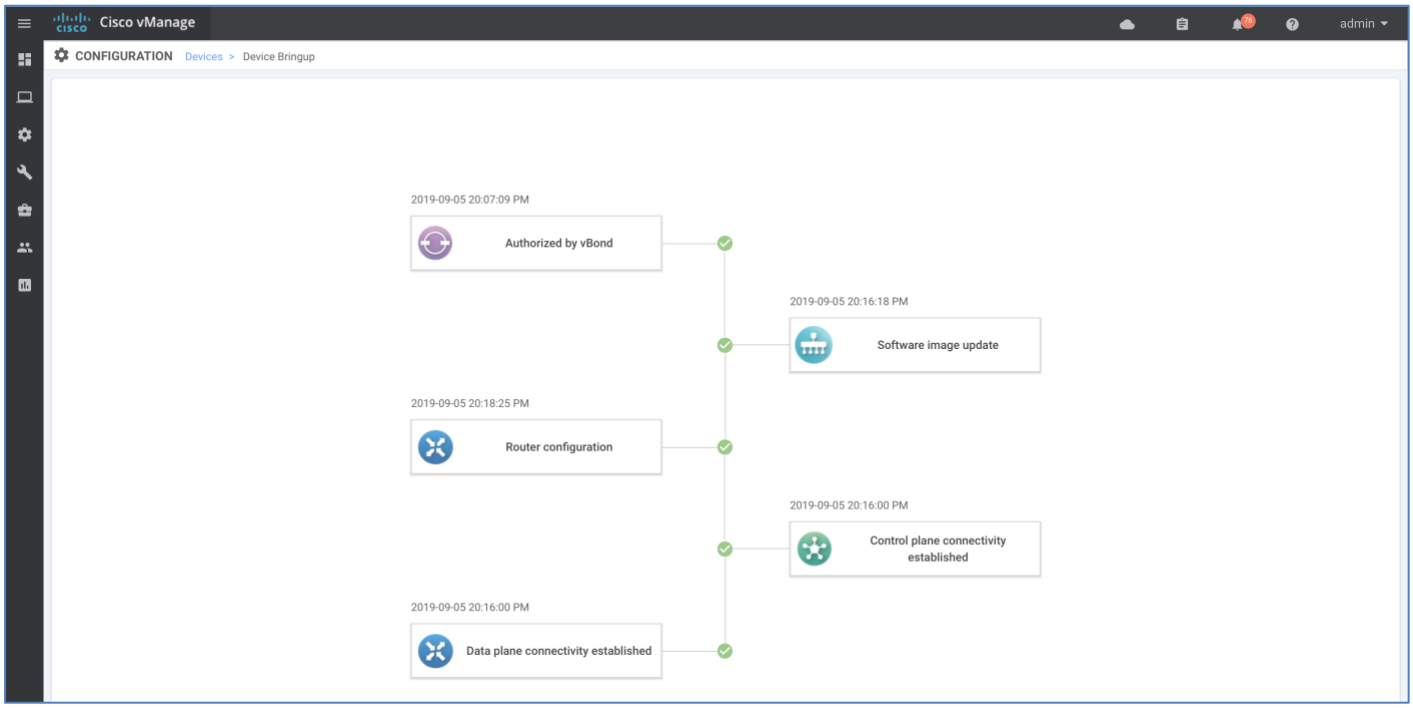
The Cisco vManage device pane dashboard provides a quick view and status of the number of WAN Edge devices onboarded in the Cisco SD-WAN overlay network.



- To view the entire device bring-up process, navigate to **Configuration > Devices**, choose the device from the **WAN Edge list** and click the three dots and select **Device Bring Up** from the options.



Make sure the device is **Authorized by vBond**, **Software image update** is successful, **Router configuration** is added, and finally ensure that the **control and data plane connectivity** is successfully established.



Option 2: Onboarding vEdge device with manual configuration

In this procedure, the vEdge is onboarded into the SD-WAN overlay network using the manual configuration process.

The minimal configuration that is needed to onboard the WAN Edge device includes **system parameters** (vBond, organization-name, system-ip, site-id) and **VPN 0** network information (interface IP address, routing protocol or default route, tunnel and encapsulation) providing connectivity to the SD-WAN controllers to authenticate and onboard the device into the SD-WAN overlay network. Optionally, a hostname and VPN 512 network information (interface IP address and routing protocol or default route) can be provided.

The below example shows the minimum configuration needed to establish control connections with the SD-WAN controllers. The command-line for the WAN Edge devices can be accessed through the management console interface on the physical platforms and through the virtual machine console for the virtual platforms. Note, the default credentials for all the SD-WAN WAN Edge devices is admin/admin and to save any newly added configurations within SD-WAN components, enter **commit and-quit** in configuration mode.

Procedure 1: Manually configure the vEdge device

Step 1 Configure the system parameters, that includes hostname**, system-ip**, **site-id**, **organization-name**, **vbond IP address/ DNS Name**.

```
system
host-name R04R07-vEdge1000
system-ip 21.21.21.12
site-id 21012
organization-name      "ENB-Solutions - 21615"
vbond 10.4.246.21
end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
```

Step 2 (Optional) Configure the out-of-band Management interface, VPN 512 with **ip-address** and **default route.**

```
vpn 512
interface mgmt0
ip address 100.119.112.31/24
no shutdown
exit
ip route 0.0.0.0/0 100.119.112.1
end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
```

Step 3 Configure the transport VPN 0 WAN interface to establish reachability to the SD-WAN controllers.

Configure the VPN 0 network interface with IP address, tunnel interface with encapsulation and color ,and routing (dynamic or default route). Only upon configuring the tunnel interface will the WAN Edge device use DTLS/TLS to establish the secure control plane connections to the SD-WAN controllers, and subsequently, IPSec to establish the secure data plane connections with the WAN Edge devices in the network.

```
vpn 0
interface ge0/1
ip address 10.5.208.62/30
no shut
tunnel-interface
encapsulation ipsec
color mpls
exit
!
ip route 0.0.0.0/0 10.5.208.61
end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
```

Note: If you are onboarding the vEdge cloud platform, continue to Procedure 2. If you are using Enterprise root CA certificates, skip to Procedure 3. To verify the device onboarding process, proceed to Procedure 4.

Procedure 2: Additional onboarding steps for vEdge Cloud platform

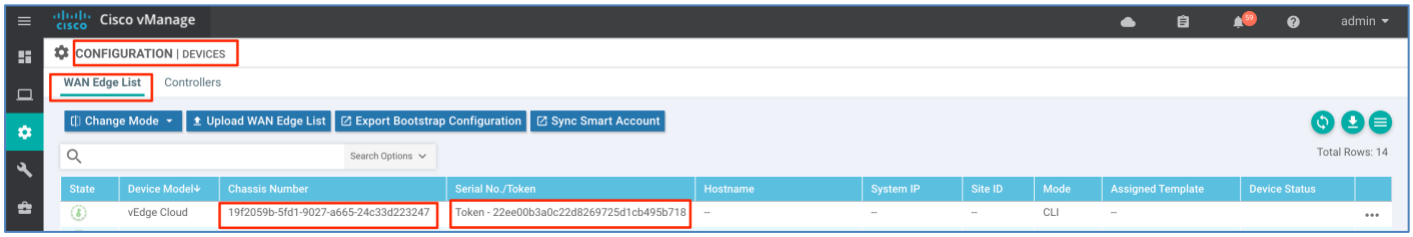
This additional step is required as the vEdge cloud contains no TPM chip, hence, no certificates are preinstalled, and no chassis-number associated to it. For such devices, PnP server generates a unique values when the device is added in the PnP portal and imported to vManage.

Refer to '**Appendix I – Install vEdge Cloud**' for detailed steps to deploy a vEdge Cloud in virtual environment if needed, '**Appendix D — Cisco Plug-and-Play Connect**' to add the WAN Edge devices in the Plug-and-Play portal and '**Appendix E — WAN Edge whitelist Authorization File'** to upload or sync the whitelist authorization file to vManage.

For the vEdge cloud platform to be authenticated, it is mandatory to associate the virtual device with **chassis-number** and **token** which is a **one-time-password**, generated by vManage when adding the device whitelist into the vManage device list.

Step 1 Locate the WAN device chassis number and token in the vManage.

In vManage, navigate to **Configuration > Devices > WAN Edge List,** identify any available **vEdge Cloud** device that is unassigned from the list and copy the **Chassis Number** and the **Serial No./Token** column.



Step 2 On the vEdge Cloud device CLI, issue the command **request vedge-cloud activate chassis-number** <**chassis-number**> **token** <**token-number**> to associate the chassis-number and the Serial No./Token (one-time password) to the vEdge cloud and to activate the device.

```
vedge#
vedge# vedge# request vedge-cloud activate chassis-number 19f2059b-5fd1-9027-a665-24c33d223247 token 22ee00b3a0c22d8269725d1cb495b718
```

The device uses the newly associated information (chassis-number and token), with the vBond and organization-name information to successfully authenticate and be a part of the SD-WAN overlay network.

Following the authentication for the first time using the one-time password, the vManage will generate a root CA certificate and unique serial number for the device, distribute it to the WAN Edge router and also update other SD-WAN controllers. From this point, any proceeding authentication that the vEdge-cloud performs uses the unique serial number and the installed certificate.

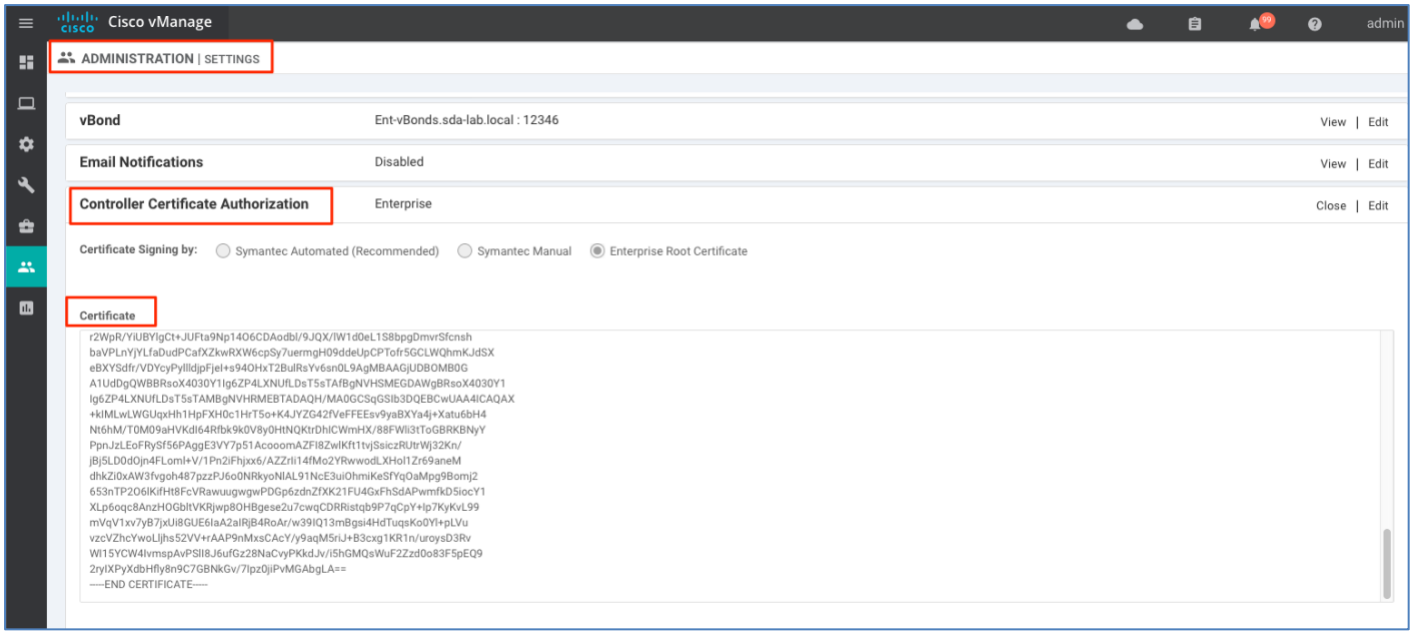
Note: If you are using Enterprise root CA certificates, proceed to Procedure 3, else to verify the device onboarding process, proceed to Procedure 4.

Procedure 3: Additional onboarding steps for vEdge physical platforms using Enterprise root-CA.

Deployment using enterprise root-ca certificate requires the installation of a trusted root-ca certificate on the device for successful authentication with the SD-WAN controller in order to join the SD-WAN overlay network.

Step 1 Download the Enterprise root-ca certificate from vManage.

In vManage, navigate to **Administration > Settings,** click **View** next to **Controller Certificate Authorization** and copy the **Certificate** to a file.



Step 2 Download the root certificate to the device on the MGMT interface using the CLI command – **request download vpn 512**.

```
vedge#
vedge# request download vpn 512 tftp://Admin:C1sco123@100.119.104.249/root-ca-chain.pem
vedge#
```

The root certificate file is downloaded to **/home/admin/ locatio**n on the vEdge, if you are logged in with the admin username. To view the file, login to the device shell by entering command **vshell.** To see the list of files, use the **ls** command. Use **exit** to return to the main mode.

```
vedge#
vedge# vshell
vedge:~$ ls -lrt
total 8
-rw-r--r-- 1 admin admin  392 Nov  8 23:19 archive_id_rsa.pub
-rw-r--r-- 1 admin admin 3968 Nov  8 23:46 root-ca-chain.pem
vedge:~$
vedge:~$ exit
exit
vedge#
```

Step 3 Install the root certificate using the CLI command **request root-cert-chain install /home/admin/root-ca-chain.pem**

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

Finally, verify the root-ca certificate is successfully installed on the vEdge platform via the CLI command **show certificate root-ca-cer**t.

```
vedge#
vedge# show certificate root-ca-cert | inc ENB
        Issuer: C=US, ST=NC, L=RTP, O=Cisco Systems Inc, OU=ENB Solutions, CN=sda-lab.local
        Subject: C=US, ST=NC, L=RTP, O=Cisco Systems Inc, OU=ENB Solutions, CN=sda-lab.local
        Issuer: C=US, ST=NC, L=RTP, O=Cisco Systems Inc, OU=ENB Solutions, CN=sda-lab.local
        Subject: C=US, ST=NC, L=RTP, O=Cisco Systems Inc, OU=ENB Solutions, CN=sda-lab.local
vedge#
```

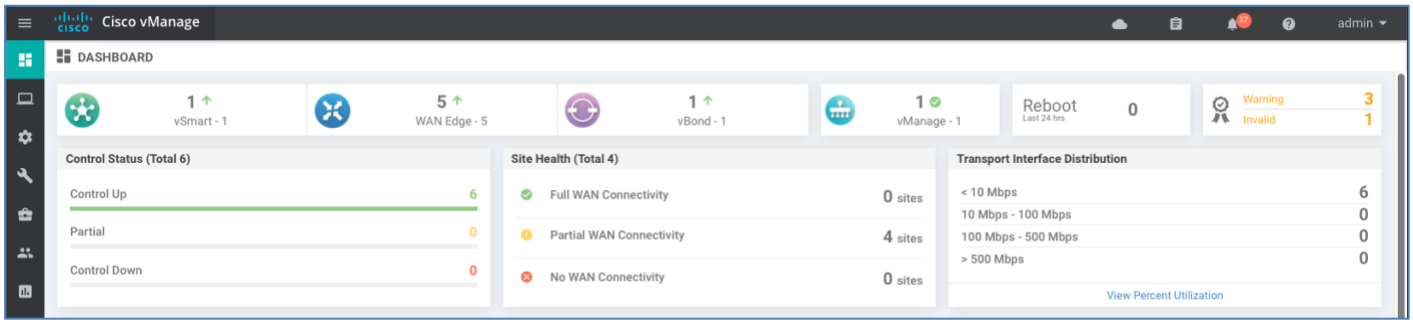
Upon establishing secure control connection with the vManage, the device template is attached to the WAN Edge and overwrites the existing basic configuration.

Note: To verify the device onboarding process proceed to **Procedure 4**.

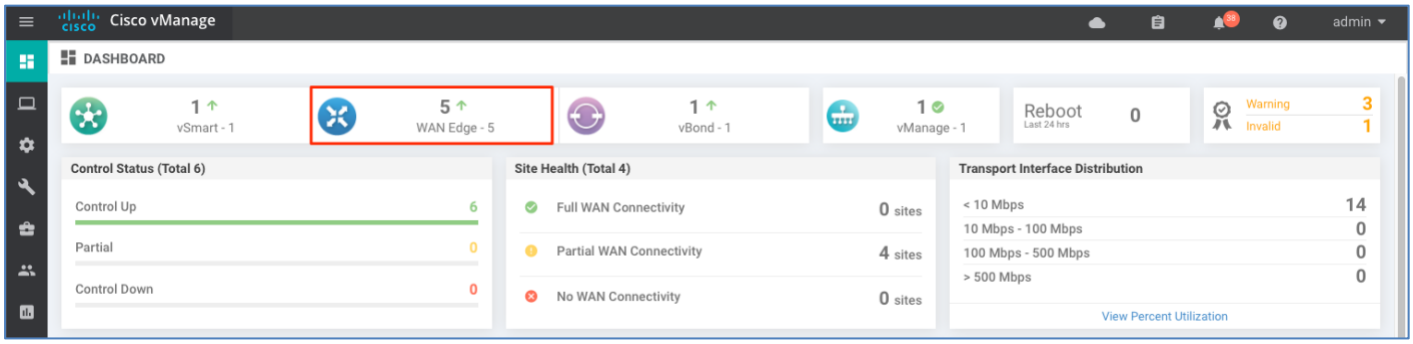
Procedure 4: Verify the WAN Edge device is successfully onboarded

This procedure section walks through the verification steps to verify the onboard process

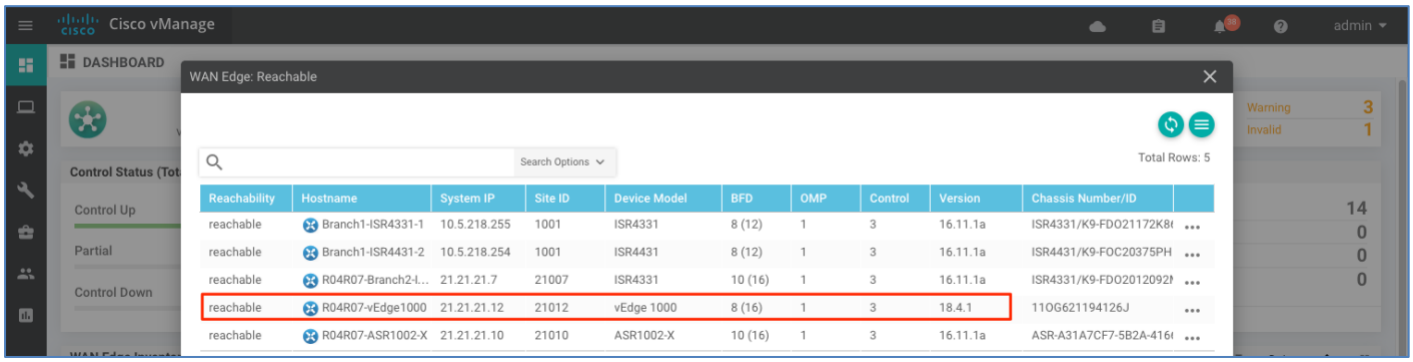
Step 1 The Cisco vManage dashboard provides a quick view and status of the number of WAN Edge devices onboarded onto the Cisco SD-WAN overlay network.



Step 2 Verify the WAN Edge details from the vManage dashboard. Click the **WAN Edge** section in the vManage overview section.

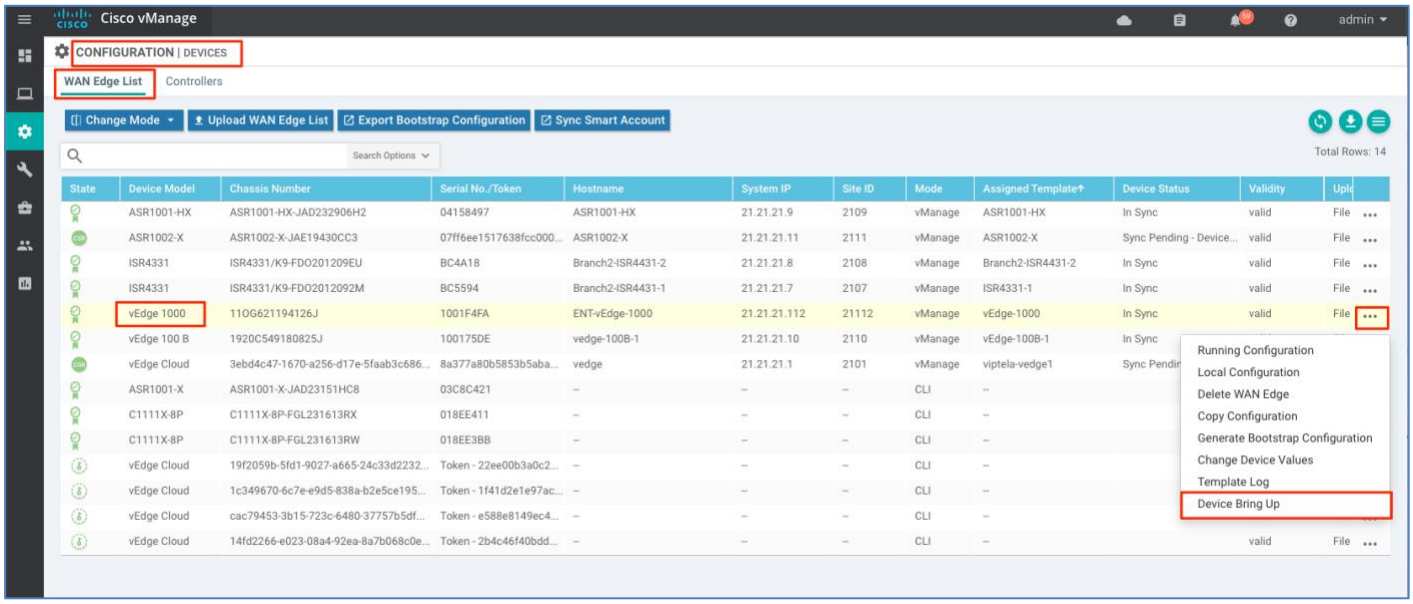


Identify the device and verify the **Reachability** and **Version** status for the platform.

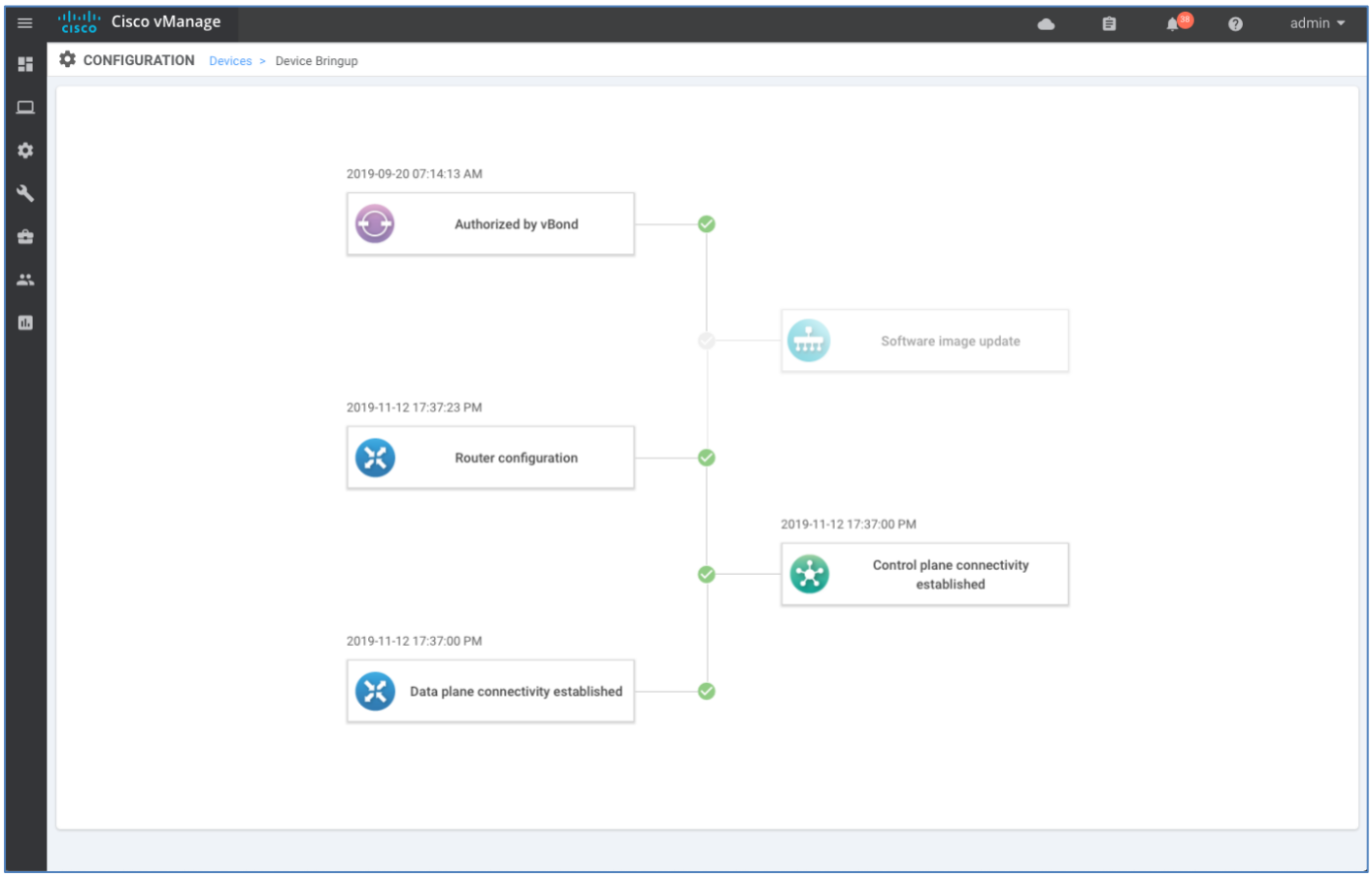


Technical Tip: If a software upgrade needs to be performed on the onboarded vEdge device, Refer to '**Appendix B — Upgrading software on SD-WAN device**' for detailed steps.

Step 3 To view the entire device bring-up process, navigate to **Configuration > Devices**, choose the device from the **WAN Edge list** and click the three dots and select **Device Bring Up** from the options.



Make sure the device is **Authorized by vBond** is successful, **Router configuration** is added, and finally ensure that the **control and data plane connectivity** is successfully established.



Process 3: Onboarding Cisco IOS-XE SD-WAN devices

Cisco IOS-XE SD-WAN WAN Edge devices can be onboarded using one of the following onboarding options:

Plug-and-Play: The day-zero automated Plug-and-Play process provides a simple, secure procedure to discover, install and provision the Cisco IOS-XE SD-WAN Edge device to join the SD-WAN overlay network.

Bootstrap: The bootstrap method helps onboard a factory-shipped WAN Edge device with the configuration needed to securely onboard and join the SD-WAN Network, when a customer is unable to leverage the automated discovery option.

Manual Configuration: Onboard IOS-XE SD-WAN devices using manual configuration via the console port.

Supported Cisco IOS-XE SD-WAN WAN Edge platforms include,

Table 8 Cisco IOS-XE SD-WAN WAN Edge onboarding options

Platform	Plug-and-Play	Bootstrap	Manual
ASR1K	✓	✓	✓
ASR1002-X	×	✓	×
ISR4K	✓	✓	✓
ISR1K	✓	✓	✓

Option 1: Automated deployment for IOS-XE SD-WAN WAN Edge device with Plug-and-Play process

In this option, the IOS-XE SD-WAN WAN Edge is initially onboarded into the SD-WAN overlay network via the PnP process.

Note, the factory default IOS-XE SD-WAN WAN Edge device has its PnP supported interfaces preconfigured with **'ip address dhcp client-id GigabitEthernet x/x/x**. Hence, the device dynamically procures an IP address and registers itself with the SD-WAN controllers.

The following table lists the PnP supported interfaces that can be leveraged to onboard devices using the Plug-and-Play automated deployment option.

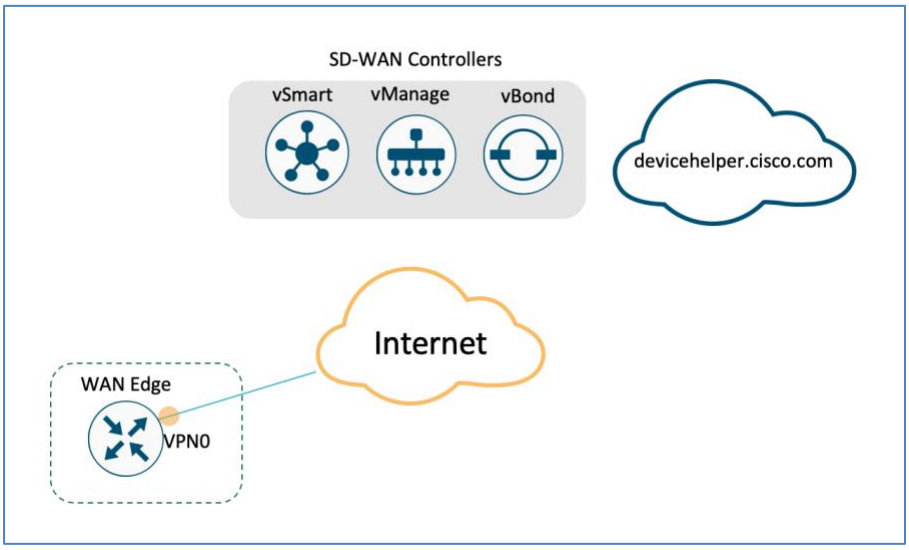
Table 9 IOS-XE SD-WAN platform – supported PnP Interfaces

Platform	Plug-and-Play	Interface
ASR1K	✓	GigabitEthernet (routed interface)
ASR1002-X	×	NA
ISR1K	✓	GigabitEthernet (routed interface) Cellular
ISR4K	✓	GigabitEthernet (routed interface) Cellular
CSR1K	×	NA

Technical-Tip: The ASR1002-X doesn't support the Plug-and-Play automated deployment option. To onboard this platform, leverage the bootstrap option to join the SD-WAN overlay network.

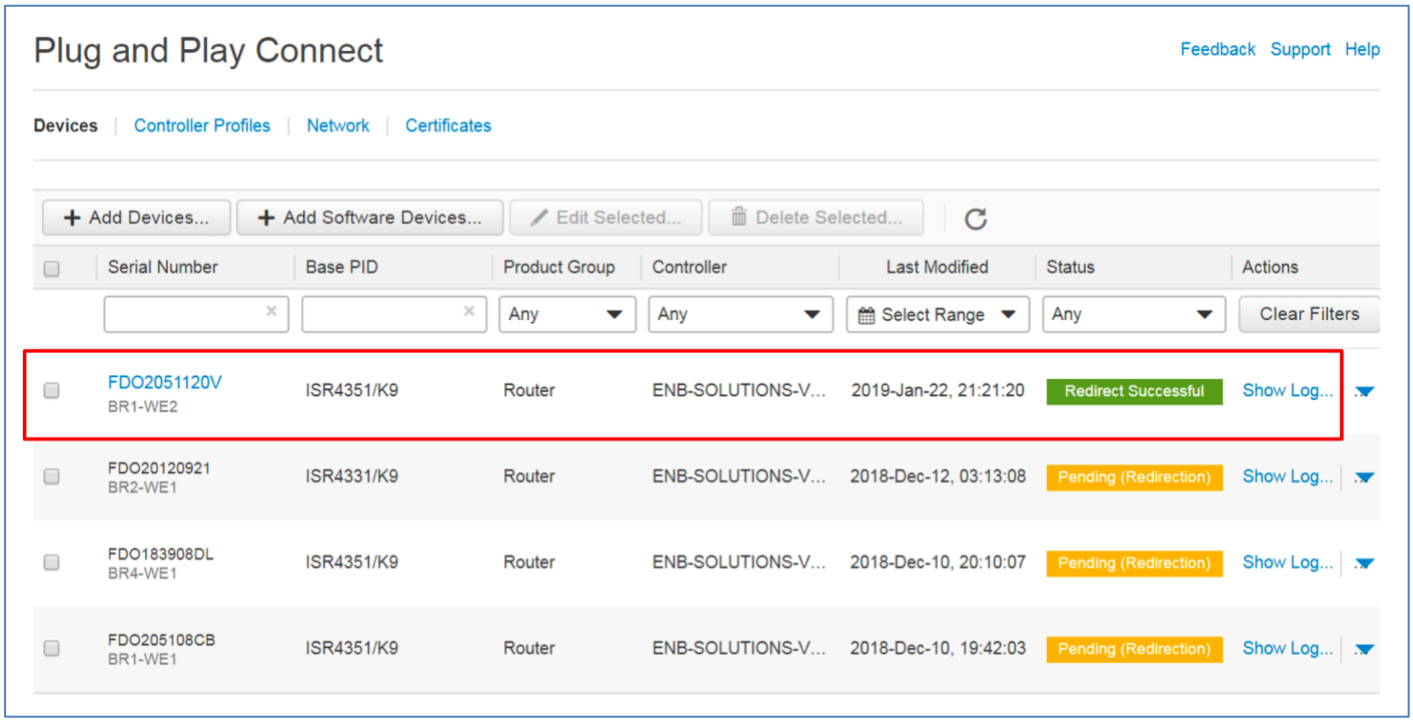
Procedure 1: Onboarding IOS-XE SD-WAN device using Plug-and-Play process

Step 1 Connect the PnP supported interface to the WAN transport (typically Internet).



Step 2 Power on the IOS-XE SD-WAN router.

- Upon bootup, the device dynamically obtains ip-address, default-gateway, and DNS information through the DHCP process from the upstream WAN transport device.
- The WAN Edge device makes a DNS request to resolve devicehelper.cisco.com to the ZTP server.
- The WAN Edge device reaches the Cisco cloud hosted PnP Connect server and presents its chassis and serial number in order to authenticate with the server.
- Upon authentication, the PnP connect portal provides information about the vBond orchestrator, organization-name and root certificates.
- Technical Tip: For deployments using enterprise root-ca certificate, device downloads the enterprise root CA certificate, along with the vBond IP address/DNS and organization-name using the HTTPS protocol. This information is used by the IOS-XE SD-WAN WAN Edge device to initiate control connections with the vBond controller.
- At this stage, the PnP portal indicates a **Redirect Successful** status when the WAN Edge device is redirected through PnP to the vBond controller, below is an example for ISR4351device being redirected successfully.

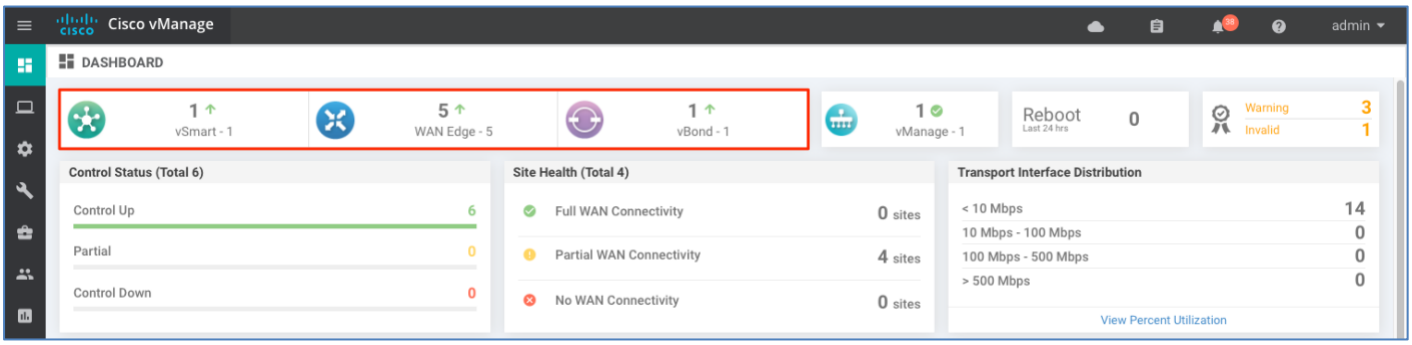


- Following authentication with the vBond orchestrator, the WAN Edge is provided with vManage and vSmart information to register and establish a secure connection.
- The device then attempts to establish a secure control connection with the vManage NMS. It is important to note that the device has no configuration and to build the connection it uses 0.0.0.0 as the system-ip to bring up the initial control connection with the vManage.
- Upon authentication, vManage responds to the vEdge with the device's system IP and forces the device to re-authenticate using the shared system-ip information.
- The WAN Edge device then re-initiates control connections to all the SD-WAN controllers (vBond, vManage and vSmart controller) using the configured system-ip IP address in order to join the SD-WAN overlay network.

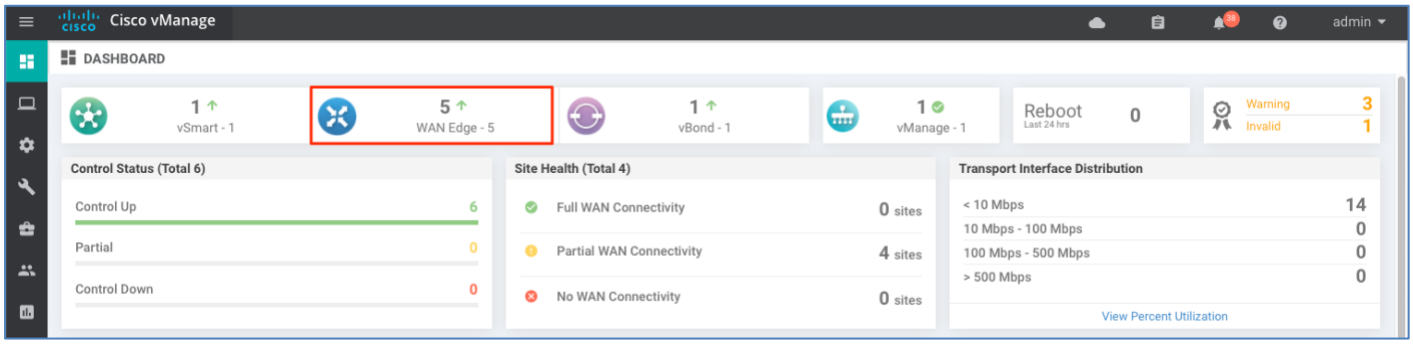
Procedure 2: Verify the onboarded WAN Edge devices using vManage NMS

Step 1 Verify the WAN Edge device is successfully onboarded via PnP.

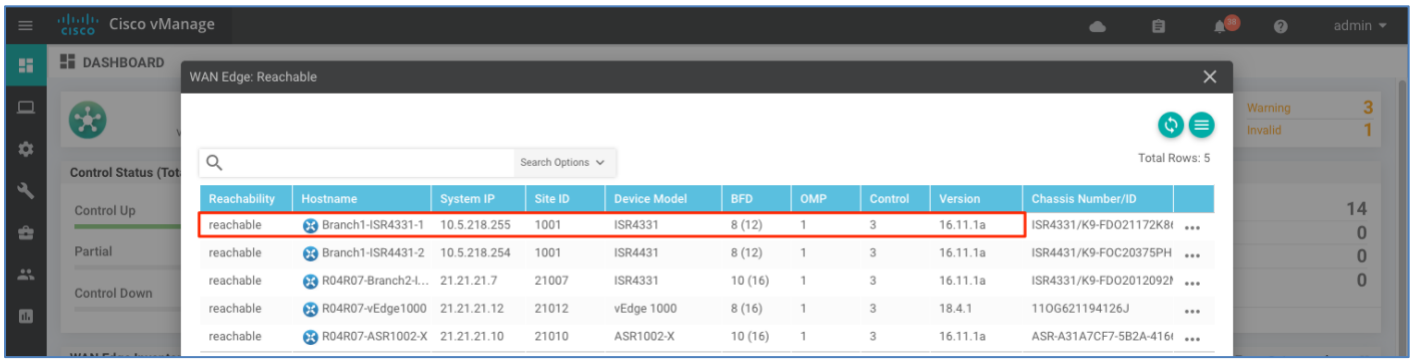
The Cisco vManage device pane dashboard provides a quick view and status of the number of WAN Edge devices onboarded in the Cisco SD-WAN overlay network.



- Verify the WAN Edge details from the vManage dashboard, click the **WAN Edge** section from the device pane in the vManage overview section.

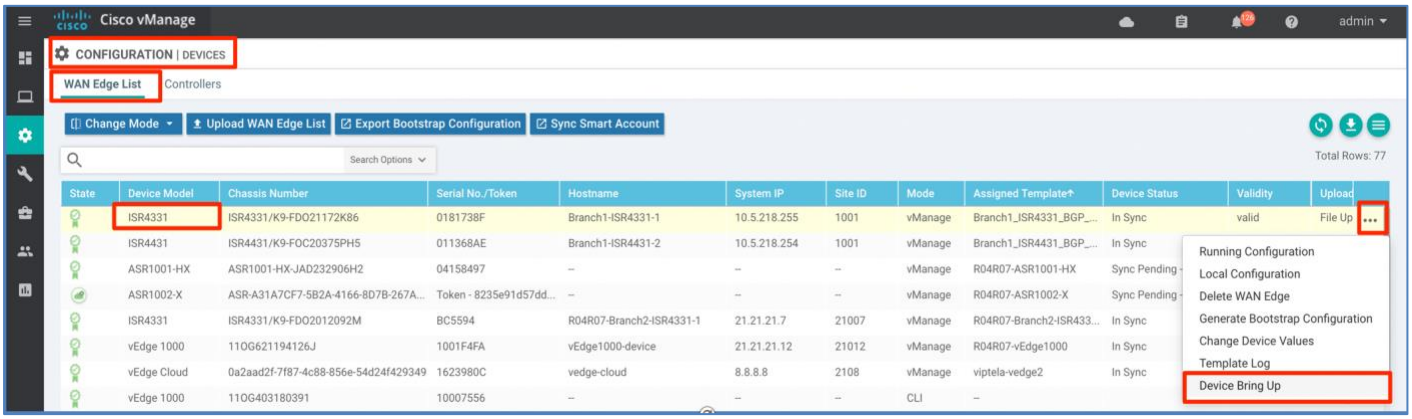


Identify the device and verify the **Reachability** and **Version** status for the platform.

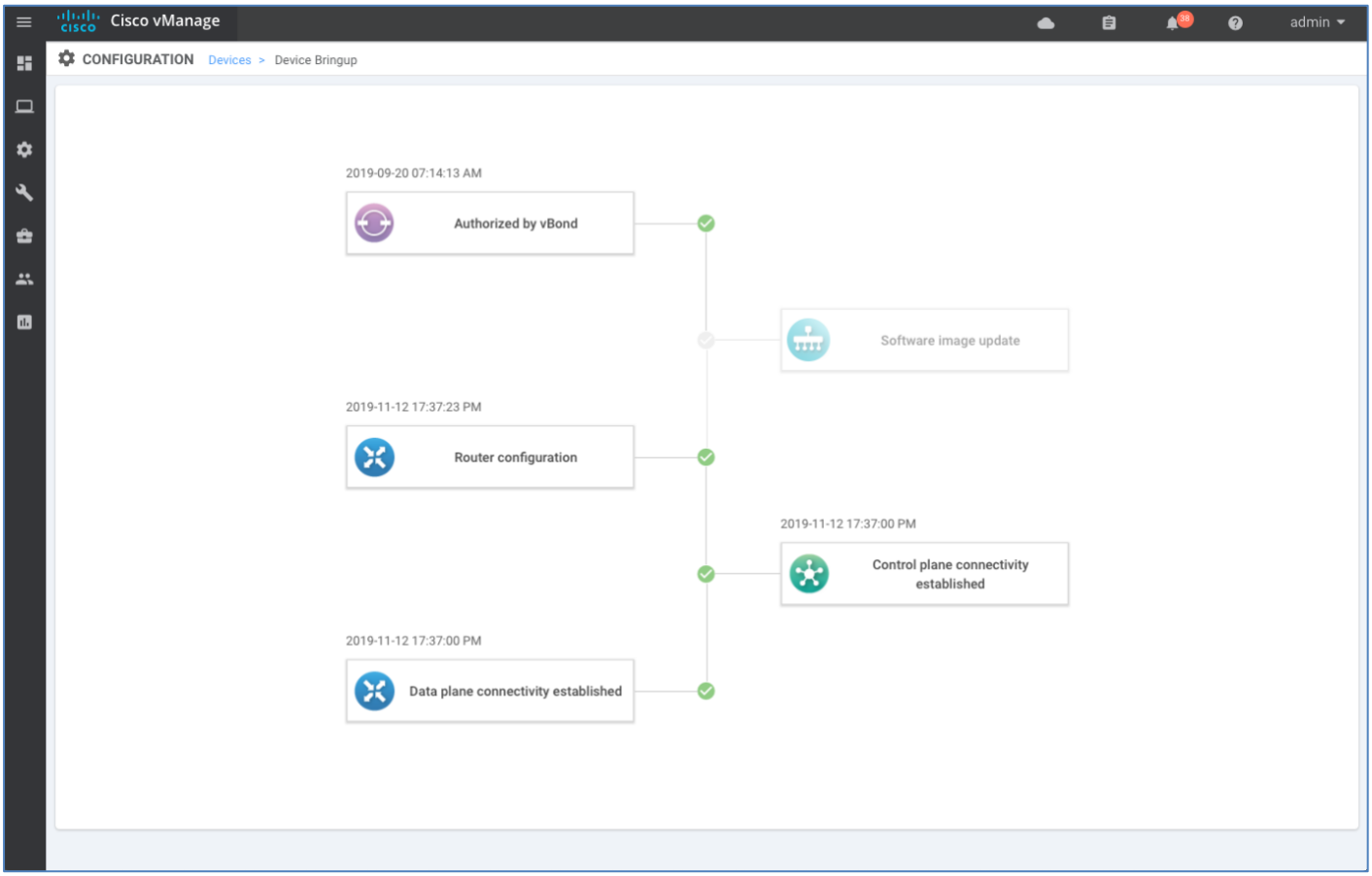


Technical Tip: If a software upgrade needs to be performed on the onboarded IOS XE SDWAN device, Refer to '**Appendix B — Upgrading software on SD-WAN device**' for detailed steps.

To view the entire device bring-up process, navigate to **Configuration > Devices**, select the device from the **WAN Edge list** and choose the three dots. Next, select **Device Bring Up.**



Make sure that **Authorized by vBond** is successful, **Router configuration** is added, and finally ensure that the **control and data plane connectivity** is successfully established.



Option 2: Onboarding Cisco IOS-XE SD-WAN WAN device with Bootstrap deployment option.

In this option, the IOS-XE SD-WAN WAN Edge is onboarded into the SD-WAN overlay network using the bootstrap process.

Note, the factory default WAN Edge device has no configuration on the device. Upon bootup, the Plug-and-Play process running on the WAN Edge device looks for a file that contains device configuration. At first, the device looks for the file in the bootflash, and if not found then searches in a bootable USB drive (if available). If the configuration file is found, the device would load the configuration to the device as part of Plug-and-Play process.

This onboard option is recommended when the device is connected to a private WAN transport (MPLS) that cannot provide a dynamic IP address or when no Internet access is available to reach the Plug and Play Connect server, or when a WAN interface needs additional configuration before achieving connectivity (PPPoE or a subinterface, for example).

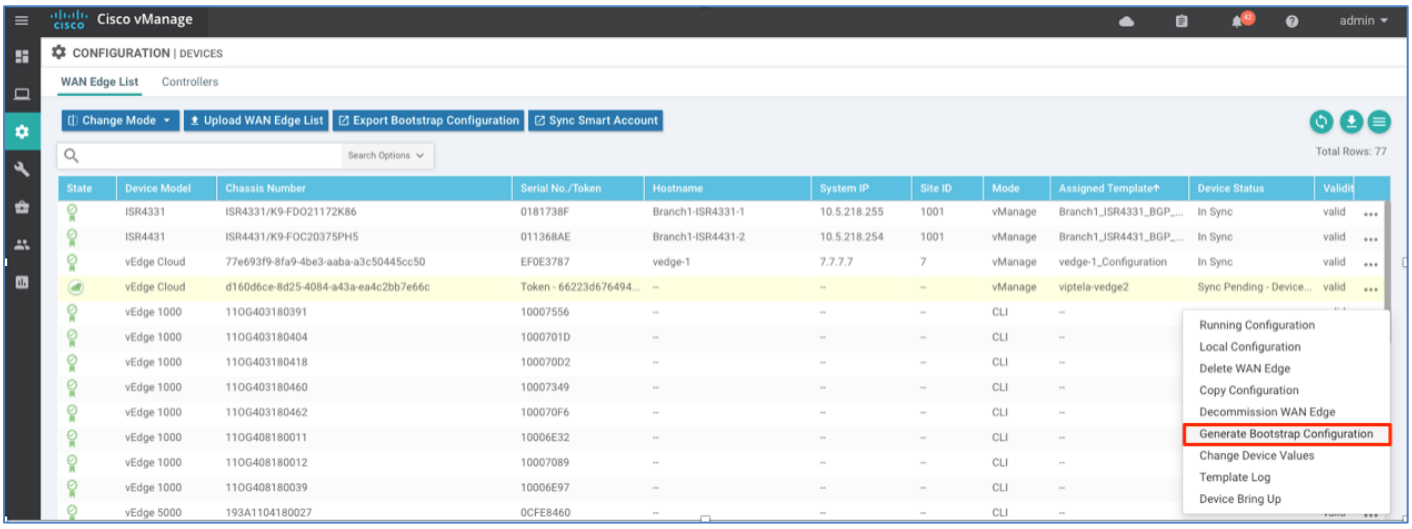
The WAN Edge could be either pre-staged before being brought to the install site, or the bootstrap configuration can be loaded onto a USB key and inserted into a WAN Edge at the install site.

The bootstrap workflow includes generating the configuration file for the device from the vManage NMS, copying and sharing the configuration file to the device's internal bootflash or to USB drive attached to device and, booting the device.

Procedure 1: Bootstrap onboarding procedure for Cisco IOS-XE SD-WAN

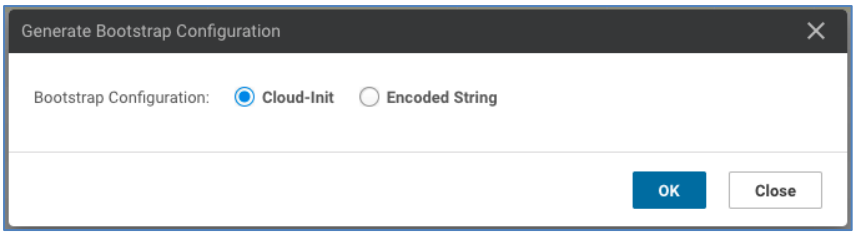
Step 1 Generate the bootstrap configuration.

In vManage, navigate to **Configuration > Devices** > **WAN Edge** to the right of the desired device, click the three dots and choose **Generate Bootstrap Configuration** from the drop-down list.

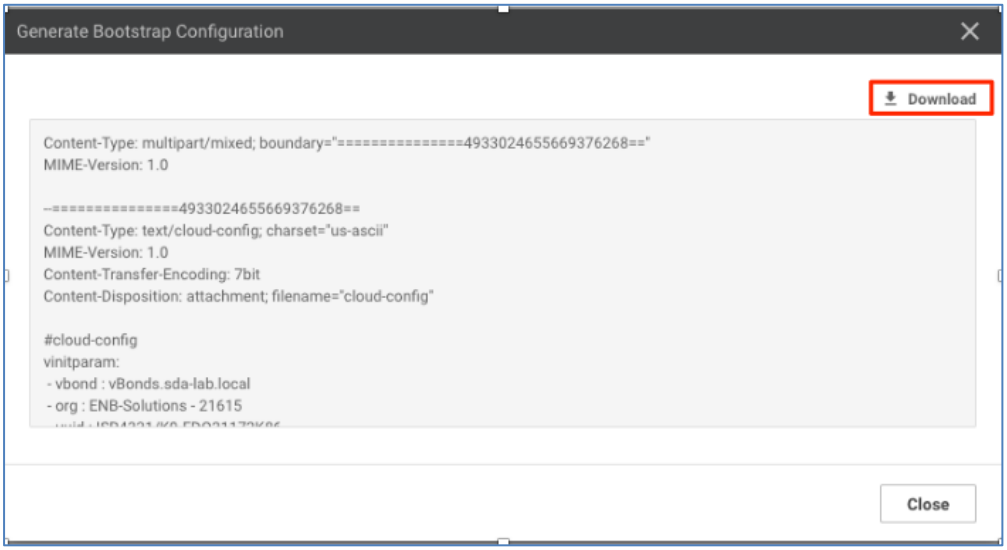


In the next few steps, the configured device template is downloaded into a local workstation.

Step 2 To begin the download of the configuration file, select the radio button **Cloud-Init** and click **OK**.



Step 3 The configured **Device template** populates the **Generate Bootstrap Configuration** screen. Click **Download** to the download the populated configuration into your local workstation.



The downloaded bootstrap file will be in the format - **<chassis_number>.cfg.** The configuration file consists of system properties (UUID, root CA certificate, vBond IP/DNS and Organization information) and configuration from the attached feature templates.

Step 4 Rename the downloaded configuration file to one of the filenames listed in the table below. Choose the filename depending on the WAN Edge platform that is to be onboarded.

Platform	Bootstrap	Configuration filename
ASR1K	✓	ciscosdwan.cfg
ISR1K	✓	
ISR4K	✓	
ASR1002-X	✓	ciscosdwan_cloud_init.cfg

Technical Tip: ASR1002-X WAN Edge devices do not have a SUDI certificate installed. To validate the device, the vManage generated cloud_init bootstrap configuration contains one-time-password (OTP) information along with other system properties (UUID, root CA, vBond and Organization name information) that is leveraged to authenticate and establish secure control connections with the controllers.

Step 5 After the filename is changed, copy the configuration file to the device bootflash. CLI command ***copy usb0:ciscosdwan.cfg bootflash*** can be used to copy the bootstrap config to WAN Edge device.

```
Router#
Router#copy usb0:ciscosdwan.cfg bootflash:
```

Alternatively, copy the configuration file to a bootable USB drive and attach the USB to the device.

Technical Tip: In case that the WAN Edge device has a config file in both bootflash and also in bootable USB drive connected to the device, internal bootflash is prioritized.

Step 6 Power on the WAN Edge device.

On IOS-XE SD-WAN WAN Edge device boot up, the device searches for the configuration file in the device bootflash or bootable USB drive. Once the file is located, the device will abort the PnP process and load the bootstrap configuration file.

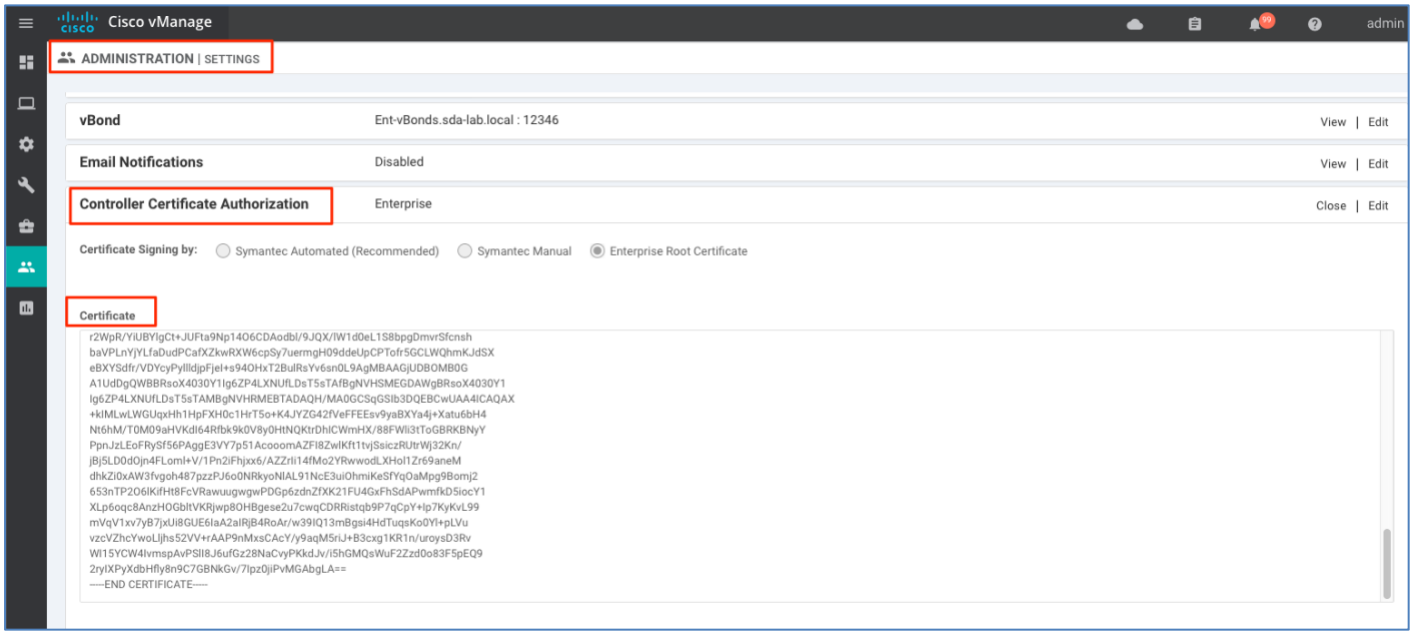
Note: Additional procedure is needed to onboard the WAN Edge device using Enterprise root CA certificate, for steps continue to **Procedure 2** and to verify the device onboarding process proceed to **Procedure 3**.

Procedure 2: Additional onboarding steps for IOS-XE WAN Edge platform using Enterprise root-ca certificate

Some additional steps are required to onboard IOS-XE SD-WAN WAN Edge platform using an enterprise root-ca certificate in addition to Procedure 1 discussed earlier. Deployment using enterprise root-ca certificate requires the installation of a trusted root-ca certificate on the device for successful authentication with the SD-WAN controller in order to join the SD-WAN overlay network.

Step 1 Download the Enterprise root-ca certificate from vManage.

In vManage, navigate to **Administration > Settings,** click **View** next to **Controller Certificate Authorization** and copy the **Certificate** to a file.



Step 2 Download the root-certificate on the WAN Edge device.

To copy the root-certificate onto the device, use the CLI command **copy tftp://username:password@WAN-Edge-VPN0-IP-Address/root-ca-chain.pem bootflash:root-ca-chain.pem vrf Mgmt-intf**

```
copy tftp://Admin:C1sco123@10.4.250.249/root-ca-chain.pem bootflash:root-ca-chain.pem vrf Mgmt-intf
```

Alternatively, copy the certificates into a USB and load it to device's bootflash.

Step 3 Install the root-certificate on the WAN Edge device.

To install the root-certificate on the device, use the CLI command **request platform software sdwan root-cert-chain install bootflash:root-ca-chain.pem**

```
request platform software sdwan root-cert-chain install bootflash:root-ca-chain.pem
```

Step 4 Finally, verify the root-ca certificate is successfully installed on the WAN platform via the CLI command **show sdwan certificate root-ca-cert**.

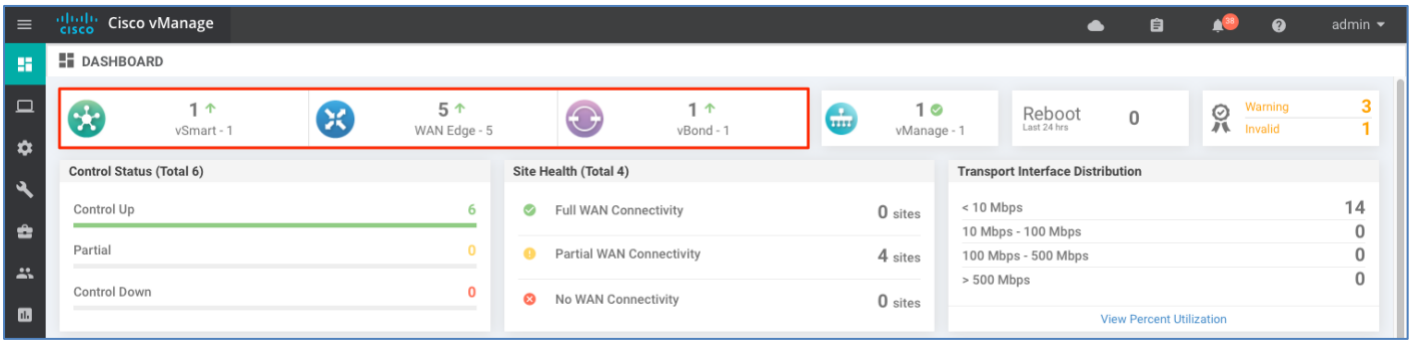
```
Branch2-ISR4331-1#sh sdwan certificate root-ca-cert | inc ENB
      Issuer: C=US, ST=NC, L=RTP, O=Cisco Systems Inc, OU=ENB Solutions, CN=sda-lab.local
      Subject: C=US, ST=NC, L=RTP, O=Cisco Systems Inc, OU=ENB Solutions, CN=sda-lab.local
      Issuer: C=US, ST=NC, L=RTP, O=Cisco Systems Inc, OU=ENB Solutions, CN=sda-lab.local
      Subject: C=US, ST=NC, L=RTP, O=Cisco Systems Inc, OU=ENB Solutions, CN=sda-lab.local
```

Once enterprise root-ca certificates are installed on the device, the WAN Edge device is authenticated (using organization-name, and whitelist chassis/serial device list) and authorized to join the SD-WAN overlay network.

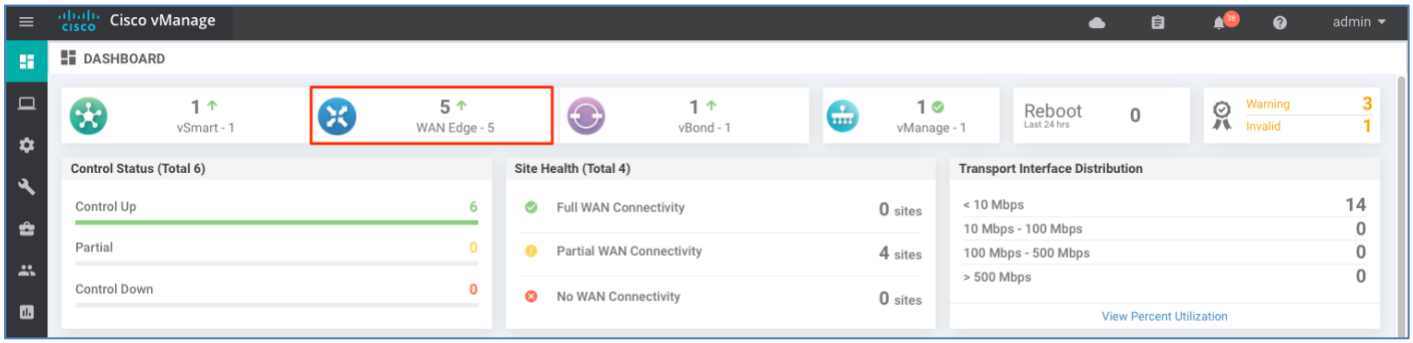
Note: To verify the device onboarding process proceed to Procedure 3.

Procedure 3: Verify the WAN Edge device is successfully onboarded

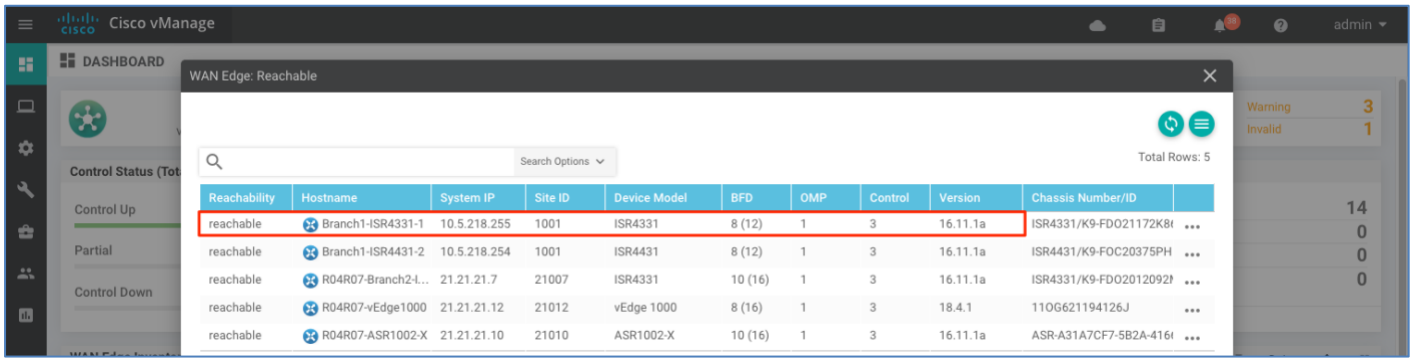
The Cisco vManage device pane dashboard provides a quick view and status of the number of WAN Edge devices onboarded in the Cisco SD-WAN overlay network.



- Verify the WAN Edge details from the vManage dashboard, click the **WAN Edge** section from the device pane in the vManage overview section

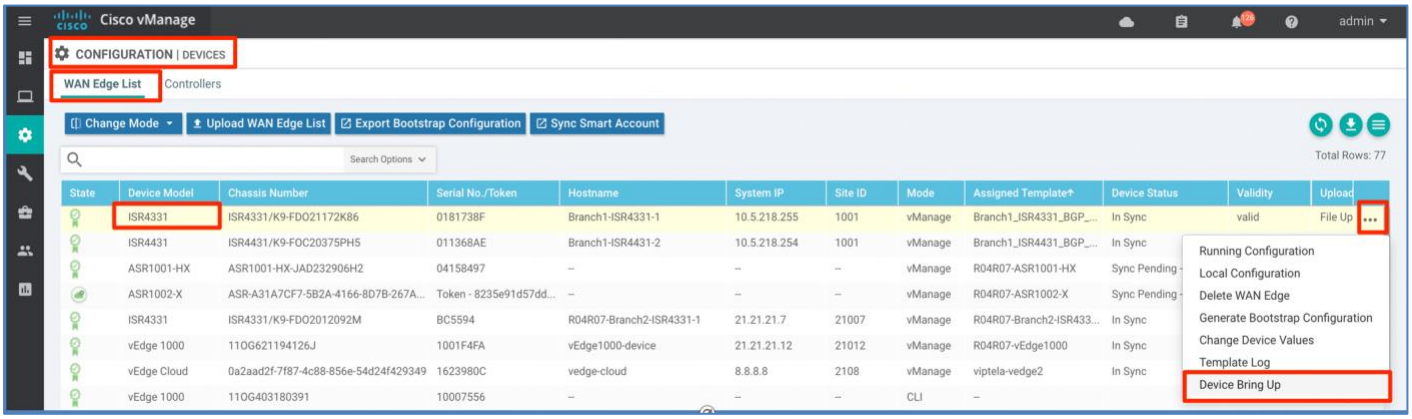


Identify the device and verify the **Reachability** and **Version** status for the platform.

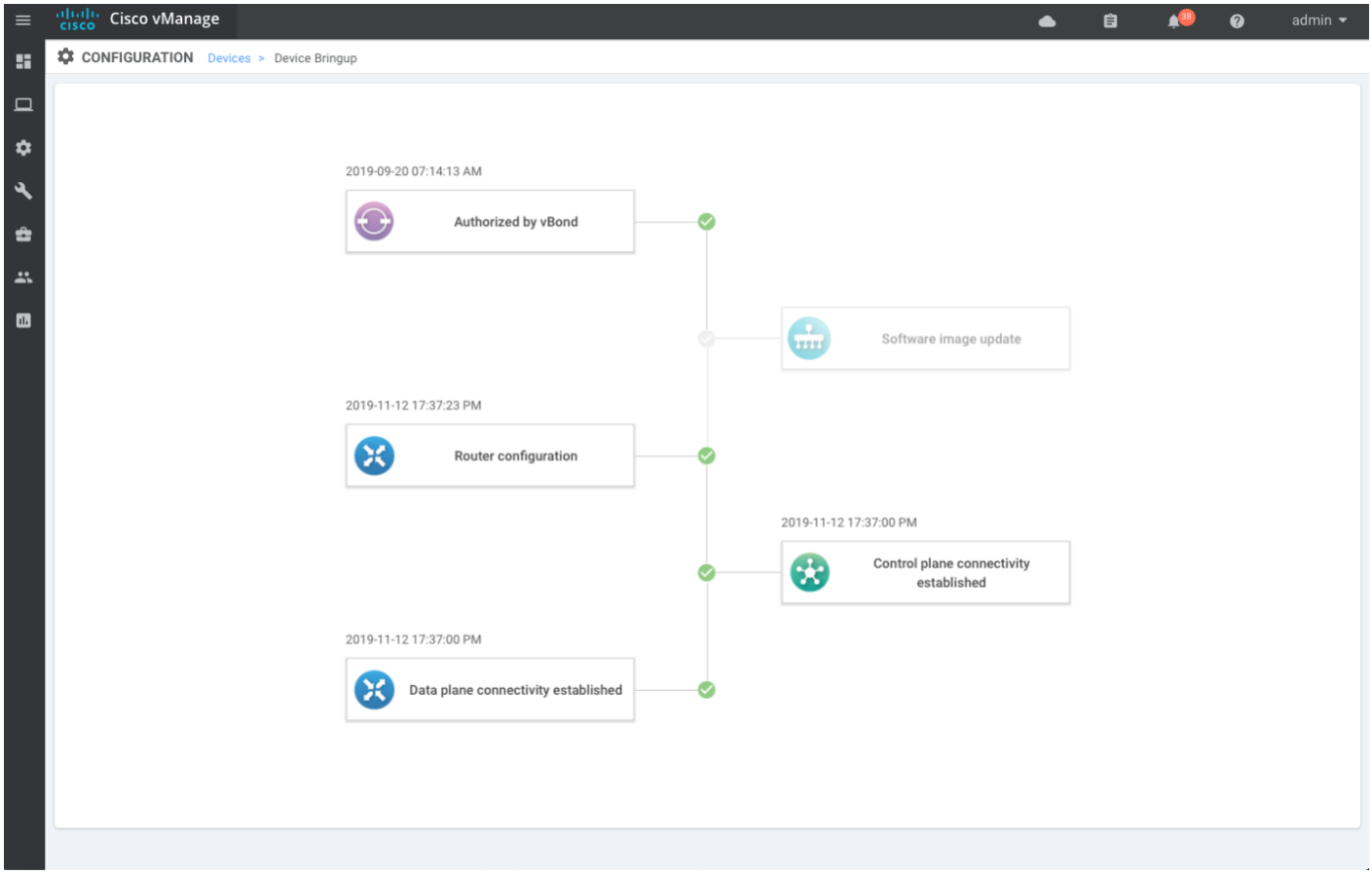


Technical Tip: If a software upgrade need to be performed on the onboarded IOS XE SDWAN device, Refer to '**Appendix B — Upgrading software on SD-WAN device**' for detailed steps.

- To view the entire device bring-up process, navigate to **Configuration > Devices** > **WAN Edge list**, select the three dots and choose **Device Bring Up** from the drop-down menu



Make sure that **Authorized by vBond** is successful, **Router configuration** is added, and finally ensure that the **control and data plane connectivity** is successfully established.



Option 3: Manual deployment for IOS-XE SD-WAN device

In this procedure, the IOS-XE SD-WAN WAN Edge is onboarded into the SD-WAN overlay network using the manual configuration process.

The minimal configuration that is needed to onboard the WAN Edge device includes **system parameters** (vBond, org-name, system-ip, site-id), **VPN 0** network information (interface ip-address, routing protocol or default interface) providing connectivity to SD-WAN controllers to authenticate and onboard the device into the SD-WAN overlay network. Optionally, a hostname and VPN 512 network information (interface IP address and routing protocol or default route) can be provided.

The below example shows the minimum configuration needed to establish control connections with the SD-WAN controllers. The command-line for the WAN Edge devices can be accessed through the management console interface on the physical platforms and through the virtual machine console for the virtual platforms. Note, the default credentials for all the SD-WAN WAN Edge devices is admin/admin and to save any newly added configurations within SD-WAN components, enter **commit and-quit** in configuration mode.

It is important to consider that the Cisco IOS-XE SD-WAN device initiates the Plug-and-Play process automatically upon bootup. To manually configure the device, the Plug-and-Play process must be aborted and can be done with the CLI command **pnpa service discovery stop**.

Procedure 1: Manually configure the IOS-XE SD-WAN WAN Edge device

Step 1 Configure the system parameters that includes hostname, system-ip, site-id, organization-name, and vbond IP address/DNS Name.

```
pnpa service discovery stop
!
config-transaction
system
system-ip          21.21.21.7
site-id            21007
organization-name     "ENB-Solutions - 21615"
vbond 10.4.246.21
exit
!
hostname Branch2-ISR4331-1
exit
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
```

Step 2 (Optional) Configure the out-of-band Management interface, vpn512 with **ip-address** and **default route**.

```
interface GigabitEthernet0
description VPN512_MGMT_Interface
no shutdown
ip address 100.119.112.27 255.255.255.0
exit
!
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 100.119.112.1
end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
```

Step 3 Configure the transport VPN 0 WAN interface to establish reachability to the SD-WAN controllers.

Configure the VPN 0 network interface with IP address, tunnel interface with encapsulation and color and routing (dynamic or default route). Only upon configuring the tunnel interface will the WAN Edge device use DTLS/TLS to establish the secure control plane connections to the SD-WAN controllers, and subsequently, IPSec to establish the secure data plane connections with the WAN Edge devices in the network.

```
interface GigabitEthernet0/0/1
description MPLS_Interface
no shutdown
ip address 10.5.208.42 255.255.255.252
exit
!
interface Tunnel1
no shutdown
ip unnumbered GigabitEthernet0/0/1
ipv6 unnumbered GigabitEthernet0/0/1
tunnel source GigabitEthernet0/0/1
tunnel mode sdwan
exit
!
sdwan
interface GigabitEthernet0/0/1
tunnel-interface
encapsulation ipsec
color mpls

exit
!
ip route 0.0.0.0 0.0.0.0 10.5.208.53
end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
```

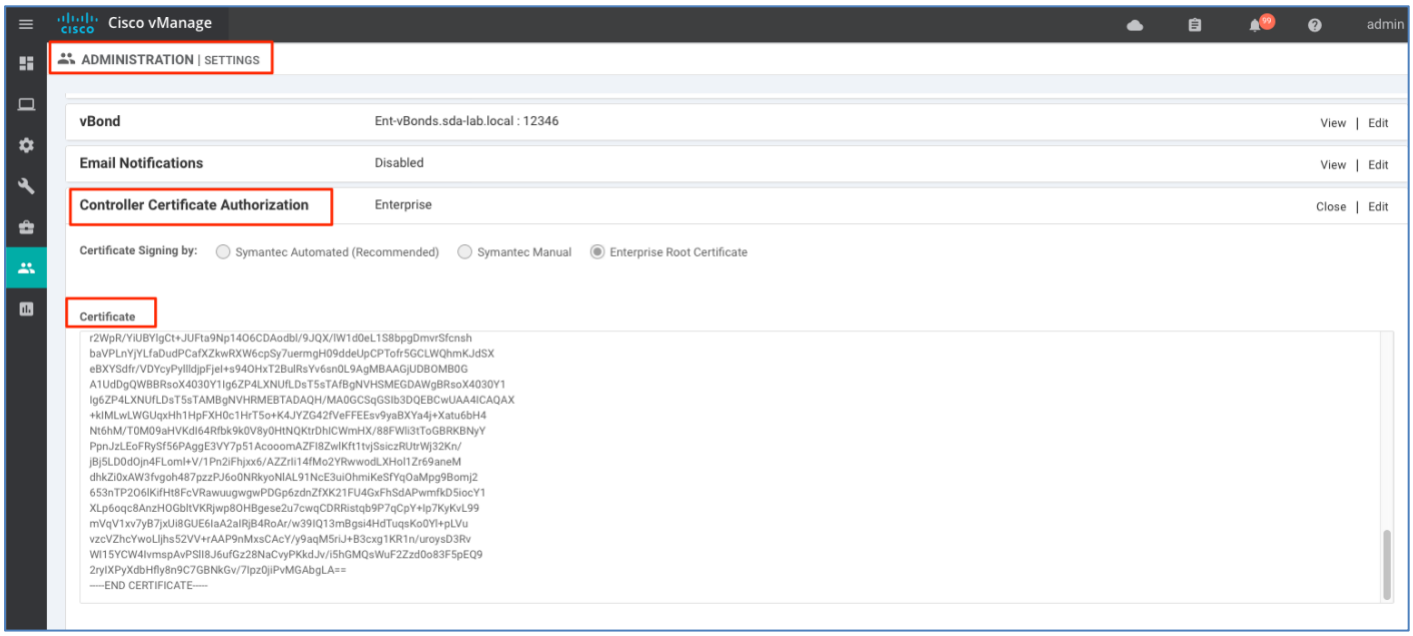
Note: : If you are using Enterprise root CA certificates, proceed to Procedure 2, else to verify the device onboarding process, proceed to Procedure 3.

Procedure 2: Additional onboarding steps for IOS-XE WAN Edge platform using Enterprise root-ca certificate

Deployment using enterprise root-ca certificate requires the installation of a trusted root-ca certificate on the device for successful authentication with the SD-WAN controller in order to join the SD-WAN overlay network.

Step 4 Download the Enterprise root-ca certificate from vManage.

In vManage, navigate to **Administration > Settings,** click view for section **Controller Certificate Authorization** and copy the **Certificate** and save to a file.



Step 5 Download the root-certificate on the WAN Edge device.

To copy the root-certificate onto the device, use the CLI command **copy tftp://username:password@WAN-Edge-VPN512-IP-Address/root-ca-chain.pem bootflash:root-ca-chain.pem vrf Mgmt-intf**

```
copy tftp://Admin:C1sco123@10.4.250.249/root-ca-chain.pem bootflash:root-ca-chain.pem vrf Mgmt-intf
```

Alternatively, copy the certificates using VPN 0 interface, or in USB and load it to device bootflash.

Step 6 Install the root-certificate on the WAN Edge device.

To install the root-certificate on the device, use the CLI command **request platform software sdwan root-cert-chain install bootflash:root-ca-chain.pem**

```
request platform software sdwan root-cert-chain install bootflash:root-ca-chain.pem
```

Step 7 Finally, verify the root-ca certificate is successfully installed on the WAN platform via the CLI command **show sdwan certificate root-ca-cer**t.

```
Branch2-ISR4331-1#sh sdwan certificate root-ca-cert | inc ENB
        Issuer: C=US, ST=NC, L=RTP, O=Cisco Systems Inc, OU=ENB Solutions, CN=sda-lab.local
        Subject: C=US, ST=NC, L=RTP, O=Cisco Systems Inc, OU=ENB Solutions, CN=sda-lab.local
        Issuer: C=US, ST=NC, L=RTP, O=Cisco Systems Inc, OU=ENB Solutions, CN=sda-lab.local
        Subject: C=US, ST=NC, L=RTP, O=Cisco Systems Inc, OU=ENB Solutions, CN=sda-lab.local
```

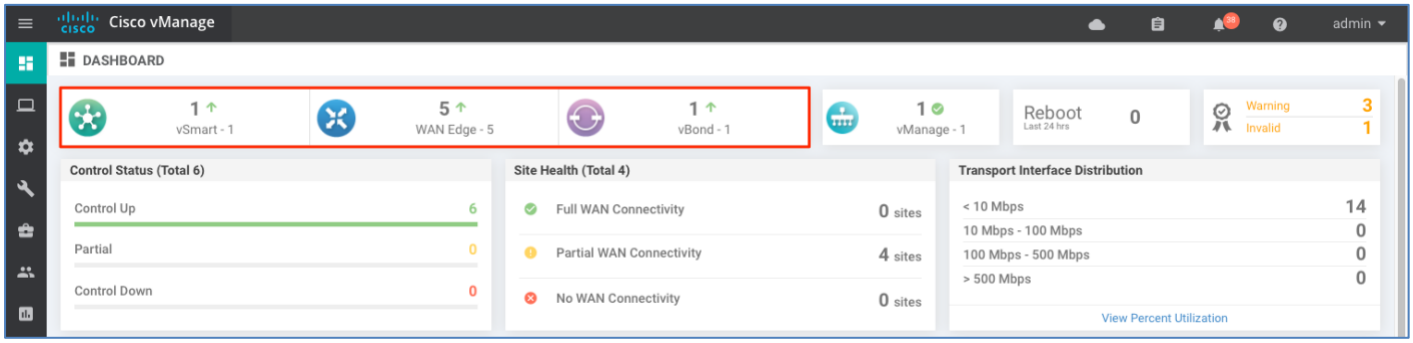
Once enterprise root-ca certificates are installed on the device, the WAN Edge device is authenticated (using organization-name, and whitelist chassis/serial device list) and authorized to join the SD-WAN overlay network.

Upon establishing a secure control connection with the vManage, if a device template is attached, the configuration is downloaded to the device and its previous configuration overwritten.

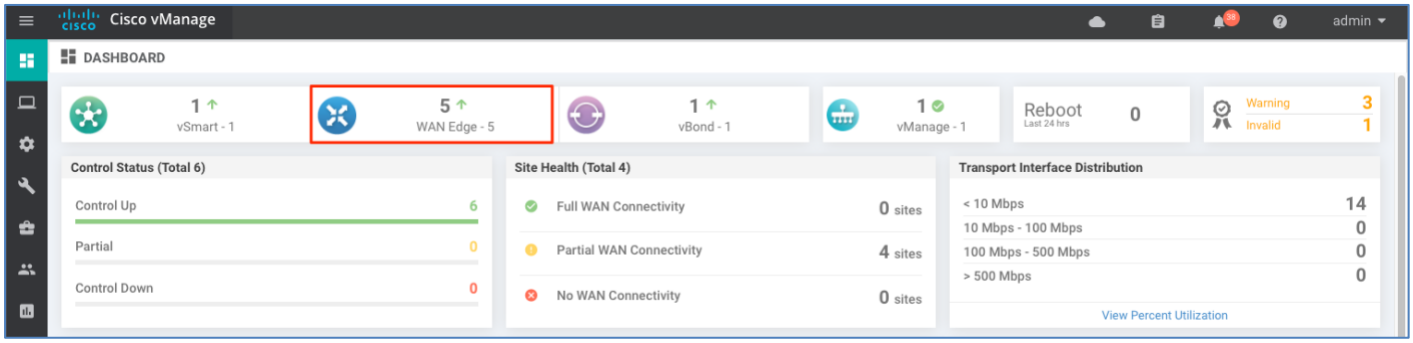
Note: To verify the device onboarding process proceed to Procedure 3.

Procedure 3: Verify the WAN Edge device is successfully onboarded

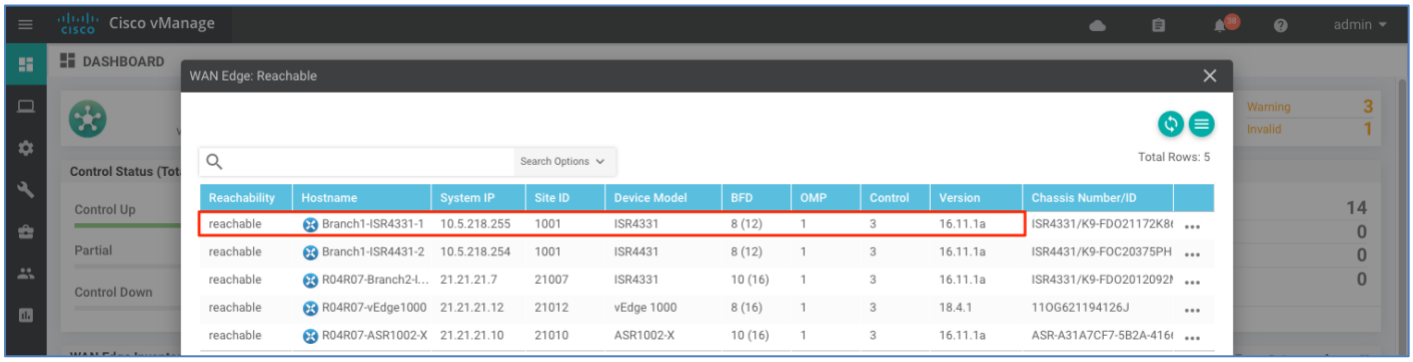
The Cisco vManage device pane dashboard provides a quick view and status of the number of WAN Edge devices onboarded in the Cisco SD-WAN overlay network.



Verify the WAN Edge details from the vManage dashboard, click the **WAN Edge** section from the device pane in the vManage overview section

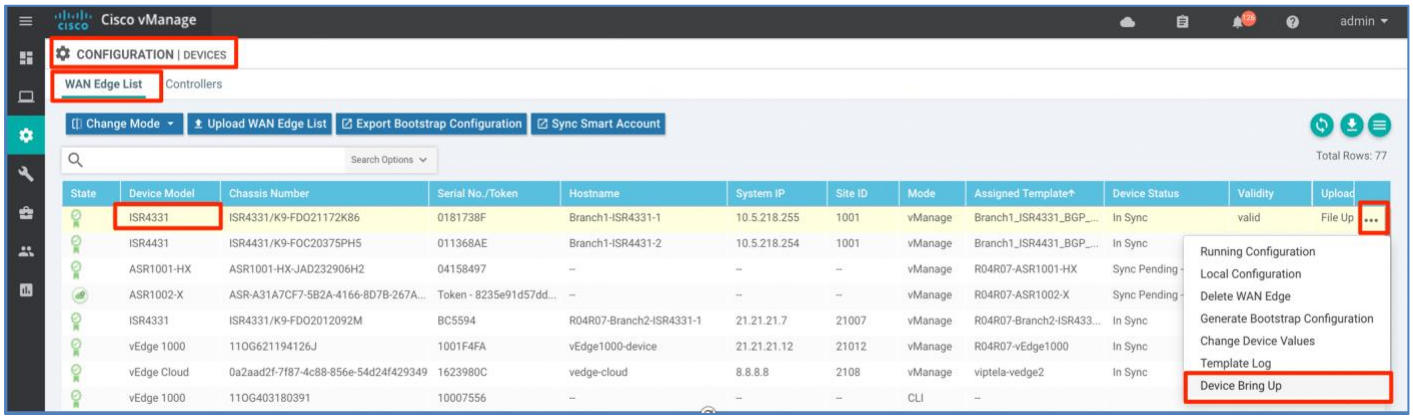


Identify the device and verify the **Reachability** and **Version** status for the platform.

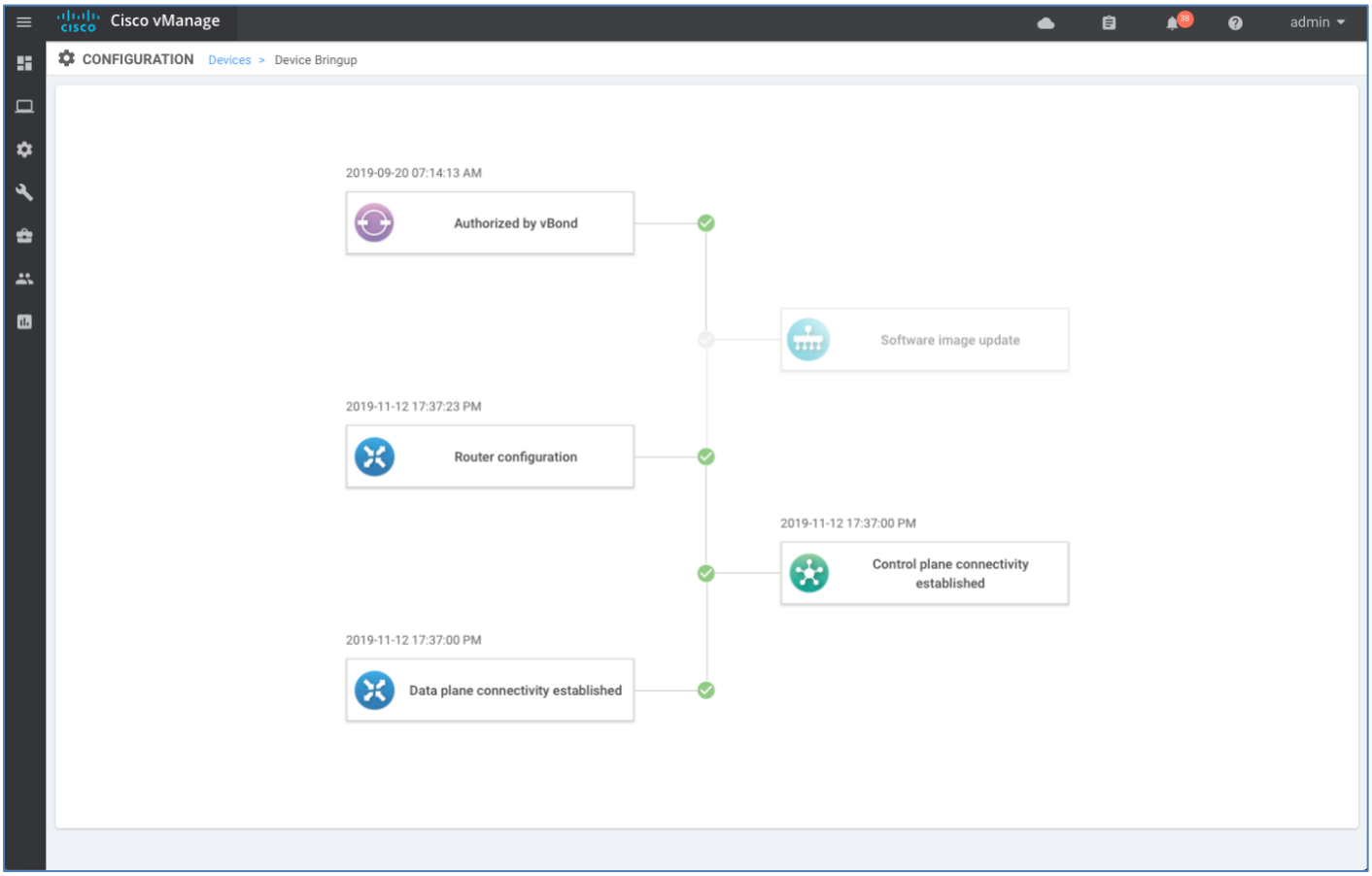


Technical Tip: If software upgrade need to be performed on the onboarded IOS XE SDWAN device, Refer to 'Appendix B — Upgrading software on SD-WAN device' for detailed steps.

To view the entire device bring-up process, navigate to **Configuration > Devices** > **WAN Edge list**, select the three dots and choose **Device Bring Up** from the drop-down menu



Make sure that **Authorized by vBond** is successful, **Router configuration** is added, and finally ensure that the **control and data plane connectivity** is successfully established.



Operate

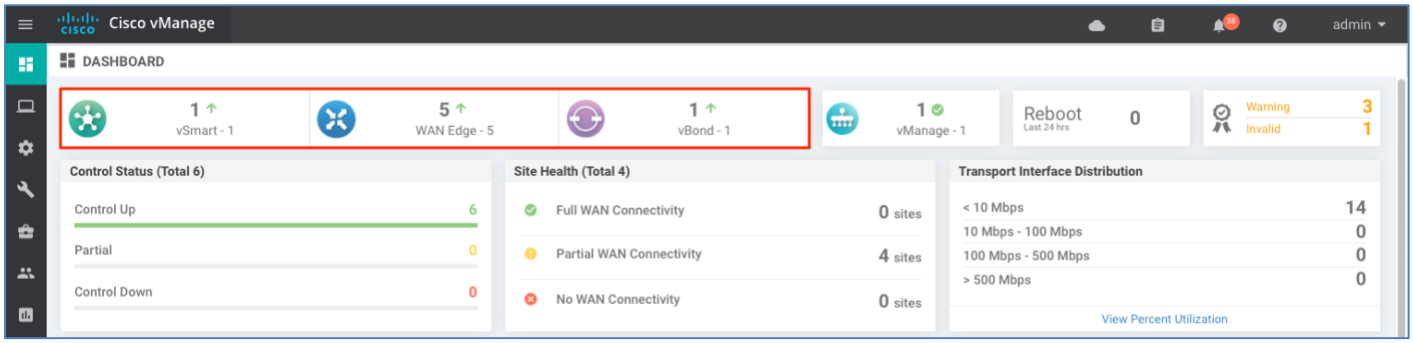
Using the vManage GUI, you can monitor, troubleshoot and manage the WAN Edge device. Some of the common troubleshooting and monitoring steps are covered in the process and procedures listed below.

Process 1: Monitor and manage the status of SD-WAN components via vManage NMS

Use the vManage dashboard screen to monitor the overall health of the SD-WAN overlay network.

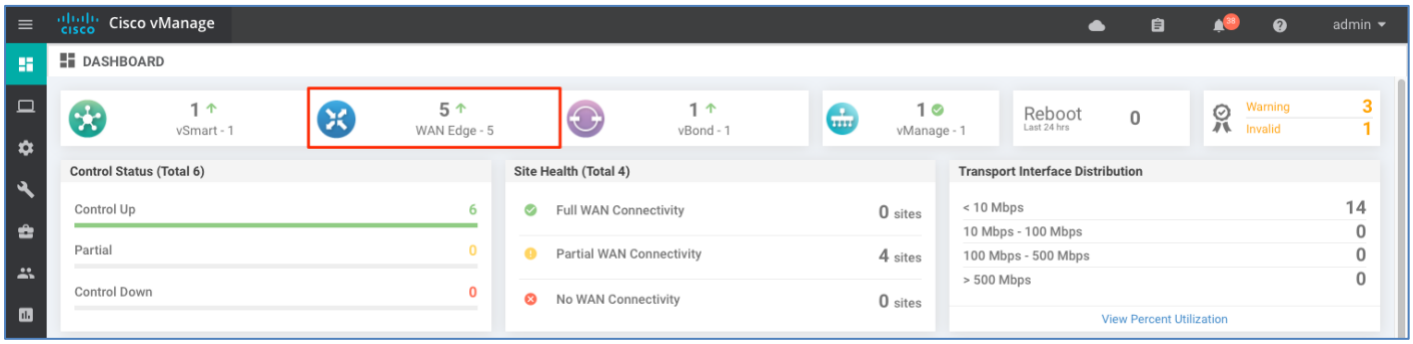
Procedure 1: Monitor the SD-WAN components via Device Pane

Step 1 View the **Device Pane** which runs across the top of the dashboard screen that displays all the control connections from the vManage NMS to the vSmart controllers, vEdge routers, and vBond orchestrators in the overlay network. The pane also displays the status of the vManage NMSs in the network. Make sure the connections for all the SD-WAN components are up (↑).

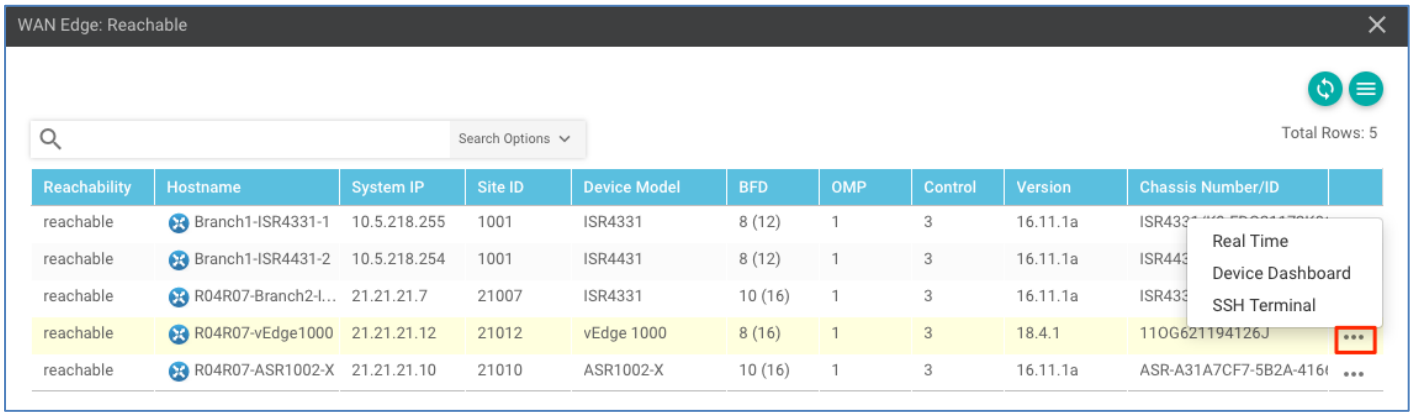


Procedure 2: View WAN Edge device details and statistics via Device Pane

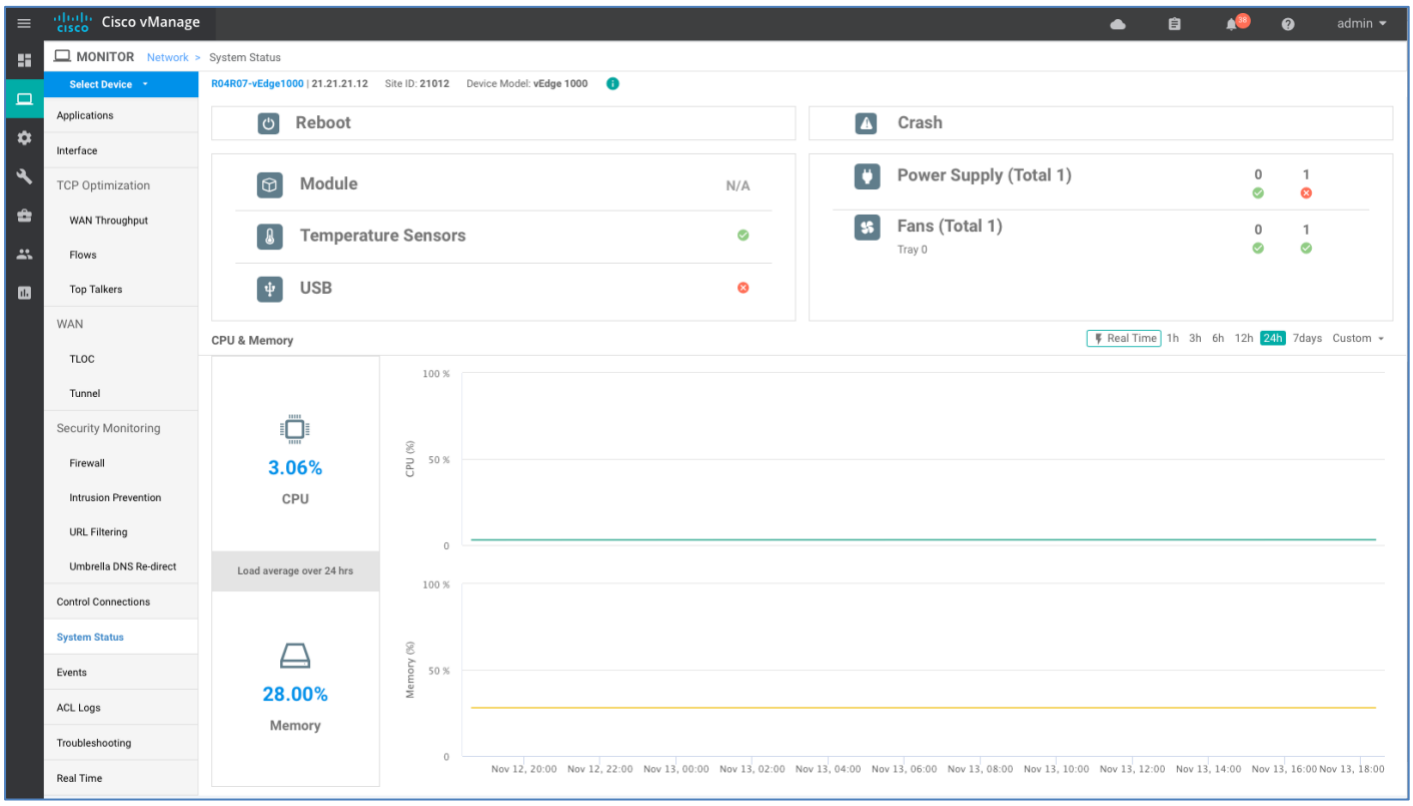
Step 1 To view device statistics, click on the number or the Up/ Down arrows above **WAN Edge** – 5 to display a table with detailed information for each connection.



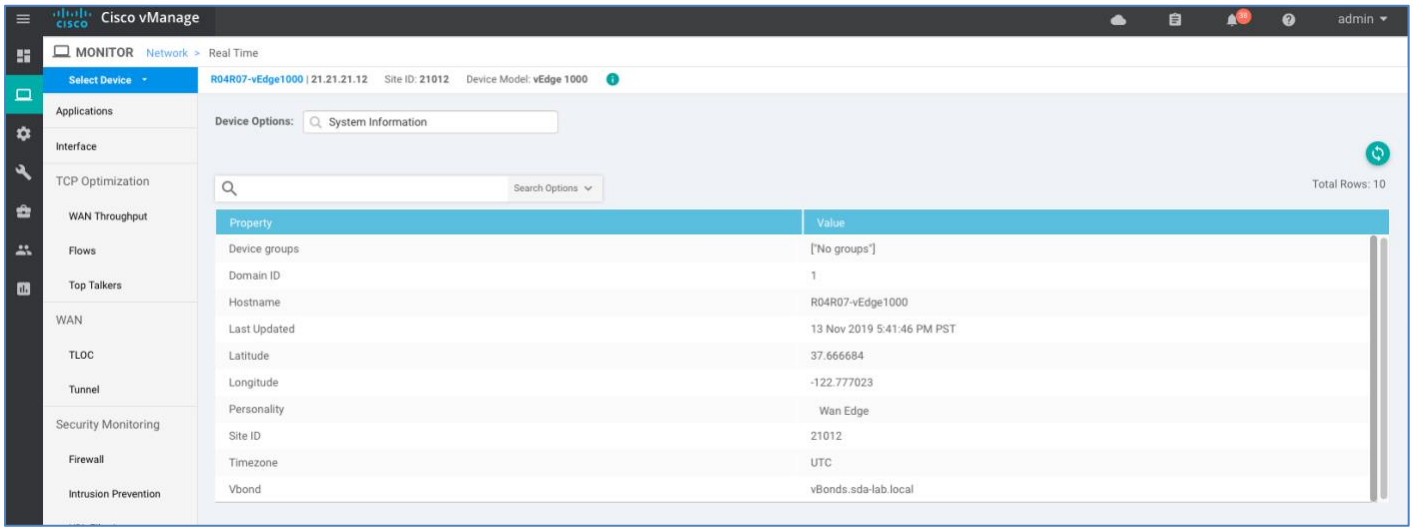
Step 2 The table lists the device's **System IP**, **Site ID**, **Device Model**, Software **Version** and more. For more device-specific information, drill down further by clicking on the **three dots** (…) to the right of each table row. From here you can access either the **Device Dashboard**, **Real Time** data, or the **SSH Terminal**.



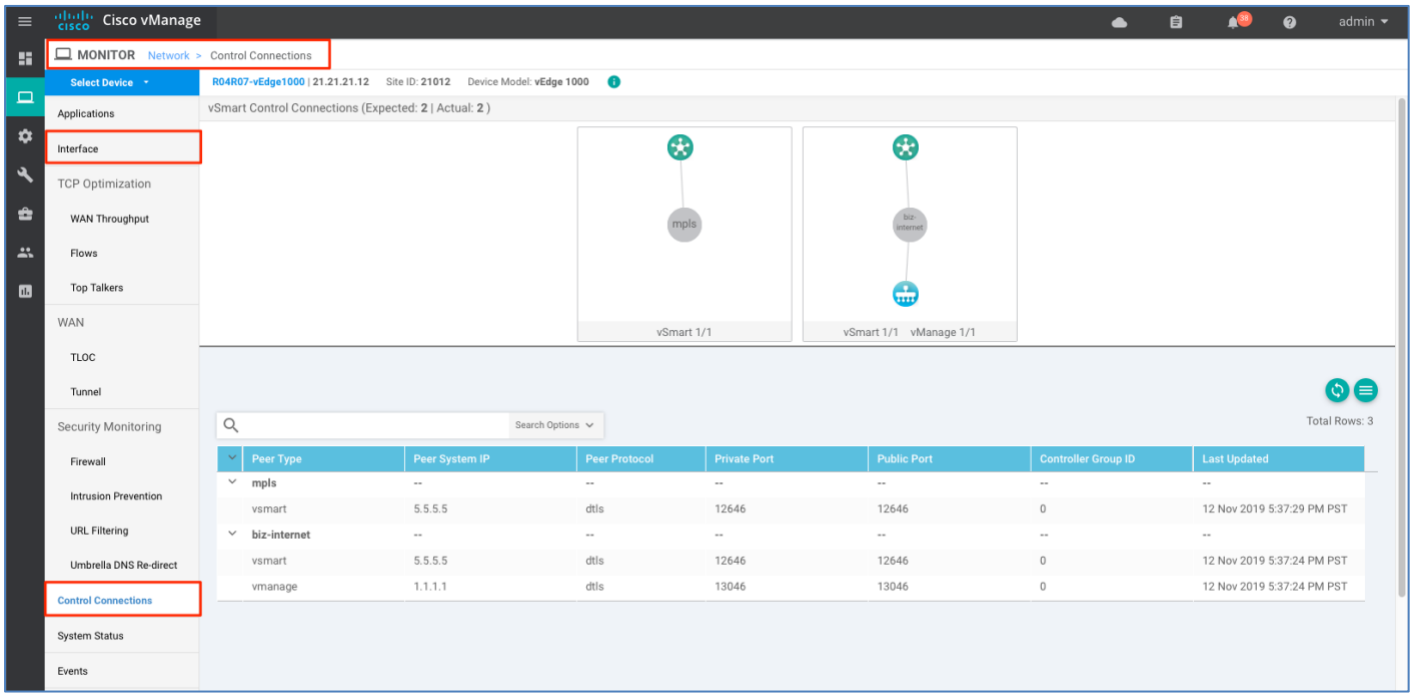
The Device Dashboard displays the device's **System Status**, the device **Module Hardware Inventory** information, **CPU & Memory** real time statistics.



Real Time displays the basic system information of the device such as **Site ID, Vbond, Hostname, Latitude, Longitude** and more.



Step 3 Additional information such as **Control Connections** over the interfaces of the WAN Edge device can be viewed from the vManage NMS. In vManage, navigate to **Monitor > Network**, select the device from the list and look for device information from the left-side panel.

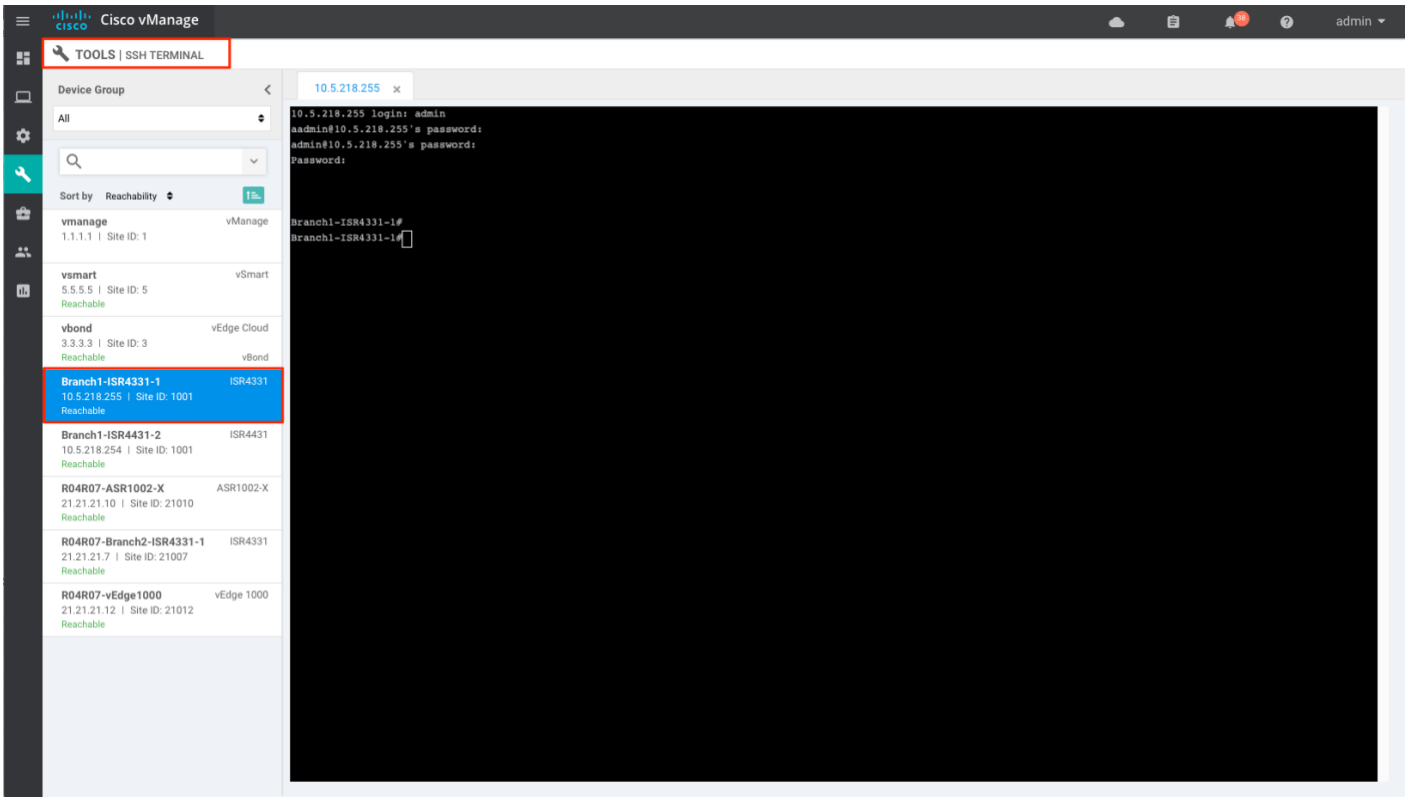


Procedure 3: Monitor WAN Edge device via vManage SSH Server Dashboard using CLI commands

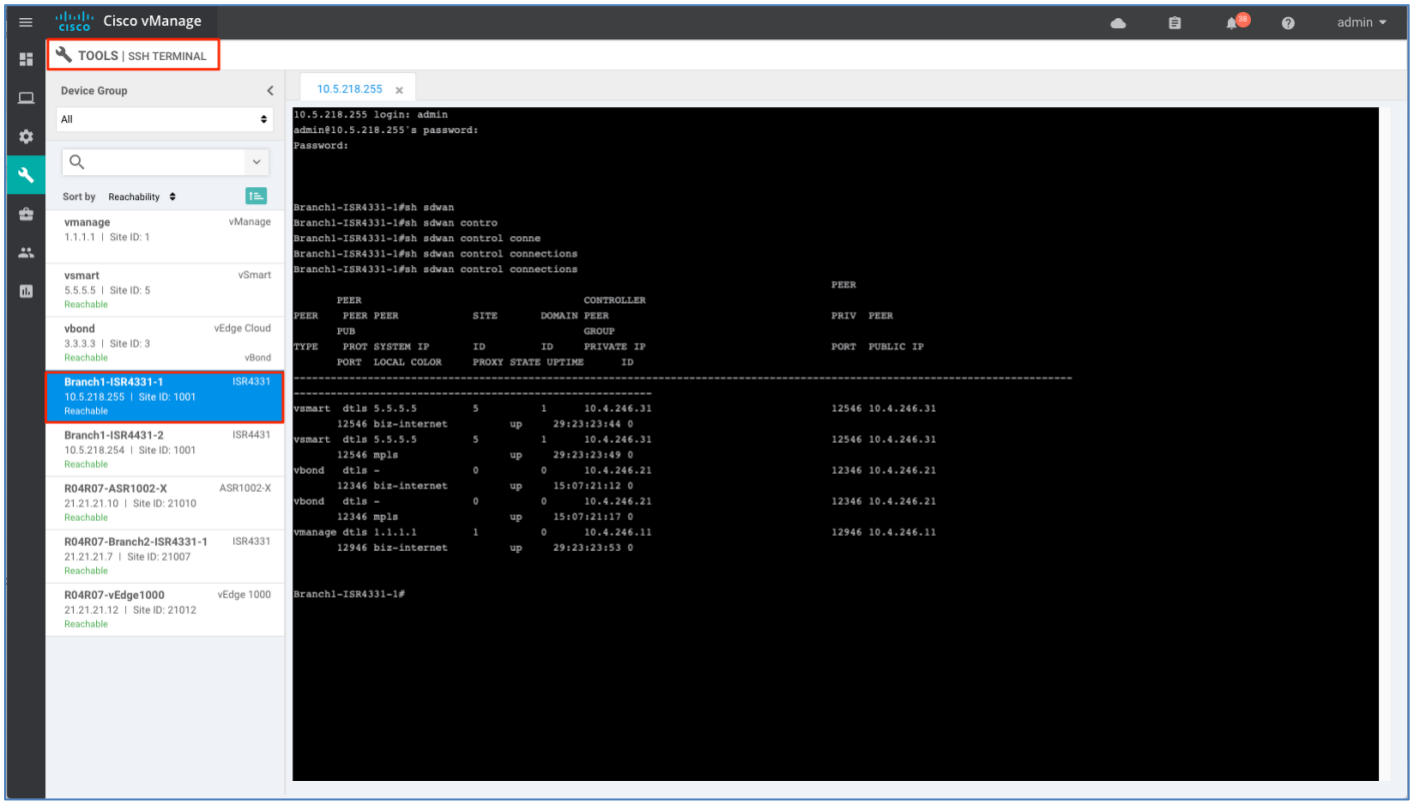
vManage NMS provides the capability to run CLI show and debug commands from the GUI.

Step 1 In vManage, navigate to **Tools** > **SSH Terminals**

Select the WAN Edge from the **Device Group**.



Step 2 To verify if the WAN Edge device has established secure control connections with the SD-WAN controllers, enter **show control connections** for vEdge devices or **show sdwan control connections** for IOS-XE SD-WAN devices.



Process 2: Troubleshooting – Device Onboarding

This process explains some of the common troubleshooting procedures.

Procedure 1: Diagnosing onboarding issues

This section covers the most common issues that could be encountered during the WAN Edge device onboarding process and recommended resolution to resolve the issues.

Step 1 To verify the WAN Edge device has established a secure control connections with the SD-WAN controllers, enter the command **show control connections** for vEdge devices or **show sdwan control connections** for IOS-XE SD-WAN devices

```
Router#
Router#sh sdwan control connections

Router#
```

Step 2 To verify the device properties used to authenticate WAN Edge devices, enter the command **show control local-properties** on vEdge devices or **show sdwan control local-properties** on IOS-XE SD-WAN devices.

Within the output, make sure:

- system parameters are configured to include **organization-name** and **site-id**
- certificate-status and root-ca-chain-status are installed

- certificate-validity is **Valid**
- **dns-name** is pointing to vBond IP address/DNS
- **system-ip** is configured and chassis-num/unique-id and serial-num/token is available on the device

```
vedge# show control local-properties
personality                 vedge
sp-organization-name        ENB-Solutions - 21615
organization-name           ENB-Solutions - 21615
certificate-status          Installed
root-ca-chain-status        Installed

certificate-validity        Valid
certificate-not-valid-before May 14 23:40:02 2013 GMT
certificate-not-valid-after  Jan 19 03:14:07 2038 GMT

dns-name                    vBonds.sda-lab.local
site-id                     0
domain-id                   1
protocol                    dtls
tls-port                    0
system-ip                   21.21.21.12
chassis-num/unique-id       11OG621194126J
serial-num                  1001F4FA
token                       -NA-
keygen-interval             1:00:00:00
retry-interval              0:00:00:18
no-activity-exp-interval    0:00:00:20
dns-cache-ttl               0:00:02:00
port-hopped                 FALSE
time-since-last-port-hop    0:00:00:00
embargo-check               success
number-vbond-peers          0
number-active-wan-interfaces 1


 NAT TYPE: E -- indicates End-point independent mapping
           A -- indicates Address-port dependent mapping
           N -- indicates Not learned
           Note: Requires minimum two vbonds to learn the NAT type

                      PUBLIC          PUBLIC PRIVATE         PRIVATE                                PRIVATE                          MAX   RESTRICT/           LAST         SPI TIME    NAT  VM
INTERFACE             IPv4            PORT   IPv4            IPv6                                   PORT    VS/VM COLOR      STATE CNTRL CONTROL/     LR/LB  CONNECTION   REMAINING   TYPE CON
                                                                                                                                    STUN                                                 PRF
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
ge0/0                 10.5.207.62     12346  10.5.207.62     ::                                     12346   0/0  default     down   2       no/yes/no   No/No  0:00:46:22   0:11:06:00  N    5
```

The above parameters must be available on the WAN Edge device to mutually authenticate with the SD-WAN controllers before establishing the connections.

Step 3 To verify the reachability of the vBond controller from the WAN Edge device.

```
vedge# ping vBonds.sda-lab.local
Ping in VPN 0
PING vBonds.sda-lab.local (10.4.246.21) 56(84) bytes of data.
64 bytes from 10.4.246.21: icmp_seq=1 ttl=62 time=30.6 ms
64 bytes from 10.4.246.21: icmp_seq=2 ttl=62 time=17.7 ms
64 bytes from 10.4.246.21: icmp_seq=3 ttl=62 time=14.7 ms
^C
```

Step 4 To view the reason for failure, if a WAN Edge device fails to establish connection with the SD-WAN controllers, enter the command **show control connections-history** for vEdge devices and **show sdwan control connection-history** for IOS-XE SD-WAN devices and view the **LOCAL ERROR** and **REMOTE ERROR** column to gather error details.

```
vedge# show control connections-history
Legend for Errors
ACSRREJ    - Challenge rejected by peer.            NOVMCFG   - No cfg in vmanage for device.
BDSGVERFL  - Board ID Signature Verify Failure.     NOZTPEN   - No/Bad chassis-number entry in ZTP.
BIDNTPR    - Board ID not Initialized.              OPERDOWN  - Interface went oper down.
BIDNTVRFD  - Peer Board ID Cert not verified.       ORPTMO    - Server's peer timed out.
BIDSIG     - Board ID signing failure.              RMGSPR    - Remove Global saved peer.
CERTEXPRD  - Certificate Expired                    RXTRDWN   - Received Teardown.
CRTREJSER  - Challenge response rejected by peer.   RDSIGFBD  - Read Signature from Board ID failed.
CRTVERFL   - Fail to verify Peer Certificate.       SERNTPRES - Serial Number not present.
CTORGNMMIS - Certificate Org name mismatch.         SSLNFAIL  - Failure to create new SSL context.
DCONFAIL   - DTLS connection failure.               STNMODETD - Teardown extra vBond in STUN server mode.
DEVALC     - Device memory Alloc failures.          SYSIPCHNG - System-IP changed.
DHSTMO     - DTLS HandShake Timeout.                SYSPRCH   - System property changed
DISCVBD    - Disconnect vBond after register reply. TMRALC    - Timer Object Memory Failure.
DISTLOC    - TLOC Disabled.                         TUNALC    - Tunnel Object Memory Failure.
DUPCLHELO  - Recd a Dup Client Hello, Reset Gl Peer. TXCHTOBD  - Failed to send challenge to BoardID.
DUPSER     - Duplicate Serial Number.               UNMSGBDRG - Unknown Message type or Bad Register msg.
DUPSYSIPDEL- Duplicate System IP.                   UNAUTHEL  - Recd Hello from Unauthenticated peer.
HAFAIL     - SSL Handshake failure.                 VBDEST    - vDaemon process terminated.
IP_TOS     - Socket Options failure.                VECRTREV  - vEdge Certification revoked.
LISFD      - Listener Socket FD Error.              VSCRTREV  - vSmart Certificate revoked.
MGRTBLCKD  - Migration blocked. Wait for local TMO. VB_TMO    - Peer vBond Timed out.
MEMALCFL   - Memory Allocation Failure.             VM_TMO    - Peer vManage Timed out.
NOACTVB    - No Active vBond found to connect.      VP_TMO    - Peer vEdge Timed out.
NOERR      - No Error.                              VS_TMO    - Peer vSmart Timed out.
NOSLPRCRT  - Unable to get peer's certificate.      XTVMTRDN  - Teardown extra vManage.
NEWVBNOVMNG- New vBond with no vMng connections.    XTVSTRDN  - Teardown extra vSmart.
NTPRVMINT  - Not preferred interface to vManage.    STENTRY    - Delete same tloc stale entry.
EMBARGOFAIL - Embargo check failed

                                                                PEER                    PEER
PEER     PEER     PEER            SITE       DOMAIN PEER       PRIVATE  PEER           PUBLIC                          LOCAL      REMOTE     REPEAT
TYPE     PROTOCOL SYSTEM IP       ID         ID     PRIVATE IP PORT     PUBLIC IP      PORT   LOCAL COLOR      STATE   ERROR      ERROR      COUNT DOWNTIME
-------------------------------------------------------------------------------------------------------------------------------------------------------------
vbond    dtls     0.0.0.0         0          0      10.4.246.21 12346    10.4.246.21    12346  default          tear_down SYSIPCHNG  NOERR      0     2019-11-09T14:17:29+0000
vmanage  dtls     1.1.1.1         1          0      10.4.246.11 12646    10.4.246.11    12646  default          tear_down CTORGNMMIS NOERR      14    2019-11-09T14:17:13+0000
```

Listed below are some of the reasons the WAN Edge device fails to establish control connections with the SD-WAN controllers.

CRTVERFL – the error state indicates the WAN Edge device authentication is failing because of a root-ca certificate mismatch between the WAN device and the SD-WAN controller. Use the **show certificate root-ca-cert** on vEdge devices or **show sdwan certificate root-ca-cert** on IOS-XE SD-WAN devices to confirm the same certificates are installed on the WAN Edge device and the SD-WAN controllers.

CTORGNMMIS - the error state indicates the WAN Edge device authentication is failing because of a mismatch organization-name, compared with the organization-name configured on the SD-WAN controller. Use **show sdwan control local-properties** on vEdge devices and **show sdwan control local-properties** on IOS-XE SD-WAN devices to confirm all the SD-WAN components are configured with same organization-name across the SD-WAN environment.

NOZTPEN – the error state indicates the onboarding vEdge device is not part of the authorized whitelist device on the ZTP server. Use **show ztp entry** on the on-prem ZTP server to verify the device whitelist.

NOVMCFG – the error status indicates the WAN Edge device has not been attached with a device template in vManage. This status is seen when onboarding the device using automated deployment options, which is the PnP or ZTP process.

VB_TMO, VM_TMO, VP_TMO, VS_TMO – the error indicates the WAN Edge device has lost reachability to the SD-WAN controllers.

Step 5 The following are miscellaneous show commands for reference to verify control connections on the WAN Edge device:

vEdge platform	IOS-XE SD-WAN platform
show control connections	**show sdwan control connections**
show control connections-history	**show sdwan control connection-history**
show control connections-info	**show sdwan control connection-info**
show control local-properties	**show sdwan control local-properties**
show control statistics	**show sdwan control statistics**

show control summary	**show sdwan control summary**
show control valid-vsmarts	**show sdwan control valid-vsmarts**
show control valid-vmanage-id	**show sdwan control valid-vmanage-id**

Procedure 2: Missing root ca certificate missing on the IOS-XE SD-WAN WAN Edge device.

If the platform being onboarded is missing root-ca-chain certificates, device authentication will fail. A device failing authentication cannot establish control connection to the SD-WAN controller. In such scenarios, follow the steps below to install **root-ca certificate** on the device components.

Login into the device and view the **root-ca-chain status** from the CLI command **show sdwan control local-properties**. Below is an example of the output showing the **root-ca-chain-status** is in **Not-Installed** state.

```
sh sdwan control local-properties
personality                vedge
sp-organization-name           ENB-Solutions - 21615
organization-name          ENB-Solutions - 21615
root-ca-chain-status       Not-Installed
```

For such platforms, the root-ca-chain status certificate must be installed. The root-ca.crt file can be downloaded from the vManage controller and uploaded to the WAN Edge device.

Note, within vManage NMS the file is located in the directory path - **/usr/share/viptela/root-ca.crt**

Step 1 Log into vManage NMS and access the **root-ca.crt** file.

```
vmanage# vshell
vmanage:~$ ls -lrt /usr/share/viptela/root-ca.crt
-rwxr-xr-x 1 root root 20091 Oct  5 21:11 /usr/share/viptela/root-ca.crt
vmanage:~$
```

Step 2 Download the certificate to your local machine and copy the **root-ca.crt** file into a USB along with the bootstrap configuration.

```
DESKTOP$ scp admin@100.119.104.210:/usr/share/viptela/root-ca.crt Desktop/
viptela 18.4.302


admin@100.119.104.210's password:
root-ca.crt                                   100%   20KB  56.7KB/s   00:00
```

```
dir bootflash:root-ca.crt

Directory of bootflash:/root-ca.crt


  23  -rw-          20091  Sep 20 2019 06:16:27 +00:00  root-ca.crt


29633794048 bytes total (25341145088 bytes free)
```

Alternatively, root-ca certificate file can be copied to the WAN Edge device directly using scp protocol on the VPN 0 interface directly from vManage.

Note that the device default configuration only allows dhcp, dns and icmp protocols and drops all other traffic. To use scp protocol, allow **sshd** protocol on the tunnel-interface of the device as show below:

```
config-transaction

sdwan

interface ge/0/0

tunnel-interface

allow-service sshd

end

Uncommitted changes found, commit them? [yes/no/CANCEL] yes
```

Enter the following CLI commands on vManage, to copy the file to the WAN Edge device.

```
vmanage# vshell

vmanage:~$ cd /usr/share/viptela/

vmanage:/usr/share/viptela$ scp root-ca.crt admin@10.5.207.50:root-ca.crt

exit
```

Step 3 On device boot up with the bootstrap configuration, enter the command - **request platform software sdwan root-cert-chain install usb0:/root-ca.crt** for IOS-XE SDWAN devices.

```
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

/tmp/sw/rp/0/0/rp_daemons/mount/usr/bin/vconfd_script_upload_root_ca_crt_chain.sh: line 197: [: ==:
unary operator expected

Successfully installed the root certificate chain
```

Step 4 Verify the certificate is installed.

```
sh sdwan control local-properties

personality                vedge

sp-organization-name           ENB-Solutions - 21615

organization-name              ENB-Solutions - 21615

root-ca-chain-status           Installed
```

About this guide

Feedback & Discussion

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

Appendix A — Hardware and Software used for validation

This guide was validated using the following hardware and software.

Functional area	Product	Software version
Cisco SD-WAN controllers	Cisco vManage, Cisco vSmart, and Cisco vBond controllers	18.4.302
Cisco IOS-XE SD-WAN Device	ISR4K, ASR1K	16.10.3a
Cisco vEdge Device	vEdge, vEdge 1000	18.4.302
Server	Hypervisor/vSphere client	VMware ESXi, 6.7.0, 10302608/version 6.7.0.20000

Appendix B — Upgrading software on SD-WAN device

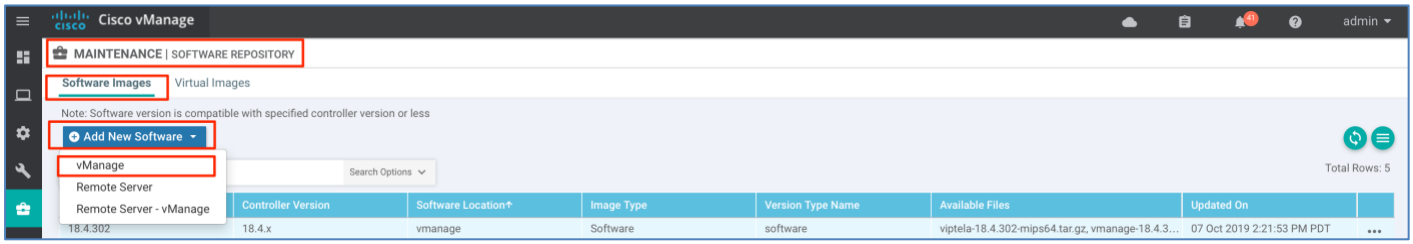
Cisco SD-WAN WAN Edge devices can be upgraded during the Zero-Touch provisioning process or at a later time from the vManage NMS as long as the device is managed by the controller.

> Technical Tip: If upgrading software on all the SD-WAN components, upgrade software on the vManage controller first, then the controllers (vBond, vSmart) before upgrading the WAN Edge devices.

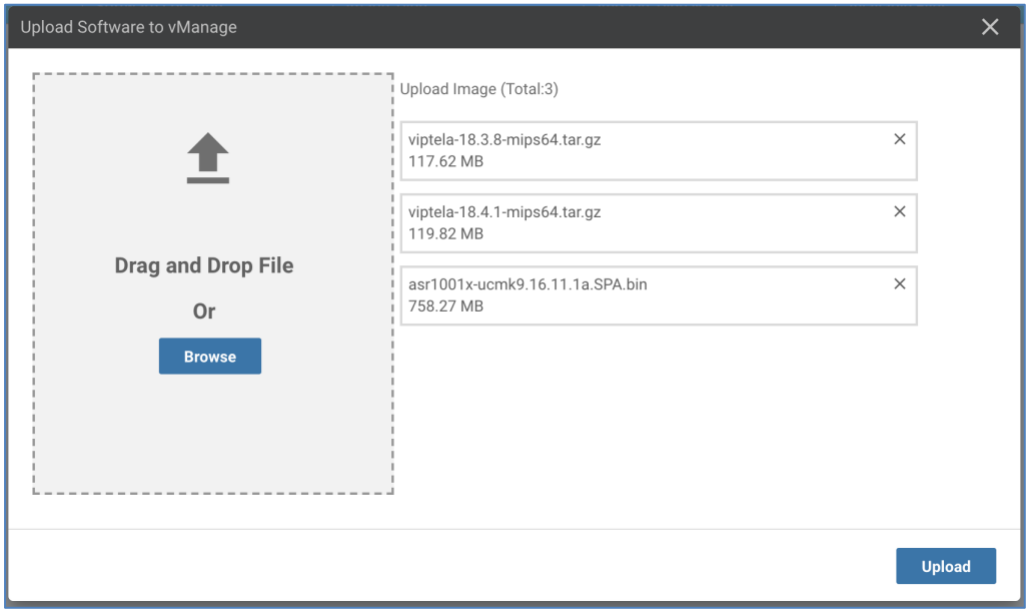
SD-WAN software can be downloaded to the local machine from https://software.cisco.com. The downloaded software image can be uploaded to vManage or a remote vManage or a remote file server and later be downloaded and activated on the WAN Edge device.

Procedure 1: Upload the Image to vManage NMS

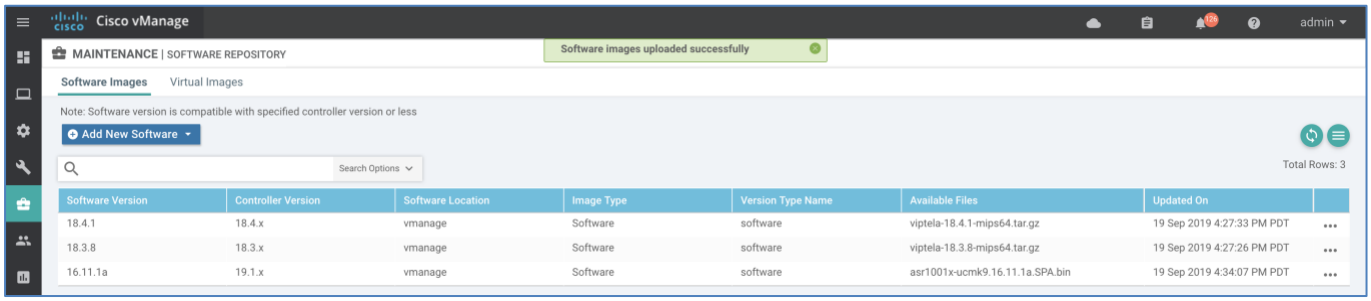
Step 1 To upload the downloaded code to the vManage, navigate to **Maintenance > Software Repository** > **Software Images**, click **Add New Software** and choose **vManage** from the drop-down menu.



Step 2 Browse and select the file(s) or **Drag and Drop** the file(s) and click **Upload.**

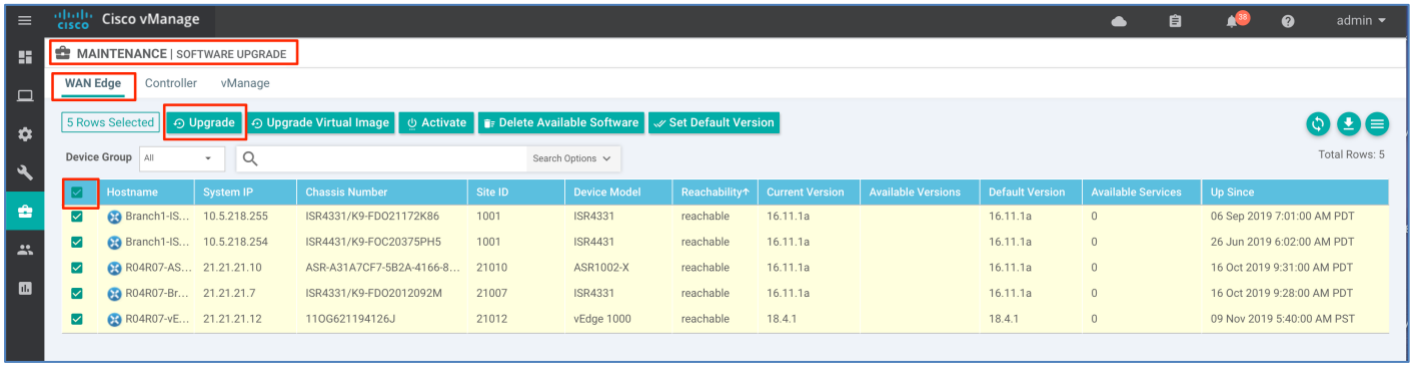


The files gets uploaded to vManage with a status message on the top indicating **Software images uploaded successfully** and upon completion, the image is available to upgrade the devices from the vManage controller.



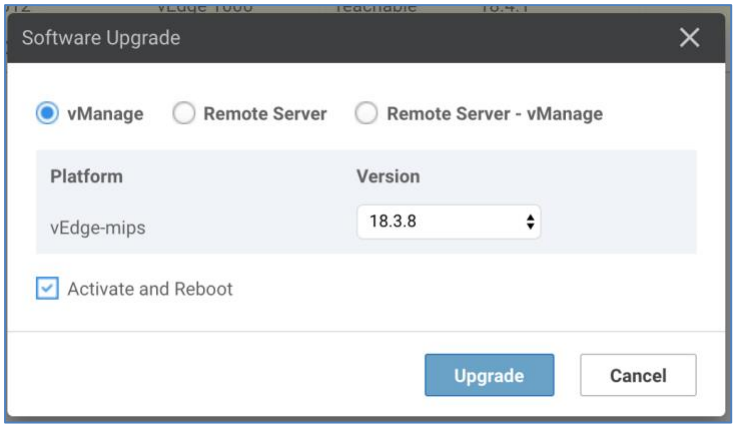
Procedure 2: Upgrading WAN Edge device

Step 1 To upgrade software on the device from vManage. Navigate **to Maintenance > Software Upgrade > WAN Edge,** select the devices from the list and click **Upgrad**e.



Step 2 Select the option **vManage** and choose the desired software version from the drop-down menu, under column **Version** for the respective device under the column **Platform**.

Select the options **Activate and Reboot** allowing the device to activate the code and perform a reboot automatically upon successfully downloading the code on the device.



Technical Tip: Software upgrade can be done automatically for vEdge devices during the Zero-Touch-Provisioning onboarding process.

Appendix C — Cisco Smart and Virtual Account

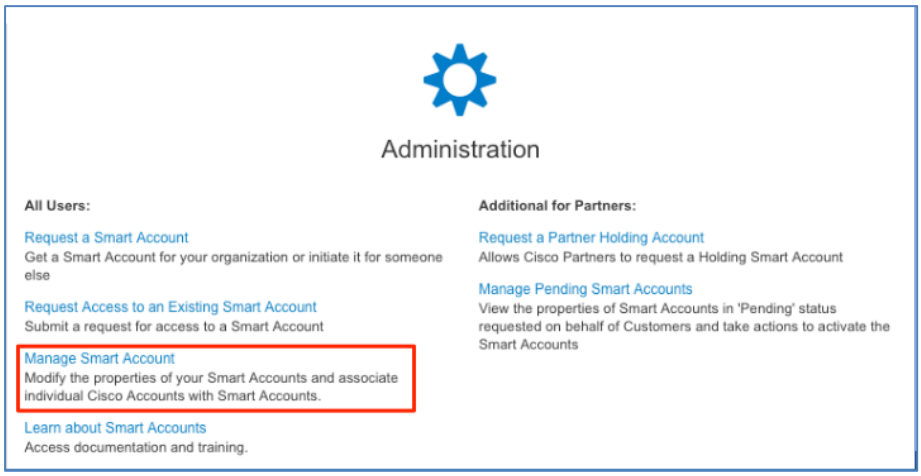
A Cisco Smart Account offers a simple-to-use, centralized visibility and self-management of Cisco assets such as network devices, licenses, agreements, users and roles across the organization. Network administrators can view, purchase, store, manage and move Cisco assets as needed across the organizations. Smart accounts combined with smart licensing provide real-time, enterprise-wide visibility into license utilization across the organization with Virtual Accounts.

With a Smart Account created, customers can create Virtual Accounts, reflecting their organizational departments, associate licenses and assets with these individual departments to manage. Departments can be categorized by Business function, User group, Technology group, Geographical locations etc. based on the business needs. Virtual Accounts help to internally organize licenses, devices, users and roles. Multiple Virtual Accounts can be part of the same Smart Account.

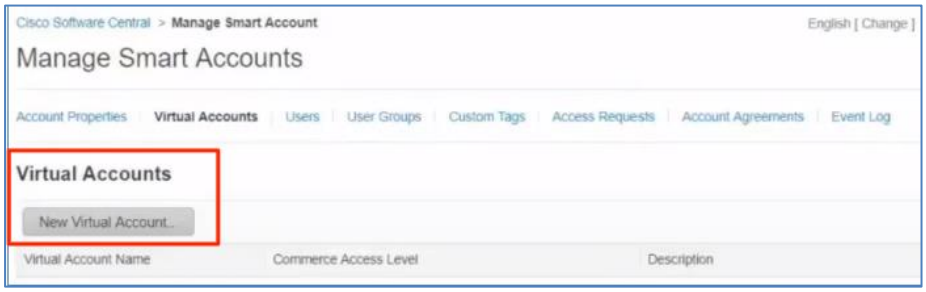
Smart Accounts and Virtual Accounts are essential in the onboarding of Cisco SD-WAN devices onto the network. While placing an order on the Cisco Commerce Workspace, you can assign the Smart Account and Virtual Account to the device in the order.

Technical Tip: You can request Smart Account or manage an existing Smart Account at https://software.cisco.com/ under the **Administration** section.

Creating Virtual Account(s) under the Smart Account is simple and easy. Log into the Cisco Software Central > **Administration** and select **Manage Smart Account .**

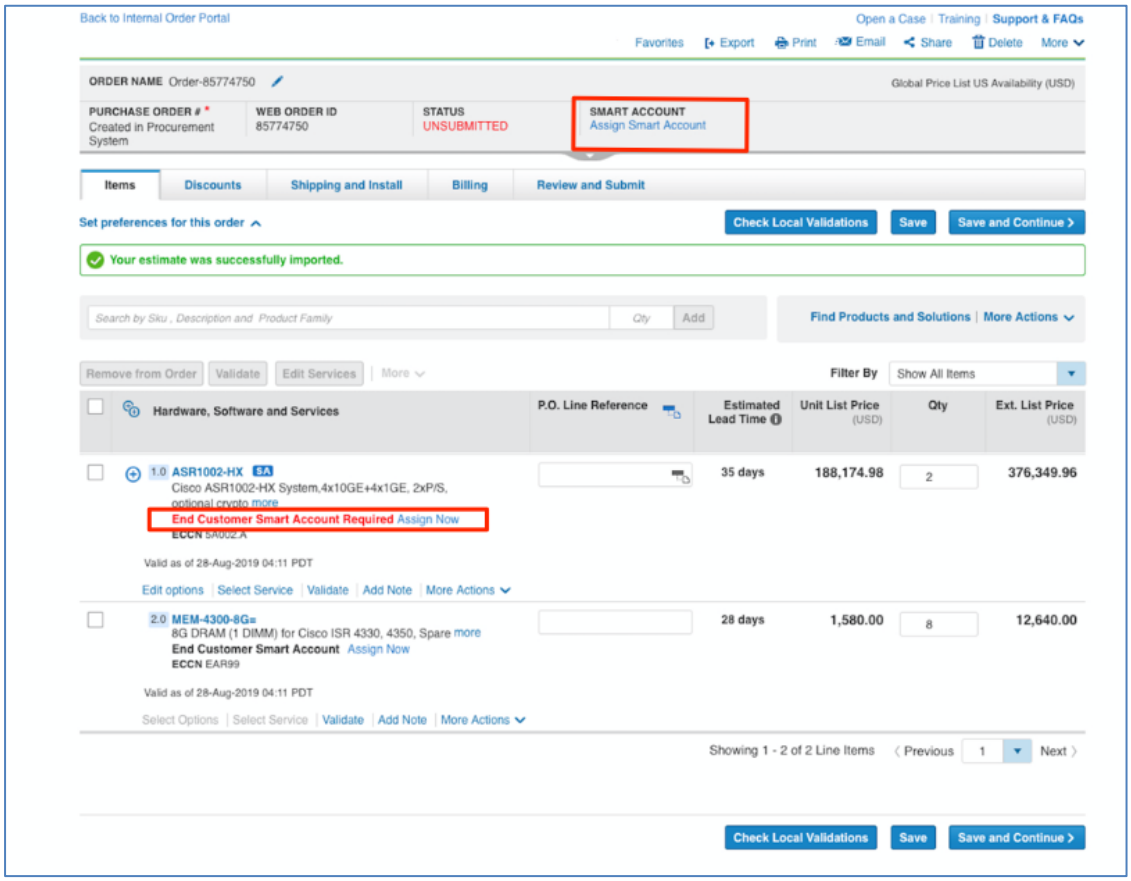


In the **Manage Smart Accounts**, under **Virtual Accounts** tab select **New Virtual Account** to create new virtual accounts based on the company's requirement.

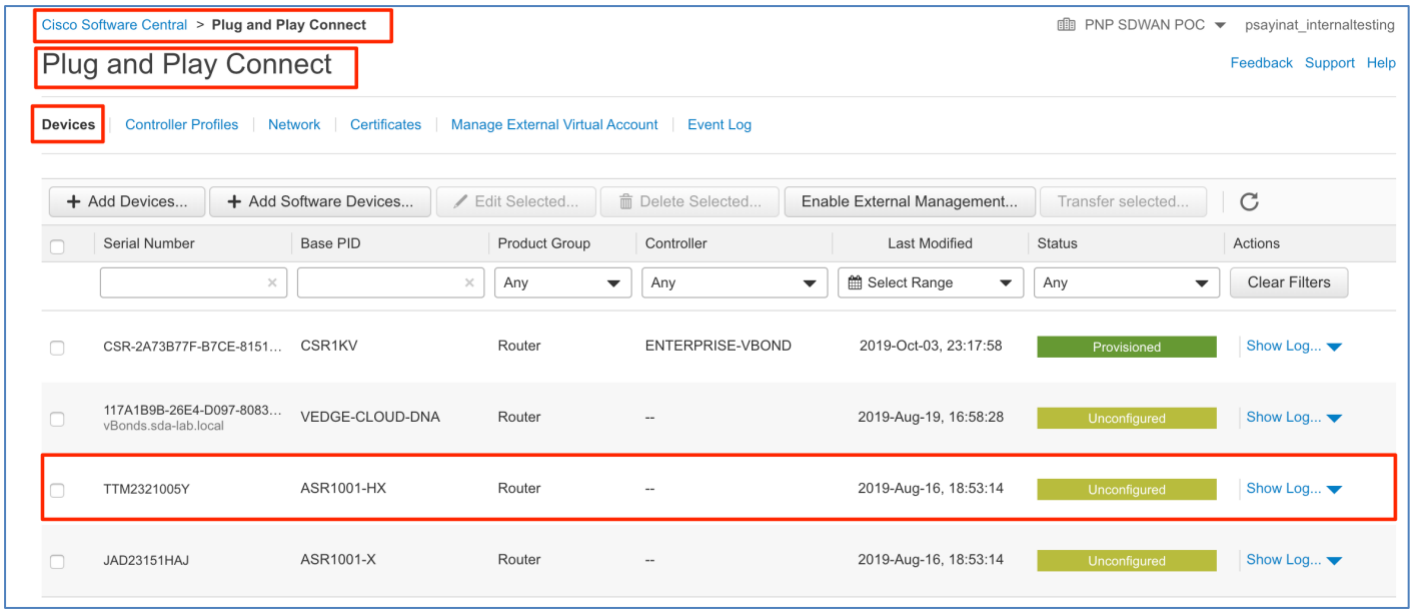


During the ordering process, Cisco assets can be associated to the Smart Account at the Cisco Commerce Workspace.

The below screenshot shows an example of the procedure to associate the device purchase order to a Smart Account, alternatively you have the flexibility to add individual devices in the order to a Smart Account.

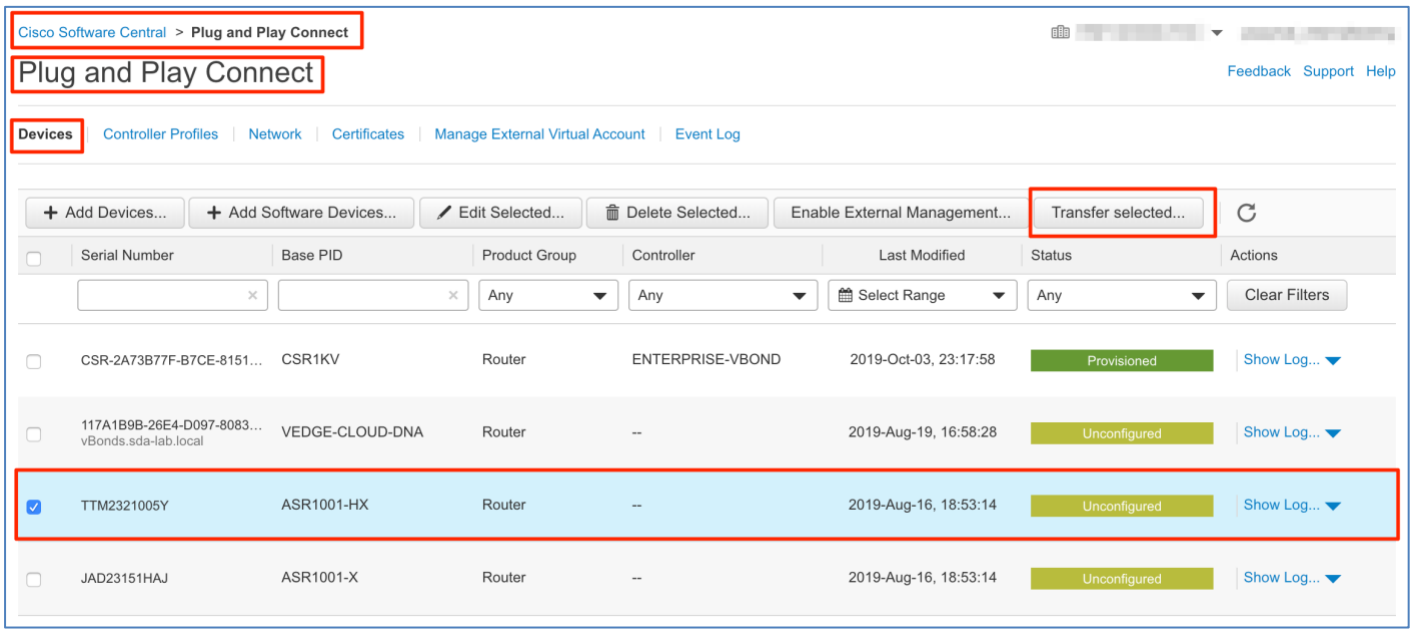


Devices shipped from manufacturing will be automatically added to the Plug and Play Connect portal. To view the complete device list associated with the smart account, log into Cisco Software Central and under the section **Network Plug and Play,** select **Plug and Play Connect**. The **Devices** tab will list the all the devices with **Serial Number** and **Status** information.

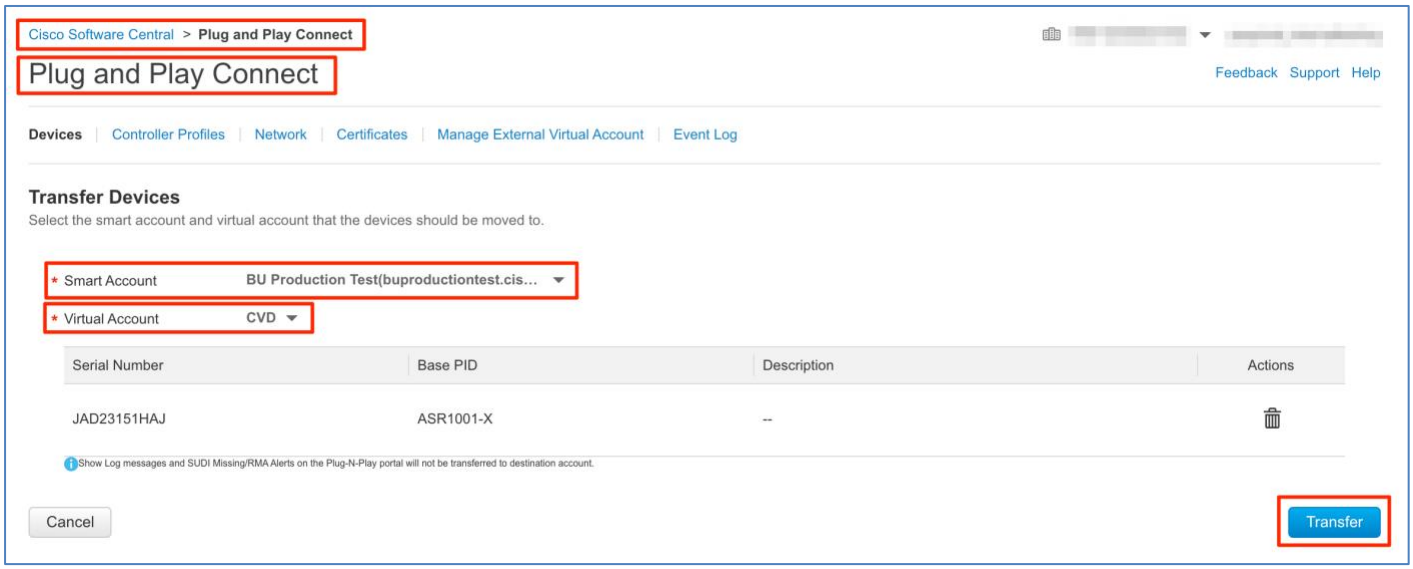


The Cisco Plug and Play portal provide the flexibility to transfer the network devices in the portal to different Smart Accounts or Virtual Accounts if necessary. Administrators with appropriate privileges can transfer the devices in the portal from one Smart Account or Virtual Account to another Smart Account or Virtual Account.

Log into Cisco Software Central **> Network Plug and Play > Plug and Play Connect**. Select the device and choose '**Transfer selected**.



To transfer the device, choose the appropriate **Smart Account** and **Virtual Account** from the drop-down menu and click **Transfer**.



Appendix D — Cisco Plug-and-Play Connect

Devices manufactured as part of the Cisco Commerce Order, with a Smart and Virtual Account assigned, will flow into the Cisco Plug-and-Play (PnP) Connect portal automatically. The Plug-and -Play portal provides administrators a centralized place to view the complete list of network devices purchased.

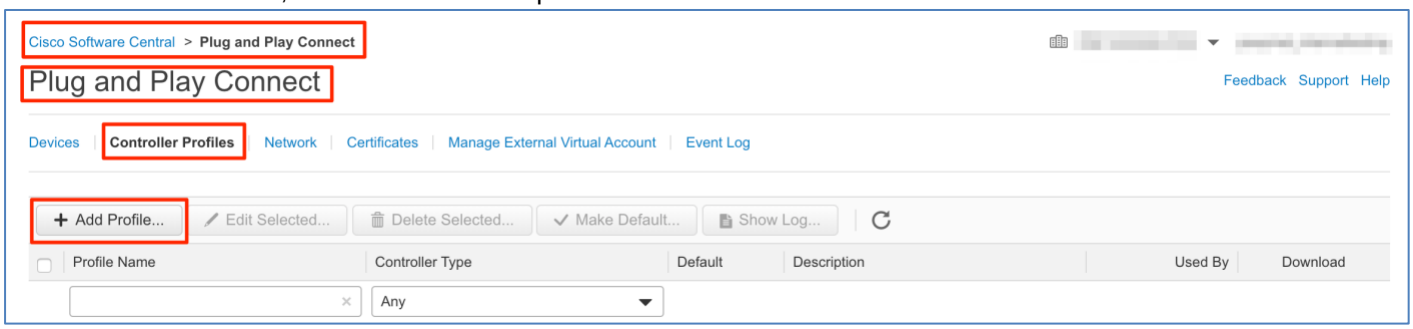
The Cisco SD-WAN solution requires the WAN Edge devices be associated with a vBond controller profile in the Plug and Play Connect portal, which is an important step in the whitelisting process, authorizing the routers to be part of the SD-WAN overlay network. The vBond controller profile contains important information such as Organization Name, vBond IP Address or Hostname information and server root-ca information that is needed for the router to successfully authenticate and join the overlay network.

For Cisco cloud-hosted SD-WAN controllers, the controller profile is automatically created based on the Smart Account and Virtual Account details. For on-premise SD-WAN deployment, the controller profile must be manually created.

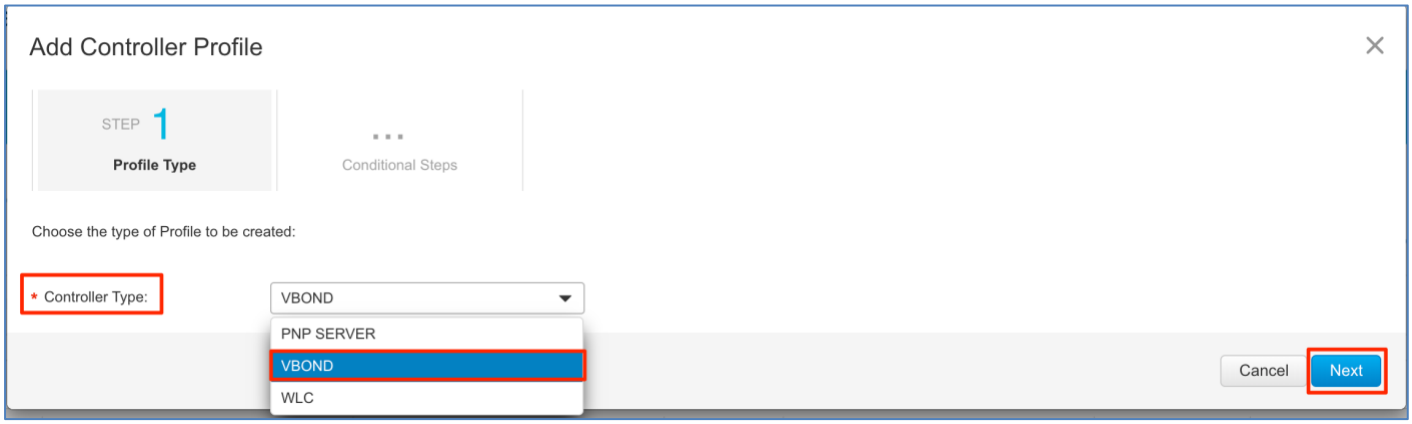
Procedure 1: Create vBond Controller Profile in Plug-and-Play Connect Portal

To create a vBond controller profile and associate the WAN Edge devices to the profile

Step 1 log into **Cisco Software Central** **> Network Plug and Play >Plug and Play Connect**. Click on the **Controller Profiles** tab, select **Add Profile** option



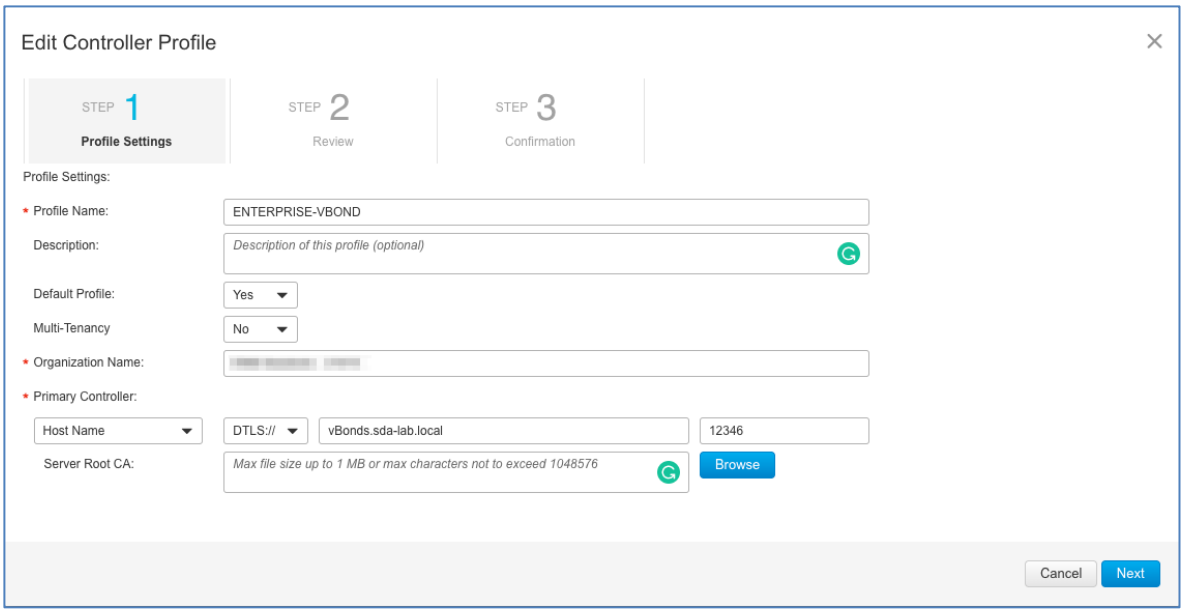
Step 2 Select **VBOND** from the drop-down menu for the **Controller Type** profile and click **Next**



Step 3 Enter **Profile Name**, **Organization Name**, and **Primary Controller** information. The Primary Controller is the vBond orchestrator information.

Please note, the Organization Name must match across all the SD-WAN components (controllers and WAN Edge devices) to be part of the same SD-WAN overlay environment.

Technical Tip: SD-WAN deployments with multiple vBond orchestrators for redundancy, choose the **Host Name** option from the drop-down menu under the **Primary Controller** section and leverage the DNS lookup to load balance which vBond orchestrator is to be used to onboard the SD-WAN WAN Edge device



Note: For SD-WAN deployments using enterprise root-ca certificates, browse and upload the root-ca certificate in the **Server Root CA** section.

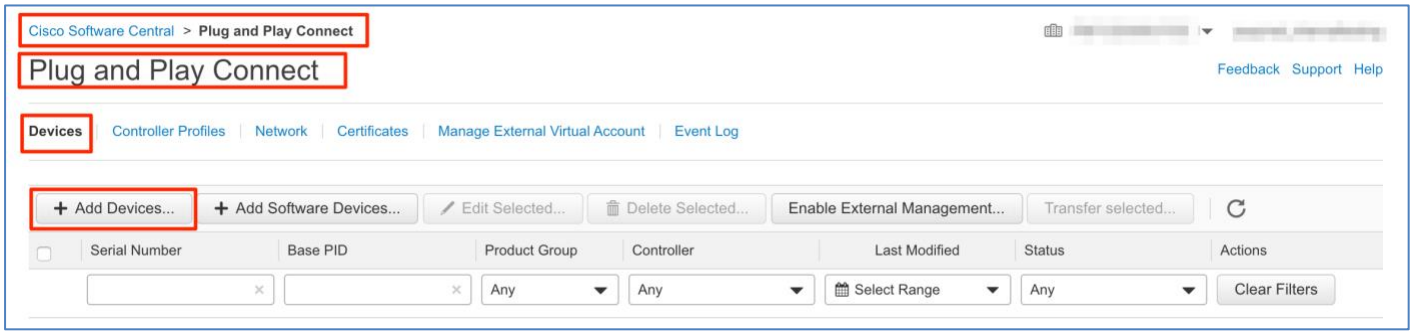
IOS-XE SD-WAN routers onboarding using the Plug-and-Play process download parameters from the Plug and Play Connect portal (vBond, Organization Name, and Root certificate if present) before initiating connections to the SD-WAN controllers.

Procedure 2: Add WAN Devices in Plug-and-Play Connect Portal

Network devices purchased with entered Smart Account and Virtual Account details are automatically added to the appropriate account in the Plug and Play (PnP) Connect portal. For devices purchased earlier or devices not in the Plug and Play Connect portal, you must add the devices manually to the portal and associate them to the controller profile. The following section walks through the steps on how to add both a physical and virtual WAN device to the PnP Connect portal and how to associate a controller profile to those devices.

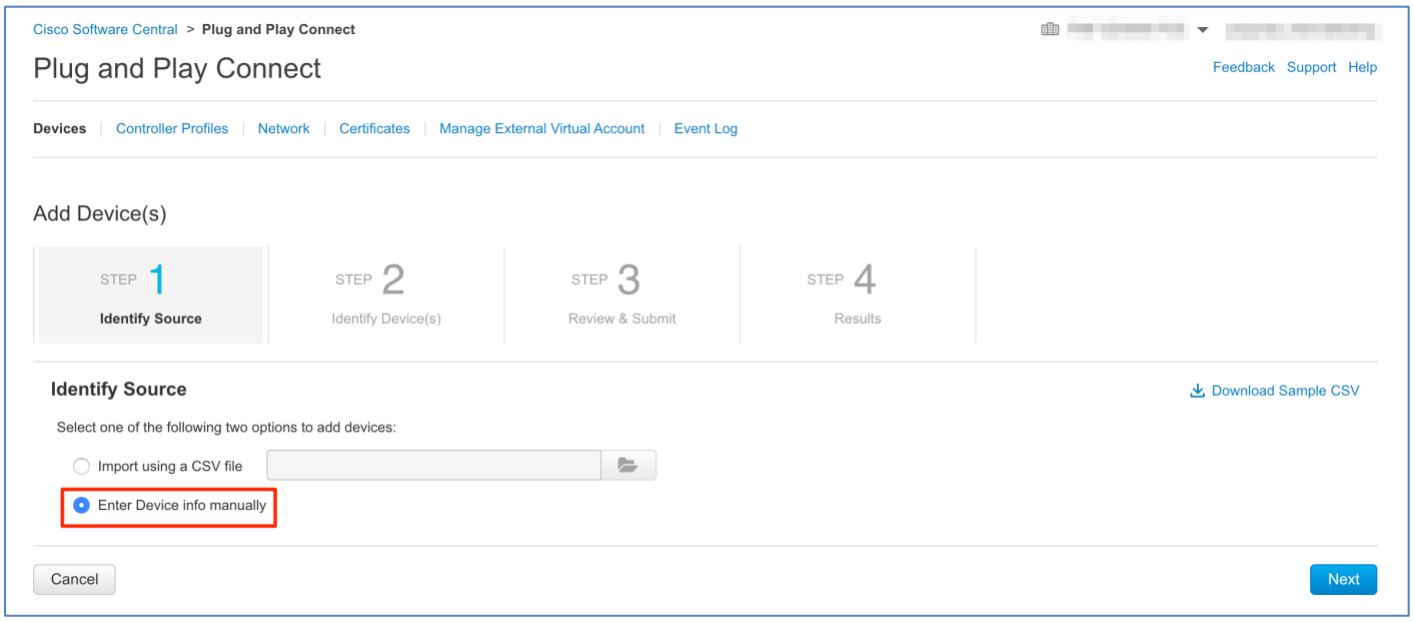
Add Physical WAN device in Plug-and-Play Connect Portal

Step 1 To add the physical WAN Edge devices (ISR, ASR1K or vEdge hardware devices) to the Plug and Play Connect portal, log **into** [Cisco Software Central](#) > **Network Plug and Play > Plug and Play Connect** and under the **Devices** tab click **Add Devices** to add the devices to the portal.

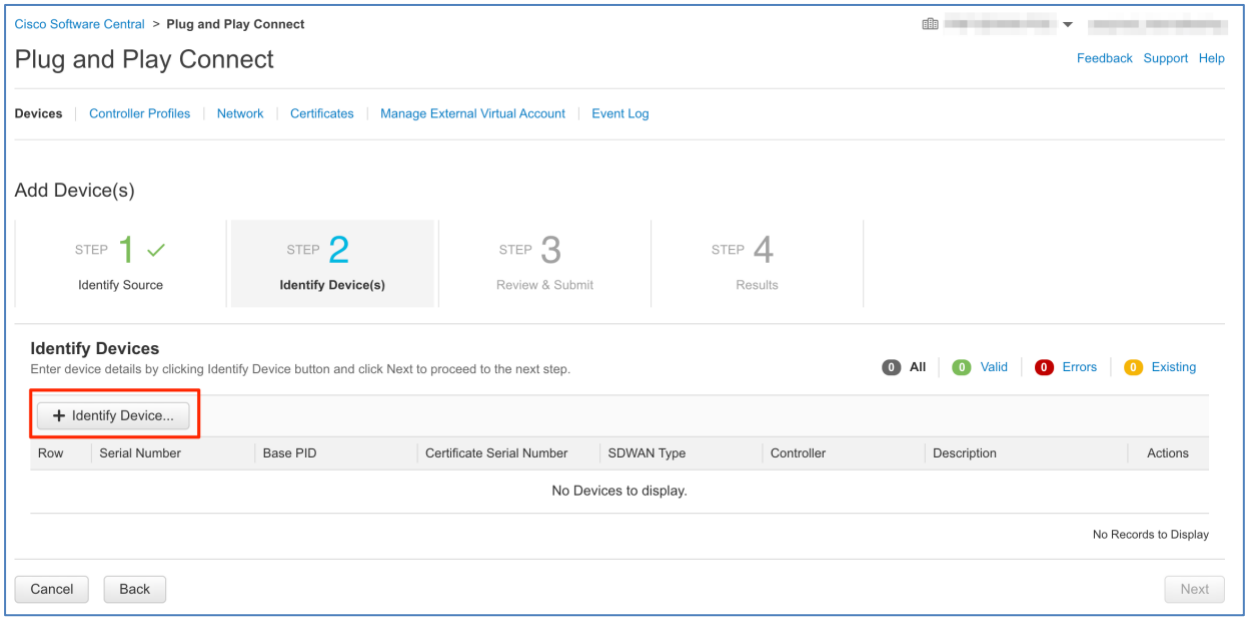


Note: Devices can be bulk imported using a CSV file or individually added as shown in the below steps.

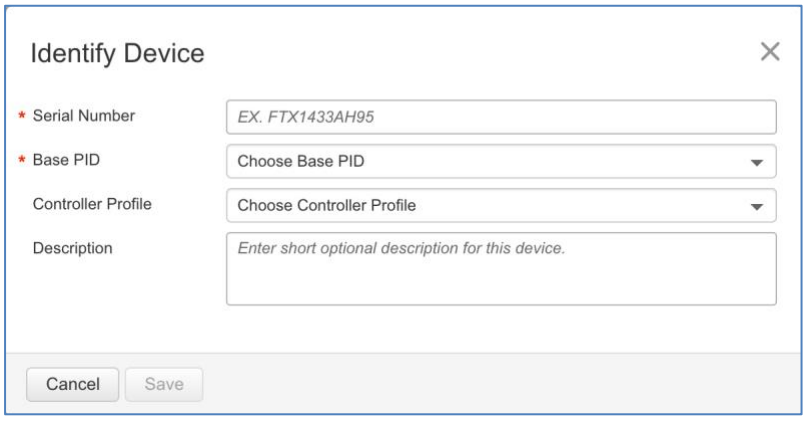
Step 2 Under the **Identify Source** section, select the option **Enter Device Info manually**. Click **Next.**



Step 3 Click **Identify Device** to add the device.



Input serial number and Base PID parameters in the **Identity Device** popup window. The next step provides ways to gather the information needed to input in the fields.



Step 4 The below steps show how to gather important information of the device that is needed to input it in the Plug-and-Play portal. The steps are categorized for IOS-XE SD-WAN and vEdge.

For **IOS-XE SD-WAN** devices**:**

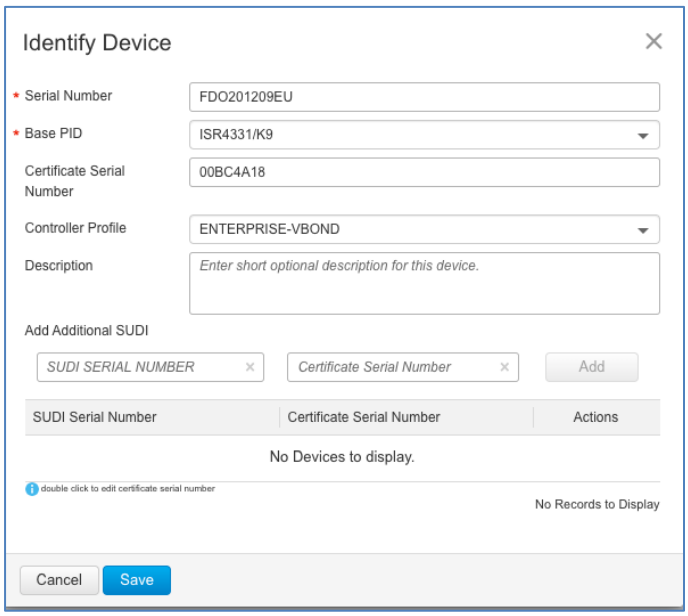
Issue **show license udi** and **show crypto pki certificates CISCO_IDEVID_SUDI** command on the device.

```
Router#show crypto pki certificates CISCO_IDEVID_SUDI
Certificate
  Status: Available
  Certificate Serial Number (hex): 00BC4A18
  Certificate Usage: General Purpose
  Issuer:
    cn=ACT2 SUDI CA
    o=Cisco
  Subject:
    Name: ISR4331/K9
    Serial Number: PID:ISR4331/K9 SN:FDO201209EU
    cn=ISR4331/K9
    ou=ACT-2 Lite SUDI
    o=Cisco
    serialNumber=PID:ISR4331/K9 SN:FDO201209EU
  Validity Date:
    start date: 15:04:15 UTC Mar 15 2016
    end   date: 15:04:15 UTC Mar 15 2026
  Associated Trustpoints: CISCO_IDEVID_SUDI
```

Note: Make sure to pick the Certificate Serial Number from the Certificate section of the output.

Technical Tip: A Certificate Serial Number is not available for the ASR1002-X or for any virtual device. When adding these PID's in the Plug and Play Connect Portal, skip adding the Certificate Serial Number option as it is not available.

Add the **Serial Number**, **Base PID**, and **Certificate Serial Number**, then select the previously created **Controller Profile** from the drop-down menu. Click **Save** and then **Next**.



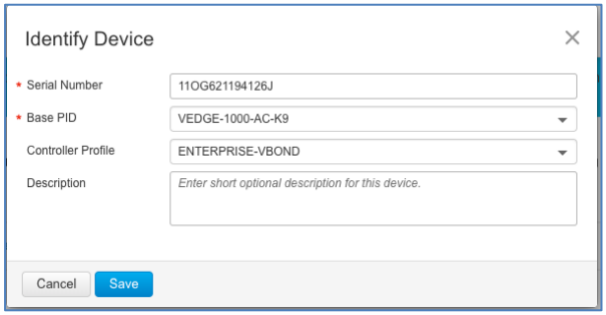
For vEdge device:

Issue **show certificate serial** command on the device.

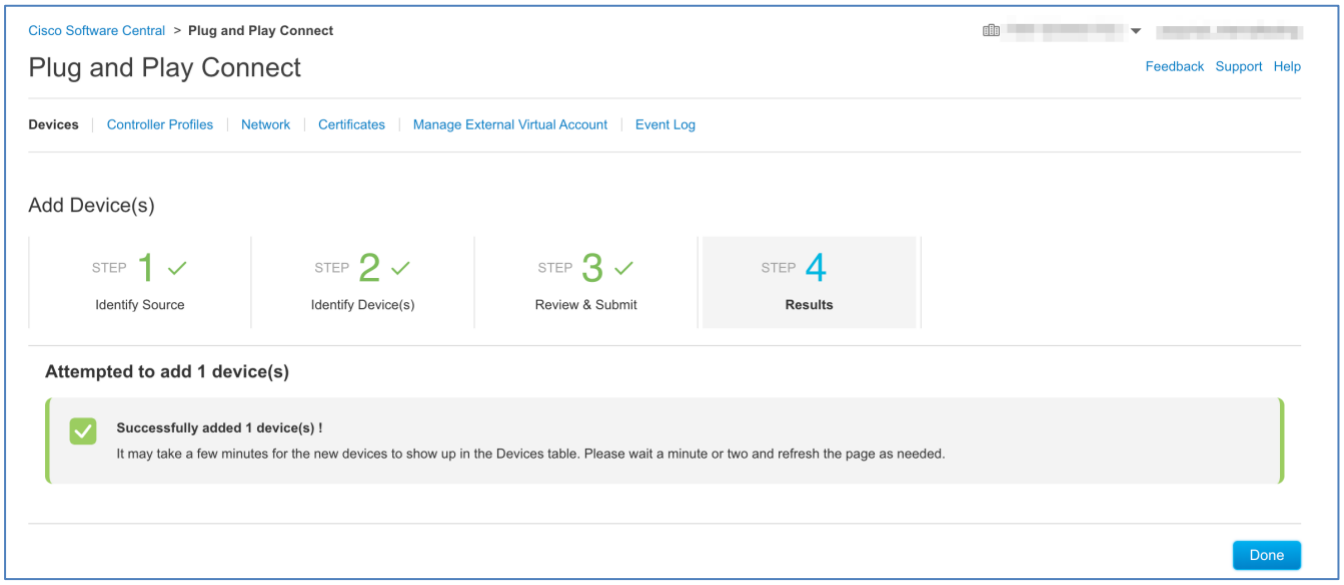
vEdge-1000# show certificate serial

Chassis number: 11OG621194126J Board ID serial number: 1001F4FA

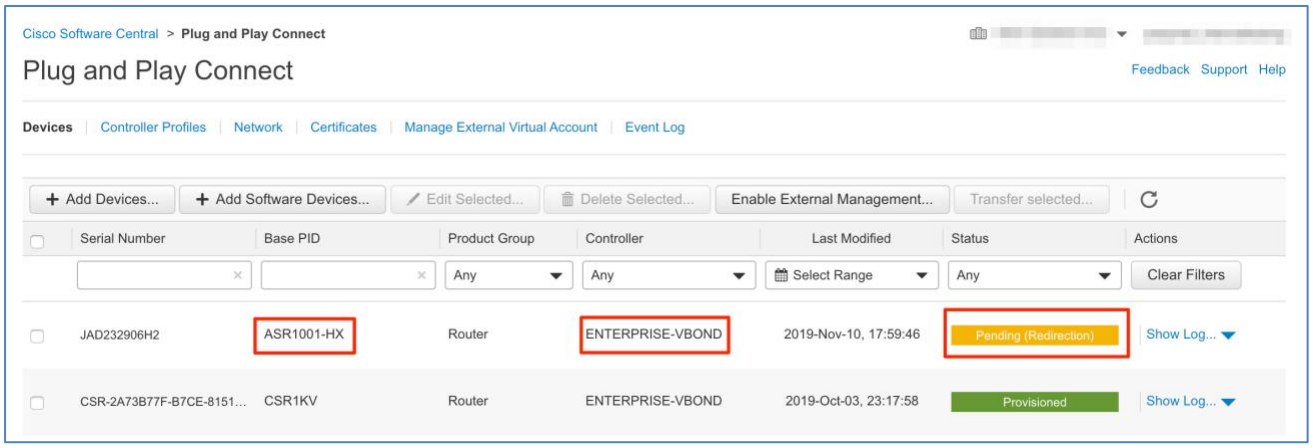
Add the **Serial Number** (this is the device chassis number) and **Base PID**, then select the previously created **Controller Profile** from the drop-down menu. Click **Save** and then **Next**.



Step 5 Review the device details and click **Submit**, click **Done.**

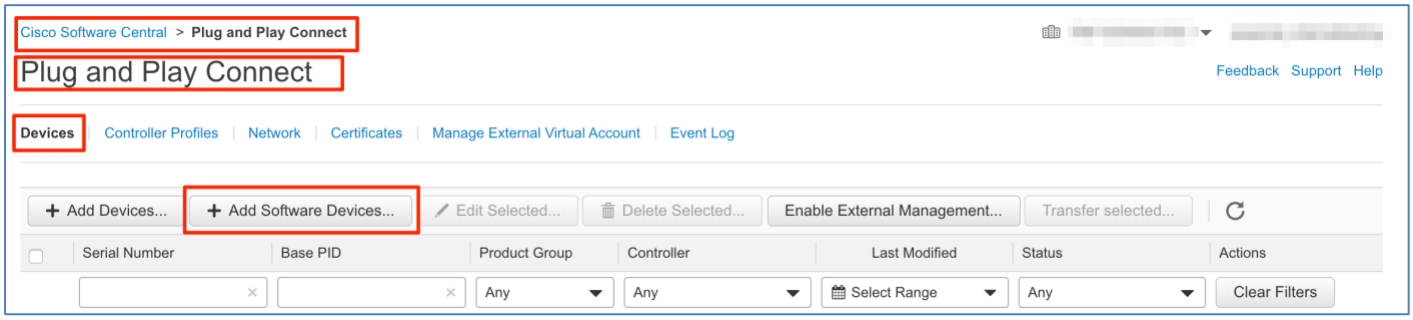


Step 6 Verify the device is successfully added to the Plug-and-Play Connect portal and associated with the vBond controller profile. Below shows an example for an ASR1001-HX device added.

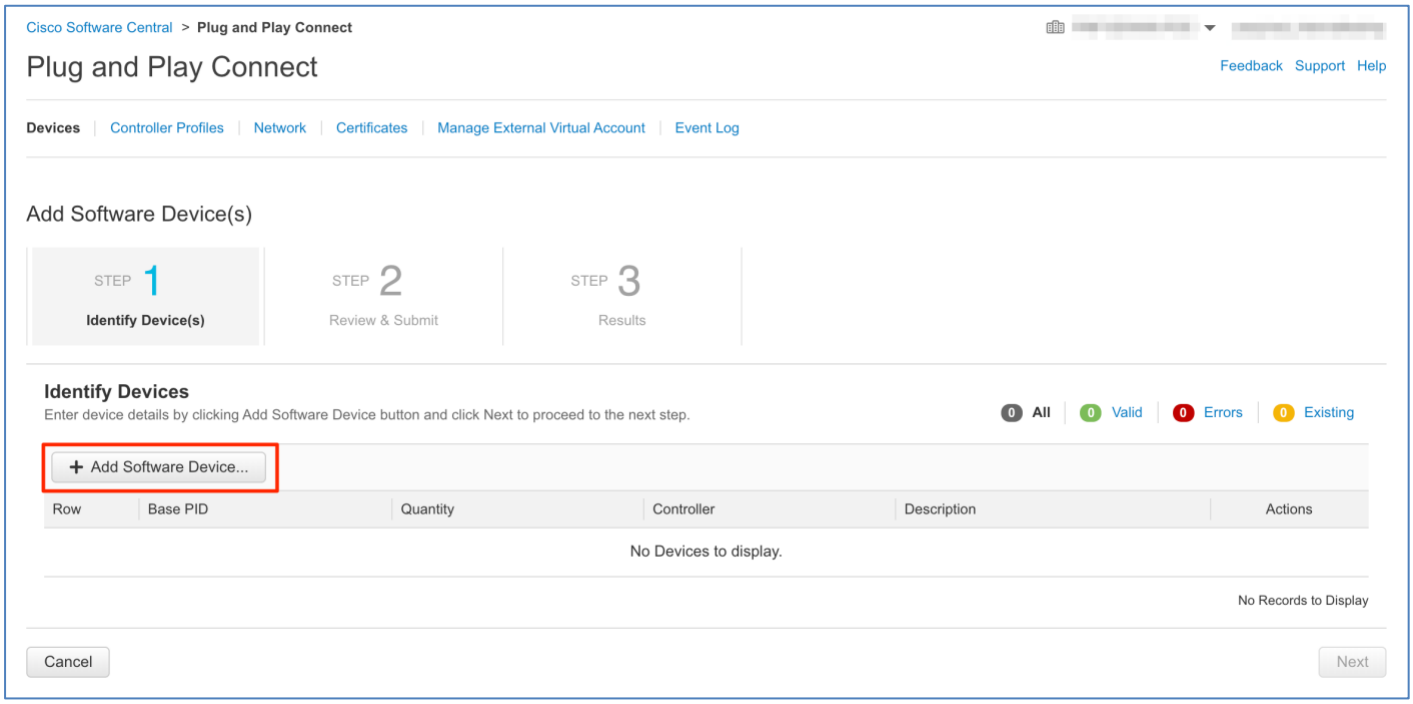


Add virtual WAN device in Plug-and-Play Connect Portal

Step 1 To add the virtual routers (ISRv, CSRv or vEdge cloud devices) to the Plug and Play Connect portal, log into Cisco Software Central > **Network Plug and Play > Plug and Play Connect**. Under the **Devices** tab, click **Add Software Devices** to add the devices to the portal.



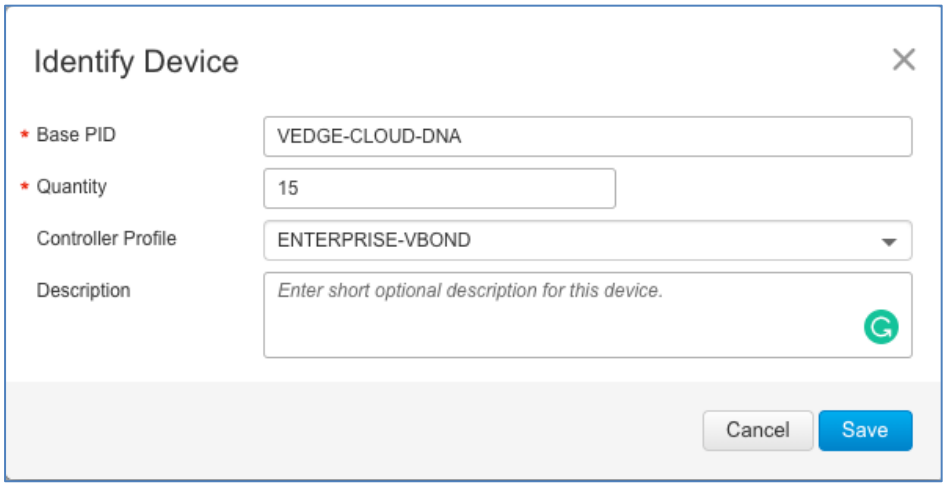
Step 2 Under Identify Devices, click **Add Software Devices.**



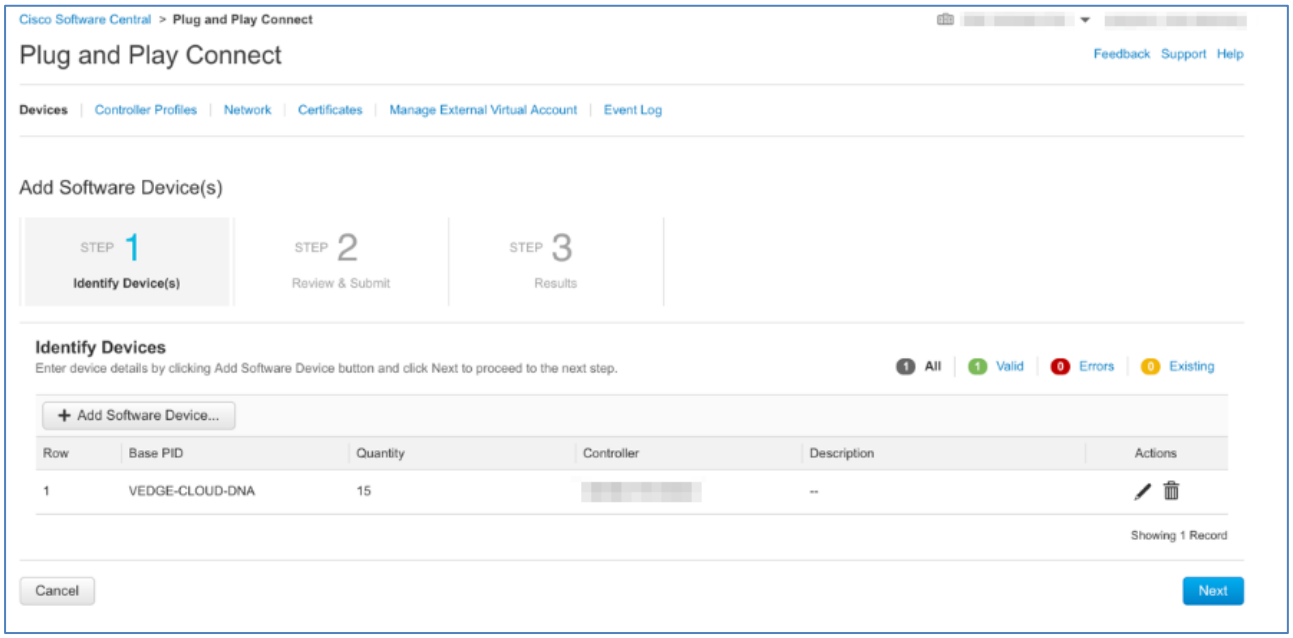
Step 3 Depending on the virtual device being added, add the following value as the Base PID:

Virtual Platform	Base ID
vEdge Cloud	VEDGE-CLOUD-DNA
Virtual ISR	ISRv
Virtual CSR	CSR1Kv

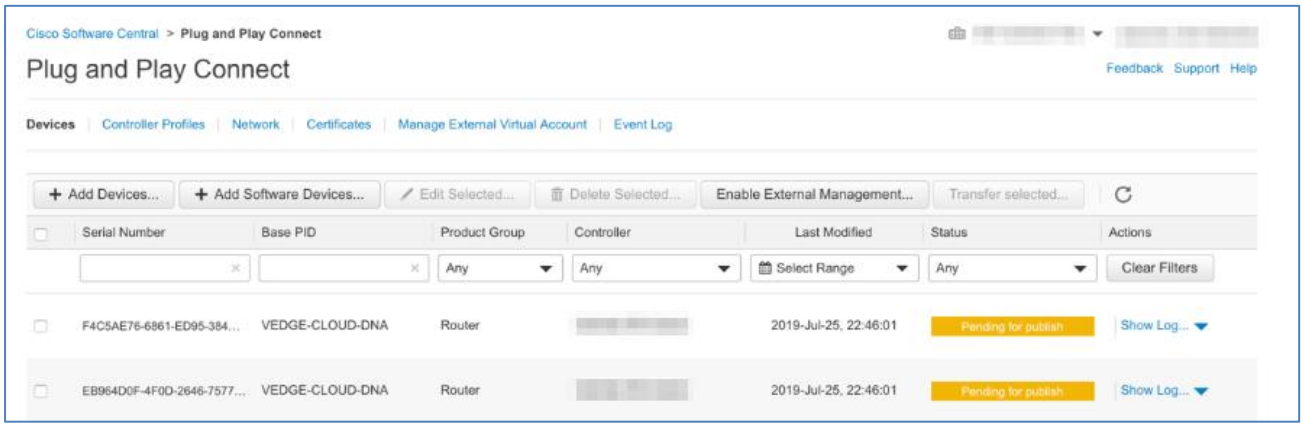
Enter the **Base PID** and **Quantity** number of the virtual devices being deployed and select the previously created **Controller Profile** from the drop-down option. Click **Save**



Step 4 Under the Identity Devices section, review the input, then click **Next** and **Submit**.



Step 5 Verify the device is successfully added to the Plug-and-Play Connect portal and associated with the vBond controller profile as shown below. Below shows an example for vEdge Cloud device added.



Procedure 3: Plug-and-Play Connect Device status

Device **Status** in the Plug-and-Play Connect portal can display any one of the following status:

- **Unconfigured**: Device has been added to the Virtual Account and is not attached to any controller profile.
- **Pending (Redirection)**: Device has been added to the Virtual Account and is attached with a controller profile. Device has not called home to obtain the redirection information of vBond information, Organization name and certificate (optional).
- **Contacted**: Device is in the state while waiting for Redirection or configuration information from the PnP connect portal.
- **Redirected**: Device status shows this message when the PnP has passed on the controller profile to the device and is waiting for a confirmation message.
- **Redirect Successful**: Device shows this message after the PnP has passed on the controller profile to the device and has received confirmation message from the device. At this time, the device has vBond, organization name and certificate (optional) information that is required to initiate connections to the vBond and other SD-WAN components.

- **Provisioned**: The state indicates that the device, that doesn't support PnP (virtual ISR, virtual CSR, vEdge or vEdge Cloud), is added to the Virtual Account and attached with a controller profile. The device is now signed (whitelisted) in the provisioning (serial) file that can be uploaded and or imported into vManage.
- **Pending for Publish**: The state indicates that the device (virtual ISR, virtual CSR, vEdge Cloud) is added to the PnP Connect Portal and will be made available in the provisioning (serial) file soon. This is a transient state, after a while the device would move to Provisioned state.
- **Error**: This suggests that something went wrong with the adding the device in the portal.

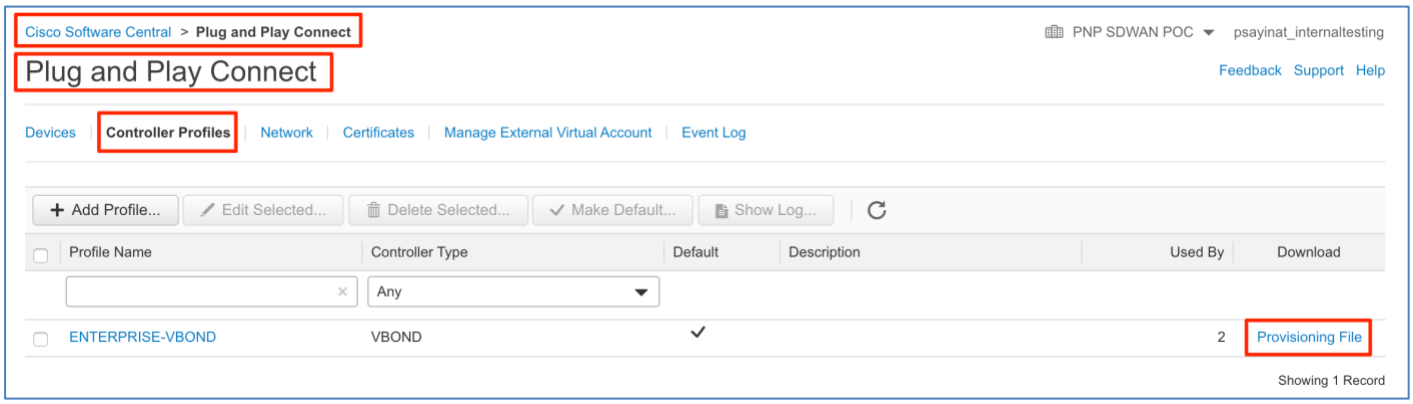
Appendix E — WAN Edge Whitelist Authorization File

Onboarding WAN Edge devices requires the SD-WAN controllers to learn the authorized device list. The whitelist device list is retrieved from the Plug and Play (PnP) Connect portal and made available to the vManage controller either by manually uploading or syncing the vManage directly with the PnP connect portal. The whitelist device list is than sent to other SD-WAN controllers from vManage.

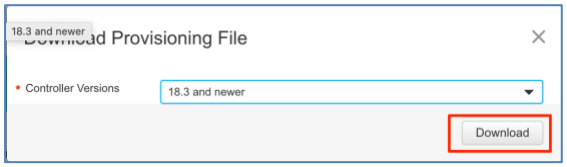
The provisioning file available in the Plug and Play (PnP) Connect portal contains the whitelist device list.

Procedure 1: Download the Provisioning File from Plug-and-Play Connect portal

Step 1 To download the provisioning file, log into Cisco Software Central and under section **Network Plug and Play,** select **Plug and Play Connect**. Click the **Controller Profiles** tab, then click the **Provisioning File** from the **Download** column.



Step 2 Select the **Controller Versions** (18.3 and newer) and click **Download**.

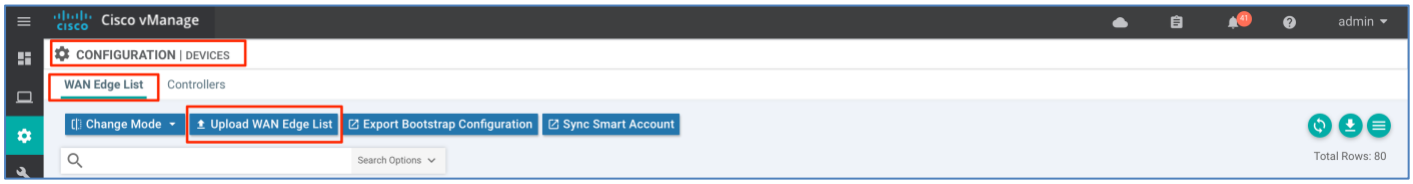


Note: 17.x version will only select vEdge Devices. 18.3 and newer version will support both vEdge and Cisco IOS XE SDWAN products.

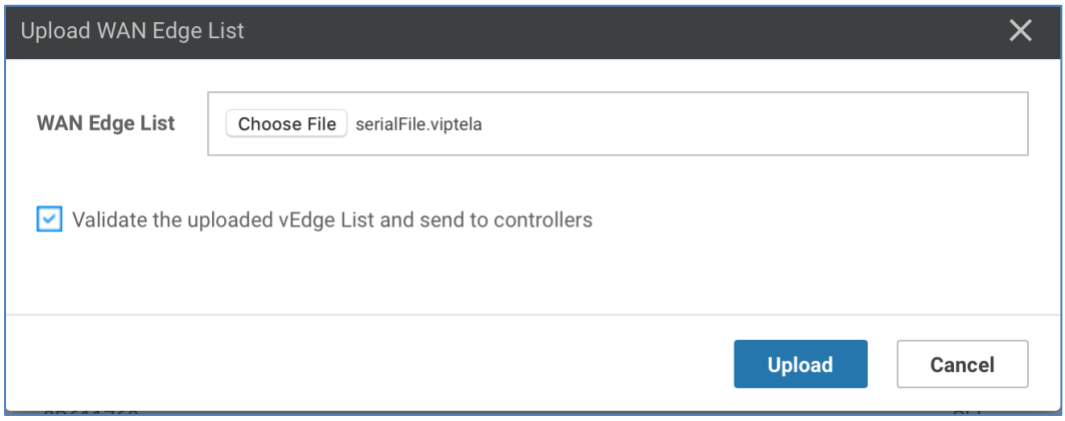
Note: The download file on the local machine is named serialFile.viptela.

Procedure 2: Manually upload the Provisioning File to SD-WAN controllers

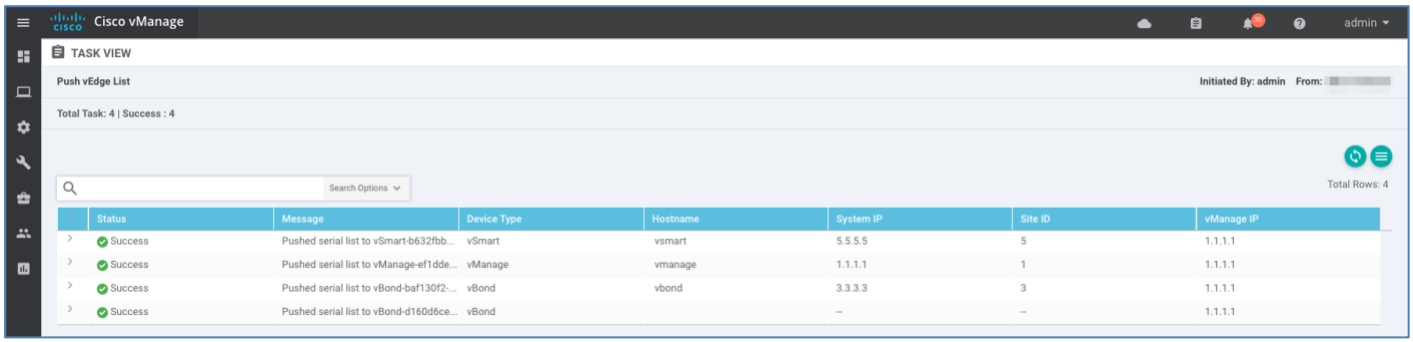
Step 1 The SD-WAN controllers must have the device whitelist available to authenticate and authorize the device to be onboarded. To upload the provisioning file in vManage, navigate to **Configuration > Devices > WAN Edge List** and click **Upload WAN Edge List**



Step 2 In the Upload WAN Edge List pop-up window, upload the previously downloaded provisioning file, check the **Validate the uploaded vEdge List and send to controllers** option, click **Upload** and click **OK**.



The authorized WAN Edge device list (both IOS-XE SD-WAN and vEdge devices) are successfully uploaded to vManage and pushed to the other SD-WAN controllers.

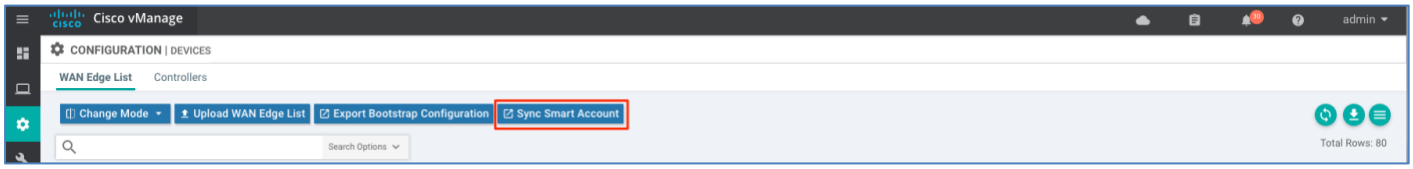


Technical Tip: If **Validate the uploaded vEdge List and send to controllers** is not selected when the provisioning file is uploaded in vManage, the WAN Edge devices will be in imported into vManage and the device will be in an Invalid state and not shared to the other SD-WAN controllers. In order to join the overlay, each WAN Edge device must be changed to a Valid state, and the updated to other SD-WAN controllers in the deployment.

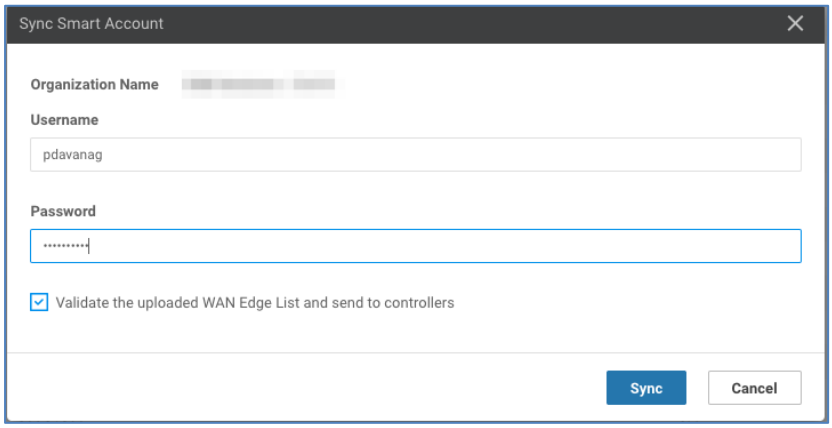
Procedure 3: Synchronize the Provisioning File to SD-WAN controllers

For deployments with vManage having reachability to the Plug-and-Play Connect server, the whitelist device list can be synced directly to vManage and made available to the other SD-WAN controllers. The vManage controller uses HTTPS to communicate with the Plug-and-Play Connect portal, and authenticates and synchronizes the list of devices with the same Organization Name as the SD-WAN controller available in the user Smart/Virtual Account.

Step 1 To synchronize the provisioning file in vManage, navigate to **Configuration > Devices > WAN Edge List** and click **Sync Smart Account**



Step 2 Provide the credentials for the Smart Account in the **Sync Smart Account** pop-up window, check the **Validate the uploaded vEdge List and send to controllers** option and click **Sync**



The Authorized WAN Edge device list (both IOS-XE SD-WAN and vEdge devices) are successfully synced with vManage and pushed to other SD-WAN controllers.

Technical Tip: If **Validate the uploaded vEdge List and send to controllers** is not selected, the WAN Edge devices will be in imported into vManage but will be in an Invalid state and not shared to other SD-WAN controllers. In order to join the overlay, each WAN Edge device must be changed to a Valid state, and the updated information pushed to the controllers.

Appendix F — Zero Touch Provisioning server

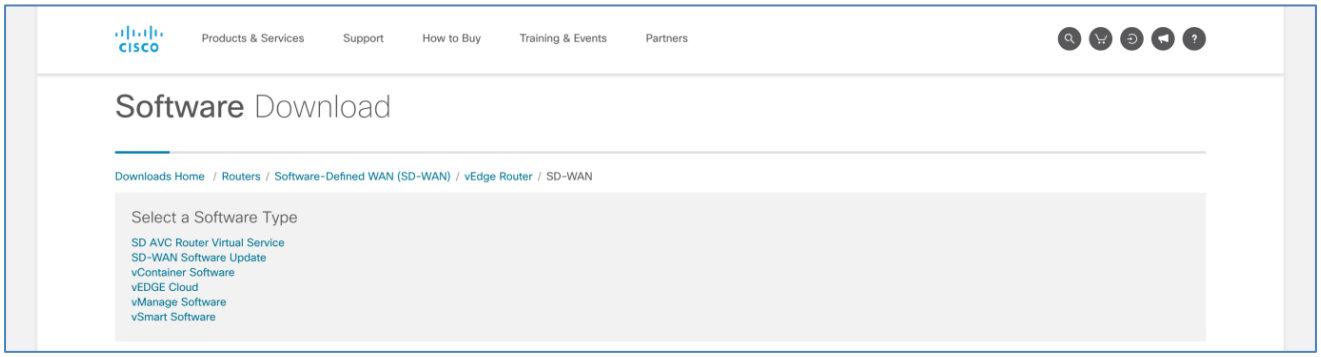
The Cisco SD-WAN solution provides automatic discovery and provisioning of vEdge hardware platform devices through the Zero-touch provisioning (ZTP) process. The ZTP process allows the vEdge device, with no configuration, to gather controller information automatically, authenticate, and then securely join the SD-WAN overlay network.

The ZTP process to onboard the vEdge devices requires an additional server, a ZTP server, to redirect the onboarding device to the enterprise vBond. The ZTP server upon authenticating the device provides basic information that is necessary for it to initiate control connections to join the overlay network such as organization name, vBond IP address or DNS name and enterprise root-ca certificates details. The ZTP server can be deployed on-premise on a virtual server or the Cisco cloud-hosted service can be leveraged. The on-prem server is a dedicated vBond server with additional configuration.

The below procedure walks through a ZTP Server deployment and configuration when deploying on-premise.

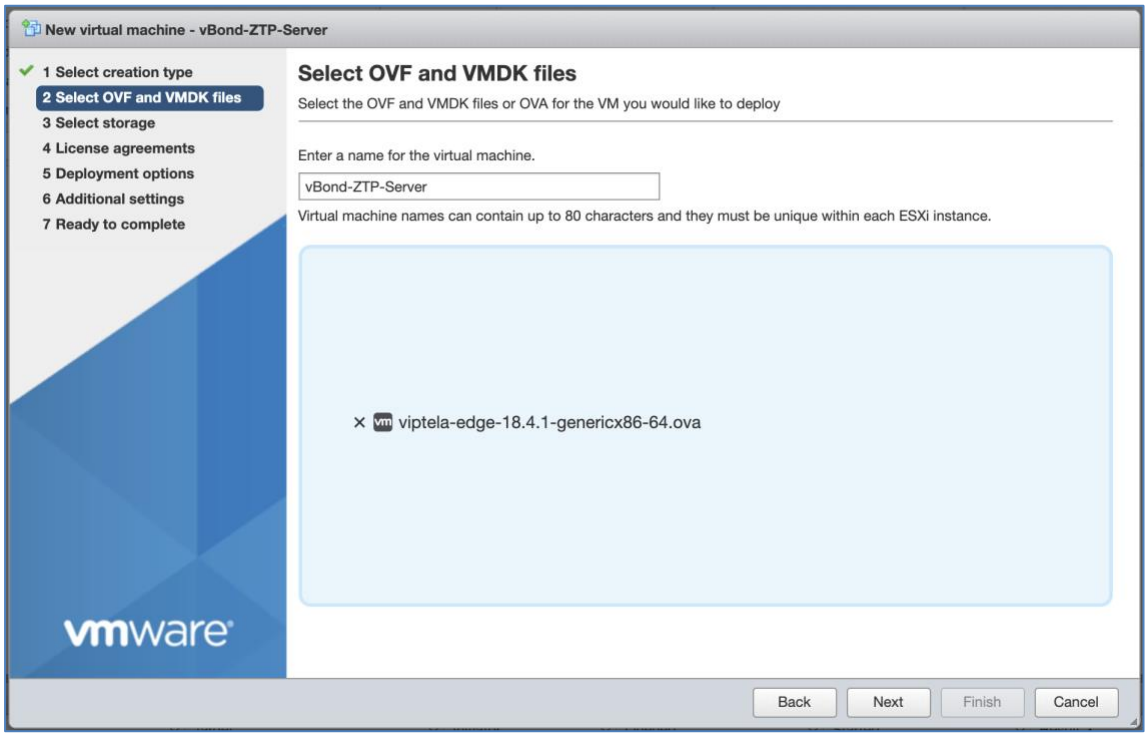
Procedure 1: Download the ZTP server

Step 1 Download the vEDGE Cloud OVF software from http://software.cisco.com

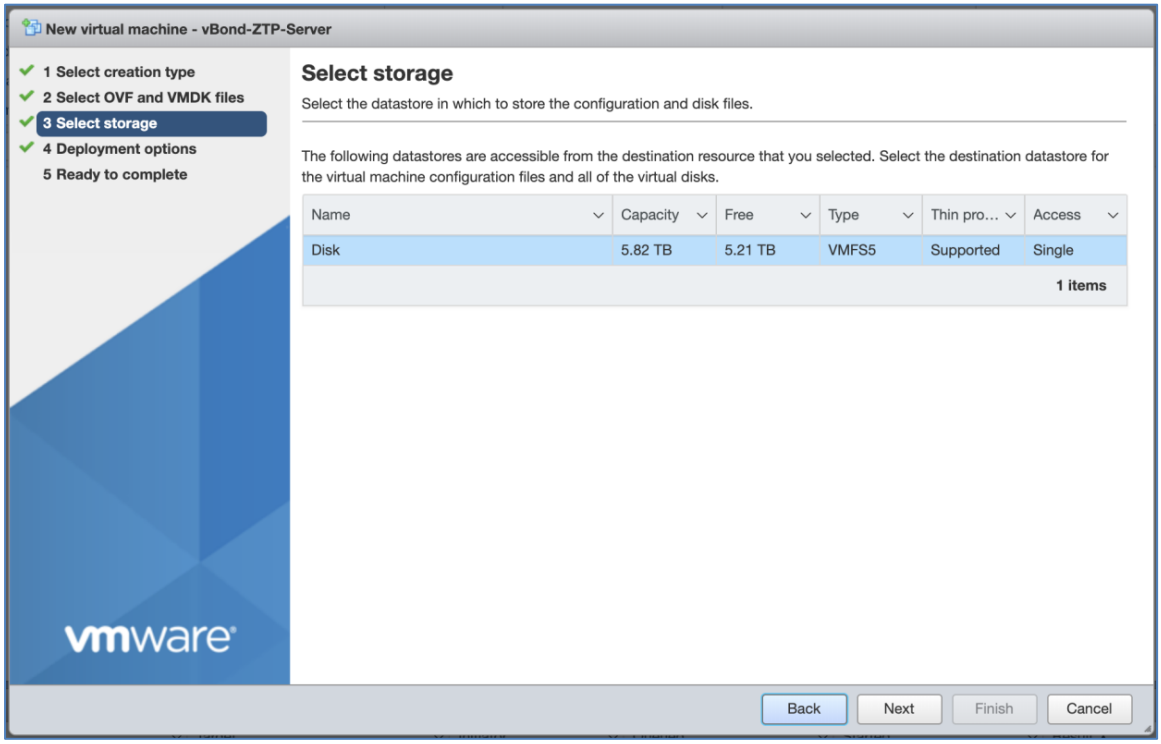


Procedure 2: Deploy the OVF template in the virtual environment.

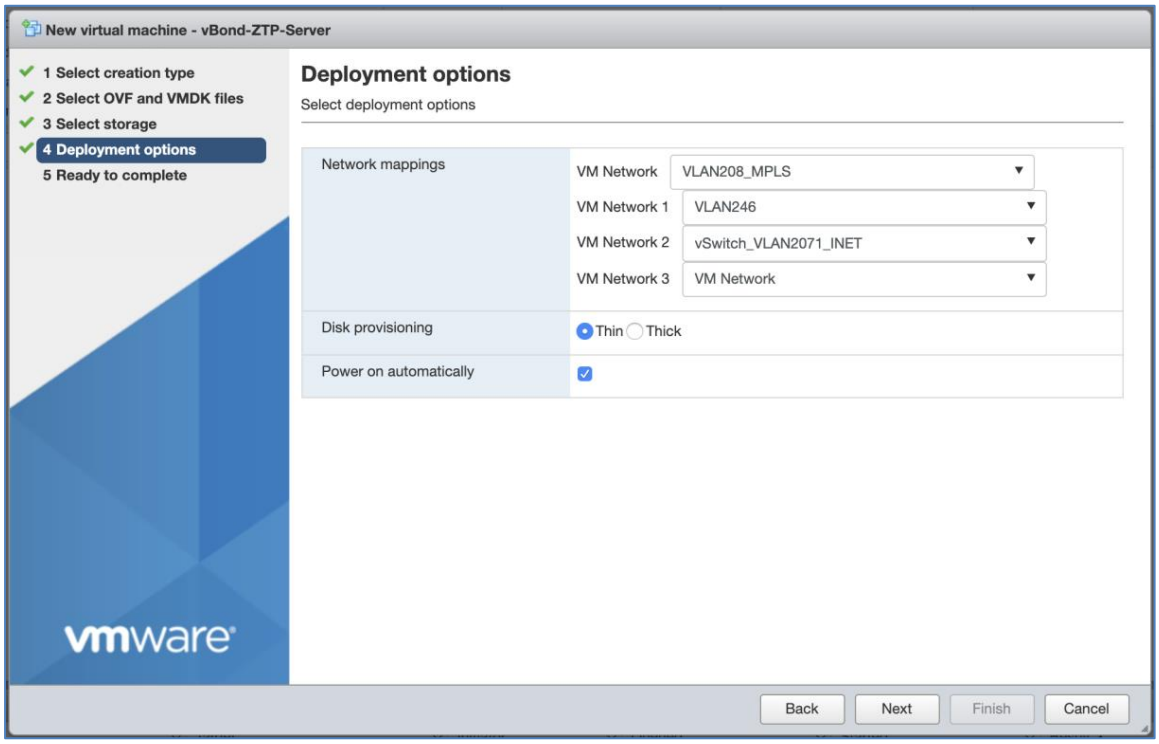
Step 1 Deploy a virtual machine with the downloaded OVF file, name the server and select the downloaded vEdge cloud image.



Step 2 Select the storage.

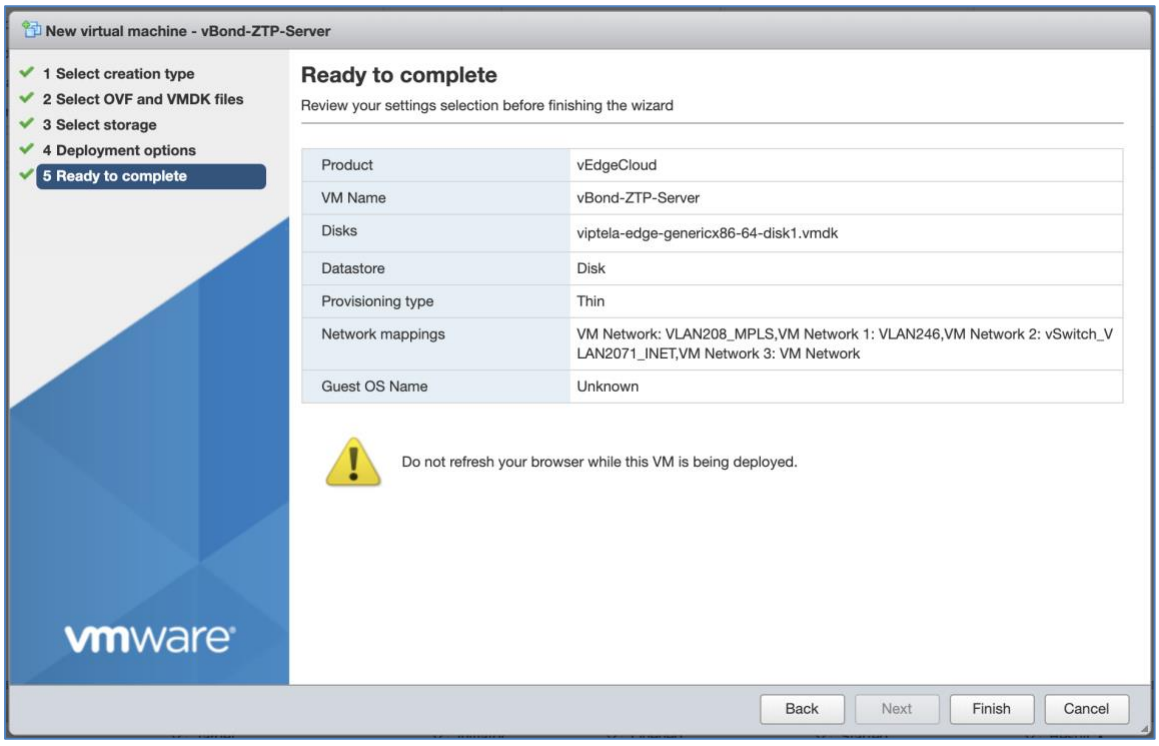


Step 3 Select the deployment options (Network mappings, Disk provisioning, and Power on automatically)



Step 4 Review your settings selection and click **Finish**.

Upon deploying the virtual router, boot the virtual machine.



Procedure 3: Configure the ZTP server

Step 1 Log into the deployed vEdge router console with the default credentials (admin / admin)

Configure the system with system parameters such as organization name and vBond. The **ztp-server** keyword in the vBond command makes this a ZTP server.

```
config
Entering configuration mode terminal
system
system-ip 9.9.9.21
site-id 21
organization-name "ENB-Solutions - 21615"
vbond 10.4.241.21 ztp-server local
host-name ZTP-Server
end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
```

Technical Tip: The IP address configured must be reachable from a vEdge device to the ZTP server across the WAN transport.

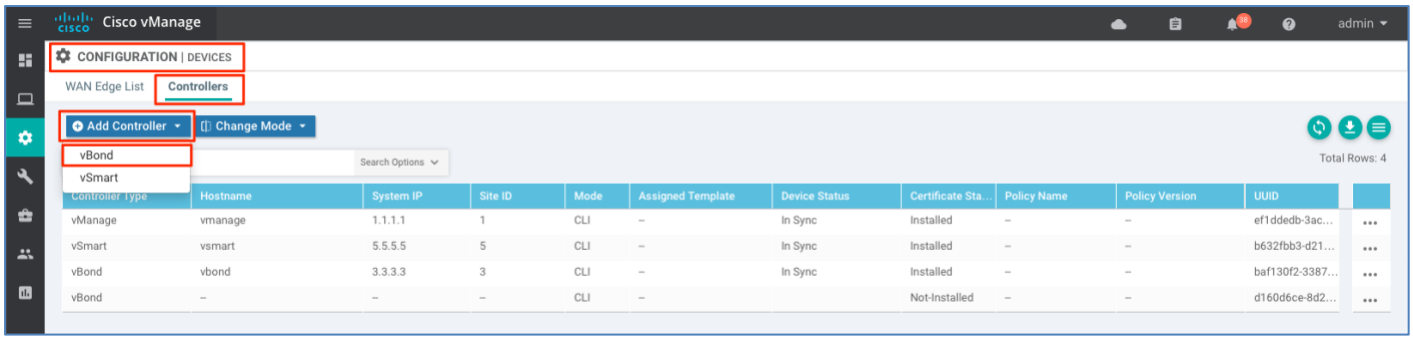
```
conf t
Entering configuration mode terminal
vpn 0
interface ge0/0
ip address 10.4.246.9/24
no shut
exit
ip route 0.0.0.0/0 10.4.246.1
end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
```

By default, the VPN 0 interface is configured with a tunnel interface. Delete the tunnel interface as this interface is used for onboarding the device and no IPsec or DTLS/TLS encryption is used.

```
config
Entering configuration mode terminal
vpn 0
interface ge0/0
no tunnel-interface
end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
```

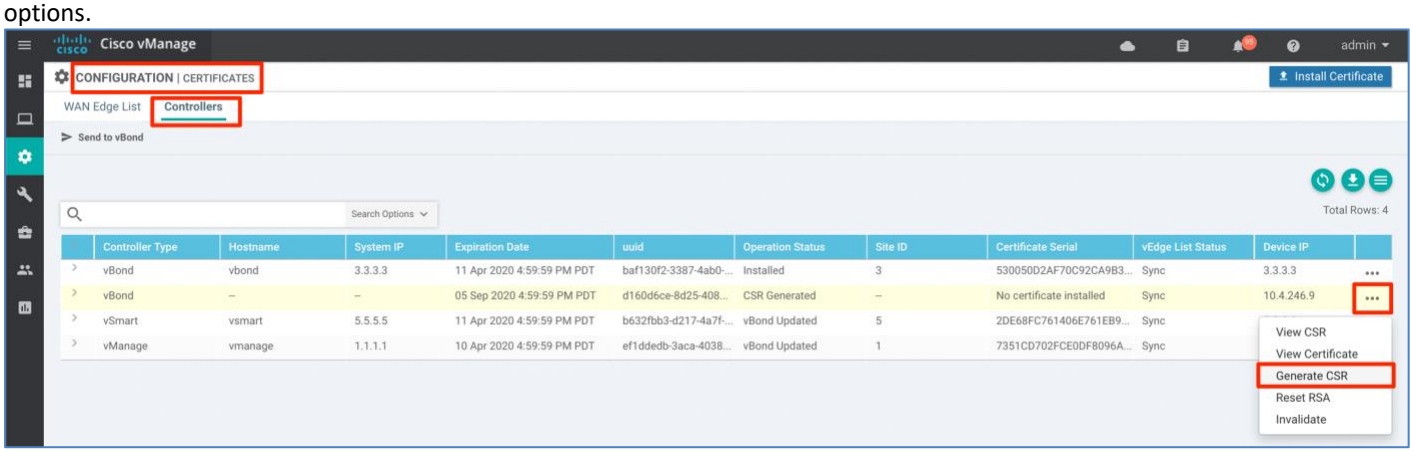
Step 2 Add the ZTP server to the vManage

Add the ZTP server in vManage, allowing the whitelist devices added in vManage to be shared with ZTP server. In vManage, navigate to **vManage** > **Configuration > Devices**, and in the **Controllers** tab**,** click **Add Controller** and select the **vBond** option from the drop-down menu.



Step 3 Generate the CSR and get the certificate signed.

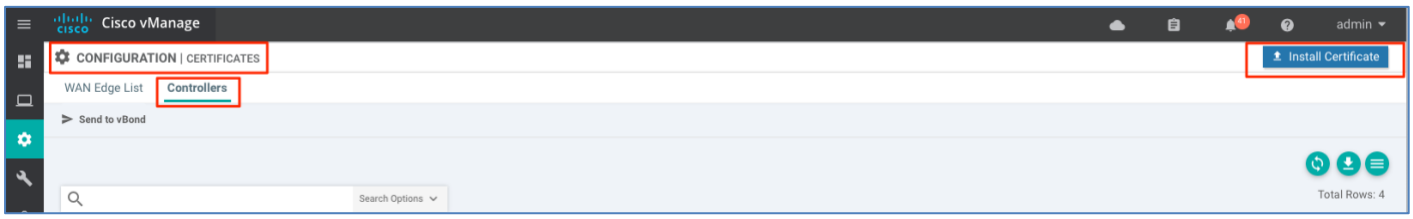
To generate the CSR for the ZTP server, navigate to **vManage** > **Configuration > Certificates**, select the **Controllers** tab**,** identify the added ZTP server device and click the three dots and choose the **Generate CSR** option from the drop-down options.



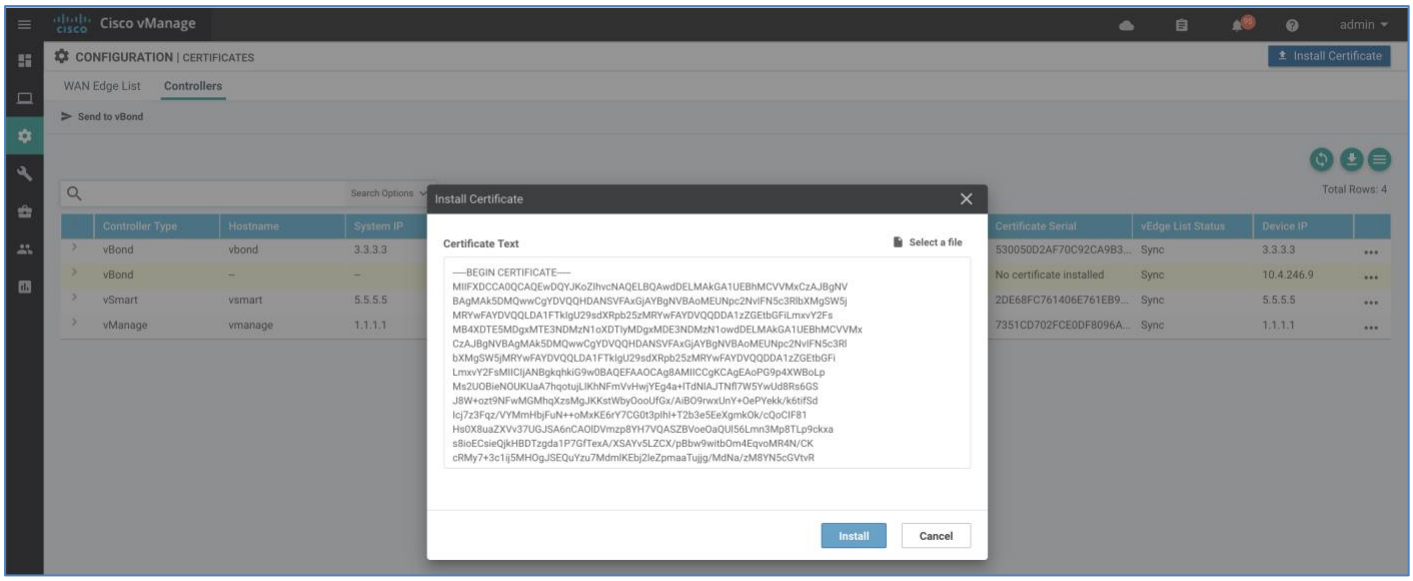
Download the CSR request and have the certificate signed by opening a case with the Cisco support team.

Step 4 Install the signed root-certificate.

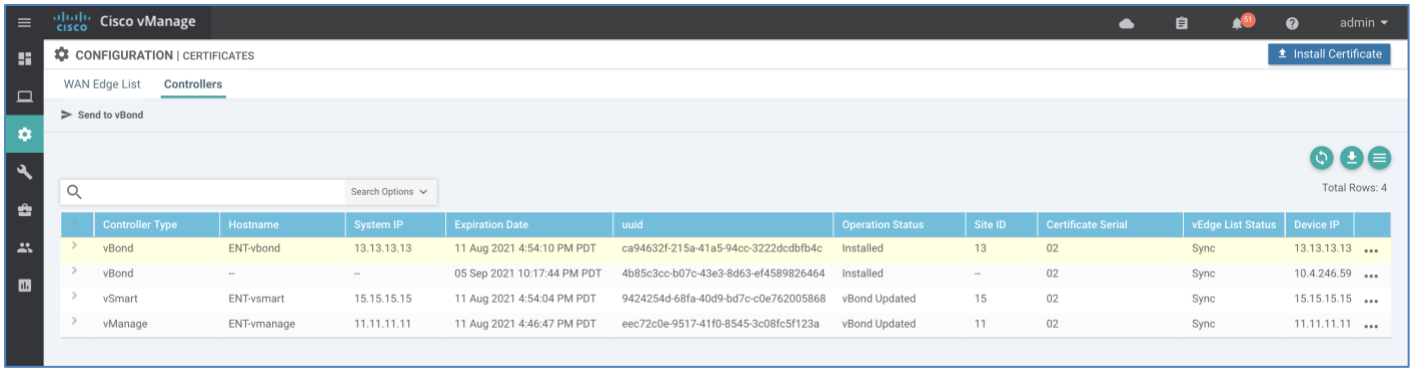
Install the signed certificate. To install the signed certificate, in vManage navigate to **Configuration > Certificates** and click the **Controllers** tab**.** Select **Install Certificate** located at the top right corner of the GUI.



Browse for the signed certificate and click **Install.**



Upon installing the certificate, the ZTP server syncs the authorized whitelisted devices.



Step 5 Verify the ZTP server has learned the valid WAN Edge list from the vManage with the **show orchestrator valid-vedges** command.

```
ZTP-Server# show orchestrator valid-vedges

CHASSIS NUMBER                          SERIAL NUMBER                                VALIDITY  ORG
-------------------------------------------------------------------------------------------------
11OG621194126J                          1001F4FA                                     valid     ENB-Solutions
14FD2266-E023-08A4-92EA-8A7B068C0ECD    2b4c46f40bdddf8edee9d5b77fe02cbe             valid     ENB-Solutions
1920C549180825J                         100175DE                                     valid     ENB-Solutions
19F2059B-5FD1-9027-A665-24C33D223247    22ee00b3a0c22d8269725d1cb495b718             valid     ENB-Solutions
1C349670-6C7E-E9D5-838A-B2E5CE195884    1f41d2e1e97ace6dc3acd9e9f71abf3e             valid     ENB-Solutions
3EBD4C47-1670-A256-D17E-5FAAB3C686C3    8a377a80b5853b5aba4d45f402c6c6e2             valid     ENB-Solutions
ASR1001-HX-JAD232906H2                  04158497                                     staging   ENB-Solutions
ASR1001-X-JAD23151HC8                   03C8C421                                     valid     ENB-Solutions
ASR1002-X-JAE19430CC3                   07ff6ee1517638fcc000a386e0f69ce9             valid     ENB-Solutions
C1111X-8P-FGL231613RW                   018EE3BB                                     valid     ENB-Solutions
C1111X-8P-FGL231613RX                   018EE411                                     valid     ENB-Solutions
CAC79453-3B15-723C-6480-37757B5DF0D3    e588e8149ec43cf177c4d8ab011d8dea             valid     ENB-Solutions
ISR4331/K9-FDO2012092M                  BC5594                                       valid     ENB-Solutions
ISR4331/K9-FDO201209EU                  BC4A18                                       valid     ENB-Solutions
```

Procedure 4: Add the vEdge devices to the ZTP device entry list

The WAN Edge device upon bootup contacts the ZTP server to request vBond, organization name and enterprise root-ca information. For the ZTP server to honor the request and provide the information, the WAN Edge device should be in the authorized device list and a ZTP entry should be available for the device.

The ZTP device entry can be added using either of the 2 methods:

- Bulk import using the CSV file
- Individually add the device using CLI command

Method 1: Bulk importing the WAN Edge device into the ZTP server.

Upload the device information using the CSV chassis file to the ZTP server using the below CLI

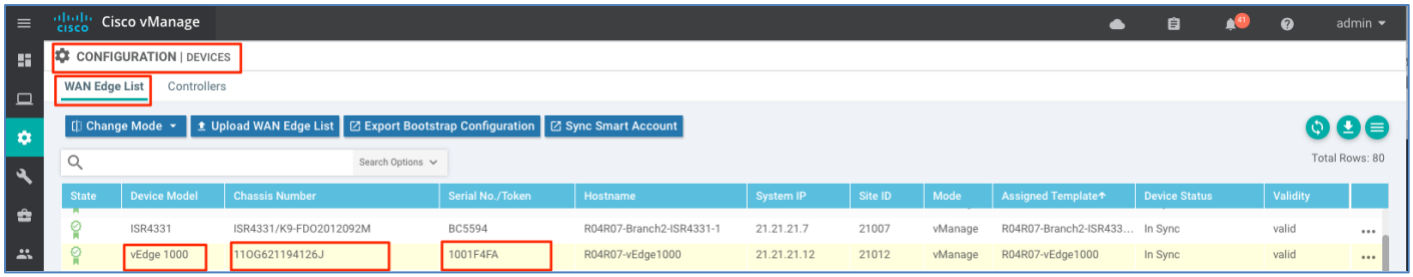
- ZTP-server# request device-upload chassis-file < http/ftp/tftp/scp:// >
- The CSV file contains the vEdge router chassis information required by the ZTP server. Each row in the CVS file must contain the below information for each vEdge router:
- vEdge router chassis number
- vEdge router serial number
- Validity (either valid or invalid)
- vBond IP address
- vBond port number (entering a value is optional)

Method 2: Individually add the WAN Edge device using CLI command.

To add the ZTP entry for the device, issue the command on the ZTP server **request device add chassis-number <device chassis-number> serial-number <device serial-number> validity valid vbond <IP address> org-name <organization-name>**

```
ZTP-Server# request device add chassis-number 11OG621194126J serial-number 1001F4FA
validity valid vbond 10.4.246.71 org-name ENB-Solutions
Chassis number 11OG621194126J successfully added to the database
```

The chassis number and the serial number for the WAN Edge device can be found in vManage. In vManage, navigate to **Configuration > Devices > WAN Edge list** to identify the device and look for values in the **Chassis Number** and **Serial No./Token** column.



To view the ZTP entry, issue **show ztp entries** on the ZTP server.

```
ZTP-Server# show ztp entries

                                                                                ROOT
                        SERIAL                                  VBOND  ORGANIZATION  CERT
INDEX  CHASSIS NUMBER   NUMBER    VALIDITY  VBOND IP          PORT   NAME          PATH
-------------------------------------------------------------------------------------------
4      11OG621194126J   1001F4FA  valid     10.4.246.71       12346  ENB-Solutions default
```

Procedure 5: Additional procedure to onboard vEdge device using Enterprise root CA certificates

For SD-WAN deployments using enterprise root-ca certificates, the WAN Edge device should also have the enterprise root-ca certificate installed in order to successfully authenticate with the SD-WAN controllers. The ZTP server can provide the enterprise root-ca along with other parameters to the WAN Edge device.

Download the root-ca certificate to the ZTP server and provide the path in the ZTP entry

```
ZTP-Server # request download tftp://Admin:C1sco123@10.4.250.249/root-ca-chain.pem

ZTP-Server #

ZTP-Server # vshell

ZTP-Server:~$ ls -lrt root-ca-chain.pem

-rw-r--r-- 1 admin admin 3968 Oct 29 14:57 root-ca-chain.pem

ZTP-Server:~$exit
```

To add the ZTP entry for the device, issue the command on the ZTP server **request device add chassis-number <device chassis-number> serial-number <device serial-number> validity valid vbond <IP address> org-name <organization-name> enterprise-root-ca <path>**

```
ZTP-Server# request device add chassis-number 11OG621194126J serial-number 1001F4FA
validity valid vbond 10.4.246.71 org-name ENB-Solutions enterprise-root-ca
/home/admin/root-ca-chain.pem

Chassis number 11OG621194126J successfully added to the database
```

To view the ZTP entry, issue **show ztp entries** on the ZTP server.

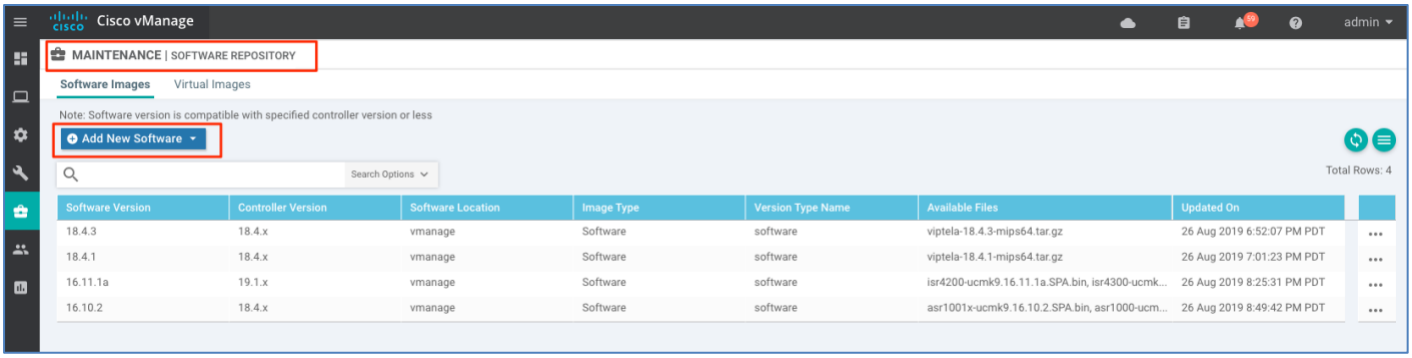
```
ZTP-Server# show ztp entries

                     SERIAL                              VBOND  ORGANIZATION
INDEX  CHASSIS NUMBER  NUMBER    VALIDITY  VBOND IP      PORT   NAME          ROOT CERT PATH
-------------------------------------------------------------------------------------------------------
5      11OG621194126J  1001F4FA  valid     10.4.246.71   12346  ENB-Solutions /home/admin/root-ca-chain.pem
```

Upon power up, the vEdge device procures an IP address, default-gateway, and DNS information from the DHCP server and requests to resolve ztp.viptela.com. To successfully resolve the domain name ztp.viptela.com to the deployed ZTP server, create an enterprise DNS A-record that redirects the DNS resolution of ztp.viptela.com to the on-prem ZTP server.

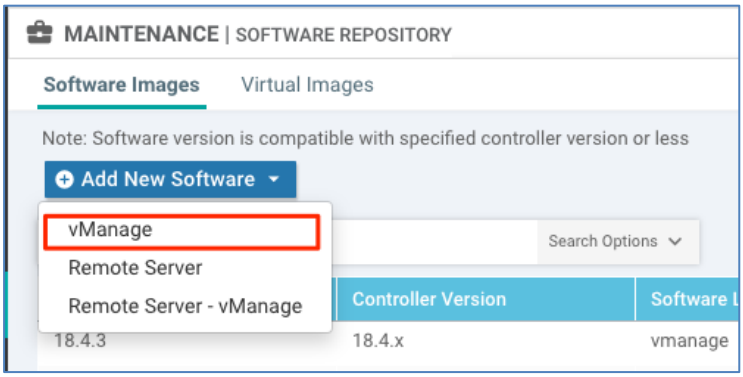
Procedure 6: Software Upgrade during ZTP process

The vEdge device software code upgrade can be done automatically during the ZTP process.

Step 1 To upgrade the software, upload the code to vManage. Navigate to **vManage > Maintenance >Software Repository** and select **Add New Software.**

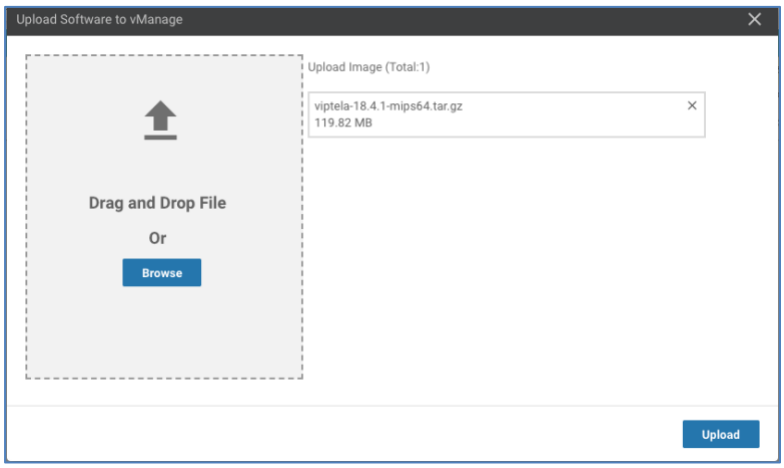


Select **vManage** from the drop-down menu.

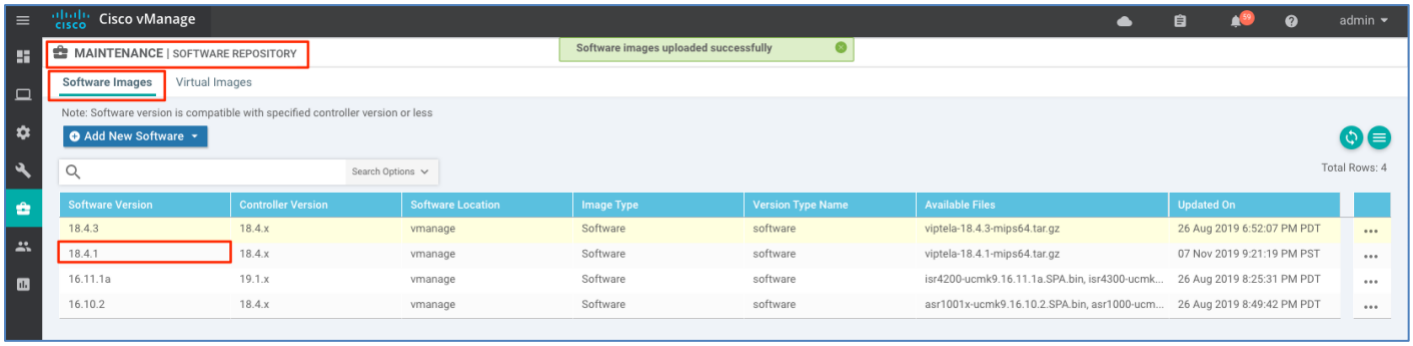


Step 2 Upload the image and have it available

In this example, download the software code from the Cisco Software Download page and upload it to vManage as shown below.



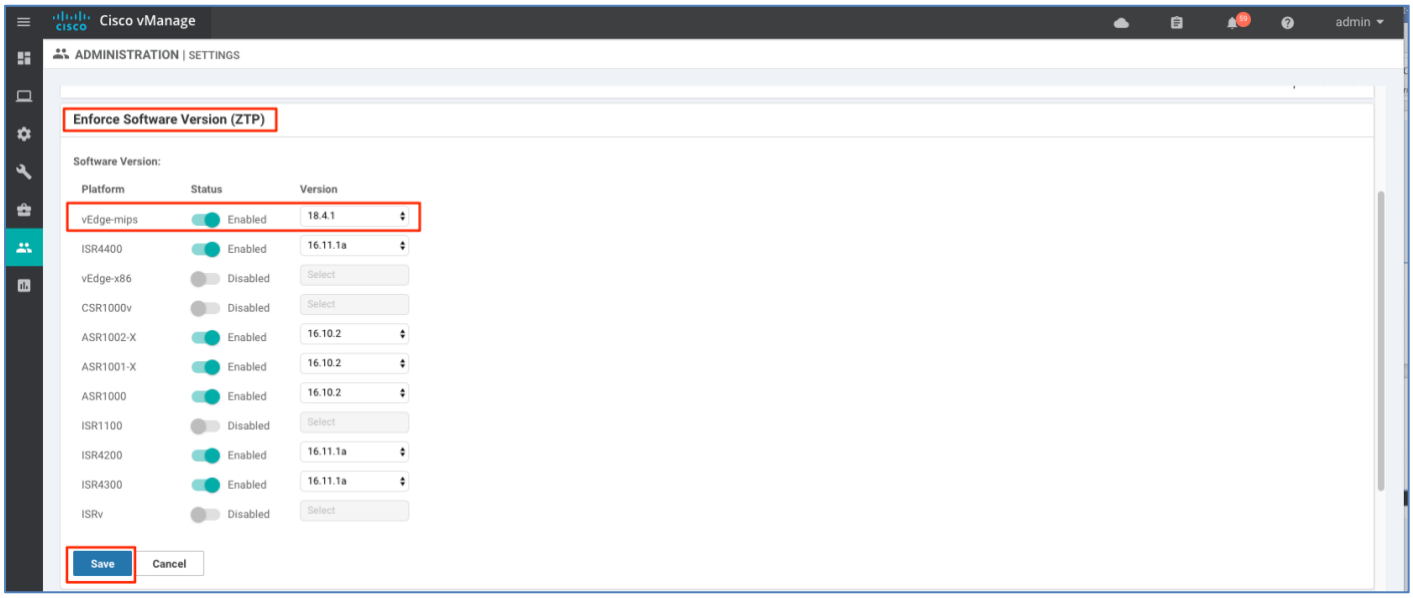
Verify the new software is uploaded and available in vManage for use.



Step 3 Enable the software upgrade during the ZTP process,

To enable software upgrade using ZTP process. In vManage, navigate to **Administration > Settings** from the vManage GUI, search the **Enforce Software Version (ZTP)** configuration and select **Edit** to the far right.

Under the expanded section, find the desired platform (**vEdge-mips**) and under **Status**, slide the bar to the right to change it to **Enabled**. Under the Version column, choose the software version to upgrade (18.4.1) and select **Save.**



Note: vEdge-x86 platform refers to vEdge Cloud device and for all physical vEdge devices choose vEdge-mips.

Appendix G - SD-WAN Device Template

This section includes the minimal feature and device templates that are used to onboard the device within the guide. The configuration is built and managed from vManage. Following device authentication with the SD-WAN controllers and successful device onboarding, vManage pushes the configuration to the device using the NETCONF protocol. For more details on deploying a feature-based device template, please refer to the SD-WAN Deployment Guide.

Feature Template

Within this section, the feature templates that are used to build the device template is shown below.

System Template

The system template configures the global system parameters for the WAN Edge device such as site id, system-ip, hostname and more.

Devices: All devices except vManage and vSmart

Template: system template

Template Name: System_Template_All_Devices

Description: System_Template_All_Devices

Section	Parameter	Type	Parameter variable / value
Basic configuration	Site ID	Device Specific	system_site_id
	System IP	Device Specific	system_system_ip
	Hostname	Device Specific	system_host_name
	Console Baud Rate (bps)	Default	

NTP Template:

The NTP template configures the global NTP parameters for the WAN Edge.

Devices: All devices except vManage and vSmart

Template: NTP template

Template Name: NTP_Template_All_Devices

Description: NTP_Template_All_Devices

Section	Parameter	Type	Parameter Variable / Value
Server	Hostname / IP address	Device Specific	ntp_server_host
	Prefer	Global	On

VPN Template

The VPN template configures the global VPN specific parameters for the WAN Edge device such as VPN number, DNS, static route and next hop information and more. In the solution, multiple VPNs are used (VPN 0 to build the SD-WAN overlay network and VPN 512 to manage the WAN Edge out-of-band).

VPN0

Devices: All devices except vManage and vSmart

Template: VPN template

Template Name: VPN0_Template_All_Devices

Description: VPN0_Template_All_Devices

Section	Parameter	Type	Parameter Variable / Value
Basic Configuration	VPN	Global	0
	Name	Global	VPN0
DNS			
	Primary DNS Address (IPv4)	Device Specific	vpn0_dns_primary
IPv4 Route New IPv4 Route	Prefix	Device Specific	vpn0_ipv4_ip_prefix
	Gateway	Next Hop	
	Next Hop	(+ Add Next Hop)	
		(+ Add Next Hop)	
	Address	Device Specific	vpn0_mpls_next_hop_ip_address
		(+ Add next hop) Device Specific	vpn0_inet_next_hop_ip_address

VPN512

Devices: All devices except vManage and vSmart

Template: VPN template

Template Name: VPN512_Template_All_Devices

Description: VPN512_Template_All_Devices

Section	Parameter	Type	Parameter Variable / Value
Basic Configuration	VPN	Global	512
	Name	Global	VPN 512
DNS	Primary DNS Address (IPv4)	Device Specific	Vpn512_dns_primary
IPv4 Route New IPv4 Route			
	Prefix	Device Specific	Vpn512_ipv4_ip_prefix
	Gateway	Next Hop	
	Next Hop	(+ Add Next Hop)	
		(+ Add Next Hop)	
	Address	Device Specific	vpn0_mpls_next_hop_ip_address

		(+ Add next hop) Device Specific	vpn0_inet_next_hop_ip_address

VPN Interface Ethernet Template

The VPN Interface Ethernet template configures the WAN Edge device interface specific parameters such as IP Address (static or dynamic), tunnel parameters, NAT, QoS and others. In this guide, 3 interfaces are used on the WAN Edge device:

- one interface connected to MPLS transport in VPN 0 to provide connectivity to SD-WAN components
- one interface connected to Internet (INET) transport in VPN 0 to provide connectivity to SD-WAN components
- one interface connected to out-of-band management in VPN 512 to manage the WAN Edge

VPN0 MPLS Interface

Devices: All devices except vManage and vSmart

Template: VPN template

Template Name: VPN0_MPLS_INT_All_Devices

Description: VPN0_MPLS_INT_All_Devices

Section	Parameter	Type	Parameter Variable / Value
Basic Configuration	Shutdown	Global	No
	Interface Name	Device Specific	vpn0_mpls_interface
	Description	Global	vpn0_mpls_interface_description
	IPV4		Static
	IPv4 Address	Device Specific	vpn0_mpls_interface_ipv4_address
	Bandwidth Upstream	Device Specific	vpn0_mpls_bandwidth_upstream
	Bandwidth Downstream	Device Specific	vpn0_mpls_bandwidth_downstream
Tunnel	Tunnel Interface	Global	On
	Color	Global	mpls
	Allow Service - BGP	Global	On
	Allow Service - DHCP	Global	Off
	Allow Service - NTP	Global	On
Advanced	Clear-Dont-Fragment	Global	On

VPN0 Internet Interface

Devices: All devices except vManage and vSmart

Template: VPN template

Template Name: VPN0_INET_INT_All_Devices

Description: VPN0_INET_INT_All_Devices

Section	Parameter	Type	Parameter variable / Value
Basic Configuration	Shutdown	Global	No
	Interface Name	Device Specific	vpn0_inet_interface
	Description	Global	vpn0_inet_interface_description
	IPV4		Dynamic
Tunnel	Tunnel Interface	Global	On
	Color	Global	biz-internet

VPN512 Out-of-Band Interface

Devices: All devices except vManage and vSmart

Template: VPN template

Template Name: VPN512_MGMT _INT_All_Devices

Description: VPN512_MGMT_INT_All_Devices

Section	Parameter	Type	Parameter variable / Value
Basic Configuration	Shutdown	Global	No
	Interface Name	Device Specific	vpn512_mgmt_interface
	Description	Global	vpn512_mgmt_interface_description
	IPv4		Static
	IPv4 Address	Device Specific	vpn512_mgmt_ipv4_address

Device Template

The device template concatenates multiple feature templates to get complete operational configuration for the WAN Edge device. A separate device template is created for each model of WAN Edge device being onboarded.

Tech Tip: A feature template can be part of multiple WAN Edge device templates. Any changes made to the feature template will affect all the devices that feature template is associate with.

Device Model: ISR4331

Template Name: Branch2-ISR4331-1_Device_Template

Description: Branch2-ISR4331-1_Device_Template

Template Type	Template Sub-Type	Feature Template Name
System	System	System_Template_All_Devices
	NTP	NTP template

VPN 0	VPN	VPN0_Template_All_Devices
	VPN Interface	VPN0_MPLS_INT_All_Devices
		VPN0_INET_INT_All_Devices
VPN 512	VPN	VPN512_Template_All_Devices
	VPN Interface	VPN512_MGMT_INT_All_Devices

The following section lists out the variable parameters used for the Branch2-ISR4331-1 device.

Device Model: ISR4331

Template Name: Branch2-ISR4331-1_Device_Template

Description: Branch2-ISR4331-1_Device_Template

Variable List	Device Value (Branch2-ISR4331-1)
Interface Name(vpn512_mgmt_interface)	GigabitEthernet0
Description(vpn512_mgmt_interface_description)	VPN512_MGMT_Interface
IPv4 Address(vpn512_mgmt_ipv4_address)	100.119.112.27/24
DNS Address(vpn0_dns_primary)	10.4.249.102
Prefix(vpn0_ipv4_ip_prefix)	0.0.0.0/0
Address(vpn0_mpls_next_hop_ip_address)	10.5.208.41
Address(vpn0_inet_next_hop_ip_address)	10.5.207.41
Interface Name(vpn0_mpls_interface)	GigabitEthernet0/0/1
Description(vpn0_mpls_interface_description)	MPLS_Interface
IPv4 Address(vpn0_mpls_interface_ipv4_address)	10.5.208.42/30
Bandwidth Upstream(vpn0_mpls_bandwidth_upstream)	95
Bandwidth Downstream(vpn0_mpls_bandwidth_downstream)	95
Interface Name(vpn0_inet_interface)	GigabitEthernet0/0/0
AS Number(bgp_as_num)	5000
Router ID(bgp_router_id)	10.5.208.42
Network Prefix(bgp_network_network_address_prefix)	10.5.208.40/30
Address(mpls_bgp_neighbor_address)	10.5.208.41
Description(mpls_bgp_neighbor_address)	MPLS_PE2_Interface
Remote AS(mpls_bgp_neighbor_remote_as)	65000
Hostname(system_host_name)	Branch2-ISR4331-1
System IP(system_system_ip)	21.21.21.7

Site ID(system_site_id)	21007
Hostname/IP Address(ntp_server_host)	10.4.249.102

Appendix H – Upgrading software to SD-WAN IOS-XE Software

The Cisco SD-WAN Solution can be deployed on the existing Cisco IOS-XE routing products by upgrading rommon and software versions on the supported platforms in order to run IOS-XE SD-WAN software. With the ROMMON and software upgrade, Cisco devices such as ISRs or ASRs running an IOS XE image can support SD-WAN feature functionality providing brownfield migration support.

Please check the compatibility matrix and rommon requirements matrix in the Release Notes for the latest details on the supported platform, network module and minimum software/ROMMON version that is needed before going any further with the upgrade. If needed, perform the ROMMON upgrade first, before loading the IOS-XE SD-WAN software on the Cisco IOS XE platform.

Minimum Rommon software version:

Platform	Rommon Version	Memory
ASR 1000	16.3 (2r)	8GB
ASR 1002-X	16.7 (1r)	8GB
ISR 4000	16.7 (3r)	4GB
ISR 1100	16.8 (1r)	4GB

Note: ROMmon auto-upgrade is supported on the ISR 4000 series routers, beginning with 16.9.1 and all subsequent releases and for ISR 1000 series routers, beginning with 16.10.3 and 16.12.1b. For older versions, the rommon needs to be upgraded manually.

Procedure 1: Upgrade Software ROMmon

Step 1 Issue a **show platform** and view the **Firmware Version** column for the current rommon firmware version installed on the platform. If the rommon upgrade is not needed, skip to the next step and proceed with the IOS-XE SD-WAN software upgrade.

Step 2 Copy the rommon software to the bootflash using the below command

```
ISR4351#copy ftp://admin:c1sco123@192.168.254.51/isr4200_4300_rommon_169_1r_SPA.pkg
bootflash:
```

Step 3 Upgrade the rommon software with the below command

```
ISR4351#upgrade rom-monitor filename bootflash:isr4200_4300_rommon_169_1r_SPA.pkg all
```

After the ROMMON upgrade is completed, reload the device to make the new ROMMON version permanent.

```
ISR4351#reload
```

```
Router#sh platform

Chassis type: ISR4331/K9

...


Slot      CPLD Version        Firmware Version

--------- ------------------- ----------------------------------------

0         15030325            16.7(3r)

1         15030325            16.7(3r)

R0        15030325            16.7(3r)

F0        15030325            16.7(3r)
```

Procedure 2: Upgrade Software version on device

The below steps walk through how to upgrade the device with IOS-XE SD-WAN software image

Step 1 Copy the IOS XE SD-WAN image into bootflash

```
ISR4351#copy ftp://admin:c1sco123@192.168.254.51/isr4300-ucmk9.16.9.3.SPA.bin
bootflash:
```

Step 2 If needed, backup and save the running configuration to device bootflash using the CLI command below.

```
ISR4351#copy run bootflash:original-xe-config
```

Step 3 Remove any existing boot statements on the device

```
ISR4351#sh run | include boot

boot-start-marker

boot system flash bootflash:isr4300-universalk9.16.03.07.SPA.bin

boot-end-marker


ISR4351#config t

Enter configuration commands, one per line. End with CNTL/Z.

ISR4351(config)#no boot system flash bootflash:isr4300-universalk9.16.03.07.SPA.bin

ISR4351#write mem
```

Step 4 Configure, verify the boot statement and reload the device to load the IOS-XE SD-WAN software image.

```
ISR4351#config t

Enter configuration commands, one per line. End with CNTL/Z.

ISR4351(config)#boot system flash bootflash:isr4300-ucmk9.16.9.3.SPA.bin


Ensure that the config register is set to 0x2102, so that the image will boot
properly from bootflash

ISR4351(config)#config-reg 0x2102

Save the configuration so that the boot variables will be saved

ISR4351#write mem


ISR4351#show bootvar

BOOT variable = bootflash:isr4300-ucmk9.16.9.3.SPA.bin,1;

CONFIG_FILE variable does not exist

BOOTLDR variable does not exist

Configuration register is 0x2102 (will be 0x2012 at next reload)


ISR4351#reload
```

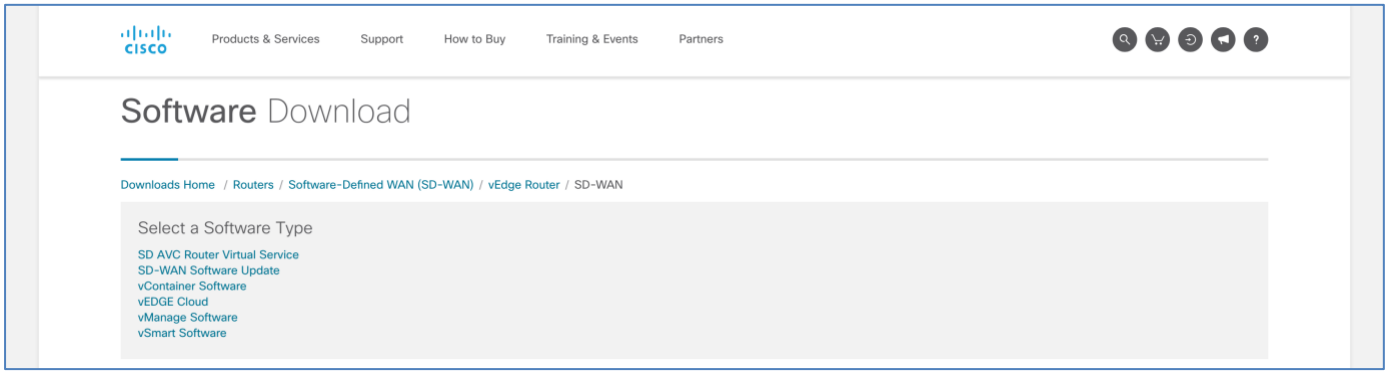
The device reloads with the new IOS-XE SD-WAN code and the device prompts for credentials to log into the command line. The default credentials for the WAN Edge device is admin/admin.

Technical Tip: The Cisco SD-WAN solution can have a mix of vEdge and IOS-XE SD-WAN devices running on the same network. Careful consideration must be taken with respect to the software version on the vEdge in order to interoperate with SD-WAN IOS-XE devices, The vEdge device must be running version 17.2.1 or later and the SD-WAN controllers (vManage, vSmart, and vBond) must be running version 18.3.0 or later. This is due to code changes that have been implemented to support Bidirectional forwarding detection (BFD) on tunnels between vEdge and IOS-XE SD-WAN devices.

Appendix I – Install vEdge Cloud

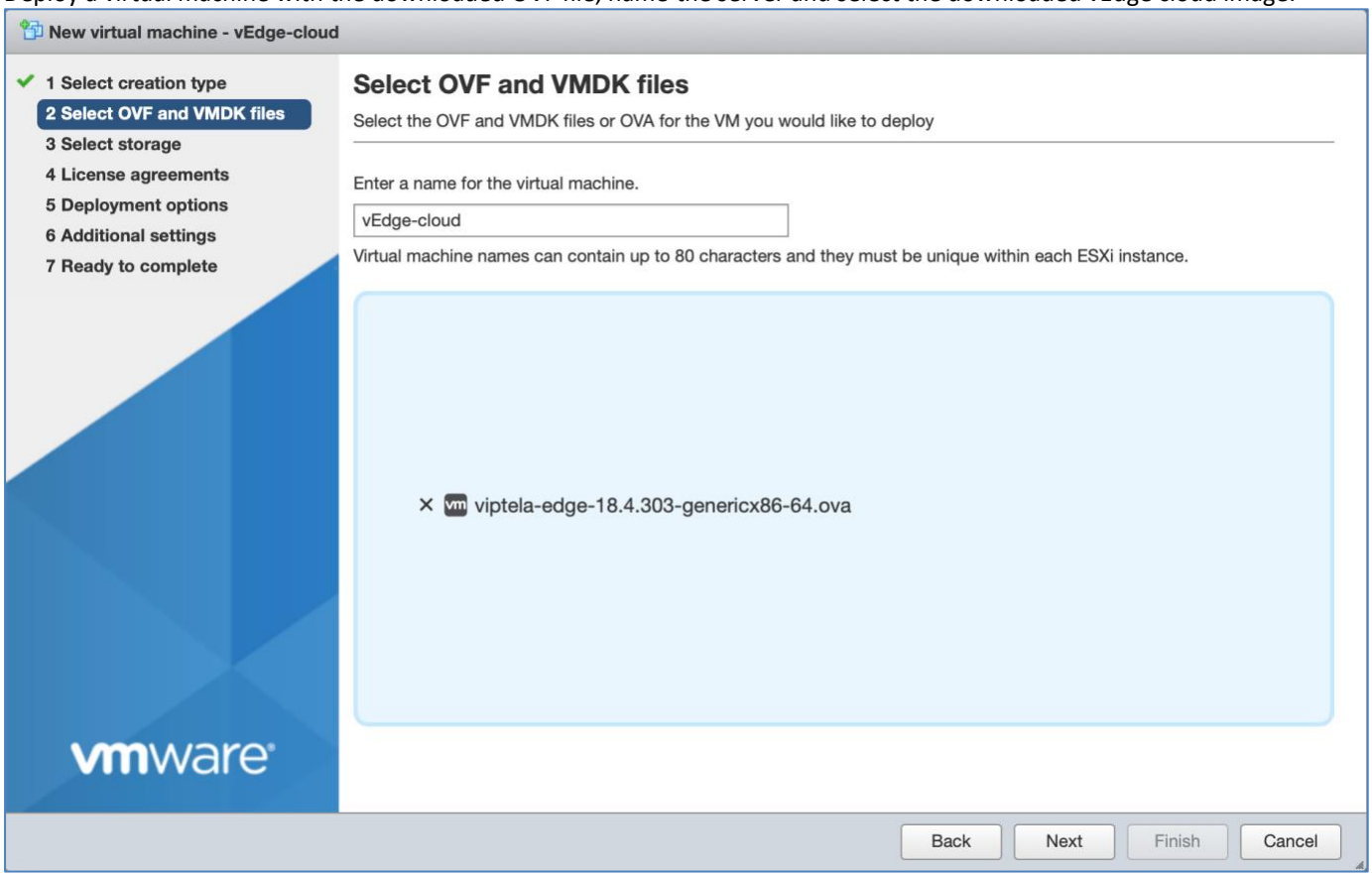
This section walks through steps to deploy vEdge cloud in a KVM environment.

Step 1 Download the vEDGE Cloud OVF software from http://software.cisco.com

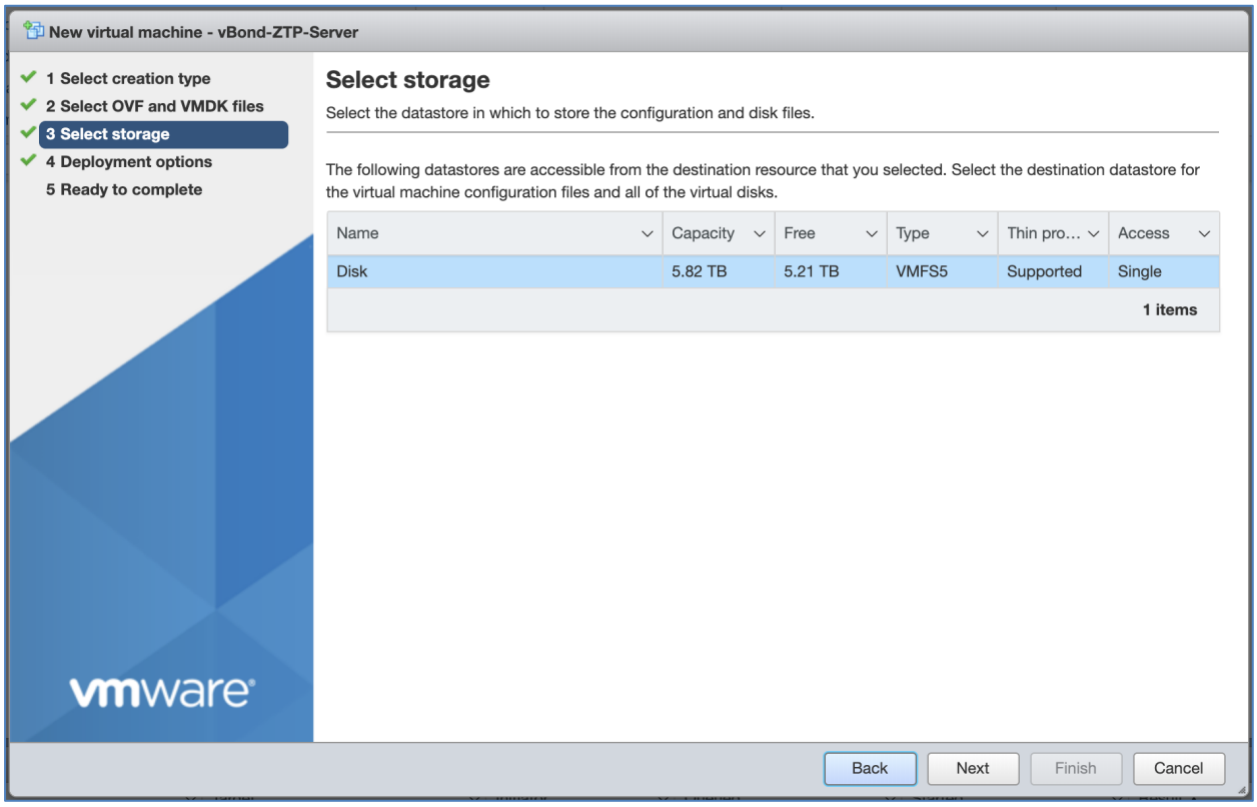


Step 2 Deploy the OVF template in the virtual environment.

Deploy a virtual machine with the downloaded OVF file, name the server and select the downloaded vEdge cloud image.

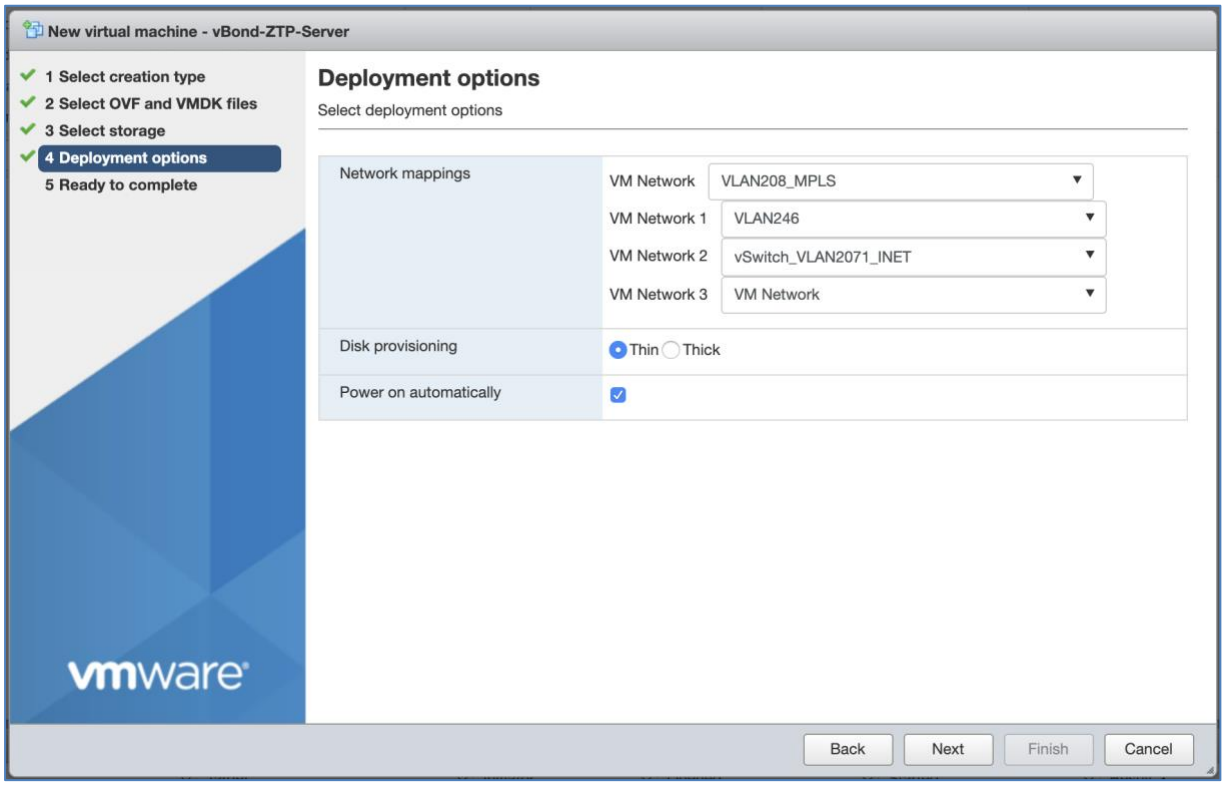


Select the storage.



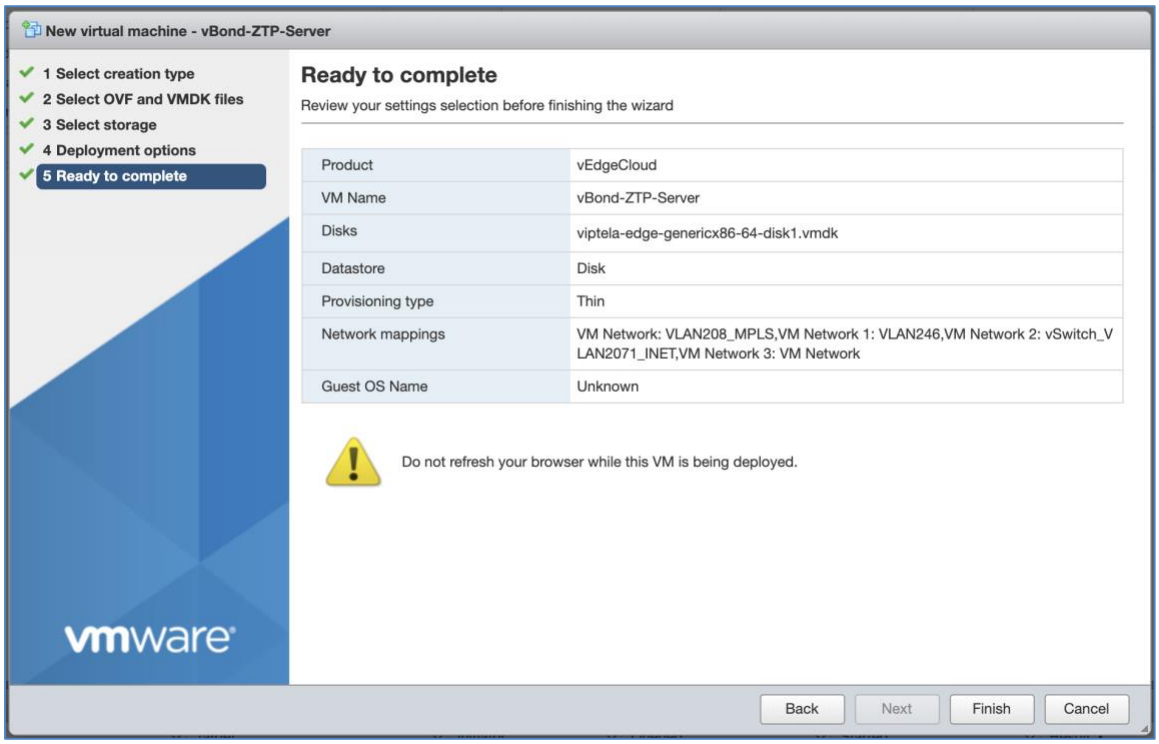
Select the deployment options (Network mappings, Disk provisioning, Power on automatically).

Note: The vEdge cloud OVF has 4 Interfaces defined (eth0 in VPN 512 and ge0/0, ge0/1, and ge0/2 in VPN 0). The default configuration has interface ge0/0 and eth0 as DHCP clients.



Step 3 Review your settings selection and click **Finish**.

After deploying the virtual router, boot the virtual machine.



Step 4 Configure the vEdge cloud.

Administrators can leverage any of the supported onboarding options discussed to configure, authenticate and join the overlay network.