# CONTENTS

## CHAPTER 1
Read Me First 1

## CHAPTER 2
What's New in Cisco IOS XE (SD-WAN) and Cisco SD-WAN Releases 3

## CHAPTER 3
The Cisco SD-WAN Solution 5

### The Cisco SD-WAN SEN
- The Need for the Cisco SD-WAN SEN 5
- The Virtual IP Fabric 7

### Components of the Cisco SD-WAN SEN
- Primary SEN Components 12
- SEN Software Services 16

### Working with the Cisco SD-WAN SEN
- Build a Basic Overlay Network 18
- Cisco SD-WAN Terminology 22

## CHAPTER 4
Hardware and Software Installation 25

### Server Recommendations
25

### On-Site Bootstrap Process for Cisco SD-WAN Devices
26

### On-Site Bootstrap Process for Cisco vEdge 5000 using SHA2 Enterprise Certificates
28

### Generate a Bootstrap File For Cisco IOS XE SD-WAN Devices Using the CLI
33

### One Touch Provisioning: Onboard Cisco IOS XE SD-WAN Devices Using Generic Bootstrap Configuration
34

### Installing Cisco SD-AVC, Cisco vManage 20.1.1 and Earlier
38
- Enabling SD-AVC on Cisco vManage
- Enable SD-AVC on Cisco vEdge Devices
- Install Cisco SD-AVC, Cisco vManage Release 20.3.1 and Later 40
Enable Cisco SD-AVC, Cisco vManage Release 20.3.1 and Later 41
Enable SD-AVC on Cisco vEdge Devices 42
Enable Cisco SD-AVC Cloud Connector 43
Software Installation and Upgrade for Cisco IOS XE Routers 44
  Before You Begin 44
  Download Cisco IOS XE SD-WAN Software for Cisco IOS XE SD-WAN Release 16.12 and Earlier 46
  Install the Cisco IOS XE SD-WAN Software for Cisco IOS XE SD-WAN Release 16.12 and Earlier 46
  Configure IOS XE Router Using CLI 48
  Add IOS XE Devices to the Plug and Play Portal 51
  Upgrading or Downgrading ROMMON 51
  Perform Factory Reset 52
Recover the Default Password 53
Software Installation and Upgrade for vEdge Routers 54
  Software Image Signing 54
  Software Version Compatibility 54
  Install the Software 54
Upgrade the Software 55
Best Practices for Software Upgrades 56
Obtain Software Images from Cisco SD-WAN 56
Add New Software Images to the Repository 57
Upgrade the Software Image 58
Activate a New Software Image 59
View Log of Software Upgrade Activities 59
Upgrade a Software Image from the CLI 59
Redundant Software Images 60
Downgrade a Cisco vEdge Device to an Older Software Image 61

CHAPTER 5 Install and Upgrade Cisco IOS XE Release 17.2.1r and Later 63
Platforms Supported in Controller Mode 64
Cisco IOS XE Image Compatibility 65
Restrictions 65
Introducing Autonomous and Controller Mode 66
Software Installation for Cisco IOS XE Routers 66
Plug and Play in Cisco IOS XE Release 17.2.1r and Later Releases 68
   Plug and Play Onboarding Workflow 68
   Mode Discovery with Plug and Play Onboarding 68
Non-PnP Onboarding 69
   Creating a Cisco SD-WAN Bootstrap Configuration File 69
New Installation: Mode Change Device Day Zero Scenario 69
   Switch Modes Using Cisco CLI 70
Mode Discovery and Mode Change 70
Controller Mode Configuration Reset 72
Mode Switching: Additional Information 73
   Configuration Persistence During Mode Switch 73
Verify Controller and Autonomous Modes 73
   Show Command Output for Controller Mode 73
   Show Command Output for Autonomous Mode 74
Change the Console Port Access After Installation, in Controller Mode 75
Upgrade to Cisco IOS XE Release 17.2.1r or Later 76
   Supported Upgrades 76
      Upgrade Using Cisco vManage 78
      Upgrade Using CLI 78
Downgrade from Cisco IOS XE Release 17.2.1r or Later Releases 80
   Downgrading to a Previously Installed Image: Inline Downgrade 80
   Downgrading to a Fresh Install of a Target Image: Clean Downgrade 80
   Downgrade Scenarios for Cisco IOS XE Release 17.2.x 80
Restore Smart Licensing and Smart License Reservation 81
   Restore Smart Licensing 81
   Restore Smart License Reservation 81
Onboard Cisco Catalyst 8000V Edge Software Hosted by a Cloud Service, Using PAYG Licensing 82
Bootstrap Process for Cisco SD-WAN Cloud-Hosted Devices 83

CHAPTER 6
Cisco SD-WAN Overlay Network Bring-Up Process 85
   Bring Up the Sequence of Events 85
      Steps to Bring Up the Overlay Network 87
Summary of the User Portion of the Bring-Up Sequence  89
Automatic Portions of the Bring-Up Sequence  92
User Input Required for the ZTP Automatic Authentication Process  92
Authentication between Cisco vSmart Controller and Cisco vBond Orchestrator  93
Authentication Between Cisco vSmart Controller  96
Authentication between Cisco vBond Orchestrator and a vEdge Router  99
Authentication between the vEdge Router and Cisco vManage  102
Authentication between Cisco vSmart Controller and the vEdge Router  104
Firewall Ports for Cisco SD-WAN Deployments  107
Download Software  112
Deploy Cisco vManage  113
  Create vManage VM Instance on ESXi  114
  Create vManage VM Instance on KVM  117
  Create Configuration Templates for Cisco vManage  119
Configure Cisco vManage  121
  Configure Certificate Settings  124
  Generate Cisco vManage Certificate  125
  Create a vManage Cluster  125
  Enable Timeout Value for a vManage Client Session  125
Deploy Cisco vBond Orchestrator  125
  Create vBond VM Instance on ESXi  126
  Create vBond VM Instance on KVM  136
  Configure Cisco vBond Orchestrator  141
  Create Configuration Templates for Cisco vBond Orchestrator  144
  Add Cisco vBond Orchestrator to the Overlay Network  147
  Start the Enterprise ZTP Server  149
vContainer Host  153
Deploy Cisco vSmart Controller  153
  Create vSmart VM Instance on ESXi  154
  Create vSmart VM Instance on KVM  166
  Configure the vSmart Controller  171
  Create Configuration Templates for Cisco vSmart Controller  176
  Add Cisco vSmart Controller to the Overlay Network  179
Deploy Cisco Catalyst 8000V Using Cloud Services Provider Portals  182
Notes and Limitations 182

Deploy Cisco CSR 1000v Using Cloud Service Provider Portals 182
Deploy Cisco Catalyst 8000V Edge Software on Alibaba Cloud 183

Features 183

Requirements for the Cisco Catalyst 8000V Instance 183
Configure the Cisco Catalyst 8000V Instance to Connect to Cisco SD-WAN 183
Create a Bootstrap File for a Cisco Catalyst 8000V Instance Using Cisco vManage 184

Deploy the vEdge Cloud routers 184

Create vEdge Cloud router VM Instance on AWS 185
Create vEdge Cloud router VM Instance on Azure 197
Create vEdge Cloud VM Instance on ESXi 206
Create vEdge Cloud VM Instance on KVM 209

Configure Certificate Authorization Settings for WAN Edge Routers 217
Install Signed Certificates on vEdge Cloud Routers 218
Send Router Serial Numbers to the Controller Devices 225
  How to Upload a Router Authorized Serial Number File 226
Configure the vEdge Routers 228
Prepare Routers for ZTP 237

CHAPTER 7

Cisco vManage Dashboards 243

View Device Pane 244
View Reboot Pane 245
View Certificates Pane 245
View Control Status Pane 245
View Site Health View Pane 246
View Transport Interface Distribution 246
View WAN Edge Inventory Pane 246
View WAN Edge Health Pane 247
View Transport Health Pane 247
View Top Applications Pane 247
View Application-Aware Routing Pane 248
View Firewall Enforcement Pane 248
View Top Signature Hits Pane 248
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>View URL Filtering Pane     249</td>
</tr>
<tr>
<td>View Advanced Malware Protection Pane 249</td>
</tr>
<tr>
<td>View Web Server Certificate Expiration Date Notification 249</td>
</tr>
<tr>
<td>View Maintenance Windows Alert Notification 250</td>
</tr>
</tbody>
</table>

**Chapter 8**

**Cluster Management** 251
- Configure the Cluster IP Address of a Cisco vManage Server 251
- Add a Cisco vManage Server to a Cluster 252
- Configure Statistics Database to Monitor Cisco vManage 253
- View Cisco vManage Service Details 253
- Edit Cisco vManage Parameters 254
- Update Configuration Database Login 254
- Upgrade Cisco vManage Cluster 255
- Manually Restart vManage Processes 256
- Remove Cisco vManage from a Cluster 258

**Chapter 9**

**Enterprise Certificates** 259
- Manage Certificates in Cisco vManage 260
  - Check the WAN Edge Router Certificate Status 261
  - Validate a WAN Edge Router 261
  - Stage a WAN Edge Router 262
  - Invalidate a WAN Edge Router 262
  - Send the Controller Serial Numbers to Cisco vBond Orchestrator 262
  - Install Signed Certificate 263
  - Export Root Certificate 263
  - View a Certificate Signing Request 263
  - View a Device Certificate Signing Request 263
  - View the Certificate 264
  - Generate a Certificate Signing Request 264
  - Generate a Feature Certificate Signing Request 264
  - Reset the RSA Key Pair 264
  - Invalidate a Device 264
  - View Log of Certificate Activities 265
  - View a Signed Certificate 265
<table>
<thead>
<tr>
<th>Page</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>265</td>
<td>Manage Root Certificate Authority Certificates in Cisco vManage</td>
</tr>
<tr>
<td>265</td>
<td>Add a Root Certificate Authority Certificate</td>
</tr>
<tr>
<td>266</td>
<td>View a Root Certificate Authority Certificate</td>
</tr>
<tr>
<td>266</td>
<td>Delete a Root Certificate</td>
</tr>
<tr>
<td>266</td>
<td>Enable Reverse Proxy</td>
</tr>
<tr>
<td>269</td>
<td>Configure Enterprise Certificates for Cisco SD-WAN Devices and Controllers</td>
</tr>
<tr>
<td>274</td>
<td>Authorize a Controller Certificate</td>
</tr>
<tr>
<td>274</td>
<td>Using Controller Certificates with Cisco PKI</td>
</tr>
<tr>
<td>275</td>
<td>Use Case: Cisco-Hosted Cloud Overlays with Software Version 19.x and Above</td>
</tr>
<tr>
<td>276</td>
<td>Use Case: Migration of an Active Existing Overlay from Digicert to Cisco PKI Controller Certificates During Certificate Renewal</td>
</tr>
<tr>
<td>278</td>
<td>Use Case: Submitting CSRs and Downloading Certificates on On-Premises Controllers</td>
</tr>
<tr>
<td>279</td>
<td>Web Server Certificate for Cisco vManage</td>
</tr>
</tbody>
</table>

**CHAPTER 10**

**Licensing on Cisco SD-WAN**

- Restrictions for Cisco SD-WAN Licensing 282
- Configure Cisco SD-WAN Licensing 282
- Verifying Call Home Configuration 284

**CHAPTER 11**

**Manage Licenses for Smart Licensing Using Policy**

- Overview 287
- Notes and Limitations 289
- License Management Workflow in Cisco vManage 289
- Provision Smart Account Credentials on Cisco vManage 290
- Fetch and Synchronize Licenses 291
- Assign License to Device 292
- Monitor License Usage 294

**CHAPTER 12**

**Onboarding Modular Cisco ASR 1000 Series Platforms**

- Cisco ASR 1006-X with an RP3 Module 295
  - Hardware Configuration 295
  - ROM Monitor Software Version 297
  - Onboarding Workflow 297
  - RMA Replacement of the Cisco ASR 1006-X Chassis 297
RMA Replacement of the Cisco RP3 Module 300

CHAPTER 13  
API Cross-Site Request Forgery Prevention 305
  Cisco SD-WAN REST API Token-Based Authentication 305
  Token Use 305
  API Docs 306
  Third Party Application Users 306

CHAPTER 14  
Appendix: vManage How-Tos 311
  RESTful API for vManage NMS 311
  Replace a vEdge Router 313
  Using Cisco vManage on Different Servers 315
  Log In to the Cisco vManage Web Application Server 316
CHAPTER 1

Read Me First

Related References

• Release Notes
• Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations

User Documentation

• Cisco IOS XE (Cisco IOS XE SD-WAN Devices)
• Cisco SD-WAN (Cisco vEdge Devices)
• Cisco IOS XE (SD-WAN) Qualified Command Reference
• Cisco SD-WAN Command Reference

Communications, Services, and Additional Information

• Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
• For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
• To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
• To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
• To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
• To view open and resolved bugs for a release, access the Cisco Bug Search Tool.
• To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.
CHAPTER 2

What's New in Cisco IOS XE (SD-WAN) and Cisco SD-WAN Releases

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco is constantly enhancing the SD-WAN solution with every release and we try and keep the content in line with the latest enhancements. The following link includes release-wise new and modified features that are documented in the Configuration, Command Reference, and Hardware Installation guides. For information on additional features and fixes that were committed to the Cisco SD-WAN solution, see the Resolved and Open Bugs section in the Release Notes.

What's New in Cisco IOS XE (SD-WAN) Release 17.x
What's New in Cisco IOS XE SD-WAN Release 16.x
What's New in Cisco SD-WAN (vEdge) Release 20.x
What's New in Cisco SD-WAN (vEdge) Release 19.x
The Cisco SD-WAN Solution

The Need for the Cisco SD-WAN SEN

Legacy networking technology has become increasingly expensive and complex, and it cannot scale to meet the needs of today’s multisite enterprises. The Cisco SD-WAN Secure Extensible Network (SEN), which is based on time-tested and proven elements of networking, offers an elegant, software-based solution that reduces the costs of running enterprise networks and provides straightforward tools to simplify the provisioning and management of large and complex networks that are distributed across multiple locations and geographies. Built into the Cisco SD-WAN SEN are inherent authentication and security processes that ensure the safety and privacy of the network and its data traffic.

The Cisco SD-WAN SEN represents an evolution of networking from an older, hardware-based model to a secure, software-based, virtual IP fabric. The Cisco SD-WAN fabric, also called an overlay network, forms a software overlay that runs over standard network transport services, including the public Internet, MPLS, and broadband. The overlay network also supports next-generation software services, thereby accelerating your shift to cloud networking.

Challenges in Legacy Network Design

The traditional approach to network design cannot scale to meet today’s needs for four fundamental reasons:

• Cost—Legacy networks run on expensive hardware such as routers and switches, which require time-consuming configuration and maintenance. In addition, these networks require expensive transport connections or carrier circuits to secure and segment the network.

• Complexity—Legacy networks operate on the old model of a distributed control plane, which means that every node in the network must be configured with routing and security rules. Remote site management, change control, and network maintenance represent major logistical challenges.

• Lengthy installation times—Legacy networks that run on dedicated carrier circuits depend on the carrier to install new circuits, which can take several months. This can dramatically delay the launch of new branch locations.
The Need for the Cisco SD-WAN SEN

- Control—Legacy networks that run on carrier circuits sacrifice control to the ISP, from network design to configuration to monitoring. Requesting changes from the ISP also requires extra time and is prone to communication errors.

Cost and complexity become even more prohibitive for legacy networks in the face of today’s requirements, including:

- Rigorous end-to-end security
- Disparate transport networks
- High-bandwidth cloud applications that are hosted in multiple data centers
- Ongoing increase in the number of mobile end users
- Any-to-any connectivity over fluid topologies
- Unique needs of particular businesses

The Cisco SD-WAN Solution

The Cisco SD-WAN SEN is a Software-Defined WAN (SD-WAN). As with all SD-WANs, it is based on the same routing principles that allowed the Internet to scale during the 1990s and 2000s. What separates the Cisco SD-WAN SEN from other SD-WANs is that it reimagines the WAN for a new generation of enterprise networks, separating the data plane from the control plane and virtualizing much of the routing that used to require dedicated hardware.

The virtualized network runs as an overlay on cost-effective hardware, whether physical routers, called vEdge routers, or virtual machines in the cloud, called vEdge Cloud routers. Centralized controllers, called Cisco vSmartControllers, oversee the control plane of the Cisco SD-WAN fabric, efficiently managing provisioning, maintenance, and security for the entire SEN overlay network. Another device, called the Cisco vBond Orchestrator, automatically authenticates all other Cisco vEdge devices when they join the SEN overlay network.
This division of labor allows each networking layer to focus on what it does best. The control plane manages the rules for the routing traffic through the overlay network, and the data plane passes the actual data packets among the network devices. The control plane and data plane form the warp and weft of a flexible, robust fabric that you weave according to your needs, on your schedule, over existing circuits.

Cisco vManage provides a simple, yet powerful, set of graphical dashboards for monitoring network performance on all devices in the overlay network, from a centralized monitoring station. In addition, Cisco vManage provides centralized software installation, upgrade, and provisioning, whether for a single device or as a bulk operation for many devices simultaneously.

The Cisco SD-WAN SEN is ideally suited to the needs of cloud networking. Cisco SD-WAN virtual IP fabric supports software services that streamline and optimize cloud networking, allowing you to take full advantage of the power of the overlay network for individual cloud applications.

**Note**

- Cisco SD-WAN controllers are purpose-built, custom stacks. Although open-source Linux components are used, our custom operating system stacks bear no resemblance to the open-source Linux components used. The Linux components are not subject to the same hardening requirements as the custom operating system stacks that they are used in.

- The root access is disabled on Cisco SD-WAN controllers and cannot be accessed from the user space.

- We meet compliance standards and requirements, such as, FedRAMP, FIPS, and CC. This compliance should be considered as proof of the security validation of our operating systems.

- We follow a secure development lifecycle outlined [here](#).

- We also follow a well-defined process run by the Cisco Product Security Incident Response Team (PSIRT) to address any new exploits or attacks, such as, CVE.

- If you are still concerned about the platform security of Cisco SD-WAN controllers, we recommend that you conduct an independent penetration testing through third parties.

---

**The Virtual IP Fabric**

The complexity in legacy enterprise networks stems from three main sources:

- There is no clear separation between entities that exchange data traffic and the transport network that binds these entities together. That is, there is no clear separation between hosts, devices, and servers on the service side of the network and the interconnects between routers on the transport side of the network.

- Policy and control decisions are embedded at every hop across the enterprise network.

- Security is a time-intensive, manual process, and security management must be implemented either at every node in the network or by using centralized security servers to manage group keys.

The Cisco SD-WAN Secure Extensible Network (SEN) uses time-tested and proven elements of networking in innovative ways to build the secure, virtual IP fabric. These networking elements include:

- Using routing and routing advertisements to establish and maintain the flow of traffic throughout the network.
• Layer 3 segmentation, sometimes called virtual routing and forwarding (VRF), to isolate different flows of traffic. This is useful to separate traffic from different customers or different business organizations within an enterprise.

• Peer-to-peer concepts to set up and maintain bidirectional connections between pairs of protocol entities

• Authentication and encryptions

• Policies for routing and data traffic

With five simple steps, the Cisco SD-WAN virtual IP fabric transforms a complex legacy network into an easy-to-manage, scalable network:

• Step 1: Separate transport from the service side of the network
• Step 2: Centralize routing intelligence and enable segmentation
• Step 3: Secure the network automatically
• Step 4: Influence reachability through centralized policy
• Step 5: Simplify orchestration and provisioning

**Step 1: Separate Transport from the Service Side of the Network**

The job of the transport network is to carry packets from one transport router to another. The transport network needs to know only about the routes to follow to reach the next-hop or destination router. It need not know about the prefixes for nontransport routers, the routers that sit behind the transport routers in their local service networks.

Separating network transport from the service side of the network allows the network administrator to influence router-to-router communication independently of the communication between users or between hosts.

This approach has many benefits:

• The network administrator can choose transport circuits based on SLA and cost.
• The routing system can assign attributes to transport links for optimal routing, load balancing, and policy-based routing.
**Step 2: Centralize Routing Intelligence and Enable Segmentation**

Every router at the edge of a network has two sides for routing: one to the transport network and one to the service side of the network. To have any-to-any communication among all routers, all routers need to learn all prefixes. Traditionally, routers learn these prefixes using full-mesh IGP/BGP or by enabling routing on an overlay tunnel (for example, BGP or IGP over MPLS or GRE). Various techniques allow the scaling issues associated with full-mesh routing adjacencies to be mitigated or eliminated, such as employing a route reflector for BGP.

The Cisco SD-WAN fabric builds on the route reflector model by centralizing routing intelligence. Essentially, all prefixes learned from the service side on a router are advertised to a centralized controller, which then reflects the information to other routers over the network's control plane. The controllers do not handle any of the data traffic; they are involved only in control plane communication.

This approach has many benefits:

- The centralized controller can use inexpensive or commodity servers for control plane processing.
- The routers can use off-the-shelf silicon, allowing cost benefits from economies of scale.
- Scale challenges associated with full-mesh routing on the transport side of the network are eliminated.
- The network administrator can create multiple segments without the need for complex signaling protocols. For example, in the figure here, all Px prefixes can be part of one VPN, while all Sx prefixes can be part of a different VPN.

**Note**

The centralized controller only “influences” routing on the routers. The controller does not participate in every flow going through the network, nor does it participate in routing on the service side. This design allows the routers to have local intelligence—enough intelligence to make local site decisions quickly.
**Step 3: Secure the Network and Links Automatically**

The Cisco SD-WAN fabric identifies transport side links and automatically encrypts traffic between sites. The associated encryption keys are exchanged over a secure session with the centralized controller. Secure sessions with the controller are set up automatically using RSA and certificate infrastructure.

This approach has many benefits:

- The Cisco SD-WAN fabric itself authenticates all devices participating in the network, which is an important step to secure the infrastructure.
- The fabric automatically exchanges encryption keys associated with the transport links, eliminating the hassle of configuring thousands of pair-wise keys.
- The fabric ensures that the network is not prone to attacks from the transport side.

**Step 4: Influence Reachability through Centralized Policy**

Policy configured on a centralized controller strongly influences how prefixes are advertised among the routers. For example, if all traffic between routers P3 and P4 in the figure here has to make a U-turn at router vEdge-1, the network administrator can apply a simple route policy on the centralized controller. The controller then passes the policy to the affected edge routers. The network administrator does not need to provision the policy on each individual router.

This approach has many benefits:

- The controller centrally influences access control, that is, which prefixes are allowed to talk to each other inside a VPN.
- The controller optimizes user experience by influencing transport link choice based on SLA or other attributes. The network administrator can color transport links (such as gold and bronze), and allow applications to map the colors to appropriate transport links.
- The network administrator can map business logic from a single centralized point.
• The network can react faster to planned and unexpected situations, such as routing all traffic from high-risk countries through an intermediate point.

• The network can centralize services such as firewalls, IDPs, and IDSs. Instead of distributing these services throughout the network at every branch and campus, the network administrator can centralize these functions, achieving efficiencies of scale and minimizing the number of touch points for provisioning.

Step 5: Simplify Provisioning and Management

Legacy network devices are provisioned and monitored manually through a CLI. Network administrators must type configurations line by line, and enter operational commands one at a time on individual devices in order to retrieve and read status information. This method is error prone and time consuming when provisioning and troubleshooting a network, and it can present serious difficulties when devices are in remote locations or when management ports are inaccessible.

The Cisco SD-WAN Solution

The Cisco SD-WAN SEN centralizes and significantly simplifies provisioning and management through Cisco vManage. Cisco vManage provides an easy-to-use, graphical dashboard from which you can monitor, configure, and maintain all Cisco vEdge devices and links in the overlay network. For example, the GUI dashboard provides a templated view of various configurations to ease provisioning a service, so all common elements, such as AAA and company-specific servers, can be pushed to multiple devices with a single click, from a single point.

This approach has many benefits:

• The network administrator provisions and manages the network as a whole, efficiently and easily, as opposed to a piece-meal approach that deals with individual devices one at a time.

• The network administrator has improved network visibility (for example, viewing network-wide VPN statistics) from a single point.

• Troubleshooting tasks are simplified and presented visually, instead of requiring network administrators to read lengthy configurations and output from individual devices.
Components of the Cisco SD-WAN SEN

Primary SEN Components

The secure, virtual IP fabric of the Cisco SD-WAN Secure Extensible Network (SEN) is made up of four fundamental components:

- **Cisco vManage**—Cisco vManage is a centralized network management system that lets you configure and manage the entire overlay network from a simple graphical dashboard.

- **Cisco vSmart Controller**—The Cisco vSmart Controller is the centralized brain of the Cisco SD-WAN solution, controlling the flow of data traffic throughout the network. The Cisco vSmart Controller works with the Cisco vBond Orchestrator to authenticate Cisco vEdge devices as they join the network and to orchestrate connectivity among the vEdge routers.

- **Cisco vBond Orchestrator**—The Cisco vBond Orchestrator automatically orchestrates connectivity between vEdge routers and Cisco vSmart Controllers. If any vEdge router or Cisco vSmart Controller is behind a NAT, the Cisco vBond Orchestrator also serves as an initial NAT-traversal orchestrator.

- **vEdge Routers**—The vEdge routers sit at the perimeter of a site (such as remote offices, branches, campuses, data centers) and provide connectivity among the sites. They are either hardware devices or software, called a vEdge Cloud router, that runs as a virtual machine. vEdge routers handle the transmission of data traffic.

Of these four components, the vEdge router can be a Cisco SD-WAN hardware device or software that runs as a virtual machine, and the remaining three are software-only components. The software vEdge router, Cisco vManage, and Cisco vSmart Controller software runs on servers, and the vBond orchestrator software runs as a process (daemon) on a vEdge router.

The figure below illustrates the components of the Cisco SD-WAN SEN. The sections below describe each component in detail.
Cisco vManage

Cisco vManage is a centralized network management system. Cisco vManage dashboard provides a visual window into the network, and it allows you to configure and manage Cisco vEdge network devices. Cisco vManage software runs on a server in the network. This server is typically situated in a centralized location, such as a data center. It is possible for Cisco vManage software to run on the same physical server as Cisco vSmart Controller software.

You can use Cisco vManage to store certificate credentials, and to create and store configurations for all Cisco vEdge network components. As these components come online in the network, they request their certificates and configurations from Cisco vManage. When Cisco vManage receives these requests, it pushes the certificates and configurations to the Cisco vEdge network devices.

For vEdge Cloud routers, Cisco vManage can also sign certificates and generate bootstrap configurations, and it can decommission the devices.

Cisco vSmart Controller

The Cisco vSmart Controller oversees the control plane of the Cisco SD-WAN overlay network, establishing, adjusting, and maintaining the connections that form the Cisco SD-WAN fabric.

The major components of the Cisco vSmart Controller are:

- Control plane connections—Each Cisco vSmart Controller establishes and maintains a control plane connection with each vEdge router in the overlay network. (In a network with multiple Cisco vSmart Controllers, a single Cisco vSmart Controller may have connections only to a subset of the vEdge routers, for load-balancing purposes.) Each connection, which runs as a DTLS tunnel, is established after device authentication succeeds, and it carries the encrypted payload between the Cisco vSmart Controller and the vEdge router. This payload consists of route information necessary for the Cisco vSmart Controller to determine the network topology, and then to calculate the best routes to network destinations and distribute this route information to the vEdge routers. The DTLS connection between a Cisco vSmart Controller and a vEdge router is a permanent connection. The Cisco vSmart Controller has no direct peering relationships with any devices that a vEdge router is connected to on the service side.

- OMP (Overlay Management Protocol)—The OMP protocol is a routing protocol similar to BGP that manages the Cisco SD-WAN overlay network. OMP runs inside DTLS control plane connections and carries the routes, next hops, keys, and policy information needed to establish and maintain the overlay network. OMP runs between the Cisco vSmart Controller and the vEdge routers and carries only control plane information. The Cisco vSmart Controller processes the routes and advertises reachability information learned from these routes to other vEdge routers in the overlay network.

- Authentication—The Cisco vSmart Controller has pre-installed credentials that allow it to authenticate every new vEdge router that comes online. These credentials ensure that only authenticated devices are allowed access to the network.

- Key reflection and rekeying—The Cisco vSmart Controller receives data plane keys from a vEdge router and reflects them to other relevant vEdge routers that need to send data plane traffic.

- Policy engine—The Cisco vSmart Controller provides rich inbound and outbound policy constructs to manipulate routing information, access control, segmentation, extranets, and other network needs.

- Netconf and CLI—Netconf is a standards-based protocol used by Cisco vManage to provision a Cisco vSmart Controller. In addition, each Cisco vSmart Controller provides local CLI access and AAA.

The Cisco vSmart Controller maintains a centralized route table that stores the route information, called OMP routes, that it learns from the vEdge routers and from any other Cisco vSmart Controllers in the Cisco SD-WAN.
overlay network. Based on the configured policy, the Cisco vSmart Controller shares this route information with the Cisco vEdge network devices in the network so that they can communicate with each other.

The Cisco vSmart Controller is software that runs as a virtual machine on a server configured with ESXi or VMware hypervisor software. The vSmart software image is a signed image that is downloadable from the Cisco SD-WAN website. A single Cisco SD-WAN root-of-trust public certificate is embedded into all vSmart software images.

During the initial startup of a Cisco vSmart Controller, you enter minimal configuration information, such as the IP addresses of the controller and the Cisco vBond Orchestrator. With this information and the root-of-trust public certificate, the Cisco vSmart Controller authenticates itself on the network, establishes a DTLS control connection with the Cisco vBond Orchestrator, and receives and activates its full configuration from Cisco vManage if one is present in the domain. (Otherwise, you can manually download a configuration file or create a configuration directly on the Cisco vSmart Controller through a console connection.) The Cisco vSmart Controller is now also ready to accept connections from the vEdge routers in its domain.

To provide redundancy and high availability, a typical overlay network includes multiple Cisco vSmart Controllers in each domain. A domain can have up to 20 vSmart controllers. To ensure that the OMP network routes remain synchronized, all the Cisco vSmart Controllers must have the same configuration for policy and OMP. However, the configuration for device-specific information, such as interface locations and addresses, system IDs, and host names, can be different. In a network with redundant Cisco vSmart Controllers, the Cisco vBond Orchestrator tells the Cisco vSmart Controllers about each other and tells each Cisco vSmart Controller which vEdge routers in the domain it should accept control connections from. (Different vEdge routers in the same domain connect to different Cisco vSmart Controllers, to provide load balancing.) If one Cisco vSmart Controller becomes unavailable, the other controllers automatically and immediately sustain the functioning of the overlay network.

Cisco vBond Orchestrator

The Cisco vBond Orchestrator automatically coordinates the initial bringup of Cisco vSmart Controllers and vEdge routers, and it facilities connectivity between Cisco vSmart Controllers and vEdge routers. During the bringup processes, the Cisco vBond Orchestrator authenticates and validates the devices wishing to join the overlay network. This automatic orchestration process prevents tedious and error-prone manual bringup.

The Cisco vBond Orchestrator is the only Cisco vEdge device that is located in a public address space. This design allows the Cisco vBond Orchestrator to communicate with Cisco vSmart Controllers and vEdge routers that are located behind NAT devices, and it allows the Cisco vBond Orchestrator to solve any NAT-traversal issues of these Cisco vEdge devices.

The major components of the Cisco vBond Orchestrator are:

• Control plane connection—Each vBond orchestrator has a persistent control plane connection in the form of a DTLS tunnel with each Cisco vSmart Controller in its domain. In addition, the Cisco vBond Orchestrator uses DTLS connections to communicate with vEdge routers when they come online, to authenticate the router, and to facilitate the router's ability to join the network. Basic authentication of a vEdge router is done using certificates and RSA cryptography.

• NAT traversal—The Cisco vBond Orchestrator facilitates the initial orchestration between vEdge routers and Cisco vSmart Controllers when one or both of them are behind NAT devices. Standard peer-to-peer techniques are used to facilitate this orchestration.

• Load balancing—In a domain with multiple Cisco vSmart Controllers, the Cisco vBond Orchestrator automatically performs load balancing of vEdge routers across the Cisco vSmart Controllers when routers come online.
The Cisco vBond Orchestrator is a software module that authenticates the Cisco vSmart Controllers and the vEdge routers in the overlay network and coordinates connectivity between them. It must have a public IP address so that all Cisco vEdge devices in the network can connect to it. (It is the only Cisco vEdge device that must have a public address.)

The Cisco vBond Orchestrator orchestrates the initial control connection between Cisco vSmart Controllers and vEdge routers. It creates DTLS tunnels to the Cisco vSmart Controllers and vEdge routers to authenticate each node that is requesting control plane connectivity. This authentication behavior assures that only valid customer nodes can participate in the Cisco SD-WAN overlay network. The DTLS connections with Cisco vSmart Controllers are permanent so that the vBond controller can inform the Cisco vSmart Controllers as vEdge routers join the network. The DTLS connections with vEdge routers are temporary; once the Cisco vBond Orchestrator has matched a vEdge router with a Cisco vSmart Controller, there is no need for the Cisco vBond Orchestrator and the vEdge router to communicate with each other. The Cisco vBond Orchestrator shares only the information that is required for control plane connectivity, and it instructs the proper vEdge routers and Cisco vSmart Controllers to initiate secure connectivity with each other. The Cisco vBond Orchestrator maintains no state.

To provide redundancy for the Cisco vBond Orchestrator, you can create multiple vBond entities in the network and point all vEdge routers to those Cisco vBond Orchestrators. Each Cisco vBond Orchestrator maintains a permanent DTLS connection with each Cisco vSmart Controller in the network. If one Cisco vBond Orchestrator becomes unavailable, the others are automatically and immediately able to sustain the functioning of the overlay network. In a domain with multiple Cisco vSmart Controllers, the vBond orchestrator pairs a vEdge router with one of the Cisco vSmart Controllers to provide load balancing.

**vEdge Routers**

The vEdge router, whether a hardware or software device, is responsible for the data traffic sent across the network. When you place a vEdge router into an existing network, it appears as a standard router.

To illustrate this, the figure here shows a vEdge router and an existing router that are connected by a standard Ethernet interface. These two routers appear to each other to be Layer 3 end points, and if routing is needed between the two devices, OSPF or BGP can be enabled over the interface. Standard router functions, such as VLAN tagging, QoS, ACLs, and route policies, are also available on this interface.

The vEdge router’s components are:

- **DTLS control plane connection**—Each vEdge router has one permanent DTLS connection to each Cisco vSmart Controller it talks to. This permanent connection is established after device authentication succeeds, and it carries encrypted payload between the vEdge router and the Cisco vSmart Controller. This payload consists of route information necessary for the Cisco vSmart Controller to determine the network topology, and then to calculate the best routes to network destinations and distribute this route information to the vEdge routers.
• OMP (Overlay Management Protocol)—As described for the Cisco vSmart Controller, OMP runs inside the DTLS connection and carries the routes, next hops, keys, and policy information needed to establish and maintain the overlay network. OMP runs between the vEdge router and the Cisco vSmart Controller and carries only control information.

• Protocols—The vEdge router supports standard protocols, including OSPF, BGP, VRRP, and BFD.

• RIB (Routing Information Base)—Each vEdge router has multiple route tables that are populated automatically with direct interface routes, static routes, and dynamic routes learned via BGP and OSPF. Route policies can affect which routes are stored in the RIB.

• FIB (Forwarding Information Base)—This is a distilled version of the RIB that the CPU on the vEdge router uses to forward packets.

• Netconf and CLI—Netconf is a standards-based protocol used by Cisco vManage to provision a vEdge router. In addition, each vEdge router provides local CLI access and AAA.

• Key management—vEdge routers generate symmetric keys that are used for secure communication with other vEdge routers, using the standard IPsec protocol.

• Data plane—The vEdge router provides a rich set of data plane functions, including IP forwarding, IPsec, BFD, QoS, ACLs, mirroring, and policy-based forwarding.

The vEdge router has local intelligence to make site-local decisions regarding routing, high availability (HA), interfaces, ARP management, ACLs, and so forth. The OMP session with the Cisco vSmart Controller influences the RIB in the vEdge router, providing non-site-local routes and the reachability information necessary to build the overlay network.

The hardware vEdge router includes a Trusted Board ID chip, which is a secure cryptoprocessor that contains the private key and public key for the router, along with a signed certificate. All this information is used for device authentication. When you initially start up a vEdge router, you enter minimal configuration information, such as the IP addresses of the vEdge router and the Cisco vBond Orchestrator. With this information and the information on the Trusted Board ID chip, the vEdge router authenticates itself on the network, establishes a DTLS connection with the Cisco vSmart Controller in its domain, and receives and activates its full configuration from Cisco vManage if one is present in the domain. Otherwise, you can manually download a configuration file or create a configuration directly on the vEdge router through a console connection.

**SEN Software Services**

To streamline and optimize cloud networking, Cisco SD-WAN offers next generation software services that run on the secure, virtual IP fabric:

• **CloudExpress service**—CloudExpress service optimizes the performance of Software as a Service (SaaS) cloud applications. It provides clear visibility of the performance of individual applications and automatically chooses the best path for each one. CloudExpress service calculates metrics about loss and latency using a formula customized for each application.

• **vAnalytics platform**—vAnalytics platform is a SaaS service hosted by Cisco SD-WAN as part of the SEN solution. vAnalytics platform provides graphical representations of the performance of your entire overlay network over time and lets you drill down to the characteristics of a single carrier, tunnel, or application at a particular time.
CloudExpress Service

Enterprises have been adopting business critical SaaS applications including Microsoft Office365, Salesforce, Dropbox, and others. Enterprises use three primary methods to offer connectivity to SaaS applications for their users:

• Direct Internet Access (DIA) from a branch office.

• Internet access through gateways in regional facilities.

• Cloud exchange or direct connection through gateways in a Carrier Neutral Facility (CNF).

Latency and packet loss have a direct impact on the performance of applications and on end-user experience, but in many cases network administrators have limited or no visibility into the network performance characteristics between the end-user and SaaS applications. When path impairment occurs and application performance suffers, shifting traffic from a primary to an alternate path usually requires the network administrator to perform a set of complex, manual, time-consuming, and error-prone steps.

Cisco SD-WAN CloudExpress service provides visibility and continuous monitoring of network performance characteristics. It makes real-time decisions by choosing the best performing path between the end-user and SaaS application for an optimal user experience. It automatically reacts to changes in network performance by intelligently re-routing application traffic away from any degraded network paths.

CloudExpress service supports all access methods for cloud-based SaaS applications, including DIA, internet access through a regional facility, and access through a CNF.

CloudExpress service calculates an application performance value called the Viptela Quality of Experience (vQoE) for enterprise cloud applications. The vQoE value weighs loss and latency using a formula customized for each application. For example, email applications tolerate latency better than video applications do, and video applications tolerate loss better than email does. The vQoE value ranges from zero to ten, with zero being the worst quality and ten being the best.

You enable CloudExpress service in Cisco vManage with a few clicks of the mouse, and then you access the CloudExpress dashboard in Cisco vManage for continuous visibility into the performance of individual applications.

vAnalytics Platform

The vAnalytics platform offers visibility into the performance of applications and the network over time. vAnalytics platform is a SaaS service hosted by Cisco SD-WAN as part of the SEN solution. vAnalytics platform provides graphical representations of your entire overlay network and lets you drill down to display the characteristics of a single carrier, tunnel, or application at a particular time.

The vAnalytics dashboard serves as an interactive overview of your network and an entrance point for more details. The dashboard by default displays information aggregated for the last 24 hours. When you drill down, you can select different time periods for different data sets to display. The dashboard displays data on application performance, WAN site usage, and carrier usage.

vAnalytics platform calculates application performance with the QoE value, which is customized for individual applications. This value ranges from zero to ten, with zero being the worst performance and ten being the best. vAnalytics platform calculates QoE based on latency, loss, and jitter, customizing the calculation for each application.

The vAnalytics platform stores data over a long period of time, displays historical trend information, and offers insights that could be used for future planning.

vAnalytics platform offers:

• Application visibility:
• Best and worst performing applications—Display the best and worst performing applications and drill down to details at the site level.

• Most bandwidth consuming applications—Display applications consuming the most bandwidth and drill down to sites and users.

• Network visibility:
  • Network availability and circuit availability—Display network availability and correlate network and circuit availability.
  • Tunnel performance—Display key performance indicators such as loss, latency and jitter over various SD-WAN tunnels.
  • Carrier usage views—Display providers and their network characteristics.

## Working with the Cisco SD-WAN SEN

### Build a Basic Overlay Network

Let’s use a simple network design, one that has two vEdge routers and one Cisco vSmart Controller, to illustrate how to form a functioning overlay network from Cisco vEdge components. In this topology, the Cisco vBond Orchestrator software has been enabled on one of the vEdge routers. Once you understand a simple network, you can start designing and building more complex topologies.

### A Simple Network Topology

The following figure illustrates our simple topology. Here, we have two sites, Site-100 and Site-200. vEdge-1 is the edge device in Site-100, and vEdge-2 is the edge device at Site-200. At each local site, the vEdge router connects to an existing traditional router via a standard Ethernet interface. vEdge-2 is connected to the transport network through a NAT device that also has firewall functionality.

The goal of our design is to create a private network so that Router-1 and Router-2 can be next to each other from a Layer 3 perspective and so that hosts connected to each of these routers can communicate through the private network.
Construct a Basic Network

The following steps allow you to create the simple overlay network depicted in the topology above.

- **Step 1:** Perform initial bringup and basic configuration.
- **Step 2:** Enable host or service-side interfaces and routing.
- **Step 3:** Enable overlay routing over OMP.
- **Step 4:** Check the automatic setup of the IPsec data plane.
- **Step 5:** Enforce policies.

Let’s look at the steps in a bit more detail.

**Step 1: Perform Initial Bring up and Basic Configuration**

From the perspective of a network administrator, the initial bringup of the Cisco vEdge network components is a straightforward and simple process, involving creating the configurations for each of the network components and ensuring that a few key authentication-related files are in place. From the perspective of a user, bringup entails simply powering up the vEdge router and plugging in a cable to connect the router to the network. The remainder of the bringup occurs automatically via a zero-touch-provisioning process.

The network administrator performs the following tasks as part of the initial bringup:

1. Configure the Cisco vBond Orchestrator function on one of the vEdge routers in the network. In our example, this is vEdge-1.
2. Optionally, configure a top-level Cisco vBond Orchestrator to act as a ZTP server. In this situation, a DNS server must be present in the enterprise network.
3. Ensure that a DHCP server is present in the enterprise network.
4. Install the signed certificate on Cisco vManage, and download that certificate to Cisco vManage orchestrator.
5. Install the vEdge router authorized serial number file on Cisco vManage, and then download it to the Cisco vSmart Controllers.
6. From Cisco vManage CLI, create a configuration for each Cisco vSmart Controller and vEdge router in the overlay network:
   a. Configure a system IP address, which is similar to the router ID address on a traditional router, identifying the Cisco vEdge device with an address that is independent of any of the interfaces on the device. System IP addresses must be pre-allocated and must be unique across each vEdge router and Cisco vSmart Controller. These addresses need not be routable through the network.
   b. Configure site IDs for the various sites in the overlay network. In our example, vEdge-1 is at site-100 and vEdge-2 is at site-200. The Cisco vSmart Controller can be collocated at a site, or it can be in its own site.
   c. Configure domain IDs. This is an optional step to create clusters. For our example, configure the domain-ID as 1.
   d. Configure the IP address or DNS name for the vBond server and the Cisco vSmart Controller.
e. Configure WAN interfaces on vEdge-1 and vEdge-2. VPN 0 is the VPN reserved for WAN transport interfaces. IP addresses can be automatically obtained through DHCP. Alternatively, you can configure a default gateway and DNS explicitly.

f. By default, DTLS and IPSec are enabled on the WAN interfaces.

g. Save the configuration.

When the Cisco vSmart Controllers join the network, they are authenticated by the Cisco vBond Orchestrator, and when vEdge routers join the network, they are authenticated by both the Cisco vBond Orchestrator and the Cisco vSmart Controllers. These devices then connect to Cisco vManage, which downloads the configuration to them.

**Example Configuration on vEdge-1:**

```plaintext
system	host-name vEdge-1
system-ip 1.0.0.1
domain-id 1
site-id 100
vbond 75.1.1.1 local

! vpn 0
    interface ge 0/0
    ip address 75.1.1.1/24
tunnel-interface
    color default
    no shutdown
    ip route 0.0.0.0/0 75.1.1.254

! The remaining sections in this article describe how to configure other common functionality on vEdge routers and Cisco vSmart Controllers. Typically, you configure all functionality at one time, in the configuration that you create on Cisco vManage and that is downloaded to the device when it joins the overlay network. However, to highlight the different functionalities, this article describes the various portions of the configuration separately.

**Step 2: Enable Host or Service-Side Interfaces and Routing**

From Cisco vManage, you can also configure service-side interfaces and regular routing:

1. Configure interfaces on vEdge-1 towards the existing traditional router. Assign IP address and put the interface in a non-default VPN. In our example, this is VPN 1. Do the same on vEdge-2.

2. Configure OSPF or BGP on the vEdge routers towards the existing routers

3. Commit

To check for standard IP reachability, routes, and next hops at the local site, use the standard **ping, traceroute**, and various **show** commands on Cisco vManage or from the CLI of the device (if you have a direct connection to the device):

**Example Configuration for the Host or Service-side VPN:**

```plaintext
vpn 1
    router
    ospf
    redistribute ospf
    area 0
    interface ge 0/1
    exit
```
exit
!

interface ge 0/1
  ip address 10.1.2.12/24
  no shutdown
!

Step 3: Enable Overlay Routing over OMP

All site-local routes are populated on the vEdge routers. Distributed these routes to the other vEdge routers this is done through the Cisco vSmart Controller, via OMP.

1. If you are using BGP or if there are OSPF external LSAs, allow OMP to redistribute the BGP routes.
2. Re-advertise OMP routes into BGP or OSPF.
3. Commit.

Example Configuration of Overlay Routing over OMP:

```
omp
  advertise ospf external
```

At this point, vEdge-1 is able to learn about the prefixes from site-200, and vEdge-2 is able to learn about prefixes from site-100. Because all the prefixes are part of VPN 1, the hosts in site-100 and site-200 have reachability with one another. From a Cisco SD-WAN overlay network point of view, this reachability is possible because vEdge-1 advertises a vRoute consisting of the address 10.100.0.0/24 and the TLOC color of default, which we write as \{75.1.1.1, default\}, to the Cisco vSmart Controller. In turn, the Cisco vSmart Controller advertises this vRoute to vEdge-2. The same process happens with prefix 10.200.0.0/24 on vEdge-2.

Step 4: Check the Automatic Setup of the IPsec Data Plane

For every TLOC on a vEdge router, the vEdge router advertises a symmetric key for encryption. The Cisco vSmart Controller reflects this key automatically and advertises the TLOC with the symmetric key. A two-way IPsec SA is set up as a result (that is, there is a different key in each direction), and data traffic automatically starts to use this IPsec tunnel. Once a tunnel is up, BFD automatically starts on the tunnel. This is done to ensure fast data plane convergence in the event of a failure in the transport network.

The setup of the IPsec data plane happens automatically. No configuration is necessary. Multiple show commands are available to check the SAs and the state of the IPsec tunnel.

Step 5: Enforce Policies

As an optional step, you can create control and data plane policies on the Cisco vSmart Controller and push them to the vEdge routers. As an example, if the network administrator wants to enforce a policy to divert traffic destined to \{vEdge-2, prefix 10.200.0.0/24\} to go to another site say vEdge-3, a control plane policy can be created on the Cisco vSmart Controller and pushed to the respective vEdge routers. The results of the policy are pushed to the vEdge routers, not the configuration itself.

Example Configuration of Policies:

```
policy
  lists
    site-list site-100
    site-id 100
    prefix-list my-prefixes
```
Advanced Options

Now that we have looked at basic routing, security, and policy, we can start adding various other elements to the network. You are encouraged to look at the Software category to add elements such as High Availability, Convergence, BFD, QoS, ACLs, segmentation, and advanced policy.

Cisco SD-WAN Terminology

The following figure summarizes the terminology used to describe a Cisco SD-WAN overlay network.

Domain ID

A domain is a logical grouping of vEdge routers and Cisco vSmart Controllers that demarcate the span of control for the Cisco vSmart Controllers. Each domain is identified by a unique integer, called the domain ID. Currently, you can configure only one domain in a Cisco SD-WAN overlay network.

Within a domain, vEdge routers can connect only with the Cisco vSmart Controllers in their own domain. The Cisco vBond Orchestrator is aware of which Cisco vSmart Controllers are in which domain, so that when new vEdge routers come up, the Cisco vBond Orchestrator can point those routers to the Cisco vSmart Controllers in the proper domain. However, the Cisco vBond Orchestrator is never a member of a domain.>
Within a domain, there is full synchronization of routing information among the Cisco vSmart Controllers and vEdge routers, and there is scope for route aggregation and summarization. An organization can divide up its network into domains to serve desired business purposes. For example, domains can correspond to a large geographic area or to data centers so that each data center and the branches for which it is responsible are contained within a single domain.

**OMP Routes**

On Cisco vSmart Controllers and vEdge routers, OMP advertises to its peers the routes and services that it has learned from its local site, along with their corresponding transport location mappings, which are called Transport Locations (TLOCs). These routes are called OMP routes, to distinguish them from standard IP routes. It is through OMP routes that the Cisco vSmart Controllers learn the network topology and the available services.

The Cisco SD-WAN control plane architecture uses three types of OMP routes:

- **OMP routes**—Prefixes that establish reachability between end points that use the OMP-orchestrated transport network. OMP routes can represent services in a central data center, services at a branch office, or collections of hosts and other end points in any location of the overlay network. OMP routes require and resolve into TLOCs for functional forwarding. In comparison with BGP, an OMP route is the equivalent of a prefix carried in any of the BGP AFI/SAFI fields.

- **TLOCs**—Identifiers that tie an OMP route to a physical location. The TLOC is the only entity of the OMP routing domain that is visible to the underlying network, and it must be reachable via routing in the underlying network. A TLOC can be directly reachable via an entry in the routing table of the physical network, or it must be represented by a prefix residing on the outside of a NAT device and must be included in the routing table. In comparison with BGP, the TLOC acts as the next hop for OMP routes.

- **Service routes**—Identifiers that tie an OMP route to a service in the network, specifying the location of the service in the network. Services include firewalls, Intrusion Detection Systems (IDPs), and load balancers.

**Site ID**

A site is a particular physical location within the Cisco SD-WAN overlay network, such as a branch office, a data center, or a campus. Each site is identified by a unique integer, called a site ID. Each Cisco vEdge device at a site is identified by the same site ID. So within a data center, all the Cisco vSmart Controllers and any vEdge routers are configured with the same site ID. A branch office or local site typically has a single vEdge router, but if a second one is present for redundancy, both routers are configured with the same site ID.

**System IP Address**

Each vEdge router and Cisco vSmart Controller is assigned a system IP address, which identifies the physical system independently of any interface addresses. This address is similar to the router ID on a regular router. The system IP address provides permanent network overlay addresses for vEdge routers and Cisco vSmart Controllers, and allows the physical interfaces to be renumbered as needed without affecting the reachability of the Cisco vEdge device. You write the system IP address as you would an IPv4 address, in decimal four-part dotted notation.

**TLOC**

A TLOC, or transport location, identifies the physical interface where a vEdge router connects to the WAN transport network or to a NAT gateway. A TLOC is identified by a number of properties, the primary of which
is an IP address–color pair, which can be written as the tuple \{IP-address, color\}. In this tuple, IP address is the system IP address and color is a fixed text string that identifies a VPN or traffic flow within a VPN. OMP advertised TLOCs using TLOC routes.

**Additional Information**

For a description of the elements in a Cisco SD-WAN overlay network, see *Components of the Cisco SD-WAN Solution*. For an understanding of how you put together an overlay network using Cisco SD-WAN software and hardware, see *Constructing a Basic Network Using Cisco SD-WAN Components*. For examples of how the components of the overlay network work, see the *Validated Examples*. 
CHAPTER 4

Hardware and Software Installation

Table 1: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate a Bootstrap File For Cisco IOS XE SD-WAN Devices Using the CLI</td>
<td>Cisco IOS XE Release 17.3.1a</td>
<td>This feature enables you to generate a minimum bootstrap configuration file directly on a device, that enables a device to reconnect to the controller in case the full configuration is ever lost or removed.</td>
</tr>
</tbody>
</table>

- Server Recommendations, on page 25
- On-Site Bootstrap Process for Cisco SD-WAN Devices, on page 26
- On-Site Bootstrap Process for Cisco vEdge 5000 using SHA2 Enterprise Certificates, on page 28
- Generate a Bootstrap File For Cisco IOS XE SD-WAN Devices Using the CLI, on page 33
- One Touch Provisioning: Onboard Cisco IOS XE SD-WAN Devices Using Generic Bootstrap Configuration, on page 34
- Installing Cisco SD-AVC, Cisco vManage 20.1.1 and Earlier, on page 38
- Install Cisco SD-AVC, Cisco vManage Release 20.3.1 and Later, on page 40
- Software Installation and Upgrade for Cisco IOS XE Routers, on page 44
- Recover the Default Password, on page 53
- Software Installation and Upgrade for vEdge Routers, on page 54

Server Recommendations

This topic links to the hardware recommendations for the Cisco vBond Orchestrator server, vEdge Cloud router server, Cisco vManage server, and Cisco vSmart Controller server:

- Cisco vManage Release 20.1.x and earlier releases
- Cisco vManage 20.3.x (On-Prem)
- Cisco vManage Release 20.4.x (On-Prem, Multitenant)
vEdge Cloud Router Server Recommendations

Refer to vEdge Cloud Datasheet.

On-Site Bootstrap Process for Cisco SD-WAN Devices

The on-site bootstrap process involves generating a bootstrap configuration file that loads from a bootable USB drive or from internal boot flash to a device that supports SD-WAN. When the device boots, it uses the information in the configuration file to come up on the network.

The on-site bootstrap process consists of this general workflow:

• Use Cisco vManage to generate a configuration file
• Copy the configuration file to a bootable USB drive and plug the drive into a device, or copy the configuration to the bootflash of a device
• Boot the device

If the configuration file is on both an inserted USB drive and on the bootflash, a device gives priority to the configuration file on the bootflash.

Device Requirements

A device that you configure by using the on-site bootstrap process must meet these requirements:

• A supported SD-WAN image must be installed on the device
• The device must be in its factory state with no added configuration

Perform the On-Site Bootstrap Process

To perform the on-site bootstrap process for a device, follow these steps:

1. Upload the Chassis ID and the serial number of the device to Cisco vManage.
   For instructions, see Upload the vEdge Serial Number File.
2. From the Cisco vManage menu, choose Administration > Settings and make sure that the Organization Name and the Cisco vBond Orchestrator IP address are configured properly.
3. If you are using your own enterprise root certificate authority (CA) for device certification in your network, take these actions in Cisco vManage:
   a. Select Administration > Settings.
   b. Click Edit in the WAN Edge Cloud Certificate Authorization row.
   c. Click Manual.
   d. Click Save.
4. From the Cisco vManage menu, choose Configuration > Templates > Feature and create a template for the device.
   For more information about creating a template, see Create a Device Template section in Templates.
5. Perform the following steps:
a. From the Cisco vManage menu, choose Configuration > Devices.

b. In the dialog box, choose Cloud-init and click OK.

The system generates a Multipurpose Internet Mail Extensions (MIME) file and displays its contents in a pop-up window. This file contains system properties for the device, the root CA if you are using an enterprise root CA, and configuration settings from the template that you created.

6. In the MIME file pop-up window, click Download.

The system downloads the file to your local system and saves it in your directory for downloads. The file name is chassis.cfg, where chassis is the device chassis ID that you uploaded in Step 1.

---

**Note**
As an alternative to this step, you can copy the contents of the MIME file from the pop-up window to a text file, save the text file with the name ciscosdwan.cfg (case sensitive), and then skip to Step 8.

---

**Note**
For hardware devices, use the bootstrap file name as ciscosdwan.cfg. This file is generated by Cisco vManage and includes UUID, but does not include OTP. For software devices (CSR and ISRv), and OTP-authenticated devices such as ASR1002-X, use the bootstrap file name as ciscosdwan_cloud_init.cfg. This file contains the OTP but not the UUID validation for ciscosdwan_cloud_init.cfg.

7. If you downloaded the MIME file, rename it to ciscosdwan.cfg (case sensitive).

---

**Note**
This is the configuration file for the on-site bootstrap process.

8. Copy the ciscosdwan.cfg file to a bootable USB drive or to the bootflash of the device.

---

**Note**
The file must be named exactly as shown or the device will not read it.

9. If you are using a USB drive, plug the USB drive into the device.

10. Boot the device.

The device reads the configuration file from the USB drive or the bootflash and uses the configuration information to come up on the network. The device give priority to a configuration file that is on its bootflash.
On-Site Bootstrap Process for Cisco vEdge 5000 using SHA2 Enterprise Certificates

Table 2: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-Site Bootstrap Process for Cisco vEdge 5000 using SHA2 Enterprise Certificates</td>
<td>Cisco SD-WAN Release 20.3.1</td>
<td>By default, a Cisco vEdge 5000 device uses an SHA1 certificate for authentication with controllers in the overlay network. With this feature, you can authenticate the device using an OTP and a Public Key, and install an SHA2 enterprise certificate on the device. By authenticating the device using an OTP and a Public Key and installing an SHA2 enterprise certificate, you can bypass SHA1 certificate authentication and secure the device against SHA1 vulnerabilities.</td>
</tr>
<tr>
<td>Cisco vManage Release 20.3.1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A Cisco vEdge 5000 device is equipped with a Trusted Platform Module (TPM 1.2) and uses SHA1 certificates for authentication while connecting to the overlay network. For information on the bootstrap process using SHA1 certificates, see On-Site Bootstrap Process for Cisco SD-WAN Devices.

From Cisco SD-WAN Release 20.3.1, while bootstrapping a Cisco vEdge 5000 device and connecting the device to the overlay network, you can authenticate the device using a One Time Password (OTP) and a Public Key, and install an SHA2 enterprise certificate on the device. By authenticating the device using an OTP and a Public Key and installing an SHA2 enterprise certificate, you can bypass SHA1 certificate authentication and secure the device against SHA1 vulnerabilities.

How Cisco vEdge 5000 is Authenticated using OTP and Public Key

1. Enter the public key for the device on Plug and Play Connect and generate the serial.viptela file.
2. Upload the serial.viptela file to Cisco vManage.
3. Cisco vManage generates a random authentication token for the device. Cisco vManage encrypts the authentication token using the device public key and populates it as the OTP in the <chassis>.config file.
4. Download the <chassis>.config file to a bootable USB drive and insert the USB drive into the device after performing a factory reset.
5. The device reads the <chassis>.config file, reads the encrypted digest from the OTP field, decrypts the digest using the device private key and obtains the authentication token.
6. The device disables AVNET/TPM1.2 SHA1 certificate authentication.
7. The device authenticates itself with Cisco vManage using the authentication token and establishes a control connection.

8. Cisco vManage pushes the initial configuration into the device.

9. Cisco vManage pushes the SHA2 enterprise certificate for the device and installs the certificate on the device.

10. Device reauthenticates itself to controllers using the SHA2 enterprise certificate and connects to controllers.

**Points to Consider**

- After a Cisco vEdge 5000 device is authenticated with Cisco vBond Orchestrator or Cisco vManage using OTP, do not reboot the device until the SHA2 enterprise certificate is installed and validated. If the device reboots before the Enterprise Certificate is validated, restart the bootstrap procedure.

- After a signed SHA2 enterprise certificate is installed on a Cisco vEdge 5000 device and the bootstrapping process is complete, if you perform a software reset, a configuration reset, or a factory reset, bootstrap the device again.

- Every time you generate the Cloud-Init(Encrypted OTP) bootstrap configuration, you must download the new configuration file to a bootable USB drive.

**Prerequisites**

1. Ensure Enterprise Certificate authorization is configured.
   a. From the Cisco vManage menu, choose Administration > Settings > Hardware WAN Edge Certificate Authorization.
   b. Click Edit and ensure that Enterprise Certificate (signed by Enterprise CA) is selected. Click Save.

2. Ensure that the Public Key entry for the device is available on the PNP server before generating the serial.viptela file. For more information, see View or Add Public Key for a Cisco vEdge 5000 Device.

3. If a Cisco vEdge 5000 device is connected to the overlay network using SHA1 certificates, you must invalidate and remove the device from the overlay network before configuring the use of OTP, Public Key, and SHA2 enterprise certificate for authentication.

**View or Add Public Key for a Cisco vEdge 5000 Device**

1. On Cisco Software Central, log in to Plug and Play Connect using the required Smart and Virtual Accounts required to access the Cisco vEdge 5000 device.

2. In the Devices list, click on the serial number of the Cisco vEdge 5000 device.
   The Device Information is displayed.

3. In the Device Information dialog box, check whether the device Public Key is available.

4. If the Public Key is not available, add the Public Key:
   a. In the Devices list, select the Cisco vEdge 5000 device using the check box.
b. Click Edit.
   The Edit Devices page is displayed.

c. In the Selected Devices area, click view/edit in the Public Key column.
   The Public Key dialog box is displayed.

d. Enter the Public Key in the text box, or click Browse to upload a file containing the Public Key.

e. Click OK to save the Public Key and close the dialog box.

f. On the Edit Devices page, click Submit to attach the Public Key to the Cisco vEdge 5000 device.

Bootstrap Procedure

The on-site bootstrap process involves generating a bootstrap configuration file that loads from a bootable USB drive. When the Cisco vEdge 5000 device boots, it uses the information in the configuration file to connect to the overlay network.

1. From the Cisco vManage menu, choose Configuration > Devices > WAN Edge List.

2. Click Upload WAN Edge List.

3. In the Upload WAN Edge List dialog box, select the the Cisco vEdge 5000 serial number file to upload. Select Validate the uploaded vEdge list and send to controllers and click Upload.
   The WAN Edge List is uploaded to controllers.
   The Cisco vEdge 5000 device is added to the WAN Edge List.

4. Attach the device to a device configuration template.
   a. From the Cisco vManage menu, choose Configuration > Templates.
   b. Click Device and select a template.
   c. For the desired template, click ... and choose Attach Devices. The Attach Devices dialog box opens.
   d. In the Available Devices column, select a group, and search to select the Cisco vEdge 5000 device.
   e. Click the arrow pointing right to move the device to the Selected Devices column.
   f. Click Attach.
      Configuration template is scheduled for the device.

5. Generate the bootstrap configuration for the newly added device.
   a. From the Cisco vManage menu, choose Configuration > Devices.
   b. Click WAN Edge List, select the Cisco vEdge 5000 device.
   c. For the selected device, click ... and choose Generate Bootstrap Configuration.
   d. In the Generate Bootstrap Configuration dialog box, select Cloud-Init(Encrypted OTP) and click OK.
   e. Click Download to download the bootstrap configuration and save the file with a filename in the <ChassisNumber>.cfg format.
f. Copy the `<ChassisNumber>.cfg` file to a bootable USB drive.

- The USB drive must be of the FAT-32 format for Cisco vEdge 5000 device to recognize and auto-mount the drive.

- Copy the `<ChassisNumber>.cfg` file to the home or parent directory of the USB drive.

---

6. Send the Cisco vEdge 5000 serial number file and OTP information to controllers.
   
   a. From the Cisco vManage menu, choose **Configuration > Certificates > WAN Edge List**.

   b. Click **Send to Controllers** to synchronize the WAN Edge list on all controllers.

   The device serial number file and OTP information are sent to controllers.

   c. (Optional) Verify the WAN Edge List on controllers using the command **show orchestrator valid-vedges hardware-installed-serial-number prestaging**.

   ```
   vbond# show orchestrator valid-vedges hardware-installed-serial-number prestaging
   
   HARDWARE
   INSTALLED SUBJECT
   SERIAL SERIAL CHASSIS NUMBER SERIAL NUMBER VALIDITY ORG
   
   193A012170001 deaedf5d39919454fdcc8470eccd8d8 valid vIPtela Inc Regression prestaging N/A
   ```

7. Perform a factory reset of the Cisco vEdge 5000 device with a default image of Cisco SD-WAN Release 20.3.1 or later.

8. When the Cisco vEdge 5000 device is ‘Up’ (indicated by a status of ‘System: Up’ on the LCD display), insert the USB drive with `<ChassisNumber>.cfg` file.

   The device reads the `<ChassisNumber>.cfg` file from the USB drive. Organization-name, Cisco vBond Orchestrator IP address, OTP token, and Enterprise root-ca are retrieved from the configuration file.

   a. (Optional) Issue the **show control local-properties** command on the device to verify the information retrieved from the configuration file.

   b. (Optional) If the device WAN interface is not assigned an IP address through DHCP, configure a static IP address and the routing information required to reach controllers.

   The device connects to Cisco vBond Orchestrator and Cisco vManage after authentication using the OTP.

   The device obtains the System IP address and the site ID from Cisco vManage configuration templates. If templates are not configured on Cisco vManage, configure the required system configuration on the device.
After the device connects to Cisco vManage, Cisco vManage retrieves the Enterprise Certificate Signing Request (CSR). From the Cisco vManage menu, choose **Configuration > Certificates > WAN Edge List**, the device certificate state is shown as **CSR**.

9. **Download CSR.**
   a. From the Cisco vManage menu, choose **Configuration > Certificates**.
   b. Select the Cisco vEdge 5000 device for which to sign a certificate.
   c. 
   d. To download the CSR, click **Download**.

10. **Send the certificate to a third-party signing authority and have them sign it.**
11. **To install the certificate on the device, perform the following steps:**
   a. From the Cisco vManage menu, choose **Configuration > Certificates > Controllers**.
   b. 
   c. In the **Install Certificate** screen, paste the certificate into the **Certificate Text** field, or click **Select a File** to upload the certificate in a file.
   d. Click **Install**.

The installed certificate serial number of the device is updated on the controllers.

From the Cisco vManage menu, choose **Configuration > Certificates > WAN Edge List**, the device certificate state is shown as installed.

12. **(Optional) Check the WAN Edge list on the controller to confirm that the device serial number is installed.**

```
vbond# show orchestrator valid-vedges hardware-installed-serial-number 12399910

+---------+-------------------+-------------------+-------------------+-------------------+
| HARDWARE | INSTALLED | SUBJECT |
| SERIAL   | SERIAL     | SERIAL     | SERIAL     |
| CHASSIS NUMBER | NUMBER | VALIDITY | ORG     |
| NUMBER     | NUMBER     | NUMBER     | NUMBER     |
+---------+-------------------+-------------------+-------------------+-------------------+
| 193A0122170001 18DB5D4F valid vIPtela Inc Regression 12399910 N/A |
```

13. **Remove the USB drive from the device.**

**Outcome**

- The Cisco vEdge 5000 device is added to the overlay network and connected to the controllers using the SHA2 Enterprise Certificate.
- The device will use the installed SHA2 Enterprise Certificate after a reboot, a software upgrade, or a software downgrade to Cisco SD-WAN Release 20.3.1 or a later release. Use of SHA1 certificates is disabled.
Generate a Bootstrap File For Cisco IOS XE SD-WAN Devices Using the CLI

To establish connectivity with the Cisco SD-WAN controller, a device requires a minimum configuration. In most situations, this minimum bootstrap configuration (MBC) can be provided initially by plug-and-play (PnP). But in some situations, such as in remote sites where it may be preferable not to use PnP, it is helpful to have a saved bootstrap configuration that can connect the device to the controller.

The `request platform software sdwan bootstrap-config save` command saves the device configuration to the bootflash. The command can be used to save the configuration at any time, but it is intended for saving a minimum bootstrap configuration (MBC) file that enables the device to reconnect to the controller in case the full configuration is ever lost or removed.

When setting up a device, add to the configuration the details that are required to connect to the controller, and then use this command to save the MBC. The file is saved to this location:

```
bootflash:/ciscosdwan.cfg
```

**Prerequisites**

- The controller root certificate is installed on the Cisco IOS XE SD-WAN device, to authenticate the device.
- The device is physically connected to the WAN through one of its interfaces.

**Procedure**

1. On the Cisco IOS XE SD-WAN device, establish connectivity to Cisco vManage, by configuring the following:
   - System IP address
   - Domain ID
   - Site ID
   - sp-organization-name
   - organization-name
   - Cisco vBond Orchestrator IP address and port number
   - Tunnel with encapsulation configured as either GRE or IPSEC

Example:

```
system
system-ip 10.0.0.10
domain-id 1
site-id 200
admin-tech-on-failure
sp-organization-name CiscoISR
organization-name CiscoISR
vbond 10.0.100.1 port 12346
!
interface Tunnel1
```
no shutdown
ip unnumbered GigabitEthernet0/1/0
tunnel source GigabitEthernet0/1/0
tunnel mode sdwan
exit
sdwan
interface GigabitEthernet0/1/0
tunnel-interface
capsulation ipsec
exit
exit
commit

2. Use `show sdwan control connections` to verify connectivity to the Cisco vManage, Cisco vSmart Controller, and Cisco vBond Orchestrator.

3. Use the `request platform software sdwan bootstrap-config save` command to save a bootstrap file to the device bootflash.

Example:

```
Device# request platform software sdwan bootstrap-config save
Saving bootstrap file 'bootflash:/ciscosdwan.cfg'...
Done
```

The configuration file is saved to this location:

```
bootflash:/ciscosdwan.cfg
```

One Touch Provisioning: Onboard Cisco IOS XE SD-WAN Devices Using Generic Bootstrap Configuration

### Table 3: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>One Touch Provisioning: Onboard Cisco IOS XE SD-WAN Devices Using Generic Bootstrap Configuration</td>
<td>Cisco IOS XE Release 17.4.1a</td>
<td>You can generate a generic bootstrap configuration on Cisco vManage and use this configuration to onboard multiple Cisco IOS XE SD-WAN devices. When you boot a device with the generic bootstrap configuration, the device is listed on Cisco vManage as an unclaimed WAN edge device. To complete the onboarding, claim the device on Cisco vManage and attach a device template that configures the system IP address and site ID.</td>
</tr>
<tr>
<td></td>
<td>Cisco vManage Release 20.4.1</td>
<td></td>
</tr>
</tbody>
</table>

**Overview of Generic Bootstrap Configuration**

To onboard a Cisco IOS XE SD-WAN device to the Cisco SD-WAN overlay network, you generate a bootstrap configuration on Cisco vManage and boot the device with this configuration. After the device connects to Cisco vManage, you complete the onboarding using the Cisco vManage GUI. The bootstrap configuration contains device-specific configuration settings, requiring you to generate a bootstrap configuration for each device that you must onboard. From Cisco IOS XE Release 17.4.1a, you can use a generic bootstrap configuration to onboard multiple Cisco IOS XE SD-WAN devices.
The generic bootstrap configuration omits device-specific details, such as the device UUID, and provides settings that a Cisco IOS XE SD-WAN device can use to connect to the Cisco vBond Orchestrator. When the device connects to the Cisco vBond Orchestrator, the device is listed as an unclaimed WAN edge device on Cisco vManage. To complete the onboarding, you must claim the device on Cisco vManage and attach a device template that configures the system IP and site ID. Cisco vManage authenticates the device using a certificate that is installed on the device as part of the generic bootstrap configuration.

The generic bootstrap configuration contains the following:

- Organization name
- WAN interface to be enabled on the Cisco IOS XE SD-WAN device
- IP address of the Cisco vBond Orchestrator
- Cisco vManage-signed certificate for authenticating the device.

To use generic bootstrap configuration to onboard a device, you must have a Dynamic Host Configuration Protocol (DHCP) server in the branch network where you are installing the device. The generic bootstrap configuration does not assign an IP address to the WAN interface. Instead, the configuration enables a DHCP client on the WAN interface so that the interface can acquire an IP address from a DHCP server in the branch network.

**How the Generic Bootstrap Configuration Works**

1. While generating the generic bootstrap configuration on Cisco vManage, you select the interface that will serve as the VPN 0 (WAN) interface on the Cisco IOS XE SD-WAN device.
2. Copy the generic bootstrap configuration file onto the device bootflash and reset the device. On reset, the device is initialized with the generic bootstrap configuration.
3. The bootstrap configuration enables a DHCP client on the designated VPN 0 interface. The interface acquires an IP address and related details from a DHCP server in the network.
4. The device connects to the Cisco vBond Orchestrator through the VPN 0 interface is listed as an unclaimed WAN edge device on the Cisco vBond Orchestrator and Cisco vManage.
5. When you claim the device on Cisco vManage, Cisco vManage authenticates the device using the certificate installed on the device as part of the bootstrap configuration. After authentication, the device is listed among the valid WAN edge devices on Cisco vManage and the Cisco vBond Orchestrator.
6. Attach and push a template containing the system IP and site ID to the device.
7. The device establishes control connections to Cisco vSmart Controllers and is added to the overlay network.

**Onboard a Cisco IOS XE SD-WAN Device using Generic Bootstrap Configuration**

1. Enable One Touch Provisioning:
   a. From the Cisco vManage menu, choose Administration > Settings.
   b. Check if One Touch Provisioning is Enabled. If Enabled, go to Step 2.
   c. If One Touch Provisioning is Disabled, click Edit.
   d. For the Enable Claim WAN Edges setting, choose Enabled and click Save.
2. From the Cisco vManage menu, choose **Configuration > Devices > WAN Edge List.**

3. Click **Export Bootstrap Configuration.**
   a. In the **Export Bootstrap Configuration** dialog box, enter the **VPN0 Interface name.**

**Note**

The **VPN 0 interface name** may vary among Cisco IOS XE SD-WAN device models. Specify the interface name based on the model you wish to onboard.

b. Click **Generate Generic Configuration.**

4. Save the generic bootstrap configuration file.
   The file is named in the format `<filename>.cfg`.

5. Rename the generic bootstrap configuration file as `ciscosdwan.cfg`.

6. Copy the `ciscosdwan.cfg` file to a bootable USB drive or to the bootflash of the device.

7. If you are using a USB drive, plug the USB drive into the device.

8. Reset the device software configuration by issuing the following commands on the CLI:
   ```
   Device# request platform software sdwan config reset
   Device# reload
   ```

9. Reboot the device.
   • While rebooting, the device reads the configuration file from the USB drive or the bootflash and applies the configuration.
   The configuration enables the VPN 0 interface and initializes a DHCP client on the interface. The interface acquires an IP address from a DHCP server in the network.
   The device connects to the Cisco vBond Orchestrator and is listed as an unclaimed WAN edge device on the Cisco vBond Orchestrator and Cisco vManage.
   • On the Cisco vBond Orchestrator, you can view the unclaimed WAN edge devices by using the command `show orchestrator unclaimed-vedges`.
   • If the device is not listed as an unclaimed WAN edge device, check whether the device can connect to the Cisco vBond Orchestrator and correct any connectivity issues.

10. Claim the device on Cisco vManage:
   a.
   b. Choose the device you wish to claim and click **Claim Device(s).**
      • The device is removed from **Unclaimed WAN Edges** and listed on **WAN Edge List.**
      • On the Cisco vBond Orchestrator, the device is listed as a valid WAN edge device. You can view the valid WAN Edge devices by issuing the command `show orchestrator valid-vedges`.

11. Attach a configuration template to the device.
   a. Ensure that the template includes the system IP address and the site ID.
b. Push the template to the device.

**Result**

The device connects to Cisco vSmart Controllers and is added to the overlay network.

To verify that the device has established control connections and is part of the overlay network, from the Cisco vManage menu, choose Dashboard > Main Dashboard and click WAN Edge devices in the Summary Pane.

**Remove a Cisco IOS XE SD-WAN Device Onboarded Using Generic Bootstrap Configuration**

1. Detach device from templates:
   a. From the Cisco vManage menu, choose **Configuration > Templates**.
   b. Click **Device** and select the template attached to the device.
   c. For the selected template, click ... and choose **Detach Devices**.
   d. In the **Available Devices** column, select the device to be detached from the template.
   e. Click the arrow pointing right to move the device to the **Selected Devices** column.
   f. Click **Detach**.

2. Connect to the device using SSH. From the device SSH terminal, shut down the VPN 0 WAN interface by using the following commands:

   ```
   Device(config)# interface vpn0-interface-name
   Device(config-if)# shutdown
   ```

3. Invalidate the device:
   a. From the Cisco vManage menu, choose **Configuration > Certificates**.
   b. Click **WAN Edge List** and choose the device to invalidate.
   c. In the **Validate** column, click **Invalid**.
   d. Click **OK** to confirm the move to the invalid state.
   e. Click **Send to Controllers** to send the chassis and serial number of the invalidated device to the controllers in the network. Cisco vManage displays the **Push WAN Edge List** screen showing the status of the push operation.

4. Delete the WAN edge device:
   a. From the Cisco vManage menu, choose **Configuration > Devices**.
   b. Click **WAN Edge List** and select the device you wish to remove.
   c. For the selected device, click ... and choose **Delete WAN Edge**.
   d. Click **OK** to confirm deletion of the device.
Installing Cisco SD-AVC, Cisco vManage 20.1.1 and Earlier

Note
Beginning with Cisco vManage Release 20.3.1/Cisco IOS XE Release 17.3.1a, the Cisco SD-AVC installation has changed. See Install Cisco SD-AVC, Cisco vManage Release 20.3.1 and Later, on page 40.

Overview
Beginning with the 18.4 release, SD-WAN can optionally incorporate Cisco Software-Defined Application Visibility and Control (SD-AVC) on Cisco IOS XE SD-WAN devices. The SD-AVC network service operates as a container within Cisco vManage.

What are the benefits of this feature?
Cisco SD-AVC uses Cisco NBAR2 and other components that operate on devices in the network to provide:

- Recognition of network application traffic for visibility, analytics, application-aware routing, and application-based policies, such as QoS and application-based firewall policy.
- Analytics at the network level.

Cisco SD-AVC Installation Requirements for Cisco vManage
The following table describes the SD-AVC installation requirements.

<table>
<thead>
<tr>
<th>Cisco vManage Installation Scenario</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco vManage 18.4 on a cloud-based server, provided fully configured by the Cisco cloud operations team</td>
<td>The SD-AVC package is pre-installed by the Cisco cloud operations team.</td>
</tr>
<tr>
<td>Cisco vManage 18.4 on a self-managed cloud or local server</td>
<td>Install the SD-AVC package as described below.</td>
</tr>
<tr>
<td>Upgrading from an earlier version of Cisco vManage to Cisco vManage 18.4</td>
<td>Install the SD-AVC package as described below.</td>
</tr>
</tbody>
</table>

Enabling SD-AVC on Cisco vManage

Prerequisites
- Download the latest container image for the SD-AVC network service. Save the file to an accessible location on the server hosting Cisco vManage. This container is required for the procedure. To download the container, open the Cisco Software Download page and enter "SD-WAN". Select "Software-Defined WAN (SD-WAN)" from the results, then "SD-WAN" in the results. In the software packages available for download, select SD-AVC.
- Ensure that routers in the network that are included in the SD-WAN topology have a DNS server configured.
• The virtual machine in which Cisco vManage operates must have the following resources available to
dedicate to the SD-AVC network service:
  • vCPU: 4
  • RAM: 5 GB
  • Storage: 40 GB

Procedure
1. Ensure that the downloaded SD-WAN image is compatible with your version of Cisco vManage.
   a. Display the checksum for the compatible image, using the following API:
     https://[vManage-IP-address]/dataservice/sdavc/checksum
     Example: https://10.0.0.1/dataservice/sdavc/checksum
   b. Verify that the checksum of the downloaded image matches this.
2. To upload the SD-AVC virtual service package to Cisco vManage:
   a. From the Cisco vManage menu, choose Maintenance > Software Repository.
   b. Click Virtual Images and select Upload Virtual Image to upload the SD-AVC package.
3. From the Cisco vManage menu, choose Administration > Cluster Management page.
4. For the desired host (the Cisco vManage portal on which you are enabling SD-AVC), click … and choose Edit.
5. In the Edit vManage dialog box, enter the username and password, using Cisco vManage credentials.
6. Select the checkbox for Enable SD-AVC. Click Update.
7. Cisco vManage prompts you to confirm before rebooting the device to apply the changes to the device. Click OK to confirm.
8. After the reboot, Cisco vManage comes up automatically and displays progress on the SD-AVC activation. Wait for the activation to complete.
9. (Optional) After installation is complete, you can verify that Cisco vManage has the SD-AVC virtual
   service installed and operating correctly.
   a. From the Cisco vManage menu, choose Administration > Cluster Management.
   b. In Service Configuration, in Cisco vManage row of the table, verify that the SD-AVC shows a green
      checkmark.

For information about Cisco vManage commands, see vManage Command Reference documentation.

Enable SD-AVC on Cisco vEdge Devices

To enable SD-AVC on the Cisco IOS XE SD-WAN device, create a localized policy that enables app visibility
and apply the policy to the template for the Cisco IOS XE SD-WAN device.
Prerequisites

- A template exists for the Cisco IOS XE SD-WAN device (example: Cisco ASR 1001-X, Cisco ISR 4321).

Procedure

1. From the Cisco vManage menu, choose Configuration > Policies.
2. Click Localized Policy.
3. To add a policy and enable Application, follow the steps below:
   a. Click Add Policy.
   b. Click Next on the several screens (Create Groups of Interest, Configure Forwarding Classes/QOS, Configure Access Control Lists, Configure Route Policy) until the Policy Overview screen.
   c. In the Policy Overview screen, enter a policy name and policy description.
   d. Select Application.
   e. Save the policy.
4. To add the localized Policy to the device template, follow the steps below:
   a. From the Cisco vManage menu, choose Configuration > Templates.
   b. For the device on which you have to enable SD-AVC, click … and select Edit from the menu.
   c. Click Additional Templates.
   d. Add the localized policy created in an earlier step of this procedure.
   e. Click Update and proceed through the next screens to push the updated template to the device.
5. (Optional) After pushing the update to the device, you can check the status of SD-AVC on the device with one of the following commands.
   - show avc sd-service info summary
   - show avc sd-service info connectivity

Install Cisco SD-AVC, Cisco vManage Release 20.3.1 and Later

Installing or upgrading to Cisco vManage Release 20.3.1 automatically includes installation of Cisco SD-AVC as a component.

Overview

Beginning with the 18.4 release, SD-WAN can optionally incorporate Cisco Software-Defined Application Visibility and Control (SD-AVC) on Cisco IOS XE SD-WAN devices. The SD-AVC network service operates as a container within Cisco vManage.
Cisco SD-AVC must operate on only one Cisco vManage instance. In a Cisco vManage cluster, enable Cisco SD-AVC on only one instance of Cisco vManage.

**Note**

All relevant Cisco SD-AVC functionality is accessed through the Cisco vManage interface.

**What are the benefits of this feature?**

Cisco SD-AVC uses Cisco NBAR2 and other components that operate on devices in the network to provide:

- Recognition of network application traffic for visibility, analytics, application-aware routing, and application-based policies, such as QoS and application-based firewall policy.
- Analytics at the network level.

---

### Enable Cisco SD-AVC, Cisco vManage Release 20.3.1 and Later

**Prerequisites**

- Ensure that routers in the network that are included in the Cisco SD-WAN topology have a DNS server configured.
- The virtual machine in which Cisco vManage operates must have a minimum of the following resources:
  - RAM: 32 GB
  - Storage: 500 GB
  - vCPU: 16

**Note**

Cisco SD-AVC must operate on only one Cisco vManage instance. In a Cisco vManage cluster, enable Cisco SD-AVC on only one instance of Cisco vManage.

To enable Cisco SD-AVC, perform the following steps.

1. From the Cisco vManage menu, choose **Administration > Cluster Management**.
2. For the desired host (the portal on which you are enabling SD-AVC), click ... and select **Edit**.
3. In the **Edit vManage** pop-up window, select the checkbox for **Enable SD-AVC**.
4. Enter the username and password, using Cisco vManage credentials. Cisco vManage reboots the device.

**Note**

The **Edit vManage** pop-up window provides an option for disabling the application server. After disabling the application server, you cannot later enable other services using this method. If you need to disable the application server, do not do this at the same time that you enable other features.
5. After the reboot, Cisco vManage comes up automatically and displays progress on the SD-AVC activation. Wait for the activation to complete.

6. (optional) After installation is complete, you can verify that Cisco vManage has the SD-AVC virtual service installed and operating correctly.
   a. From the Cisco vManage menu, choose **Administration > Cluster Management**.
   b. Click **Service Configuration**, in the vManager row of the table, verify that SD-AVC shows a green checkmark.

---

### Enable SD-AVC on Cisco vEdge Devices

To enable SD-AVC on the Cisco IOS XE SD-WAN device, create a localized policy that enables app visibility and apply the policy to the template for the Cisco IOS XE SD-WAN device.

**Prerequisites**
- A template exists for the Cisco IOS XE SD-WAN device (example: Cisco ASR 1001-X, Cisco ISR 4321).

**Procedure**

1. From the Cisco vManage menu, choose **Configuration > Policies**.
2. Click **Localized Policy**.
3. To add a policy and enable Application, follow the steps below:
   a. Click **Add Policy**.
   b. Click **Next** on the several screens (Create Groups of Interest, Configure Forwarding Classes/QOS, Configure Access Control Lists, Configure Route Policy) until the **Policy Overview** screen.
   c. In the **Policy Overview** screen, enter a policy name and policy description.
   d. Select **Application**.
   e. Save the policy.
4. To add the localized Policy to the device template, follow the steps below:
   a. From the Cisco vManage menu, choose **Configuration > Templates**.
   b. For the device on which you have to enable SD-AVC, click ... and select **Edit** from the menu.
   c. Click **Additional Templates**.
   d. Add the localized policy created in an earlier step of this procedure.
   e. Click **Update** and proceed through the next screens to push the updated template to the device.
5. (Optional) After pushing the update to the device, you can check the status of SD-AVC on the device with one of the following commands.

```bash
show avc sd-service info summary
```
Enable Cisco SD-AVC Cloud Connector

Table 4: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco SD-AVC Cloud Connector</td>
<td>Cisco IOS XE Release 17.3.1a</td>
<td>When enabling Cloud onRamp for SaaS to manage Office 365 traffic, you can limit best path selection to apply only to some Office 365 traffic, according to the Office 365 traffic categories defined by Microsoft, or to include all Office 365 traffic. The Cisco SD-AVC Cloud Connector provides support for this functionality.</td>
</tr>
<tr>
<td></td>
<td>Cisco vManage Release 20.3.1</td>
<td></td>
</tr>
</tbody>
</table>

Cisco SD-AVC Cloud Connector is a necessary component for Cloud onRamp for SaaS to manage Office 365 traffic according to the Office 365 traffic category.

1. From the Cisco vManage menu, choose **Administration > Settings**.

2. If **SD-AVC Cloud Connector** is disabled, click **Edit and Enabled**.

3. When prompted, see the following instructions for creating the credentials:

   Click (i) for **Client ID** and open the Cisco API Console page in a browser window to create Cloud Connector credentials if you do not already have credentials.

   - **SD-AVC Cloud Connector credentials:**
     - **Client ID**
     - **Client Secret**
     - **Organization Name:** Use the descriptive name that you entered on the Cisco API Console page in the **Name of your application** field.

   - **Affinity:** (optional) Select a geographical location for storing the Cloud Connector data. For organizations located in Europe, it is recommended to change the location to Europe, in accordance with EU General Data Protection Regulation (GDPR) regulations.

   - **Telemetry:** (optional) Disable collecting telemetry data.

Create Credentials on the Cisco API Console

The following steps show how to create credentials in the Cisco API Console. These steps are provided here for convenience, and are subject to change.

1. On the Cisco API Console page, sign in using your Cisco credentials.
2. Click My Apps and keys. A page opens for registering a new application.

3. To register SD-AVC, follow the steps below:
   a. Name of your application: Use any descriptive name. Save this name for a later step.
   b. Select the Client Credentials checkbox.
   c. Select the Hello API checkbox.
   d. In the Terms of Service section, select the check box to agree with the terms.
   e. Click Register. The Cisco API Console page displays the Client ID and Client Secret details. Keep this page open to complete the procedure.

Note
These credentials expire after 90 days.

Software Installation and Upgrade for Cisco IOS XE Routers

You can install up to two Cisco SD-WAN images on the same router.

Supported Hardware Platforms and Interface Modules
For supported Hardware platforms and interface modules, see Release Notes.

Supported Crypto Modules
The following crypto modules are required for the ASR 1000 series routers:

• ASR1001HX-IPSECHW, for the ASR 1001-HX
• ASR1002HX-IPSECHW, for the ASR 1002-HX

Before You Begin

Before you deploy an IOS XE router in the overlay network, review the following:

• The controller devices—Cisco vBond Orchestrators, Cisco vManage instances, and Cisco vSmart Controllers—are running Cisco SD-WAN Software Release 18.3.

• If you deploy both IOS XE and vEdge routers in the overlay network, the vEdge routers are running Release 17.2.1 or higher of the Cisco SD-WAN software. With these software versions, the vEdge and IOS XE software can interoperate, allowing BFD tunnels to be established between vEdge routers and IOS XE routers.

• If you deploy both IOS XE and vEdge routers in the same site, the vEdge routers are running Cisco SD-WAN Software Release 18.3.

• The ISR 4000 series router has at least 4 gigabytes (GB) of DRAM installed. It is recommended that the router have 8 GB of DRAM.
• The ASR 1000 Cisco vBond Orchestrator series router has at least 8 GB of DRAM installed. The ASR 1002-HX router has at least 16 GB of DRAM installed.

• The router's bootflash has a minimum of 1.5 GB space available for the XE SD-WAN image.

• If using your enterprise root certificate to authenticate the router, the certificate is copied to the router's bootflash before installing the XE SD-WAN software.

• All unsupported modules are removed from the router before installing the XE SD-WAN software. For a list of supported modules, see Supported Interface Modules and Supported Crypto Modules.

• For information about deploying a Cisco ASR 1006-X with an RP3 module, see Cisco ASR 1006-X with an RP3 Module.

• The updated device list is uploaded to Cisco vManage and sent to the Cisco vBond Orchestrator. To do so:

1. Obtain the router's chassis and board ID serial number by issuing the `show crypto pki certificates CISCO_IDEVID_SUDI` command at the system prompt. If running Release 16.6.1 or earlier on an ASR series router, issue the `show sdwan certificate serial` command.

2. Add the router's serial number to Plug and Play (PnP) Connect portal. See Add the IOS XE Router to the PnP Portal section for more details.

3. From the Cisco vManage menu, choose Configuration > Devices. Click Sync Smart Account to download the updated device list to Cisco vManage and send it to the Cisco vBond Orchestrator.

• Device configuration templates are created and attached to the router using Cisco vManage Configuration > Templates. This ensures that the router can obtain a configuration and establish full control connections when it comes up.

• If the router exceeds the unidirectional encrypted bandwidth of 250 Mbps and if the HSECK9 license is not already installed, the license file is copied to the router's bootflash and license installed on the router license install file path.

• The ASR 1000 series, ISR 1000 series, and ISR 4000 series router is running the required version of the ROM monitor software (ROMMON), as shown in the following table. To verify the ROMMON version running on the router, issue the `show rom-monitor` or `show platform` command at the system prompt.

<table>
<thead>
<tr>
<th>Hardware Platform</th>
<th>Required ROM Monitor Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR 1000 series</td>
<td>16.3 (2r)</td>
</tr>
<tr>
<td>ISR 1000 series</td>
<td>16.9 (1r)</td>
</tr>
<tr>
<td>ISR 4000 series</td>
<td>16.7 (3r)</td>
</tr>
</tbody>
</table>

• The ISRv router is running the minimum required version of the CIMC and NFVIS software, as shown in the following table:

<table>
<thead>
<tr>
<th>Hardware Platform</th>
<th>CIMC</th>
<th>NFVIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISRv</td>
<td>3.24</td>
<td>3.8.1</td>
</tr>
</tbody>
</table>
Download Cisco IOS XE SD-WAN Software for Cisco IOS XE SD-WAN Release 16.12 and Earlier

Download the Cisco IOS XE SD-WAN Software
To download the Cisco IOS XE SD-WAN software from the Cisco site:

2. Click Support & Downloads from the menu on the left side.
3. In the Products and Downloads page, in the Downloads search box, choose Software-Defined WAN (SD-WAN).
4. In the Select a Product page, from the right-most pane, choose XE SD-WAN Routers.
5. From the right-most pane, select your router model.
6. Click the desired software release version to download it. The software image name has the format router-model-ucmk9.release-number
7. Copy the software image to an HTTP or FTP file server in your local network.

Install the Cisco IOS XE SD-WAN Software for Cisco IOS XE SD-WAN Release 16.12 and Earlier
All new Cisco IOS XE SD-WAN devices ship with the Cisco IOS XE SD-WAN software already installed. If you have an existing Cisco IOS XE SD-WAN device, follow these steps to install the Cisco IOS XE SD-WAN software. The router reboots with the Cisco IOS XE SD-WAN image.

1. Download the Cisco IOS XE SD-WAN software image from the Cisco site.
2. Upload the Cisco IOS XE SD-WAN software image from the file server to the bootflash of the device. Sample syntax for FTP is given below:

```
Device# (config)# ip ftp source-interface interface
Device# copyftp:// username:password@server-IP/file-location bootflash:
```

TFTP:
```
Device(config)# ip tftp source-interface interface
Device(config)# ip tftp blocksize 8192
Device(config)#exit
Device#copy tftp: bootflash:
```

SCP (assumes SSH is enabled):
```
Device# configure terminal
Device# (config)# ip scp server enable
FileServer$ scp filenameusername@router-IP:/filename
```
3. Ensure that the device is connected to a management console.
4. Create a backup of the current configuration that can be saved in the bootflash of the device.
```
Device# copy run bootflash:original-xe-config
```
5. Remove all existing boot statements and save the configuration.
```
ISR4K# (config)# no boot system ...
ISR4K# wr mem
```
6. Verify that the BOOT variable is blank in the following output.

   ISR4K# show bootvar
   BOOT variable = 
   CONFIG_FILE variable does not exist
   BOOTLDR variable does not exist
   Configuration register is 0x2102
   Standby not ready to show bootvar

7. Add a boot variable that points to the Cisco IOS XE SD-WAN image.

   Device(config)# boot system flash bootflash:
   SDWAN-image
   Device(config)# exit
   ISR4K# write memory

8. Verify that the BOOT variable points to the Cisco IOS XE SD-WAN image.

   Device# show bootvar
   BOOT variable = bootflash:isr4300-ucmk9.16.10.1a.SPA.bin,1;
   CONFIG_FILE variable does not exist
   BOOTLDR variable does not exist
   Configuration register is 0x2102
   Standby not ready to show bootvar

9. Remove all existing configurations from the router.

   Device# write erase

10. Set the config-register to 0x2102.

    Device# configure terminal
    Device(config)# config-register 0x2102
    Device(config)# end

11. Verify that the config-register is set to 0x2102 or that it will be set to 0x2102 at the next reboot.

    Device# show bootvar

12. Reboot the router.

    ISR4K# reload
    Proceed with reload? [confirm] Yes
    If prompted to save the configuration, enter No. The router reboots with the XE SD-WAN image.

13. If prompted to enter the initial configuration dialog, enter No.

    --- System Configuration Dialog ---
    Would you like to enter the initial configuration dialog? [Yes/No]: No

14. If prompted to terminate auto-install, enter Yes.

    Would you like to terminate auto-install? [Yes/No]: Yes

15. At the login prompt, log in with the default username and password as admin.

    The default password can be used once and then must be changed. If the initial configuration session times out or if the session is interrupted or terminated before the password is changed and saved, subsequent login attempts fail. To restore login access to the device, you must reset the password to its default value through the local console in ROMMON mode. Then the initial provision process must be restarted. For information about restoring the password, see Recover the Default Password, on page 53.

16. Stop PnP and allow the Cisco IOS XE SD-WAN packages to install:
ISR4K# pnpa service discovery stop

17. Configure the upgrade on Cisco IOS XE SD-WAN device using `request platform software sdwan software upgrade-confirm`.

Router# request platform software sdwan software upgrade-confirm
Router#
*Sep 21 00:26:29.242: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install commit PACKAGE
*Sep 21 00:26:30.153: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed install commit PACKAGE
Router#

18. Ensure output of `show sdwan software` shows CONFIRMED state as user and no other value.

Router# sh sdwan software
VERSION ACTIVE DEFAULT PREVIOUS CONFIRMED TIMESTAMP
-----------------------------------------------
16.12.1b.0.4 true true true user 2019-09-21T00:24:22-00:00
Total Space: 388M Used Space: 86M Available Space: 298M

19. Configure the Cisco IOS XE SD-WAN device using `request platform software sdwan software reset`.

Router# request platform software sdwan software reset
*Sep 21 00:27:20.025: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install activate bootflash:isr4300-ucmk9.16.12.1b.SPA.bin
*Sep 21 00:27:43.105: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
*Sep 21 00:28:47.233: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed install activate PACKAGESep 21 00:28:54.240: %PMAN-5-EXITACTION: R0/0: pvp: Process manager

Once you have installed this image, remember to use the command `config-transaction` to open CLI configuration mode. The `config terminal` command is not supported on SD-WAN routers.

Note

Downgrading to fresh install of old image versions is not supported. You can only downgrade to a previous existing version of old image. For example, if you have never installed Cisco IOS XE SD-WAN 16.10.3 on your Cisco IOS XE SD-WAN device, and if you try to downgrade from Cisco IOS XE SD-WAN 16.11.1 release to Cisco IOS XE SD-WAN 16.10.3 release then this operation is unsupported and results in unpredictable behavior. However, if you had a 16.10.3 image installed previously, then you could reactivate it by using the `request platform software sdwan activate` command.

---

Configure IOS XE Router Using CLI

If your Cisco IOS XE SD-WAN device is connected to a DHCP server, PnP runs automatically and Cisco vManage automatically configures the device after the control connections are up. To verify that the control connections are up and the device is validated, enter the following command at the system prompt:

Device# show sdwan control connections
If your IOS Ex router is connected to a DHCP server and you are not using PnP, or if your IOSXE router is not connected to a DHCP server on the WAN, configure the router manually using the CLI as shown in the following steps.

You also can configure the hostname by using the `system host-name hostname` command. Configuring the hostname is optional, but it is recommended because this name is included as part of the prompt in the CLI and it is used on various Cisco vManage screens to refer to the device. This command is not available on the device CLI but it is available when using the CLI device template.

1. Connect to the router using a management console.
2. Stop PnP to allow access to the CLI:
   ```
   Device# pnpa service discovery stop
   ```
3. Enter configuration mode:
   ```
   Device# config-transaction
   Device(config)#
   ```
4. Configure the system IP address.
   ```
   Device(config-system)# system-ip ip-address
   ```
   Cisco vManage uses the system IP address to identify the device so that the NMS can download the full configuration to the device.
5. Configure the numeric identifier of the site where the device is located:
   ```
   Device(config-system)# site-id site-id
   ```
6. Configure the IP address of the Cisco vBond Orchestrator or a DNS name that points to the Cisco vBond Orchestrator. The Cisco vBond Orchestrator’s IP address must be a public IP address, to allow the router to reach the Cisco vBond Orchestrator.
   ```
   Device(config-system)# vbond (dns-name | ip-address)
   ```
7. Configure the organization name, which is the name that is included in the certificates on all devices in the overlay network. This name must be the same on all devices.
   ```
   Device(config-system)# organization-name name
   ```
8. Configure the tunnel interface to use for overlay connectivity. Ensure that the tunnel interface ID does not conflict with any other interface IDs that may be auto-assigned by Cisco vManage. You can verify this in configuration preview.
   ```
   Device(config)# interface Tunnel #
   Device(config-if)# ip unnumbered wan-physical-interface
   Device(config-if)# tunnel source wan-physical-interface
   Device(config-if)# tunnel mode sdwan
   ```

**Note**

- If you are using Cisco vManage feature templates for your configuration, a tunnel interface is automatically assigned based on the WAN interface used.
- If you switch to Cisco vManage mode from CLI mode, the tunnel interface you configured may change because Cisco vManage automatically assigns a tunnel interface number based on the WAN interface used. This change in tunnel number can cause the tunnel to go down before it comes up again when the configuration is pushed.
9. If the router is not connected to a DHCP server, configure the IP address of the WAN interface:

```plaintext
Device(config)# interface GigabitEthernet #
Device(config)# ip address ip-address mask
Device(config)# no shut
Device(config)# exit
```

10. Configure tunnel parameters:

```plaintext
Device(config)# sdwan
Device(config-sdwan)# interface WAN-interface-name
Device(config-interface-name)# tunnel-interface
Device(config-tunnel-interface)# color color/path-name
Device(config-tunnel-interface)# encapsulation ipsec
```

11. If an IP address is manually configured on the router, configure a default route:

```plaintext
Device(config)# ip route 0.0.0.0 0.0.0.0 next-hop-ip-address
```

12. If the Cisco vBond Orchestrator address was defined as a hostname, configure DNS:

```plaintext
Device(config)# ip domain lookup
Device(config)# ip name-server dns-server-ip-address
```

13. Save the changes and exit configuration mode:

```plaintext
Device(config)# commit and-quit
Device# exit
```

14. If you are using a certificate signed by your enterprise root CA, install the certificate:

```plaintext
Device# request platform software sdwan root-cert-chain install bootflash: certificate
```

15. Verify that the control connections are up and the router is validated.

```plaintext
Device# show sdwan control connections
```

<table>
<thead>
<tr>
<th>PEER</th>
<th>PEER</th>
<th>PEER</th>
<th>SITE</th>
<th>DOMAIN</th>
<th>PEER</th>
<th>PEER</th>
<th>PEER</th>
<th>PEER</th>
<th>PEER</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsmart</td>
<td>dtls</td>
<td>192.168.1.2</td>
<td>10</td>
<td>1</td>
<td>172.1.1.3</td>
<td>12346</td>
<td>172.1.1.3</td>
<td>12346</td>
<td></td>
</tr>
<tr>
<td>biz-internet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vbond</td>
<td>dtls</td>
<td>192.168.1.1</td>
<td>10</td>
<td>0</td>
<td>172.1.1.4</td>
<td>12346</td>
<td>172.1.1.4</td>
<td>12346</td>
<td></td>
</tr>
<tr>
<td>biz-internet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vmanage</td>
<td>dtls</td>
<td>192.168.1.1</td>
<td>10</td>
<td>0</td>
<td>172.1.1.2</td>
<td>12346</td>
<td>172.1.1.2</td>
<td>12346</td>
<td></td>
</tr>
<tr>
<td>biz-internet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CONTROLLER</th>
<th>GROUP</th>
<th>PROXY</th>
<th>STATE</th>
<th>UPTIME</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>up</td>
<td></td>
<td>1:19:51:40</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>up</td>
<td></td>
<td>1:19:51:45</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>up</td>
<td></td>
<td>1:19:51:38</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

You can now configure SD-WAN features on the router using Cisco vManage templates.
Add IOS XE Devices to the Plug and Play Portal

Table 5: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On Premises ZTP Server for Cisco SD-WAN</td>
<td></td>
<td>This feature extends the on-premise Plug and Play implementation support to Cisco IOS XE SD-WAN routers.</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 17.3.1a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco vManage Release 20.3.1</td>
<td></td>
</tr>
</tbody>
</table>

To add a device to the Plug and Play portal:

- If the device can reach the PNP portal, see Cisco Plug and Play Support Guide for Cisco SD-WAN Products.
- If the device does not have access to the PNP portal, see Start the Enterprise ZTP Server and Prepare Routers for ZTP sections in the Cisco SD-WAN Overlay Bring-up chapter.

Note

When devices are due for Return Materials Authorization (RMA), the device details are with Cisco PNP. However, you cannot delete these devices from the RMA list in Cisco vManage. Instead Cisco vManage administrator can mark the devices returned as invalidated as per RMA.

For information regarding Cisco IOS XE Release 17.2 and later, see Install and Upgrade Cisco IOS XE Release 17.2.1r and Later.

Upgrading or Downgrading ROMMON

This section describes how to upgrade or downgrade the ROM monitor (ROMmon) version that is running on a device. Perform this procedure if you need to change a ROMmon version to a required version that is shown in the “Before You Begin” section.

To determine the ROMmon version that is running on a device, enter the following command:

```
Device# show rom-monitor R0
```

To upgrade or downgrade ROMmon, follow these steps:

1. Take either of these actions:
   a. Load the ROMmon file into the device bootflash using a method such as SCP, FTP, TFTP, or a USB drive.
   b. If you do not have out-of-band management access to the router, transfer the ROMmon file by using Cisco vManage CLI, as shown in the following example:
      ```
vManage# request execute vpn 0 scp -P 830 C1100-rommon-16-1r-SPA.pkg admin@router-ip-address:/bootflash/vmanage-admin/C1100-rommon-169-1r-SPA.pkg
```

2. Take either of these actions to verify that the ROMmon file that you loaded or transferred appears in the directory output:
   a. If you loaded the ROMmon file into the device bootflash, enter the following command:
      ```
      Device# dir bootflash
      ```
Perform Factory Reset

This section describes the Factory Reset feature and how it can be used to protect or restore a router to an earlier fully functional state. For information on factory reset procedures on different platforms, see:

- Cisco ASR 1000 Series Aggregation Services Routers
- Cisco 4000 Series Integrated Services Routers
- Cisco Cloud Services Router 1000V Series

To perform factory-reset on a Cisco IOS XE SD-WAN ASR 1000 router, ensure that the router is booted in subpackages mode. Execute `show version` command and check the output for `system image file` to determine the booted image.

```
Device# show version
Cisco IOS XE Software, Version BLD_POLARIS_DEV_LATEST_20200303_002119_V17_X_X
Cisco IOS Software [Amsterdam], ASR1000 Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Copyright (c) 1986-2020 by Cisco Systems, Inc.
Compiled Tue 03-Mar-20 00:29 by mcpre
```

Note

To transfer the ROMmon file by using the Cisco vManage CLI, enter the following command:

```
vManage# dir bootflash:vmanage-admin
```

3. Enter the following command to set config-register to 0x2102:

```
Device# config-register 0x2102
```

4. Upgrade (or downgrade) the ROMmon file on your device by using the upgrade command as shown in the following examples:

```
• Example upgrade command if you loaded the ROMmon file into the device bootflash:

  Device# upgrade rom-monitor filename bootflash: C1100-rommon-169-1r-SPA.pkg R0

• Example upgrade command if you transferred the ROMmon file by using Cisco vManage CLI:

  vManage# upgrade rom-monitor filename
  bootflash:vmanage-admin/C1100-rommon-169-1r-SPA.pkg R0
```

5. After a series of messages pertaining to the upgrade display and the router prompt displays, enter the following command to reload the router:

```
Device# Reload
```

6. Enter the following command and verify that the output shows the new ROMmon version:

```
ISR4K# Show rom-monitor R0
```
Recover the Default Password

The default password for a Cisco IOS XE SD-WAN device is admin. After using this password for the first time, the administrator must create a new password. If the initial configuration session times out or if the session is interrupted or terminated before a new password is created, subsequent login attempts fail. In this situation, you must recover the default password.

To recover the default password for a device, follow these steps:

1. Power the device down and then back up.
2. In the local console of the device, enter ROMMON mode.
3. Enter the following command to set the config-register value to 0x8000:
   
   ```
   rommon 1 > confreg 0x8000
   ```
4. Power the device down and then back up so that your update takes effect.
5. Log in to the device with the user name and the password as admin.
6. In the local console of the device, enter SD-WAN config mode.
7. Enter the following command to set the config-register value to 0x2102:
   
   ```
   Device# confreg 0x2102
   ```
8. In the local console of the device, enter privileged exec mode.
9. Take either of these actions:
   
   - For Cisco IOS XE SD-WAN 16.10 releases beginning with release 16.10.4 or for Cisco IOS XE SD-WAN 16.12 releases beginning with release 16.12.2:
     
     ```
     Device# request platform software sdwan config reset
     Device# reload
     ```
   
   - For Cisco IOS XE SD-WAN 16.10 releases earlier than release 16.10.4 or for Cisco IOS XE SD-WAN 16.12 releases earlier than 16.12.2:
     
     ```
     Device# request platform software sdwan software reset
     ```
10. After the device comes back up, configure a new admin password.
Software Installation and Upgrade for vEdge Routers

This article describes how to install software on all Cisco vEdge devices—Cisco vManage instances, Cisco vSmart Controllers, Cisco vBond Orchestrators, and vEdge routers—and how to upgrade the software on devices already running the Cisco SD-WAN software.

Software Image Signing

Cisco SD-WAN software images are digitally signed to ensure that the images are official Cisco SD-WAN images and to guarantee that the code has not been altered or corrupted since the image was created and signed. All standard Cisco SD-WAN software images are signed, while patch images are not. Standard software images are identified with three numeric fields (such as 16.1.0) and patch software images are identified with four numeric fields (such as 16.1.0.1).

Signed images include a revocation mechanism so that Cisco SD-WAN can revoke an image if it is found to be dangerous, either due to a bug or a security flaw. These revocation mechanisms protect from attacks if you attempt to install a previously signed image that has a known vulnerability.

After you have installed a signed image onto a Cisco SD-WAN device, you can no longer install an unsigned image onto the device.

Software image signing is available in Releases 16.1 and later.

Software Version Compatibility

You can upgrade the software version on the controller devices—Cisco vManage instances, Cisco vSmart Controllers, and Cisco vBond Orchestrators—without upgrading the vEdge routers to the same version. However, the software version running on the controller devices must be compatible with the version running on the vEdge routers.

For a list of compatible versions on Controllers and vEdge routers, see Release Notes.

Note

All controller devices of the same type must run the same software version. That is, all Cisco vManage instances must run the same software version, all Cisco vSmart Controllers must run the same software version, and all Cisco vBond Orchestrators must run the same version.

Install the Software

Before you begin, download the software from the Cisco SD-WAN Support site.

You install software on Cisco SD-WAN devices when you first bring up the overlay network and add those devices to the network:

- To install software on a Cisco vBond Orchestrator, see Create vBond VM Instance on ESXi or Create vBond VM Instance on KVM. During the process of creating the VM, you install the vBond.ova file.

- To install software on a vEdge Cloud router, see Create vEdge Cloud VM Instance on AWS, Create vEdge Cloud VM Instance on ESXi, or Create vEdge Cloud VM Instance on KVM. During the process of creating the VM, you install the vEdge Cloud.ova file.
• To install software on a Cisco vManage, see Create vManage VM Instance on ESXi or Create vManage VM Instance on KVM. During the process of creating the VM, you install vManage.ova file.

• To install software on a Cisco vSmart Controller, see Create vSmart VM Instance on ESXi or Create vSmart VM Instance on KVM. During the process of creating the VM, you install the vSmart.ova file.

• To install software on a hardware vEdge router, nothing is required. All vEdge hardware routers ship with the software already installed.

**Upgrade the Software**

From Cisco vManage, you can upgrade the software image running on a Cisco vEdge device in the overlay network and reboot it with the new software. You can do this for a single device or for multiple devices simultaneously.

To upgrade the software, you obtain the software images from Cisco SD-WAN, add the new software images to the repository located on either Cisco vManage or a remote server, and install the new software image on the device. The next reboot occurs immediately if you select the **Activate and Reboot** check box, or you can wait until the next regularly scheduled maintenance window. If an upgrade fails and the device does not come back up, Cisco vManage automatically reverts the device to the previously running software image.

Before you upgrade the software on Cisco vEdge devices, ensure that the devices are running the required software version.

---

**Note**

Cisco SD-WAN releases starting with Releases 18.4.5, 19.2.2, and 20.1.1 have a security lockout. When any of these software versions (or later) are installed and activated on a device, a 30-day timer is set for the removal of any old images that were previously installed on the device. After the timer expires, the old images are deleted. For example, if you install and activate Release 18.4.5, a 30-day timer starts on the previously installed Release 19.2.1 image, but not on Release 19.2.2. Similarly if you install and activate Release 19.2.2, a 30-day timer starts on the previously installed Release 18.4.4 image, but not on Release 18.4.5.

You can continue to activate an older image that is already installed, before the 30-day timer runs out. If the device restarts before the 30-day timer expires, the timer is reset.

See **Cisco SD-WAN Command Reference** guide for more information.

- **request software secure-boot set** - Makes the system immediately delete old images* without waiting the 30 days.

- **request software secure-boot status** - Displays the installed old images*.

- **request software secure-boot list** - Prints a list of all old images* that are installed.

*old images = before releases 18.4.5, 19.2.2, and 20.1.1

---

**Note**

Cisco vManage downgrade is not supported. Ensure that you take a snapshot of the VM prior to upgrading Cisco vManage. To rollback to an earlier Cisco vManage release, revert to the snapshot.

For additional information and caveats regarding software upgrades, see **Release Notes**.
Best Practices for Software Upgrades

- Upgrade the software from Cisco vManage rather than from the CLI.
- If you are upgrading the software image on a remote Cisco vManage, the overlay network must already be up and operational.
- If you are upgrading all devices in the overlay network, you must perform the upgrade in the following order:
  1. Upgrade Cisco vManage instances.
  2. Upgrade the Cisco vBond Orchestrators.
  3. Upgrade one-half of the Cisco vSmart Controllers.
  4. Have the upgraded Cisco vSmart Controllers run for at least one day (24 hours) to ensure that the Cisco vEdge devices and the overlay network are stable and running as expected.
  5. Upgrade the remainder of the Cisco vSmart Controllers.
  6. Upgrade 10 percent of the vEdge routers. For multirouter sites, it is recommended that you upgrade only one router per site.
  7. Have the upgraded vEdge routers run for at least one day (24 hours) to ensure that the Cisco SD-WAN devices and the overlay network are stable and running as expected.
  8. Upgrade the remainder of vEdge routers.

- If the new software images are located on an FTP server, ensure that the FTP server can handle concurrent file transfers.
- If the new software images are in the image repository on Cisco vManage, ensure that the WAN in which Cisco vManage is located has sufficient capacity for concurrent file transfers.
- You cannot include Cisco vManage in a group software upgrade operation. You must upgrade and reboot Cisco vManage server by itself.
- In a group software upgrade operation, you can upgrade up to 40 Cisco vEdge devices or Cisco IOS XE SD-WAN devices and reboot or activate up to 100 Cisco vEdge devices or Cisco IOS XE SD-WAN devices simultaneously (when the new image is available locally). These maximum numbers assume that Cisco vManage is idle and only upgrade and reboot operations are being carried out. In case of other management tasks occurring on Cisco vManage at the same time, the number of available sessions reduces.
- When you are setting a software image to be the default software image, activate it first, before making it the default image.

Obtain Software Images from Cisco SD-WAN

To upgrade the software running on the devices in the overlay network, you must first obtain the new software packages from the Cisco SD-WAN website. To do so, go to http://viptela.com/support/, log in to Cisco SD-WAN Support, and download the software packages for the new release. You can also download the software images to an FTP server in your network and, from Cisco vManage, point to the upgrade packages on the remote host.
For initial software installation, the software package names for Releases 16.1 and later have the following format, where `x.x.x` represents the Cisco SD-WAN software release version. These packages contain the virtual machines and the Cisco SD-WAN software.

- **vEdge Cloud router**
  - viptela-x.x.x-edge-genericx86-64.ova (for ESXi Hypervisor)
  - viptela-edge-genericx86-64.qcow2 (for KVM Hypervisor)

- **Cisco vBond Orchestrator**
  - viptela-edge-genericx86-64.ova (for ESXi Hypervisor)
  - viptela-edge-genericx86-64.qcow2 (for KVM Hypervisor)

- **Cisco vSmart Controller**
  - viptela-smart-genericx86-64.ova (for ESXi Hypervisor)
  - viptela-smart-genericx86-64.qcow2 (for KVM Hypervisor)

- **Cisco vManage**
  - viptela-vmanage-genericx86-64.ova (for ESXi Hypervisor)
  - viptela-vmanage-genericx86-64.qcow2 (for KVM Hypervisor)

The software upgrade package names for Releases 16.1 and later have the following format, where `x.x.x` represents the release version. The strings mips64 and x86_64 represent the underlying chip architecture.

- **vEdge router hardware**—viptela-x.x.x-mips64.tar.gz
- **Cisco vBond Orchestrator, vEdge Cloud router, and Cisco vSmart Controller**—viptela-x.x.x-x86_64.tar.gz
- **Cisco vManage**—vmanage-x.x.x-x86_64.tar.gz

For Releases 15.4 and earlier, the software upgrade packages are in files with the extension .tar.bz2, or in the case of the vEdge 100 router, .tar.gz. The package names have the following format, where `x.x.x` represents the release version. The strings mips64 and x86_64 represent the underlying chip architecture.

- **vEdge router**—viptela-x.x.x-mips64.tar.bz2
- **Cisco vBond Orchestrator and Cisco vSmart Controller**—viptela-x.x.x-x86_64.tar.bz2
- **Cisco vManage**—vmanage-x.x.x-x86_64.tar.bz2

### Add New Software Images to the Repository

Once you have downloaded the new software packages from the Cisco SD-WAN website, upload them into Cisco vManage repository. If you downloaded the software images to an FTP server, from Cisco vManage, point to the upgrade packages on the remote host.

1. In Cisco vManage, select the **Maintenance > Software Upgrade** screen.
2. Click the **Repository** button located on the right side of the title bar. The Software Repository screen opens.
3. Click Add New Software, and select the location from which to download the software image. The location can be:
   - Cisco vManage—To select an image stored on the local Cisco vManage.
   - Remote Server—To select an image stored on a remote file server.
   - Remote Server – Cisco vManage—To select an image stored on a remote Cisco vManage. This location is available in Releases 17.2 and later.

4. If you select Cisco vManage, the Upload Software to Cisco vManage dialog box opens.
   a. Click Choose File to select the software images for vEdge routers, Cisco vSmart Controllers, or Cisco vManage.
   b. Click Upload to add the images to Cisco vManage repository.

5. If you select Remote Server, the Location of Software on Remote Server dialog box opens.
   a. Enter the version number of the software image.
   b. Enter the URL of the FTP or HTTP server on which the images reside.
   c. Click OK to point to the software images on the remote host.

6. If you select Remote Server – Cisco vManage, the Upload Software to Cisco vManage dialog box opens.
   a. Enter the hostname of the Cisco vManage server.
   b. Click Choose File to select the software images for vEdge routers, Cisco vSmart Controllerss, or Cisco vManage.
   c. Click Upload to add the images to Cisco vManage repository.

The added software images are listed in Cisco vManage repository table and are available for installing on the devices. The table displays the name and type of image, when it was updated, and the URL.

To return to Device List view, click Device List.

**Upgrade the Software Image**

After the software images are present in Cisco vManage image repository, you can upload the software image on a device:

1. In Cisco vManage, select the Maintenance > Software Upgrade screen.
2. Click the check box to the left of each row to select one or more devices on which to upgrade the software image. To search for a device, use the Device Groups drop-down and/or the Search box located directly above the device table.
3. Click the Upgrade button located in the upper left corner of the screen. The Software Upgrade dialog box opens.
4. From the Version drop-down, select the version of the software image you want to install. Cisco vManage and Remote Server buttons are activated.
5. Select whether the software image is available on Cisco vManage or on the Remote Server.
6. If you select Remote Server in Step 5, choose the appropriate VPN for Cisco vSmart Controller/Cisco vManage and for vEdge, and continue with Step 8.

7. If you select Cisco vManage in Step 5, you can choose to automatically activate the new software image and reboot the device by selecting the **Activate and Reboot** check box. (Note that if you do not select the **Activate and Reboot** check box, the new software image is still installed but the device continues to use the existing software image. To activate the newly installed software image, see Activate a New Software Image below.)

8. Click **Upgrade**. A progress bar indicates the status of the software upgrade.

   If the upgrade does not complete successfully within 60 minutes, it times out.

   If the control connection to Cisco vManage does not come up within 15 minutes, Cisco vManage automatically reverts the device to the previously running software image.

---

**Activate a New Software Image**

If you select **Activate and Reboot** check box when uploading the software image, then when you click **Upgrade**, the new software activates automatically and the device reboots.

If you uploaded the software image from a Remote Server, or if you did not select **Activate and Reboot** check box when uploading the software image from Cisco vManage, the new image is installed on the device but the device continues to use the existing software image. To activate the new software image:

1. In Cisco vManage, select the **Maintenance > Software Upgrade** screen.

2. Click the check box to the left of each row to select one or more devices on which to activate the new software image. To search for a device, use the Device Groups drop-down and/or the Search box located directly above the device table.

3. Click the **Activate** button located in the upper left corner of the screen to activate the new software. The activation process reboots the device and upgrades it to the newly installed software.

   If the control connection between the device and Cisco vManage does not come up within 15 minutes, Cisco vManage automatically reverts the device to the previously running software image.

---

**View Log of Software Upgrade Activities**

To view the status of software upgrades on each device and a log of related activities:

1. Click the **Active Devices** toggle button. The top of the screen, directly below the title bar, displays the total number of upgrades performed along with the total number of successes and failures. The Software Upgrade table displays the status of each upgrade operation.

2. Click the right angle bracket to the left of each table row to see details of the operation. To close the details, click the down angle bracket.

---

**Upgrade a Software Image from the CLI**

If you need to upgrade a software image directly on a device, or if you are not using Cisco vManage in your network, to upgrade the software image, you can either repeat the installation process or you can install the software image from within the CLI.
To upgrade the software image from within the CLI:

1. Configure the time limit for confirming that a software upgrade is successful. The time can be from 1 through 60 minutes.

   Device# system upgrade-confirmminutes

2. Install the software:

   vEdge# request software install url /viptela-release -mips64.tar.bz2 [reboot] [vpn vpn-id]

   vSmart# request software install url/viptela-release -x86_64.tar.bz2 [reboot] [vpn vpn-id]

   Specify the image location in one of the following ways:
   - The image file is on the local server:
     /directory-path/
     You can use the CLI's autocompletion feature to complete the path and filename.
   - The image file is on an FTP server.
     ftp://hostname/
   - The image file is on an HTTP server.
     http://hostname/
   - The image file is on a TFTP server.
     tftp://hostname/

   Optionally, specify the VPN identifier in which the server is located.

   The reboot option activates the new software image and reboots the device after the installation completes.

3. If you did not include the reboot option in Step 2, activate the new software image and reboot the device:

   Viptela# request software activate

4. Confirm, within the configured upgrade confirmation time limit, that the software upgrade was successful:

   Viptela# request software upgrade-confirm

   If you do not issue this command within this time limit, the device automatically reverts to the previous software image.

---

Redundant Software Images

You can download and store multiple software images on a Cisco vEdge device.

To list the currently installed software version and to see which software image is currently running, use the following command:

Viptela# show software

<table>
<thead>
<tr>
<th>VERSION</th>
<th>ACTIVE</th>
<th>DEFAULT</th>
<th>PREVIOUS</th>
<th>CONFIRMED</th>
<th>TIMESTAMP</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.4.3</td>
<td>true</td>
<td>false</td>
<td>false</td>
<td>user</td>
<td>2016-02-04T03:45:13-00:00</td>
</tr>
<tr>
<td>15.4.2</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>user</td>
<td>2015-12-06T14:01:12-00:00</td>
</tr>
</tbody>
</table>
To upgrade the software to a specific version, use the following command:

```
Viptela# request software activate
```

---

**Downgrade a Cisco vEdge Device to an Older Software Image**

To downgrade a Cisco vEdge Device to a previous software image using CLI:

1. If necessary, remove an existing software image to provide space for loading a new software image.
   
   ```
   vEdge# request software remove previous-installed-build
   ```

2. Download the software image for the downgrade.

3. Install the downloaded image.
   
   ```
   vEdge# request software install desired-build
   ```

   We recommend copying the image to local storage before installing, but you can specify the image location in one of the following ways:
   
   - The image file is on the local server:
     
     `/directory-path/`
     
     You can use the CLI's autocompletion feature to complete the path and filename.
   
   - The image file is on an FTP server.
     
     `ftp://hostname/`
   
   - The image file is on an HTTP server.
     
     `http://hostname/`
   
   - The image file is on a TFTP server.
     
     `tftp://hostname/`

4. Set the installed image as the default.
   
   ```
   vEdge# request software set-default desired-build
   ```

5. Perform a reset. This resets the device, deleting any existing configuration. The device starts in day zero configuration.
   
   ```
   vEdge# request software reset
   ```
Install and Upgrade Cisco IOS XE Release 17.2.1r and Later

Table 6: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install and Upgrade</td>
<td>Cisco IOS XE Release 17.2.1r</td>
<td>This feature supports the use of a single &quot;universalk9&quot; image to deploy Cisco IOS XE SD-WAN and Cisco IOS XE functionality on all the supported devices. This universalk9 image supports two modes - Autonomous mode (for Cisco IOS XE features) and Controller mode (for Cisco SD-WAN features).</td>
</tr>
<tr>
<td>Cisco Catalyst 8000V Edge SoftwarePlatform</td>
<td>Cisco IOS XE Release 17.4.1a</td>
<td>Support added for the Cisco Catalyst 8000V Edge Software platform. Upgrading Cisco CSR1000V or Cisco ISRv platforms to Cisco IOS XE Release 17.4.1a includes upgrading to the platform type to the Cisco Catalyst 8000V.</td>
</tr>
</tbody>
</table>

Starting with Cisco IOS XE Release 17.2.1r, use the universalk9 image to deploy both Cisco IOS XE SD-WAN and Cisco IOS XE on Cisco IOS XE devices.

Starting Cisco IOS XE Release 17.2.1r, UCMK9 image is not available.

This release helps in seamless upgrades of both the SD-WAN and non SD-WAN features and deployments.

Access the Cisco IOS XE and Cisco IOS XE SD-WAN functionality through Autonomous and Controller execution modes, respectively. The Autonomous mode is the default mode for the routers and includes the Cisco IOS XE functionality. To access Cisco IOS XE SD-WAN functionality, switch to the Controller mode. You can use the existing Plug and Play Workflow to determine the mode of the device.

- Platforms Supported in Controller Mode, on page 64
Platforms Supported in Controller Mode

Platforms Supported on Controller Mode

- Cisco ASR 1000 Series Aggregation Services Routers
- Modular Cisco ASR 1006-X with ASR1000-RP3 module (Cisco IOS XE Release 17.5.1a or later, see Cisco ASR 1006-X with an RP3 Module.)
- Cisco ISR 1000 Series Integrated Services Routers
- Cisco ISR 4000 Series Integrated Services Routers
- Cisco 1101 Industrial Integrated Services Router
- Cisco CSR 1000v Series Cloud Services Routers
- Cisco Integrated Services Virtual Router (ISRv)
- Cisco Catalyst 8200 Series Edge Platforms
- Cisco Catalyst 8300 Series Edge Platforms
- Cisco Catalyst 8500 Series Edge Platforms
- Cisco Catalyst 8000V Edge Software (Cisco IOS XE Release 17.4.1a or later)

Platforms Not Supported in Controller Mode

Modular platforms based on the following ASR 1000 Series Routers are not supported in controller mode:

- ASR1000-RP2
Supported Crypto Modules for Controller Mode

The following crypto modules are required for the ASR 1000 series routers:

- ASR1001HX-IPSECHW, for the ASR 1001-HX
- ASR1002HX-IPSECHW, for the ASR 1002-HX

Cisco IOS XE Image Compatibility

<table>
<thead>
<tr>
<th>Deployment Image Version</th>
<th>SD-WAN</th>
<th>Non SD-WAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Releases 16.9.x, 16.10.x, 16.11.x, 16.12.x</td>
<td>ucmk9</td>
<td>universalk9</td>
</tr>
<tr>
<td>Cisco IOS XE Release 17.1.x</td>
<td>NA</td>
<td>universalk9</td>
</tr>
<tr>
<td>Cisco IOS XE Release 17.2.x and later</td>
<td>universalk9*</td>
<td>universalk9**</td>
</tr>
</tbody>
</table>

* For SD-WAN use case, non-LI and non-payload encryption image types are not supported.

** For non SD-WAN use case, non-LI and non-payload encryption image types are supported (universalk9_noli, universalk9_npe, universalk9_npe_noli).

Restrictions

Restrictions for single "universalk9" image

- Dual-IOSd is supported only in autonomous mode.
- Images without payload encryption and NO-LI (universalk9_npe, universalk9_noli, universalk9_npe_noli) images are not supported in controller mode. Only universalk9 images are supported.
- After onboarding and determining the mode of operation, changing from Controller mode to Autonomous mode or vice-versa, results in the loss of configuration.
- Reset button functionality is not supported in controller mode on Cisco ISR 1000 series Integrated Service Routers. The reset button does not function to restore a golden image or configuration in controller mode.
- Auto-install (Python and TCL scripts) and ZTP—Autoinstall and ZTP are not supported in controller mode. If DHCP discovers an attempt to install using either of these processes, a mode change to Autonomous mode is triggered.
- WebUI—In controller mode, WebUI is not supported and an error message is displayed, if used.
Introducing Autonomous and Controller Mode

The Cisco IOS XE Release 17.2.1r release introduces two installation modes – Autonomous and Controller modes. The autonomous mode supports the functionality of Cisco IOS XE non SD-WAN deployment and the controller mode supports the Cisco SD-WAN solution.

The following are the main differences between Autonomous mode and Controller mode:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Autonomous Mode</th>
<th>Controller Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Method</td>
<td>• Command Line Interface (CLI)</td>
<td>YANG-based configuration</td>
</tr>
<tr>
<td></td>
<td>• NETCONF</td>
<td>• Cisco vManage</td>
</tr>
<tr>
<td></td>
<td>• NETCONF</td>
<td>• NETCONF</td>
</tr>
<tr>
<td>Onboarding Modes</td>
<td>• Plug and Play</td>
<td>• Plug and Play</td>
</tr>
<tr>
<td></td>
<td>• Config-Wizard</td>
<td>• Bootstrap (USB, bootflash, and so on)</td>
</tr>
<tr>
<td></td>
<td>• WebUI</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Bootstrap (USB, bootflash, and so on)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Auto-Install (Python Script, TCL Script)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ZTP (Using DHCP Option 150 and Option 67)</td>
<td></td>
</tr>
<tr>
<td>Licensing</td>
<td>Cisco Smart Licensing</td>
<td>Cisco High Performance Security (HSEC) software licensing. No device licensing.</td>
</tr>
<tr>
<td>Image Type</td>
<td>Universalk9</td>
<td>Universalk9</td>
</tr>
<tr>
<td>Dual-IOSd redundancy model</td>
<td>Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>High Availability</td>
<td>Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Global configuration mode</td>
<td>configure terminal</td>
<td>config-transaction</td>
</tr>
</tbody>
</table>

Software Installation for Cisco IOS XE Routers

Download the Software for Cisco IOS XE Release 17.2.1r or Later

Download the `router-model-universalk9.release-number` image for Cisco IOS XE Release 17.2.1r or later software from the Cisco site [https://software.cisco.com](https://software.cisco.com).
Install Software on Cisco AR, Cisco ISR and Cisco ENCS Platforms

Refer to the following documents for installation instructions:

- Cisco ISR 1000 Series Integrated Services Router
- Cisco ISR 4000 Series Integrated Services Routers
- Cisco ASR 1000 Series Aggregation Services Routers
- Installing Cisco Enterprise NFVIS on Cisco ENCS 5100 and ENCS 5400

Install Software on Cisco CSR 1000v Platform

Based on the cloud in which you are deploying the CSR 1000v instance, see the following to perform the bootstrap and/or the day 0 configuration:

- Deploying the OVA to the VM
- Manually creating the Cisco CSR 1000v VM using the .iso file (Citrix XenServer)
- Creating a CSR 1000v VM using the self installing .run package
- Manually creating the VM using the .iso file (Microsoft Hyper-V)
- Booting the CSR 1000v Instance
- Deploying a CSR 1000v VM Using Custom Data
- Deploying a CSR 1000v VM on Microsoft Azure

Install a Cisco Catalyst 8000V Edge Software Platform

Beginning with Cisco IOS XE Release 17.4.1a, the Cisco Catalyst 8000V is a newly supported virtual router platform replacing the Cisco CSR1000V and Cisco ISRV. Installing the Cisco Catalyst 8000V in an Cisco SD-WAN environment requires Cisco vManage Release 20.4.1 or later.

When downloading the Cisco IOS XE Release 17.4.1a software image, note that there are no images for the Cisco CSR1000V or Cisco ISRV. Download the image for the Cisco Catalyst 8000V and have it ready to upload to the Cisco vManage software image repository. The file name begins with: c8000v-universalk9

Refer to the following document for complete information about the platform: Cisco Catalyst 8000V Edge Software Installation and Configuration Guide

Clean Install

We recommend a clean install of the Cisco Catalyst 8000V. This ensures support for all features, provides the most up-to-date licensing, and ensures that devices and the controller stay synchronized. For cases where upgrade is necessary, see the procedure in Upgrade to Cisco IOS XE Release 17.2.1r or Later.

Note

After a clean install of the Cisco Catalyst 8000V, it is not possible to downgrade the device to a release earlier than Cisco IOS XE Release 17.4.1a.

Upgrading
Upgrading a Cisco CSR1000V or Cisco ISRv virtual router to Cisco IOS XE Release 17.4.1a includes upgrading to the Cisco Catalyst 8000V. Note the following:

- The Cisco Catalyst 8000V preserves all of the functionality available on Cisco CSR1000V or Cisco ISRv platforms.
- Performing the upgrade in Cisco vManage preserves the configuration of the device(s) being upgraded.

Plug and Play in Cisco IOS XE Release 17.2.1r and Later Releases

Plug and Play Onboarding Workflow

1. Place an order for the device in Cisco Commerce with Smart Account and Virtual Account details of the customer.

2. The device information from Cisco Commerce like Device serial number, Smart Account, and Virtual Account are added to the Plug and Play portal.

3. Add a vBond controller profile into the Plug and Play (PnP) portal for the same Smart Account and Virtual Accounts.

4. Associate the new device to the vBond controller profile manually.

5. PnP sends all relevant information including vBond details, device serial number, organization name, and network ID to Zero Touch Provisioning (ZTP).

6. Download the device serial number file (provisioning file) from PnP and upload it to Cisco vManage. The devices are now available on Cisco vManage. You can also use the Sync Smart Account option on vManage to sync the device with your virtual account and populate the device in Cisco vManage.

Note

For more information, refer to the Plug and Play Support Guide.

Mode Discovery with Plug and Play Onboarding

The PnP-based discovery process determines the mode in which the device operates, based on the controller discovery and initiates a mode change, if required. The mode change results in a reboot of the device. Once reboot is complete, the device performs appropriate discovery process.

When you upgrade to Cisco IOS XE Release 17.2.1r or later, on a Cisco device that already runs a Cisco IOS XE or Cisco SD-WAN image, the device starts in autonomous mode or controller mode depending on the configured controller.

Plug and Play (PnP) deployment include the following discovery process scenarios:
Table 8:

<table>
<thead>
<tr>
<th>Boot up Mode</th>
<th>Deployment Mode</th>
<th>On-boarding agent</th>
<th>vBond Orchestrator</th>
<th>Discovery Process</th>
<th>Mode Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autonomous</td>
<td>Cisco Digital Network Architecture (DNA)</td>
<td>Plug and Play</td>
<td>No</td>
<td>Plug and Play Connect Discovery or on-premise plug and play server discovery</td>
<td>No Mode change</td>
</tr>
<tr>
<td>Autonomous</td>
<td>Cisco vManage</td>
<td>Plug and Play</td>
<td>Yes</td>
<td>Plug and Play Connect Discovery</td>
<td>Mode change to controller mode</td>
</tr>
<tr>
<td>Controller</td>
<td>Cisco DNA</td>
<td>Plug and Play</td>
<td>No</td>
<td>Plug and Play Connect Discovery or on-premise plug and play server discovery</td>
<td>Mode change to autonomous mode</td>
</tr>
<tr>
<td>Controller</td>
<td>Cisco vManage</td>
<td>Plug and Play</td>
<td>Yes</td>
<td>Plug and Play Connect Discovery</td>
<td>No mode change</td>
</tr>
</tbody>
</table>

Non-PnP Onboarding

Creating a Cisco SD-WAN Bootstrap Configuration File

See On-Site Bootstrap Process for Cisco SD-WAN Devices and Generate a Bootstrap File For Cisco IOS XE SD-WAN Devices Using the CLI for information about generating a bootstrap file.

New Installation: Mode Change Device Day Zero Scenario

1. If the device is running a pre-17.2 universalalk9 image on a new box, or for an existing box where you performed `write erase` and `reload` and loaded a Cisco IOS XE 17.2 or newer image, the device boots in day zero configuration and in autonomous mode.

2. The new device determines if a mode change is required based on the bootstrap file.
   - If `ciscosdwan.cfg` or `ciscosdwan_cloud_init.cfg` bootstrap file in a plugged in the bootstrap location, mode change to controller mode is initiated. After the device boots up in controller mode, the configuration present in the configuration file is applied.
   - If a `ciscorctr.cfg` bootstrap file or config-wizard is discovered, mode change is not initiated and the boot up continues in the Autonomous mode.
Switch Modes Using Cisco CLI

Use the controller-mode command in Privileged EXEC mode to switch between controller and autonomous modes.

The **controller-mode disable** command switches the device to autonomous mode.

```
Device# controller-mode disable
```

The **controller-mode enable** command switches the device to controller mode.

```
Device# controller-mode enable
```

Note
------------------------
- If device is booted with bundle mode (Super packages), after reboot, the image gets automatically expanded and activated to prepare the router for SDWAN operation. Devices with 4GB RAM may require an additional reboot to free up space in /bootflash. The following devices with 4GB RAM need reload:
  - Cisco ISR 4451
  - Cisco ISR 4431
  - Cisco ISR 4461
  - Cisco ISR 4351
  - Cisco ISR 4331
  - Cisco ISR 4321

Mode Discovery and Mode Change

On a device that already runs a Cisco IOS XE non SD-WAN image, after upgrading to a Cisco IOS XE Release 17.2.1r or later image, the device boots up in autonomous mode.

Note
------------------------
- If there is a previous SD-WAN configuration file present on the device, the device boots in controller mode. Before performing an upgrade, ensure that you remove any stale SD-WAN configuration files from bootflash.

On a device that already runs a Cisco IOS XE SD-WAN image, after upgrading to a Cisco IOS XE Release 17.2.1r or later image, the device boots up in controller mode.

Use the **controller-mode enable** command to switch from autonomous to controller mode and the **controller-mode disable** command to switch from controller mode to autonomous mode.
To switch modes using CLI, ensure that the appropriate configuration files mentioned in the table below are present. After the device boots up, the configuration present in the configuration file is applied. The device reads the configuration file and uses the configuration information to come up on the network.

**Table 9: Configuration File Prerequisites for Mode Change**

<table>
<thead>
<tr>
<th>Current Mode</th>
<th>Mode change to</th>
<th>Platforms</th>
<th>Configuration file and location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller</td>
<td>Autonomous</td>
<td>All supported platforms</td>
<td>ciscort.cfg in any file system available to the device</td>
</tr>
</tbody>
</table>
| Autonomous   | Controller     | • Cisco Cloud Services Router, CSR1000v  
                |                                 | • Cisco Integrated Services Virtual Router, ISRv  
                |                                 | • Cisco Catalyst 8000V  
                |                                 | • Cisco ASR1002-X |

On a Cisco CSR1000v device (for Cisco IOS XE Release 17.2 or later) and a Cisco Catalyst 8000V (for Cisco IOS XE Release 17.4 or later) image deployment, if you want to boot up the device in controller mode, load the bootstrap file generated by Cisco vManage by bootstrap (ESXi and KVM) or user-data (AWS) or custom-data (Azure and GCP).

The following fields must be present in the ciscosdwan_cloud_init.cfg bootstrap file:

- `otp`
- `uuid`
- `vbond`
- `org`

When the device mode is switched from autonomous to controller, the startup configuration and the information in NVRAM (certificates), are erased. This action is equivalent to running the `write erase` command.
Controller Mode Configuration Reset

If you use `request platform software sdwan config reset` or `request platform software sdwan software reset` commands to bring the device back to controller-mode day-zero configuration, the device performs one of the following actions:

- Performs mode discovery. See *Mode Discovery with Plug and Play Onboarding, on page 68.*
- Uses the appropriate configuration file to perform bootstrap. See *Creating a Cisco SD-WAN Bootstrap Configuration File, on page 69.*

To erase the SD-WAN configuration of the current active image, use the following CLI:

```
Device# request platform software sdwan config reset
%WARNING: Bootstrap file doesn't exist and absence of it can cause loss of connectivity to the controller.
For saving bootstrap config, use:
request platform software sdwan bootstrap-config save
Proceed to reset anyway? [confirm]  
Backup of running config is saved under /bootflash/sdwan/backup.cfg
WARNING: Reload is required for config-reset to become effective.
```

The warning listed in the above configuration is visible only on Cisco IOS XE Release 17.3.1a and later images.

For the changes to take effect, you must reload the router after running the CLI. Running this CLI ensures the configuration for the currently installed version is wiped along with crypto keys and the device enters the day zero workflow after the reload.

If the device is not set up to use PnP for onboarding, then it reads the configuration file in the bootflash and uses the configuration information to come up on the network. If the device is setup to use PnP onboarding, then after reload, the PnP discovery will start again.

In the case of public clouds, just like a fresh install, additional bootstrap configuration is provisioned that allows you to login to the instance.
In public cloud and NFVIS environments, ensure that a latest day-zero bootstrap configuration file (exported from Cisco vManage) is available in a supported location and following standard file naming conventions (example: bootflash:ciscosdwan_cloud_init.cfg file), before the configuration reset operation is performed.

**Note**
Failure to follow save the bootstrap file in these environments cause loss of virtual machine connectivity.

**Mode Switching: Additional Information**

**Configuration Persistence During Mode Switch**

<table>
<thead>
<tr>
<th>Current Configuration Mode</th>
<th>Mode Switched to</th>
<th>Behavior</th>
</tr>
</thead>
</table>
| Autonomous                 | Controller      | Contents of NVRAM and the startup configuration are erased. Configuration is not be restored. Device is reverted to Day zero configuration. Previous running configuration is stored in bootflash.  
**Note**  When you switch from autonomous mode to controller mode, and switch back to autonomous mode, the Cisco IOS XE configuration is not restored because the startup configuration is empty. You have to manually restore configuration from the backup. |
| Controller                 | Autonomous      | CDB contents are erased (for subsequent mode switches) and Cisco IOS configuration are not restored (as startup configuration is empty). You have to manually restore configuration from the backup. |

**Verify Controller and Autonomous Modes**

**Show Command Output for Controller Mode**

```
Device# show logging | inc OPMODE_LOG  
*Dec 8 16:01:17.339: %BOOT-5-OPMODE_LOG: R0/0: bins: System booted in CONTROLLER mode

Device# show version | inc operating  
Router operating mode: Controller-Managed
```
Device# `show platform software device-mode`
Operating device-mode: Controller

Device-mode bootup status:
-------------------------------------
Success

Device# `show platform software chasfs r0 brief | inc device_managed_mode`
/tmp/chassis/local/rp/chasfs/etc/device_managed_mode : [controller]
/tmp/fp/chasfs/etc/device_managed_mode : [controller]

Device# `show version | inc Last reload`
Last reload reason: Enabling controller-mode

---

Show Command Output for Autonomous Mode

Device# `show logging | include OPMODE_LOG`
*Dec 8 17:01:17.339: %BOOT-5-OPMODE_LOG: R0/0: binos: System booted in AUTONOMOUS mode

Device# `show version | inc operating`
Router operating mode: Autonomous

Device# `show platform software device-mode`
Operating device-mode: Autonomous

Device-mode bootup status:
-------------------------------------

Device# `show platform software chasfs r0 brief | inc device_managed_mode`
/tmp/chassis/local/rp/chasfs/etc/device_managed_mode : [autonomous]
/tmp/fp/chasfs/etc/device_managed_mode : [autonomous]

Device# `show version | inc Last reload`
Last reload reason: Enabling autonomous-mode

---

Note
If the device is in controller mode, the `show sdwan running-config` command does not display the following information:

- All service commands under `/native/service` except `tcp-small-servers`, `udp-small-servers`, `tcp-keepalives-in`, and `tcp-keepalives-out`
- Configurations under line VTY except for transport, access-class, and ipv6 access-class
- IPv6 unicast routing configuration
- Commands in `/native/enable`

To verify these configuration use the `show running-config` command.
Change the Console Port Access After Installation, in Controller Mode

Before You Begin
Before beginning this procedure, ensure that you have access to the Cisco CSR1000V or Cisco Catalyst 8000V router through the currently configured console access method.

Change the Console Port Access
This procedure changes the method for connecting to the console to access a Cisco CSR1000V or Cisco Catalyst 8000V software device.

The image used for deploying the Cisco CSR1000V or Cisco Catalyst 8000V software determines the default type of console access to use, which can be virtual or serial.

The procedure includes changing the mode from controller to autonomous, and then back to controller, which is required for operation with Cisco SD-WAN. These mode changes cause the device to reload.

Perform the following steps to change the console port access.

1. In EXEC mode, enter `enable` to enter privileged EXEC mode.

   `Router> enable`

2. Disable controller mode. Enter the following command and follow the prompts to complete the command.

   `Device# controller-mode disable`

   **Note**
   This reboots the device in autonomous mode.

3. After the device restarts, enter `enable` to enter privileged EXEC mode.

   `Router> enable`

4. Enter global configuration mode.

   `Device# configure terminal`

5. Use one of the following options to configure the type of access:

   - **virtual**: This option specifies that the device is accessed through the hypervisor virtual VGA console.

     `Device(config)# platform console virtual`

   - **serial**: This option specifies that the device is accessed through the serial port on the virtual machine (VM).

     `Device(config)# platform console serial`

     **Note**
     Use this option only if your hypervisor supports serial port console access.
• auto: (This option has been deprecated and is not recommended.) This option specifies that the device console is detected automatically. This is the default setting during the initial installation boot process. For additional information, see Booting the Cisco CSR 1000v as the VM.

6. Exit configuration mode.
   Device(config)# end

7. Save the configuration.
   Device# write memory

8. Copy the running configuration to the startup configuration.
   Device# copy system:running-config nvram:startup-config

9. Change the device back to controller mode. Enter the following command and follow the prompts to complete the command.
   Device# controller-mode enable

---

**Note**
This step reboots the device in controller mode.

---

## Upgrade to Cisco IOS XE Release 17.2.1r or Later

### Supported Upgrades

**Table 11: Cisco CSR1000V and Cisco ISRv Routers**

<table>
<thead>
<tr>
<th>You Can Upgrade to...</th>
<th>From these Releases</th>
</tr>
</thead>
</table>
| Cisco IOS XE Release 17.4.1a | Cisco IOS XE SD-WAN 17.3.1a or later  
Cisco IOS XE SD-WAN 17.2.2 or later  
Cisco IOS XE SD-WAN 16.12.4a or later  |

**Note**

- To upgrade a Cisco CSR1000V or Cisco ISRv router to Cisco IOS XE Release 17.4.1a from a release not listed here requires first upgrading to one of these releases.

- Upgrading a Cisco CSR1000V or Cisco ISRv router to Cisco IOS XE Release 17.4.1a includes upgrading to the Cisco Catalyst 8000V.
### Supported Upgrades

<table>
<thead>
<tr>
<th>You Can Upgrade to...</th>
<th>From these Releases</th>
</tr>
</thead>
</table>
| Cisco IOS XE 17.3.x                 | Cisco IOS XE Release 17.2.1r  
|                                     | Cisco IOS XE Release 17.2.1v  
|                                     | Cisco IOS XE SD-WAN 16.12.x  
|                                     | Cisco IOS XE SD-WAN 16.11.x  
|                                     | Cisco IOS XE SD-WAN 16.10.x  
|                                     | Cisco IOS XE SD-WAN 16.9.x  |
| Cisco IOS XE Release 17.2.1r        | Cisco IOS XE SD-WAN 16.12.x  
|                                     | Cisco IOS XE SD-WAN 16.11.x  
|                                     | Cisco IOS XE SD-WAN 16.10.x  
|                                     | Cisco IOS XE SD-WAN 16.9.x  |

Table 12: All Routers Supported by Cisco SD-WAN Except Cisco CSR1000V, Cisco ISRv, and Cisco Catalyst 8000V

<table>
<thead>
<tr>
<th>You Can Upgrade to...</th>
<th>From these Releases</th>
</tr>
</thead>
</table>
| Cisco IOS XE Release 17.4.1a        | Cisco IOS XE SD-WAN 17.3.1a or later  
|                                     | Cisco IOS XE SD-WAN 17.2.1 or later  
|                                     | Cisco IOS XE SD-WAN 16.12.4a or later  |
| Cisco IOS XE 17.3.x                  |                                                                                      |
| Cisco IOS XE Release 17.2.1r        | Cisco IOS XE SD-WAN 16.12.x  
|                                     | Cisco IOS XE SD-WAN 16.11.x  
|                                     | Cisco IOS XE SD-WAN 16.10.x  
|                                     | Cisco IOS XE SD-WAN 16.9.x  |

Use the following procedures to upgrade your device to Cisco IOS XE Release 17.2.1r or later images.

**Note**

Do not delete the existing image to ensure that you have a rollback option.
When upgrading to Cisco IOS XE Release 17.4.1a from Cisco IOS XE Releases 17.3.1a or earlier, we recommend that you do not make any changes to the device configuration using CLI, while a feature template is detached. Starting Cisco IOS XE Release 17.4.1a, we use Cisco vManage assisted upgrades. In this upgrade procedure, Cisco vManage saves the device configuration before the upgrade. If the configuration on the device, that is modified using CLI is not same as on Cisco vManage, then the device has inconsistent configuration after the upgrade.

For example, if you configure the BGP AS number of a device to a different value using CLI, the device can have inconsistent configuration and the upgrade fails. If the upgrade is performed when the device is in CLI mode, then you must revert the BGP AS number to the original value and then upgrade the device. Therefore, we recommend that you upgrade the device using Cisco vManage.

**Note**

Beginning with Cisco IOS XE Release 17.5.1a, if you are upgrading the firmware for a device on which the primary tunnel interface is a cellular interface and the backup tunnel interface is a gigabit interface, use the gigabit interface as the primary interface for the firmware upgrade.

For information about configuring the priority of a tunnel interface, see the vmanage-connection-preference command in *Cisco SD-WAN Command Reference*. An interface that is configured with a higher preference value has a higher priority.

---

**Upgrade Using Cisco vManage**

We recommend using Cisco vManage to upgrade. This keeps devices and the controller synchronized.

1. Use the Cisco vManage upgrade and activate procedure described in the *Cisco SD-WAN Monitor and Maintain* guide.

---

**Upgrade Using CLI**

We recommend using Cisco vManage to upgrade. This keeps devices and the controller synchronized. If it is necessary to upgrade using the CLI, use the following steps.

**Back Up Configuration Files**

Use these following steps to make configuration file copies before performing the manual upgrade process. Without these steps, the router will lose its configuration during the upgrade.

**Note**

If the deployment is on a public cloud service, such as Amazon Web Services (AWS), failure to save the configuration before upgrading manually can cause an unrecoverable loss of connectivity with the device. In contrast to a hardware device, there may be no way to gain any type of console access to the virtual router.

1. Use the following command to make a backup copy of the Cisco IOS XE SD-WAN configuration:

   ```
   show running-config | redirect bootflash:sdwan/ios.cli
   ```

2. Use the following command to make a backup copy of the Cisco SD-WAN running configuration:
show sdwan running-config | redirect bootflash:sdwan/sdwan.cli

Upgrade Procedure

1. Download the Cisco IOS XE Release 17.2 image for your device from https://software.cisco.com
2. Upload the image to the device.
3. Install the new software. Example:
   
   Device# request platform software sdwan software install bootflash:isr4300-universalk9.17.2.1.SPA.bin

4. Activate the software. The device reloads when the activation is complete. Example:
   
   Device# request platform software sdwan software activate 17.2.01r.9.3

5. Verify that the software is activated.
   
   Device# show sdwan software

<table>
<thead>
<tr>
<th>VERSION</th>
<th>ACTIVE</th>
<th>DEFAULT</th>
<th>PREVIOUS</th>
<th>CONFIRMED</th>
<th>TIMESTAMP</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.12.1d.0.48</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>auto</td>
<td>2020-03-04T10:43:45-00:00</td>
</tr>
<tr>
<td>17.2.01r.9.3</td>
<td>true</td>
<td>false</td>
<td>false</td>
<td>user</td>
<td>2020-03-04T11:15:20-00:00</td>
</tr>
</tbody>
</table>

   Total Space:388M Used Space:100M Available Space:285M

6. (Optional) To ensure that the new version is preserved if software reset required, use the following command. Example:
   
   Device# request platform software sdwan software set-default 17.2.01r.9.3

7. Verify the upgrade using request platform software sdwan software upgrade-confirm.
   
   Device# request platform software sdwan software upgrade-confirm

---

Note

In controller mode, use the config-transaction command to enter global configuration mode. The configuration terminal command is not supported in Controller mode.

<table>
<thead>
<tr>
<th>Existing Installation (image)</th>
<th>Upgraded to (image)</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE SD-WAN Release 16.12 and earlier (ucmk9)</td>
<td>Cisco IOS XE Release 17.2.1r (universalk9)</td>
<td>Device boots up in controller mode and configuration is preserved.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 16.12 and earlier (universalk9)</td>
<td>Cisco IOS XE Release 17.2.1r (universalk9)</td>
<td>Device boots up in autonomous mode and configuration is preserved (via startup configuration)</td>
</tr>
</tbody>
</table>
Downgrade from Cisco IOS XE Release 17.2.1r or Later Releases

Downgrading to a Previously Installed Image: Inline Downgrade

If you want to downgrade to a previously installed image, use the `request platform software sdwan activate` command to reactivate the install.

```
Device# show sdwan software
VERSION ACTIVE DEFAULT PREVIOUS CONFIRMED TIMESTAMP
16.10.400.0.0 false true true auto 2019-11-20T04:40:05-00:00
17.2.1.0.102822 true false false auto 2019-12-10T11:01:22-00:00
```
Total Space:387M Used Space:251M Available Space:131M

Downgrading to a Fresh Install of a Target Image: Clean Downgrade

Downgrading to a fresh install of an image of older release versions, brings the device to Day Zero configuration. For example, if you have never installed Cisco IOS XE SD-WAN 16.10.4 on your device and attempt to downgrade from Cisco IOS XE Release or later releases to Cisco IOS XE SD-WAN 16.10.4 the following warning displays:

⚠️ Warning

You are trying to activate an old image which will remove all device configuration and bring the device back to day-0 state. To proceed, use the `clean` option at activation.

To activate a fresh install of an old image use the `request platform software sdwan activate clean` command.

Downgrade Scenarios for Cisco IOS XE Release 17.2.x

<table>
<thead>
<tr>
<th>Existing Installation (image)</th>
<th>Downgrade to (image)</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 17.2.1r (universalk9) in controller mode</td>
<td>Cisco IOS XE SD-WAN Release 16.12 and earlier (ucmk9)</td>
<td>Device boots up with ucmk9 image and configuration is restored if the uckm9 image was previously installed on the device. Downgrading to a fresh install of old image versions brings the device to Day 0 configuration. To proceed, use the <code>clean</code> option at activation.</td>
</tr>
<tr>
<td>Cisco IOS XE Release 17.2.1r (universalk9) in autonomous mode</td>
<td>Cisco IOS XE Release 17.1.1 and earlier (universalk9)</td>
<td>Device boots up with universalk9 image and configuration is restored.</td>
</tr>
</tbody>
</table>
• Downgrading directly from controller mode to Cisco IOS XE Amsterdam Release 17.1.x or earlier universalk9 or other non SD-WAN images is not supported. To downgrade from controller mode to earlier IOS XE images, switch to autonomous mode and follow the downgrade process.

• Downgrading directly from autonomous mode to Cisco IOS XE SD-WAN 16.12 or earlier ucmk9 SD-WAN images is not supported. To downgrade from autonomous mode to earlier IOS XE SD-WAN images, switch to controller mode and follow the downgrade process.

---

**Restore Smart Licensing and Smart License Reservation**

The smart licensing authorization is lost when a device switches from autonomous to controller mode and back to autonomous mode again.

---

**Note**

For more information about Smart Licensing, refer to Smart Licensing Guide for Access and Edge Routers.

---

**Restore Smart Licensing**

1. Reconfigure device to reach Cisco Smart Software Manager (CSSM).
2. Register the device using `license smart register idtoken` `token force` command in privileged EXEC mode.
3. Set the required crypto throughput using `platform hardware throughput crypto` `crypto-value`.
4. Save the configuration using `write memory` in privileged EXEC mode.
5. Reload the device and verify that the new crypto throughput value is applied using the `show platform hardware throughput crypto` command.

---

**Restore Smart License Reservation**

1. Enable the reservation mode using the `license smart reservation` command in global configuration mode.
2. Set the required crypto throughput using `platform hardware throughput crypto` `crypto-value`.
3. Save the configuration using `write memory`.
4. Reload the device and verify that the new crypto throughput value is applied using the `show platform hardware throughput crypto` command.
Onboard Cisco Catalyst 8000V Edge Software Hosted by a Cloud Service, Using PAYG Licensing

To onboard a Cisco Catalyst 8000V platform hosted by a cloud service, using pay as you go (PAYG) licensing, perform these steps.

You can also use Cisco Cloud onRamp for Multi-Cloud to onboard a Cisco Catalyst 8000V platform using PAYG licensing. For information, see Cloud OnRamp Configuration Guide, Cisco IOS XE Release 17.x.

---

**Note**

This procedure is applicable to a Cisco Catalyst 8000V hosted by Amazon Web Services (AWS).

1. In Cisco vManage, choose **Configuration > Devices**, and click **Add PAYG WAN Edges**.

2. In the **Add PAYG WAN Edges** dialog box, enter the number of PAYG devices to onboard into Cisco SD-WAN, check the **Validate** check box, and click **Add**.

   The **Task View** page opens, showing the progress as Cisco vManage creates logical devices.

   **Note**

   Validating causes Cisco vManage to publish the list of devices to the Cisco vBond Orchestrator and Cisco vSmart Controller controllers in the network.

3. After the **Task View** page shows that the logical devices have been created successfully, choose **Configuration > Devices** to view the new logical devices on the **Devices** page.

   **Note**

   The **Chassis Number** column shows the unique identifier for each logical device.

4. In the row of one of the logical devices that you created, click **More Options (…)** and choose **Generate Bootstrap Configuration**.

5. (Optional) Attach a device template to the logical devices that you have created.

6. In the **Generate Bootstrap Configuration** dialog box, click **Cloud-Init** and then click **OK**.

   The **Generate Bootstrap Configuration** dialog box shows the content of the bootstrap configuration, which includes the UUID of the logical device, and includes the configuration details provided by the device template if you have attached one.

   **Note**

   The UUID corresponds to the identifier in the **Chassis Number** column in the **Devices** table.

7. There are different methods for loading the bootstrap configuration onto a C8000V instance on a cloud service. The method you use depends on the cloud service. We recommend clicking **Download** in the **Generate Bootstrap Configuration** dialog box to save a copy of the bootstrap configuration.
8. In the cloud services portal, create a PAYG instance of the Cisco Catalyst 8000V. When configuring the instance, use the bootstrap configuration that you created in Cisco vManage. The details of how to load the Cisco SD-WAN bootstrap configuration onto the instance are specific to the cloud services provider.

Note
On AWS, the workflow for bringing up an instance includes a user data step that enables loading the bootstrap configuration.

9. On the cloud service platform, start the Cisco Catalyst 8000V instance using the bootstrap configuration from an earlier step.

When the Cisco Catalyst 8000V instance boots up, it joins the Cisco SD-WAN overlay automatically. In Cisco vManage, on the Devices page, this Cisco Catalyst 8000V instance shows a green medal icon in the State column and In Sync in the Device Status column.

Note
On the Devices page, for logical devices that have not joined the Cisco SD-WAN overlay, the State column shows a dotted-circle icon.

Bootstrap Process for Cisco SD-WAN Cloud-Hosted Devices

We recommend that you attach a device template to the logical device before creating the bootstrap configuration. The device template provides the configuration details that enable the device to connect to Cisco vManage. To create the bootstrap configuration file, perform the following steps:

1. In Cisco vManage, choose Configuration > Devices.

2. In the table of devices, locate the row with the logical device that you are using for a new cloud-hosted instance. The logical device includes the UUID to use for the instance.

3. In the row with the logical device, click More Actions (…) at the right and choose Generate Bootstrap Configuration.

4. In the Generate Bootstrap Configuration dialog box, choose Cloud-Init and click OK. The Generate Bootstrap Configuration dialog box displays the bootstrap configuration, including the OTP token for the license, vBond address, UUID, and organization information.

Note
The UUID corresponds to the identifier in the Chassis Number column in the Devices table.

Note
Ensure that the bootstrap configuration does not include more interfaces than the virtual device instance has in the cloud environment.

5. There are different methods for loading the bootstrap configuration onto a device instance on a cloud service. The method you use depends on the cloud service. We recommend that you click Download in the Generate Bootstrap Configuration dialog box to save a copy of the bootstrap configuration.
You can use the bootstrap configuration when setting up a device instance in the cloud service. The configuration enables the device instance to connect to Cisco SD-WAN.
CHAPTER 6

Cisco SD-WAN Overlay Network Bring-Up Process

- Bring Up the Sequence of Events, on page 85
- Download Software, on page 112
- Deploy Cisco vManage, on page 113
- Deploy Cisco vBond Orchestrator, on page 125
- vContainer Host, on page 153
- Deploy Cisco vSmart Controller, on page 153
- Deploy Cisco Catalyst 8000V Using Cloud Services Provider Portals, on page 182
- Deploy Cisco CSR 1000v Using Cloud Service Provider Portals, on page 182
- Deploy Cisco Catalyst 8000V Edge Software on Alibaba Cloud, on page 183
- Deploy the vEdge Cloud routers, on page 184

Bring Up the Sequence of Events

The bring-up process for edge devices—which includes authenticating and validating all the devices and establishing a functional overlay network—occurs with only minimal user input. From a conceptual point of view, the bring-up process can be divided into two parts, one that requires user input and one that happens automatically:

1. In the first part, you design the network, create virtual machine (VM) instances for cloud routers, and install and boot hardware routers. Then, in Cisco vManage, you add the routers to the network and create configurations for each router. This process is described in the Summary of the User Portion of the Bring-Up Sequence.

2. The second part of the bring-up process occurs automatically, orchestrated by the Cisco SD-WAN software. As routers join the overlay network, they validate and authenticate themselves automatically, and they establish secure communication channels between each other. For Cisco vBond Orchestrators and Cisco vSmart Controllers, a network administrator must download the necessary authentication-related files from Cisco vManage, and then these Cisco vSmart Controllers and Cisco vBond Orchestrators automatically receive their configurations from Cisco vManage. For vEdge Cloud routers, you must generate a certificate signing request (CSR), install the received certificate, and then upload the serial number that is included in the certificate to Cisco vManage. After Cisco hardware routers start, they are authenticated on the network and receive their configurations automatically from Cisco vManage through a process called zero-touch provisioning (ZTP). This process is described in the Automatic Portions of the Bring-Up Sequence.
The end result of this two-part process is an operational overlay network.

This topic describes the sequence of events that occurs during the bring-up process, starting with the user portion and then explaining how automatic authentication and device validation occur.

**Sequence of Events of the Bring-Up Process**

From a functional point of view, the task of bringing up the routers in the overlay network occurs in the following sequence:

*Figure 1: Bring-Up Sequence of Events*

1. The Cisco vManage software starts on a server in the data center.
2. The Cisco vBond Orchestrator starts on a server in the DMZ.
3. The Cisco vSmart Controller starts on a server in the data center.
4. Cisco vManage and the Cisco vBond Orchestrator authenticate each other, Cisco vManage and the Cisco vSmart Controller authenticate each other, and the Cisco vSmart Controller and the Cisco vBond Orchestrator securely authenticate each other.
5. Cisco vManage sends configurations to the Cisco vSmart Controller and the Cisco vBond Orchestrator.
6. The routers start in the network.
7. The routers authenticate themselves with the Cisco vBond Orchestrator.
8. The routers authenticate themselves with Cisco vManage.
9. The routers authenticate themselves with the Cisco vSmart Controller.
10. Cisco vManage sends configurations to the routers.

Before you start the bring-up process, note the following:
To provide the highest level of security, only authenticated and authorized routers can access and participation in the Cisco SD-WAN overlay network. To this end, the Cisco vSmart Controller performs automatic authentication on all the routers before they can send data traffic over the network.

After the routers are authenticated, data traffic flows, regardless of whether the routers are in a private address space (behind a NAT gateway) or in a public address space.

To bring up the hardware and software components in a Cisco SD-WAN overlay network, a transport network (also called a transport cloud), which connects all the routers and other network hardware components, must be available. Typically, these components are in data centers and branch offices. The only purpose of the transport network is to connect all the network devices in the domain. The Cisco SD-WAN solution is agnostic with regards to the transport network, and, therefore, can be any type, including the internet, Multiprotocol Label Switching (MPLS), Layer 2 switching, Layer 3 routing, and Long-Term Evolution (LTE), or any mixture of transports.

For hardware routers, you can use the Cisco SD-WAN zero-touch provisioning (ZTP) SaaS to bring up the routers. For more information, see Prepare Routers for ZTP.

Steps to Bring Up the Overlay Network

Bringing Up the Overlay Network

The following table lists the tasks for bringing up the overlay network using Cisco vManage.

Table 15:

<table>
<thead>
<tr>
<th>Bring-Up Task</th>
<th>Step-by-Step Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1: Start the Cisco vManage.</td>
<td>1. On the hypervisor, create a VM instance.</td>
</tr>
<tr>
<td></td>
<td>2. Boot Cisco vManage server, start the VM, and enter login information.</td>
</tr>
<tr>
<td></td>
<td>3. In vManage &gt; Administration &gt; Settings, configure certificate authorization settings. Select Automated to allow the certificate-generation process to occur automatically when a CSR is generated for a controller device.</td>
</tr>
<tr>
<td></td>
<td>4. In vManage &gt; Certificates, generate the CSR.</td>
</tr>
<tr>
<td></td>
<td>5. Check for a confirmation email from Symantec that your request has been received.</td>
</tr>
<tr>
<td></td>
<td>6. Check for an email from Symantec that Viptela has approved your request and the certificate is signed.</td>
</tr>
<tr>
<td></td>
<td>7. In vManage &gt; Configuration &gt; Devices, check that the certificate has been installed.</td>
</tr>
</tbody>
</table>
### Step 2: Start the Cisco vBond Orchestrator.

<table>
<thead>
<tr>
<th>Bring-Up Task</th>
<th>Step-by-Step Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. On the hypervisor, create a VM instance.</td>
</tr>
<tr>
<td></td>
<td>2. Boot the vBond server and start the VM.</td>
</tr>
<tr>
<td></td>
<td>3. In vManage &gt; Configuration &gt; Devices &gt; Controller, add Cisco vBond Orchestrator and generate the CSR.</td>
</tr>
<tr>
<td></td>
<td>4. Check for a confirmation email from Symantec that your request has been received.</td>
</tr>
<tr>
<td></td>
<td>5. Check for an email from Symantec that Viptela has approved your request and the certificate is signed.</td>
</tr>
<tr>
<td></td>
<td>6. In vManage &gt; Configuration &gt; Devices, check that the certificate has been installed.</td>
</tr>
<tr>
<td></td>
<td>7. In vManage &gt; Configuration &gt; Templates:</td>
</tr>
<tr>
<td></td>
<td>a. Create a configuration template for the Cisco vBond Orchestrator.</td>
</tr>
<tr>
<td></td>
<td>b. Attach the template to Cisco vBond Orchestrator.</td>
</tr>
<tr>
<td></td>
<td>8. In vManage &gt; Dashboard, verify that the Cisco vBond Orchestrator is operational.</td>
</tr>
</tbody>
</table>

### Step 3: Start the Cisco vSmart Controller.

<table>
<thead>
<tr>
<th>Bring-Up Task</th>
<th>Step-by-Step Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. On the hypervisor, create a VM instance.</td>
</tr>
<tr>
<td></td>
<td>2. Boot the vSmart server and start the VM.</td>
</tr>
<tr>
<td></td>
<td>3. In vManage &gt; Configuration &gt; Devices &gt; Controller, add Cisco vSmart Controller and generate the CSR.</td>
</tr>
<tr>
<td></td>
<td>4. Check for a confirmation email from Symantec that your request has been received.</td>
</tr>
<tr>
<td></td>
<td>5. Check for an email from Symantec that Viptela has approved your request and the certificate is signed.</td>
</tr>
<tr>
<td></td>
<td>6. In vManage &gt; Configuration &gt; Devices, check that the certificate has been installed.</td>
</tr>
<tr>
<td></td>
<td>7. In vManage &gt; Configuration &gt; Templates:</td>
</tr>
<tr>
<td></td>
<td>a. Create a configuration template for Cisco vSmart Controller.</td>
</tr>
<tr>
<td></td>
<td>b. Attach the template to Cisco vSmart Controller.</td>
</tr>
<tr>
<td></td>
<td>8. In vManage &gt; Dashboard, verify that Cisco vSmart Controller is operational.</td>
</tr>
</tbody>
</table>
### Step-by-Step Procedure

1. **In vManage > Configuration > Devices > WAN Edge List**, upload the router authorized serial number file.
2. **In vManage > Configuration > Certificates > WAN Edge List**, check that the router's chassis and serial number are in the list.
3. **In vManage > Configuration > Certificates > WAN Edge List**, authorize each router by marking it Valid in the Validity column.
4. **In vManage > Configuration > Certificates > WAN Edge List**, send the WAN Edge list to the controller devices.
5. **In vManage > Configuration > Templates**:
   
a. Create a configuration template for the router.
   
b. Attach the template to the router.

### Summary of the User Portion of the Bring-Up Sequence

Generally, what you do to bring up the Cisco SD-WAN overlay network is what you do to bring up any network. You plan out the network, create device configurations, and then deploy the network hardware and software components. These components include all the Cisco vEdged devices, all the traditional routers that participate in the overlay network, and all the network devices that provide shared services across the overlay network, such as firewalls, load balancers, and IDP systems.

The following table summarizes the steps for the user portion of the Cisco SD-WAN overlay network bring-up sequence. The details of each step are provided in the articles that are listed in the Procedure column. While you can bring up the Cisco vEdged devices in any order, it is recommended that you deploy them in the order listed below, which is the functional order in which the devices verify and authenticate themselves.

If your network has firewall devices, see Firewall Ports for Cisco SD-WAN Deployments.
### Table 16: Summary of the User Portion of the Bring-Up Sequence

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Plan out your overlay network. See Components of the Cisco SD-WAN Solution.</td>
</tr>
<tr>
<td>2</td>
<td>On paper, create device configurations that implement the desired architecture and functionality. See the Software documentation for your software release.</td>
</tr>
<tr>
<td>3</td>
<td>Download the software images.</td>
</tr>
</tbody>
</table>
## Summary of the User Portion of the Bring-Up Sequence

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| **4**    | **Deploy Cisco vManage in the data center:**  
1. Create a Cisco vManage VM instance, either on an ESXi or a KVM hypervisor.  
2. Create either a minimal or a full configuration for each Cisco vManage server.  
3. Configure certificate settings and generate a certificate for Cisco vManage.  
4. Create a Cisco vManage cluster.  

![Diagram of Deploy vManage](image)

| **5**    | **Deploy the Cisco vBond Orchestrator:**  
1. Create a Cisco vBond Orchestrator VM instance, either on an ESXi or a KVM hypervisor.  
2. Create a minimal configuration for the Cisco vBond Orchestrator.  
3. Add the Cisco vBond Orchestrator to the overlay network. During this process, you generate a certificate for the Cisco vBond Orchestrator.  
4. Create a full configuration for the Cisco vBond Orchestrator.  

![Diagram of Deploy vBond](image)

| **6**    | **Deploy the Cisco vSmart Controller in the data center:**  
1. Create a Cisco vSmart Controller VM instance, either on an ESXi or a KVM hypervisor.  
2. Create a minimal configuration for the Cisco vSmart Controller.  
3. Add the Cisco vSmart Controller to the overlay network. During this process, you generate a certificate for the Cisco vSmart Controller.  
4. Create a full configuration for the Cisco vSmart Controller.  

![Diagram of Deploy vSmart](image)
Automatic Portions of the Bring-Up Sequence

After the Cisco vEdge devices boot and start running with their initial configurations, the second part of the bring-up process begins automatically. This automatic process is led by the Cisco vBond Orchestrator, as illustrated in the figure below. Under the leadership of the Cisco vBond Orchestrator software, the Cisco vEdge devices set up encrypted communication channels between themselves. Over these channels, the devices automatically validate and authenticate each other, a process that establishes an operational overlay network. Once the overlay network is running, the Cisco vEdge devices automatically receive and activate their full configurations from the Cisco vManage server. (The exception is the Cisco vManage. You must manually configure each Cisco vManage server itself).

The following sections explain what happens under the covers, during the automatic portion of the bring-up process. This explanation is provided to help you understand the detailed workings of the Cisco SD-WAN software so that you can better appreciate the means by which the Cisco SD-WAN solution creates a highly secure overlay framework to support your networking requirements.

User Input Required for the ZTP Automatic Authentication Process

The automatic validation and authentication of Cisco vEdge devices that occurs during the bring-up process can happen only if Cisco vSmart Controllers and Cisco vBond Orchestrators know the serial and chassis numbers of the devices that are permitted in the network. Let's first define these two terms:

- **Serial number**—Each Cisco vEdge device has a serial number, which is a 40-byte number that is included in the device's certificate. For Cisco vBond Orchestrator and Cisco vSmart Controller, the certificate can be provided by Symantec or by an enterprise root CA. For the vEdge routers, the certificate is provided in the hardware's trusted board ID chip.
• Chassis number—In addition to a serial number, each vEdge router is identified by a chassis number. Because the vEdge router is the only Cisco SD-WAN manufactured hardware, it is the only Cisco vEdge device that has a chassis number. There is a one-to-one mapping between a vEdge router’s serial number and its chassis number.

The Cisco vSmart Controllers and Cisco vBond Orchestrators learn the serial and chassis numbers during the initial configuration of these devices:

- vSmart authorized serial numbers—The Cisco vManage learns the serial numbers for all Cisco vSmart Controllers that are allowed to be in the network while it is creating a CSR and installing the signed certificate. You download these serial numbers to Cisco vBond Orchestrator, and Cisco vBond Orchestrator pushes them to the Cisco vSmart Controller during the automatic authentication process.

- vEdge authorized serial number file—This file contains the serial and chassis numbers of all the vEdge routers that are allowed to be in the network. You upload this file to Cisco vBond Orchestrators and Cisco vSmart Controllers.

In addition to the device serial and chassis numbers, the automatic validation and authentication procedure depends on having each device configured with the same organization name. You configure this name on Cisco vManage, and it is included in the configuration file on all devices. The organization name must be identical on all the devices that belong to a single organization (the name is case-sensitive). The organization name is also included in the certificate for each device, which is created either by Cisco SD-WAN or by an enterprise root CA.

**Authentication between Cisco vSmart Controller and Cisco vBond Orchestrator**

From a functional point of view, the first two devices on the Cisco SD-WAN overlay network that validate and authenticate each other are Cisco vSmart Controller and Cisco vBond Orchestrator. This process is initiated by Cisco vSmart Controller.

![Authentication Diagram](image)

When Cisco vSmart Controller comes up, it initiates a connection to Cisco vBond Orchestrator, which is how Cisco vBond Orchestrator learns about Cisco vSmart Controller. These two devices then automatically begin a two-way authentication process—Cisco vSmart Controller authenticates itself with Cisco vBond Orchestrator, and Cisco vBond Orchestrator authenticates itself with Cisco vSmart Controller. The two-way handshaking between the two devices during the authentication process occurs in parallel. However, for clarity, the figure here, which is a high-level representation of the authentication steps, illustrates the handshaking sequentially. If the authentication handshaking succeeds, a permanent DTLS communication channel is established between the vSmart and vBond devices. If any one of the authentication steps fails, the device noting the failure tears down the connection between the two devices, and the authentication attempt terminates.
The vSmart controller knows how to reach Cisco vBond Orchestrator, because one of the parameters that you provision when you configure it is the IP address or DNS name of Cisco vBond Orchestrator. Cisco vBond Orchestrator is primed to respond to requests from Cisco vSmart Controller because:

- It knows that its role is to be the authentication system, because you included this information in the vBond configuration.
- You downloaded the vSmart authorized serial numbers from Cisco vManage to Cisco vBond Orchestrator.

If Cisco vBond Orchestrator has not yet started when Cisco vSmart Controller initiates the authentication process, Cisco vSmart Controller periodically attempts to initiate a connection until it is successful.

Below is a more detailed step-by-step description of how the automatic authentication occurs between Cisco vSmart Controller and Cisco vBond Orchestrator.

To initiate a session between Cisco vSmart Controller and Cisco vBond Orchestrator, Cisco vSmart Controller initiates an encrypted DTLS connection to Cisco vBond Orchestrator. The encryption is provided by RSA. Each device automatically generates an RSA private key–public key pair when it boots.

Over this encrypted channel, Cisco vSmart Controller and Cisco vBond Orchestrator authenticate each other. Each device authenticates the other in parallel. For our discussion, let's start with Cisco vSmart Controller authentication of Cisco vBond Orchestrator:

1. Cisco vBond Orchestrator sends its trusted root CA signed certificate to the vSmart controller.
2. Cisco vBond Orchestrator sends the vEdge authorized serial number file to the vSmart controller.
3. Cisco vSmart Controller uses its chain of trust to extract the organization name from the certificate and compares it to the organization name that is configured on Cisco vSmart Controller. If the two organization names match, Cisco vSmart Controller knows that the organization of Cisco vBond Orchestrator is proper. If they do not match, Cisco vSmart Controller tears down the DTLS connection.
4. Cisco vSmart Controller uses the root CA chain to verify that the certificate has indeed been signed by the root CA (either Symantec or the enterprise CA). If the signature is correct, Cisco vSmart Controller knows that the certificate itself is valid. If the signature is incorrect, Cisco vSmart Controller tears down the DTLS connection.
After performing these two checks, Cisco vSmart Controller authentication of Cisco vBond Orchestrator is complete.

In the other direction, Cisco vBond Orchestrator authenticates Cisco vSmart Controller:

1. Cisco vSmart Controller sends its trusted root CA signed certificate to Cisco vBond Orchestrator.

2. Cisco vBond Orchestrator uses its chain of trust to extract Cisco vSmart Controller serial number from the certificate. The number must match one of the numbers in the vSmart authorized serial number file. If there is no match, Cisco vBond Orchestrator tears down the DTLS connection.

3. Cisco vBond Orchestrator uses its chain of trust to extract the organization name from the certificate and compares it to the organization name that is configured on Cisco vBond Orchestrator. If the two organization names match, the vBond Orchestrator knows that the organization of Cisco vSmart Controller is proper. If they do not match, Cisco vBond Orchestrator tears down the DTLS connection.

4. The vBond Orchestrator uses the root CA chain to verify that the certificate has indeed been signed by the root CA (either Symantec or the enterprise CA). If the signature is correct, Cisco vBond Orchestrator knows that the certificate itself is valid. If the signature is incorrect, Cisco vBond Orchestrator tears down the DTLS connection.
After performing these three checks, the vBond authentication of Cisco vSmart Controller is complete.

After the bidirectional authentication completes between the two devices, the DTLS connection between Cisco vBond Orchestrator and Cisco vSmart Controller transitions from being a temporary connection to being a permanent connection, and the two devices establish an OMP session over the connection.

In a domain that has multiple Cisco vSmart Controllers for redundancy, this process repeats between each pair of vSmart and vBond devices. In coordination with Cisco vBond Orchestrator, Cisco vSmart Controllers learn about each other and they synchronize their route information. It is recommended that you connect the different vSmart controllers to the WAN network through different NAT devices for higher availability.

A Cisco vBond Orchestrator has only as many permanent DTLS connections as the number of Cisco vSmart Controllers in the network topology. These DTLS connections are part of the network's control plane; no data traffic flows over them. After all Cisco vSmart Controllers have registered themselves with Cisco vBond Orchestrator, Cisco vBond Orchestrator and Cisco vSmart Controllers are ready to validate and authenticate the vEdge routers in the Cisco SD-WAN network.

### Authentication Between Cisco vSmart Controller

**Authentication between Cisco vSmart Controllers**

In a domain with multiple Cisco vSmart Controllers, the controllers must authenticate each other so that they can establish a full mesh of permanent DTLS connection between themselves for synchronizing OMP routes. Cisco vSmart Controller learns the IP address of the other Cisco vSmart Controller from Cisco vBond Orchestrator.

Cisco vSmart Controller learns about the possibility of other Cisco vSmart Controllers being present on the network during the authentication handshaking with the vBond orchestrator, when it receives a copy of the vSmart authorized serial number file. If this file has more than one serial number, it indicates that the network may, at some point, have multiple Cisco vSmart Controllers.
As one Cisco vSmart Controller authenticates with Cisco vBond Orchestrator, Cisco vBond Orchestrator sends Cisco vSmart Controller the IP address of other Cisco vSmart Controllers it has authenticated with. If Cisco vBond Orchestrator later learns of another Cisco vSmart Controller, it sends that controller’s address to the other already authenticated Cisco vSmart Controllers.

Then, Cisco vSmart Controllers perform the steps below to authenticate each other. Again, each device authenticates the other in parallel, but for clarity, we describe the process sequentially.

1. vSmart1 initiates an encrypted DTLS connection to vSmart2 and sends its trusted root CA signed certificate to vSmart2.

2. vSmart2 uses its chain of trust to extract the vSmart1’s serial number. The number must match one of the numbers in the vSmart authorized serial number file. If there is no match, vSmart2 tears down the DTLS connection.

3. vSmart2 uses its chain of trust to extract the organization name from the certificate and compares it to the locally configured organization name. If the two organization names match, vSmart2 knows that the organization of vSmart1 is proper. If they do not match, vSmart2 tears down the DTLS connection.

4. vSmart2 uses the root CA chain to verify that the certificate has indeed been signed by the root CA (either Symantec or the enterprise CA). If the signature is correct, vSmart2 knows that the certificate itself is valid. If the signature is incorrect, vSmart2 tears down the DTLS connection.

After performing these three checks, vSmart2 authentication of vSmart1 is complete.

Now, vSmart1 authenticates vSmart2, performing the same steps as above.

1. First, vSmart2 sends its trusted root CA signed certificate to vSmart1.

2. vSmart1 uses its chain of trust to extract the vSmart2’s serial number. The number must match one of the numbers in the vSmart authorized serial number file. If there is no match, vSmart1 tears down the DTLS connection.

3. vSmart1 uses its chain of trust to extract the organization name from the certificate and compares it to the locally configured organization name. If the two organization names match, vSmart2 knows that the organization of vSmart2 is proper. If they do not match, vSmart1 tears down the DTLS connection.

4. vSmart1 uses the root CA chain to verify that the certificate has indeed been signed by the root CA (either Symantec or the enterprise CA). If the signature is correct, vSmart2 knows that the certificate itself is valid. If the signature is incorrect, vSmart1 tears down the DTLS connection.
Authentication Between Cisco vSmart Controller

1. Trusted root CA signed certificate
2. Verify serial number
3. Verify organization name
4. Verify certificate signed by root CA
5. DTLS Connection
6. One-way SSL authentication
7. Verify serial number
8. Verify organization name
9. Verify certificate signed by root CA
10. Permanent DTLS Connection
11. Two-way SSL authentication
After performing these three checks, vSmart1 authentication of vSmart2 is complete, and the temporary DTLS connection between the two devices becomes permanent.

After all the Cisco vSmart Controllers have registered themselves with Cisco vBond Orchestrator, Cisco vBond Orchestrator and Cisco vSmart Controllers are ready to validate and authenticate the vEdge routers in the Cisco SD-WAN network.

**Authentication between Cisco vBond Orchestrator and a vEdge Router**

When you deploy a vEdge router in the network, it first needs to do two things:

- Establish a secure connection with Cisco vManage so that it can receive its full configuration.
- Establish a secure connection with Cisco vSmart Controller can begin participating in the Cisco SD-WAN overlay network.

When a vEdge device comes up, how does it automatically discover Cisco vManage and Cisco vSmart Controller and establish connections with them? It does so with help from Cisco vBond Orchestrator. The initial configuration on the vEdge router contains the vBond system’s IP address (or DNS name). Using this information, the vEdge router establishes a DTLS connection with Cisco vBond Orchestrator, and the two devices authenticate each other to confirm that they are valid Cisco vEdge devices. Again, this authentication is a two-way process that happens automatically. When the authentication completes successfully, Cisco vBond Orchestrator sends the vEdge router the IP addresses of Cisco vManage and Cisco vSmart Controller. Then, the vEdge router tears down its connection with Cisco vBond Orchestrator and begins establishing secure DTLS connections with the other two devices.

After you boot vEdge routers and manually perform the initial configuration, they automatically start looking for their Cisco vBond Orchestrator. Cisco vBond Orchestrator and Cisco vSmart Controllers are able to recognize and authenticate the vEdge routers in part because you have installed the vEdge authorized device list file on both these devices.

After you boot a vEdge router, you manually perform the initial configuration, at a minimum setting the IP address of DNS name of Cisco vBond Orchestrator. The vEdge router uses this address information to reach Cisco vBond Orchestrator. Cisco vBond Orchestrator is primed to respond to requests from a vEdge router because:

- It knows that its role is to be the authentication system, because you included this information in the initial vBond configuration.
- As part of the initial configuration, you installed the vEdge authorized serial number file on Cisco vBond Orchestrator.

After you boot vEdge routers and manually perform the initial configuration, they automatically start looking for their Cisco vBond Orchestrator. Cisco vBond Orchestrator and Cisco vSmart Controllers are able to recognize and authenticate the vEdge routers in part because you have installed the vEdge authorized device list file on both these devices.

After you boot a vEdge router, you manually perform the initial configuration, at a minimum setting the IP address of DNS name of Cisco vBond Orchestrator. The vEdge router uses this address information to reach Cisco vBond Orchestrator. Cisco vBond Orchestrator is primed to respond to requests from a vEdge router because:

- It knows that its role is to be the authentication system, because you included this information in the initial vBond configuration.
- As part of the initial configuration, you installed the vEdge authorized serial number file on Cisco vBond Orchestrator.
If Cisco vBond Orchestrator has not yet started when a vEdge router initiates the authentication process, the vEdge router periodically attempts to initiate a connection until the attempt succeeds.

Below is a more detailed step-by-step description of how the automatic authentication occurs between Cisco vBond Orchestrator and a vEdge router.

First, the vEdge router initiates an encrypted DTLS connection to the public IP address of Cisco vBond Orchestrator. The encryption is provided by RSA. Each device automatically generates an RSA private key–public key pair when it boots. Cisco vBond Orchestrator receives the vEdge router's original interface address and uses the outer IP address in the received packet to determine whether the vEdge router is behind a NAT. If it is, Cisco vBond Orchestrator creates a mapping of the vEdge router's public IP address and port to its private IP address.

Over this encrypted DTLS channel, the vEdge router and Cisco vBond Orchestrator proceed to authenticate each other. As with other device authentication, the vEdge router and Cisco vBond Orchestrator authenticate each other in parallel. We start our discussion by describing how the vEdge router authenticates Cisco vBond Orchestrator:

1. Cisco vBond Orchestrator sends its trusted root CA signed certificate to the vEdge router.
2. The vEdge router uses its chain of trust to extract the organization name from the certificate and compares it to the organization name that is configured on the router itself. If the two organization names match, the vEdge routers knows that the organization of Cisco vBond Orchestrator is proper. If they do not match, the vEdge router tears down the DTLS connection.
3. The vEdge router uses the root CA chain to verify that the certificate has indeed been signed by the root CA (either Symantec or the enterprise CA). If the signature is correct, the vEdge router knows that the certificate itself is valid. If the signature is incorrect, the vEdge router tears down the DTLS connection.

After performing these two checks, the vEdge router knows that Cisco vBond Orchestrator is valid, and its authentication of Cisco vBond Orchestrator is complete.

In the opposite direction, Cisco vBond Orchestrator authenticates the vEdge router:

1. Cisco vBond Orchestrator sends a challenge to the vEdge router. The challenge is a 256-bit random value.
2. The vEdge router sends a response to the challenge that includes the following: • vEdge serial number • vEdge chassis number • vEdge board ID certificate • 256-bit random value signed by the vEdge router's private key
3. Cisco vBond Orchestrator compares the serial and chassis numbers to the list in its vEdge authorized device list file. The numbers must match one of the number pairs in the file. If there is no match, Cisco vBond Orchestrator tears down the DTLS connection.

4. Cisco vBond Orchestrator checks that the signing of the 256-bit random value is proper. It does this using the vEdge router's public key, which it extracts from the router's board ID certificate. If the signing is not correct, Cisco vBond Orchestrator tears down the DTLS connection.

5. Cisco vBond Orchestrator uses the root CA chain from the vEdge router's board ID certificate to validate that the board ID certificate is itself valid. If the certificate is not valid, Cisco vBond Orchestrator tears down the DTLS connection.

After performing these three checks, Cisco vBond Orchestrator knows that vEdge router is valid, and its authentication of the router is complete.

When the two-way authentication succeeds, Cisco vBond Orchestrator performs the final step of its orchestration, sending messages to the vEdge router and Cisco vSmart Controller in parallel. To the vEdge router, Cisco vBond Orchestrator sends the following:

- The IP addresses of Cisco vSmart Controllers in the network so that the vEdge router can initiate connections to them. The address can be public IP addresses, or for the controllers that are behind a NAT gateway, the addresses are a list of the public and private IP addresses and port numbers. If the vEdge router is behind a NAT gateway, Cisco vBond Orchestrator requests that the vEdge router initiate a session with Cisco vSmart Controller.

- Serial numbers of Cisco vSmart Controllers that are authorized to be in the network.

To Cisco vSmart Controller, Cisco vBond Orchestrator sends the following:

- A message announcing the new vEdge router in the domain.

- If the vEdge router is behind a NAT gateway, Cisco vBond Orchestrator sends a request to Cisco vSmart Controller to initiate a session with the vEdge router.
Then, the vEdge router tears down the DTLS connection with the vBond orchestrator.

**Authentication between the vEdge Router and Cisco vManage**

After the vEdge router and Cisco vBond Orchestrator have authenticated each other, the vEdge router receives its full configuration over a DTLS connection with Cisco vManage:

1. The vEdge router establishes a DTLS connection with Cisco vManage.
2. Cisco vManage server sends the configuration file to the vEdge router.
3. When the vEdge router receives the configuration file and activates its full configuration.
4. The vEdge router starts advertising prefixes to Cisco vSmart Controller.

If you are not using Cisco vManage, you can log in to the vEdge router and either manually load its configuration file or manually configure the router.

Below is a more detailed step-by-step description of how the automatic authentication occurs between a vEdge router and Cisco vManage.

First, the vEdge router initiates an encrypted DTLS connection to the IP address of Cisco vManage. The encryption is provided by RSA. Each device automatically generates an RSA private key–public key pair when it boots. Cisco vManage receives the vEdge router's original interface address and uses the outer IP address in the received packet to determine whether the vEdge router is behind a NAT. If it is, Cisco vManage creates a mapping of the vEdge router's public IP address and port to its private IP address.

Over this encrypted DTLS channel, the vEdge router and Cisco vManage proceed to authenticate each other. As with other device authentication, the vEdge router and Cisco vManage authenticate each other in parallel. We start our discussion by describing how the vEdge router authenticates Cisco vManage:

1. Cisco vManage sends its trusted root CA signed certificate to the vEdge router.
2. The vEdge router uses its chain of trust to extract the organization name from the certificate and compares it to the organization name that is configured on the router itself. If the two organization names match, the vEdge routers knows that the organization of Cisco vManage is proper. If they do not match, the vEdge router tears down the DTLS connection.
3. The vEdge router uses the root CA chain to verify that the certificate has indeed been signed by the root CA (either Symantec or the enterprise CA). If the signature is correct, the vEdge router knows that the certificate itself is valid. If the signature is incorrect, the vEdge router tears down the DTLS connection.
After performing these two checks, the vEdge router knows that Cisco vManage is valid, and its authentication of Cisco vManage is complete.

In the opposite direction, Cisco vManage authenticates the vEdge router:

1. Cisco vManage sends a challenge to the vEdge router. The challenge is a 256-bit random value.

2. The vEdge router sends a response to the challenge that includes the following: • vEdge serial number • vEdge chassis number • vEdge board ID certificate (for a hardware vEdge router) or the signed certification (for a vEdge Cloud router) • 256-bit random value signed by the vEdge router's private key

3. Cisco vManage compares the serial and chassis numbers to the list in its vEdge authorized device list file. The numbers must match one of the number pairs in the file. If there is no match, Cisco vManage the vManage NMS tears down the DTLS connection.

4. Cisco vManage checks that the signing of the 256-bit random value is proper. It does this using the vEdge router's public key, which it extracts from the router's board ID certificate. If the signing is not correct, Cisco vManage tears down the DTLS connection.

5. Cisco vManage uses the root CA chain from the vEdge routers board ID certificate to validate that the board ID certificate is itself valid. If the certificate is not valid, Cisco vManage tears down the DTLS connection.

After performing these three checks, Cisco vManage knows that vEdge router is valid, and its authentication of the router is complete.

When the two-way authentication succeeds, Cisco vManage server sends the configuration file to the vEdge router. When the vEdge router receives the configuration file, it activates its full configuration and starts advertising prefixes to Cisco vSmart Controller.
Authentication between Cisco vSmart Controller and the vEdge Router

The last step in the automatic authentication process is for Cisco vSmart Controller and the vEdge router to authenticate each other. In this step, Cisco vSmart Controller performs authentication to ensure that the vEdge router belongs in its network, and the vEdge router also authenticates Cisco vSmart Controller. When the authentication completes, the DTLS connection between the two devices becomes permanent, and Cisco vSmart Controller establishes an OMP peering session running over the DTLS connection. Then, the vEdge router starts sending data traffic over the Cisco SD-WAN overlay network.

In this section below, is a more detailed step-by-step description of how the automatic authentication occurs between Cisco vSmart Controller and a vEdge router.

To initiate a session between Cisco vSmart Controller and a vEdge router, one of the two devices initiates an encrypted DTLS connection to the other. The encryption is provided by RSA. Each device automatically generates an RSA private key–public key pair when it boots.

The authentication between Cisco vSmart Controller and a vEdge router is a two-way process that occurs in parallel. Let's start our discussion with how Cisco vSmart Controller authenticates a vEdge router:

1. Cisco vSmart Controller sends a challenge to the vEdge router. The challenge is a 256-bit random value.

2. The vEdge router sends a response to the challenge that includes the following: • vEdge serial number • vEdge chassis number • vEdge board ID certificate • 256-bit random value signed by the vEdge router's private key

3. Cisco vSmart Controller compares the serial and chassis numbers to the list in its vEdge authorized device list file. The numbers must match one of the number pairs in the file. If there is no match, Cisco vSmart Controller tears down the DTLS connection.

4. Cisco vSmart Controller checks that the signing of the 256-bit random value is proper. It does this using the vEdge router's public key, which it extracts from the router's board ID certificate. If the signing is not correct, Cisco vSmart Controller tears down the DTLS connection.

5. Cisco vSmart Controller uses the root CA chain from the vEdge routers board ID certificate to validate that the board ID certificate is itself valid. If the certificate is not valid, Cisco vSmart Controller tears down the DTLS connection.

6. Cisco vSmart Controller compares the response with the original challenge. If the response matches the challenge that Cisco vBond Orchestrator issued, authentication between the two devices occurs. Otherwise, Cisco vSmart Controller tears down the DTLS connection.
After performing these three checks, Cisco vSmart Controller knows that vEdge router is valid, and its authentication of the router is complete.

In the other direction, the vEdge router authenticates Cisco vSmart Controller:

1. Cisco vSmart Controller sends its trusted root CA signed certificate to the vEdge router.

2. The vEdge router uses its chain of trust to extract Cisco vSmart Controller's serial number from the certificate. The number must match one of the numbers in the vSmart authorized serial number file. If there is no match, the vEdge router tears down the DTLS connection.

3. The Edge router uses its chain of trust to extract the organization name from the certificate and compares it to the organization name that is configured on the vEdge router. If the two organization names match, the vEdge router knows that the organization of Cisco vSmart Controller is proper. If they do not match, the vEdge router tears down the DTLS connection.

4. The vEdge router uses the root CA chain to verify that the certificate has indeed been signed by the root CA (either Symantec or the enterprise CA). If the signature is correct, the vEdge router knows that the certificate itself is valid. If the signature is incorrect, the vEdge router tears down the DTLS connection.
After performing these three checks, the vEdge authentication of Cisco vSmart Controller is complete. The DTLS connection that is used for authentication now becomes a permanent (nontransient) connection, and the two devices establish an OMP session over it that is used to exchange control plane traffic.

This authentication procedure repeats for each Cisco vSmart Controller and each vEdge router that you introduce into the overlay network.

Each vEdge router in the network must connect to at least one Cisco vSmart Controller. That is, a DTLS connection must be successfully established between each vEdge router and one Cisco vSmart Controller. The Cisco SD-WAN network has the notion of a domain. Within a domain, it is recommended that you have multiple Cisco vSmart Controllers for redundancy. Then each vEdge router can connect to more than one Cisco vSmart Controller.

Over the OMP session, a vEdge router relays various control plane–related information to Cisco vSmart Controller so that Cisco vSmart Controller can learn the network topology:

- The vEdge router advertises the service-side prefixes and routes that it has learned from its local static and dynamic (BGP and OSPF) routing protocols.
- Each vEdge router has a transport address, called a TLOC, or transport location, which is the address of the interface that connects to the WAN transport network (such as the Internet) or to the NAT gateway that connects to the WAN transport. Once the DTLS connection comes up between the vEdge router and Cisco vSmart Controller, OMP registers the TLOCs with Cisco vSmart Controller.
- The vEdge router advertises the IP addresses of any services that are located on its service-side network, such as firewalls and intrusion detection devices.

Cisco vSmart Controller installs these OMP routes in its routing database and advertises them to the other vEdge routers in the Cisco SD-WAN overlay network. Cisco vSmart Controller also updates the vEdge router with the OMP route information that it learns from other vEdge routers in the network. Cisco vSmart Controller can apply inbound policy on received routes and prefixes before installing them into its routing table, and it can apply outbound policy before advertising routes from its routing table.
Firewall Ports for Cisco SD-WAN Deployments

This article describes which ports Cisco SD-WAN devices use. If your network has firewall devices, you must open these ports on the firewalls so that devices in the Cisco SD-WAN overlay network can exchange traffic.

Cisco SD-WAN-Specific Port Terminology

By default, all Cisco vEdge devices use base port 12346 for establishing the connections that handle control and traffic in the overlay network. Each device uses this port when establishing connections with other Cisco vEdge devices.

Port Offset

When multiple Cisco vEdge devices are installed behind a single NAT device, you can configure different port numbers for each device so that the NAT can properly identify each individual device. You do this by configuring a port offset from the base port 12346. For example, if you configure a device with a port offset of 1, that device uses port 12347. The port offset can be a value from 0 through 19. The default port offset is 0.

For NAT devices that can differentiate among the devices behind the NAT, you do not need to configure the port offset.

Port Hopping

In the context of a Cisco SD-WAN overlay network, port hopping is the process by which devices try different ports when attempting to establish connections with each other, in the event that a connection attempt on the first port fails. After such a failure, the port value is incremented and the connection attempt is retried. The software rotates though a total of five base ports, waiting longer and longer between each connection attempt.

If you have not configured a port offset, the default base port is 12346, and port hopping is done sequentially among ports 12346, 12366, 12386, 12406, and 12426, and then returning to port 12346.

If you have configured a port offset, that initial port value is used and the next port is incremented by 20. For example, for a port configured with an offset of 2, port hopping is done sequentially among ports 12348, 12368, 12388, 12408, and 12428, and then returning to port 12348.

Incrementing the ports by 20 ensures that there is never any overlap among the possible base port numbers.

Cisco vEdge devices use port hopping when attempting to establish connections to Cisco vManage, Cisco vBond Orchestrator, and Cisco vSmart Controllers. You can also manually request a Cisco vEdge device to port-hop.

Cisco vSmart Controllers and Cisco vManage instances are normally installed behind a properly behaving NAT device, so port hopping is generally not needed and generally does not occur on these devices.

Cisco vBond Orchestrators always connect to other Cisco vEdge devices using port 12346. They never use port hopping.

To describe how port hopping works, we use as an example a Cisco vEdge device with the default base port of 12346. When a router has attempted to connect to another Cisco vEdge device but the connection does not succeed within a certain time, the router hops to the next base port and tries establishing the connection on that port.
If the first connection attempt on the initial base port does not succeed after about 1 minute, the router hops to port 12366. After about 2 minutes, it hops to port 12386; after about 5 minutes, it hops to port 12406; and after about 6 minutes, it hops to port 12426. Then the cycle returns to initial port, 12346.

With a full-cone NAT device, the source ports for all connections initiated by a given Cisco vEdge device remain consistent across all sessions initiated by the Cisco vEdge device. For example, if the router initiates a session with public source port 12346, this is the port used for all communication.

**Effects of Port Hopping**

Cisco vEdge devices use port hopping to make every attempt to keep the control plane of the overlay network up and operational. If a controller device—Cisco vBond Orchestrator, Cisco vManage, or Cisco vSmart Controller—goes down for any reason and the Cisco vEdge devices remain up, when the controller device comes back up, the connection between it and the Cisco vEdge device might shut down and restart, and in some cases the BFD sessions on the Cisco vEdge device might shut down and restart. This behavior occurs because of port hopping: When one device loses its control connection to another device, it port hops to another port in an attempt to re-establish the connection.

Two examples illustrate when this might occur:

- When Cisco vBond Orchestrator crashes, Cisco vManage might take down all connections to the Cisco vEdge devices. The sequence of events that occurs is as follows: When Cisco vBond Orchestrator crashes, Cisco vManage might lose or close all its control connections. Cisco vManage then port hops, to try to establish connections to the Cisco vSmart Controllers on a different port. This port hopping on Cisco vManage shuts down and then restarts all its control connections, including those to the Cisco vEdge devices.

- All control sessions on all Cisco vSmart Controllers go down, and BFD sessions on the Cisco vEdge devices remain up. When any one of the Cisco vSmart Controllers comes back up, the BFD sessions on the routers go down and then come back up because the Cisco vEdge devices have already port hopped to a different port in an attempt to reconnect to Cisco vSmart Controllers.

**Ports Used by Cisco vEdge devices**

When a Cisco vEdge device joins the overlay network, it establishes DTLS control plane connections with the controller devices—Cisco vBond Orchestrator, Cisco vManage, and Cisco vSmart Controller. The router uses these control connections to learn the location of Cisco vSmart Controller from Cisco vBond Orchestrator, to receive its configuration from Cisco vManage, and to receive its policy and any policy updates from Cisco vSmart Controller. When initially establishing these DTLS connections, the Cisco vEdge device uses the base port 12346. If it is unable to establish a connection using this base port, it port-hops through ports 12366, 12386, 12406, and 12426, returning, if necessary, to 12346, until it successfully establishes the DTLS connections with the three controller devices. This same port number is used to establish the IPsec connections and BFD sessions to the other Cisco vEdge devices in the overlay network. Note that if the vEdge configuration...
includes a port offset, the base port number and the four sequential port numbers are incremented by the configured offset.

To see which port DTLS and BFD are using for the control and data connections, look at the Private Port column in the output of the `show control local-properties` command. The command output also shows the public port number that the interface is using. If the WAN port of the Cisco vEdge device is not connected to a NAT device, the private and public port numbers are the same. If a NAT device is present, the port number listed in the Public Port column is the one being used by the NAT device, and it is the port that BFD is using. This public port number is the one remote Cisco vEdge devices use to send traffic to the local site.

If a NAT device is present, the port number listed in the Public Port column is used by the NAT device, and BFD. This public port number is used by remote Cisco vEdge devices to send traffic to the local site.

---

**Note**

If a tunnel interface using a TLOC extension is behind a NAT device of the SD-WAN peer router, the remote site uses port 5063 as a target for BFD.

---

In a network with firewall devices, you must open the Cisco SD-WAN base ports on the firewall devices to allow traffic to flow across the overlay network. You open all the base ports that the Cisco vEdge devices in the network might use, which are the default base ports and the four base ports that the router can port-hop among.

---

**Note**

Port hopping is generally not needed on Cisco vSmart Controllers and on Cisco vManage.

---

For additional details regarding DTLS, TLS, and IPsec ports for SD-WAN device connections, see [Firewall Port Considerations](#).

For Cisco vEdge devices configured to use DTLS tunnels, which use UDP, at a minimum you must open the five base ports that are used by a Cisco vEdge device with a default port offset of 0. Specifically, you open:

- Port 12346
- Port 12366
- Port 12386
- Port 12406
- Port 12426

If you have configured a port offset value on any of the Cisco vEdge devices, you also need to open the ports configured with the port offset value:

- Port (12346 + port offset value)
- Port (12366 + port offset value)
- Port (12386 + port offset value)
- Port (12406 + port offset value)
- Port (12426 + port offset value)
Ports Used by Cisco SD-WAN Devices Running Multiple vCPUs

The Cisco vSmart Controllers can run on a virtual machine (VM) with up to eight virtual CPUs (vCPUs). Cisco vManage can be configured to a minimum of 16 vCPUs, and eight vCPUs are used for control connection ports. The vCPUs are designated as Core0 through Core7.

Each core is allocated separate base ports for control connections. The base ports differ, depending on whether the connection is over a DTLS tunnel (which uses UDP) or a TLS tunnel (which uses TCP).

---

Note
Cisco vBond Orchestrators do not support multiple cores. Cisco vBond Orchestrators always use DTLS tunnels to establish control connections with other Cisco vEdge devices, so they always use UDP. The UDP port is 12346.

The following table lists the port used by each vCPU core for Cisco vManage. Each port is incremented by the configured port offset, if offset is configured.

**Table 17:**

<table>
<thead>
<tr>
<th>Core Number</th>
<th>Ports for DTLS (UDP)</th>
<th>Ports for TLS (TCP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core0</td>
<td>12346</td>
<td>23456</td>
</tr>
<tr>
<td>Core1</td>
<td>12446</td>
<td>23556</td>
</tr>
<tr>
<td>Core2</td>
<td>12546</td>
<td>23656</td>
</tr>
<tr>
<td>Core3</td>
<td>12646</td>
<td>23756</td>
</tr>
<tr>
<td>Core4</td>
<td>12746</td>
<td>23856</td>
</tr>
<tr>
<td>Core5</td>
<td>12846</td>
<td>23956</td>
</tr>
<tr>
<td>Core6</td>
<td>12946</td>
<td>24056</td>
</tr>
<tr>
<td>Core7</td>
<td>13046</td>
<td>24156</td>
</tr>
</tbody>
</table>

Administrative Ports Used by Cisco vManage

Cisco vManage uses the following administrative ports for protocol-specific communication:

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Traffic Direction</th>
<th>Protocol</th>
<th>Port Number</th>
</tr>
</thead>
</table>
| Netconf | Bidirectional
Between Cisco vManage and Cisco vSmart Controllers or Cisco vBond Orchestrators. This port is used in Cisco vManage to establish initial discovery. | TCP      | 830         |
<p>| HTTPS   | Incoming                  | TCP      | 443         |</p>
<table>
<thead>
<tr>
<th>Purpose</th>
<th>Traffic Direction</th>
<th>Protocol</th>
<th>Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP query</td>
<td>Incoming</td>
<td>UDP</td>
<td>161</td>
</tr>
<tr>
<td>SSH</td>
<td>Incoming</td>
<td>TCP</td>
<td>22</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Outgoing</td>
<td>UDP</td>
<td>1812</td>
</tr>
<tr>
<td>SNMP trap</td>
<td>Outgoing</td>
<td>UDP</td>
<td>162</td>
</tr>
<tr>
<td>Syslog</td>
<td>Outgoing</td>
<td>UDP</td>
<td>514</td>
</tr>
<tr>
<td>TACACS</td>
<td>Outgoing</td>
<td>TCP</td>
<td>49</td>
</tr>
</tbody>
</table>

vManage clusters use the following ports for communication among the NMSs that comprise the cluster:

<table>
<thead>
<tr>
<th>vManage Service</th>
<th>Traffic Direction</th>
<th>Protocol</th>
<th>Port Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application server</td>
<td>Bidirectional</td>
<td>TCP</td>
<td>80, 443, 7600, 8080, 8443, 57600</td>
</tr>
<tr>
<td>Configuration database</td>
<td>Bidirectional</td>
<td>TCP</td>
<td>2424, 2434</td>
</tr>
<tr>
<td>Coordination server</td>
<td>Bidirectional</td>
<td>TCP</td>
<td>2181, 3888</td>
</tr>
<tr>
<td>Message bus</td>
<td>Bidirectional</td>
<td>TCP</td>
<td>9092</td>
</tr>
<tr>
<td>Statistics database</td>
<td>Bidirectional</td>
<td>TCP</td>
<td>9200, 9300</td>
</tr>
<tr>
<td>Tracking of device configurations</td>
<td>Bidirectional</td>
<td>TCP</td>
<td>830</td>
</tr>
<tr>
<td>(NCS and Netconf)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Configure the Port Offset**

When two or more Cisco vEdge devices are behind the same full-cone NAT device, one device can use the default port offset, and you should configure a port offset on the remaining devices:

```
Device(config)# system port-offset number
```

The port offset can be a value from 0 through 19. The default port offset is 0.

In the following example, vEdge-1 uses the default port offset of 0, and on vEdge-2 the port offset is set to 1.
In this example:

- vEdge-1 attempts to connect first using base port 12346. If that attempt is not successful, the router attempts port 12366, 12386, 12406, and 12426.

- vEdge-2 has a port offset of 1, so the first port it attempts to connect on is 12347 (12346 plus offset of 1). If it fails to connect using port 12347, the router hops by increments of 20 and attempts to connect on ports 12367, 12387, 12407, and 12427.

**Perform Port Hopping Manually**

You can manually request a Cisco vEdge device to port-hop:

```shell
vEdge# request port-hop
```

One reason to use this command is if the router's control connections are up, but BFD is not starting. The `request port-hop` command restarts the control connections on the next port number, and BFD should then also start.

### Download Software

Cisco SD-WAN software is available on the Cisco website.

For the initial software installation on Cisco vManage instances, Cisco vBond Orchestrators, vEdge Cloud routers, and Cisco vSmart Controllers, all of which run as virtual machines (VMs) on a server, the software is provided as open virtualization (.ova) files, with one file for each device type:

- `vbond-software-release.ova`
- `viptela-edge-software-release.ova`
- `vmanage-software-release.ova`
- `vsmart-software-release.ova`

The software release is identified with three numeric fields (such as 16.1.0).

Hardware vEdge routers ship with software already installed, so you do not need to download a software image when you are first installing the routers.
To download the Cisco SD-WAN software:

2. Click Downloads.
3. Select the software release version.
4. Click the desired .ova software image file to download it. (Note that the .tar files are software bundles that you use only when upgrading the software. They are not required for initial software installation.)
5. Copy the software image to the desired HTTP or FTP file server in your local network.

**Deploy Cisco vManage**

The Cisco vManage is a centralized network management system that provides a GUI interface to easily monitor, configure, and maintain all Cisco vEdge devices and links in the overlay network. The Cisco vManage runs as a virtual machine (VM) on a network server.

An SD-WAN overlay network can be managed by one Cisco vManage, or it can managed by a cluster, which consists of a minimum of three Cisco vManage instances. It is recommended that you build a network, especially a larger network, with a vManage cluster. The Cisco vManage manages all the Cisco vEdge devices in the overlay network, providing dashboard and detailed views of device operation, and controlling device configurations and certificates.

To deploy Cisco vManage instances:

1. Create a vManage VM instance, either on an ESXi or a KVM hypervisor.
2. Create either a minimal or a full configuration for each of the Cisco vManage instance. You can configure Cisco vManage by creating a device configuration template, or you can use SSH to open a CLI session and then manually configure Cisco vManage. If you create the configuration manually and if you later create a device configuration template and attach it to Cisco vManage, the existing configuration on Cisco vManage is overwritten. Note that you must configure each Cisco vManage in the cluster individually, from that vManage server itself. You cannot create a vManage configuration template on one vManage server and attach other Cisco vManage to that device template.
3. Configure certificate settings and generate a certificate for the Cisco vManage.
4. Create a vManage cluster.

**vManage Web Server Ciphers**

In Releases 16.3.0 and later, vManage web servers support the following ciphers:

- TLS_DHE_DSS_WITH_AES_128_GCM_<wbr/>SHA256
- TLS_DHE_DSS_WITH_AES_256_GCM_<wbr/>SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_<wbr/>SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_<wbr/>SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_<wbr/>GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_<wbr/>GCM_SHA384
Create vManage VM Instance on ESXi

To run Cisco vManage, you must create a virtual machine (VM) instance for it on a server that is running hypervisor software. This topic describes how to create a virtual machine on a server running the VMware vSphere ESXi Hypervisor. You can also create the virtual machine on a server running the Kernel-based Virtual Machine (KVM) hypervisor.

For server requirements, see Server Hardware Recommendations.

To create a Cisco vManage virtual machine instance on an ESXi hypervisor:

1. Start the vSphere Client and create a Cisco vManage VM instance.
2. Create a new virtual disk that has a volume of at least 100 GB for the Cisco vManage database.
3. Add another vNICs.
4. Start the Cisco vManage VM instance and connect to the Cisco vManage console.
5. To create a Cisco vManage cluster, repeat Steps 1 through 4 to create a VM for each Cisco vManage instance.

If you are using the VMware vCenter Server to create the Cisco vManage VM instance, follow the same procedure.

Launch vSphere Client and Create vManage VM Instance

1. Launch the VMware vSphere Client application, and enter the IP address or name of the ESXi server, your username, and your password. Click Login to log in to the ESXi server.
   The system displays the ESXi screen.
2. Click File > Deploy OVF Template to deploy the virtual machine.
3. In the Deploy OVF Template screen, enter the location to install and download the OVF package. This package is the vmanage.ova file that you downloaded from the Support page. Click **Next**.

4. Click **Next** to verify OVF template details.

5. Enter a name for the deployed template and click **Next**.

6. Click **Next** to accept the default format for the virtual disks.

7. From the **Destination Networks** drop-down list, select the destination network for the deployed OVF template, and click **Next**.

8. In the Ready to Complete screen, click **Finish** to complete deployment of the Cisco vManage VM instance.

The system has successfully created the VM instance with the parameters you just defined and displays the vSphere Client screen with the **Getting Started** tab selected. By default, this includes one vNIC. This vNIC is used for the tunnel interface.

**Create a New Virtual Disk**

You must create a new virtual disk with a volume of at least 100 GB for the Cisco vManage database:

1. In the left navigation bar of the vSphere Client screen, select the Cisco vManage VM instance that you just created, and click **Edit** virtual machine settings.

2. In the vManage Virtual Machine Properties screen, click **Add** to add a new virtual disk, and then click **OK**.

3. In the Add Hardware screen, select **Hard Disk** for the device type you want to add to your VM, and click **Next**.

4. In the Select a Disk screen, select **Create a new virtual** disk, and click **Next**.
5. In the Create a Disk screen, specify the disk capacity for the Cisco vManage database to be 100 GB, and click **Next**.

6. In the Advanced Options screen, choose IDE (starting Cisco vManage Release 20.3.1, choose SCSI) for the virtual storage device, and click **Next**. If you are using IDE for release older than Cisco vManage Release 20.3.1, the virtual store device must be IDE.

7. In the Ready to Complete screen, click **Finish** to complete creating a new virtual disk with a capacity of 500 GB.

The system displays the vSphere Client screen with the **Getting Started** tab selected.

### Add Additional vNICs

To add another vNICs for the management interface and for the Message Bus:

1. In the left navigation bar of the vSphere Client, select the Cisco vManage VM instance that you just created, and click **Edit** virtual machine settings.

2. In the Cisco vManage – Virtual Machine Properties screen, click **Add** to add a new vNIC for the management interface. Then click **OK**.

3. Click Ethernet Adapter for the type of device you wish to add. Then click **Next**.

4. In the **Adapter Type** drop-down, select VMXNET3 for the vNIC to add. Then click **Next**.

5. In the Ready to Complete screen, click **Finish**.

6. The Cisco vManage – Virtual Machine Properties screen opens showing that the new vNIC is being added. Click **OK** to return to the vSphere Client screen.

7. If the Cisco vManage instance is part of a cluster, repeat Steps 2 through 6 to create a third vNIC. This vNIC is used for the Message Bus.

### Connect Cisco vManage VM Instance to Cisco vManage Console

1. In the left navigation bar of the vSphere Client, select the Cisco vManage VM instance that you just created, and click **Power on the virtual machine**. The Cisco vManage virtual machine is powered on.

2. Select the **Console** tab, to connect to the Cisco vManage console. The Cisco vManage console is displayed. Log in to Cisco vManage.

3. Select the storage device to use.

4. Select **hdc**, which is the new partition you added for the Cisco vManage database.

5. Confirm that you want to format the new partition, **hdc**. The system then reboots and displays the Cisco vManage instance.

6. To connect to the Cisco vManage instance using a web browser, configure an IP address on the Cisco vManage instance:

   a. Log in to Cisco vManage.

   b. In the management VPN, VPN 512, configure an IP address on interface eth0. Specify an IP address that is reachable on your network. If necessary, add a default route:
7. To connect to the Cisco vManage instance, type the following string in the URL:
   https://ip-address:8443/

8. Log in.

Create vManage VM Instance on KVM

To run Cisco vManage, you must create a virtual machine (VM) instance for it on a server that is running hypervisor software. This topic describes the process for creating a VM on a server running VMware Kernel-based Virtual Machine (KVM) Hypervisor. You can also create the VM on a server running VMware vSphere ESXi Hypervisor.

For server requirements, see Server Hardware Requirements.

Create Cisco vManage VM Instance on the KVM Hypervisor

To create a Cisco vManage VM instance on the KVM hypervisor:

1. Launch the Virtual Machine Manager client application. The system displays the Virtual Machine Manager screen.

2. Click New to deploy the virtual machine. The Create a new virtual machine screen opens.

3. Enter the name of the virtual machine.
   a. Select Import existing disk image radio button.
   b. Click Forward. The virtual disk is imported and associated to the VM instance you are creating.

4. Provide the existing storage path box, click Browse to find the Cisco vManage software image.
   a. In the OS Type field, select Linux.
   b. In the Version field, select the Linux version that you are running.
   c. Click Forward.

5. Specify Memory and CPU based on your network topology and number of sites, and click Forward.

6. Select Customize configuration before install, and click Finish.

7. Select Disk 1 in the left navigation bar.
   a. Click Advanced Options.
   b. In the Disk Bus field, choose IDE (starting Cisco vManage Release 20.3.1, choose SCSI).
   c. In the Storage Format field, choose qcow2.
d. Click **Apply** to create the VM instance with the parameters you defined. By default, this VM instance includes one vNIC, which is used for the tunnel interface.

---

**Note**

Cisco SD-WAN supports only VMXNET3 vNICs.

8. In the Cisco vManage Virtual Machine window, click **Add Hardware** to add a new virtual disk for the Cisco vManage database.

9. In the Add New Virtual Hardware screen, specify the following for the new virtual disk:
   a. In Create a disk image on the computer's hard drive, specify the disk capacity for the Cisco vManage database to be 100GB.
   b. In the **Device Type** field, specify IDE disk (starting Cisco vManage Release 20.3.1, specify SCSI disk) for the virtual storage.
   c. In the **Storage Format** field, specify *qcow2*.
   d. Click **Finish** to complete the creation of a new virtual disk with a capacity of 100 GB.

10. In the Cisco vManage Virtual Machine screen, click **Add Hardware** to add another vNIC for the management interface.

11. In the Add New Virtual Hardware screen, click **Network**.
   a. In the **Host Device** field, select an appropriate host device.
   b. Click **Finish**.

   The newly created vNIC is listed in the left pane. This vNIC is used for the management interface.

12. If the Cisco vManage instance is a part of a cluster, repeat Steps 10 and 11 to create a third vNIC. This vNIC is used for the Message Bus.

13. In the Cisco vManage Virtual Machine screen click **Begin Installation** in the top upper-left corner of the screen.

14. The system creates the virtual machine instance and displays the Cisco vManage console.

15. At the login prompt, log in with the default username, which is **admin**, and the default password, which is **admin**. The system prompts you to select the storage device to use.

16. Select **hdc**, which is the new partition you added for the vManage database.

17. Confirm that you want to format the new partition, **hdc**. The system reboots and displays the Cisco vManage instance.

18. To create a Cisco vManage cluster, repeat Steps 1 through 17 to create a VM for each Cisco vManage instance.

---

**Connect to a Cisco vManage Instance**

To connect to a Cisco vManage instance using a web browser, configure an IP address on the Cisco vManage instance:
1. Log in with the default username and password:

   Login: admin password: admin

2. In the management VPN, VPN 512, configure an IP address on interface eth0. Specify an IP address that is reachable on your network. If necessary, add a default route:

   ```
   # config
   (config)# vpn 512
   (config)# ip route prefix/length next-hop-ip-address
   (config-vpn-512)# interface eth0
   (config-interface-eth0)# ip address ip-address
   (config-interface-eth0)# no shutdown
   (config-interface-eth0)# command and-quit
   #
   ``

3. To connect to the vManage instance, type the following string in the URL:

   ```
   https://ip-address:8443
   ```

4. Log in with the username admin and the password admin.

---

**Create Configuration Templates for Cisco vManage**

You should create configuration templates for Cisco vManage.

**Configuration Prerequisites**

**Security Prerequisites**

Before you can configure Cisco vManage in the Cisco SD-WAN overlay network, you must have generated a certificate for it, and the certificate must already be installed on the device. See Generate a Certificate.

**Variables Spreadsheet**

The feature templates that you create will contain variables. For Cisco vManage to populate the variables with actual values when you attach a device template to a device, either enter the values manually or click Import File in the upper right corner to load an Excel file in CSV format that contains the variables values.

In the spreadsheet, the header row contains the variable name and each row after that corresponds to a device, defining the values of the variables. The first three columns in the spreadsheet must be (in order):

- csv-deviceId—Serial number of the device (used to uniquely identify the device).
- csv-deviceIP—System IP address of the device (used to populate the system ip address command).
- csv-host-name—Hostname of the device (used to populate the system hostname command).

You can create a single spreadsheet for all devices in the overlay network—Cisco vManages, routers, Cisco vSmart Controllers, and Cisco vBond Orchestrators. You do not need to specify values for all variables for all devices.

**Feature Templates for Cisco vManages**

-->

---
The following features are mandatory for Cisco vManage operation, so you must create a feature template for each of them:

Table 18:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Template Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication, Authorization, and Accounting (AAA)</td>
<td>AAA</td>
</tr>
<tr>
<td>Security</td>
<td>Security</td>
</tr>
<tr>
<td>System-wide parameters</td>
<td>System</td>
</tr>
<tr>
<td>Transport VPN (VPN 0)</td>
<td>VPN, with the VPN ID set to 0.</td>
</tr>
<tr>
<td>Management VPN (for out-of-band management traffic)</td>
<td>VPN, with the VPN ID set to 512.</td>
</tr>
</tbody>
</table>

Create Feature Templates

Feature templates are the building blocks of a Cisco vManage's complete configuration. For each feature that you can enable on Cisco vManage, a template form is provided that you fill out with the desired parameters for that feature.

You must create feature templates for the mandatory Cisco vManage features.

You can create multiple templates for the same feature.

To create vManage feature templates:

1. In Cisco vManage, select Configuration > Templates.
2. From the Templates title bar, select Feature.
3. Click Add Template.
4. In the left pane, from Select Devices, select vManage. You can create a single feature template for features that are available on both Cisco vManage and other devices. You must, however, create separate feature templates for software features that are available only on Cisco vManage.
5. In the right pane, select the template. The template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining parameters applicable to that template. Optional parameters are generally grayed out. A plus (+) sign is displayed to the right when you can add multiple entries for the same parameter.
6. Enter a template name and description. These fields are mandatory. You cannot use any special characters in template names.
7. For each required parameter, choose the desired value, and if applicable, select the scope of the parameter. Select the scope from the drop-down menu available to the left of each parameter field.
8. Click the plus sign (+) below the required parameters to set values for additional parameters, if applicable.
9. Click Create.
10. Create feature templates for each of the required features listed in the previous section.
a. For the transport VPN, use the template called VPN-vManage and in the VPN Template section, set the VPN to 0, with a scope of Global.

b. For the management VPN, use the template called VPN-vManage and in the VPN Template section, set the VPN to 512, with a scope of Global.

11. Create any additional feature templates for each optional feature that you want to enable on Cisco vManage.

**Release Information**

Introduced in Cisco vManage in Release 15.3.

**Configure Cisco vManage**

Once you have set up and started the virtual machines (VMs) for Cisco vManage, they come up with a factory-default configuration. You then configure each Cisco vManage instance directly from Cisco vManage server itself, by creating a device configuration template, so that Cisco vManage can be authenticated and verified and can join the overlay network. At a minimum, you must configure the IP address of your network's Cisco vBond Orchestrator, the device's system IP address, and a tunnel interface in VPN 0 to use for exchanging control traffic among the network controller devices (the Cisco vBond Orchestrator, Cisco vManage, and Cisco vSmart Controller devices).

For the overlay network to be operational and for Cisco vManage instances to participate in the overlay network, you must do the following:

- Configure a tunnel interface on at least one interface in VPN 0. This interface must connect to a WAN transport network that is accessible by all Cisco vEdge devices. VPN 0 carries all control plane traffic among the Cisco vEdge devices in the overlay network.

- Ensure that the Overlay Management Protocol (OMP) is enabled. OMP is the protocol responsible for establishing and maintaining the Cisco SD-WAN control plane. OMP is enabled by default, and you cannot disable it. If you edit the configuration from the CLI, do not remove the `omp` configuration command.

**Note**

For a vManage cluster, you must configure each Cisco vManage instance in the cluster individually, from that Cisco vManage server itself. You cannot create Cisco vManage configuration template on one Cisco vManage server and attach other Cisco vManage to that device template.

**Configure Cisco vManage with a Device Configuration Template**

To configure Cisco vManage, create a device configuration template:

1. Configure the address of Cisco vBond Orchestrator:
   a. Select **Administration > Settings**.
   b. Click the **Edit** button to the right of the vBond bar.
c. In the vBond DNS/IP Address: Port field, enter the DNS name that points to Cisco vBond Orchestrator or the IP address of Cisco vBond Orchestrator and the port number to use to connect to it.

d. Click Save.

2. In Cisco vManage, select Configuration > Templates.

3. In the Device tab, click Create Template.

4. From the Create Template drop-down list, select From Feature Template.

5. From the Device Model drop-down list, select vManage. Cisco vManage displays all the feature templates for configuring Cisco vManage. The required feature templates are indicated with an asterisk (*), and the remaining templates are optional. The factory-default template for each feature is selected by default.

6. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

7. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

8. In the System feature template, configure the Site ID, System IP Address, Hostname, Location, Timezone, and GPS Location.

9. In the AAA feature template, in the Local tab, click Users, and change the password for the user "admin".

10. In the VPN feature template, select VPN 0 and configure the system IP address and the address or hostname of a DNS server. If necessary, click the Route tab and add a static route.

11. If you need to add a static route in VPN 512, in a second VPN feature template, select VPN 512, click Route tab, and add the static route.

12. In the VPN-Interface-Ethernet feature template, configure the interface in VPN 0 to use as a tunnel interface to connect to the WAN transport network. In Shutdown, click No, enter the Interface Name, and assign the interface either a dynamic or static address. In the Interface Tunnel tab, in Tunnel Interface, click On. Then assign a color to the tunnel interface, and select the desired services to allow on the tunnel.

**Note**

You must configure a tunnel interface on at least one interface in VPN 0 for the overlay network to come up and for Cisco vManage to be able to participate in the overlay network. This interface must connect to a WAN transport network that is accessible by all Cisco vEdge devices. VPN 0 carries all control plane traffic among the Cisco vEdge devices in the overlay network.

13. In a second VPN-Interface-Ethernet feature template, configure the interface to use as the management interface in VPN 512. In Shutdown, click No, enter the Interface Name, and assign the interface either a dynamic or static address.


15. Optionally, modify the default Archive, Banner, Logging, NTP, and SNMP feature templates. Use the Banner template to configure MOTD and login banners that are displayed when you log in to the device
through the CLI. To create a login banner that is displayed when you log in to the Cisco vManage server, select **Administration > Settings > Banner**.

16. Click **Create**. The new configuration template is displayed in the Device Template table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

17. In the Device Template table, locate the desired device template.

18. Click **More Actions** icon to the right of the row, and select **Attach Devices**.

19. In the **Attach Devices** box, select the local Cisco vManage from the **Available Devices** list, and click the right-pointing arrow to move it to the **Selected Devices** box.

20. Click **Attach**.

**Sample CLI Configuration**

Below is an example of a simple Cisco vManage configuration. Note that this configuration includes a number of settings from the factory-default configuration and shows a number of default configuration values.

```
vManage# show running-config
system
  host-name vManage
  gps-location latitude 40.7127837
  gps-location longitude -74.00594130000002
  system-ip 172.16.255.22
  site-id 200
  organization-name "Cisco"
  clock timezone America/Los_Angeles
vbond 10.1.14.14
aaa
  auth-order local radius tacacs
usergroup basic
  task system read write
  task interface read write
  !
usergroup netadmin
  !
usergroup operator
  task system read
  task interface read
  task policy read
  task routing read
  task security read
  !
user admin
  password encrypted-password
  !
logging
disk
  enable
  !
no shutdown
snmp
  view v2
  oid 1.3.6.1
```
Configure Certificate Settings

New controller devices in the overlay network—Cisco vManage instances, Cisco vBond Orchestrators, and Cisco vSmart Controllers—are authenticated using signed certificates. From Cisco vManage, you can automatically generate the certificate signing requests (CSRs), retrieve the generated certificates, and install them on all controller devices when they are added to the network.

---

Note

All controller devices must have a certificate installed on them to be able to join the overlay network.

To automate the certification generation and installation process, configure the name of your organization and certificate authorization settings before adding the controller devices to the network.

For more information, see Certificates.
**Generate Cisco vManage Certificate**

For Cisco vManage to be able to join the overlay network, you must generate a certificate signing request (CSR) for Cisco vManage instance. Cisco vManage automatically retrieves the generated certificate and installs it.

For more information, see Certificates.

**Create a vManage Cluster**

A vManage cluster is a collection of three or more Cisco vManage instances in a Cisco SD-WAN overlay network domain. The cluster collectively provides network management services to all Cisco vEdge devices in the network. Some of the services, such as determining which vManage instance connects to and handles requests for a router, are distributed automatically, while for others (the statistics and configuration databases, and the messaging server), you configure which Cisco vManage instance handles the service.

For more information, refer to Cluster Management.

**Enable Timeout Value for a vManage Client Session**

By default, a user's session to a Cisco vManage client remains established indefinitely and never times out.

To set how long a Cisco vManage client session is inactive before a user is logged out:

1. In Cisco vManage, navigate to Administration > Settings.
2. Click Edit to the right of the Client Session Timeout bar.
3. In the Session Timeout field, click Enabled.
4. In the Timeout field, enter the timeout value, in minutes. This value can be from 10 to 180 minutes.
5. Click Save.

The client session timeout value applies to all Cisco vManage servers in a Cisco vManage cluster.

**Deploy Cisco vBond Orchestrator**

Cisco vBond Orchestrator is a software module that authenticates the Cisco vSmart Controllers and the vEdge routers in the overlay network and coordinates connectivity between them. It must have a public IP address so that all Cisco vEdge devices in the network can connect to it (it is the only Cisco vEdge device that must have a public address). While the Cisco vBond Orchestrator can be located anywhere in the network, it is strongly recommended that you place it in a DMZ. Assigning a public IP address to the orchestrator allows Cisco vSmart Controllers and vEdge routers that are situated in private address spaces, secured behind different NAT gateways, to establish communication connections with each other. Cisco vBond Orchestrator runs as a VM on a network server.

A Cisco SD-WAN overlay network can have one or more Cisco vBond Orchestrators.

To deploy Cisco vBond Orchestrators:

1. Create a vBond VM instance, either on an ESXi or a KVM hypervisor.
2. Create a minimal configuration for Cisco vBond Orchestrator, to allow it to be accessible on the network. You do this by using SSH to open a CLI session to Cisco vBond Orchestrator and manually configuring the device.

3. Add Cisco vBond Orchestrator to the overlay network so that Cisco vManage is aware of it.

4. If you are hosting Cisco SD-WAN zero-touch-provisioning (ZTP) vBond server in your enterprise, configure one Cisco vBond Orchestrator to perform this role.

5. Create a full configuration for Cisco vBond Orchestrator. You create the initial configuration by using SSH to open a CLI session to Cisco vBond Orchestrator. Then you create the full configuration by creating configuration templates on Cisco vManage and then attaching the templates to Cisco vBond Orchestrator. When you attach the configuration templates to Cisco vBond Orchestrator, the configuration parameters in the templates overwrite the initial configuration.

Create vBond VM Instance on ESXi

To start Cisco vBond Orchestrator, you must create a virtual machine (VM) instance for it on a server that is running hypervisor software. This article describes how to create a VM on a server running the VMware vSphere ESXi Hypervisor. You can also create the VM on a server running the Kernel-based Virtual Machine (KVM) Hypervisor software.

For server information, see Server Hardware Recommendations.

To create a vBond VM instance on the ESXi hypervisor:

1. Launch the vSphere client and Create a vBond VM instance.
2. Add a vNIC for the tunnel interface.
3. Start the vBond VM instance and connect to the console.

The details of each step are provided below.

If you are using the VMware vCenter Server to create the vBond VM instance, follow the same procedure. Note, however, that the vCenter Server screens looks different than the vSphere Client screens shown in the procedure.

Launch vSphere Client and Create a vBond VM Instance

1. Launch the VMware vSphere Client application, and enter the IP address or name of the EXSi server, your username, and your password. Click Login to log in to the ESXi server.
2. Click **File > Deploy OVF Template** to deploy the virtual machine.
3. In the Deploy OVF Template screen, enter the location to install and download the OVF package. This package is the vedge.ova file that you downloaded from Cisco. Then click **Next**.

4. Click **Next** to verify OVF template details.

5. Enter a name for the deployed template and click **Next**. The figure below specifies a name for the vBond instance.

6. Click **Next** to accept the default format for the virtual disks.
7. Click **Next** to accept your destination network name as the destination network for the deployed OVF template. In the figure below, CorpNet is the destination network.
8. In the Ready to Complete screen, click **Finish**. The figure below shows the name for the vBond instance.
The system has successfully created the VM instance with the parameters you just defined and displays the vSphere Client screen with the **Getting Started** tab selected. By default, this includes one vNIC. This vNIC is used for the management interface.

**Add a vNIC for the Tunnel Interface**

1. In the left navigation bar of the vSphere Client, select the vBond VM instance you just created, and click **Edit virtual machine settings**.
2. In the vEdge Cloud – Virtual Machine Properties screen, click Add to add a new vNIC for the management interface. Then click OK.

3. Click Ethernet Adapter for the type of device you wish to add. Then click Next.
4. In the Adapter Type drop-down, select VMXNET3 for the vNIC to add. Then click Next.

5. In the Ready to Complete screen, click Finish.

6. The vEdge Cloud – Virtual Machine Properties screen opens showing that the new vNIC is being added. Click OK to return to the vSphere Client screen.
Start the vBond VM Instance and Connect to the Console

1. In the left navigation bar of the vSphere Client, select the vBond virtual machine instance you created, and click **Power** on the virtual machine. The vBond virtual machine is powered on.
2. Select the **Console** tab to connect to the vBond console.
3. At the login prompt, log in with the default username, which is `admin`, and the default password, which is `admin`.

What's Next

See Configure Cisco vBond Orchestrator.

Create vBond VM Instance on KVM

To start Cisco vBond Orchestrator, you must create a virtual machine (VM) instance for it on a server that is running hypervisor software. This article describes how to create a VM on a server running the Kernel-based Virtual Machine (KVM) Hypervisor. You can also create the VM on a server running the vSphere ESXi Hypervisor software.

For server information, see Server Hardware Recommendations.

To create a vBond VM instance on the KVM hypervisor:

1. Launch the Virtual Machine Manager (virt-manager) client application. The system displays the Virtual Machine Manager screen.
2. Click **New** to deploy the virtual machine. The system opens the Create a new virtual machine screen.

3. Enter the name of the virtual machine. The figure below specifies a name for the vBond instance.
   a. Choose **Import existing disk image** option to install the operating system.
   b. Click **Forward**.

4. For **Provide the existing storage path** field, click **Browse** to find the vBond software image.
   a. In the **OS Type** field, choose **Linux**.
   b. In the **Version** field, choose the Linux version that you are running.
c. Click **Forward**.

5. Specify Memory and CPU based on your network topology and the number of sites, and click **Forward**.

6. Check **Customize configuration before install**. Then click **Finish**.
7. Choose Disk 1 in the left navigation bar. Then:
   a. Click Advanced Options.
   b. In the Disk Bus field, choose IDE.
   c. In the Storage Format field, choose qcow2.
   d. Click Apply to create the VM instance with the parameters you had defined. By default, this includes one vNIC. This vNIC is used for the management interface.

   ![Virtual Machine Configuration](image)

   The software supports only VMXNET3 vNICs.

8. In the vEdge Cloud Virtual Machine screen, click Add Hardware to add a second vNIC for the tunnel interface.

9. In the Add New Virtual Hardware screen, click Network.
   a. In the Host Device field, choose an appropriate Host device.
   b. Click Finish.
The newly created vNIC is listed in the left pane. This vNIC is used for the tunnel interface.

10. In the vBond Virtual Machine screen, click **Begin Installation** in the top upper-left corner of the screen.

11. The system creates the virtual machine instance and displays the vBond console.
In the login screen, log in with the default username, which is `admin`, and the default password, which is `admin`.

**What's Next**

See *Configure Cisco vBond Orchestrator*.

---

## Configure Cisco vBond Orchestrator

Once you have set up and started the virtual machine (VM) for Cisco vBond Orchestrator in your overlay network, Cisco vBond Orchestrator comes up with a factory-default configuration. You then need to manually configure a few basic features and functions so that the devices can be authenticated and verified and can join the overlay network. Among these features, you configure the device as Cisco vBond Orchestrator providing the system IP address, and you configure a WAN interface that connects to the Internet. This interface must have a public IP address so that all Cisco vEdge devices in the overlay network can connect to Cisco vBond Orchestrator.

You create the initial configuration by using SSH to open a CLI session to Cisco vBond Orchestrator.

After you have created the initial configuration, you create the full configuration by creating configuration templates on Cisco vManage and then attach the templates to Cisco vBond Orchestrator. When you attach the configuration templates to Cisco vBond Orchestrator, the configuration parameters in the templates overwrite the initial configuration.

### Create Initial Configuration for Cisco vBond Orchestrator

To create the initial configuration on Cisco vBond Orchestrator using a CLI session:

1. Open a CLI session to Cisco vEdge device via SSH.
2. Log in as the user `admin`, using the default password, `admin`. The CLI prompt is displayed.
3. Enter configuration mode:

   ```
   vBond#config
   vBond(config)#
   ```

4. Configure the hostname:

   ```
   vBond(config)# system host-name hostname
   ```

   Configuring the hostname is optional, but is recommended because this name is included as part of the prompt in the CLI and it is used on various Cisco vManage screens to refer to the device.

5. Configure the system IP address:

   ```
   vBond(config-system)# system-ip ip-address
   ```

   Cisco vManage uses the system IP address to identify the device so that the NMS can download the full configuration to the device.

6. Configure the IP address of Cisco vBond Orchestrator. Cisco vBond Orchestrator's IP address must be a public IP address, to allow all Cisco vEdge devices in the overlay network to reach Cisco vBond Orchestrator:

   ```
   vBond(config-system)# vbond ip-address local
   ```
In Releases 16.3 and later, the address can be an IPv4 or an IPv6 address. In earlier releases, it must be an IPv4 address. A vBond orchestrator is effectively a vEdge router that performs only the orchestrator functions. The local option designates the device to be Cisco vBond Orchestrator, not a vEdge router. Cisco vBond Orchestrator must run on a standalone virtual machine (VM) or hardware router; it cannot coexist in the same device as a software or hardware vEdge router.

7. Configure a time limit for confirming that a software upgrade is successful:

   vBond(config-system)#upgrade-confirm minutes

   The time can be from 1 through 60 minutes. If you configure this time limit, when you upgrade the software on the device, Cisco vManage (when it comes up) or you must confirm that a software upgrade is successful within the configured number of minutes. If the device does not receive the confirmation within the configured time, it reverts to the previous software image.

8. Change the password for the user "admin":

   vBond(config-system)#user admin password password

   The default password is "admin".

9. Configure an interface in VPN 0, to connect to the Internet or other WAN transport network. In Releases 16.3 and later, the IP address can be an IPv4 or an IPv6 address. In earlier releases, it must be an IPv4 address. Ensure that the prefix you configure for the interface contains the IP address that you configure in the vbond local command.

   vBond(config)#vpn 0 interface interface-name
   vBond(config-interface)#ip address ipv4-prefix/length
   vBond(config-interface)#ipv6 address ipv6-prefix/length
   vBond(config-interface)#no shutdown

   The IP address must be a public address so that all devices in the overlay network can reach Cisco vBond Orchestrator.

10. Commit the configuration:

    vBond(config)#commit and-quit

11. Verify that the configuration is correct and complete:

    vBond#show running-config

   After the overlay network is up and operational, create a vBond configuration template on the Cisco vManage that contains the initial configuration parameters. Use the following vManage feature templates:

   - System feature template to configure the hostname, system IP address, and vBond functionality.
   - AAA feature template to configure a password for the "admin" user.
   - VPN Interface Ethernet feature template to configure the interface in VPN 0.

   In addition, it is recommended that you configure the following general system parameters:

   - Organization name, on Cisco vManage Administration > Settings screen.
   - Timezone, NTP servers, and device physical location, from the Configuration > Templates > NTP and System feature configuration template.
• Login banner, from the Configuration > Templates > Banner feature configuration template.

• Logging parameters, from the Configuration > Templates > Logging feature configuration template.

• AAA, and RADIUS and TACACS+ servers, from the Configuration > Templates > AAA feature configuration template.

• SNMP, from the Configuration > Templates > SNMP feature configuration template.

Note: The IP address must be a public address so that all devices in the overlay network can reach Cisco vBond Orchestrator.

**Sample Initial CLI Configuration**

Below is an example of a simple configuration on Cisco vBond Orchestrator. Note that this configuration includes a number of settings from the factory-default configuration and shows a number of default configuration values.

```
vBond# show running-config
system
  host-name vBond
  gps-location latitude 40.7127837
  gps-location longitude -74.00594130000002
  system-ip 172.16.240.161
  organization-name "Cisco"
  clock timezone America/Los_Angeles
  vbond 11.1.1.14 local
  aaa
    auth-order local radius tacacs
    usergroup basic
      task system read write
      task interface read write
    !
    usergroup netadmin
    !
    usergroup operator
    task system read
    task interface read
    task policy read
    task routing read
    task security read
    !
    user admin
      password encrypted-password
    !
    !
    logging
      disk
      enable
    !
    !
    vpn 0
    interface ge0/0
      ip address 11.1.1.14/24
      no shutdown
    !
    ip route 0.0.0.0/0 11.1.1.1
    !
    vpn 512
    interface eth0
      ip dhcp-client
      no shutdown
```
Create Configuration Templates for Cisco vBond Orchestrator

This article describes how to configure Cisco vBond Orchestrators that are being managed by Cisco vManage. These devices must be configured from Cisco vManage. If you configure them directly from the CLI on the router, Cisco vManage overwrites the configuration with the one stored on the NMS system.

**Configuration Prerequisites**

**Security Prerequisites**

Before you can configure Cisco vBond Orchestrators in the Cisco SD-WAN overlay network, you must have generated a certificate for Cisco vBond Orchestrator, and the certificate must already be installed on the device. See Generate a Certificate.

**Variables Spreadsheet**

The feature templates that you create will most likely contain variables. To have Cisco vManage populate the variables with actual values when you attach a device template to a device, either enter the values manually or click Import File in the upper right corner to load an Excel file in CSV format that contains the variables values.

In the spreadsheet, the header row contains the variable name and each row after that corresponds to a device, defining the values of the variables. The first three columns in the spreadsheet must be (in the order listed below):

- csv-deviceId—Serial number of the device (used to uniquely identify the device).
- csv-deviceIP—System IP address of the device (used to populate the system ip address command).
- csv-host-name—Hostname of the device (used to populate the system hostname command).

You can create a single spreadsheet for all devices in the overlay network— routers, Cisco vSmart Controllers, and Cisco vBond Orchestrators. You do not need to specify values for all variables for all devices.

**Feature Templates for Cisco vBond Orchestrators**

The following features are mandatory for Cisco vBond Orchestrator operation, and so creating a feature template for each of them is required:

**Table 19:**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Template Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>AAA</td>
</tr>
<tr>
<td>Security</td>
<td>Security</td>
</tr>
</tbody>
</table>
Create Feature Templates

Feature templates are the building blocks of a Cisco vBond Orchestrator's complete configuration. For each feature that you can enable on Cisco vBond Orchestrator, Cisco vManage provides a template form that you fill out with the desired parameters for that feature.

You must create feature templates for the mandatory Cisco vBond Orchestrator features.

You can create multiple templates for the same feature.

To create vBond feature templates:

1. In Cisco vManage, select Configuration > Templates.
2. From the Templates title bar, select Feature.
3. Click Add Template.
4. In the left pane, from Select Devices, select Cloud router.
5. In the right pane, select the template. The template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining required parameters applicable to that template. Optional parameters are generally grayed out. A plus sign (+) is displayed to the right when you can add multiple entries for the same parameter.
6. Enter a template name and description. These fields are mandatory. You cannot use any special characters in template names.
7. For each required parameter, choose the desired value, and if applicable, select the scope of the parameter. Select the scope from the drop-down menu available to the left of each parameter’s value box.
8. Click the plus sign (+) below the required parameters to set the values for additional parameters, if applicable.
9. Click Create.
10. Create feature templates for each of the required features listed in the previous section.
   a. In the System template, in the top portion, configure all desired parameters except for Controller Groups, Maximum Controllers, and Maximum OMP Sessions. These parameters are specific to routers and have no meaning for Cisco vBond Orchestrator. In the Advanced Options portion, in vBond Only and Local vBond, click On. These two parameters are what instantiate the Cisco vBond Orchestrator.
   b. Create two VPN templates, one for VPN 0 (the VPN that connects to the Internet or other public transport network) and one for VPN 512 (the VPN that handles out-of-band management traffic).
   c. Create AAA and Security templates.
11. Create feature templates for each feature that you want to enable on Cisco vBond Orchestrators:
a. Create Archive and Banner templates

b. Create one Interface Ethernet template for each additional Ethernet interface you want to configure on the Cisco vBond Orchestrator. Do not create any tunnel interfaces, or tunnels of any kind, for Cisco vBond Orchestrators.

Create Device Templates

Device templates contain all or large portions of a device's complete operational configuration. You create device templates by consolidating together individual feature templates. You can also create them by entering a CLI text-style configuration directly on Cisco vManage. You can use both styles of device templates when configuring the Cisco vBond Orchestrator.

To create vBond device templates from feature templates:

1. In Cisco vManage, select Configuration > Templates.
2. From the Templates title bar, select Device.
3. Click Create Template, and from the drop-down list, select From Feature Templates.
4. From the Device Model drop-down list, select a Cloud router.
5. Enter a name and description for the Cisco vBond Orchestrator device template. These fields are mandatory. You cannot use any special characters in template names.
6. From the bar beneath the template name and description, select the desired group of templates.
7. In each section, select the desired template. All required templates are marked with an asterisk (*). Initially, the drop-down list for each template lists the default feature template.
   a. For each required and optional template, select the feature template from the drop-down list. These templates are the ones that you previously created (see Create Feature Templates above). Do not select a BFD or an OMP template for Cisco vBond Orchestrators.
   b. For additional templates, click the plus (+) sign next to the template name, and select the feature template from the drop-down list.
8. Click Create. The new device template is listed in the Templates table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

To create device templates by entering a CLI text-style configuration directly on Cisco vManage:

1. In Cisco vManage, select Configuration > Templates.
2. From the Templates title bar, select Device.
3. Click Create Template, and from the drop-down list, select CLI Template.
4. In the Add Device CLI Template box, enter a template name and description, and select vBond Software.
5. Enter the configuration in the CLI Configuration box, either by typing it, cutting and pasting it, or uploading a file.
6. To convert an actual configuration value to a variable, select the value and click Create Variable. Enter the variable name, and click Create Variable. You can also type the variable name directly, in the format {{variable-name}}; for example, {{hostname}}.

7. Click Add. The right pane on the screen lists the new device template. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "CLI" to indicate that the device template was created from CLI text.

**Attach Device Templates To Cisco vBond Orchestrator**

To configure Cisco vBond Orchestrator, you attach one device template to the orchestrator. You can attach the same template to multiple Cisco vBond Orchestrators simultaneously.

To attach a device template to the Cisco vBond Orchestrator:

1. In Cisco vManage, select Configuration > Templates.
2. From the Templates title bar, select Device.
3. In the right pane, select the desired device template.
4. Click the More Actions icon to the right of the row, and select Attach Devices.
5. In the Attach Devices box, select the desired Cisco vBond Orchestrator from the Available Devices list, and click the right-pointing arrow to move them to the Selected Devices box. You can select one or more orchestrators. Click Select All to choose all listed orchestrator.
6. Click Attach.
7. If the device template contains variables, either enter the values manually or click Import file in the upper right corner to load an Excel file in CSV format that contains the variable values.
8. Click Next.
9. To send the configuration in the device template to the Cisco vBond Orchestrator, click Configure Devices.

**Add Cisco vBond Orchestrator to the Overlay Network**

After you create a minimal configuration for Cisco vBond Orchestrator, you must add it to overlay network by making Cisco vManage aware of Cisco vBond Orchestrator. When you add Cisco vBond Orchestrator, a signed certificate is generated and is used to validate and authenticate the orchestrator.

**Add Cisco vBond Orchestrator and Generate Certificate**

To add Cisco vBond Orchestrator to the network, automatically generate the CSR, and install the signed certificate:

1. In Cisco vManage, select Configuration > Devices.
2. In the Controllers tab, click Add Controller and select vBond.
3. In the Add vBond dialog box:
   a. Enter the vBond management IP address.
   b. Enter the username and password to access Cisco vBond Orchestrator.
   c. Select the Generate CSR checkbox to allow the certificate-generation process to occur automatically.
   d. Click Add.

   Cisco vManage generates the CSR, retrieves the generated certificate, and automatically installs it on Cisco vBond Orchestrator. The new controller device is listed in the Controller table with the controller type, hostname of the controller, IP address, site ID, and other details.
**Verify Certificate Installation**

To verify that the certificate is installed on Cisco vBond Orchestrator:

1. In Cisco vManage, select **Configuration > Devices**.
2. In the Controller table, select the row listing the new device, and check the Certificate Status column to ensure that the certificate has been installed.

![Certificate Status in Cisco vManage](image)

**What's Next**

See **Start the Enterprise ZTP Server**.

---

**Start the Enterprise ZTP Server**

The ZTP server must be configured before the ZTP workflow starts.

If you are hosting the Cisco SD-WAN zero-touch-provisioning (ZTP) Cisco vBond Orchestrator server in your enterprise, you must configure one Cisco vBond Orchestrator to perform this role. This Cisco vBond Orchestrator provides the Cisco vEdge devices in the overlay network with the IP address of your enterprise Cisco vBond Orchestrator and with the enterprise root CA chain. You can think of this Cisco vBond Orchestrator server as a top-level Cisco vBond Orchestrator, analogous to a top-level domain server in the Internet.

If you are using the Cisco SD-WAN ZTP hosted service, there is no need to set up a top-level Cisco vBond Orchestrator.

This section provides step-by-step instructions on how to start the Cisco vBond Orchestrator and perform initial configuration.

**Requirements for ZTP**

To start the Cisco vBond Orchestrator software, you need the following hardware and software components:

- A Cisco vEdge device on which the Cisco vBond Orchestrator software software has been installed or the Cisco vBond Orchestrator VM instance on the hypervisor.
• Appropriate power cables. See the packing list for your hardware platform.

• An enterprise DNS server that has been configured with a record that redirects the URL ztp.cisco.com to your enterprise ZTP server. The recommended URL for this enterprise server is ztp.local-domain.

• Certificate generated as a result of a Certificate Signing Request (CSR).

• Enterprise root CA chain.

• For releases through Cisco SD-WAN Release 20.1.1 on Cisco vEdge devices, a CSV file that contains the Cisco vEdge device chassis information required by the Cisco vBond Orchestrator that is acting as the ZTP server. Each row in the CSV file must contain the following information for each Cisco vEdge device.

  Note Some operating systems, including Microsoft Windows, may add carriage return special characters (such as ^M) at the end of each line in this file. Use a text editor to remove these characters before you upload the file.

  • vEdge router chassis number
  • vEdge router serial number
  • Validity (either valid or invalid)
  • Cisco vBond Orchestrator IP address
  • Cisco vBond Orchestrator port number (entering a value is optional)
  • Organization name as specified in the device certificate
  • Path to the enterprise root certification (entering a value is optional)

• For releases beginning with Cisco SD-WAN Release 20.3.1 on Cisco vEdge devices, a JSON file that contains the router chassis information that the Cisco vBond Orchestrator that acts as the ZTP server requires. This file is extracted from the PNP portal downloaded zip bundled device file. The JSON file contains the following information for each router:

  • Organization name as specified in the device certificate
  • Certificate information
  • Router chassis number
  • Router serial number
  • Validity (either valid or invalid)
  • Cisco vBond Orchestrator IP address
  • Cisco vBond Orchestrator port number (optional)

From Cisco SD-WAN Release 20.4.1, if Multi-Tenancy is enabled in controller profile on the PNP portal, the JSON file also contains the SP Organization Name.

For Cisco SD-WAN Release 20.3.1, download the Chassis ZIP file from the PNP portal and extract the JSON file from it. Use the following command to upload the JSON file to the ZTP server:
Here is an example of a JSON file:

```json
{
    "version": "1.1",
    "organization": "vIPtela Inc Regression",
    "overlay": "vIPtela Inc Regression",
    "root_cert_bundle": "-----BEGIN CERTIFICATE-----
<certificate>
----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<certificate>
----END CERTIFICATE-----",
    "controller_details": {
        "primary_ipv4": "10.0.12.26",
        "primary_port": "12346"
    },
    "chassis_list": [{
        "chassis": "JAE214906FZ",
        "SKU": "ASR1002-HX",
        "HWPID": "ASR1002-HX",
        "serial_list": [{
            "sudi_subject_serial": "JAE214906FX",
            "sudi_cert_serial": "021C0203",
            "HWPID": "ASR1002-HX"}
        }
    }
],
    "timestamp": "2019-10-21 23:40:02.248"
}
```

From Cisco SD-WAN Release 20.3.2, you need not extract the JSON file from the Chassis ZIP file that you download from the PNP portal. Use the `request device-upload chassis-file` command to upload the serialFile.Viptela file downloaded from the PNP portal to the ZTP server. The ZTP server extracts the JSON file from serialFile.Viptela and loads the chassis entries into the database.

```
vBond# request device-upload chassis-file /home/admin/serialFile.viptela
Uploading chassis numbers via VPN 0
Copying ... /home/admin/serialFile.viptela via VPN 0
file: /tmp/tmp.DkaQ18u3aM/viptela_serial_file
PnP
Verifying public key received from PnP against production root cert is_public_key_ok against production root ca: O = Cisco, CN = MMI Signer STG - DEV error 20 at 0 depth lookup:unable to get local issuer certificate
Verifying public key received from PnP against engineering root cert is_public_key_ok against engineering root ca: OK
Signature verified for viptela_serial_file
final file: /tmp/tmp.DkaQ18u3aM/viptela_serial_file
Removing unsigned file (cisco_cert.cer).
Signature verification Succeeded.
Success: Serial file is /tmp/tmp.DkaQ18u3aM/viptela_serial_file
INFO: Input File specified was '/usr/share/viptela/chassis_numbers.tmp'
INFO: Root Cert File is /home/admin/vIPtela Inc Regression.crt
INFO: # of complete chassis entries written: 19
Json to CSV conversion succeeded!
Successfully loaded the chassis numbers file to the database.
```

Optionally, you can configure the Cisco vEdge device information manually using the `request device` command.

### Configuring a Router to be a ZTP Server

To start the top-level Cisco vBond Orchestrator software and perform initial configuration:

1. Boot the Cisco vEdge device.
2. Use a console cable to connect a PC to the Cisco vEdge device.

3. Log in to the Cisco vEdge device using the default username, which is **admin**, and the default password, which is **admin**. The CLI prompt is displayed.

4. Configure the Cisco vEdge device to be a top-level Cisco vBond Orchestrator:

   ```
   vBond# config
   vBond(config)# system vbond
   vBond(config)# system vbond ip-address local ztp-server
   ```

   The IP address must be a public address so that the Cisco vBond Orchestrator is reachable by all vSmart controllers and Cisco vEdge devices through the transport network. The **local** option indicates that this Cisco vEdge device is acting as the Cisco vBond Orchestrator. It is this option that starts the Cisco vBond Orchestrator software process on the Cisco vEdge device. The **ztp-server** option establishes this Cisco vBond Orchestrator as the ZTP server.

5. Configure an IP address for the interface that connects to the transport network:

   ```
   vBond(config)# vpn 0 interface ge slot/port
   vBond(config)# interface ge slot/port
   vBond(config)# ip address prefix/length
   vBond(config)# no shutdown
   ```

6. Commit the configuration:

   ```
   vBond(config)# commit
   ```

7. Exit configuration mode:

   ```
   vBond(config)# exit
   ```

8. Verify that the configuration is correct and complete:

   ```
   vBond# show running-config
   ```

   ```
   system
   host-name vm3
   system-ip 172.16.255.2
   admin-tech-on-failure
   route-consistency-check
   organization-name "Cisco Inc"
   vbond 10.1.15.13 local ztp-server
   ```

9. If the certificate has been signed by your enterprise CA authority, install the chain of trust for the device:

   ```
   vBond# request root-cert-chain install path
   ```

   *path* is the directory path to a local file or a file on a remote device that is reachable via FTP, TFTP, HTTP, or SCP.

10. Install the signed certificate:

    ```
    vBond# request certificate install filepath
    ```

    *filepath* can be one of the following:

    - **filename**—Path to a file in your home directory on the local Cisco Cisco vEdge device.
    - **ftp**: **filepath**—Path to a file on an FTP server.
    - **http:// url/file-path**—Path to a file on a webserver.
    - **scp**: **user@host:file-path**
    - **tftp**: **filepath**—Path to a file on a TFTP server.
11. Upload the JSON file that contains the router chassis information to the ZTP server:

```
vBond# request device-upload chassis-file path
```

`path` is the path to a local file or a file on a remote device that is reachable via FTP, TFTP, HTTP, or SCP.

12. Verify that the list of Cisco vEdge device chassis numbers are present on the Cisco vBond Orchestrator using one of the following commands:

```
vBond# show ztp entries
vBond# show orchestrator valid-devices
```

Here is an example of the configuration of a top-level Cisco vBond Orchestrator:

```
vBond# show running-config vpn 0
interface ge0/0
 ip address 75.1.15.27/24
 !
 no shutdown
 !

vBond# show running-config system
system
 vbond 75.1.15.27 local ztp-server
!
```

What's Next

See Deploy the vSmart Controller.

vContainer Host

The support for vContainer Host is deferred. For more information, refer to deferral notice.

Deploy Cisco vSmart Controller

Cisco vSmart Controller is the brains of the centralized control plane for the Cisco SD-WAN overlay network, maintaining a centralized routing table and centralized routing policy. Once the network is operational, Cisco vSmart Controller effects its control by maintaining a direct DTLS control plane connection to each vEdge router. Cisco vSmart Controller runs as a virtual machine (VM) on a network server.

A Cisco SD-WAN overlay network can have one or more Cisco vSmart Controllers. Cisco vSmart Controllers provide a means to control the flow of data traffic throughout the overlay network. It is recommended that an overlay network have at least two Cisco vSmart Controllers to provide redundancy. A single Cisco vSmart Controller can support up to 2,000 control sessions (that is, up to 2,000 TLOCs). Cisco vManage or vManage cluster can support up to 20 Cisco vSmart Controllers in the overlay network.

To deploy a Cisco vSmart Controller:

1. Create a vSmart VM instance, either on an ESXi or a KVM hypervisor.

2. Create a minimal configuration for the Cisco vSmart Controller, to allow it to be accessible on the network. You do this by using SSH to open a CLI session to Cisco vSmart Controller and manually configuring the device.
3. Add Cisco vSmart Controller to the overlay network so that Cisco vManage is aware of it.

4. Create a full configuration for Cisco vSmart Controller. You do this by creating a vManage template for the Cisco vSmart Controller and attaching that template to the controller. When you attach the vManage template, the initial minimal configuration is overwritten.

Create vSmart VM Instance on ESXi

To start the vSmart controller, you must create a virtual machine (VM) instance for it on a server that is running hypervisor software. This article describes how to create a VM on a server running the VMware vSphere ESXi Hypervisor software. You can also create the VM on a server running the Kernel-based Virtual Machine (KVM) Hypervisor software.

For server requirements, see Server Hardware Recommendations.

To create a vSmart VM instance on the ESXi hypervisor:

1. Launch the vSphere Client and create a vSmart VM instance.
2. Add a vNIC for the management interface.
3. Start the vSmart VM instance and connect to the console.

The details of each step are provided below.

If you are using the VMware vCenter Server to create the vSmart VM instance, follow the same procedure. Note, however, that the vCenter Server screens look different than the vSphere Client screens shown in the procedure.

Launch vSphere Client and Create a vSmart VM Instance

1. Launch the VMware vSphere Client application, and enter the IP address or name of the ESXi server, your username, and your password. Click Login to log in to the ESXi server.

   The system displays the ESXi screen.
2. Click **File > Deploy OVF Template** to deploy the virtual machine.
3. In the Deploy OVF Template screen, enter the location to install and download the OVF package. This package is the vsmart.ova file that you downloaded from Cisco. Then click **Next**.
4. Click **Next** to verify OVF template details.
5. Enter a name for the deployed template and click **Next**. The figure below specifies a name for the vSmart instance.
6. Click **Next** to accept the default format for the virtual disks.
7. Click Next to accept your destination network as the destination network for the deployed OVF template. In the figure below, CorpNet is the destination network.
8. In the Ready to Complete screen, click **Finish**. The figure below shows the name for the vSmart instance.
The system has successfully created the VM instance with the parameters you just defined and displays the vSphere Client screen with the **Getting Started** tab selected. By default, this includes one vNIC. This vNIC is used for the tunnel interface.

**Add a vNIC for the Management Interface**

1. In the left navigation bar of the vSphere Client, select the vManage VM instance you just created, and click **Edit virtual machine settings**.
2. In the vManage – Virtual Machine Properties screen, click Add to add a new vNIC for the management interface. Then click OK.

3. Click Ethernet Adapter for the type of device you wish to add. Then click Next.
4. In the **Adapter Type** drop-down, select VMXNET3 for the vNIC to add. Then click **Next**.

5. In the **Ready to Complete** screen, click **Finish**.

6. The **vManage – Virtual Machine Properties** screen opens showing that the new vNIC is being added. Click **OK** to return to the vSphere Client screen.
Start the vSmart VM Instance and Connect to the Console

1. In the left navigation bar of the vSphere Client, select the virtual machine instance you just created, and click **Power on the virtual machine**. The vSmart virtual machine is powered on.

2. Select the **Console** tab to connect to the vSmart console.
3. At the login prompt, log in with the default username, which is **admin**, and the default password, which is **admin**.

**What's Next**

See *Configure Cisco vSmart Controller*.

Create vSmart VM Instance on KVM

To start the vSmart controller, you must create a virtual machine (VM) instance for it on a server that is running hypervisor software. This article describes how to create a VM on a server running the Kernel-based Virtual Machine (KVM) Hypervisor software. You can also create the VM on a server running the VMware vSphere ESXi Hypervisor software.

For server requirements, see *Server Hardware Recommendations*.

To create a vSmart VM instance on the KVM hypervisor:

1. Launch the Virtual Machine Manager (virt-manager) client application. The system displays the Virtual Machine Manager screen.
2. Click **New** to deploy the virtual machine. The system opens the Create a new virtual machine screen.

3. Enter the name of the virtual machine. The figure below specifies a name for the vSmart instance.
   a. Select **Import existing disk image**.
   b. Click **Forward**.

4. In **Provide the existing storage path** field, click **Browse** to find the vSmart software image.
   a. In the **OS Type** field, select **Linux**.
   b. In the **Version** field, select the Linux version you are running.
c. Click **Forward**.

5. Specify Memory and CPU based on your network topology and the number of sites, and click **Forward**.

6. Select Customize configuration before install. Then click **Finish**.
7. Select Disk 1 in the left navigation bar. Then:
   a. Click Advanced Options.
   b. In the Disk Bus field, select IDE.
   c. In the Storage Format field, select qcow2.
   d. Click Apply to create the VM instance with the parameters you just defined. By default, this includes one vNIC. This vNIC is used for the tunnel interface.

   ![Virtual Machine Manager screenshot showing disk configuration](image)

   **Note**
   The software supports only VMXNET3 vNICs.

8. In the vSmart Virtual Machine screen, click Add Hardware to add a second vNIC for the management interface.

9. In the Add New Virtual Hardware screen, click Network.
   a. In the Host Device field, select an appropriate host device.
   b. Click Finish.
10. In the vSmart Virtual Machine screen, click **Begin Installation** in the top upper-left corner of the screen.

11. The system creates the virtual machine instance and displays the vSmart console.
12. At the login prompt, log in with the default username, which is `admin`, and the default password, which is `admin`.

What's Next
See Configure Cisco vSmart Controller.

Configure the vSmart Controller

Once you have set up and started the virtual machines (VMs) for the vSmart controllers in your overlay network, they come up with a factory-default configuration. You then need to manually configure a few basic features and functions so that the devices can be authenticated and verified and can join the overlay network. These features include the IP address of your network's vBond orchestrator, the device's system IP address, and a tunnel interface in VPN 0 to use for exchanging control traffic among the network controller devices (the vBond, vManage, and vSmart devices).

For the overlay network to be operational and for the vSmart controllers to participate in the overlay network, do the following:

- Configure a tunnel interface on at least one interface in VPN 0. This interface must connect to a WAN transport network that is accessible by all Cisco vEdge devices. VPN 0 carries all control plane traffic among the Cisco vEdge devices in the overlay network.

- Ensure that the Overlay Management Protocol (OMP) is enabled. OMP is the protocol responsible for establishing and maintaining the Cisco SD-WAN control plane. It is enabled by default, and you cannot disable it. When you edit the configuration from the CLI, do not remove the `omp` configuration command.

You create these initial configuration by using SSH to open a CLI session to the the vSmart controller.
After you have created the initial configuration, you create the full configuration by creating configuration templates on the vManage NMS and then attaching them to the vSmart controllers. When you attach the configuration template to the vSmart controllers, the configuration parameters in the templates overwrite the initial configuration.

In this initial configuration, you should assign a system IP address to the vSmart controller. This address, which is similar to the router ID on non-Cisco SD-WAN routers, is a persistent address that identifies the controller independently of any interface addresses. The system IP is a component of the device's TLOC address. Setting the system IP address for a device allows you to renumber interfaces as needed without affecting the reachability of the Cisco vEdge device. Control traffic over secure DTLS or TLS connections between vSmart controllers and vEdge routers and between vSmart controllers and vBond orchestrators is sent over the system interface identified by the system IP address. In the transport VPN (VPN 0), the system IP address is used as the device's loopback address. You cannot use this same address for another interface in VPN 0.

For the overlay network to function properly and predictably, the policies configured on all vSmart controllers must be identical.

Create Initial Configuration for the vSmart Controller

To create the initial configuration on a vSmart controller from a CLI session:

1. Open a CLI session to the Cisco vEdge device via SSH.
2. Log in as the user admin, using the default password, admin. The CLI prompt is displayed.
3. Enter configuration mode:
   ```
   vSmart# config
   vSmart(config)#
   ```
4. Configure the hostname:
   ```
   Cisco(config)# system host-name hostname
   ```
   Configuring the hostname is optional, but is recommended because this name is included as part of the prompt in the CLI and it is used on various vManage NMS screens to refer to the device.
5. Configure the system IP address. In Releases 16.3 and later, the IP address can be an IPv4 or an IPv6 address. In earlier releases, it must be an IPv4 address. Releases 19.1 and later do not allow the configuration of IPv6 unique local addresses. In these releases, configure IPv6 addresses from the FC00::/7 prefix range.
   ```
   vSmart(config-system)# system-ip ip-address
   ```
   The vManage NMS uses the system IP address to identify the device so that the NMS can download the full configuration to the device.
6. Configure the numeric identifier of the site where the device is located:
   ```
   vSmart(config-system)# site-id site-id
   ```
7. Configure the numeric identifier of the domain in which the device is located:
   ```
   vSmart(config-system)# domain-id domain-id
   ```
8. Configure the IP address of the vBond orchestrator or a DNS name that points to the vBond orchestrator. The vBond orchestrator's IP address must be a public IP address, to allow all Cisco vEdge devices in the overlay network to reach it.

   vSmart(config-system)# vbond (dns-name | ip-address)

9. Configure a time limit for confirming that a software upgrade is successful:

   vSmart(config-system)# upgrade-confirm minutes

   The time can be from 1 through 60 minutes. If you configure this time limit, when you upgrade the software on the device, the vManage NMS (when it comes up) or you must confirm that a software upgrade is successful within the configured number of minutes. If the device does not receive the confirmation within the configured time, it reverts to the previous software image.

10. Change the password for the user "admin":

    vSmart(config-system)# user admin password password

    The default password is "admin".

11. Configure an interface in VPN 0 to be used as a tunnel interface. VPN 0 is the WAN transport VPN, and the tunnel interface carries the control traffic among the devices in the overlay network. The interface name has the format eth number. You must enable the interface and configure its IP address, either as a static address or as a dynamically assigned address received from a DHCP server. In Releases 16.3 and later, the address can be an IPv4 or an IPv6 address, or you can configure both to enable dual-stack operation. In earlier releases, it must be an IPv4 address.

    vSmart(config)# vpn 0
    vSmart(config-vpn-0)# interface interface-name
    vSmart(config-interface)# (ip dhcp-client | ip address prefix/length)
    vSmart(config-interface)# (ipv6 address ipv6-prefix/length | ipv6 dhcp-client [dhcp-distance number | dhcp-rapid-commit])
    vSmart(config-interface)# no shutdown
    vSmart(config-interface)# tunnel-interface
    vSmart(config-tunnel-interface)# allow-service netconf

    **Note**

    You must configure a tunnel interface on at least one interface in VPN 0 in order for the overlay network to come up and for the vSmart controller to be able to participate in the overlay network. This interface must connect to a WAN transport network that is accessible by all Cisco vEdge devices. VPN 0 carries all control plane traffic among the Cisco vEdge devices in the overlay network.

12. Configure a color for the tunnel to identify the type of WAN transport. You can use the default color (default), but you can also configure a more appropriate color, such as mpls or metro-ethernet, depending on the actual WAN transport.

    vSmart(config-tunnel-interface)# color color

13. Configure a default route to the WAN transport network:

    vSmart(config-vpn-0)# ip route 0.0.0.0/0 next-hop

14. Commit the configuration:

    vSmart(config)# commit and-quit
    vSmart#

15. Verify that the configuration is correct and complete:
After the overlay network is up and operational, create a vSmart configuration template on the vManage NMS that contains the initial configuration parameters. Use the following vManage feature templates:

- System feature template to configure the hostname, system IP address, and vBond functionality.
- AAA feature template to configure a password for the "admin" user.
- VPN Interface Ethernet feature template to configure the interface, default route, and DNS server in VPN 0.

In addition, it is recommended that you configure the following general system parameters:

- Organization name, on the vManage Administration ► Settings screen.
- Timezone, NTP servers, and device physical location, from the Configuration ► Templates ► NTP and System feature configuration templates.
- Login banner, from the Configuration ► Templates ► Banner feature configuration template.
- Logging parameters, from the Configuration ► Templates ► Logging feature configuration template.
- AAA, and RADIUS and TACACS+ servers, from the Configuration ► Templates ► AAA feature configuration template.
- SNMP, from the Configuration ► Templates ► SNMP feature configuration template.

### Sample Initial CLI Configuration

Below is an example of a simple configuration on a vSmart controller. Note that this configuration includes a number of settings from the factory-default configuration and shows a number of default configuration values.

```bash
vSmart# show running-config
system
  host-name vSmart
gps-location latitude 40.7127837
gps-location longitude -74.00594130000002
system-ip 172.16.240.172
site-id 200
organization-name "Cisco"
clock timezone America/Los_Angeles
upgrade-confirm 15
vbond 184.122.2.2
aaa
  auth-order local radius tacacs
usergroup basic
    task system read write
    task interface read write
  !
usergroup netadmin
  !
usergroup operator
  task system read
task interface read
task policy read
task routing read
task security read
  !
user admin
```
Configure the vSmart Controller

password encrypted-password
!
logging
disk	enable
!
server 192.168.48.11
    vpn 512
    priority warm
exit
!
omp
    no shutdown
    graceful-restart
!
snmp
    no shutdown
    view v2
    oid 1.3.6.1
!
    community private
    view v2
    authorization read-only
!
    trap target vpn 0 10.0.1.1 16662
    group-name Cisco
    community-name private
!
    trap group test
    all
    level critical major minor
exit
!
vpn 0
    interface eth1
    ip address 10.0.12.22/24
    tunnel-interface
color public-internet
    allow-service dhcp
    allow-service dns
    allow-service icmp
    no allow-service sshd
    allow-service netconf
    no allow-service ntp
    no allow-service stun
!
    no shutdown
!
vpn 512
    interface eth0
    ip dhcp-client
    no shutdown
!
!
What's Next

See Add the vSmart Controller to the Overlay Network.
Create Configuration Templates for Cisco vSmart Controller

For Cisco vSmart Controllers that are being managed by a Cisco vManage, you must configure them from Cisco vManage. If you configure them directly from the CLI on Cisco vSmart Controller, Cisco vManage overwrites the configuration with the one stored on vManage.

Configuration Prerequisites

Security Prerequisites

Before you can configure Cisco vSmart Controllers in the Cisco overlay network, you must have generated a certificate for Cisco vSmart Controller, and the certificate must already be installed on the device. See Generate a Certificate.

Variables Spreadsheet

The feature templates that you create will most likely contain variables. To have Cisco vManage populate the variables with actual values when you attach a device template to a device, either enter the values manually or click Import File in the upper right corner to load an Excel file in CSV format that contains the variables values.

In the spreadsheet, the header row contains the variable name and each row after that corresponds to a device, defining the values of the variables. The first three columns in the spreadsheet must be (in order):

- csv-deviceId—Serial number of the device (used to uniquely identify the device).
- csv-deviceIP—System IP address of the device (used to populate the system ip address command).
- csv-host-name—Hostname of the device (used to populate the system hostname command).

You can create a single spreadsheet for all devices in the overlay network— routers, Cisco vSmart Controllers, and Cisco vBond Orchestrators. You do not need to specify values for all variables for all devices.

Feature Templates for Cisco vSmart Controllers

The following features are mandatory for Cisco vSmart Controller operation, so you must create a feature template for each of them:

Table 20:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Template Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication, Authorization, and Accounting (AAA)</td>
<td>AAA</td>
</tr>
<tr>
<td>Overlay Management Protocol (OMP)</td>
<td>OMP</td>
</tr>
<tr>
<td>Security</td>
<td>Security</td>
</tr>
<tr>
<td>System-wide parameters</td>
<td>System</td>
</tr>
<tr>
<td>Transport VPN (VPN 0)</td>
<td>VPN with the VPN ID set to 0</td>
</tr>
<tr>
<td>Management VPN (for out-of-band management traffic)</td>
<td>VPN with the VPN ID set to 512</td>
</tr>
</tbody>
</table>
Create Feature Templates

Feature templates are the building blocks of Cisco vSmart Controller's complete configuration. For each feature that you can enable on Cisco vSmart Controller, Cisco vManage provides a template form that you fill out with the desired parameters for that feature.

You must create feature templates for the mandatory Cisco vSmart Controller features. You can create multiple templates for the same feature.

To create vSmart feature templates:

1. In Cisco vManage, select Configuration > Templates.
2. From the Templates title bar, select Feature.
3. Click Add Template.
4. In the left pane, from Select Devices, select vSmart. You can create a single feature template for features that are available on both Cisco vSmart Controllers and other devices. You must, however, create separate feature templates for software features that are available only on Cisco vSmart Controllers.
5. In the right pane, select the template. The template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining parameters applicable to that template. Optional parameters are generally grayed out. A plus sign (+) is displayed to the right when you can add multiple entries for the same parameter.
6. Enter a template name and description. These fields are mandatory. You cannot use any special characters in template names.
7. For each required parameter, choose the desired value, and if applicable, select the scope of the parameter. Select the scope from the drop-down menu to the left of each parameter field.
8. Click the plus sign (+) below the required parameters to set values for additional parameters, if applicable.
9. Click Create.
10. Create feature templates for each of the required features listed in the previous section. For the transport VPN, use the template called VPN-vSmart and in the VPN Template section, set the VPN to 0, with a scope of Global. For the management VPN, use the template called VPN-vSmart and in the VPN Template section, set the VPN to 512, with a scope of Global.
11. Create any additional feature templates for each optional feature that you want to enable on Cisco vSmart Controllers.

Create Device Templates

Device templates contain a device's complete operational configuration. You create device templates by consolidating together individual feature templates. You can also create them by entering a CLI text-style configuration directly on Cisco vManage.

You can attach only one device template to configure a Cisco vSmart Controller, so it must contain, at a minimum, all the required portions of the vSmart configuration. If it does not, the Cisco vManage returns an error message. If you attach a second device template to the Cisco vSmart Controller, it overwrites the first one.

To create device templates from feature templates:

1. In Cisco vManage, select Configuration > Templates.
2. From the **Templates** title bar, select **Device**.

3. Click **Create Template**, and from the drop-down list select **From Feature Templates**.

4. From the **Device Model** drop-down list, select **vSmart**.

5. Enter a name and description for the vSmart device template. These fields are mandatory. You cannot use any special characters in template names.

6. Complete the **Required Templates** section. All required templates are marked with an asterisk.
   a. For each required template, select the feature template from the drop-down list. These templates are the ones that you previously created (see Create Feature Templates above). After you select a template, the circle next to the template name turns green and displays a green check mark.
   b. For templates that have Sub-Templates, click the plus (+) sign or the Sub-Templates title to display a list of sub-templates. As you select a sub-template, the name of the sub-template along with a drop-down is displayed. If the sub-template is mandatory, its name is marked with an asterisk.
   c. Select the desired sub-template.

7. Complete the **Optional Templates** section, if required. To do so:
   a. Click **Optional Templates** to add optional feature templates to the device template.
   b. Select the template to add.
   c. Click the template name and select a specific feature template.

8. Click **Create**. The new device template is listed in the Templates table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

To create device templates by entering a CLI text-style configuration directly on Cisco vManage:

1. In Cisco vManage, select **Configuration > Templates**.

2. From the **Templates** title bar, select **Device**.

3. Click **Create Template**, and from the drop-down list, select **CLI Template**.

4. In the **Add Device CLI Template** box, enter a template name and description, and select **vSmart**.

5. Enter the configuration in the **CLI Configuration** box, either by typing it, cutting and pasting it, or uploading a file.

6. To convert an actual configuration value to a variable, select the value and click **Create Variable**. Enter the variable name, and click **Create Variable**. You can also type the variable name directly, in the format `{{variable-name}}`; for example, `{{hostname}}`.

7. Click **Add**. The right pane on the screen lists the new device template. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "CLI" to indicate that the device template was created from CLI text.

**Attach a Device Template To Cisco vSmart Controllers**

To configure a Cisco vSmart Controller, you attach one device template to the controller. You can attach the same template to multiple Cisco vSmart Controllers simultaneously.
To attach a device template to Cisco vSmart Controllers:

1. In Cisco vManage, select Configuration > Templates.
2. From the Templates title bar, select Device.
3. In the right pane, select the desired device template.
4. Click the More Actions icon to the right of the row, and select Attach Devices.
5. In the Attach Devices box, select the desired Cisco vSmart Controller from the Available Devices list, and click the right-pointing arrow to move them to the Selected Devices box. You can select one or more controllers. Click Select All to choose all listed controllers.
6. Click Attach.
7. If the device template contains variables, either enter the values manually or click Import file in the upper right corner to load an Excel file in CSV format that contains the variable values.
8. Click Next.
9. To preview the configuration that is about to be sent to Cisco vSmart Controller, in the left pane, click the device. The configuration is displayed in the right pane, in the Device Configuration Preview window.
10. To send the configuration in the device template to Cisco vSmart Controllers, click Configure Devices.

Add Cisco vSmart Controller to the Overlay Network

After you create a minimal configuration for Cisco vSmart Controller, you must add it to an overlay network by making Cisco vManage aware of the controller. When you add Cisco vSmart Controller, a signed certificate is generated and is used to validate and authenticate the controller.

Cisco vManage can support up to 20 Cisco vSmart Controllers in the network.

Add a Cisco vSmart Controller and Generate Certificate

To add a Cisco vSmart Controller to the network, automatically generate the CSR, and install the signed certificate:

1. In Cisco vManage, select Configuration > Devices.
2. In the Controllers tab, click Add Controller and select vSmart.
3. In the **Add vSmart** dialog box:
   
a. Enter the system IP address of Cisco vSmart Controller.
   
b. Enter the username and password to access Cisco vSmart Controller.
   
c. Select the protocol to use for control-plane connections. The default is DTLS.
   
d. If you select TLS, enter the port number to use for TLS connections. The default is 23456.
   
e. Select the **Generate CSR** check-box to allow the certificate-generation process to occur automatically.
   
f. Click **Add**.
Cisco vManage automatically generates the CSR, retrieves the generated certificate, and installs it on Cisco vSmart Controller. The new controller is listed in the Controller table with the controller type, hostname of the controller, IP address, site ID, and other details.

**Verify Certificate Installation**

To verify that the certificate is installed on a Cisco vSmart Controller:

1. In Cisco vManage, select **Configuration > Devices**.

2. In the Controllers table, select the row listing the new controller, and check the Certificate Status column to ensure that the certificate has been installed.

**Note**

If Cisco vSmart Controller and Cisco vBond Orchestrator have the same system IP addresses, they do not appear in Cisco vManage as devices or controllers. The certificate status of Cisco vSmart Controller and Cisco vBond Orchestrator is also not displayed. However, the control connections still successfully come up.

**What’s Next**

*See Deploy the vEdge Routers.*
Deploy Cisco Catalyst 8000V Using Cloud Services Provider Portals

Table 21: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for Deploying Cisco Catalyst 8000V Instances for Supported Cloud Services Provider Platforms</td>
<td>Cisco IOS XE Release 17.4.1a</td>
<td>Starting from this release, Cisco Catalyst 8000V instances can be deployed on Cloud Services Provider portals such as Google Cloud Platform, Microsoft Azure and Amazon Web Services.</td>
</tr>
<tr>
<td>Support for Deploying Cisco Catalyst 8000V Instances on Alibaba Cloud</td>
<td>Cisco IOS XE Release 17.5.1a</td>
<td>Starting from this release, Cisco Catalyst 8000V instances can be deployed on Alibaba Cloud.</td>
</tr>
</tbody>
</table>

For information on supported instances of Cisco Catalyst 8000V and how to deploy them on the supported cloud service provider portals, see the following links:

- Deploying Cisco Catalyst 8000V Edge Software on Amazon Web Services
- Deploying Cisco Catalyst 8000V Edge Software on Microsoft Azure
- Deploying Cisco Catalyst 8000V Edge Software on Google Cloud Platform

Notes and Limitations

- Creating new Cisco Catalyst 8000V instances by snapshot: Creating a new Cisco Catalyst 8000V instance by snapshot (cloning) results in a new instance with the same serial number as the original. This creates a conflict in Cisco SD-WAN. You can use the snapshot (cloning) function to create a new instance only if the new instance is replacing an existing one, so that the serial number will be used with only one Cisco Catalyst 8000V instance.

Deploy Cisco CSR 1000v Using Cloud Service Provider Portals

For information on supported instances of Cisco CSR 1000v routers and how to deploy them on the supported cloud service provider portals, see the following links:

- Cisco CSR 1000v Series Cloud Services Router Deployment Guide for Amazon Web Services
- Cisco CSR 1000v Deployment Guide for Microsoft Azure
Deploy Cisco Catalyst 8000V Edge Software on Alibaba Cloud

This section provides information helpful when using the Alibaba Cloud instance with Cisco SD-WAN. For detailed information about the Cisco Catalyst 8000V Edge Software deployment process, see the deployment guide for Alibaba Cloud.

Features

The following Cisco Catalyst 8000V features are not supported in an Alibaba Cloud deployment when operating as part of Cisco SD-WAN:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment and Licensing</td>
<td>Connect the Cisco Catalyst 8000V to Cisco SD-WAN by creating a bootstrap file, as described in Create a Bootstrap File for a Cisco Catalyst 8000V Instance Using Cisco vManage, on page 184. Deployment by Cloud onRamp is not supported.</td>
</tr>
<tr>
<td>Pay as you go (PAYG) licensing</td>
<td>None</td>
</tr>
</tbody>
</table>

Requirements for the Cisco Catalyst 8000V Instance

The Cisco Catalyst 8000V instance deployed in Alibaba Cloud must meet the following requirements to work with Cisco SD-WAN:

- Alibaba Cloud Elastic Compute Service (ECS) instance type: G5ne
- vCPU: 2
- RAM: 8 GB

The following image options are supported by Cisco SD-WAN:

- ecs.g5ne.large: 2 vCPU and 8 GB RAM
- ecs.g5ne.xlarge: 4 vCPU and 16 GB RAM
- ecs.g5ne.2xlarge: 8 vCPU and 32 GB RAM

Configure the Cisco Catalyst 8000V Instance to Connect to Cisco SD-WAN

When you create a Cisco SD-WAN instance on Alibaba Cloud, create a Day 0 bootstrap file using Cisco vManage and use this bootstrap file on the Cisco Catalyst 8000V instance to onboard the instance to Cisco SD-WAN. When the instance starts up using the bootstrap file, it connects to the Cisco vBond Orchestrator and Cisco vManage controller.
Create a Bootstrap File for a Cisco Catalyst 8000V Instance Using Cisco vManage

1. For instructions on creating a bootstrap file for a cloud-hosted device, using Cisco vManage, see Bootstrap Process for Cisco SD-WAN Cloud-Hosted Devices.

2. In the Alibaba Cloud portal, create an instance of the Cisco Catalyst 8000V. When configuring the instance, use the bootstrap configuration that you created in Cisco vManage.

Deploy the vEdge Cloud routers

vEdge routers, as their name implies, are edge routers that are located at the perimeters of the sites in your overlay network, such as remote office, branches, campuses, and data centers. They route the data traffic to and from their site, across the overlay network.

vEdge routers are either physical hardware routers or software vEdge Cloud router, which run as virtual machines on a hypervisor or an AWS server.

An overlay network can consist of a few or a large number of vEdge routers. A single Cisco vManage, which provides management and configuration services to the vEdge routers, can support up to about 2,000 routers, and a vManage cluster can support up to about 6,000 routers.

To deploy vEdge Cloud routers:

1. For software vEdge Cloud routers, create a VM instance, either on an AWS server, or on an ESXi or a KVM hypervisor.

2. For software vEdge Cloud router, install a signed certificate on the router. In Releases 17.1 and later, Cisco vManage can act as a Certificate Authority (CA) and can automatically generate and installed signed certificates on vEdge Cloud router. In earlier releases, send a certificate signing request to Symantec and then install that certificate on the router so that the router can be authenticated on and can participate in the overlay network.

3. From Cisco vManage, send the serial numbers of all vEdge Cloud routers to Cisco vSmart Controllers and Cisco vBond Orchestrators in the overlay network.

4. Create a full configuration for the vEdge Cloud router. You do this by creating a vManage template for Cisco vBond Orchestrator and attaching that template to the orchestrator. When you attach the vManage template, the initial minimal configuration is overwritten.

5. Prepare hardware vEdge Cloud router for automatic provisioning, which is done using the Cisco SD-WAN zero-touch provisioning (ZTP) tool. The ZTP process allows hardware routers to join the overlay network automatically.

Starting with Release 18.2.0, vEdge Cloud routers that are hosted in countries affected by United States government embargoes cannot connect to overlay network controllers (Cisco vBond Orchestrators, Cisco vManages, and Cisco vSmart Controllers) that are hosted in the Cisco cloud. Any vEdge Cloud router from an embargoed country that attempts to connect to one of these controllers will be disabled. (The vEdge Cloud routers can, however, connect to controllers that are hosted in other clouds). As a result, when a vEdge Cloud router initially attempts to connect to a controller in the Cisco cloud, the router might not come up and might remain in a pending state if the Cisco vBond Orchestrator and the Cisco vManage are unable to communicate with each other or if the Cisco cloud server is down.
Create vEdge Cloud router VM Instance on AWS

To start a software vEdge Cloud router, you must create a virtual machine (VM) instance for it. This article describes how to create a VM instance on Amazon AWS. You can also create the VM on a server running the vSphere ESXi Hypervisor software or the Kernel-based Virtual Machine (KVM) Hypervisor software.

To start the vEdge Cloud router virtual machine (VM) instance on Amazon AWS, first create a Virtual Private Cloud (VPC). The VPC is a self-contained environment in which you build the infrastructure you need in order to build your network.

Plan your network addressing carefully before creating the VPC. The VPC can use addresses only in the range you specify, and once you create a VPC, you cannot modify it. If your network addressing requirements change, you must delete the VPC and create a new one.

Starting Cisco SD-WAN 18.4 Release, Cisco Cloud Services 1000v (CSR 1000v) Router SD-WAN version is supported on AWS.

To start a vEdge Cloud router on Amazon AWS:

1. Create a VPC.
2. Set up the vEdge Cloud router VM instance.
3. Define additional interfaces.

Create a VPC

Plan your network address blocks carefully before creating the VPC. Once you create a VPC, you cannot modify it. To make any changes to the network addressing, you must delete the VPC and create a new one.

1. Log in to AWS. In the Networking section of the AWS home page, click VPC.

2. On the screen that opens, click Start VPC wizard.
3. On the Select a VPC Configuration screen, select VPC with Public and Private Subnets.
4. On the VPC with Public and Private Subnets screen:
   a. In IP CIDR Block, enter the desired IP addressing block. The VPC can use addresses only in this range.
   b. Specify a public subnet and a private subnet from within the IP CIDR block.
   c. In Elastic IP Allocation ID, enter the address of your Internet gateway. This gateway translates internal traffic for delivery to the public Internet.
   d. Add endpoints for S3 only if you need extended storage space, such as for a large database.
   e. To use the AWS automatic registration of IP addresses to DNS, enable DNS hostnames.
   f. Select the desired Hardware tenancy, either shared or dedicated. You can share your AWS hardware with other AWS clients, or you can have dedicated hardware. With dedicated hardware, the device assigned to you can host only your data. However, the cost is higher.
   g. Click Create VPC.

Wait a few minutes until the VPC Dashboard displays the VPC Successfully Created message.
The infrastructure is now complete and ready for you to deploy applications, appliances, and the vEdge Cloud router. Click the links on the left to see the subnets, route tables, internet gateways, and NAT address translation points in the VPC.

Set Up the vEdge Cloud router VM Instance

1. Click Services > EC2 to open the EC2 Dashboard, and then click Launch Instance.
1. Choose an Amazon Machine Image (AMI) screen opens. The Cisco SD-WAN AMI has a name in the format release-number-vEdge; for example, 16.1.0-vEdge. The Cisco SD-WAN AMI is private. Contact your Cisco SD-WAN sales representative, who can share it with you.

2. Choose the Cisco SD-WAN AMI, then click Select.

3. The Choose an Instance Type screen appears. Determine which instance type best meets your needs, according to the following table. The minimum requirement is 2 vCPUs.

<table>
<thead>
<tr>
<th>Instance Type</th>
<th>vCPU</th>
<th>Memory (GB)</th>
<th>Instance Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Purpose — Current Generation</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>m4.large</td>
<td>2</td>
<td>8</td>
<td>EBS only</td>
</tr>
<tr>
<td>m4.xlarge</td>
<td>4</td>
<td>16</td>
<td>EBS only</td>
</tr>
<tr>
<td>m4.2xlarge</td>
<td>8</td>
<td>32</td>
<td>EBS only</td>
</tr>
<tr>
<td>m4.4xlarge</td>
<td>16</td>
<td>64</td>
<td>EBS only</td>
</tr>
<tr>
<td>m4.10xlarge</td>
<td>40</td>
<td>160</td>
<td>EBS only</td>
</tr>
<tr>
<td><strong>Compute Optimized — Current Generation</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c4.large</td>
<td>2</td>
<td>3.75</td>
<td>EBS only</td>
</tr>
<tr>
<td>c4.xlarge</td>
<td>4</td>
<td>7.5</td>
<td>EBS only</td>
</tr>
<tr>
<td>c4.2xlarge</td>
<td>8</td>
<td>15</td>
<td>EBS only</td>
</tr>
<tr>
<td>c4.4xlarge</td>
<td>16</td>
<td>30</td>
<td>EBS only</td>
</tr>
<tr>
<td>c4.8xlarge</td>
<td>36</td>
<td>60</td>
<td>EBS only</td>
</tr>
<tr>
<td>c3.large</td>
<td>2</td>
<td>3.75</td>
<td>2 x 16 SSD</td>
</tr>
<tr>
<td>c3.xlarge</td>
<td>4</td>
<td>7.5</td>
<td>2 x 40 SSD</td>
</tr>
<tr>
<td>c3.2xlarge</td>
<td>8</td>
<td>15</td>
<td>2 x 80 SSD</td>
</tr>
</tbody>
</table>
Create vEdge Cloud router VM Instance on AWS

<table>
<thead>
<tr>
<th>vCPU</th>
<th>Memory (GB)</th>
<th>Instance Storage (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>c3.4xlarge</td>
<td>16</td>
<td>2 x 160 SSD</td>
</tr>
<tr>
<td>c3.8xlarge</td>
<td>32</td>
<td>2 x 320 SSD</td>
</tr>
</tbody>
</table>

4. Select the preferred instance type, then click Next: Configure Instance Details.

Configure Instance Details

On the Configure Instance Details screen:

1. In Network, select the VPC you just created.
2. In Subnet, select the subnet for your first interface.
3. In Network Interfaces, click Add Device and select a subnet for each additional interface.

**Note**

Starting from Cisco SD-WAN Release 20.5.1, a Cisco vEdge Cloud router VM with the default username and password (admin/admin) cannot be deployed on AWS. Therefore, when you deploy a Cisco vEdge Cloud router VM using a third-party cloud provider, ensure that you use the following cloud configuration to continue using the default credentials.

In the User Data field, enter the following cloud configuration:

```bash
#cloud-config

hostname: vedge
write_files:
  - content: "vedge\n"
    owner: root:root
    path: /etc/default/personality
    permissions: '0644'
    - content: "1\n"```
owner: root:root
path: /etc/default/inited
permissions: '0600'
path: /etc/confd/init/zcloud.xml
content: |
  <config xmlns="http://tail-f.com/ns/config/1.0">
    <system xmlns="http://viptela.com/system">
      <aaa>
        <user>
          <name>admin</name>
          <password>$6$9ac6af7651b0d01b41c3a6666111/1s34f2zhkey/FS9J57aJ0mhb/H1/FS1T64a1W59/TSKd20wmpm/9C3mK-4PfjC22/</password>
          <group>netadmin</group>
        </user>
        </aaa>
    </system>
  </config>

This cloud configuration configures the VM with admin/admin credentials, and forces a password change on your first login.

5. Click Next: Add Storage.

1. The Add Storage screen opens. You do not need to change any settings on this screen. Click Next: Tag Instance.
1. The Tag Instance screen opens. Enter your desired Key and Value, and then click Next: Configure Security Group.

1. The Configure Security Group screen opens. Add rules to configure your firewall settings. These rules apply to outside traffic coming into your vEdge Cloud router.

   a. Below Type, select SSH.

   b. Below Source, select My IP.
1. Click **Add Rule**, then fill out the fields as follows:
   a. Below **Type**, select **Custom UDP Rule**.
   b. Below **Port Range**, enter **12346**.
   c. Below **Source**, select **Anywhere**. 12346 is the default port for IPSec.
   d. If **port hopping** is enabled, you may need to add more rules.

1. Click **Review and Launch**. The Review Instance Launch screen opens. Click **Launch**.
2. Select **Proceed without a key pair**, click the acknowledgement check box, then click **Launch Instances**.
Wait a few minutes, the instance initializes. The vEdge Cloud router is now running. The first interface, eth0, is always the management interface. The second interface, ge0/0, appears in VPN 0, but you can configure it to be in a different VPN.

Define Additional Interfaces

The vEdge Cloud router supports a total of nine interfaces. The first is always the management interface, and the remaining eight are transport and service interfaces. To configure additional interfaces:

1. In the left pane, click Network Interfaces.

2. Click Create Network Interface. Select the Subnet and Security group, and then click Yes, Create. Note that two interfaces in the same routing domain cannot be in the same subnet.
3. Select the check box to the left of the new interface, and click Attach.

4. Select the vEdge Cloud router, and click Attach.

5. Reboot the vEdge Cloud router, because the vEdge Cloud router detects interfaces only during the boot process.
The new interface is now up. The interface in VPN 0 connects to a WAN transport, such as the internet. The interface in VPN 1 faces a service-side network and can be used for appliances and applications. The interface in VPN 512 is dedicated to out-of-band management.

6. To allow the interface to carry jumbo frames (packets with an MTU of 2000 bytes), configure the MTU from the CLI. For example:

```bash
Router# show interface
```
The following instances support jumbo frames:

- Accelerated computing—CG1, G2, P2
- Compute optimized—C3, C4, CC2
• General purpose—M3, M4, T2
• Memory optimized—CR1, R3, R4, X1
• Storage optimized—D2, HI1, HS1, I2

What's Next
See Install Signed Certificates on vEdge Cloud Routers.

Create vEdge Cloud router VM Instance on Azure

To start a software vEdge Cloud router, you must create a virtual machine (VM) instance for it. This article describes how to create a VM instance on Microsoft Azure. You can also create the VM on Amazon AWS or on a server running the vSphere ESXi Hypervisor software or the Kernel-based Virtual Machine (KVM) Hypervisor software.

Note: Cisco SD-WAN offers only a Bring Your Own License (BYOL) for the vEdge Cloud router, so you are not actually purchasing the Cisco SD-WAN product. You are charged hourly for the VNET instance.

For server requirements, see Server Hardware Recommendations.

Launch Azure Marketplace and Create a vEdge Cloud router VM Instance

1. Launch the Azure Marketplace application:
   a. In the left pane, click New to create a new vEdge Cloud router VM instance.
   b. In the Search box, search for Cisco.
2. In the right pane, select Cisco vEdge Cloud router (3 NICs) (Staged).

3. In the Cisco vEdge Cloud router (3 NICs) (Staged) screen, click Basics in the left pane to configure basic settings for the vEdge Cloud router VM:
   a. In the VM Name field, enter a name for the vEdge Cloud router VM instance.
   b. In the Username field, enter the name of a user who can access the VM instance.
   c. In the Authentication type field, select either Password or SSH public key.
   d. If you selected password, enter, and then confirm, your password. You use the username and password to open SSH session to the VM instance.
   e. If you selected SSH public key, see https://docs.microsoft.com/en-us/azure/create-ssh-keys for instructions about how to generate an SSH key pair for Linux VMs.
   f. In the Subscription field, select Pay-As-You-Go from the drop-down menu.
   g. In the Resource Group field, click Create new to create a new resource group, or click Use existing to select an existing resource group from the drop-down menu.
   h. In the Location field, select the location in which you wish to bring up the vEdge Cloud router VM instance.
   i. Click OK.
4. In the left pane, click **vEdge Settings** to configure the vEdge Cloud router infrastructure settings.

5. In the Infrastructure Settings pane:
   
a. Click **Size**. In the **Choose a size** pane, select D3_V2 Standard for the instance type and click **Select**. This is the recommended instance type.
b. Click Storage Account. In the Choose storage account pane, click Create New to create a new storage account or select one of the listed storage accounts. Then click OK.

c. Click Public IP Address. In the Choose public IP address pane, click Create New to create a new public IP address, or select one of the listed public IP address to use for the public IP subnet. Then click OK.
d. In the **Domain Name** field, select *vedge* from the drop-down menu.

e. Click **Virtual Network**. In the Choose virtual network pane, click Create New to create a new virtual network (VNET), or select an existing VNET to launch the vEdge Cloud instance in. Then click **OK**.

f. If you selected an existing VNET, use the drop-down menu to choose available subnets within the VNET. Then click **OK**.

You must have three subnets available within the VNET; otherwise, the vEdge Cloud router VM instance will fail to launch. Also, ensure that route tables associated with your VM subnets have a user-defined route (UDR) towards the service subnet of the vEdge Cloud router. The UDR ensures that the VM subnets use the vEdge Cloud router as the gateway. See the example topology below.
g. If you created a new VNET, define the address space within that VNET. Then click **OK** in the Subnets pane.

Cisco SD-WAN prepopulates subnet names and assigns IP addresses per subnet from the VNET address space you defined. If you plan to connect your VNET instances through the service subnet associated to the vEdge Cloud router, you do not need to make updates to the route table.

6. In the Summary pane, click **OK**. The Summary pane validates and displays the configuration you defined for the vEdge Cloud router VM instance.
7. Click **Buy to purchase**. Then click **Purchase** in the **Purchase** pane.

**Note**

Cisco SD-WAN offers only a Bring Your Own License (BYOL) for the vEdge Cloud router, so you are not actually purchasing the Viptela product. You are charged hourly for the VNET instance.

The system creates the vEdge Cloud router VM instance and notifies you that the deployment has succeeded.
8. Click the vEdge VM instance you just created.

The system displays the public IP address and DNS name of the vEdge Cloud router VM instance.
9. SSH into the public IP address of the vEdge Cloud router VM instance.

![SSH into the public IP address of the vEdge Cloud router VM instance.]

10. At the login prompt, log in with the username and password you created in Step 3. To view the vEdge Cloud router default configuration, enter the following command:

```
vEdge# show running-config
```

When you create a vEdge Cloud router VM, the security group configuration shown below is applied to the NIC associated with the public subnet. This security group does not restrict traffic from specific sources, but it does restrict specific services. Custom services for TCP and UDP that need to be enabled for Cisco SD-WAN control protocols are also automatically configured. You can change the security group configuration to suit your requirements.
vEdge Cloud Router Interface and Subnet Mapping

To create a vEdge Cloud router VM instance on Azure Marketplace, a minimum of three NICs are required—one each for management, service, and transport. The table below shows the mapping of the vEdge Cloud router interface with the subnet associated to these NICs.

<table>
<thead>
<tr>
<th>vEdge Cloud Router Interface</th>
<th>Subnet</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>Management subnet</td>
<td>In-band management</td>
</tr>
<tr>
<td>ge0/1</td>
<td>Service subnet</td>
<td>Connects the vEdge Cloud router as a gateway device</td>
</tr>
<tr>
<td>ge0/0</td>
<td>Transport subnet</td>
<td>Transport/WAN link</td>
</tr>
</tbody>
</table>

What's Next

See Install Signed Certificates on vEdge Cloud Routers.

Create vEdge Cloud VM Instance on ESXi

To start a software vEdge Cloud router, you must create a virtual machine (VM) instance for it. This article describes how to create a VM instance on a server running the vSphere ESXi Hypervisor software. You can also create the VM on Amazon AWS or on a server running the Kernel-based Virtual Machine (KVM) Hypervisor software.

For server requirements, see Server Hardware Recommendations.

To create a vEdge Cloud VM instance on the ESXi hypervisor:

1. Launch the vSphere Client and create a vEdge Cloud VM instance.
2. Add a vNIC for the tunnel interface.
3. Start the vEdge Cloud VM instance and connect to the console.
The details of each step are provided below.

If you are using the VMare vCenter Server to create the vEdge Cloud VM instance, follow the same procedure. Note, however, that the vCenter Server screens look different than the vSphere Client screens shown in the procedure.

Launch vSphere Client and Create a vEdge Cloud VM Instance

1. Launch the VMware vSphere Client application, and enter the IP address or name of the ESXi server, your username, and your password. Click Login to log in to the ESXi server.
   The system displays the ESXi screen.

2. Click **File > Deploy OVF Template** to deploy the virtual machine.

3. In the Deploy OVF Template screen, enter the location to install and download the OVF package. This package is the vedge.ova file that you downloaded from Cisco. Then click **Next**.

4. Click **Next** to verify OVF template details.

5. Enter a name for the deployed template and click **Next**. The figure below specifies a name for the vEdge instance.

6. Click **Next** to accept the default format for the virtual disks.

7. Click **Next** to accept your destination network name as the destination network for the deployed OVF template. In the figure below, CorpNet is the destination network.

8. In the Ready to Complete screen, click **Finish**.
   The system has successfully created the VM instance with the parameters you just defined and displays the vSphere Client screen with the **Getting Started** tab selected. By default, this includes four vNICs which can be used for the management, tunnel, or service interface.

Add a New vNIC

1. In the left navigation bar of the vSphere Client, select the vEdge Cloud VM instance you just created, and click **Edit virtual machine settings**.

2. In the vEdge Cloud – Virtual Machine Properties screen, click **Add** to add a new vNIC. Then click **OK**.

3. Click Ethernet Adapter for the type of device you wish to add. Then click **Next**.

4. In the **Adapter Type** drop-down, select VMXNET3 for the vNIC to add. Then click **Next**.

5. In the Ready to Complete screen, click **Finish**.

6. The vEdge Cloud – Virtual Machine Properties screen opens showing that the new vNIC is being added. Click **OK** to return to the vSphere Client screen.

Modify the MTU for a vSwitch

To allow the interface to carry jumbo frames (packets with an MTU of 2000 bytes), configure the MTU for each virtual switch (vSwitch):

1. Launch the ESXi Hypervisor and select the **Configuration** tab.
2. In the **Hardware** field, click **Networking**. The network adapters you added are displayed in the right pane.
   a. Click **Properties** for the vSwitch whose MTU you wish to modify.

3. In the vSwitch Properties screen, click **Edit**.

4. In the **Advanced Properties MTU** drop-down, change the vSwitch MTU to the desired value. The range is 2000 to 9000. Then click **OK**.

**Start the vEdge Cloud VM Instance and Connect to the Console**

1. In the left navigation bar of the vSphere Client, select the vEdge Cloud VM instance you just created, and click **Power** on the virtual machine. The vEdge Cloud virtual machine is powered on.

2. Select the **Console** tab to connect to the vEdge Cloud console.

3. At the login prompt, log in with the default username, which is **admin**, and the default password, which is **admin**. To view the vEdge Cloud router default configuration, enter the following command:

   ```
vEdge# show running-config
   ```

**Mapping vNICs to Interfaces**

When you create a vEdge Cloud router VM instance on ESXi in the procedure in the previous section, you create two vNICs: vNIC 1, which is used for the management interface, and vNIC 2, which is used as a tunnel interface. From the perspective of the VM itself, these two vNICs map to the eth0 and eth1 interfaces, respectively. From the perspective of the Cisco SD-WAN software for the vEdge Cloud router, these two vNICs map to the mgmt0 interface in VPN 512 and the ge0/0 interface in VPN 0, respectively. You cannot change these mappings.

You can configure up to five additional vNICs, numbered 3 through 7, on the VM host. You can map these vNICs to interfaces eth2 through eth7 as desired, and to Cisco SD-WAN interfaces ge0/1 through ge0/7, as desired.

The table below summarizes the mapping between vNICs, VM host interfaces, and vEdge Cloud interfaces.

**Table 24:**

<table>
<thead>
<tr>
<th>vNIC</th>
<th>Interface on VM Host</th>
<th>Interface in vEdge Cloud Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>vNIC 1</td>
<td>eth0</td>
<td>mgmt0 in VPN 512</td>
</tr>
<tr>
<td>vNIC 2</td>
<td>eth1</td>
<td>ge0/0</td>
</tr>
<tr>
<td>vNIC 3 through 7</td>
<td>eth2 through eth7</td>
<td>ge0/1 through ge0/7</td>
</tr>
</tbody>
</table>
The traffic destined to VRRP IP is not forwarded by ESXi, since VRRP MAC address is not learned by the Virtual Software Switch of ESXi associated with the vEdge Ethernet interface. This is due to the limitation of the VMWare ESXi, which does not allow multiple unicast MAC address configuration on vNIC. As a workaround, place the vNIC in promiscuous mode and perform MAC filtering in the software. To let Cisco vEdge software place interface in promiscuous mode, Virtual Software Switch port-group or switch configuration must be changed to allow the same. Be aware that ESXi VSS forwards all packets to all virtual machines that are connected to the port-group or switch. This can have an adverse performance impact on the ESXi Host other virtual machines. This might also have an adverse effect on the vEdge packet processing performance. Design your network carefully to avoid performance impact.

What's Next

See Install Signed Certificates on vEdge Cloud Routers.

Create vEdge Cloud VM Instance on KVM

To start a software vEdge Cloud router, you must create a virtual machine (VM) instance for it. This article describes how to create a VM instance on a server running the Kernel-based Virtual Machine (KVM) Hypervisor software. You can also create the VM on Amazon AWS or on a server running the vSphere ESXi Hypervisor software.

For server requirements, see Server Hardware Recommendations.

Create vEdge Cloud VM Instance on the KVM Hypervisor

To create a vEdge Cloud VM instance on the KVM hypervisor:

1. Launch the Virtual Machine Manager (virt-manager) client application. The system displays the Virtual Machine Manager screen.

2. Click New to deploy the virtual machine. The system opens the Create a new virtual machine screen.
3. Enter the name of the virtual machine. The figure below specifies a name for the vEdge Cloud instance.
   a. Select **Import existing disk image**.
   b. Click **Forward**.

4. In **Provide the existing storage path** field, click **Browse to find the vEdge Cloud software image**.
   a. In the **OS Type** field, select **Linux**.
   b. In the **Version** field, select the Linux version you are running.
   c. Click **Forward**.
5. Specify Memory and CPU based on your network topology and the number of sites. Click Forward.

6. Select Customize configuration before install. Then click Finish.

7. Select Disk 1 in the left navigation bar. Then:
a. Click **Advanced Options**.

b. In the **Disk Bus** field, select **IDE**.

c. In the **Storage Format** field, select **qcow2**.

d. Click **Apply** to create the VM instance with the parameters you just defined. By default, this includes one vNIC. This vNIC is used for the management interface.

---

**Note**

Cisco SD-WAN software supports VMXNET3 and Virtio vNICs. It is recommended, however, that you use the Virtio vNICs.

8. In the vEdge Cloud Virtual Machine screen, click **Add Hardware** to add a second vNIC for the tunnel interface.

9. In the Add New Virtual Hardware screen, click **Network**.

   a. In the Host Device field, select an appropriate host device.

   b. Click Finish.
The newly created vNIC is listed in the left pane. This vNIC is used for the tunnel interface.

10. Create an ISO file to include a cloud-init configuration for the vEdge Cloud router.

11. In the Virtual Machine Manager screen, click Add Hardware to attach the ISO file you created.
12. In the Add New Virtual Hardware screen:
   a. Click Select managed or other existing storage.
   b. Click Browse and select the ISO file you created.
   c. In the Device type field, select IDE CDROM.
   d. Click Finish.
13. To allow the interface to carry jumbo frames (packets with an MTU of 2000 bytes), configure the MTU for each virtual network (vnet) and virtual bridge NIC-containing VNET (virbr-nic) interface to a value in the range of 2000 to 9000:

a. From the VM shell, issue the following command to determine the MTU on the vnet and virbr-nic interfaces:

```
user@vm:~$ ifconfig -a
```

```
virbr1-nic Link encap:Ethernet HWaddr 52:54:00:14:4e:6f
    BROADCAST MULTICAST MTU:1500 Metric
    RX packets:0 errors:0 dropped:0 overruns:0 frame:0
    TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:500
    RX bytes:0 (0.0 B) TX bytes:0 (0.0B)
```

```
vnet0 Link encap:Ethernet HWaddr fe:50:56:00:10:1e
    inet6 addr: fe80::fc50:56ff:fe00:11e/64 Scope:Link
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:167850 errors:0 dropped:0 overruns:0 frame:0
    TX packets:663186 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:500
    RX bytes:19257426 (19.2 MB) TX bytes:42008544 (42.0 MB)
```

b. Change the MTU of each vnet:

```
user@vm:~$ sudo ifconfig vnet number mtu 2000
```

c. Change the MTU of each virbr-nic:

```
user@vm:~$ sudo ifconfig virbr-nic number mtu 2000
```

d. Verify the MTU value:

```
user@vm:~$ ifconfig -a
```
14. In the vEdge Cloud Virtual Machine screen, click Begin Installation in the top upper-left corner of the screen.

![vEdge Cloud Virtual Machine screen](image)

15. The system creates the virtual machine instance and displays the vEdge Cloud console.

![vEdge Cloud console](image)

16. At the login prompt, log in with the default username, which is **admin**, and the default password, which is **admin**. To view the vEdge Cloud router default configuration, enter the following command:
vEdge# show running-config

Note that the Cisco SD-WAN software supports VMXNET3 and Virtio vNICs. It is recommended, however, that you use the Virtio vNICs.

Mapping vNICs to Interfaces

When you create a vEdge Cloud router VM instance on KVM in the procedure in the previous section, you create two vNICs: vNIC 1, which is used for the management interface, and vNIC 2, which is used as a tunnel interface. From the perspective of the VM itself, these two vNICs map to the eth0 and eth1 interfaces, respectively. From the perspective of the Cisco SD-WAN software for the vEdge Cloud router, these two vNICs map to the mgmt0 interface in VPN 512 and the ge0/0 interface in VPN 0, respectively. You cannot change these mappings.

You can configure up to five additional vNICs, numbered 3 through 7, on the VM host. You can map these vNICs to interfaces eth2 through eth7 as desired, and to Cisco SD-WAN interfaces ge0/1 through ge0/7, as desired.

The table below summarizes the mapping between vNICs, VM host interfaces, and vEdge Cloud interfaces.

<table>
<thead>
<tr>
<th>vNIC</th>
<th>Interface on VM Host</th>
<th>Interface in vEdge Cloud Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>vNIC 1</td>
<td>eth0</td>
<td>mgmt0 in VPN 512</td>
</tr>
<tr>
<td>vNIC 2</td>
<td>eth1</td>
<td>ge0/0</td>
</tr>
<tr>
<td>vNIC 3 through 7</td>
<td>eth2 through eth7</td>
<td>ge0/1 through ge0/7</td>
</tr>
</tbody>
</table>

What's Next

See Install Signed Certificates on Edge Cloud Routers.

Configure Certificate Authorization Settings for WAN Edge Routers

Certificates are used to authenticate routers in the overlay network. Once authentication is complete, the routers can establish secure sessions with other devices in the overlay network.

By default, the WAN Edge Cloud Certificate Authorization is automated. This is the recommended setting.

If you use third-party certificate authorization, configure certificate authorization to be manual:

1. In Cisco vManage, navigate to Administration > Settings.
2. Click Edit to the right of the Hardware WAN Edge Certificate Authorization bar.
3. In the Security field, select Enterprise Certificate (signed by Enterprise CA).
4. Click Save.
Install Signed Certificates on vEdge Cloud Routers

When a vEdge Cloud router virtual machine (VM) instance starts, it has a factory-default configuration, which allows the router to boot. However, the router is unable to join the overlay network. For the router to be able to join the overlay network, you must install a signed certificate on the router. The signed certificates are generated based on the router's serial number, and they are used to authorize the router to participate in the overlay network.

In Releases 17.1 and later, the vManage NMS can act as a Certificate Authority (CA), and in this role it can automatically generate and install signed certificates on vEdge Cloud routers. You can also use another CA and then install the signed certificate manually. In Releases 16.3 and earlier, you manually install signed Symantec certificates on vEdge Cloud routers.

To install signed certificates:

1. Retrieve the vEdge authorized serial number file. This file contains the serial numbers of all the vEdge routers that are allowed to join the overlay network.
2. Upload the vEdge authorized serial number file to vManage NMS.
3. Install a signed certificate on each vEdge Cloud router.

Retrieve vEdge Authorized Serial Number File

2. Click Downloads.
3. Click My Serial Number Files. The screen displays the serial number files. For Releases 17.1 and later, the filename extension is .viptela. For Releases 16.3 and earlier, the filename extension is .txt.
4. Click the most recent serial number file to download it.

Upload vEdge Authorized Serial Number File

1. In vManage NMS, select the Configuration ► Devices screen.
2. In the vEdge List tab, click Upload vEdge List.
3. In the Upload vEdge window:
   a. Click Choose File, and select the vEdge authorized serial number file you downloaded from Cisco.
   b. To automatically validate the vEdge routers and send their serial numbers to the controllers, click and select the checkbox Validate the Uploaded vEdge List and Send to Controllers. If you do not select this option, you must individually validate each router in the Configuration ► Certificates ► vEdge List screen.
4. Click Upload.

During the process of uploading the vEdge authorized serial number file, the vManage NMS generates a token for each vEdge Cloud router listed in the file. This token is used as a one-time password for the router. The vManage NMS sends the token to the vBond orchestrator and the vSmart controller.
After the vEdge authorized serial number file has been uploaded, a list of vEdge routers in the network is displayed in the vEdge Routers Table in the Configuration ► Devices screen, with details about each router, including the router's chassis number and its token.

**Install Signed Certificates in Releases 17.1 and Later**

In Releases 17.1 and later, to install a signed certificates on a vEdge Cloud router, you first generate and download a bootstrap configuration file for the router. This file contains all the information necessary to allow the vManage NMS to generate a signed certificate for the vEdge Cloud router. You then copy the contents of this file into the configuration for the router's VM instance. For this method to work, the router and the vManage NMS must both be running Release 17.1 or later. Finally, you download the signed certificate to the router. You can configure the vManage NMS to do this automatically or manually.

The bootstrap configuration file contains the following information:

- UUID, which is used as the router's chassis number.
- Token, which is a randomly generated one-time password that the router uses to authenticate itself with the vBond orchestrator and the vManage NMS.
- IP address or DNS name of the vBond orchestrator.
- Organization name.
- If you have already created a device configuration template and attached it to the vEdge Cloud router, the bootstrap configuration file contains this configuration. For information about creating and attaching a configuration template, see Create Configuration Templates for a vEdge Router.

You can generate a bootstrap configuration file that contains information for an individual router or for multiple routers.

In Releases 17.1 and later, you can also have Symantec generate signed certificates that you install manually on each router, as described later in this article, but this method is not recommended.

**Configure the vBond Orchestrator and Organization Name**

Before you can generate a bootstrap configuration file, you must configure the vBond orchestrator DNS name or address and your organization name:

1. In vManage NMS, select the Administration ► Settings screen.
2. In the vBond bar, click Edit.
3. In the vBond DNS/IP Address: Port field, enter the DNS name or IP address of the vBond orchestrator.
4. Click Save.
5. In the Organization Name bar, click Edit.
6. In the Organization Name field, enter the name of your organization. This name must be identical to that configured on the vBond orchestrator.
7. In the Confirm Organization name field, re-enter and confirm the organization name.
8. Click Save.
**Configure Automatic or Manual vEdge Cloud Authorization**

Signed certificates must be installed on each vEdge cloud router so that the router is authorized to participate in the overlay network. You can use the vManage NMS as the CA to generate and install the signed certificate, or you can use an enterprise CA to install the signed certificate.

It is recommended that you use the vManage NMS as a CA. In this role, the vManage NMS automatically generates and installs a signed certificate on the vEdge Cloud router. Having the vManage NMS act as a CA is the default setting. You can view this setting in the vManage Administration ► Settings screen, in the vEdge Cloud Certificate Authorization bar.

To use an enterprise CA for generating signed certificates for vEdge Cloud routers:

1. In vManage NMS, select the Administration ► Settings screen.
3. Click Save.

**Generate a Bootstrap Configuration File**

To generate a bootstrap configuration file for a vEdge Cloud router:

1. In vManage NMS, select the Configuration ► Devices screen.
2. To generate a bootstrap configuration file for one or multiple vEdge Cloud routers:
   a. In the vEdge List tab, select Export Bootstrap Configuration.
   b. In the Generate Bootstrap Configuration field, select the file format:
      - For a vEdge Cloud router on a KVM hypervisor or on an AWS server, select Cloud-Init to generate a token, vBond orchestrator IP address, vEdge Cloud router UUID, and organization name.
      - For a vEdge Cloud router on a VMware hypervisor, select Encoded String to generate an encoded string.
   c. In the Available Devices window, select one or more routers.
   d. Click Generate Configuration. The bootstrap configuration is downloaded in a .zip file, which contains one .cfg file for each router.
3. To generate a bootstrap configuration file individually for each vEdge Cloud router:
   a. In the vEdge List tab, select the desired vEdge Cloud router.
   b. Click the More Actions icon to the right of the row, and select Generate Bootstrap Configuration.
   c. In the Generate Bootstrap Configuration window, select the file format:
      - For a vEdge Cloud router on a KVM hypervisor or on an AWS server, select Cloud-Init to generate a token, vBond orchestrator IP address, vEdge Cloud router UUID, and organization name.
      - For a vEdge Cloud router on a VMware hypervisor, select Encoded String to generate an encoded string.
d. Click Download to download the bootstrap configuration. The bootstrap configuration is downloaded in a .cfg file.

Then use the contents of the bootstrap configuration file to configure the vEdge Cloud router instance in AWS, ESXi, or KVM. For example, to configure a router instance in AWS, paste the text of the Cloud-Init configuration into the User data field:

By default, the ge0/0 interface is the router's tunnel interface, and it is configured as a DHCP client. To use a different interface or to use a static IP address, and if you did not attach a device configuration template to the router, change the vEdge Cloud router's configuration from the CLI. See Configuring Network Interfaces.

**Install the Certificate on the vEdge Cloud Router**

If you are using automated vEdge Cloud certificate authorization, which is the default, after you configure the vEdge Cloud router instance, vManage NMS automatically installs a certificate on the router and the router's token changes to its serial number. You can display the router's serial number in the Configuration ► Devices screen. After the router's control connections to the vManage NMS come up, any templates attached to the router are automatically pushed to the router.

If you are using manual vEdge Cloud certificate authorization, after you configure the vEdge Cloud router instance, follow this procedure to install a certificate on the router:

1. Install the enterprise root certificate chain on the router:
   
   ```
   vEdge# request root-cert-chain install filename [vpn vpn-id]
   ```

   Then, the vManage NMS generates a CSR.

2. Download the CSR:
   
   a. in vManage NMS, select the Configuration ► Certificates screen.

   b. Select the vEdge Cloud router for which to sign a certificate.
c. Click the More Actions icon to the right of the row and select View CSR.
d. To download the CSR, click Download.

3. Send the certificate to a third-party signing authority, to have them sign it.

4. Import the certificate into the device:
   a. In the Configuration ► Certificates screen, click the Controllers tab.
   b. Click the Install Certificate button located in the upper-right corner of the screen.
   c. In the Install Certificate screen, paste the certificate into the Certificate Text field, or click Select a File to upload the certificate in a file.
   d. Click Install.

5. Issue the following REST API call, specifying the IP address of your vManage NMS:

   \[ https://vmanage-ip-address/dataservice/system/device/sync/rootcertchain \]

**Create the vEdge Cloud Router Bootstrap Configuration from the CLI**

It is recommended that you generate the vEdge Cloud router's bootstrap configuration using the vManage NMS. If, for some reason, you do not want to do this, you can create the bootstrap configuration using the CLI. With this process, you must still, however, use the vManage NMS. You collect some of this information for the bootstrap configuration from the vManage NMS, and after you have created the bootstrap configuration, you use the vManage NMS to install the signed certificate on the router.

Installing signed certificates by creating a bootstrap configuration from the CLI is a three-step process:

1. Edit the router's configuration file to add the DNS name or IP address of the vBond orchestrator and your organization name.
2. Send the router's chassis and token numbers to the vManage NMS.
3. Have the vManage NMS authenticate the vEdge Cloud router and install the signed certificate on the router.

To edit the vEdge Cloud router's configuration file from the CLI:

1. Open a CLI session to the vEdge Cloud router via SSH. To do this in vManage NMS, select the Tools ► SSH Terminal screen, and select the desired router.
2. Log in as the user **admin**, using the default password, **admin**. The CLI prompt is displayed.
3. Enter configuration mode:

   ```
   vEdge# config
   vEdge(config)#
   ```

4. Configure the IP address of the vBond orchestrator or a DNS name that points to the vBond orchestrator. The vBond orchestrator's IP address must be a public IP address:

   ```
   vEdge(config)# system vbond (dns-name | ip-address)
   ```

5. Configure the organization name:

   ```
   vEdge(config-system)# organization-name name
   ```
6. Commit the configuration:

   vEdge(config)# commit and-quit
   vEdge#

To send the vEdge Cloud router's chassis and token numbers to the vManage NMS:

1. Locate the vEdge Cloud router's token and chassis number:
   a. In vManage NMS, select the Configuration ► Devices screen.
   b. In the vEdge List tab, locate the vEdge Cloud router.
   c. Make a note of the values in the vEdge Cloud router's Serial No./Token and Chassis Number columns.

2. Send the router's bootstrap configuration information to the vManage NMS:

   vEdge# request vedge-cloud activate chassis-number chassis-number token token-number

Issue the **show control local-properties** command on the router to verify the vBond IP address, the organization name the chassis number, and the token. You can also verify whether the certificate is valid.

Finally, have the vManage NMS authenticate the vEdge Cloud router and install the signed certificate on the router.

If you are using automated vEdge Cloud certificate authorization, which is the default, the vManage NMS uses the chassis and token numbers to authenticate the router. Then, the vManage NMS automatically installs a certificate on the router and the router's token changes to a serial number. You can display the router's serial number in the Configuration ► Devices screen. After the router's control connections to the vManage NMS come up, any templates attached to the router are automatically pushed to the router.

If you are using manual vEdge Cloud certificate authorization, after you configure the vEdge Cloud router instance, follow this procedure to install a certificate on the router:

1. Install the enterprise root certificate chain on the router:

   vEdge# request root-cert-chain install filename [vpn vpn-id]

   After you install the root chain certificate on the router, and after the vManage NMS receives the chassis and token numbers, the vManage NMS generates a CSR.

2. Download the CSR:
   a. In vManage NMS, select the Configuration ► Certificates screen.
   b. Select the vEdge Cloud router for which to sign a certificate.
   c. Click the More Actions icon to the right of the row and select View CSR.
   d. To download the CSR, click Download.

3. Send the certificate to a third-party signing authority, to have them sign it.

4. Import the certificate into the device:
   a. In the Configuration ► Certificates screen, click the Controllers tab.
   b. Click the Install Certificate button located in the upper-right corner of the screen.
   c. In the Install Certificate screen, paste the certificate into the Certificate Text field, or click Select a File to upload the certificate in a file.
d. Click Install.

5. Issue the following REST API call, specifying the IP address of your vManage NMS:

   https://vmanage-ip-address/dataservice/system/device/sync/rootcertchain

Install Signed Certificates in Releases 16.3 and Earlier

For vEdge Cloud router virtual machine (VM) instances running Releases 16.3 and earlier, when the vEdge Cloud router VM starts, it has a factory-default configuration, but is unable to join the overlay network because no signed certificate is installed. You must install a signed Symantec certificate on the vEdge Cloud router so that it can participate in the overlay network.

To generate a certificate signing request (CSR) and install the signed certificate on the vEdge Cloud router:

1. Log in to the vEdge Cloud router as the user admin, using the default password, admin. If the vEdge Cloud router is provided through AWS, use your AWS key pair to log in. The CLI prompt is displayed.

2. Generate a CSR for the vEdge Cloud router:

   vEdge# request csr upload path

   path is the full path and filename where you want to upload the CSR. The path can be in a directory on the local device or on a remote device reachable through FTP, HTTP, SCP, or TFTP. If you are using SCP, you are prompted for the directory name and filename; no file path name is provided. When prompted, enter and then confirm your organization name. For example:

   vEdge# request csr upload home/admin/vm9.csr
   Uploading CSR via VPN 0
   Enter organization name : Cisco
   Re-enter organization name : Cisco
   Generating CSR for this vEdge device
   ..........[DONE]
   Copying ... /home/admin/vm9.csr via VPN 0
   CSR upload successful

3. Log in to the Symantec Certificate Enrollment portal:

   https://certmanager.websecurity.symantec.com/vbmcelp/enroll/index?jur_hash=f422d7ce50824a32474a4f740757338

   Viptela Inc - SSL Certificate Portal
   Managed PKI for SSL Subscriber Services
   Enroll  Select Certificate Type : Standard Intranet SSL  Go

   Renew  Renew a current certificate to ensure uninterrupted service. You can renew a certificate as far in advance as 90 days prior to expiration.

   Replace  Replace a valid certificate in case of incorrect information, loss or destruction of the private key, or other malfunction.

   Revoke  Revoke a valid certificate in case of compromise or other security issue.

   Search  Find a certificate by the technical contact's email address or the certificate's common name.
4. In the Select Certificate Type drop-down, select Standard Intranet SSL and click Go. The Certificate Enrollment screen is displayed. Cisco SD-WAN uses the information you provide on this form to confirm the identity of the certificate requestor and to approve your certificate request. To complete the Certificate Enrollment form:

a. In the Your Contact Information section, specify the First Name, Last Name, and Email Address of the requestor.

b. In the Server Platform and Certificate Signing section, select Apache from the Select Server Platform drop-down. In the Enter Certificate Signing Request (CSR) box, upload the generated CSR file, or copy and paste the contents of the CSR file. (For details about how to do this, log in to support.viptela.com. Click Certificate, and read the Symantec certificate instructions.)

c. In the Certificate Options section, enter the validity period for the certificate.

d. In the Challenge Phrase section, enter and then re-enter a challenge phrase. You use the challenge phrase to renew, and, if necessary, to revoke a certificate on the Symantec Customer Portal. It is recommended that you specify a different challenge phrase for each CSR.

e. Accept the Subscriber Agreement. The system generates a confirmation message and sends an email to the requestor confirming the certificate request. It also sends an email to the Cisco to approve the CSR.

5. After Cisco approves the CSR, Symantec sends the signed certificate to the requestor. The signed certificate is also available through the Symantec Enrollment portal.

6. Install the certificate on the vEdge Cloud router:

   vEdge# request certificate install filename [vpn vpn-id]

   The file can be in your home directory on the local device, or it can be on a remote device reachable through FTP, HTTP, SCP, or TFTP. If you are using SCP, you are prompted for the directory name and filename; no file path name is provided.

7. Verify that the certificate is installed and valid:

   vEdge# show certificate validity

After you have installed the certificate on the vEdge Cloud router, the vBond orchestrator is able to validate and authenticate the router, and the router is able to join the overlay network.

**What's Next**

See [Send vEdge Serial Numbers to the Controller Devices](#).

## Send Router Serial Numbers to the Controller Devices

**Table 26: Feature History**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Onboarding Enhancement</td>
<td>Cisco IOS XE Release 17.3.1a, Cisco vManage Release 20.3.1</td>
<td>This feature provides an enhancement to onboard your device to Cisco vManage by directly uploading a .csv file.</td>
</tr>
</tbody>
</table>
Only authorized routers can join the overlay network. The controller devices Cisco vManage, Cisco vSmart Controllers and Cisco vBond Orchestrators learn which routers are authorized to join the overlay network from the router-authorized serial number file. This is a file that you receive from Cisco. The router authorized serial number file lists the serial numbers and corresponding chassis numbers for all authorized routers. Upload the file to one of the Cisco vManage in your network, and it then distributes the file to the controllers.

When you upload the router serial number file, you can place the routers in one of these states:

- **Invalid**: When you power on the routers, they are not authorized to join the overlay network.
- **Staging**: When you power on the routers, they are validated and authorized to join the overlay network, and can establish connections only to the control plane. Over the control plane, the routers receive their configuration from Cisco vManage. However, the routers are unable to establish data plane connections, so they cannot communicate with other routers in the network. The Staging state is useful when you are preparing routers at one location and then sending them to different sites for installation. Once the routers reach their final destination, you change their state from Staging to Valid, to allow the routers to establish data plane connections and to fully join the overlay network.
- **Valid**: When you power on the routers, they are validated and authorized to join the overlay network, and they are able to establish both control plane and data plane connections in the network. Over the control plane, the routers receive their configuration from Cisco vManage. Over the data plane, they are able to communicate with other routers. The Valid state is useful when the routers are being installed at their final destination.

### How to Upload a Router Authorized Serial Number File

The following sections describe how to upload the router authorized serial number file to Cisco vManage and distribute the file to all the overlay network controllers.

#### Enabling PnP Connect Sync (Optional)

To sync the uploaded device to your Smart Account or Virtual Account and for your device to reflect on the PnP (Plug and Play) Connect portal, when an unsigned .csv file is uploaded through Cisco vManage, enable the PnP Connect Sync.

Ensure you have an active connection to the PnP (Plug and Play) Connect portal and an active Smart Account and Virtual Account. You have to also use a CCO ID that is associated as the Smart Account or Virtual Account admin of the account, on PnP Connect portal.

---

**Note**

PnP Connect Sync is only applicable to .csv file upload. It does not affect the .viptela file (which is downloaded from the PnP Connect portal) upload process.

**Note**

You will be allowed to enable PnP Connect Sync only once you enter the Smart Account credentials.

To enable the PnP Connect Sync:

1. Choose **Administration > Settings** screen.
2. Go to **Smart Account Credentials** and click **Edit**.
3. Enter **Username** and **Password** and click **Save**.
4. Go to PnP Connect Sync and click Edit.
5. Click Enabled and click Save.

**Place Routers in Valid State**

Perform the following task to place the routers in the Valid state so that they can establish control and data plane connections and can receive their configurations from the Cisco vManage:

1. In Cisco vManage, select the Configuration > Devices screen.
2. From the Devices title bar, choose WAN Edge List tab.
3. Click Upload WAN Edge List.
4. You can upload WAN Edge devices in the following two ways:
   - Upload a signed file (.viptela file). You can download this .viptela file from the Plug and Play Connect portal.
   - Starting from Cisco vManage Release 20.3.1, you can upload an unsigned file (.csv file). This enhancement is only applicable when you add hardware platforms on-demand onto Cisco vManage. To upload the .csv file this:
     a. Click Sample CSV. An excel file will be downloaded.
     b. Open the downloaded .csv file. Enter the following parameters:
        - Chassis number
        - Product ID (mandatory for Cisco vEdge devices, blank value for all other devices)
        - Serial number
        - SUDI serial

      Either the Serial number or SUDI number is mandatory for Cisco IOS XE SD-WAN devices, along with chassis number. Cisco ASR1002-X is an exception and does not need Serial or SUDI numbers, it can be onboarded with only the chassis number on the .csv file.
     c. To view your device details in Cisco vManage, go to Tools > SSH Terminal. Choose your device and use one of the following command-
        - `show certificate serial` (for vEdge devices)
        - `show sdwan certificate serial` (for Cisco IOS XE SD-WAN devices)
     d. Enter the specific device details in the downloaded .csv file.
5. To upload the .viptela or .csv file on Cisco vManage click Choose file and upload the file that contains the product ID, serial number and chassis number of your device.

**Note**

If you have enabled PnP Sync Connect, the .csv file can contain upto 25 devices. If you have more than 25 devices, you can split them and upload multiple files.

6. Check the check box next to Validate the uploaded vEdge List and send to controllers.
7. Click **Upload**.

8. You should now see your device listed in the table of devices.

   If you have enabled the PnP Sync Connect previously, your device will also reflect on the PnP Portal.

A list of routers in the network is displayed, showing detailed information about each router. To verify that the routers are in the Valid state, select **Configuration > Certificates**.

---

### Place Routers in Invalid State

To upload the authorized serial number file to the Cisco vManage, but place the routers in Invalid state so that they cannot establish control plane or data plane connections and cannot receive their configurations from Cisco vManage:

1. Choose **Configuration > Devices** screen.
2. From the **Devices** title bar, choose **WAN Edge List** tab.
3. Click **Upload WAN Edge List**.
4. In the **Upload WAN Edge List** dialog box, choose the file to upload.
5. To upload the router serial number file to Cisco vManage, click **Upload**.

A list of routers in the network is displayed, showing detailed information about each router. To verify that the routers are in the Invalid state, choose **Configuration > Certificates**.

---

### Place Routers in Staging State

To move the routers from the Invalid state to the Staging state and then send the serial number file to the controllers, follow the steps below. In the Staging state, the routers can establish control plane connections, over which they receive their configurations from Cisco vManage. However, the routers cannot establish data plane connections.

1. Choose **Configuration > Certificates**.
2. From the **Certificates** title bar, choose **WAN Edge List** tab.
3. In the **Validate** column, click **Staging** for each router.
4. Click **Send to Controller**.
5. When you are ready to have the router join the data plane in the overlay network, in the **Validate** column, click **Valid** for each router, and then click **Send to Controller**. Placing the routers in the Valid state allows them to establish data plane connections and to communicate with other routers in the overlay network.

---

### Configure the vEdge Routers

Once you have set up and started the virtual machines (VMs) for the vEdge Cloud routers and set up and started the hardware vEdge routers in your overlay network, they come up with a factory-default configuration.
Log In to a Device for the First Time: When you first deploy a Cisco SD-WAN overlay network, log in to the Cisco vBond Orchestrator, Cisco vManage, and Cisco vSmart Controller to manually create the device's initial configuration. Routers are shipped with a factory default configuration. If you choose to modify this configuration manually, log in through the router's console port.

For the overlay network to be operational and for the vEdge routers to be able to participate in the overlay network, you must do the following:

- Configure a tunnel interface on at least one interface in VPN 0. This interface must be connected to a WAN transport network that is accessible to all Cisco vEdge devices. VPN 0 carries all control plane traffic between the Cisco vEdge devices in the overlay network.

- Ensure that the Overlay Management Protocol (OMP) is enabled. OMP is the protocol responsible for establishing and maintaining the Cisco SD-WAN control plane. It is enabled by default, and you cannot disable it. If you edit the configuration from the CLI, do not remove the `omp` configuration command.

- Ensure that BFD is enabled. BFD is the protocol that the transport tunnels on vEdge routers use for transmitting data traffic through the overlay network. BFD is enabled by default, and cannot be disabled. If you edit the configuration from the CLI, do not remove the `bfd color` command.

- Configure the IP address of DNS name of your network's vBond orchestrator.

- Configure the router's IP address.

The DNS cache timeout should be proportional to the number of Cisco vBond Orchestrator IP addresses that DNS has to resolve, otherwise the control connection for Cisco vManage may not occur during a link failure. This is because, when there are more than six IP addresses (this is the recommended number since the default DNS cache timeout is currently two minutes) to be checked, the DNS cache timer expires even as the highest preferred interface tries all vBond IP addresses, before failing over to a different color. For instance, it takes about 20 seconds to attempt to connect to one IP address. So, if there are eight IP addresses to be resolved, the DNS cache timeout should be 20*8=160 seconds or three minutes.

You should also assign a system IP address to each vEdge router. This address, which is similar to the router ID on non-Cisco vEdge devices, is a persistent address that identifies the router independently of any interface addresses. The system IP is a component of the device's TLOC address. Setting the system IP address for a device allows you to renumber interfaces as needed without affecting the reachability of the Cisco vEdge device. Control traffic over secure DTLS or TLS connections between Cisco vSmart Controllers and vEdge routers and between Cisco vSmart Controllers and Cisco vBond Orchestrators is sent over the system interface identified by the system IP address. In the transport VPN (VPN 0), the system IP address is used as the loopback address of the device. You cannot use the same address for another interface in VPN 0.

You can also configure other features and functions required for your network topology.

You configure vEdge routers by creating configuration templates on the Cisco vManage. For each configuration templates, you create one or more feature templates, which you then consolidate into a vEdge router device template. You then attach the device template to a vEdge router. When the vEdge router joins the overlay network, the Cisco vManage automatically pushes the configuration template to the router.
It is strongly recommended that you create the full configuration for vEdge routers by creating configuration templates on the Cisco vManage. When the Cisco vManage discovers a router in the overlay network, it pushes the appropriate configuration template to the device. The configuration parameters in the configuration template overwrite the initial configuration.

**Create Configuration Templates for the vEdge Routers**

To create vEdge configuration templates, first create feature templates:

1. In Cisco vManage, select *Configuration > Templates*.
2. From the *Templates* title bar, select *Feature*.
3. Click *Add Template*.
4. In the left pane, select vEdge Cloud or a router model.
5. In the right pane, select the *System feature template*. Configure the following parameters:
   a. Template Name
   b. Description
   c. Site ID
   d. System IP
   e. Timezone
   f. Hostname
   g. Console baud rate (vEdge hardware routers only)
   h. GPS location

6. Click *Save* to save the System template.
7. In the right pane, select *VPN-Interface-Ethernet feature template*. Configure the following parameters:
   a. Template Name
   b. Description
   c. Shutdown No
   d. Interface name
   e. IPv4 address (static or DHCP)
   f. IPv6 address (static of DHCPv6), if desired (in Releases 16.3 and later)
   g. Tunnel interface (for VPN 0), color, encapsulation, and services to allow.

8. Click *Save* to save the VPN-Interface Ethernet template.
9. In the right pane, select other templates to configure any desired features. Save each template when you complete the configuration. For information about configuration cellular parameters for vEdge 100m and vEdge 100wm routers, see the next section in this article.
For information about configuration templates and parameters, see the vManage configuration help articles for your software release.

Next, create a device template that incorporates all the feature templates for the vEdge router:

1. In the Cisco vManage, select Configuration > Templates.
2. From the Templates title bar, select Device.
3. Click Create Template, and from the drop-down list select From Feature Template.
4. From the Device Model drop-down, select the type of device for which you are creating the device template. vManage NMS displays the feature templates for the device type you selected. Required templates are indicated with an asterisk (*).
5. Enter a name and description for the device template. These fields are mandatory. The template name cannot contain special characters.
6. In the Transport & Management VPN section, under VPN 0, from the drop-down list of available templates, select the desired feature template. The list of available templates shows the ones that you have previously created.
7. To include additional feature templates in the device template, in the remaining sections, select the feature templates in turn, and from the drop-down list of available templates, select the desired template. The list of available templates are the ones that you have previously created. Ensure that you select templates for all mandatory feature templates and for any desired optional feature templates.
8. Click Create to create the device template.

To attach a device template to a device:

1. In the vManage NMS, select the Configuration ► Templates screen.
2. From the Templates title bar, select Device.
3. Select a template.
4. Click the More Actions icon to the right of the row and click Attach Device.
5. In the Attach Device window, either search for a device or select a device from the Available Device(s) column to the left.
6. Click the arrow pointing right to move the device to the Selected Device(s) column on the right.
7. Click Attach.

When the vManage NMS discovers that the vEdge router has joined the overlay network, it pushes the configuration template to the router.

Configuring Cellular Routers

For vEdge 100m and vEdge 100wm routers, you configure cellular interface parameters on the VPN-Interface-Cellular feature template. In this template, the default Profile ID is 0, which enables automatic profile selection. The automatic profile uses the Mobile Country Code/Mobile Network Code (MCC/MNC) values on the router's SIM card. Profile 0 enables the cellular router to automatically join the overlay network during the Cisco SD-WAN ZTP automatic provisioning process.
If your MCC/MNC is not supported, the automatic profile selection process fails, and the ZTP process is unable to autodetect the router. In this case, you must configure a cellular profile as follows:

1. In the right pane, select the Cellular Profile feature template.
2. Set the Profile ID to a value from 1 through 15, and configure the desired cellular parameters.
3. Save the Cellular Profile feature template.
4. In the right pane, select the VPN-Interface-Cellular template.
5. Select the Profile ID you configured in Step 2, and for Shutdown, click Yes.
7. Include the Cellular Profile and VPN-Interface Cellular templates in a device template.
8. Attach the device template to the vEdge router to activate the MCC/MCN.
9. In the right pane, select the VPN-Interface-Cellular template.
10. For Shutdown click No, to enable the cellular interface.
11. Save the VPN-Interface-Cellular feature template.
12. Repush the device template to the vEdge router. This is the device template that you pushed in Step 8.

Configure the vEdge Routers from the CLI

Normally, you create vEdge router configurations using vManage configuration templates. However, in some situations, such as network test and proof-of-concept (POC) environments, you might want to configure vEdge routers manually, either to speed up the configuration process or because your test environment does not include a vManage NMS. In such situations, you can configure vEdge routers from the router's CLI.

If you configure a vEdge router manually from the CLI and then the router later becomes managed by a vManage NMS, when the vManage NMS discovers the router, it pushes the router's configuration from the vManage server to the router, overwriting the existing configuration.

For vEdge Cloud routers, use SSH to open a CLI session to the router. For hardware vEdge routers, connect to the router via the management console.

Configure Minimum Parameters from the CLI

To create the initial configuration on a Cisco vEdge device from a CLI session:

1. Open a CLI session to the Cisco vEdge device via SSH or the console port.
2. Log in as the user admin, using the default password, admin. The CLI prompt is displayed.
3. Enter configuration mode:
   ```
   vEdge# config
   vEdge(config)#
   ```
4. Configure the hostname:
   ```
   vEdge(config)# system host-name hostname
   ```
Configuring the hostname is optional, but is recommended because this name is included as part of the prompt in the CLI and it is used on various vManage NMS screens to refer to the device.

5. Configure the system IP address. In Releases 16.3 and later, the IP address can be an IPv4 or an IPv6 address. In earlier releases, it must be an IPv4 address.

   vEdge(config-system)# system-ip ip-address

The vManage NMS uses the system IP address to identify the device so that the NMS can download the full configuration to the device.

6. Configure the numeric identifier of the site where the device is located:

   vEdge(config-system)# site-id site-id

7. Configure the organization name:

   vEdge(config-system)# organization-name organization-name

8. Configure the IP address of the vBond orchestrator or a DNS name that points to the vBond orchestrator. The vBond orchestrator's IP address must be a public IP address, to allow all Cisco vEdge devices in the overlay network to reach the vBond orchestrator:

   vEdge(config-system)# vbond (dns-name | ip-address)

9. Configure a time limit for confirming that a software upgrade is successful:

   vEdge(config-system)# upgrade-confirm minutes

The time can be from 1 through 60 minutes. If you configure this time limit, when you upgrade the software on the device, the vManage NMS (when it comes up) or you must confirm that a software upgrade is successful within the configured number of minutes. If the device does not receive the confirmation within the configured time, it reverts to the previous software image.

10. Change the password for the user "admin":

    vEdge(config-system)# user admin password password

The default password is "admin".

11. Configure an interface in VPN 0 to be used as a tunnel interface. VPN 0 is the WAN transport VPN, and the tunnel interface carries the control traffic among the devices in the overlay network. For vEdge Cloud routers, the interface name has the format eth number. For hardware vEdge routers, the interface name has the format ge slot l port. You must enable the interface and configure its IP address, either as a static address or as a dynamically assigned address received from a DHCP server. In Releases 16.3 and later, the IP address can be an IPv4 or an IPv6 address, or you can configure both to enable dual-stack operation. In earlier releases, it must be an IPv4 address.

   vEdge(config)# vpn 0
   vEdge(config-vpn-0)# interface interface-name
   vEdge(config-interface)# (ip dhcp-client | ip address prefix/length)
   vSmart(config-interface)# (ipv6 address ipv6-prefix/length | ipv6 dhcp-client
   {dhcp-distance number | dhcp-rapid-commit})
   vEdge(config-interface)# no shutdown
   vEdge(config-interface)# tunnel-interface
You must configure a tunnel interface on at least one interface in VPN 0 in order for the overlay network to come up and for the vManage NMS to be able to participate in the overlay network. This interface must connect to a WAN transport network that is accessible by all Cisco vEdge devices. VPN 0 carries all control plane traffic among the Cisco vEdge devices in the overlay network.

12. Configure a color for the tunnel to identify the type of WAN transport. You can use the default color (default), but you can also configure a more appropriate color, such as mpls or metro-ethernet, depending on the actual WAN transport.

   vEdge(config-tunnel-interface)# color color

13. Configure a default route to the WAN transport network:

   vEdge(config-vpn-0)# ip route 0.0.0.0/0 next-hop

14. Commit the configuration:

   vEdge(config)# commit and-quit
   vEdge#

15. Verify that the configuration is correct and complete:

   vEdge# show running-config

After the overlay network is up and operational, create a vEdge configuration template on the vManage NMS that contains the initial configuration parameters. Use the following vManage feature templates:

- System feature template to configure the hostname, system IP address, and vBond functionality.
- AAA feature template to configure a password for the "admin" user.
- VPN-Interface-Ethernet feature template to configure the interface in VPN 0.

In addition, it is recommended that you configure the following general system parameters:

- Organization name, on the vManage Administration ► Settings screen.
- Timezone, NTP servers, and device physical location, from the Configuration ► Templates ► NTP and System feature configuration templates.
- Login banner, from the Configuration ► Templates ► Banner feature configuration template.
- Logging parameters, from the Configuration ► Templates ► Logging feature configuration template.
- AAA, and RADIUS and TACACS+ servers, from the Configuration ► Templates ► AAA feature configuration template.
- SNMP, from the Configuration ► Templates ► SNMP feature configuration template.

Sample Initial CLI Configuration

Below is an example of a simple configuration on a vEdge router. Note that this configuration includes a number of settings from the factory-default configuration and shows a number of default configuration values.

vEdge# show running-config
system
host-name vEdge
gps-location latitude 40.7127837
gps-location longitude -74.0059413
system-ip 172.16.251.20
site-id 200
max-controllers 1
organization-name "Cisco"
clock timezone America/Los_Angeles
upgrade-confirm 15
tbond 184.122.2.2

aaa
auth-order local radius tacacs
usergroup basic
  task system read write
  task interface read write
!
usergroup netadmin
!
usergroup operator
  task system read
  task interface read
  task policy read
  task routing read
  task security read
!
user admin
  password encrypted-password
!

logging
disk
  enable
!

.ntp
keys
  authentication 1 md5 $4$L3rwZmsIic8zj4BgLEFXKw==
  authentication 2 md5 $4$LyLwZmsIif8BvrJgLEFXKw==
  authentication 60124 md5 $4$LXbzZmcKj5BD+/BgLEFXKw==
  trusted 1 2 60124
!
server 180.20.1.2
  key 1
  source-interface ge0/3
  vpn 1
  version 4
  exit
!
radius
server 180.20.1.2
  vpn 1
  source-interface ge0/3
  secret-key $4$L3rwZmsIic8zj4BgLEFXKw==
  exit
!
tacacs
server 180.20.1.2
  vpn 1024
  source-interface ge0/3
  secret-key $4$L3rwZmsIic8zj4BgLEFXKw==
  exit
!

omp
no shutdown
gradeful-restart
advertise bgp
advertise connected
advertise static
!
security
ipsec
  authentication-type ah-shal-hmac shal-hman
!
snmp
no shutdown
view v2
  oid 1.3.6.1
  !
  community private
  view v2
  authorization read-only
!
trap target vpn 0 10.0.1.1 16662
  group-name Cisco
  community-name private
!
trap group test
  all
  level critical major minor
  exit
  exit
!
vpn 0
interface ge0/0
  ip address 184.111.20.2/24
tunnel-interface
  encapsulation ipsec
color mpls restrict
  no allow-service bgp
  allow-service dhcp
  allow-service dns
  allow-service icmp
  no allow-service sshd
  no allow-service netconf
  no allow-service ntp
  no allow-service ospf
  no allow-service stune
!
no shutdown
bandwidth-upstream 60
bandwidth-downstream 60
!
interface ge0/1
  no shutdown
!
interface ge0/2
  no shutdown
!
ip route 0.0.0.0/0 184.111.20.1
!
vpn 1
router
  bgp 111000
    neighbor 172.16.1.20
    no shutdown
Enable Data Stream Collection from a WAN Edge Router

By default, collecting streams of data from a network device is not enabled.

To collect data streams from a WAN Edge router in the overlay network, use the following steps:

1. In Cisco vManage, navigate to Administration > Settings.
2. Click Edit to the right of the Data Stream bar.
3. In the Data Stream field, click Enabled.
4. In the Hostname field, enter the name of the host to collect the data. It is recommended that this host be one that is used for out-of-band management and that is located in the management VPN.
5. In the VPN field, enter the number of the VPN in which the host is located. It is recommended that this be the management VPN, which is typically VPN 512.
6. Click Save.

Prepare Routers for ZTP

Cisco SD-WAN provides an automatic provisioning software as a service (SaaS) called zero-touch provisioning (ZTP), which allows hardware vEdge routers to join the overlay network automatically. The ZTP process begins when you power on a hardware vEdge router for the first time.

For the ZTP process to work:

- The edge or gateway router at the site where the hardware vEdge router is located must be able to reach public DNS servers. We recommend that the router be configured to reach the Google public DNS servers.
- For Cisco vEdge devices, the edge or gateway router at the site must be able to reach ztp.viptela.com.
- For Cisco IOS XE SD-WAN devices, the edge or gateway router at the site must be able to reach ztp.local-domain.
- A network cable must be plugged into the interface that the hardware router uses for ZTP. These interfaces are:
  - For Cisco vEdge 1000 routers: ge0/0
  - For Cisco vEdge 2000 routers: ge2/0
- For Cisco vEdge 100 series routers: ge0/4

- For Cisco IOS XE SD-WAN devices, there is no specific interface that is used for connection to the ZTP server. The router attempts to obtain a DHCP IP address on one interface at a time. It uses the first interface on which it obtains the DHCP IP address to resolve the domain name `ztp.local-domain` to the IP address of the ZTP server.

The ZTP process occurs in the following sequence:

1. The hardware router powers up.
2. The router attempts to contact a DHCP server, sending a DHCP discovery message.
   a. If a DHCP server is present in the network, the router receives a DHCP offer message that contains the IP address of its ZTP interface. Then, the ZTP process continues with Step 3.
   b. For Cisco vEdge devices, if no DHCP server is present, router does not receive a DHCP offer. In this situation, the router initiates an automatic IP address detection process (also referred to as auto-IP). This process examines the ARP packets on the subnetwork and, from these packets, it infers the IP address of the ZTP interface. Then, the ZTP process continues with Step 3.

   For Cisco IOS XE SD-WAN devices, if no DHCP server is present, the ZTP process does not continue.
3. The router contacts a DNS server to resolve the hostname `ztp.viptela.com` (for Cisco vEdge devices) or `ztp.local-domain` (Cisco IOS XE SD-WAN devices) and receives the IP address of the Cisco SD-WAN ZTP server.
4. The router connects to the ZTP server. The ZTP server verifies the vEdge router and sends the IP address of the Cisco vBond Orchestrator. This Cisco vBond Orchestrator has the same Organization name as the vEdge router.
5. The router establishes a transient connection to the Cisco vBond Orchestrator and sends its chassis ID and serial number. (At this point in the ZTP process, the router does not have a system IP address, so the connection is established with a null system IP address.) The Cisco vBond Orchestrator uses the chassis ID and serial number to verify the router. The Cisco vBond Orchestrator then sends the IP address of Cisco vManage to the router.

6. The router establishes a connection to and is verified by Cisco vManage. Cisco vManage sends the router its system IP address.

7. The router re-establishes a connection to the Cisco vBond Orchestrator using its system IP address.

8. The router re-establishes a connection to Cisco vManage using its system IP address.
   For Cisco vEdge devices, if necessary, Cisco vManage pushes the proper software image to the vEdge router. As part of the software image installation, the router reboots.

9. After the reboot, the router re-establishes a connection to the Cisco vBond Orchestrator, which again verifies the router.

10. The router establishes a connection to Cisco vManage, which pushes the full configuration to the router. (If the router has rebooted, it re-establishes a connection to Cisco vManage.)

11. The router joins the organization's overlay network.

---

**Note**

For the ZTP process to succeed, Cisco vManage must contain a device configuration template for the vEdge router. If the Cisco vManage instance has no template, the ZTP process fails. Ignore the device-model and ztp-status display in the configuration preview and intent configuration. This information is visible after you push the configuration on device side.

---

**Using ZTP on Non-Wireless Routers**

The default configuration that is shipped on non-wireless hardware vEdge routers includes the following commands that allow the ZTP process to occur automatically:

- `system vbond ztp.viptela.com`—Configures the initial Cisco vBond Orchestrator to be the Cisco SD-WAN ZTP SaaS server.
- `vpn 0 interface ip dhcp-client`—Enables DHCP on one of the interfaces in VPN 0, which is the transport interface. Note that the actual interface in the default configuration varies by router model. This interface must be connected to the Internet, MPLS, metro Ethernet, or other WAN network.

Warning: For ZTP to work, do not modify or delete either of these configuration commands before you connect the vEdge router to a WAN.

**Using ZTP on Wireless Routers**

The vEdge 100m and vEdge 100wm are wireless routers. On these routers, ZTP is supported using both the cellular and the Ethernet interfaces.

---

**Note**

In Release 16.3, you cannot use the LTE USB dongle on a vEdge 1000 router for ZTP.
The vEdge 100m router supports software Releases 16.1 and later. If the vEdge 100m router is running Release 16.2.10 or later, we recommend, when performing ZTP, that Cisco vManage also be running Release 16.2.10 or later.

The vEdge 100wm router supports software Releases 16.3 and later.

The default configuration that is shipped on wireless hardware vEdge routers includes the following commands that allow the ZTP process to occur automatically on the cellular interface:

- `system vbond ztp.viptela.com` — Configure the initial Cisco vBond Orchestrator to be the Cisco SD-WAN ZTP SaaS server.

- `vpn 0 interface cellular0 ip dhcp-client` — Enable DHCP on one of the cellular interface called `cellular0` in VPN 0, which is the transport interface. This interface must be connected to the cellular network.

- `vpn 0 interface cellular0 technology` — Associate a radio access technology (RAT) with the cellular interface. In the default configuration, the RAT is set to `lte`. For ZTP to work, you must change this value to `auto`.

- `vpn 0 interface cellular0 profile 0` — Enable automatic profile selection. For firmware-dependent mobile carriers, the automatic profile uses the firmware default values. For other carriers, the automatic profile uses the Mobile Country Code/Mobile Network Code (MCC/MNC) values on the SIM card. One exception is the vEdge 100m-NT: The automatic profile tries OCN MVNO APN before the firmware default, which is NTT Docomo. If the router finds a matching entry, it autocreates profile 16, which is used for the ZTP connection. To check which profile is being used for the active ZTP connection, look at the Active profile entry in the `show cellular sessions` command output.

The `profile 0` configuration command recognizes the MCCs and MCNs listed in the vEdge SKU Information table. If your MCC/MNC is supported, you do not need to configure them in the Cellular Profile feature template or with the `profile` command. If your MCC/MNC is not supported, you must configure them manually, using the Cellular-Profile configuration template or the `profile CLI` command.

If you need to use Cisco vManage configuration templates to create the portions of the default configuration that allow ZTP to occur automatically, use the VPN-Interface-Cellular feature template. The following figure shows that in the upper portion of the template the Profile ID field is set to 0 and that in the Tunnel Interface tab the tunnel interface is enabled. In Releases 16.3.1 and later, the Technology field has been added, and the default value is "lte". To match the vEdge router's ZTP cellular0 configuration, change the value to "auto".
The following guidelines help to troubleshoot issues that can occur when using ZTP from a wireless router:

- For ZTP to work correctly, ensure that you are using the correct SIM with the correct modem model (SKU).

- If the default profile APN is not configured correctly, the ZTP process does not work correctly. If ZTP does not work, issue the `show cellular status` command to display the error. If an error occurs, configure the appropriate APN and retry the ZTP process.

- For SKUs that do not have default profile APN configurations, such as Generic (MC7304) and North America (MC7354) SKUs, if the automatic profile selection does not detect the APN on the SIM card, configure the profile, including an APN. If the router has a second circuit that has access to Cisco vManage, add the profile information, including the APN, to the feature configuration template and then
push the device template to the cellular router. Otherwise, configure the profile on the cellular router from the CLI, including an APN.

- To check whether the router is unable to detect the SIM card, issue the `show cellular status` command. Check for the SIM Read error. To correct this problem, insert the SIM card correctly in the router.

- In Release 16.3.0, after you run ZTP on a cellular router, the cellular interface is in a `no shutdown` state. Because of this, Cisco vManage is unable to push a device configuration template to the router. To correct this problem, from the CLI on the router, configure the cellular interface state to be in `shutdown` state.
Use the Cisco vManage dashboard screens (Main, VPN, ad Security) to monitor, at a glance, the overall health and security of the Cisco SD-WAN overlay network.

Top Bar
The top bar is located at the top of every Cisco vManage screen and includes the following screen elements:

- Menu icon—Click the icon to expand or collapse the Cisco vManage menu. The Cisco vManage menu is closed by default.

- Cisco vManage application server logo.

- Cloud onRamp icon—Enables Cloud onRamp service to optimize access to cloud applications. When Cloud onRamp service is enabled, the icon turns blue.

- Tasks icon—Click on the icon to see a list of all active and completed tasks started from Cisco vManage. While the task is in progress, the Tasks tab displays a counter on the top. When the task is completed, the count disappears and Completed Tasks count is incremented. To view details about any task, click the task to display its Status screen.

- Alarm bell icon—Displays the total count of all active alarms. Click on the icon to see a list of all active and cleared alarms. To view details about any alarm, click the alarm to display its Alarms Details screen.

- Help—Links to product help, software version information, and the current time and timezone on Cisco vManage.

- Hostname—Hostname of Cisco vManage that you are logged into.

- User profile drop-down—Click to sign out or edit user-related options in your profile.
View Device Pane

The Device pane, which runs across the top of the Dashboard screen, displays all control connections from the vManage NMS to the vSmart controllers, WAN Edge routers, and vBond orchestrators in the overlay network. It also displays the status of the vManage NMSs in the network.

For each device, the Device pane shows:

- Total number of connections.
• Number of up connections.
• Number of down connections.

Click the number or the Up or Down arrow to display a table with detailed information for each connection. The Dashboard page automatically refreshes when the status of the members of a vManage cluster changes.

Click the More Actions icon to the right of each table row to access the Device Dashboard or Real Time view in the Monitor > Network screen or to access the Tools > SSH Terminal screen.

**View Reboot Pane**

The Reboot pane displays the total number of reboots in the last 24 hours for all devices in the network, including soft and cold reboots and reboots that occurred as a result of power-cycling a device. Click the Reboot pane to open the Reboot popup window which lists, for each reboot, the system IP and hostname of the device that rebooted, the time the reboot occurred, and the reason for the reboot. If the same device reboots more than each, each reboot option is reported separately.

In the Reboot popup window, click the Crashes tab to list, for all device crashes, the system IP and hostname of the device on which the crash occurred, the crash index, and the core time and filename.

**View Certificates Pane**

The Certificates pane displays the state of all certificates on all controller devices, and it shows a count of all expired or invalidated certificates. Click the Certificates pane to open the Certificate Details popup window, which displays the hostname and system IP of the device on which the certificate is installed, the certificate serial number, and its expiration date and status.

**View Control Status Pane**

The Control Status pane displays whether vSmart and WAN Edge devices are connected to the required number of vSmart controllers. Each vSmart controller must connect to all other vSmart controllers in the network. Each WAN Edge router must connect to the configured maximum number of vSmart controllers.

The Control Status pane shows three counts:

• Control Up—Total number of devices with the required number of operational control plane connections to a vSmart controller.

• Partial—Total number of devices with some, but not all, operational control plane connections to vSmart controllers.

• Control Down—Total number of devices with no control plane connection to a vSmart controller.

---

**Note**

The Control Status pane depends upon both Cisco vManage control connection and vSmart control connection states.
Click any row to display a table with device details. Click the More Actions icon to the right of each table row to access the Device Dashboard or Device Details view in the Monitor > Network screen.

**View Site Health View Pane**

The Site Health View pane displays the state of a site's data connections. When a site has multiple WAN Edge routers, this pane displays the state for the entire site, not for individual devices. The Site Health View pane displays three states:

- **Full WAN Connectivity**—Total number of sites where all BFD sessions on all WAN Edge routers are in the up state.
- **Partial WAN Connectivity**—Total number of sites where a TLOC or a tunnel is in the down state. These sites still have limited data plane connectivity.
- **No WAN Connectivity**—Total number of sites where all BFD sessions on all WAN Edge routers are in the down state. These sites have no data plane connectivity.

*Note*

The Site Count includes only Sites with the installed devices that are up and running. Some Sites are excluded from the Site Count if one of the installed devices in the Site is down or if TLOC or tunnels are down (relevant for sites with two devices).

Click a row to display a popup window with detailed information on each site, node, or tunnel. Click the More Actions icon to the right of each table row to access the Device Dashboard or Real Time view in the Monitor > Network screen or the Tools > SSH Terminal screen.

**View Transport Interface Distribution**

The Transport Interface Distribution pane displays interface usage in the last 24 hours for all WAN Edge interfaces in VPN 0. This includes all TLOC interfaces. Click a row to see details of interface usage.

**View WAN Edge Inventory Pane**

The WAN Edge Inventory pane provides four counts:

- **Total**—Total number of WAN Edge routers whose authorized serial number has been uploaded on the vManage server. The serial number is uploaded in the Configuration > Devices screen.
- **Authorized**—Total number of authorized WAN Edge routers in the overlay network. These are routers marked as Valid in the Configuration > Certificates > WAN Edge List screen.
- **Deployed**—Total number of deployed WAN Edge routers. These are routers marked as Valid that are now operational in the network.
- **Staging**—Total number of WAN Edge routers in staging state. These are routers you configure at a staging site before shipping them to the actual branch and making them a part of the overlay network.
These routers do not take part in any routing decisions nor do they affect network monitoring through the vManage NMS.

Click any row to display a table with the hostname, system IP, site ID, and other details of each router.

**View WAN Edge Health Pane**

The WAN Edge Health pane displays an aggregated view for each router state and a count of how many WAN Edge routers are in that state, thereby describing the health of the hardware nodes. The three states are:

- **Normal**—Number of routers with memory, hardware, and CPU in normal state. Using less than 70% of total memory or total CPU is classified as normal.
- **Warning**—Number of routers with memory, hardware, or CPU in warning state. Using between 70% and 90% of total memory or total CPU is classified as a warning.
- **Error**—Number of routers with memory, hardware, or CPU in error state. Using more than 90% of total memory or total CPU is classified as an error.

Click the number or the state to display a table with the last one hour of memory usage, CPU utilization, and hardware-related alarms, including temperature, power supply, and PIM modules. Click the More Actions icon to the right of each table row to access the Device Dashboard or Device Details view in the Monitor > Network screen or the Tools > SSH Terminal screen.

**View Transport Health Pane**

The Transport Health pane displays the aggregated average loss, latency, and jitter for all links and all combinations of colors (for example, all LTE-to-LTE links, all LTE-to-3G links).

From the Type drop-down, select loss, latency, or jitter.

Click the Filter icon to select a time period for which to display data.

Click the Expand icon to open the Transport Health pop-up window. This full-screen window displays a more detailed view of the same information. To display the information in tabular format, click the Details tab. You can change the displayed type and time period as described above.

**View Top Applications Pane**

The Top Applications pane in the Cisco vManage Dashboard screen displays DPI flow information for traffic transiting WAN Edge routers in the overlay network.

To list top applications by VPN, select a VPN from the Filter drop-down list.

To list top applications in a larger pop-up window:

1. Click the full-screen button to the right of the Filter drop-down list.
2. In the Filter drop-down list, select the desired VPN, and then click Search.
3. Click Chart to list the applications.
4. Click **Details** to display more information about the applications.

5. Click the X in the upper right corner to close the window and return to the Dashboard screen.

### View Application-Aware Routing Pane

The Application-Aware Routing pane displays the 10 worst tunnels based on criteria you specify from the **Type** drop-down list, including loss, latency, and jitter. So, if you choose loss, this pane shows the ten tunnels with the greatest average loss over the last 24 hours.

Click any row to display a graphical representation of the data. Select a time period for which to display data or click **Custom** to display a drop-down for specifying a custom time period.

Click the **Expand** icon to open the Application-Aware Routing pop-up window. This full-screen window displays the 25 worst tunnels based on criteria you specify from the **Type** drop-down list, including loss, latency, and jitter.

### View Firewall Enforcement Pane

The FireWall Enforcement pane displays the number of sessions that were inspected or dropped over the specified time period.

Cisco’s Enterprise Firewall with Application Awareness uses a flexible and easily understood zone-based model for data traffic inspection. Zone-based firewalls allow inspection of TCP, UDP, and ICMP data traffic. A zone can contain a group of one or more VPNS. Grouping VPNS into zones allows users to establish security boundaries in the overlay network so that users can control all data traffic that passes between zones.

A firewall policy defines the conditions that the data traffic flow from the source zone must match to allow the flow to the destination zone. Firewall policies can match IP prefixes, IP ports, the protocols TCP, UDP, and ICMP, and applications. Matching flows for prefixes, ports, and protocols can be accepted or dropped, and the packet headers can be logged.

Click the **Inspected** filter to see the number of inspected data sessions.

Click the **Dropped** filter to see the number of dropped packets.

Click the **Filter** icon to select a time period for which to display data.

Click the **Expand** icon to open the FireWall Enforcement pop-up window. This full-screen window displays a more detailed view of the same information. To display the information in tabular format, click the **Details** tab. You can change the time period as described in this section.

### View Top Signature Hits Pane

The Top Signature Hits pane displays the Intrusion Prevention System (IPS) signature violations by severity or by count over the specified time period. IPS uses Cisco Talos signatures for monitoring network traffic.

Click the **By Severity** filter to filter signature violations by severity.

Click the **By Count** filter to filter signature violations by count.

Click the **Filter** icon to select a time period for which to display data.
Click the **Expand** icon to open the Top Signature Hits pop-up window. This full-screen window displays a more detailed view of the same information. To display the information in tabular format, click the Details tab. You can change the time period as described above.

### View URL Filtering Pane

The URL Filtering pane displays the number and types of URLs that were blocked or allowed over the specified time period.

Click the **Blocked** filter to see the list of blocked websites.

Click the **Allowed** filter to see the list of allowed websites.

Click the **Filter** icon to select a time period for which to display data.

Click the **Expand** icon to open the URL Filtering pop-up window. This full-screen window displays a more detailed view of the same information. To display the information in tabular format, click the **Details** tab. You can change the time period as described above.

### View Advanced Malware Protection Pane

Cisco Advanced Malware Protection (AMP) blocks malware based on file reputation and uploads unknown files to Cisco AMP Threat Grid for further analysis. This pane shows the number of file reputation and file analysis events over the specified time period.

Click the **File Reputation** filter to see the number of malicious files detected by AMP over the selected time interval.

Click the **File Analysis** filter to see the number of unknown files uploaded to Cisco AMP Threat Grid over the selected time interval.

Click the **Filter** icon to select a time period for which to display data.

Click the **Expand** icon to open the URL Filtering pop-up window. This full-screen window displays a more detailed view of the same information. To display the information in tabular format, click the **Details** tab. You can change the time period as described above.

### View Web Server Certificate Expiration Date Notification

When you establish a secure connection between your web browser and the vManage server using authentication certificates, you configure the time period for which the certification is valid, in the **Administration > Settings** screen. At the end of this time period, the certificate expires. The Web Server Certificate bar shows the expiration date and time.

Starting 60 days before the certificate expires, the vManage Dashboard displays a notification indicating that the certificate is about to expire. This notification is then redisplayed 30, 15, and 7 days before the expiration date, and then daily.
View Maintenance Windows Alert Notification

If an upcoming maintenance window is configured on the vManage server, in the Administration > Settings screen, the vManage Dashboard displays a maintenance window alert notification two days before the start of the window.
Cluster Management

Use the Administration > Cluster Management screen to create a Cisco vManage cluster and perform related tasks.

Note

We recommend that all members of a Cisco vManage cluster be located in the same data center.

We recommend that the IP addresses of all members of the Cisco vManage cluster be in the same subnet.

The members of a vManage cluster rely on timestamps to synchronize data and to track device uptime. For this time-dependent data to remain accurate, you cannot change the clock time on any one of the Cisco vManage servers of the cluster after you create the cluster.

View Available Cluster Services

To view the services that are available and reachable on all members in the Cisco vManage cluster, click the Service Reachability tab.

- Configure the Cluster IP Address of a Cisco vManage Server, on page 251
- Add a Cisco vManage Server to a Cluster, on page 252
- Configure Statistics Database to Monitor Cisco vManage, on page 253
- View Cisco vManage Service Details, on page 253
- Edit Cisco vManage Parameters, on page 254
- Update Configuration Database Login, on page 254
- Upgrade Cisco vManage Cluster, on page 255
- Manually Restart vManage Processes, on page 256
- Remove Cisco vManage from a Cluster, on page 258

Configure the Cluster IP Address of a Cisco vManage Server

When you start Cisco vManage for the first time, the default IP address of the Cisco vManage server is shown as "localhost." Before you can add a new Cisco vManage server to a cluster, you must change "localhost" to an out-of-band IP address.

Cluster interconnection between Cisco vManage servers requires that each of the servers be assigned a static IP address. Do not use DHCP to assign IP addresses to Cisco vManage servers that are to be part of a cluster. Configure the IP address on a non-tunnel interface in VPN 0.
Configure the IP Address

Configure the IP address of a Cisco vManage server before you add the server to the cluster. To do so, follow these steps:

1. In the Administration > Cluster Management > Service Configuration tab, click Add vManage. The Edit vManage screen opens.
2. From the vManage IPAddress drop-down list, choose an IP address to assign to the Cisco vManage server.
3. Enter the username and password for logging in to the Cisco vManage server.
4. Click Update.

The Cisco vManage server reboots and displays the Cluster Management screen.

Add a Cisco vManage Server to a Cluster

Add a Cisco vManage Server to a Cluster

To add a new Cisco vManage to the cluster, perform the following steps on the primary Cisco vManage server:

1. In the Administration > Cluster Management > Service Configuration tab, click Add vManage. The Add vManage screen opens.
2. From the Cisco vManage IP Address drop-down list, select an IP address to assign to the Cisco vManage server.
3. Enter the a username and password for logging in to the Cisco vManage server.
4. Enter the IP address of the Cisco vManage server you are adding to the cluster.
5. Specify the user name and password for the new Cisco vManage server.
6. Select the services to run on the Cisco vManage server. You can select from the services listed below. Note that the Application Server field is not editable. The Cisco vManage Application Server is the local Cisco vManage HTTP web server.
   - Statistics Database—Stores all real-time statistics from all Cisco SD-WAN devices in the network.
   - Configuration Database—Stores all the device and feature templates and configurations for all Cisco SD-WAN devices in the network.
   - Messaging Server—Distributes messages and shares state among all Cisco vManage cluster members.
7. Click Add. The Cisco vManage server that you just added then reboots before joining the cluster.

In a cluster, we recommend that you run at least three instances of each service.
Configure Statistics Database to Monitor Cisco vManage

View Statistics Database Space Usage

To view the amount of space available and utilized for the statistics database on the local Cisco vManage, in the Administration > Settings > Statistics Database Configuration and click View. The top of the screen shows the maximum space available for the database and the total amount of space currently being utilized. The table shows the disk space currently being utilized for each statistics type.

Configure Statistics Database

To configure the statistics database, which stores all real-time statistics from the local Cisco vManage:

1. In the Administration > Settings > Statistics Database Configuration screen, click Edit. The top of the screen specifies the maximum space available for the database.
2. For each Statistics Type field, assign the amount of storage to allocate, in gigabytes (GB). The total value of all fields cannot exceed the maximum available space.
3. Click Save.

Cisco vManage updates the storage allocations you have assigned once a day, at midnight.

View Cisco vManage Service Details

To view detailed information about the services running on a Cisco vManage server:

1. In the Administration > Cluster Management > Service Configuration tab, click the hostname of the Cisco vManage server. The vManage Details screen opens. This screen displays the process IDs of all the Cisco vManage services that are enabled on Cisco vManage.
2. Click Cluster Management in the breadcrumb in the title bar to return to the Cluster Management screen.

View Devices Connected to Cisco vManage

To view a list of devices connected to Cisco vManage:

1. To view a detailed list of all devices connected to Cisco vManage, click the Managed Devices tab in Administration > Cluster Management > Service Configuration screen.
   
   Alternatively:

1. In the Administration > Cluster Management > Service Configuration tab, for Cisco vManage, click the More Actions icon to the right of its row.
2. Click Device Connected.

If a device is connected to Cisco vManage from a cluster, ensure that you do not configure the data stream hostname to the Cisco vManage system IP address. However, you can configure the management IP address on VPN 512 or internet public IP address on VPN 0. To know more about data stream troubleshooting tools, see Data Stream Troubleshooting Tools FAQ.
Edit Cisco vManage Parameters

1. In the Administration > Cluster Management > Service Configuration tab, for a Cisco vManage, click the More Actions icon to the right of its row and click Edit. The Edit vManage screen opens.

2. Select an IP address to edit.

3. Enter the username and password, and edit the cluster services provided by that Cisco vManage.

4. Click Update.

Update Configuration Database Login

Update Configuration Database Admin User Credentials

To update the default login credentials of configuration database, access Cisco vManage using a terminal and run the following commands:

Note

Don’t use the SSH terminal option in Cisco vManage to run these commands, because it leads to losing access to the Cisco vManage GUI.

1. Use request nms application-server stop to stop application servers on all Cisco vManage servers.

2. Use one of the following commands to reset the user name and password for the configuration database:
   • For Cisco SD-WAN Release 20.1.1 and earlier:
     
     request nms configuration-db update-admin-user username username password password newusername newadminuser newpassword newpassword
   • For releases beginning with Cisco SD-WAN Release 20.1.2:
     request nms configuration-db update-admin-user
     
     When prompted, enter your current user name and password, and your new user name and password.

Note

When you execute one of the commands described above, Cisco vManage restarts the application server.

Note

a. If you do not know the default credentials of config DB, contact Cisco TAC to retrieve the credentials.

b. You cannot use an older user name.

c. Password can only be a mix of characters A to Z (upper or lowercase), digits 0-9, and special characters @#*.
Example

- For Cisco SD-WAN Release 20.1.1 and earlier:
  
  ```request nms configuration-db update-admin-user username neo4j password ******** newusername myusername newpassword mypassword```

- For releases beginning with Cisco SD-WAN Release 20.1.2:
  
  ```request nms configuration-db update-admin-user

  Enter current user name: neo47
  Enter current user password: 123
  Enter new user name: myusername
  Enter new user password: mypassword```

After configuration database admin user update, if you are unable to view a specific Cisco vManage instance, use the `request nms application-server restart` command to restart the application server on that Cisco vManage instance again.

**Upgrade Cisco vManage Cluster**

**Table 27: Feature History**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco vManage Cluster Upgrade</td>
<td>Cisco IOS XE Release 17.3.1a</td>
<td>This feature outlines the upgrade procedure for Cisco vManage servers in a cluster to Cisco vManage Release 20.3.1.</td>
</tr>
<tr>
<td></td>
<td>Cisco SD-WAN Release 20.3.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco vManage Release 20.3.1</td>
<td></td>
</tr>
</tbody>
</table>

**Upgrade Cisco vManage instances in a Cluster**

In Cisco vManage, use the **Tools > SSH Terminal** screen to establish an SSH session with Cisco vManage. From an SSH session, use the following commands to upgrade Cisco vManage instances in a cluster. For information on SSH terminal, see **SSH Terminal**.

1. Take a snapshots of all vManage servers. Take a backup of the configuration database and save it to location outside of the Cisco vManage server using the following command:
   ```request nms configuration-db backup path </home/admin/backup_file_name>```

2. Ensure that Cisco vManage release 18.3 or later is installed.

3. Copy the Cisco vManage Release 20.3.1 image on each Cisco vManage server in the cluster and install the image on each Cisco vManage server. Do not activate the image at this time:
   ```request software install <path>```

4. Stop NMS services on all Cisco vManage instances in the cluster using the following command on each Cisco vManage instance:
   ```request nms all stop```
5. Activate the Cisco vManage Release 20.3.1 or later image on each Cisco vManage server using the following command. All servers reboot simultaneously.

   `request software activate now <version>`

6. When each Cisco vManage server is active, confirm the upgrade using the following commands:

   `request software upgrade-confirm`

   This step is essential to prevent the software from reverting to the previous image version.

7. Use the following command to upgrade the configuration database on config DB node in the cluster. You can find config DB node from Cisco vManage:

   `request nms configuration-db upgrade`

   • Enter login credentials, if prompted. Login credentials are prompted if all vManage server establish control connection with each other. After a successful upgrade, all configuration-db services are UP across the cluster and the application-server is started.

8. After the vManage devices reboot, stop NMS services on all vManage devices in the cluster:

   `request nms all stop`

---

**Note**

If you are upgrading a cluster that utilizes Cisco vManage signed certificates and contains Cisco CSR100vs, Cisco ISRv (ENCS), Cisco ASR 1002-X, or any other Cisco IOS XE SD-WAN cloud-based devices, contact Cisco SD-WAN TAC Support after upgrading the cluster and before upgrading any of these devices to 17.3.x or higher.

---

**Note**

If you are upgrading a Cisco vManage cluster setup from Cisco vManage Release 20.3.1 and Cisco vManage Release 20.4.1 to Cisco vManage Release 20.5.1 or higher, you must do it through CLI.

---

**Note**

You can check the database upgrade logs at the following location:

`<vmanage-server>/var/log/nms/neo4j-upgrade.log`

For information on how to upgrade Cisco vManage clusters through Cisco vManage GUI, refer to [Upgrade the Software Image on a Device](#).

---

**Manually Restart vManage Processes**

When the cluster is in a bad state as part of the upgrade, you should manually restart the NMS processes. Restart the processes one at a time in an orderly manner instead of using `request nms all restart` or a similar command. The following manual restart order might vary for your cluster, depending on what services you are running on the vManage devices in the cluster. The following order is based on a basic cluster with three vManage devices.
Consider bringing up the services manually as mentioned in the following method whenever you have to reboot a vManage device or after an upgrade.

1. On each vManage device, stop all NMS services.
   request nms all stop

2. Verify that all services have stopped. It is normal for the above command to give some message about failing to stop a service if it takes too long, so use the following command to verify that everything is stopped before proceeding.
   request nms all status

3. Start the Statistics database on each device that is configured to run it. Wait for the service to start each time before proceeding to the next vManage device.
   request nms statistics-db start

4. Verify that the service is started before proceeding to start it on the next vManage. After service starts, perform step 3 to start the Statistics database on the next vManage device. Once all the vManage devices have the Statistics database running, proceed to the next step.
   request nms statistics-db status

5. Start the Configuration database on each device that is configured to run it. Wait for the service to start each time before proceeding to the next vManage device.
   request nms configuration-db start

6. Verify that the service has started before proceeding to start it on the next vManage device. Go to vshell and tail a log file to look for a database is online message. When confirmed, go to step 5 to start the Configuration database on the next vManage device. After all vManage devices have the Configuration database running, proceed to the next step.
   tail -f -n 100 /var/log/nms/vmanage-orientdb-database.log

7. Start the Coordination server on each device. Wait for the service to start each time before proceeding to the next vManage device.
   request nms coordination-server start

8. Verify that the service is started before proceeding to start it on the next vManage device. After verifying, go to step 7 to start the Coordination server on the next vManage device. After the Coordination server runs on all the vManage devices, proceed to the next step.
   request nms coordination-server status

9. Start the Messaging server on each device. Wait for the service to start each time before proceeding to the next vManage device.
   request nms messaging-server start

10. Verify that the service has started before proceeding to start it on the next vManage device. After verifying, go to step 9 to start the Messaging server on the next vManage device. After the Messaging server runs on all vManage devices, proceed to the next step.
    request nms messaging-server status

11. Start the Application server on each device. Wait for the service to start each time before proceeding to the next vManage device.
12. Verify that the service has started before proceeding to start it on the next vManage device. To verify if the service is fully started, open the GUI of that vManage device. After the GUI is fully loaded and you are able to log in, go to step 11 to start the Application server on the next vManage device.

13. Restart the NMS cloud services on each device. Wait for the service to start each time before proceeding to the next vManage device.

    request nms cloud-agent start

14. Verify that the service has started before proceeding to start it on the next vManage device. After verifying, go to step 12 to start the cloud services on the next vManage device. After the cloud services run on all vManage devices, proceed to the next step.

    request nms cloud-agent status

15. For Cisco vManage Release 20.3.1 and later releases, on each Cisco vManage device, start the server-proxy service as follows:

    request nms server-proxy start

16. To verify that there are no errors and everything has loaded cleanly, tail the log files.

Remove Cisco vManage from a Cluster

1. In the Administration > Cluster Management > Service Configuration tab, click the More Actions icon to the right of its row and click Remove. The Remove vManage dialog box opens.

2. Enter the username and password to confirm removal of the device from the network.

3. Click Remove.

The Cisco vManage instance is removed from the cluster, the device is invalidated, and the certificates for that device are deleted. The remaining members in the cluster rebalance the network management services.

Note

You can only remove n - 2 Cisco vManage instances from a cluster of n instances. You must retain at least two Cisco vManage instances in a cluster.
Enterprise Certificates

In the Cisco IOS XE SD-WAN Release 16.11.1 and Cisco SD-WAN Release 19.1, enterprise certificates were introduced. Enterprise certificates replace the controller certificates authorization that were used previously.

**Note**

When using enterprise certificates for Cisco SD-WAN devices and controllers, make sure to use root certificates with a RSA key that is at least 2048 bit.

**Note**

For purposes of certificate management, the term *controller* is used to collectively refer to the vManage NMS, the vSmart controller, and the vBond orchestrator.

**Note**

For additional information about enterprise certificates, see the Cisco SD-WAN Controller Certificates and Whitelist Authorization File Prescriptive Deployment Guide.

Use the Certificates screen to manage certificates and authenticate WAN edge and controller devices in the overlay network.

Two components of the Cisco SD-WAN solution provide device authentication:

- Signed certificates are used to authenticate devices in the overlay network. Once authenticated, devices can establish secure sessions between each other. It is from the vManage NMS that you generate these certificates and install them on the controller devices—vManage NMSs, vBond orchestrators, and vSmart controllers.

- WAN edge authorized serial number file contains the serial numbers of all valid vEdge and WAN routers in your network. You receive this file from Cisco SD-WAN, mark each router as valid or invalid, and then from the vManage NMS, send the file to the controller devices in the network.

You must install the certificates and the WAN edge authorized serial number file on the controller devices to allow the Cisco SD-WAN overlay network components to validate and authenticate each other and thus to allow the overlay network to become operational.

- Manage Certificates in Cisco vManage, on page 260
- Manage Root Certificate Authority Certificates in Cisco vManage, on page 265
Manage Certificates in Cisco vManage

Perform certificate operations in Cisco vManage on the **Configuration > Certificates** page.

- **Top bar**—On the left are the menu icon, for expanding and collapsing the Cisco vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.

- **Title bar**—Includes the title of the screen, Certificates.

- **WAN Edge List tab**—Install the router authorized serial number file on the controllers in the overlay network and manage the serial numbers in the file. When you first open the Certificates screen, the WAN Edge List tab is selected.
  - Send to Controllers—Send the WAN edge router chassis and serial numbers to the controllers in the network.
  - Table of WAN edge routers in the overlay network—To re-arrange the columns, drag the column title to the desired position.

- **Controllers tab**—Install certificates and download the device serial numbers to the vBond orchestrator.
  - Send to vBond—Send the controller serial numbers to the Cisco vBond Orchestrator.
  - Install Certificate—Install the signed certificates on the controller devices. This button is available only if you select Manual in **Administration > Settings > Certificate Signing by Symantec**.
  - Export Root Certificate—Display a copy of the root certificate for the controller devices that you can download to a file.
  - Table of controller devices in the overlay network—To re-arrange the columns, drag the column title to the desired position.

- **Certificate status bar**—Located at the bottom of the screen, this bar is available only if you select Server Automated in **Administration > Settings > Certificate Authorization**. It displays the states of the certificate installation process:
  - Device Added
  - Generate CSR
  - Waiting for Certificate
  - Send to Controllers

A green check mark indicates that the step has been completed. A grey check mark indicates that the step has not yet been performed.

- **Search box**—Includes the Search Options drop-down, for a Contains or Match string.

- **Refresh icon**—Click to refresh data in the device table with the most current data.
Check the WAN Edge Router Certificate Status

In the **WAN Edge List** tab, check the **Validate** column. The status can be one of the following:

- **Valid** (shown in green) — The router's certificate is valid.
- **Staging** (shown in yellow) — The router is in the staging state.
- **Invalid** (shown in red) — The router's certificate is not valid.

Validate a WAN Edge Router

When you add Cisco vEdge devices and WAN routers to the network using the **Configuration > Devices** screen, you can automatically validate the routers and send their chassis and serial numbers to the controller devices by clicking the checkbox **Validate the uploaded WAN Edge List and send to controllers**. If you do not select this option, you must individually validate each router and send their chassis and serial numbers to the controller devices. To do so:

1. In the **WAN Edge List** tab, select the router to validate.
2. In the **Validate** column, click **Valid**.
3. Click **OK** to confirm the move to the valid state.
4. Repeat the steps above for each router you wish to validate.
5. Click the **Send to Controllers** button in the upper left corner of the screen to send the chassis and serial numbers of the validated routers to the controller devices in the network. Cisco vManage NMS displays the Push WAN Edge List screen showing the status of the push operation.

### Stage a WAN Edge Router

When you initially bring up and configure a WAN Edge router, you can place it in staging state using the Cisco vManage NMS. When the router is in this state, you can configure the router, and you can test that the router is able to establish operational connections with the vSmart controller and the vManage NMS.

After you physically place the router at its production site, you change the router's state from staging to valid. It is only at this point that the router joins the actual production network. To stage a router:

1. In the WAN Edge List tab, select the router to stage.
2. In the **Validate** column, click **Staging**.
3. Click **OK** to confirm the move to the staging state.
4. Click **Send to Controllers** in the upper left corner of the screen to sync the WAN edge authorized serial number file with the controllers. vManage NMS displays the Push WAN Edge List screen showing the status of the push operation.
5. To unstage, validate the WAN Edge Router.

### Invalidate a WAN Edge Router

1. In the WAN Edge List tab, select the router to invalidate.
2. In the **Validate** column, click **Invalid**.
3. Click **OK** to confirm the move to the invalid state.
4. Repeat the steps above for each router you wish to invalidate.
5. Click the **Send to Controllers** button in the upper left corner of the screen to send the chassis and serial numbers of the validated routers to the controller devices in the network. Cisco vManage NMS displays the Push WAN Edge List screen showing the status of the push operation.

### Send the Controller Serial Numbers to Cisco vBond Orchestrator

To determine which controllers in the overlay network are valid, the Cisco vBond Orchestrator keeps a list of the controller serial numbers. The Cisco vManage NMS learns these serial numbers during the certificate-generation process.

To send the controller serial numbers to the Cisco vBond Orchestrator:

1. In the **Controllers** tab, check the certificate status bar at the bottom of the screen. If the **Send to Controllers** check mark is green, all serial numbers have already been sent to the Cisco vBond Orchestrator. If it is grey, you can send one or more serial numbers to the Cisco vBond Orchestrator.
2. Click the **Send to vBond** button in the **Controllers** tab. A controller's serial number is sent only once to the Cisco vBond Orchestrator. If all serial numbers have been sent, when you click **Send to vBond**, an
error message is displayed. To resend a controller’s serial number, you must first select the device and then select **Invalid** in the **Validity** column.

After the serial numbers have been sent, click the **Tasks** icon in the Cisco vManage toolbar to display a log of the file download and other recent activities.

### Install Signed Certificate

If in **Administration > Settings > Certificate Signing by Symantec**, you selected the **Manual** option for the certificate-generation process, use the **Install Certificate** button to manually install certificates on the controller devices.

After Symantec or your enterprise root CA has signed the certificates, they return the files containing the individual signed certificates. Place them on a server in your local network. Then install them on each controller:

1. In the **Controllers** tab, click **Install Certificate**.
2. In the **Install Certificate** window, select a file, or copy and paste the certificate text.
3. Click **Install** to install the certificate on the device. The certificate contains information that identifies the controller, so you do not need to select the device on which to install the certificate.
4. Repeat Steps the steps above to install additional certificates.

### Export Root Certificate

1. In the **Controllers** tab, click the **Export Root Certificate** button.
2. In the **Export Root Certificate** window, click **Download** to export the root certificate to a file.
3. Click **Close**.

### View a Certificate Signing Request

1. In the WAN Edge List or **Controllers** tab, select a device.
2. Click the **More Actions** icon to the right of the row, and click **View CSR** to view the certificate signing request (CSR).

### View a Device Certificate Signing Request

1. In the **WAN Edge List** or **Controllers** tab, select a Cisco IOS XE SD-WAN device.
2. Click the **More Actions** icon to the right of the row, and click **View Device CSR** to view the certificate signing request (CSR).

For a Cisco IOS XE SD-WAN device where trustpoint has been configured, clicking the **More Actions** icon allows you to view three options:

- View Device CSR
- Generate Feature CSR
View Feature CSR

View the Certificate

1. In the Controllers tab, select a device.
2. Click the More Actions icon to the right of the row and click View Certificate.

Generate a Certificate Signing Request

1. In the Controllers tab, select a device.
2. Click the More Actions icon to the right of the row and click Generate CSR.
3. In the Generate CSR window, click Download to download the file to your local PC (that is, to the PC you are using to connect to the Cisco vManage NMS).
4. Repeat the steps above for each controller for which you are generating a CSR.

Generate a Feature Certificate Signing Request

1. In the WAN Edge List tab, choose a Cisco IOS XE SD-WAN device.
2. Click the More Actions icon to the right of the row and click Generate Feature CSR.
3. In the Generate Feature CSR window, click OK to continue with the generation of feature CSR. This step authenticates the device trustpoint that has been set and extracts the CSR from the device.
4. Repeat the steps above for each device for which you are generating a CSR.

Reset the RSA Key Pair

1. In the Controllers tab, select a device.
2. Click the More Actions icon to the right of the row and click Reset RSA.
3. Click OK to confirm resetting of the device's RSA key and to generate a new CSR with new public or private keys.

Invalidate a Device

1. In the Controllers tab, select a device.
2. Click the More Actions icon to the right of the row and click Invalidate.
3. Click OK to confirm invalidation of the device.
View Log of Certificate Activities

To view the status of certificate-related activities:

1. Click the Tasks icon located in the vManage toolbar. Cisco vManage NMS displays a list of all running tasks along with the total number of successes and failures.
2. Click a row to see details of a task. Cisco vManage NMS opens a status window displaying the status of the task and details of the device on which the task was performed.

View a Signed Certificate

Signed certificates are used to authenticate Cisco SD-WAN devices in the overlay network. To view the contents of a signed certificate using Cisco vManage:

1. In Cisco vManage, select the Configuration ➤ Certificates screen.
2. From the Certificates title bar, select Controllers.
3. Select the device whose certificate you wish to view.
4. Click the More Actions icon to the right of the row, and select View Certificate to view the installed certificate.

Manage Root Certificate Authority Certificates in Cisco vManage

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for Managing Root CA Certificates in Cisco vManage</td>
<td>Cisco IOS XE Release 17.4.1a&lt;br&gt;Cisco SD-WAN Release 20.4.1&lt;br&gt;Cisco vManage Release 20.4.1</td>
<td>This feature enables you to add and manage root certificate authority (CA) certificates.</td>
</tr>
</tbody>
</table>

Add a Root Certificate Authority Certificate

1. In Cisco vManage, choose Administration > Root CA Management.
2. Click Modify Root CA.
3. In the Root Certificate field, paste in certificate text, or click Select a File to load a certificate from a file.
4. Click Add. The new certificate appears in the certificate table. The Recent Status column indicates that the certificate has not yet been installed.
5. Click Next and review the details of any certificates that have not been installed.
6. Click Save to install the certificate(s). The new certificate appears in the certificate table.
View a Root Certificate Authority Certificate

1. In Cisco vManage, choose Administration > Root CA Management.
2. (optional) In the search field, enter text to filter the certificate view. You can filter by certificate text or attribute values, such as serial number.
3. In the table of certificates, click More Actions (…) and choose View. A pop-up window appears, displaying the certificate and its details.

Delete a Root Certificate

Use this procedure to delete a root Certificate Authority (CA) certificate.

1. In Cisco vManage, choose Administration > Root CA Management.
2. Click Modify Root CA.
3. Select one or more root certificates in the table and click the trash icon in the Action column. The table shows the certificate as marked for deletion.
4. Click Next and review the details of any certificates that are marked for deletion.
5. Click Save to delete the certificate(s).

Enable Reverse Proxy

In a standard overlay network, routers initiate direct connections to the Cisco SD-WAN controllers—Cisco vManage and Cisco vSmart Controllers—over which they exchange control plane information. Because routers are typically located in branch sites and hence access the Cisco SD-WAN controllers over the internet, the result is that Cisco vManage and Cisco vSmart Controllers have connections directly to the internet.

If, for security or other reasons, you do not want these devices to have direct internet connections, you can insert a reverse proxy between the Cisco SD-WAN controllers and the routers. The reverse proxy acts as an intermediary to pass control traffic between the Cisco SD-WAN controllers and the routers. So instead of communicating directly with Cisco vManage and the Cisco vSmart Controllers, the routers communicate directly with the intermediate proxy device, and the proxy device relays the traffic to and from Cisco vManage and Cisco vSmart Controller controller devices.

The following figure illustrates a reverse proxy inserted between a router and the vSmart and vManage controllers.
Enable Reverse Proxy

To enable reverse proxy services in the overlay network:

1. Click the Edit button to the right of the Reverse Proxy bar.
2. Click Enabled.
3. Click Save.

To configure reverse proxy on individual Cisco vManage and Cisco vSmart Controller devices, in Cisco vManage, select Configuration > Devices and click the Controllers tab. For the desired device, click the More Actions icon to the right of the row, and click Add Reverse Proxy. Configure the private and proxy IP addresses and ports for the device.

Provision Certificates on the Proxy

For reverse proxy to work, the reverse proxy device and the routers must authenticate each other.

On the reverse proxy device you must provision a certificate that is signed by the same CA with which the Cisco SD-WAN controller’s certificate is signed.

This certificate is used by the reverse proxy to verify the routers.

Generate a Certificate Signing Request for the Reverse Proxy

To generate a Certificate Signing Request (CSR) for the reverse proxy and have it signed by Cisco, do the following:

1. Run the following command on the proxy. See the table for values to enter when prompted.

   ```bash
   proxy$ openssl req -new -days 365 -newkey rsa:2048 -nodes -keyout Proxy.key -out Proxy.csr
   ```
Enable Reverse Proxy

<table>
<thead>
<tr>
<th>Property</th>
<th>What to enter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country Name (2 letter code)</td>
<td>Any country code.</td>
</tr>
<tr>
<td></td>
<td>Example: US</td>
</tr>
<tr>
<td>State or Province Name (full name)</td>
<td>Any state or province.</td>
</tr>
<tr>
<td></td>
<td>Example: CA</td>
</tr>
<tr>
<td>Locality Name (eg, city)</td>
<td>Any locality.</td>
</tr>
<tr>
<td></td>
<td>Example: San Jose</td>
</tr>
<tr>
<td>Organization Name (eg, company)</td>
<td>Use either &quot;viPtel Inc&quot; or &quot;Viptela LLC&quot;.</td>
</tr>
<tr>
<td></td>
<td>Example: Viptela LLC</td>
</tr>
<tr>
<td>Organizational Unit Name (eg, section)</td>
<td>Use the “organization” name configured on the overlay.</td>
</tr>
<tr>
<td></td>
<td>Example: cisco-sdwan - 12345</td>
</tr>
<tr>
<td>Common Name (eg, fully qualified host name)</td>
<td>Host name ending with “.viptela.com”.</td>
</tr>
<tr>
<td></td>
<td>Example: proxy.viptela.com</td>
</tr>
<tr>
<td>Email Address</td>
<td>Use any valid email address.</td>
</tr>
<tr>
<td></td>
<td>Example: <a href="mailto:someone@example.com">someone@example.com</a></td>
</tr>
</tbody>
</table>

2. Get the CSR signed by Cisco:
   • If you use Symantec/Digicert on the controllers, open a case with Cisco TAC to sign the CSR.
   • If you Cisco Public Key Infrastructure (PKI), submit the CSR on the Cisco Network Plug and Play (PnP) application and retrieve the signed certificate.

Configure Reverse Proxy on Controllers

To configure reverse proxy on individual Cisco vManage and Cisco vSmart Controller devices:

1. In Cisco vManage select the Configuration > Devices screen.
2. Click the Controllers tab.
3. For the desired device, click the More Actions icon to the right of the row, and click Add Reverse Proxy. The Add Reverse Proxy popup is displayed.
4. Click Add Reverse Proxy.
5. Configure the private IP address and port number for the device. The private IP address is the IP address of the transport interface in VPN 0. The default port number is 12346. This is the port used to establish the connections that handle control and traffic in the overlay network.
6. Configure the proxy IP address and port number for the device, to create the mapping between the private and public IP addresses and port numbers.
7. If the Cisco vManage or Cisco vSmart Controller has multiple cores, repeat Steps 5 and 6 for each core.
8. Click Add.

9. In the Security feature configuration template for Cisco vManage and the Cisco vSmart Controller, set the transport protocol to be TLS.

To display a device's private and proxy (public) IP addresses and port numbers, in the vManage Monitor > Network screen, select the device, click Real Time, and select the Control Connections command. To display these IP address and port numbers in the CLI, issue the `show control local-properties` command.

To verify the mapping between the private and proxy IP addresses and port numbers, issue the `show orchestrator reverse-proxy-mapping` command on the Cisco vBond Orchestrator.

In the output of the `show control connections` command on a router, if the Proxy column value is Yes, the Peer Public IP and Peer Public Port fields show the proxy IP address and port number, respectively, and the output indicates that the connection is the controller device is through the proxy.

**Have Router Generate Certificate**

After you configure reverse proxy on the overlay network controllers, any router that joins the overlay network or that is already operating in the overlay network requires a signed certificate to establish a secure connection to the proxy device. The process for generating the signed certificate is initiated automatically by the router as soon as it learns that reverse proxy is enabled in the network, and the router receives a signed certificate that it uses to establish a secure connection to the reverse proxy device.

To view the signed certificate, issue the `show certificate reverse-proxy` command on the router.

---

### Configure Enterprise Certificates for Cisco SD-WAN Devices and Controllers

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for Secondary Organizational Unit</td>
<td>Cisco IOS XE Release 17.2.1r</td>
<td>This optional feature allows you to configure a secondary organizational unit when configuring the certificates. If specified, this setting is applied to all controllers and edge devices.</td>
</tr>
<tr>
<td></td>
<td>Cisco SD-WAN Release 20.1.1</td>
<td></td>
</tr>
<tr>
<td>Support for Subject Alternative Name (SAN)</td>
<td>Cisco IOS XE Release 17.4.1a</td>
<td>This feature enables you to configure subject alternative name (SAN) DNS Names or uniform resource identifiers (URIs). It enables multiple host names and URIs to use the same SSL certificate.</td>
</tr>
<tr>
<td></td>
<td>Cisco SD-WAN Release 20.4.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco vManage Release 20.4.1</td>
<td></td>
</tr>
</tbody>
</table>

Enterprise certificates allow organizations to use their own private certificate signing authority rather than having to rely on public certificate signing authorities. You can also apply custom certificate properties using the Set CSR Properties field.
In the 16.11/19.1 release, enterprise certificates were introduced. Enterprise certificates replace the controller certificates authorization that were used previously. An independent organization handles the signing of enterprise certificates.

Use the Configuration > Certificates screen to manage certificates and authenticate WAN edge and controller devices in the overlay network.

Two components of the Cisco SD-WAN solution provide device authentication:

- Signed certificates are used to authenticate devices in the overlay network. Once authenticated, devices can establish secure sessions between each other. It is from the vManage NMS that you generate these certificates and install them on the controller devices—vManage NMSs, vBond orchestrators, and vSmart controllers.

- WAN edge authorized serial number file contains the serial numbers of all valid vEdge and WAN routers in your network. You receive this file from Cisco Plug and Play (PnP), mark each router as valid or invalid, and then from the vManage NMS, send the file to the controller devices in the network.

You must install the certificates and the WAN edge authorized serial number file on the controller devices to allow the Cisco SD-WAN overlay network components to validate and authenticate each other and thus to allow the overlay network to become operational.

For purposes of certificate management, the term controller is used to collectively refer to the vManage NMS, the vSmart controller, and the vBond orchestrator.

Once you reset a WAN edge device, you have to install the enterprise root certificate manually on the device. If you perform an upgrade, your certificate is retained.

Cisco vManage supports only Base 64 encoded certificates. Other formats, such as DER, encoded are not supported.

For example, the PEM extension is used for different types of X.509v3 files that contain ASCII (Base64) armored data prefixed with a --BEGIN ... line.

### Enterprise Certificate Supported Devices

The following are the supported enterprise supported devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>vManage</td>
<td>Yes</td>
</tr>
<tr>
<td>vBond</td>
<td>Yes</td>
</tr>
<tr>
<td>vSmarts</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Configure Enterprise Certificates for Cisco SD-WAN Devices and Controllers

**Device**

<table>
<thead>
<tr>
<th>Edges</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>All hardware WAN edges</td>
</tr>
<tr>
<td></td>
<td>vEdge/IOS-XE-SD-WAN</td>
</tr>
<tr>
<td></td>
<td>except ASR1002-X, ISRv,</td>
</tr>
<tr>
<td></td>
<td>CSR1000v</td>
</tr>
</tbody>
</table>

**Configuring Enterprise Certificates**

1. Navigate to **Administration > Settings > Hardware WAN Edge Certificate Authorization** and choose **Edit**.

2. Click **Enterprise Certification** (signed by Enterprise CA).

   **Security**: **On Box Certificate (TPM/SUDI Certificate)** is the default option.

3. Click **Set CSR Properties** if you want to specify custom certificate properties. The following properties are listed under the CSR Properties checkbox.

   - Domain Name
   - Organizational Unit

**Note**

Organizational Unit is a noneditable field. Organization Unit needs to be the same as Organization Name on vManage.
Configure Enterprise Certificates for Cisco SD-WAN Devices and Controllers

- Secondary Organization Unit: This optional field is only available in Cisco IOS XE Release 17.2 or Cisco SD-WAN Release 20.1.x and onwards. Note that if this optional field is specified, it will be applied to all controllers and edge devices.

- Organization
- City
- State
- Email
- 2-Letter Country Code

- Subject Alternative Name (SAN) DNS Names: (optional) You can configure multiple host names to use the same SSL certificate. Example: cisco.com and cisco2.com

- Subject Alternative Name (SAN) URIs: (optional) You can configure multiple uniform resource identifiers (URIs) to use the same SSL certificate. Example: cisco.com and support.cisco.com

4. Choose **Select a file** to upload a root certificate authority file.
   The uploaded root certificate authority displays in the text box.

5. Select **Save**.

6. Navigate to **Configuration > Devices**.

7. Select the **Upload WAN Edge List** tab.

8. Browse to the location of the Cisco IOS XE SD-WAN devices and Cisco vEdge devices list and click **Upload**.

9. At the **Configuration > Certificates** page, using the **More options**, select the appropriate action, **View Enterprise CSR**, **View Enterprise Certificate**, **Renew Enterprise CSR**, or **Revoke Enterprise Certificate**.

   - **View Enterprise CSR** (certificate signing request): Copy the CSR and sign it using the enterprise root certificate, and upload the signed certificate on vManage using the Install Certificate operation. vManage automatically discovers on which hardware edge the certificate needs to be installed on.

   - **View Enterprise Certificate**: After the certificate is installed, you can see the installed certificate and download it.

   - **Renew Enterprise CSR**: If you need to install a new certificate on the hardware device, you can use the Renew Enterprise CSR option. The Renew Enterprise CSR option generates the CSR. You can then view the certificate (View Enterprise CSR option) and install the certificate (Install Certificate option). This step flaps the control connections as a new serial number. You can see the new serial number and expiry data on the Configuration > Certificates page.

   - **Revoke Enterprise Certificate**: This option removes the enterprise certificate from the device and moves it back to prestaging. The device has only vBond and vManage controls up.

For a Cisco IOS XE SD-WAN device, using the **More options**, select the appropriate action, **View Feature CSR**, **View Feature Certificate**, or **Revoke Feature Certificate**.

   - **View Feature CSR**:
     - Copy the CSR available from the Cisco IOS XE SD-WAN device.
• Sign the certificate using the enterprise root certificate from a certifying authority.

• Upload the signed certificate on Cisco vManage using the Install Feature Certificate operation.

Cisco vManage automatically discovers on which hardware edge the certificate needs to be installed. After you install feature certificate, the option View Feature Certificate is available.

• View Feature Certificate: After you install the feature certificate, you can view the feature certificate and download it.

• Revoke Feature Certificate: This option removes the feature certificate or trustpoint information from the Cisco IOS XE SD-WAN device. After revoking a certificate, all actions against devices are not available. To view all actions for a device, ensure that you configure logging information of the device to a Transport Layer Security (TLS) profile with authentication type as server, and then configure back to mutual. Alternatively, to view the actions, reset Cisco IOS XE SD-WAN device to factory default configuration.

To reset a device to factory default:

• Click Configuration > Templates.

• Create a device template with the factory-default template.

The factory-default template is, Factory_Default_feature-name_Template. See Create a Device Template from Feature Templates for information about creating a device template with feature template.

10. Select Install Certificate or Install Feature Certificate to upload the signed certificate.

The certificate has to be a signed certificate. Initially, the state is CSR Generated.

The state changes to Certificate Installed when successfully installed.

11. On the Configuration > Certificates page, you can see enterprise certificate columns, including the device type, chassis-id, enterprise serial number, and enterprise certificate date.

Generating a Bootstrap Configuration

The on-site bootstrap process involves generating a bootstrap configuration file that loads from a bootable USB drive or from internal boot flash to a device that supports SD-WAN. When the device boots, it uses the information in the configuration file to come up on the network.

Note

If you need to generate a bootstrap configuration, use the Configuration > Devices page, and choose Generate Bootstrap Configuration under More options.

Deleting a WAN Edge Device

Before deleting a WAN edge device, invalidate the device on the Configuration > Certificates page.
Authorize a Controller Certificate

1. In Cisco vManage, click Administration > Settings.
2. In the Controller Certificate Authorization section, click Edit.
3. Click Enterprise Root Certificate. If a warning appears, click Proceed to continue.
4. Click Set CSR Properties.
5. Paste an SSL certificate into the Certificate field or click Select a file and navigate to an SSL certificate file.
6. (Optional) In the Subject Alternative Name (SAN) DNS Names field, you can enter multiple host names to use the same SSL certificate.
   Example: cisco.com and cisco2.com
7. (Optional) In the Subject Alternative Name (SAN) URIs field, you can enter multiple URIs to use the same SSL certificate.
   Example: cisco.com and support.cisco.com
   This is helpful for an organization that uses a single certificate for a host name, without using different subdomains for different parts of the organization.

Using Controller Certificates with Cisco PKI

From software release 19.x and onwards, there is an option to use Cisco as the certificate authority (CA) instead of Symantec/Digicert for the controller certificates.

This section goes through the different deployment types, scenarios to administer, install, and troubleshoot controller certificates using Cisco public key infrastructure (PKI). Cisco PKI provides certificate management to support security protocols such as IP Security (IPSec), secure shell (SSH), and secure socket layer (SSL).

The major difference between Symantec/Digicert and Cisco PKI certificates is that Cisco PKI certificates are linked to a customer's Smart Account (SA) and Virtual Account (VA) in Plug and Play (PnP) and do not require manual approval using a portal like Digicert. Each VA has a limit of 100 certificates; that is, each overlay has a limit of 100 certificates and once the certificate signing request (CSR) is generated, the approval and installation happens automatically if the vManage Settings are set correctly.

Devices are added and certificates are installed automatically from the Cisco PKI servers. There is no human intervention required to approve the certificate.

Supported Devices for Cisco PKI Certificates

The following are the supported devices for using Cisco PKI certificates.

<table>
<thead>
<tr>
<th>Device</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco vManage</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco vBond Orchestrator</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Use Case: Cisco-Hosted Cloud Overlays with Software Version 19.x and Above

Prerequisites
Cisco vManage and the controllers should all be running the same 19.x software version.

Ensure OOB IP address and credentials are updated at Configuration > Devices > Controllers tab and click on the More (dot) menu. Make sure it is updated for all the controllers.

You can verify the software version for the new or expired overlays without having control connections using SSH.

1. SSH to each of the controllers and the version should show during the SSH process.

2. You do not need to actually have the credentials work, therefore you can run this on a controller where the credentials do not work.

   Repeat this process for all the controllers in the overlay to make sure.

3. Customer Smart Account credentials need to be ready using either of the following methods:
   a. Email and request the customer contact from PnP trigger notifications to individually email you and provide the Smart Account credentials.

   or

   b. Email and request the customer contact to log on to Cisco vManage and add them. Also ensure that you ask the customer for their IPs to be added to the allowed list.

   Ensure that if asking the customer to provide their customer contact to log on, this step is done after asking the customer for their IPs to be added to the allowed list, so that they can reach the Cisco vManage GUI, be able to log in, and input their Smart Account credentials.

   You can find your Smart Account credentials in the Cisco vManage GUI in Administration ► Settings ► Smart Account Credentials at the bottom of the page.

   Enter the user name and password and select Save.
Runbook to Request and Install Cisco PKI Certificates

1. Verify that you have satisfied the prerequisites and that you have added the Smart Account credentials.
3. Select the radio button Cisco Automated (Recommended).

Note: You get an error if the Smart Account credentials are not added. Check the prerequisites.

4. Set the validity period to 1 year for POCs, 2 years for production overlays in the drop-down.
5. Set Certificate Retrieve Interval to 1 minute and press Save.

Note: Currently there is no customer email field to notify customers about approval because the certificates are auto-approved as soon as the CSR request is done.

6. From this step onwards, the process is the same as for the Symantec/Digicert controllers in the Cisco vManage GUI.
   Navigate to the Configuration ► Certificates ► Controllers tab. Click on the More (dot) menu on the right ► Generate CSR.
   The operation status shows the CSR sent for signing, the certificate signed and installed automatically without needing human intervention.

7. The certificates get installed automatically and shows the expiration date and status of a successful install.
   The operation status shows Installed for vBonds and vBond Updated for vSmarts and Cisco vManage along with the certificate serial number.

8. Ensure that the control connections have come up to the controllers on the Cisco vManage dashboard.

Use Case: Migration of an Active Existing Overlay from Digicert to Cisco PKI Controller Certificates During Certificate Renewal

Prerequisites

Cisco vManage, controllers, and vEdges should all have their control connections up.
Ensure OOB IP address and credentials are updated at Configuration > Devices > Controllers tab and click on the More (dot) menu. Make sure it is updated for all the controllers.

1. Verify that the control connections to controllers and vEdges are up in the Cisco vManage GUI dashboard.
   If the control connections are not up, let the customer know that migrating from Digicert to Cisco PKI cannot proceed until the control is up.
   If the control connections are only partially up, that is some vEdges are control down, then let the customer know that those vEdges will not be able to automatically reconnect to the controllers if their control comes up once the certificates have been moved to Cisco PKI.
If it is a case of expired certificates and control connections are down, then certificates need to be renewed on Digicert first and control connections need to be brought up before migrating them to the Cisco PKI controller certificates.

2. Verify that the software version of the controllers is 19.x.

**How to Verify the Software Version for the Active Existing Overlays (with Valid Control Connections to Controllers) Using the Cisco vManage GUI**

a. Navigate to the Maintenance ► Software Upgrade in the Cisco vManage GUI menu.

b. Select the vManage tab and look for the column Current Version. Verify that it is 19.x or above.

If the control connections are up and Cisco vManage and controller versions are not 19.x, then let the customer know to upgrade them to 19.x first (vEdges need not be upgraded) before migration to Cisco PKI can be done.

---

**Note**

It is mandatory that controllers upgraded to 19.x should immediately have their certificates renewed with Cisco PKI as part of the upgrade; they cannot be allowed to run with the existing Symantec certificates even if those certificates are going to remain valid.

---

c. Once the prerequisites are verified, check that the Cisco PKI root-CA has been propagated to all the controllers and the vEdges.

This requires SSH access to the controllers.

1. SSH into the Cisco vManage and controllers and run the following command: `show certificate root-ca-cert | include Cisco`.

   If the output is blank or does not show the result, escalate to the cloud infrastructure team.

d. Customer Smart Account credentials need to be ready by either of the following methods:

   1. Email and request the customer contact from a PnP trigger notification to individually email you and provide the Smart Account credentials.

   or

   2. Email and request your customer contact to log on to the Cisco vManage themselves and add them. Also ensure that you ask for the customer IPs to be added to the allowed list.

      Ensure that if asking the customer to provide, this step is done after asking the customer for their IPs to be added to the allowed list, so that they can reach the Cisco vManage GUI, be able to log on, and input the Smart Account Credentials.

      You can find the Smart Account credentials in the Cisco vManage GUI at Administration ► Settings ► Smart Account Credentials (at the very bottom).

3. Enter the username and password and press Save.

   Once all the prerequisites have been satisfied, follow the Runbook to Request and Install Cisco PKI Certificates to request CSRs and get the Cisco certificates installed. Verify that all the control connections to the controllers and the vEdges have come back up. If not, then escalate to the cloud infrastructure team.
Runbook to Request and Install Cisco PKI Certificates

1. Verify that you have satisfied the prerequisites and that you have added the Smart Account credentials.
3. Select the radio button Cisco Automated (Recommended).

---

Note
You get an error if the Smart Account credentials are not added. Check the prerequisites.

4. Set the validity period to 1 year for POCs, 2 years for production overlays in the drop-down.
5. Set Certificate Retrieve Interval to 1 minute and press Save.

---

Note
Currently there is no customer email field to notify customers about approval because the certificates are auto-approved as soon as the CSR request is done.

6. From this step onwards, the process is the same as for the Symantec/Digicert controllers in the Cisco vManage GUI.

   Navigate to the Configuration ► Certificates ► Controllers tab. Click on the More (dot) menu on the right ► Generate CSR.
   
   The operation status shows the CSR sent for signing, the certificate signed and installed automatically without needing human intervention.

7. The certificates get installed automatically and shows the expiration date and status of a successful install. The operation status shows Installed for vBonds and vBond Updated for vSmarts and Cisco vManage along with the certificate serial number.

8. Ensure that the control connections have come up to the controllers on the Cisco vManage dashboard.
9. Set Certificate Retrieve Interval to 1 minute.
10. Click on Sync Root Certificate to migrate the vEdge or IOS XE devices up in Cisco vManage to Cisco pki. This support available from 19.2.1 version or above.
11. Click Save.

Use Case: Submitting CSRs and Downloading Certificates on On-Premises Controllers

The following steps require access to PnP and to the SA/VA in question. Customers have access to their own SA/VA.

Prerequisites
The prerequisites are the same in the above cases, except that you use the manual method for installing the certificates.
Runbook


2. Generate the CSRs for the controllers.
   
   Navigate to the Configuration ► Certificates ► Controllers tab. Click on the More (dot) menu on the right and then select Generate CSR.
   
   Download each CSR to a file with a filename .csr and keep it ready to submit to the PnP portal for getting the signed certificates.

3. Log on to the PnP portal to the required SA/VA and select the Certificates tab.

4. Click on Generate Certificate and follow the steps to give a name for the certificate file, paste the CSR, and download the signed certificate.
   
   The finished certificate is ready for download. Repeat this process for each CSR and download all the required certificates.

5. You can install the downloaded certificates in the Cisco vManage GUI by navigating to Configuration ► Certificates ► Controllers ► Install Certificate button (top right).
   
   Once installed, verify that the control connections are up.

Debugging and Log Information

1. Check the vBond profile under the VA in PnP to verify that the correct organization name exists.

2. Check the output at /var/log/nms/vmanage-server.log on Cisco vManage for logs of the entire certificate process.

3. Cisco vManage should have internet connectivity to reach the Cisco PKI servers.

Web Server Certificate for Cisco vManage

To establish a secure connection between your web browser and the Cisco vManage server using authentication certificates, you must generate a CSR to create a certificate, have it signed by a root CA, and then install it. To do so:

1. From the Cisco vManage menu, choose Administration > Settings.

2. In the Web Server Certificate area, click CSR.

3. In the Common Name field, enter the domain name or IP address of the Cisco vManage server. For example, the fully-qualified domain name of Cisco vManage could be vmanage.org.local.

4. In the Organizational Unit field, enter the unit name within your organization, for example, Network Engineering.

5. In the Organization field, enter the exact name of your organization as specified by your root CA, for example, Viptela Inc.

6. In the City field, enter the name of the city where your organization is located, for example, San Jose.

7. In the State field, enter the state in which your city is located, for example, California.
8. In the **2-Letter Country Code** field, enter the two-letter code for the country in which your state is located. For example, the two-letter country code for the United States of America is US.

9. From the **Validity** drop-down, select the validity period for the certificate.

10. Optionally, in the **Subject Alternative Name (SAN) DNS Names** field, enter the names of DNS servers to which the certificate trust should be extended. If you enter more than one DNS server name, separate each name with a space or a comma.

---

**Note**  
Cisco SD-WAN supports SAN DNS names beginning with Cisco IOS XE SD-WAN release 16.11 and Cisco SD-WAN release 19.1.

---

11. Optionally, in the **Subject Alternative Name (SAN) URIs** field, enter the URIs of resources to which the certificate trust should be extended. If you enter more than one URI, separate each URI with a space or a comma.

   Enter each URI in **scheme:value** format, where **scheme** is the protocol for accessing the resource and **value** is the resource. For example, `https://sample.cisco.com` or `scp://sample.cisco.com`.

---

**Note**  
Cisco SD-WAN supports SAN URIs beginning with Cisco IOS XE SD-WAN release 16.11 and Cisco SD-WAN release 19.1.

---

12. Click **Generate** to generate the CSR.

13. Send the CSR to your CA server to have it signed.

14. When you receive the signed certificate, click the **Certificate** button to the right of the Web Server Certificate bar to install the new certificate. The View box displays the current certificate on the Cisco vManage server.

15. Copy and paste the new certificate in the box. Or click the **Import** button, click **Select a File** to download the new certificate file, and click Import.

16. Restart the application server and log in to Cisco vManage.

---

**View Web Server Certificate Expiration Date**

When you establish a secure connection between your web browser and the Cisco vManage server using authentication certificates, you configure the time period for which the certification is valid (in Step 8 in the previous section). At the end of this time period, the certificate expires. The Web Server Certificate bar shows the expiration date and time.

Starting 60 days before the certificate expires, the Cisco vManage Dashboard displays a notification indicating that the certificate is about to expire. This notification is then redisplayed 30, 15, and 7 days before the expiration date, and then daily.
Licensing on Cisco SD-WAN

Cisco DNA Software subscriptions for SD-WAN gives the flexibility to consume the latest technology, either on the Cloud or On-Premises across the entire routing stack. Cisco DNA Software subscriptions provide customers with four key benefits:

- Investment protection of software purchases through software-services-enabled license portability
- Software suites that address typical customer use-case scenarios at an attractive price
- Flexible licensing models to smoothly distribute your software spending over time
- Access to new technology from Cisco

Cisco DNA licenses offer both portability and flexibility to move from cloud management (Cisco vManage) to on-premises management (Cisco DNA Center) and across hardware platforms.

For information about Cisco DNA Software subscriptions, including a comparison of subscription types, see Cisco DNA Software for SD-WAN and Routing.

- Restrictions for Cisco SD-WAN Licensing, on page 282
- Configure Cisco SD-WAN Licensing, on page 282
- Verifying Call Home Configuration, on page 284
Restrictions for Cisco SD-WAN Licensing

- Smart Licensing, a standardized licensing platform that simplifies the Cisco software experience, is supported across ISR Series, ASR series, CSR1000V, and ISRv routers. However, Cisco SD-WAN does not support Smart Licensing. Although you can use the Cisco SD-WAN functionalities through the CSR1000V 17.2.1r image - controller mode, Cisco SD-WAN does not support Smart Licensing.

- Beginning with Cisco IOS XE Release 17.5.1a and Cisco vManage Release 20.5.1, Cisco SD-WAN supports Smart License Using Policy. See Manage Licenses for Smart Licensing Using Policy.

- You cannot view license consumption information on Cisco IOS XE SD-WAN devices and Cisco vEdge devices.

Configure Cisco SD-WAN Licensing

For devices operating with Cisco SD-WAN, note the following:

- Cisco CSR1000V, Cisco Catalyst 8000V, and Cisco Integrated Services Virtual Router (ISRv) devices operating with a throughput of up to 250 Mbps do not require any manual configuration for licensing.

- Cisco CSR1000V, Cisco Catalyst 8000V, and Cisco Integrated Services Virtual Router (ISRv) devices operating with a throughput of more than 250 Mbps require Cisco Smart Licensing, as described in this section.

To configure Smart Licensing, perform the following steps:

1. Configure Smart Call Home.
2. Generate the token or authorization ID on Cisco Smart Software Manager (Cisco SSM) satellite.
3. Register the ISR, CSR1000v, or ISRv device to Cisco SSM.

You can purchase Cisco SD-WAN licenses by placing a sales order. For more information, contact your Cisco sales team.

Configure SD-WAN Licensing for Integrated Services Router Series

For Cisco Integrated Services Routers, if you want more than 250 Mbps of IPSec throughput, you must have a HSECK9 license. This requirement is due to the US export control regulations. If you ordered the HSECK9 license when you ordered the router, the HSECK9 license is installed by default. If the HSECK9 license was not installed by default, you must get a HSECK9 PAK license file and install the license file on each router.

Configure SD-WAN Licensing for Cisco CSR1000V, Cisco Catalyst 8000V, and Cisco Integrated Services Virtual Router

For virtual routers such as the Cisco CSR1000V, Cisco Catalyst 8000V, and Cisco Integrated Services Virtual Router (ISRv), if you want more than 250 Mbps throughput, perform one of the following configurations to configure the call-home profile and then perform the other steps to configure a Smart License.

Default Configuration
For platforms other than the Cisco Catalyst 8000V, the following call-home configuration is a part of the default configuration. This minimal configuration is applicable for direct cloud access either using the Smart Call Home Transport Gateway or using the HTTPS proxy, where the device reaches out to the cloud-hosted Cisco SSM service. You can verify whether this configuration is applied by executing the `show running-config` command.

```plaintext
call-home
    contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
    active
    destination transport-method http
    destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
```

For Cisco Catalyst 8000V platforms, the following call-home configuration is part of the default configuration:

```plaintext
smart license url default
license smart transport smart
```

### Configure a Device With Multiple Interfaces

To configure two or more interfaces that can reach the Cisco SSM portal, execute the `ip http client source interface` CLI so that the device uses that specific interface to reach out to the Cisco SSM portal.

```plaintext
ip http client source-interface <interface-name>
```

```plaintext
call-home
    contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
    active
    destination transport-method http
    destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
```

### Configure Call Home for DNS Resolution

To configure a call home profile for DNS resolution, execute the `http resolve-hostname ipv4-first` command so that the device uses an IPv4 interface for DNS resolution and to reach out to the Cisco SSM. If there are multiple IPv4 interfaces, one after another is tried for successful DNS resolution, and that specific interface is used to reach out to the Cisco SSM.

```plaintext
http resolve-hostname ipv4-first
```

```plaintext
profile "CiscoTAC-1"
    active
    destination transport-method http
    destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
```

---

**Note**

For detailed information about call-home profile for Cisco CSR1000V and Cisco ISRv devices, see [Configuring Call Home Profile for Cisco CSR1000V](#).

**Note**

For information about restoring Smart Licensing when a device switches from autonomous to controller mode and back to autonomous mode again, see [Restore Smart Licensing and Smart License Reservation](#).

### Allow-Service

If you configure call-home to use a service-side interface, and not VPN0, for connectivity to the Cisco Smart Licensing portal, you do not need to configure `allow-service`. 
We recommend using a service-side interface.

If you use VPN0 for connectivity to the Cisco Smart Licensing portal, configure `allow-service` as follows:

```
allow-service http
```

## Verifying Call Home Configuration

To verify the call-home configuration, use the `show call-home detail` command:

```plaintext
router#show call-home detail
Profile Name: CiscoTAC-1
  Profile status: ACTIVE
  Profile mode: Full Reporting
  Reporting Data: Smart Call Home, Smart Licensing
  Preferred Message Format: xml
  Message Size Limit: 3145728 Bytes
  Transport Method: http
  HTTP address: https://tools.cisco.com/its/service/oddce/services/DDCEService
  Other address(es): default

  Periodic configuration info message is scheduled every 17 day of the month at 14:07
  Periodic inventory info message is scheduled every 17 day of the month at 13:52

  Alert-group            Severity
  ----------------------- ------------
  crash                   debugging
  inventory               normal

  Syslog-Pattern          Severity
  ----------------------- ------------
  .*                       major
```

### Verify Throughput and License Status Before Registration

```plaintext
router#show platform hardware throughput level
The current throughput level is 250000 kb/s

router#show license status
Smart Licensing is ENABLED
Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: NOT ALLOWED

License Authorization:
```
Status: No Licenses in Use

Export Authorization Key:
Features Authorized:
<none>

Note the throughput level of 250000 kb/s when the license is in the Unregistered state.

Verify Throughput Level and License Status After Registration

router#show platform hardware throughput level
The current throughput level is 200000000 kb/s

router#show license status
Smart Licensing is ENABLED

Utility:
Status: DISABLED

Data Privacy:
Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
Type: Callhome

Registration:
Status: REGISTERED
Smart Account: InternalTestDemoAccount8.cisco.com
Virtual Account: RTP-CSR-DT-Prod
Export-Controlled Functionality: ALLOWED
Initial Registration: SUCCEEDED on May 19 04:49:46 2020 UTC
Last Renewal Attempt: None
Next Renewal Attempt: Nov 15 04:49:45 2020 UTC
Registration Expires: May 19 04:44:44 2021 UTC

License Authorization:
Status: AUTHORIZED on May 19 04:49:49 2020 UTC
Last Communication Attempt: SUCCEEDED on May 19 04:49:49 2020 UTC
Next Communication Attempt: Jun 18 04:49:49 2020 UTC
Communication Deadline: Aug 17 04:44:48 2020 UTC

Export Authorization Key:
Features Authorized:
<none>

Note that the Throughput level is 200000000 kb/s after the license enters the Registered state.

Configuration Output When License Registration Fails

router#show license status
Smart Licensing is ENABLED

Utility:
Status: DISABLED

Data Privacy:
Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED
Transport:
  Type: Callhome

Registration:
  Status: REGISTERING - REGISTRATION IN PROGRESS
  Export-Controlled Functionality: NOT ALLOWED
  Initial Registration: FAILED on May 19 04:40:14 2020 UTC
    Failure reason: Fail to send out Call Home HTTP message.
  Next Registration Attempt: May 19 04:46:34 2020 UTC

License Authorization:
  Status: No Licenses in Use

Export Authorization Key:
  Features Authorized:
    <none>

Miscellaneous:
  Custom Id: <empty>

---

**Note**

If the configuration fails, to begin with, check the reachability of the Cisco SSM portal from the device, whether you are out of licenses, and whether your token and account is valid.

---

**Verify Call Home Configuration for On-Prem**

```plaintext
router#show running config all
call-home
  contact-email-addr sch-smart-licensing@cisco.com
  profile "CiscoTAC-1"
    active
    destination transport-method http
    destination address http https://<on-prem-cssm-server>/path/to/http/service
```

For an On-Prem or a Satellite CSSM where a manual or periodic sync updates the license information to the cloud, the destination address http CLI must point to the corresponding Satellite CSSM service.
CHAPTER 11

Manage Licenses for Smart Licensing Using Policy

Table 28: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Management for Smart Licensing Using Policy, Using Cisco vManage</td>
<td>Cisco IOS XE Release 17.5.1a</td>
<td>Cisco SD-WAN operates together with Cisco Smart Software Manager (Cisco SSM) to provide license management through Cisco vManage. Cisco vManage shows available DNA licenses, assigns licenses to devices, and reports license consumption to Cisco SSM.</td>
</tr>
<tr>
<td></td>
<td>Cisco vManage Release 20.5.1</td>
<td></td>
</tr>
</tbody>
</table>

- Overview, on page 287
- Notes and Limitations, on page 289
- License Management Workflow in Cisco vManage, on page 289
- Provision Smart Account Credentials on Cisco vManage, on page 290
- Fetch and Synchronize Licenses, on page 291
- Assign License to Device, on page 292
- Monitor License Usage, on page 294

Overview

Cisco Smart Software Manager (SSM) manages Smart Licensing Using Policy (SLP) purchases, tracking availability and consumption of licenses. A Smart Account (SA) contains the licenses purchased by an organization. Virtual Accounts (VA) are subaccounts within the Smart Account that further organize the licenses, such as by department, product, geography, and so on. For more information, see Smart Software Manager.

Cisco SD-WAN operates together with Cisco SSM to provide license management through Cisco vManage for devices operating with Cisco SD-WAN. Cisco vManage can show available DNA licenses, assign licenses to devices, monitor license usage, and report license consumption to CSSM. When you set up Cisco vManage to manage licenses, Cisco vManage operates between Cisco SSM and the devices in the network, as shown in the following illustration.
Supported Licenses
Cisco vManage supports a subset of the license entitlements by default. The license entitlement types include the following:

- **Pre-paid**
  - A la carte: These entitlements are delivered based on orders in Cisco Commerce Workspace (CCW).
  - Enterprise agreement (EA): These entitlements are delivered by reporting on the EA workspace.

- **Post-paid**
  - MSLA-U: These entitlements are delivered based on orders in CCW.
  - MSLA-C: These entitlements are delivered based on orders in CCW.

For information about Smart Licensing Using Policy, see Smart Licensing Using Policy for Cisco Enterprise Routing Platforms.

Supported Entitlements
A license may include more than one entitlement. Each entitlement included with a license provides a specific functionality, such as routing features or a specific traffic throughput. The applicability of these entitlements on a particular device depends on the Cisco IOS XE software release operating on the device, and on the operation mode of the device, which can be autonomous or controller mode.

Your organization's Smart Account shows the entitlements included in each associated license.

Cisco vManage manages the following types of entitlements.

- DNA entitlements (for example, DNA Routing Advantage Tier 1)
- High Security (HSEC)

Other entitlements may appear in the Smart Account, but are not managed by Cisco vManage. Examples may include network stack entitlements, IP Base, App, Sec, Perf, Boost, DNA Essentials for SDWAN, and DNA Advantage for SDWAN.

---

**Note**
DNA Essentials for SDWAN (SDWAN-DNA-E) and DNA Advantage for SDWAN (SDWAN-DNA-A) are considered obsolete entitlement types and are not managed by Cisco vManage.
Supported Devices
License management using Cisco vManage supports Cisco IOS XE SD-WAN devices and Cisco vEdge devices.

Role-Based Access Control
When configuring role-based access control, you can configure permissions for license management.

• Read permission: The user can only view the license management overview.
• Write permission: The user can manage licenses fully.

For information about configuring role-based access control, see Role-Based Access Control.

Notes and Limitations

• We recommend assigning a license to every device in the network.

  Note
  If a device appears in the device list but is not currently intended for use, it is not necessary to assign a license.

• License management in Cisco vManage is limited to licenses in a single Cisco Smart Account.

• Ensure that the licenses in Cisco SSM that you are managing with Cisco vManage are organized into virtual accounts (VA).

• When assigning licenses to devices, have Cisco SSM available to view license details that do not appear in Cisco vManage.

• License management by Cisco vManage does not support isolated networks, on-premises Smart Software Manager (SSM), or proxy deployment.

• Automated reporting and billing is not supported for MSLA-C licenses.

• Some devices (including Cisco ISR 1000 Series, Cisco ISR 4000 Series, Cisco Catalyst 8000 Series, and Cisco Catalyst 8000V) require an additional type of license called a High Security (HSEC) license to enable throughput above 250 Mbps. The HSEC license is in addition to the typical type of device license, such as DNA Advantage. When applying a device license for a throughput above 250 Mbps to one of these devices, ensure that the device has an HSEC license installed. Otherwise the throughput is limited to 250 Mbps even for a device license with a higher entitlement.

• Assigning a DNA Premier entitlement to a device does not automatically enable Cisco Umbrella Secure Internet Gateway (SIG).

License Management Workflow in Cisco vManage

The following steps show the workflow for managing licenses using Cisco vManage.

1. Connect Cisco vManage to the Cisco SSM server.
This preparatory step is only required when setting up license management. It requires adding several commands to the vpn 0 section of the running configuration of the Cisco vManage server. These commands provide the DNS entries and next hop IP routes that enable Cisco vManage to connect to the Cisco SSM server.

Contact the Cisco support for the required configuration information.

2. Prepare the licenses.

Purchase licenses and ensure that they are in the correct Smart Account for your organization. In Cisco SSM, make note of how the licenses are organized in the Virtual Accounts within the Smart Account. This information is required in a later step of the workflow.

3. In Cisco vManage, provide Smart Account credentials.

After you provide credentials, Cisco vManage connects to the Smart Account and receives the information about available licenses in the account. After you begin using Cisco vManage for license management, Cisco vManage reports license assignments back to Cisco SSM to keep license details synchronized between Cisco vManage and Cisco SSM.

See Provision Smart Account Credentials on Cisco vManage, on page 290.

4. In Cisco vManage, select the Virtual Accounts to use, within the Smart Account.

Cisco vManage downloads the details of available licenses in the selected Virtual Accounts. There are options to manage only prepaid licenses, only postpaid licenses, or both, in the selected Virtual Accounts.

---

**Note** Configuring Cisco vManage to manage compatible licenses requires confirmation before proceeding.

See Fetch and Synchronize Licenses, on page 291.

5. In Cisco vManage, assign licenses to devices.

Assign licenses using existing license templates or create a new license template.

See Assign License to Device, on page 292.

6. In Cisco vManage, monitor license usage.

See Monitor License Usage, on page 294.

---

**Provision Smart Account Credentials on Cisco vManage**

**Prerequisite:**

- Ensure that you have configured DNS host and next-hop IP route entries for the Cisco SSM servers under VPN 0 on Cisco vManage. Without this configuration, Cisco vManage cannot communicate with Cisco SSM.

1. In Cisco vManage, go to **Administration > License Management**.

2. Click **Smart Account Credentials**.

3. In the **Smart Account Credentials** dialog box, configure the following:
Username| Username of the account you use to access the Smart Accounts and Virtual Accounts for which you have administrative privileges.
---|---
Password| Password for the account you use to access Smart Accounts and Virtual Accounts.

4. Click **Save**.

Cisco vManage authenticates the Smart Account credentials, and on successful authentication, saves the credentials in the database.

## Fetch and Synchronize Licenses

**Prerequisite:**
- Ensure licenses belong to the correct Smart Accounts or Virtual Accounts on Cisco SSM.

1. In Cisco vManage, go to **Administration > License Management**.
2. Click **Sync Licenses & Refresh Devices**.
3. In the **Sync Licenses & Refresh Devices** dialog box, configure the following:

| Select Smart/Virtual Accounts to Fetch/Sync Licenses | Select the Smart Accounts or Virtual Accounts for which Cisco vManage must fetch licenses from the Cisco SSM. Cisco vManage also reports license usage for the licenses in these accounts.  

**Note**  
Selecting an Smart Account automatically selects all the Virtual Accounts under the Smart Account.  
To stop Cisco vManage from fetching and synchronizing license information with Cisco SSM for an Smart Account or Virtual Account registered earlier, deselect the Smart Account or Virtual Account. You can deregister the Smart Account or Virtual Account only if you have not assigned any licenses from the account. |
|---|---|
| Advanced > Type of Licenses | Choose the type of licenses that must be fetched by Cisco vManage from among the license types that may belong to the selected Smart Accounts and Virtual Accounts.  
Select one of the following:  
- **Prepaid**  
- **Postpaid (MSLA-U)**  
- **Mixed** (both Prepaid and Postpaid) |
| Advanced > Multiple Entitlement | Select one of the following:  
- **On**: You can assign more than one license to a device.  
- **Off**: You can assign only one license to a device.  

**Note** Set this setting to **On** only if you need to map more than one DNA entitlement to a single device.
4. Click Sync.

The selected Smart Accounts and Virtual Accounts are registered with Cisco vManage. Cisco vManage fetches and synchronizes the license information with Cisco SSM, and reports usage of the licenses in these accounts.

Assign License to Device

1. In Cisco vManage, go to Administration > License Management.
2. Click the Device tab.
3. Select the devices to which you wish to assign a license using the check box for each device.
4. Click Assign License/Subscription.
   The Assign License/Subscription dialog box appears.
5. In the Assign License/Subscription dialog box, configure the following:

<table>
<thead>
<tr>
<th>Are you using utility-based licensing (MSLA)?</th>
<th>Check this check box if you wish to apply an MSLA license. By default, the check box is unchecked.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template Name</td>
<td>To use a new template, enter a unique name for the template.</td>
</tr>
<tr>
<td></td>
<td>To use an existing template,</td>
</tr>
<tr>
<td></td>
<td>a. turn on the Use existing template toggle.</td>
</tr>
<tr>
<td></td>
<td>b. choose an existing template.</td>
</tr>
<tr>
<td>Virtual Account</td>
<td>Choose Virtual Account from which you wish to assign a license to the device.</td>
</tr>
</tbody>
</table>
Choose license to apply to the device. If you have enabled Multiple Entitlements in the Sync Licenses & Refresh Devices dialog box, you can assign up to three licenses to the device.

**Note**
- Select a license that belongs to the Virtual Account you have selected. On Cisco SSM, you can check the licenses that are available in a Virtual Account.
- Check the device license applicability matrix in the Cisco DNA Software for SD-WAN and Routing Ordering Guide to ensure that you assign a license that is applicable to the device. Different device models support different throughputs.

If you apply an incompatible license, the license may have no effect on device behavior. However, Cisco vManage will record the consumption of the license.

- When assigning licenses, Cisco vManage shows the throughput entitlement levels as tiers. Select the tier that matches the license you have purchased. If you purchased a license with a throughput expressed as a throughput value, find the tier that corresponds to the throughput that the license provides.

For example, for a Routing DNA Advantage license, Tier 2 provides up to 1 Gbps throughput. If your DNA Advantage license provides 1 Gbps, choose Tier 2.

| Tier 0: 10M-15M (up to 30M aggregate) |
| Tier 1: 25M-100M (up to 200M aggregate) |
| Tier 2: 250M-1G (up to 2G aggregate) |
| Tier 3: 2.5G-10G (up to 20G aggregate) |

- When assigning licenses, Cisco vManage shows the throughput entitlement levels as tiers. Select the tier that matches the license you have purchased. If you purchased a license with a throughput expressed as a throughput value, find the tier that corresponds to the throughput that the license provides.

For example, for a Routing DNA Advantage license, Tier 2 provides up to 1 Gbps throughput. If your DNA Advantage license provides 1 Gbps, choose Tier 2.

| Tier 0: 10M-15M (up to 30M aggregate) |
| Tier 1: 25M-100M (up to 200M aggregate) |
| Tier 2: 250M-1G (up to 2G aggregate) |
| Tier 3: 2.5G-10G (up to 20G aggregate) |

Choose the subscription ID to be used to track license consumption.

6. Click **Save**.

The license is assigned and you are returned to License Management > Device tab. In the table listing the devices, entries are made in the following columns in accordance with the license assignment:

- Template Name: name of the template used to assign the license
- Virtual Account: name of Virtual Account to which license belongs
- MSLA:
  - True for an MSLA license
  - False for an a la carte or EA license
- License Status: subscribed
- License Type: prepaid, postpaid, or mixed based on the types of licenses assigned to the device.
- Subscription ID: The subscription ID used for billing purposes in case of a postpaid license. For a prepaid license, this column has a blank entry.
Monitor License Usage

License Management Overview

From the Cisco vManage menu, select Administration > License Management to display the License Management Overview.

The License Management Overview page shows license information, including what percent of devices have licenses assigned, the top types of licenses assigned to devices, license usage, and so on.

License Management Overview

After you have assigned at least one license, the Overview tab in the Administration > License Management page provides the following information:

| Device Assignment Distribution | • Percentage of licensed devices  
|                               | • Percentage of unlicensed devices |
| Top 5 licenses                | Lists the top 5 licenses in use and shows the usage percentage for each license. |
| License Usage vs Availability | The dashlet features a bar chart with stacked columns. |
|                               | The chart uses two stacked columns for each of the three license packages Advantage, Essentials, and Premier. |
|                               | For each package, the column on the left represents the count of used licenses; the column on the right represents the count of available licenses. |
|                               | The stacked segments in each column represent a particular license tier (such as Tier 0 or Tier 1). The segment for each tier is of a different color, as identified in the legend. |
| License and Devices Overview  | This section provides the following details for each license assigned: |
|                               | • Name (for example, Routing DNA Essentials: Tier 0) |
|                               | • Number of Licensed Devices: Number of devices to which this license is assigned. |
|                               | • Number of Total Licenses: Sum of the number of licenses assigned and number of licenses available. |
|                               | • Last Assigned On: Date and time when the license was most recently assigned. |
CHAPTER 12

Onboarding Modular Cisco ASR 1000 Series Platforms

• Cisco ASR 1006-X with an RP3 Module, on page 295

Cisco ASR 1006-X with an RP3 Module

Table 29: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco SD-WAN Support for the Cisco ASR 1006-X Platform with an RP3 Module</td>
<td>Cisco IOS XE Release 17.5.1a</td>
<td>Starting from this release, Cisco SD-WAN supports the Cisco ASR 1006-X platform with a Cisco ASR 1000 Series Route Processor 3 module installed.</td>
</tr>
<tr>
<td></td>
<td>Cisco vManage Release 20.5.1</td>
<td></td>
</tr>
</tbody>
</table>

Cisco SD-WAN supports the Cisco ASR 1006-X platform with a Cisco ASR 1000 Series Route Processor 3 (Cisco ASR1000-RP3) module.

Note

Cisco SD-WAN supports this configuration only when the Cisco ASR 1006-X and RP3 module are ordered as a unit for operation with Cisco SD-WAN.

Hardware Configuration

The Cisco ASR 1006-X operates with Cisco SD-WAN in the following configuration.

Table 30: Hardware Configuration

<table>
<thead>
<tr>
<th>ASR 1006-X Slot</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>R0</td>
<td>Cisco ASR 1000 Series Route Processor 3 (Cisco ASR1000-RP3) module</td>
</tr>
<tr>
<td>F0</td>
<td>Cisco ASR 1000 Series 200-Gbps Embedded Services Processor (ASR1000-ESP200-X)</td>
</tr>
</tbody>
</table>
### ASR 1006-X Slot

<table>
<thead>
<tr>
<th>Slot</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC0</td>
<td>Cisco ASR1000-MIP100 carrier card + 1 or 2 EPA cards in the subslots of the carrier&lt;br&gt;<strong>Note</strong> See below for supported EPA cards. When using only one EPA card in the carrier, you can place the EPA card in either subslot.</td>
</tr>
<tr>
<td>CC1</td>
<td>Cisco ASR1000-MIP100 carrier card + 1 or 2 EPA cards in the subslots of the carrier&lt;br&gt;<strong>Note</strong> See below for supported EPA cards. When using only one EPA card in the carrier, you can place the EPA card in either subslot.</td>
</tr>
<tr>
<td>R1</td>
<td>This slot must be empty.</td>
</tr>
<tr>
<td>F1</td>
<td>This slot must be empty.</td>
</tr>
</tbody>
</table>

*Figure 2: Cisco ASR 1006-X Slots and Modules*

For information about installing the ASR1000-MIP100 carrier card and EPA cards, see the [Cisco ASR 1000 Series Modular Interface Processor Hardware Installation Guide](#).

#### Supported Cards and Modules

The following Ethernet port adapter (EPA) cards are supported. Each ASR1000-MIP100 carrier card supports two EPA cards, and you can install a total of up to four EPA cards.

- **10-port 10 Gigabit Ethernet (10x10G):**
  - EPA-10X10GE

- **2-port 40 Gigabit Ethernet (2x40G):**
  - EPA-2X40GE

- **1-port 100 Gigabit Ethernet (1x100G):**
EPA-QSFP-1X100GE

Notes and Limitations

• Hardware redundancy
  Use only one ASR1000-RP3 and one ASR1000-ESP200-X, as described in the Hardware Configuration table above. Dual RP module or dual ESP hardware redundancy is not supported for the Cisco ASR 1006-X in this Cisco SD-WAN use-case.

• ISSU and OIR
  The modules and cards do not support in-service software upgrade (ISSU) or online insertion and removal (OIR).

ROM Monitor Software Version

• For the Cisco ASR 1006-X platform, there are no specific ROM monitor (ROMmon) version requirements.
• The RP3 module requires ROM monitor (ROMmon) software version 16.9(5r) or later.

Onboarding Workflow

1. Verify that the Cisco ASR 1006-X meets the requirements described in Hardware Configuration, on page 295 and ROM Monitor Software Version, on page 297.
2. Follow the Plug and Play onboard procedures described in the Cisco Plug and Play Support Guide for Cisco SD-WAN Products.
3. Follow the Cisco SD-WAN onboarding procedure described in Plug and Play Onboarding Workflow.

RMA Replacement of the Cisco ASR 1006-X Chassis

Use this procedure if it is necessary to replace the Cisco ASR 1006-X chassis as part of a return material authorization (RMA) process. This procedure replaces the Cisco ASR 1006-X chassis, but keeps the current cards (RP3 module, ESP200 module, MIP100 carrier cards, EPA cards).

Prerequisites

• The Cisco ASR 1006-X (which is now faulty) with an RP3 module has been fully onboarded in Cisco vManage.
• Make note of the following serial numbers:
  • Replacement Cisco ASR 1006-X chassis serial number
  • Certificate serial number for the RP3 module
  • SUDI serial number for the RP3 module

To replace the Cisco ASR 1006-X chassis, perform the following steps.
In tables listing devices, Cisco vManage does not distinguish between the Cisco ASR 1006-X chassis and the RP3 module installed in the chassis. A single row in the table shows the combined information for both.

1. (Perform this step only if you have applied a feature template to the current device (which is now faulty), and if you want to save the existing configuration to use it on the replacement device.)

   Save the device settings file for the RP3 module.
   a. In Cisco vManage, choose Configuration > Templates > Device.
   b. Click More Options (…) for the template that is attached to the Cisco ASR 1006-X containing the RP3 module, and choose Export CSV to download the device settings CSV file.

2. In the Cisco Plug and Play (PnP) Connect web portal, remove the current Cisco ASR 1006-X chassis.

   The PnP Connect web portal is linked to Cisco commerce workspace (CCW), facilitating automatic registration of the serial numbers and PIDs of purchased devices in the PnP Connect web portal. For more information see the Cisco Plug and Play Support Guide for Cisco SD-WAN Products, and the RMA topic in the Cisco Network Plug and Play Connect Capability Overview.

   The functionality of the PnP Connect web portal is subject to change, and is outside the scope of this document. For additional details, see the PnP Connect web portal documentation.

   In the PnP Connect web portal, use Devices > Delete Selected Device to remove the current Cisco ASR 1006-X chassis.

3. In the Cisco Plug and Play (PnP) Connect web portal, add the replacement Cisco ASR 1006-X chassis.
   a. In the PnP Connect web portal, choose Devices > Add Device and select the option to enter new device details.
   b. Enter the serial number for the replacement Cisco ASR 1006-X chassis.
   c. Add the SUDI serial number and certificate serial number of the RP3 module.
   d. Save the update.

4. Remove the entry for the current Cisco ASR 1006-X chassis in Cisco vManage.
a. In Cisco vManage, detach the current device template from the current Cisco ASR 1006-X chassis.

b. In Cisco vManage, choose Configuration > Certificates.

c. In the row with the current Cisco ASR 1006-X, in the Validate column, click Invalid, and OK. The task view indicates when the process is complete.

d. Click Send to Controllers.

e. In Cisco vManage, choose Configuration > Devices.

f. In the row with the current Cisco ASR 1006-X, click More Options (…) and choose Delete WAN Edge.

5. In Cisco vManage, choose Configuration > Devices and click Sync Smart Account.

Cisco vManage loads the details of the replacement Cisco ASR 1006-X chassis from your Smart Account.

6. If you saved a CSV file in an earlier step, edit the file to update it with the device ID of the replacement chassis.
   a. In Cisco vManage, choose Configuration > Devices > WAN Edge List.
   b. Copy device ID of the new chassis from the Chassis Number column in the device list.
   c. Open the CSV file in a text editor or spreadsheet application, and edit the csv-deviceId value in the first column, updating it to use the device ID of the new chassis.

7. Attach a device template to the replacement Cisco ASR 1006-X. Use the same device template that was used for previous chassis. If you saved a CSV file in an earlier step, use it in the substeps that follow.
   a. In Cisco vManage, choose Configuration > Templates and click the Device tab.
   b. In the row of the template that was previously attached to the current chassis, click More Actions (…) and choose Attach Devices.
   c. In the Available Devices pane, select the replacement chassis and move it to the Selected Devices pane.
   d. Click Attach. The Configuration Templates page opens.
   e. If you saved a CSV file in an earlier step, click the up arrow button to upload a CSV file.
   f. If you saved a CSV file in an earlier step, in the Upload CSV File pop-up window, select the CSV file edited in a previous step, and click Upload. The values stored in the CSV file are copied to the device template.
   g. Click Next.
   h. Click Configure Devices to push the device template to the replacement Cisco ASR 1006-X chassis. The task status shows this task as Scheduled because the replacement device is not yet reachable.

8. Save the device configuration file.
   a. In Cisco vManage, choose Configuration > Devices > WAN Edge List.
   b. In the row of the Cisco ASR 1006-X, click More Options (…) and choose Generate Bootstrap Configuration.
c. In the pop-up window, click the Cloud-Init radio button.
d. Click Download to download the configuration file.
e. Rename the downloaded file to: ciscosdwan.cfg

9. Copy the bootstrap file (ciscosdwan.cfg) created in an earlier step, to a USB flash drive, and plug this into the current RP3 module.

10. If the current Cisco ASR 1006-X chassis is still operating, power it down.

11. Remove the modules and cards (RP3 module, ESP200 module, MIP100 carrier cards, EPA cards) from the current Cisco ASR 1006-X chassis.

12. Connect the USB flash drive, which has the configuration file saved in an earlier step, to the RP3 module.

13. Install the modules and cards in the new Cisco ASR 1006-X chassis.
   For information about RP3 module installation, see the Cisco ASR 1000 Route Processor 3 Installation and Configuration Guide.
   For information about MIP100 and EPA installation, see the Cisco ASR 1000 MIP and EPA Hardware Installation Guide.

14. Power up the replacement Cisco ASR 1006-X router.

15. After the router is powered up, execute the controller-mode reset command on the router to reset the RP3 module.
   When the RP3 module starts, the following occurs:
   • The RP3 module loads the configuration from the ciscosdwan.cfg file on the USB flash drive.
   • The RP3 module boots up in controller mode.
   • When the connection to the controller is established, the controller pushes the device template, which was in Scheduled state, to the RP3 module.

**RMA Replacement of the Cisco RP3 Module**

Use this procedure if it is necessary to replace the RP3 module used with the Cisco ASR 1006-X as part of a return material authorization (RMA) process.

**Prerequisites**

- The Cisco ASR 1006-X with an RP3 module (which is now faulty) has been onboarded in Cisco vManage.
- Make note of the following serial numbers:
  • Cisco ASR 1006-X chassis serial number
  • Certificate serial number for the replacement RP3 module
  • SUDI serial number for the replacement RP3 module

To replace the Cisco RP3 module, perform the following steps.
In tables listing devices, Cisco vManage does not distinguish between the Cisco ASR 1006-X chassis and the RP3 module installed in the chassis. A single row in the table shows the combined information for both.

1. (Perform this step only if you have applied a feature template to the current device (which is now faulty), and if you want to save the existing configuration to use it on the replacement device.)

   Save the device settings file for the RP3 module.
   a. In Cisco vManage, choose Configuration > Templates > Device.
   b. Click More Options (…) for the template that is attached to the Cisco ASR 1006-X containing the RP3 module, and choose Export CSV to download the device settings CSV file.

2. Save the device configuration file for the RP3 module.
   a. In Cisco vManage, choose Configuration > Devices > WAN Edge List.
   b. In the row for the Cisco ASR 1006-X containing the RP3 module, click More Options (…) and choose Generate Bootstrap Configuration.
   c. In the pop-up window, click the Cloud-Init radio button.
   d. Click Download to download the configuration file.
   e. Rename the downloaded file to: ciscosdwan.cfg

3. In the Cisco Plug and Play (PnP) Connect web portal, update the SUDI serial number and certificate serial number within the Cisco ASR 1006-X entry, to use the serial numbers of the replacement RP3 module.

   The PnP Connect web portal is linked to Cisco commerce workspace (CCW), facilitating automatic registration of the serial numbers and PIDs of purchased devices in the PnP Connect web portal. For more information see the Cisco Plug and Play Support Guide for Cisco SD-WAN Products, and the RMA topic in the Cisco Network Plug and Play Connect Capability Overview.

   The functionality of the PnP Connect web portal is subject to change, and is outside the scope of this document. For additional details, see the PnP Connect web portal documentation.

   a. In the PnP Connect web portal, choose Devices > Edit Device and select the Cisco ASR 1006-X entry for the device that contains the RP3 module that is being replaced.
   b. In the Cisco ASR 1006-X entry, delete the SUDI serial number and certificate serial number of any existing RP3 module entries (there may be more than one).
   c. Add the SUDI serial number and certificate serial number for the replacement RP3 module.
   d. Save the update.

4. In Cisco vManage, remove the current RP3 module and add the replacement RP3 module.
a. In Cisco vManage, choose Configuration > Certificates.

b. In the row with the Cisco ASR 1006-X device containing the RP3 module, in the Validate column, click Invalid, and OK.

   The task view indicates when the process is complete.

c. Click Send to Controllers.

d. In Cisco vManage, choose Configuration > Devices.

e. In the row with the Cisco ASR 1006-X device containing the RP3 module, click More Options (…) and choose Delete WAN Edge.

f. In Cisco vManage, choose Configuration > Devices and click Sync Smart Account.

   Cisco vManage loads the details of the replacement RP3 module. At this point, before you have physically replaced the RP3 module, the device table shows the following in the row of the Cisco ASR 1006-X device:
   
   • Device Model: ASR1006-X
   • Chassis Number: No change to the chassis number
   • Serial No./Token: Updated to show the serial number of the replacement RP3 module, as loaded from the Smart Account

5. Attach a device template to the replacement Cisco ASR 1006-X. Use the same device template that was used for previous chassis. If you saved a CSV file in an earlier step, use it in the substeps that follow.

a. In Cisco vManage, choose Configuration > Templates and click the Device tab.

b. In the row of the template that was previously attached to the current chassis, click More Actions (…) and choose Attach Devices.

c. In the Available Devices pane, select the replacement chassis and move it to the Selected Devices pane.

d. Click Attach. The Configuration Templates page opens.

e. If you saved a CSV file in an earlier step, click the up arrow button to upload a CSV file.

f. If you saved a CSV file in an earlier step, in the Upload CSV File pop-up window, select the CSV file and click Upload. The values stored in the CSV file are copied to the device template.

g. Click Next.

h. Click Configure Devices to push the device template to the replacement Cisco ASR 1006-X chassis. The task status shows this task as Scheduled because the replacement device is not yet reachable.

6. Copy the bootstrap file (ciscosdwan.cfg) created in an earlier step, to a USB flash drive, and plug this into the replacement RP3 module.

7. Remove the previous RP3 module from the Cisco ASR 1006-X chassis, and install the replacement RP3 module.

   For information about RP3 module installation, see the Cisco ASR 1000 Route Processor 3 Installation and Configuration Guide.
When the RP3 module starts, the following occurs:

- The RP3 module loads the configuration from the ciscosdwan.cfg file on the USB flash drive.
- The RP3 module boots up in controller mode.
- When the connection to the controller is established, the controller pushes the device template, which was in Scheduled state, to the RP3 module.
RMA Replacement of the Cisco RP3 Module
CHAPTER 13

API Cross-Site Request Forgery Prevention

Table 31: Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>API Cross-Site Request Forgery Prevention</td>
<td>Cisco IOS XE SD-WAN Release 16.12.1b</td>
<td>This feature adds protection against Cross-Site Request Forgery (CSRF) that occurs when using Cisco SD-WAN REST APIs. This protection is provided by including a CSRF token with API requests. You can put requests on an allowed list so that they do not require protection if needed.</td>
</tr>
<tr>
<td></td>
<td>Cisco SD-WAN Release 19.2.1</td>
<td></td>
</tr>
</tbody>
</table>

- Cisco SD-WAN REST API Token-Based Authentication, on page 305
- Token Use, on page 305
- API Docs, on page 306
- Third Party Application Users, on page 306

Cisco SD-WAN REST API Token-Based Authentication

Cisco SD-WAN release 19.2 offers token-based authentication when you use the SD-WAN REST API. This protection is provided by requiring that a token be included with API requests. Each API session uses a unique token that is valid throughout the session. If an API request does not include this token, vManage rejects the request, unless the endpoint is included on an allowed list. (For assistance with adding endpoints to an allowed list, open a case with the Cisco TAC or escalation support team.)

Token Use

The following sections describe how the token is used with the API when you use API docs or third party applications.
API Docs

Cisco vManage automatically generates a token and appends the token to every request that you send from the vManage API Docs page. This process requires no action from you, and you will not notice any difference from previous releases in how the API Docs page operates.

If there are API requests that you want to exclude from this token-based authentication, you can request that these API endpoints be included in an allowed list by opening a case with the Cisco TAC or escalation support team.

Third Party Application Users

If you use scripts or third party applications such as Postman, LiveAction, SolarWinds, or SevOne for vManage API requests, each request must include the token, unless the API is included in an allowed list. If an API request does not include a token and is not included in the allowed list, Cisco vManage rejects the request and returns the response code 403 (forbidden) with the message, “SessionTokenFilter: Token provided via HTTP Header does not match the token generated by the server.”

To request that certain API endpoints be included in an allowed list, open a case with the Cisco TAC or escalation support team.

To include the token in a third party API request:

Method 1

In the first method, the session you create is stored in the cookies.txt file and the same session can be used for all subsequent requests, using the jsessionid that the file contains. This is the recommended method.

1. To log into Cisco vManage, use the following example command and modify the URL according to your IP address:

   ```bash
   ```

   To verify the login, see the cookies.txt file.

2. After logging in to Cisco vManage, obtain a token by making a request, where vManage_IP is the IP address of your vManage server. You can obtain a token in string format or in JSON format.

   To obtain a token in string format, use the following URL:

   ```none
   https://vManage_IP/dataservice/client/token
   ```

   To obtain a token in JSON format (beginning with Cisco IOS XE SD-WAN Release 16.12 and Cisco SD-WAN Release 19.2), use the following URL:

   ```none
   https://vManage_IP/dataservice/client/token?json=true
   ```

   The token that these calls return is valid for the rest of your current session. The following example shows requests for obtaining a token:

   Command for obtaining a token in string format:

   ```bash
   sampleuser$ TOKEN=$(curl "https://vManage_IP/dataservice/client/token" -X GET -b cookies.txt -s -insecure)
   ```
Output in string format:
FC5B19BB3521EE20CFBDCD3CEDCC48F50CB1095C9654407936029E9C0EF99FEA50440B60E49F7CD4A0B8B5307C2855F2E0C

Command for obtaining a token in JSON format:

```bash
TOKEN=$(curl "https://vManage_IP/dataservice/client/token?json=true" -X GET -b cookies.txt -s -insecure)
```

Output in JSON format:

```bash
sampleuser$ echo $TOKEN
{"token":"56CF324A8F67993B6FCCF57302068B0756DA8703E712FAEA18D4D9055B11312843FB3B48A3902320FFAA8659AD01202A69"}
```

**Note**

JSON format is not supported for curl commands.

3. In the header of each subsequent API request in the current session, include the X-XSRF-TOKEN key, with a value that consists of the token that you generated.

The following examples show a GET request and a POST request that include a generated token in the header:

**Command:**

```bash
```

**Output:**

```json
{"Architecture":"amd64","Available processors":2}
```

**Command**

```bash
sampleuser$ curl "https://vManage_IP/dataservice/settings/configuration/emailNotificationSettings" -X POST -b cookies.txt -silent -insecure -H "X-XSRF-TOKEN: $TOKEN" -d '{"enabled":true,"from_address":"test@mydomain.com","protocol":"smtp","smtp_server":"a.com","smtp_port":25,"reply_to_address":"test@test.com","notification_use_smtp_authentication":false}=
```

**Output:**

```json
{"data":{"enabled":true,"notification_use_email_settng_authentication":false,"notification_use_smtp_authentication":false}}
```

4. To prevent memory leaks, you must logout after each API call, including the token, starting from Cisco SD-WAN Release 19.2.1.

The following example shows how you can logout:

**Command:**

```bash
sampleuser$ curl "https://vManage_IP/logout" -b cookies.txt -insecure -H "X-XSRF-TOKEN:$TOKEN"
```

**Output:**

```
Replaced cookie JSESSIONID="DcOke5mqix_15qCpWA1blIJVAMnVg3lDMU4ABRgVInvalid" for domain 209.165.200.254, path /, expire 0
< set-cookie: JSESSIONID=DcOke5mqix_15qCpWA1blIJVAMnVg3lDMU4ABRgVInvalid
```
To verify that you have logged out of the session, check the jsessionid and ensure that it ends with ‘invalid’.

Method 2

In the second method, the session you create is not stored and you must create a new session for each request.

1. After logging in to Cisco vManage, obtain a token by making a request, where vManage_IP is the IP address of your vManage server. You can obtain a token in string format or in JSON format.

To obtain a token in string format, use the following URL:
https://vManage_IP/dataservice/client/token

To obtain a token in JSON format (beginning with Cisco IOS XE SD-WAN Release 16.12 and Cisco SD-WAN Release 19.2), use the following URL:
https://vManage_IP/dataservice/client/token?json=true

The token that these calls return is valid for the rest of your current session. The following example shows requests for obtaining a token:

Command for obtaining a token in string format:
sampleuser$ curl --user admin:admin https://vManage_IP/dataservice/client/token --insecure

Output in string format:
FC5B19BB3521EE20CFBDCD3CEDCC48F50CB1095C9654407936029E90CEF99FEE50440B60E49F7CD4A0BABB5307C2855F2E0C

Command for obtaining a token in JSON format:
sampleuser$ curl --user admin:admin https://vManage_IP/dataservice/client/token?json=true --insecure

Output in JSON format:
FC5B19BB3521EE20CFBDCD3CEDCC48F50CB1095C9654407936029E90CEF99FEE50440B60E49F7CD4A0BABB5307C2855F2E0C

2. In the header of each subsequent API request in the current session, include the X-XSRF-TOKEN key, with a value that consists of the token that you generated.

The following examples show a GET request and a POST request that include a generated token in the header:

Command:
sampleuser$ curl "https://vManage_IP/dataservice/server/info" -H "Cookie: JSESSIONID=pSwrx3AEWokiD0IK1TkFl0jgSefP=1TNdFh7Xj9PsL.c331d01e-91d7-41cc-ab90-b629c2ae6d97" --insecure -H "X-XSRF-TOKEN=" FC5B19BB3521EE20CFBDCD3CEDCC48F50CB1095C9654407936029E90CEF99FEE50440B60E49F7CD4A0BABB5307C2855F2E0C

Output:
{"Architecture":"amd64","Available processors":2}

Command
sampleuser$ "https://vManage_IP/dataservice/settings/configuration/emailNotificationSettings" -H "Cookie: JSESSIONID=pSwrx3AEWokiD0IK1TkFl0jgSefP=1TNdFh7Xj9PsL.c331d01e-91d7-41cc-ab90-b629c2ae6d97"
--insecure -H "X-XSRF-TOKEN="
FC5B19B3521EE20CF86C3E9DCE48F50CB1095C965407936029E9C08EF99FEAE520440B60E49F7CD4A08AB5307C2855F2E0C"
-X POST --insecure -d
'{"enabled":true,"from_address":"test@mydomain.com","protocol":"smtp","smtp_server":"a.com","smtp_port":25,"reply_to_address":"test@test.com","notification_use_smtp_authentication":false}='

Output:
{
"data": [{"enabled":true,"protocol":"smtp","smtp_server":"a.com","from_address":"test@mydomain.com","smtp_port":25,"notification_use_smtp_authentication":false,"reply_to_address":"test@test.com"}]
}

3. To prevent memory leaks, you must logout after each API call, including the token, starting from Cisco SD-WAN Release 19.2.1.

The following example shows how you can logout:

Command:

```
sampleuser$ curl "https://vManage_IP/logout" -b cookies.txt --insecure -H "X-XSRF-TOKEN:$TOKEN"
```

Output:

```
Replaced cookie JSESSIONID="Dc0Ke5mQix_15qCpWA1b1JVMnVg31DMU4ABRgVinvalid" for domain 209.165.200.254, path /, expire 0
< set-cookie: JSESSIONID=Dc0Ke5mQix_15qCpWA1b1JVMnVg31DMU4ABRgVinvalid
```

To verify that you have logged out of the session, check the jsessionid and ensure that it ends with 'invalid'.

Note
Appendix: vManage How-Tos

- RESTful API for vManage NMS, on page 311
- Replace a vEdge Router, on page 313
- Using Cisco vManage on Different Servers, on page 315
- Log In to the Cisco vManage Web Application Server, on page 316

RESTful API for vManage NMS

The Cisco vManage supports RESTful (Representational State Transfer) API, which provides calls for retrieving real-time and static information about the Cisco SD-WAN overlay network and the devices in the network and for uploading device configuration templates and other configuration-related information. Using the RESTful API, you can design a custom portal for interacting with the vManage NMS.
The Cisco vManage API documentation is provided as part of the vManage software, at the URL https://vmanage-ip-address/apidocs. (More accurately, the full URL includes the Cisco vManage port number, https://vmanage-ip-address:8443/apidocs.) vmanage-ip-address is the IP address of the vManage server.

API calls are provided for the following categories of operations:

- Certificate Management
- Configuration
- Device and Device Inventory
- Monitoring
- Real-Time Monitoring
- Troubleshooting Tools

For each group of API calls, click Show/Hide to list the individual calls and the URL for each call. Each call shows its response class, required parameters, and response messages (status codes).

To display the request URL for each API call and the format of the response body, click the Try It Out button. The request URL consists of the vManage NMS's URL, followed by /dataservice. For example, https://10.0.1.32:8443/dataservice/device/interface/statistics/ge0/0?deviceId=172.16.255.11
Below are a few examples of the URLs to use for API calls:

Table 32:

<table>
<thead>
<tr>
<th>Requested Information</th>
<th>API Call</th>
</tr>
</thead>
<tbody>
<tr>
<td>List all network devices</td>
<td><code>dataservice/deviceListallnetworkdevices</code></td>
</tr>
<tr>
<td>Health status of hardware device components, such as CPU, memory, fan, and power</td>
<td><code>dataservice/device/hardware/environment?deviceId=system-ip-address</code></td>
</tr>
<tr>
<td>Status of a device's transport interfaces</td>
<td><code>dataservice/device/interface?deviceId=system-ip-address&amp;port-type=transport</code></td>
</tr>
<tr>
<td>Interface statistics, errors, and packet drops</td>
<td><code>dataservice/device/interface?deviceId=system-ip-address</code></td>
</tr>
<tr>
<td>DTLS/TLS control connection status</td>
<td><code>dataservice/device/control/connections?deviceId=system-ip-address</code></td>
</tr>
<tr>
<td>OMP peering</td>
<td><code>dataservice/device/omp/peers?deviceId=system-ip-address</code></td>
</tr>
<tr>
<td>BGP peering on the service side</td>
<td><code>dataservice/device/bgp/neighbors?deviceId=system-ip-address</code></td>
</tr>
</tbody>
</table>

Replace a vEdge Router

This article describes how to replace a vEdge router at a particular location. You might do this when a vEdge router has failed completely or when a component in a router, such as one of the power supplies, has failed, and you want to replace the entire router.

At a high level, to replace one vEdge router with another, you simply copy the configuration from the router you are removing to the new router and then put the new router into the network.

Before you can replace the vEdge router in the vManage NMS, the NMS must have learned the chassis number and serial number of the replacement vEdge router.

- If the replacement vEdge router is a router that you have previously received, such as a router that part of your spares inventory, the vManage NMS will have already learned the router's chassis and serial number when you previously uploaded the serial number file to the NMS.

- If you initiated an RMA process and have received a new router as a replacement, you need to upload the updated version of the authorized vEdge serial number file to the NMS.

You perform the procedure for replacing the failed router from the vManage NMS, by doing the following:

1. Copy the configuration from the failed router to the replacement router.
2. Invalidate the failed router. Invalidating a router deactivates its certificate and thus removes it from the overlay network.
3. Validate the replacement router, to activate its certificate.
Because the new router is a complete replacement for the failed router, its configuration is identical to that of the failed router. (Remember, though, that each router has a unique chassis number and a unique serial number in its certificate.) After you copy the configuration from the failed router to the replacement, both routers have the same configurations, including the same IP address. Because two routers with the same IP address cannot be present in the network at the same time, one router must be in valid state on the vManage NMS and the other must be in invalid state—or both routers must be in invalid state.

**Before You Begin**

Ensure that you have uploaded the vEdge serial number file to the vManage NMS.

**Copy the Configuration from the Failed to the Replacement Router**

From the vManage NMS, you copy the configuration from the failed vEdge router to the replacement router. The vEdge router that you are copying the configuration from can be a device that is active in the overlay network (that is, it is in a valid state) or it can be one that is inactive (that is, it is in invalid state). For example, if you are replacing a router in which one of the two power supplies has failed, the router might still be active in the network, but if you are replacing one that has failed completely, you might have already marked it as invalid to remove it from the network.

The vEdge router that you are copying the configuration to must be in invalid state.

To view the state of a vEdge router or to change the validity state, see Validate or Invalidate a vEdge Router.

To copy the configuration from the failed router to the replacement router:

1. In vManage NMS, select the Configuration ► Devices screen.
2. From the list of vEdge routers, locate the failed router.
3. Click the More Actions icon to the right of the row and click Copy Configuration.
4. In the Copy Configuration window, select the replacement router.
5. Click Update.

**Remove the Failed Router**

To remove the failed vEdge router from the overlay network:

1. In vManage NMS, select the Configuration ► Certificates screen.
2. From the list of vEdge routers, locate the failed router.
3. In the Validate column, click Invalid.
4. Click OK to confirm invalidation of the device.
5. Click Send to Controllers.

**Add the Replacement Router**

To add the replacement vEdge router into the overlay network:

1. In vManage NMS, select the Configuration ► Certificates screen.
2. From the list of vEdge routers, locate the replacement router.

3. In the Validate column, click Valid.

4. Click OK to confirm validation of the device.

5. Click Send to Controllers.

If you attempt to validate a router that has the same IP address as another router in the network, an error message is displayed, and the validation process is terminated.

**Release Information**

Introduced in vManage NMS in Release 15.4.

### Using Cisco vManage on Different Servers

You can perform the following operations in parallel from one or more Cisco vManage servers:

- Upgrade the software image on a device (Maintenance ► Software Upgrade screen)
- Activate a software image on a device (Maintenance ► Software Upgrade screen)
- Delete a software image from a device (Maintenance ► Software Upgrade screen)
- Set a software image to be the default image on a device (Maintenance ► Software Upgrade screen)
- Reboot a device (Maintenance ► Device Reboot screen)
- Manage templates (Configuration ► Templates screen):
  - Attach devices to a device template
  - Detach devices from a device template
  - Change the variable values for a device template that has devices attached to it

For template operations, the following rules apply:

- When a device template is already attached to a device, you can modify one of its feature templates. Then when you click Update ► Configure Devices, all other template operations—including attach devices, detach devices, and edit device values—are locked on all vManage servers until the update operation completes. This means that a user on another vManage server cannot perform any template operations until the update completes.

- You can perform the attach and detach device template operations on different devices, from one or more vManage servers, at the same time. However, if any one of these operations is in progress on one vManage server, you cannot edit any feature templates on any of the servers until the attach or detach operation completes.
Log In to the Cisco vManage Web Application Server

The Cisco vManage NMS runs as a web application server through which you log in to a running Cisco vManage NMS.

In an overlay network with a single Cisco vManage NMS, to log in to the NMS, use HTTPS, and specify the IP address of the NMS. Enter a URL in the format https://ip-address:8443, where 8443 is the port number used by Cisco vManage NMS. On the login page, enter a valid username and password, and then click Log In. You have five chances to enter the correct password. After the fifth incorrect attempt, you are locked out of the device, and you must wait 15 minutes before attempting to log in again.

In an overlay network that has a cluster of Cisco vManage NMSs, the cluster allows you to log in to one of the Cisco vManage NMSs that is operating in the role of a web application server. Use HTTPS, specifying the IP address of one of the Cisco vManage NMSs, in the format https://ip-address:8443. The cluster software load-balances login sessions among the individual Cisco vManage NMSs that are acting as web application servers. You cannot control which of the individual Cisco vManage NMSs you log in to.

With a Cisco vManage cluster, if you enter invalid login credentials, it might take some time for you to see an invalid login error message, and the amount of time increases as the size of the cluster increases. This delay happens because each Cisco vManage NMS attempts sequentially to validate the credentials. If none of the Cisco vManage NMSs validates you, only then do you see an invalid login error message.

To determine which Cisco vManage NMS you are logged in to, look in the Cisco vManage toolbar, which is located at the top of the every screen. The penultimate button shows the name of the NMS you are logged in to. To display more information about this particular NMS server, enter the name of the NMS in the Search filter of the Monitor ► Network screen.