



Cisco SD-WAN Overlay Network Bring-Up Process

- [Bring Up the Sequence of Events, on page 1](#)
- [Download Software, on page 28](#)
- [Deploy Cisco vManage, on page 29](#)
- [Deploy Cisco vBond Orchestrator, on page 41](#)
- [vContainer Host, on page 69](#)
- [Deploy Cisco vSmart Controller, on page 69](#)
- [Deploy Cisco Catalyst 8000V Using Cloud Services Provider Portals, on page 97](#)
- [Deploy Cisco CSR 1000v Using Cloud Service Provider Portals, on page 97](#)
- [Deploy the vEdge Cloud routers, on page 97](#)

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](#).

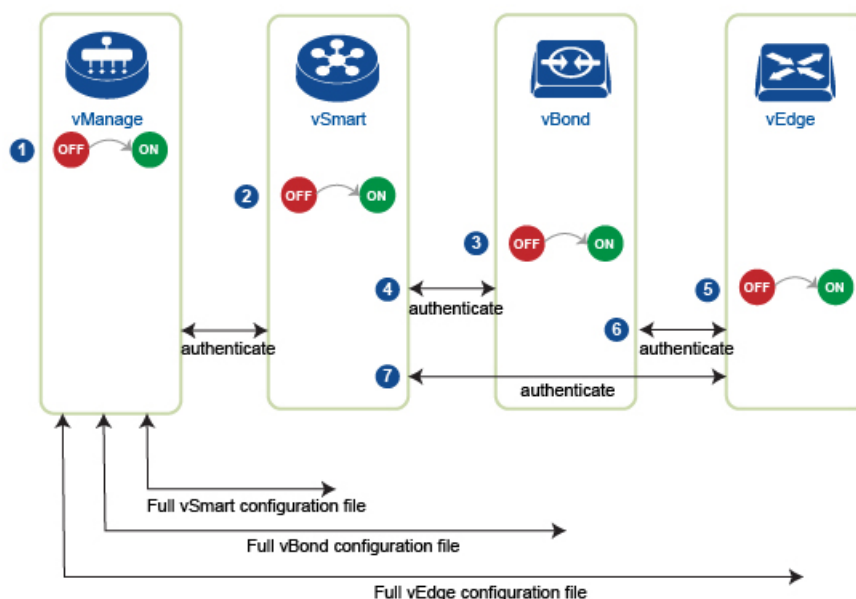
The end result of this two-part process is an operational overlay network.

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



368439

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 1:

Bring-Up Task	Step-by-Step Procedure
Step 1: Start the Cisco vManage.	<ol style="list-style-type: none"> 1. On the hypervisor, create a VM instance. 2. Boot Cisco vManage server, start the VM, and enter login information. 3. In vManage > Administration > 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. 4. In vManage > Certificates, generate the CSR. 5. Check for a confirmation email from Symantec that your request has been received. 6. Check for an email from Symantec that Viptela has approved your request and the certificate is signed. 7. In vManage > Configuration > Devices, check that the certificate has been installed.

Bring-Up Task	Step-by-Step Procedure
Step 2: Start the Cisco vBond Orchestrator.	<ol style="list-style-type: none"> 1. On the hypervisor, create a VM instance. 2. Boot the vBond server and start the VM. 3. In vManage > Configuration > Devices > Controller, add Cisco vBond Orchestrator and generate the CSR. 4. Check for a confirmation email from Symantec that your request has been received. 5. Check for an email from Symantec that Viptela has approved your request and the certificate is signed. 6. In vManage > Configuration > Devices, check that the certificate has been installed. 7. In vManage > Configuration > Templates: <ol style="list-style-type: none"> a. Create a configuration template for the Cisco vBond Orchestrator. b. Attach the template to Cisco vBond Orchestrator. 8. In vManage > Dashboard, verify that the Cisco vBond Orchestrator is operational.
Step 3: Start the Cisco vSmart Controller.	<ol style="list-style-type: none"> 1. On the hypervisor, create a VM instance. 2. Boot the vSmart server and start the VM. 3. In vManage > Configuration > Devices > Controller, add Cisco vSmart Controller and generate the CSR. 4. Check for a confirmation email from Symantec that your request has been received. 5. Check for an email from Symantec that Viptela has approved your request and the certificate is signed. 6. In vManage > Configuration > Devices, check that the certificate has been installed. 7. In vManage > Configuration > Templates: <ol style="list-style-type: none"> a. Create a configuration template for Cisco vSmart Controller. b. Attach the template to Cisco vSmart Controller. 8. In vManage > Dashboard, verify that Cisco vSmart Controller is operational.

Bring-Up Task	Step-by-Step Procedure
Step 4: Configure the router.	<ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> a. Create a configuration template for the router. b. Attach the template to the router.
Step 5: Connect AC power and boot a hardware router.	<ol style="list-style-type: none"> 1. Connect AC power to the router. 2. If needed, flip the On/Off switch on the rear of the router to the ON position. 3. In vManage > Dashboard or in vManage > Monitor > Network > Device Dashboard, verify that the router is operational.

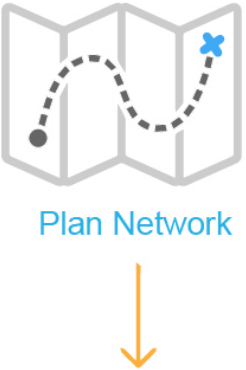
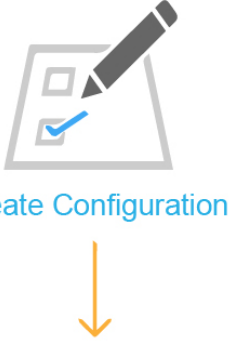
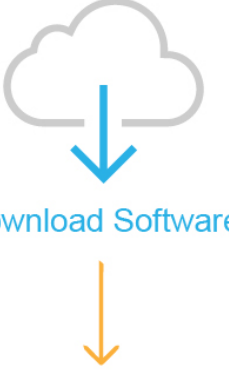
Summary of the User Portion of the Bring-Up Sequence

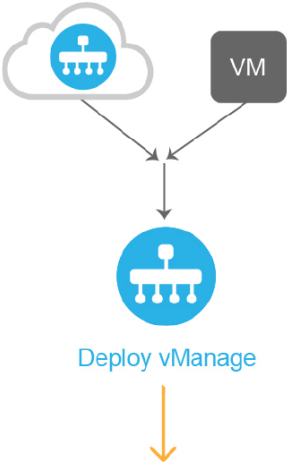
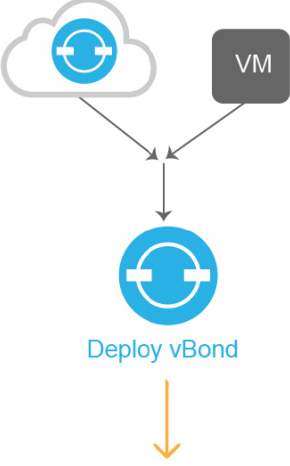
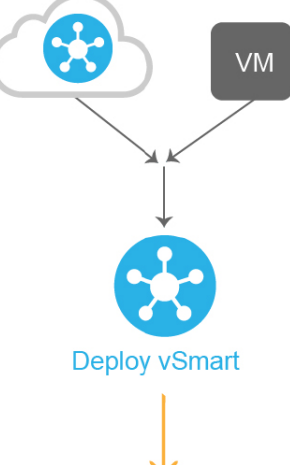
Generally, what you do to bring up the Cisco SD-WAN overlay network is what you do to bring up any network. You plan out the network, create device configurations, and then deploy the network hardware and software components. These components include all the Cisco vEdge devices, all the traditional routers 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.

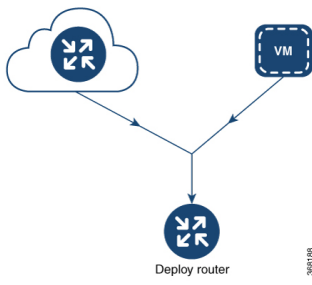
The following table summarizes the steps for the user portion of the Cisco SD-WAN overlay network bring-up sequence. The details of each step are provided in the articles that are listed in the **Procedure** column. While you can bring up the Cisco vEdge devices in any order, it is recommended that you 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 2:

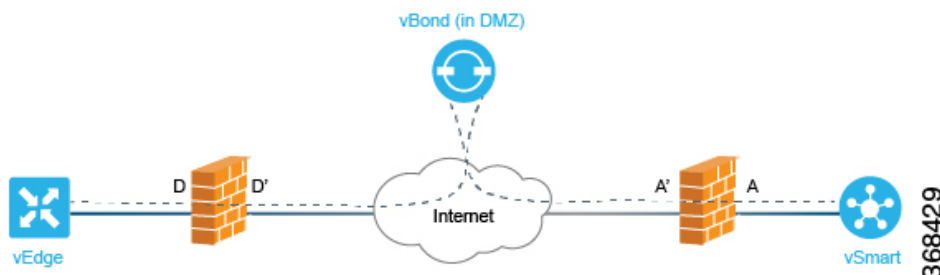
	Workflow	Procedure
1	 368182	Plan out your overlay network. See Components of the Cisco SD-WAN Solution.
2	 368183	On paper, create device configurations that implement the desired architecture and functionality. See the Software documentation for your software release.
3	 368184	Download the software images.

Workflow	Procedure
<p>4</p>  <p>366185</p>	<p>Deploy Cisco vManage in the data center:</p> <ol style="list-style-type: none"> 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.
<p>5</p>  <p>366186</p>	<p>Deploy the Cisco vBond Orchestrator:</p> <ol style="list-style-type: none"> 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.
<p>6</p>  <p>366187</p>	<p>Deploy the Cisco vSmart Controller in the data center:</p> <ol style="list-style-type: none"> 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.

Workflow	Procedure
<p>7</p> 	<p>Deploy the Cisco vEdge routers in the overlay network:</p> <ol style="list-style-type: none"> 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 routers, send a certificate signing request to Symantec and then install the signed certificate on the router. 3. From Cisco vManage, send the serial numbers of all Cisco vEdge routers to the Cisco vSmart Controller and Cisco vBond Orchestrators in the overlay network. 4. Create a full configuration for the Cisco vEdge routers.

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 bringup 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.

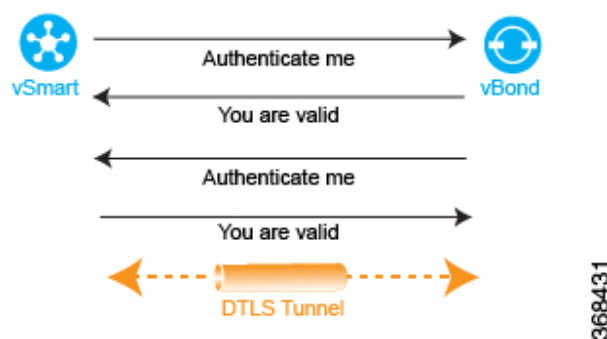
The Cisco vSmart Controllers and Cisco vBond Orchestrators learn the serial and chassis numbers during the initial configuration of these devices:

- 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.



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.

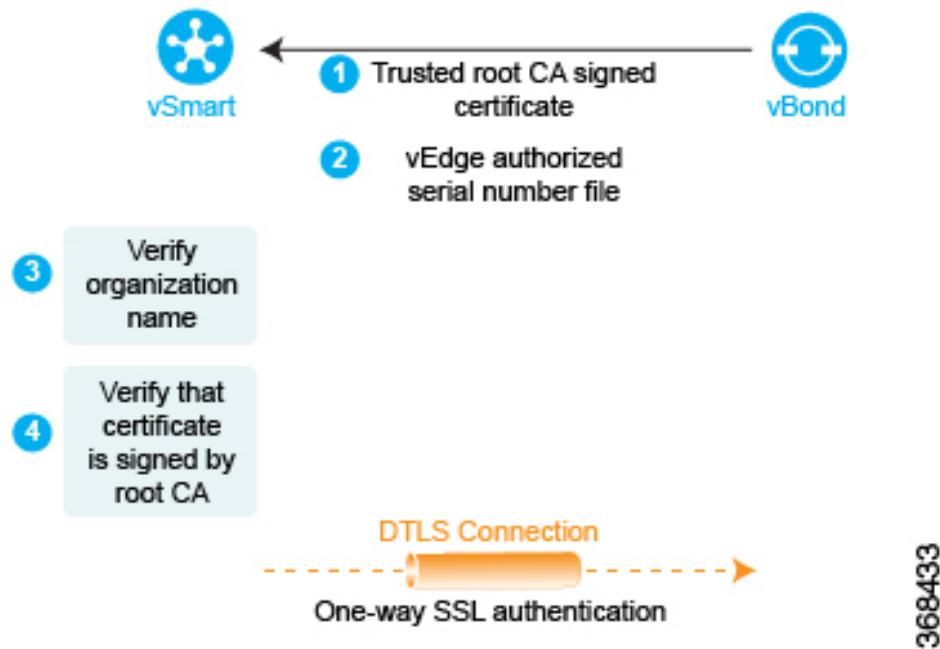
If Cisco vBond Orchestrator has not yet started when Cisco vSmart Controller initiates the authentication process, Cisco vSmart Controller periodically attempts to initiate a connection until it is successful.

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:

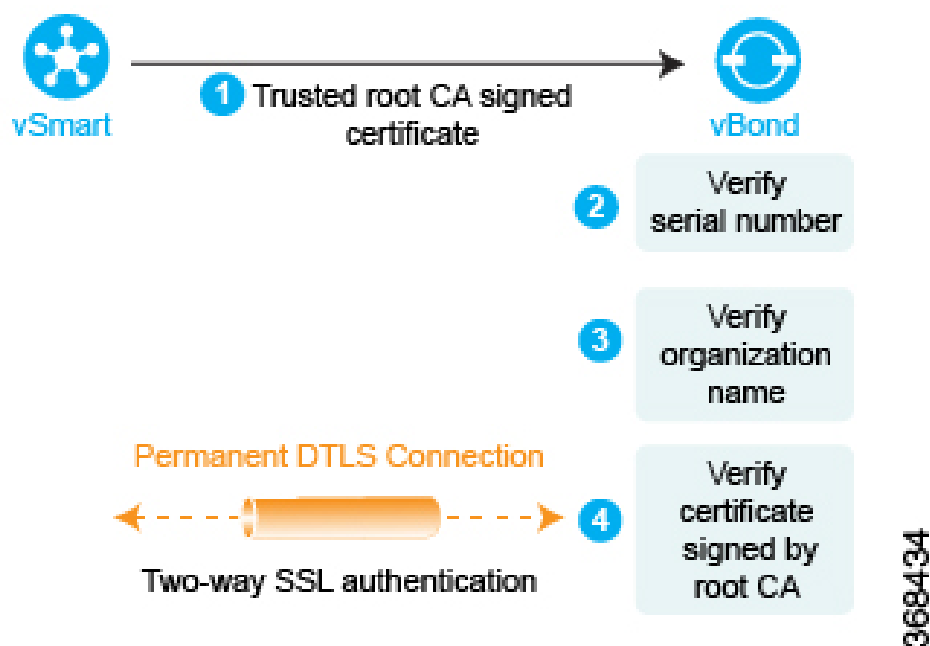
1. Cisco vBond Orchestrator sends its trusted root CA signed certificate to the vSmart controller.
2. Cisco vBond Orchestrator sends the vEdge authorized serial number file to the vSmart controller.
3. Cisco vSmart Controller uses its chain of trust to extract the organization name from the certificate 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.

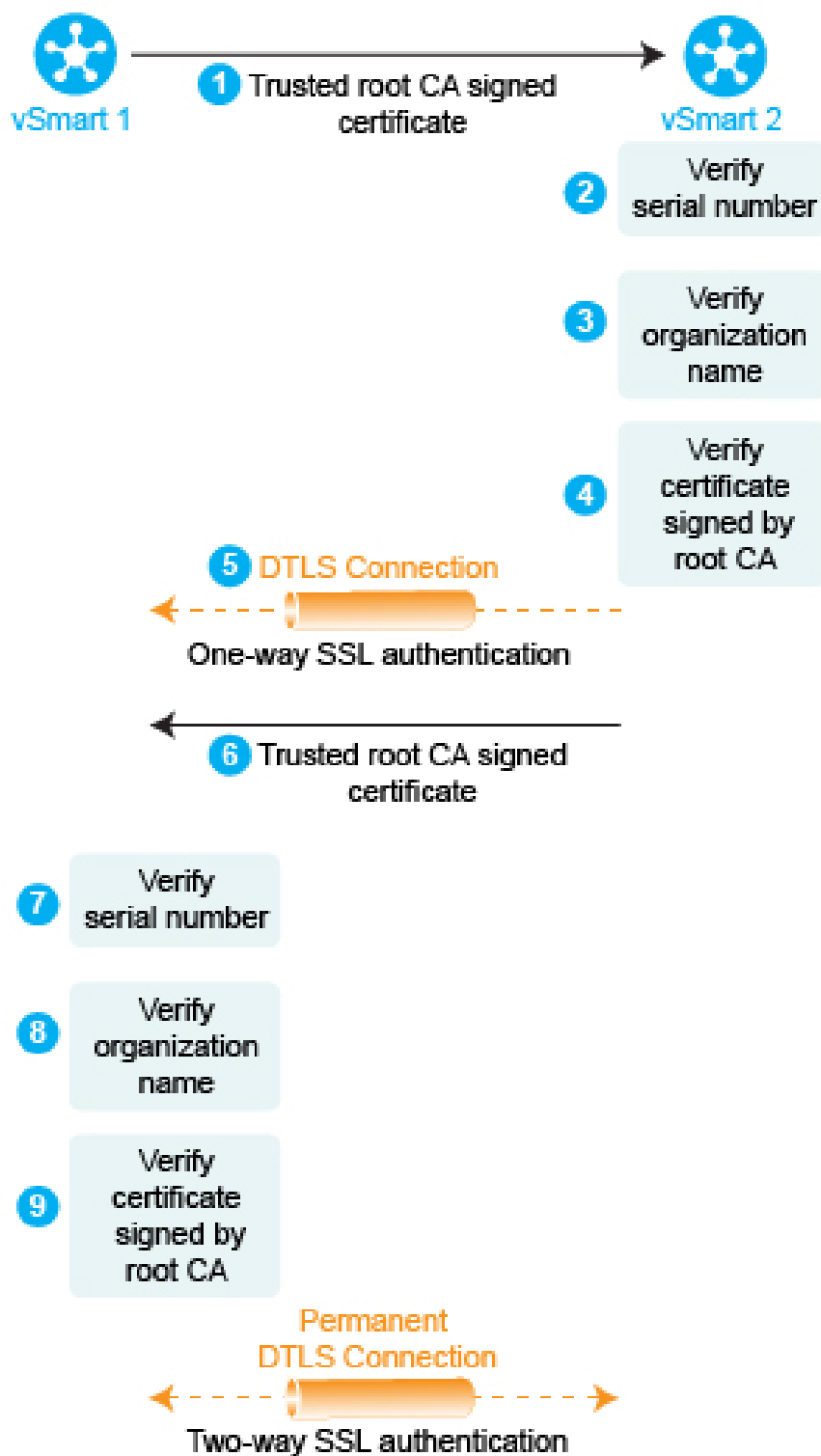
Then, Cisco vSmart Controllers perform the steps below to authenticate each other. Again, each device authenticates the other in parallel, but for clarity, we describe the process sequentially.

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.



368466

After performing these three checks, vSmart1 authentication of vSmart2 is complete, and the temporary DTLS connection between the two devices becomes permanent.

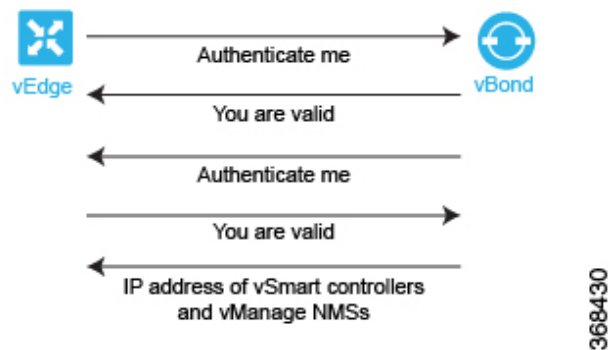
After all the Cisco vSmart Controllers have registered themselves with Cisco vBond Orchestrator, Cisco vBond Orchestrator and Cisco vSmart Controllers are ready to validate and authenticate the vEdge routers in the Cisco SD-WAN network.

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 or 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.

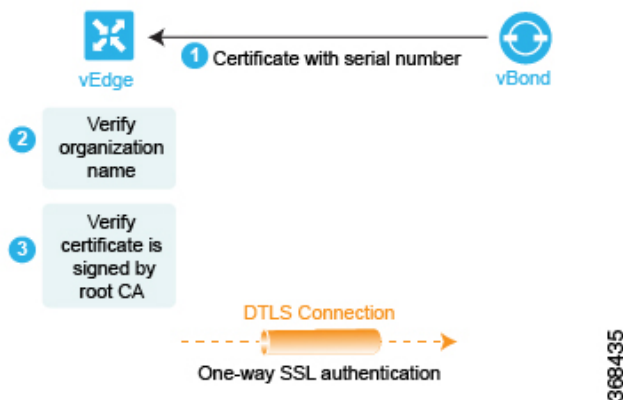
If Cisco vBond Orchestrator has not yet started when a vEdge router initiates the authentication process, the vEdge router periodically attempts to initiate a connection until the attempt succeeds.

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 router 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.

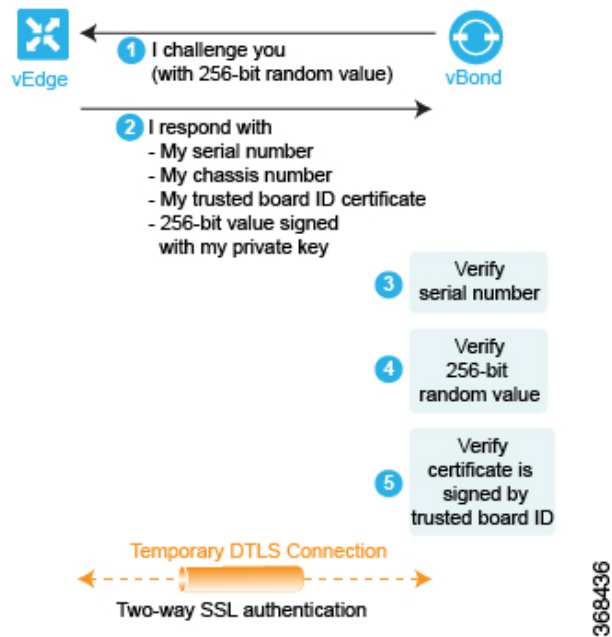


After performing these two checks, the vEdge router knows that Cisco vBond Orchestrator is valid, and its authentication of Cisco vBond Orchestrator is complete.

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 routers 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.

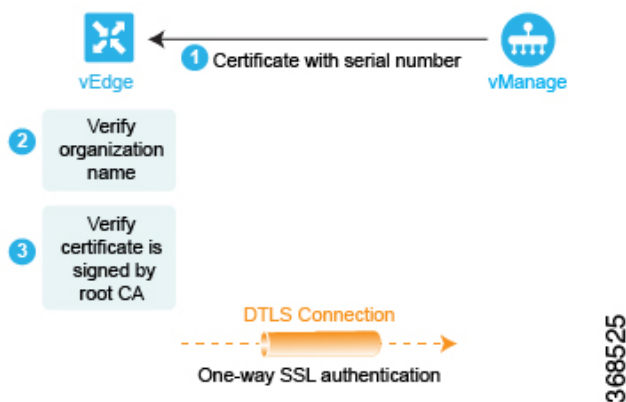
If you are not using Cisco vManage, you can log in to the vEdge router and either manually load its configuration file or manually configure the router.

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:

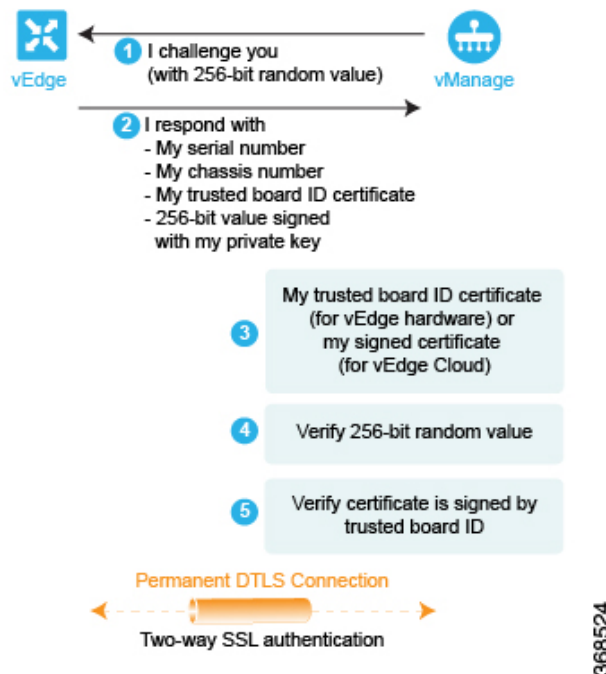
1. Cisco vManage sends its trusted root CA signed certificate to the vEdge router.
2. The vEdge router uses its chain of trust to extract the organization name from the certificate and compares it to the organization name that is configured on the router itself. If the two organization names match, the 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 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.

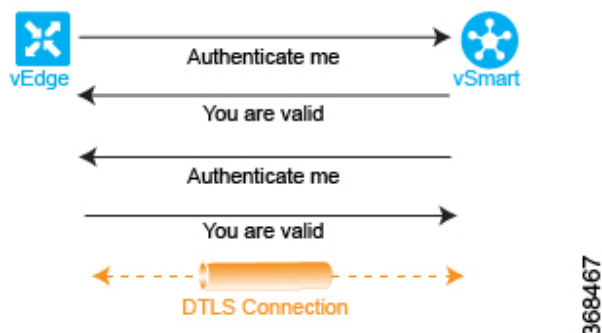


After performing these three checks, Cisco vManage knows that vEdge router is valid, and its authentication of the router is complete.

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.

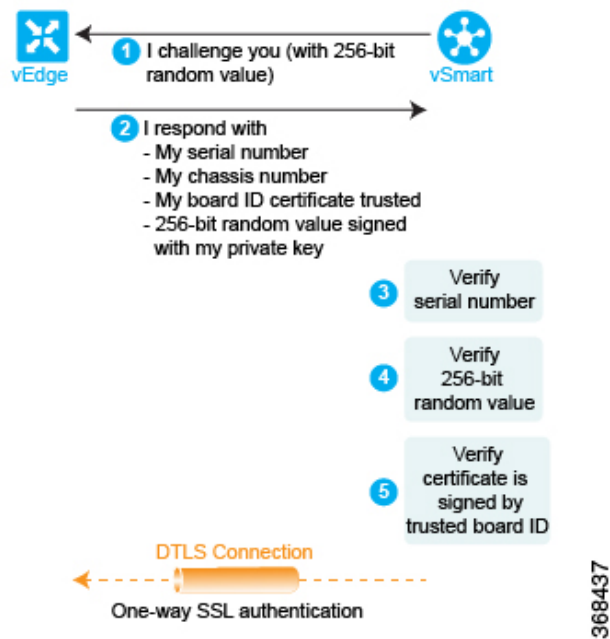


In this section below, is a more detailed step-by-step description of how the automatic authentication occurs between Cisco vSmart Controller and a vEdge router.

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:

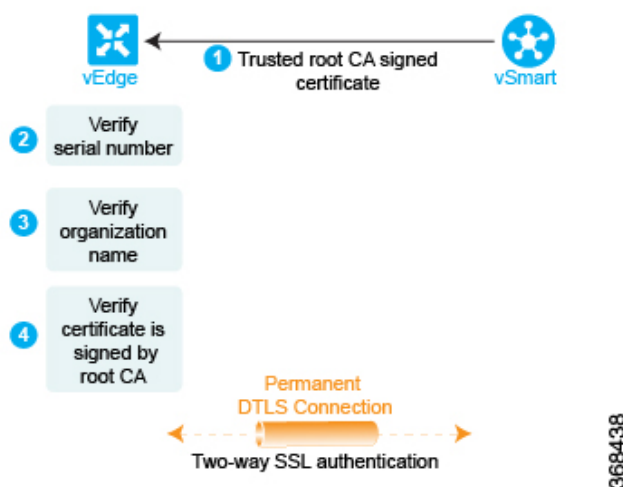
1. Cisco vSmart Controller sends a challenge to the vEdge router. The challenge is a 256-bit random value.
2. The vEdge router sends a response to the challenge that includes the following:
 - vEdge serial number
 - vEdge chassis number
 - vEdge board ID certificate
 - 256-bit random value signed by 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 through 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.

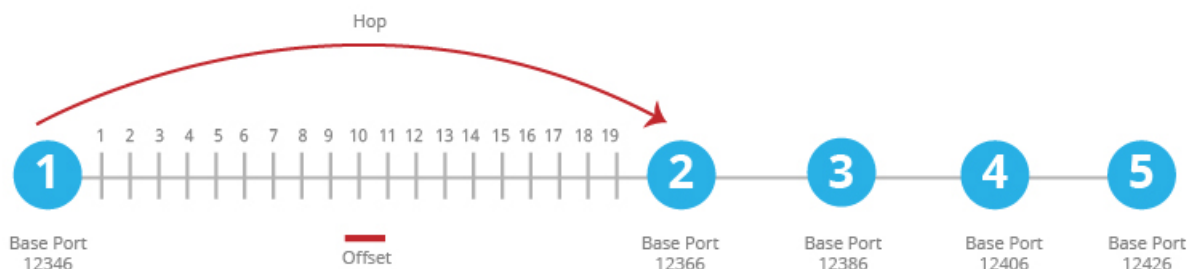
Incrementing the ports by 20 ensures that there is never any overlap among the possible base port numbers.

vEdge routers use port hopping when attempting to establish connections to Cisco vManage, Cisco vBond Orchestrator, and Cisco vSmart Controllers. You can also manually request a vEdge router 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 vEdge router 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.



368513

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 vEdge router remain consistent across all sessions initiated by the vEdge router. 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 vEdge routers remain up, when the controller device comes back up, the connection between it and the vEdge router might shut down and restart, and in some cases the BFD sessions on the vEdge router 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 vEdge routers. 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 vEdge routers.
- All control sessions on all Cisco vSmart Controllers go down, and BFD sessions on the vEdge routers 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 vEdge routers have already port hopped to a different port in an attempt to reconnect to Cisco vSmart Controllers.

Ports Used by vEdge Routers

When a vEdge router 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 vEdge router 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 vEdge routers 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 vEdge router's WAN port 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 vEdge routers 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 vEdge routers 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 vEdge routers 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 Cisco vEdge routers configured to use TLS tunnels, which use TCP, the routers select a random TCP port. Therefore, you must configure proper NAT entries for Cisco vManage and Cisco vSmart Controllers to be able to communicate with Cisco vEdge routers.

For Cisco vEdge routers configured to use DTLS tunnels, which use UDP, at a minimum you must open the five base ports that are used by a vEdge router 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 3:

Core Number	Ports for DTLS (UDP)	Ports for TLS (TCP)
Core0	12346	23456
Core1	12446	23556
Core2	12546	23656
Core3	12646	23756
Core4	12746	23856
Core5	12846	23956
Core6	12946	24056
Core7	13046	24156

Administrative Ports Used by Cisco vManage

Cisco vManage uses the following administrative ports for protocol-specific communication:

Purpose	Traffic Direction	Protocol	Port Number
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
HTTPS	Incoming	TCP	443

Purpose	Traffic Direction	Protocol	Port Number
SNMP query	Incoming	UDP	161
SSH	Incoming Cisco vManage uses SCP to install signed certificates onto the controllers if DTLS/TLS connections are not yet formed between them. SSH uses TCP destination port 22.	TCP	22
RADIUS	Outgoing	UDP	1812
SNMP trap	Outgoing	UDP	162
Syslog	Outgoing	UDP	514
TACACS	Outgoing	TCP	49

vManage clusters use the following ports for communication among the NMSs that comprise the cluster:

vManage Service	Traffic Direction	Protocol	Port Numbers
Application server	Bidirectional	TCP	80, 443, 7600, 8080, 8443, 57600
Configuration database	Bidirectional	TCP	2424, 2434
Coordination server	Bidirectional	TCP	2181, 3888
Message bus	Bidirectional	TCP	9092
Statistics database	Bidirectional	TCP	9200, 9300
Tracking of device configurations (NCS and Netconf)	Bidirectional	TCP	830

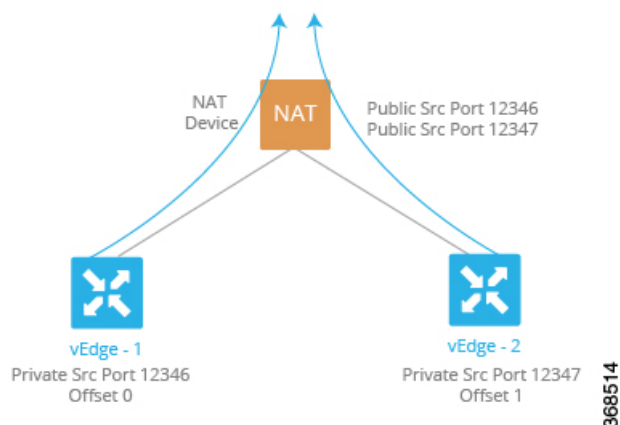
Configure the Port Offset

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 vEdge router to port-hop:

```
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:

1. Go to <http://viptela.com/support/> and log in.
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 be 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.
5. Create a multitenant Cisco vManage.

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_
GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_
GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_
GCM_SHA384

In Release 16.2, vManage web servers support the following ciphers:

- TLS_ECDHE_ECDSA_WITH_AES_128_
CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_
CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

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.

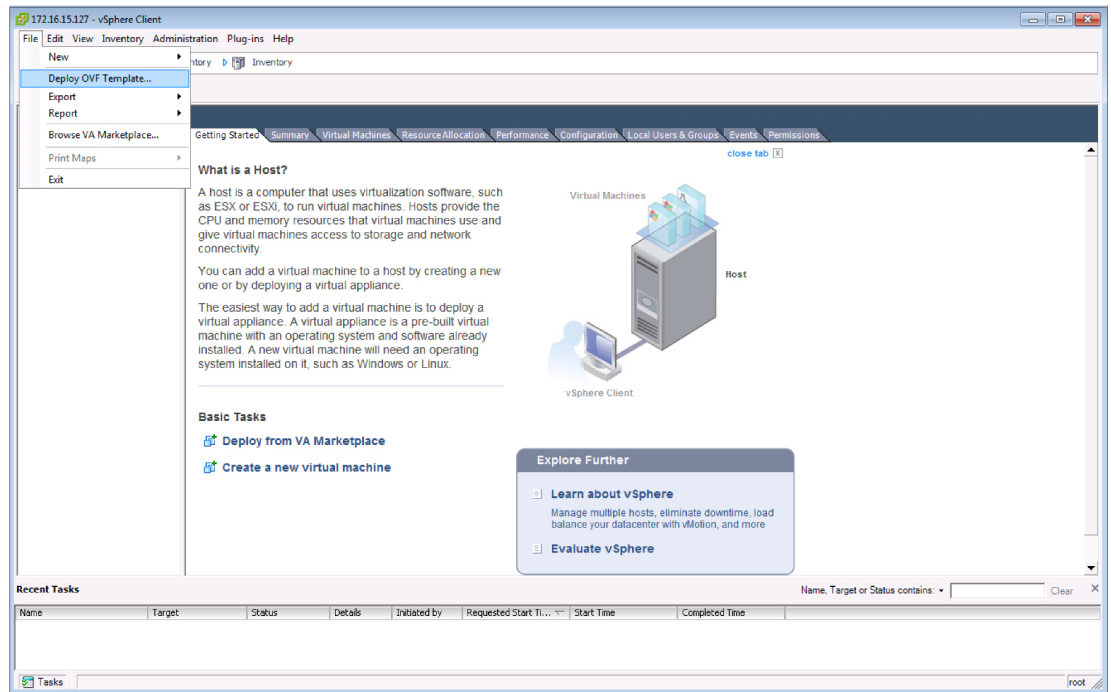
If you are using the VMware vCenter Server to create the Cisco vManage VM instance, follow the same procedure.

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 100 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:

```
# 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)# commit and-quit
#
```

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 4:

Feature	Template Name
Authentication, Authorization, and Accounting (AAA)	AAA
Security	Security
System-wide parameters	System
Transport VPN (VPN 0)	VPN, with the VPN ID set to 0.
Management VPN (for out-of-band management traffic)	VPN, with the VPN ID set to 512.

-->

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 the 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.
14. In the Security feature template, configure the control plane protocol.
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
 !
 !
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 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
  allow-service https
  !
  no shutdown
  !
ip route 0.0.0.0/0 10.0.12.13
!
vpn 512
  interface eth0
  ip 172.16.14.145/23
  no shutdown
  !
ip route 0.0.0.0/0 172.16.14.1
!

```

What's Next

See *Configure Certificate Settings*.

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:

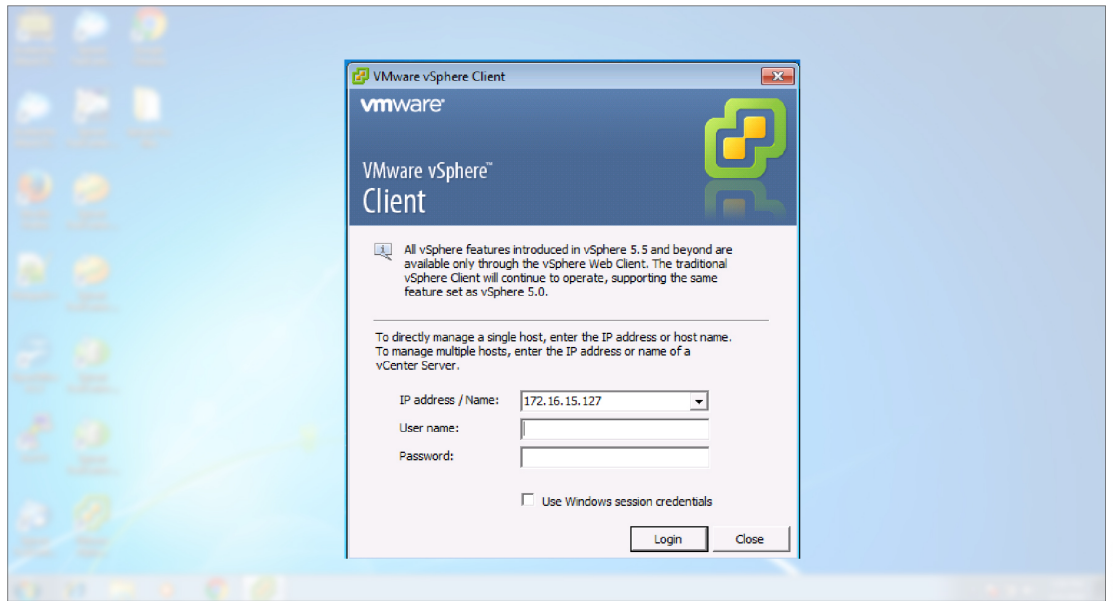
1. Launch the vSphere client and Create a vBond VM instance.
2. Add a vNIC for the tunnel interface.
3. Start the vBond VM instance and connect to the console.

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 look different than the vSphere Client screens shown in the procedure.

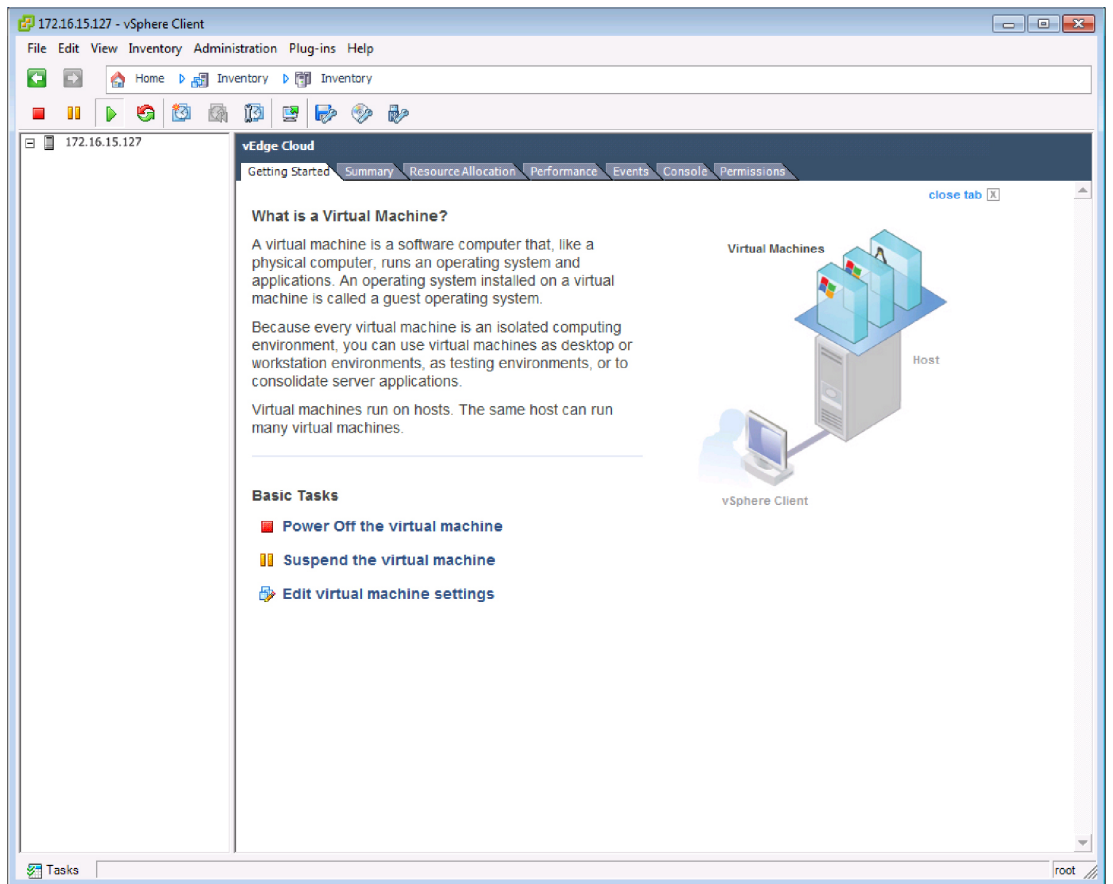
Launch vSphere Client and Create a vBond VM Instance

1. Launch the VMware vSphere Client application, and enter the IP address or name of the ESXi server, your username, and your password. Click **Login** to log in to the ESXi server.



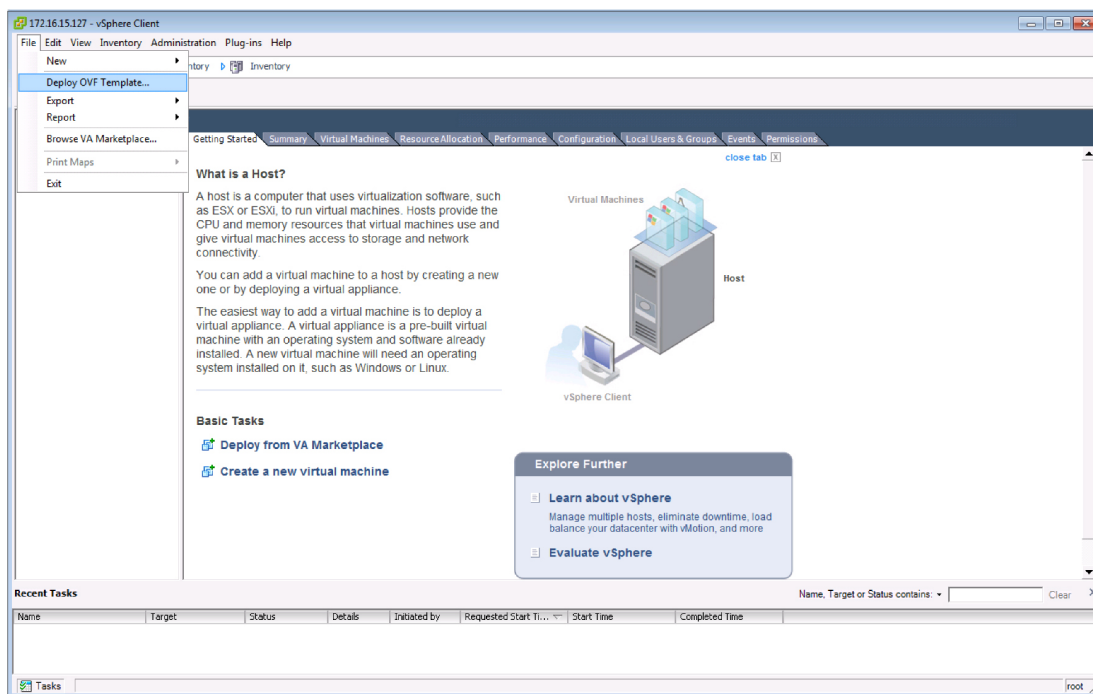
368256

The system displays the ESXi screen.

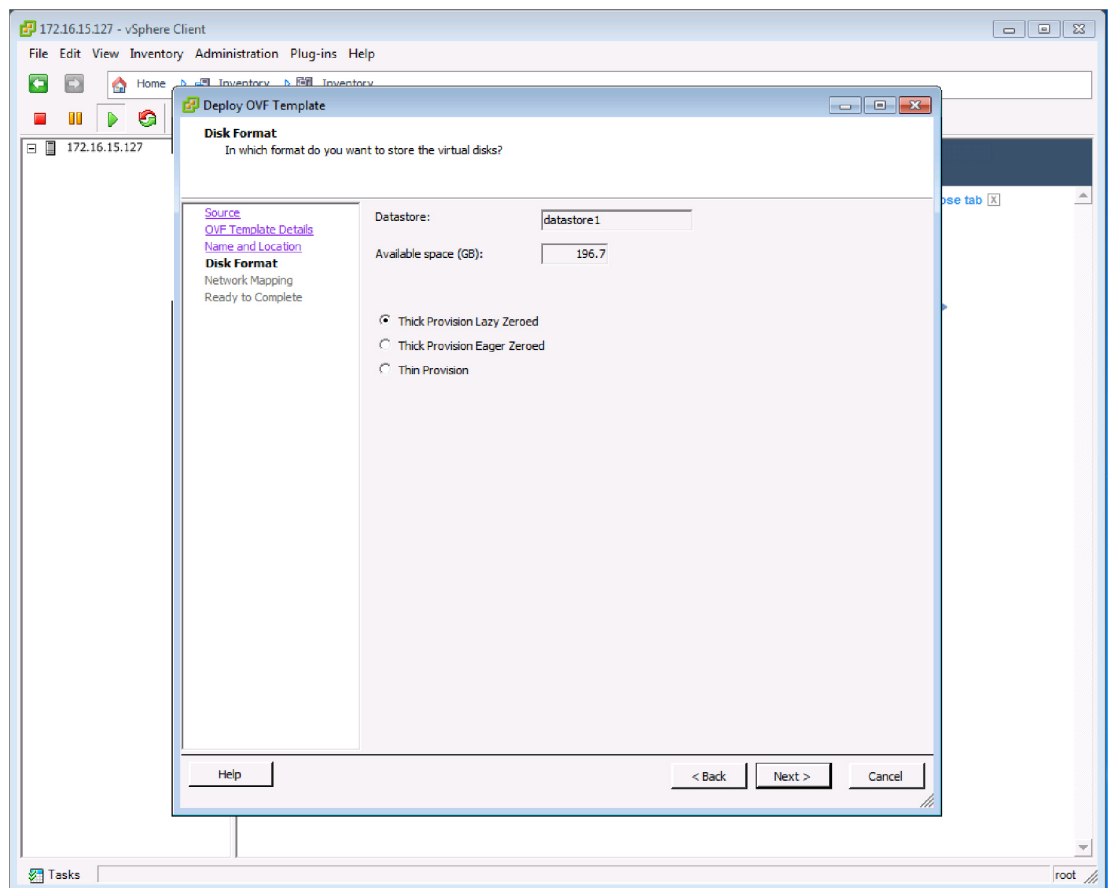


368239

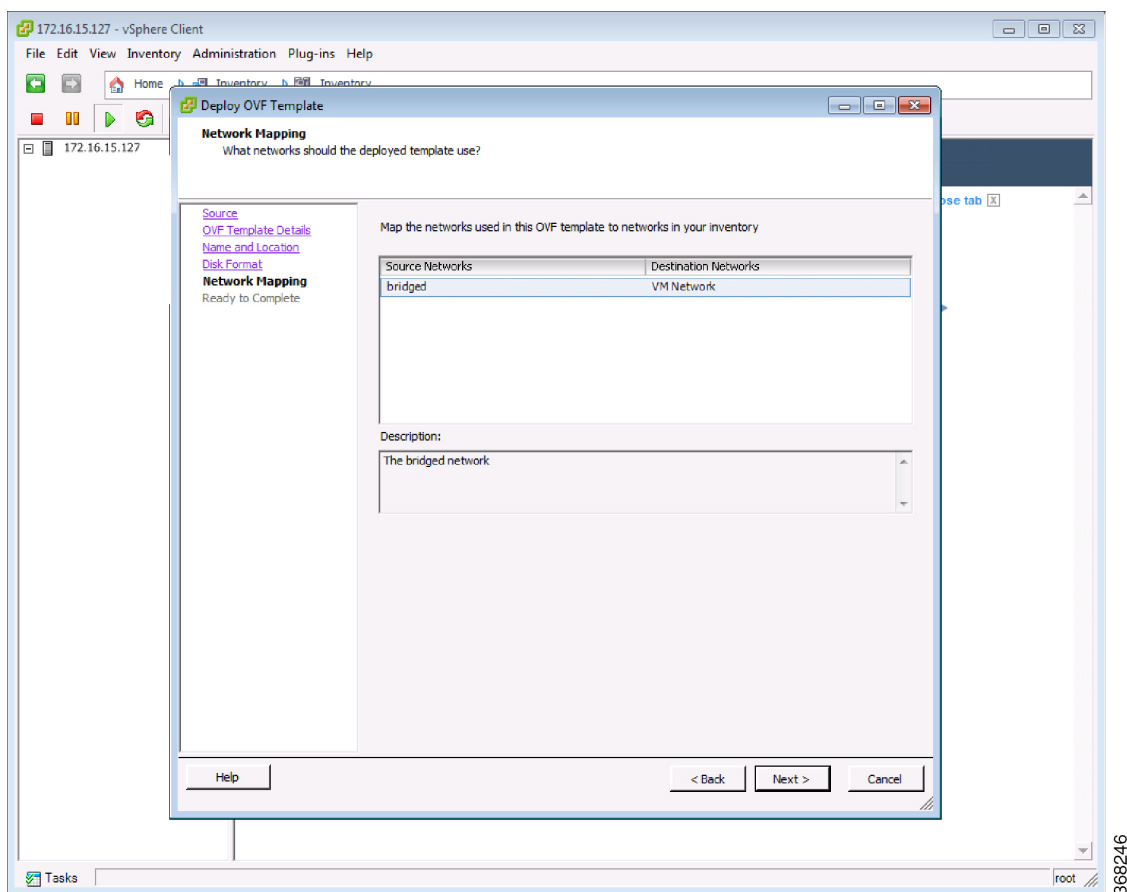
2. Click **File > Deploy OVF Template** to deploy the virtual machine.



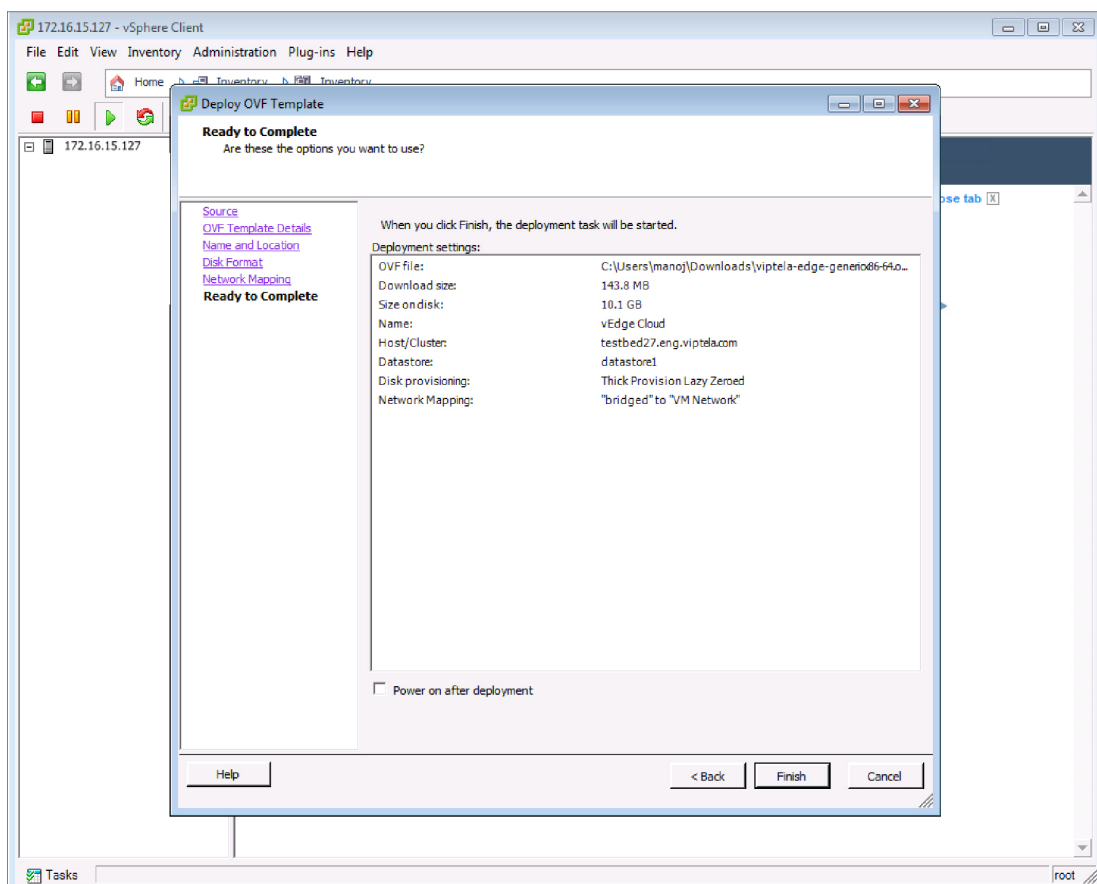
3. In the Deploy OVF Template screen, enter the location to install and download the OVF package. This package is the vedge.ova file that you downloaded from Cisco. Then click **Next**.
4. Click **Next** to verify OVF template details.
5. Enter a name for the deployed template and click **Next**. The 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.



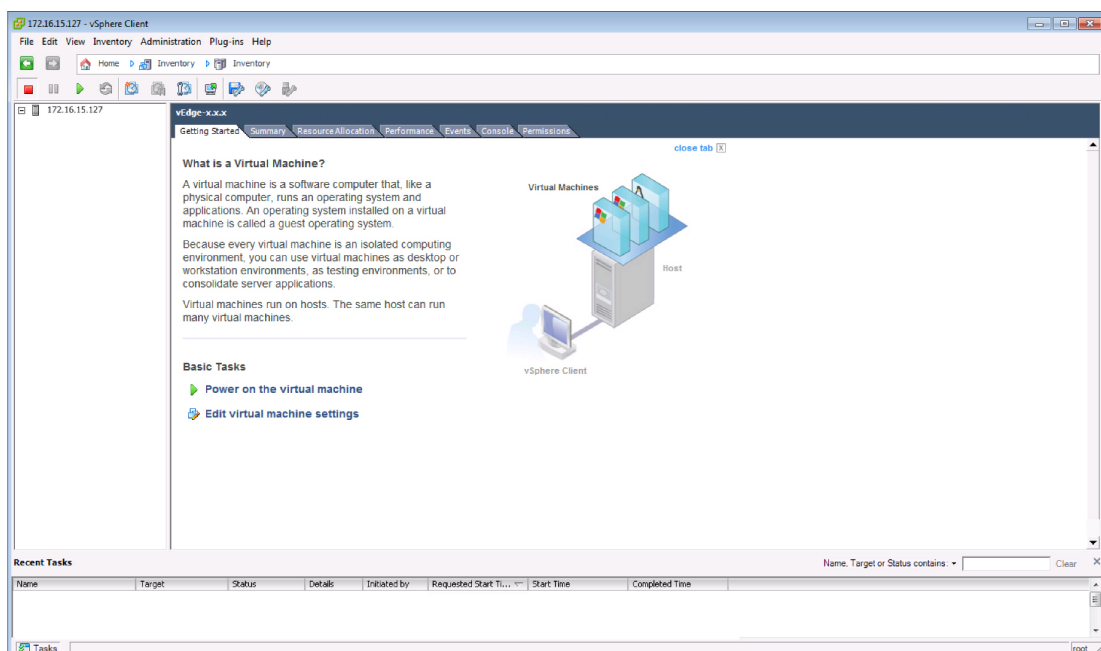
8. In the Ready to Complete screen, click **Finish**. The figure below shows the name for the vBond instance.



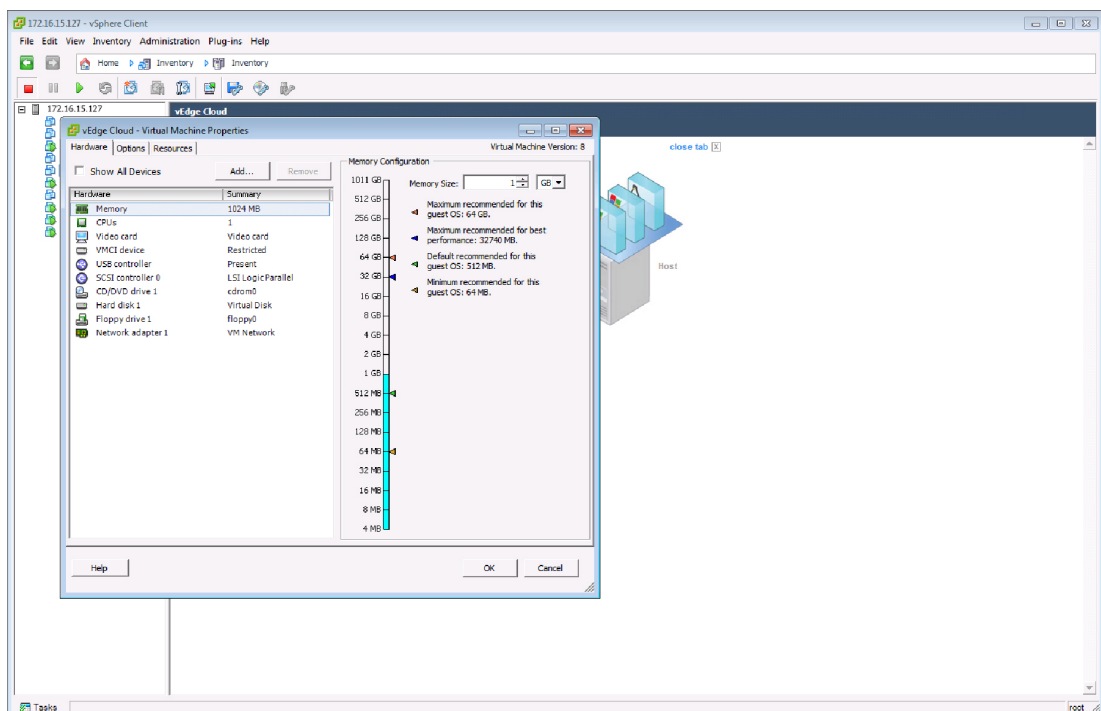
The system has successfully created the VM instance with the parameters you just defined and displays the vSphere Client screen with the **Getting Started** tab selected. By default, this includes one vNIC. This vNIC is used for the management interface.

Add a vNIC for the Tunnel Interface

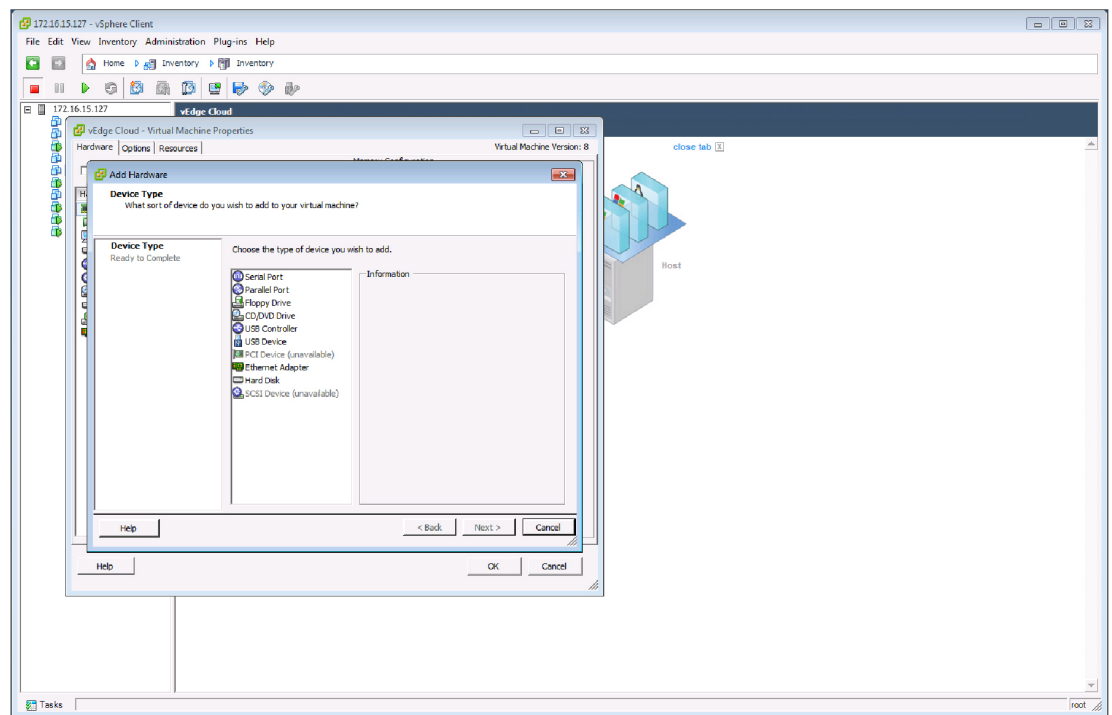
1. In the left navigation bar of the vSphere Client, select the vBond VM instance you just created, and click **Edit virtual machine settings**.



- In the vEdge Cloud – Virtual Machine Properties screen, click **Add** to add a new vNIC for the management interface. Then click **OK**.

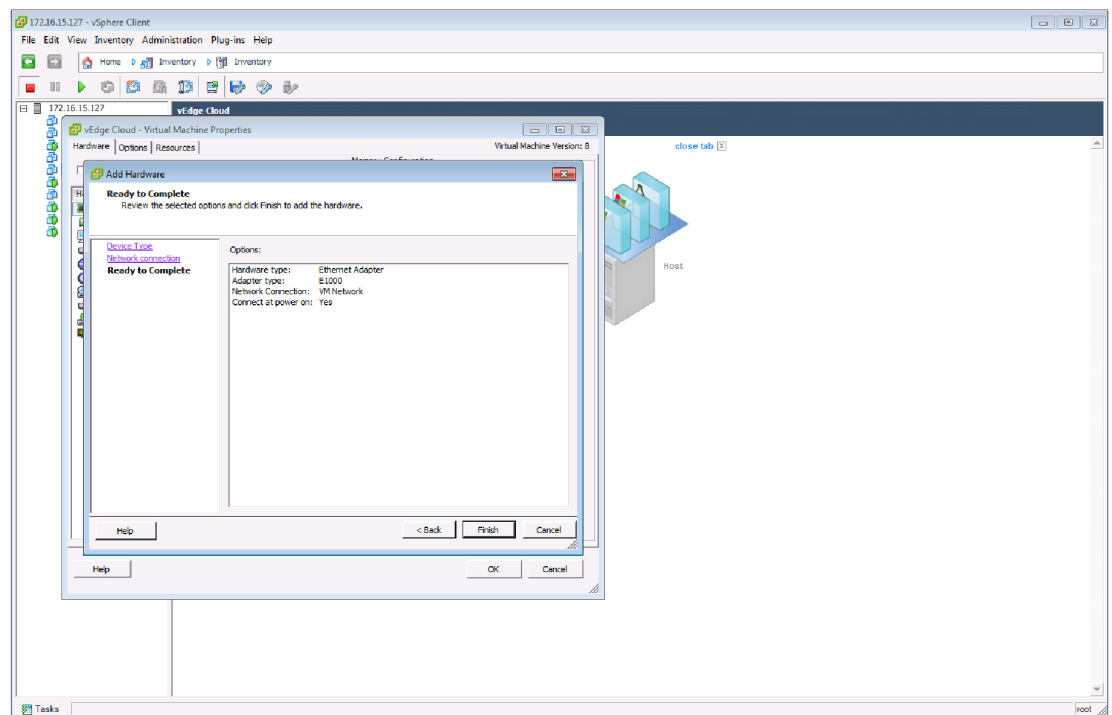


- Click Ethernet Adapter for the type of device you wish to add. Then click **Next**.



368332

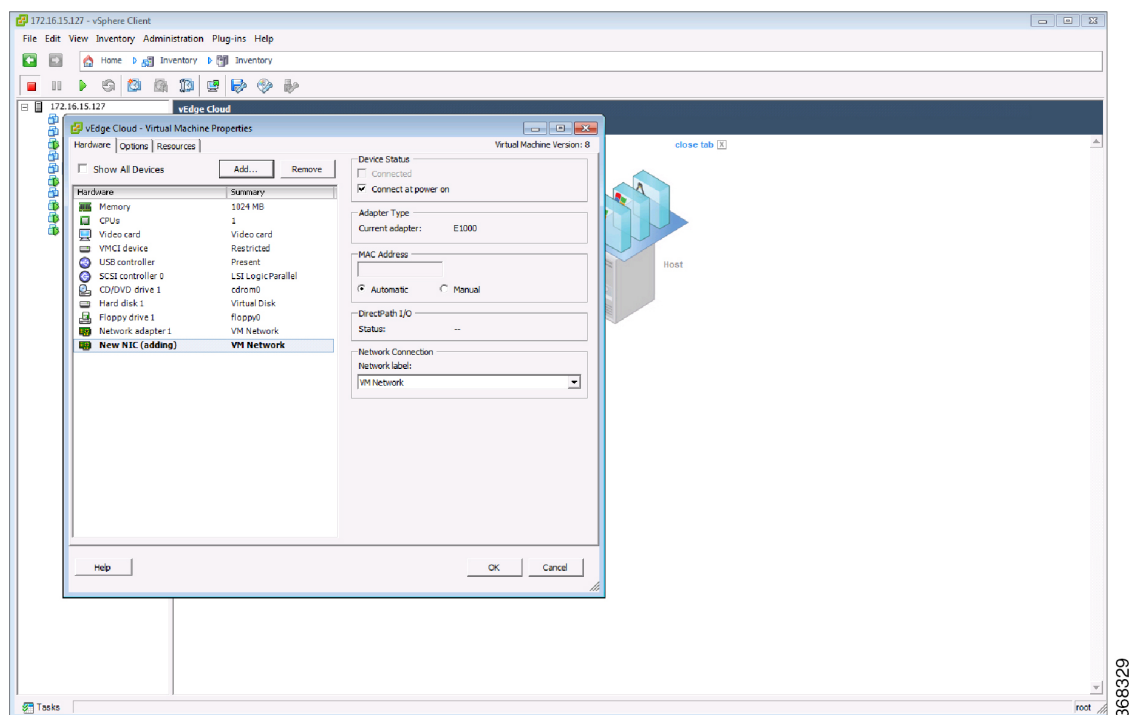
4. In the **Adapter Type** drop-down, select VMXNET3 for the vNIC to add. Then click **Next**.
5. In the Ready to Complete screen, click **Finish**.



368330

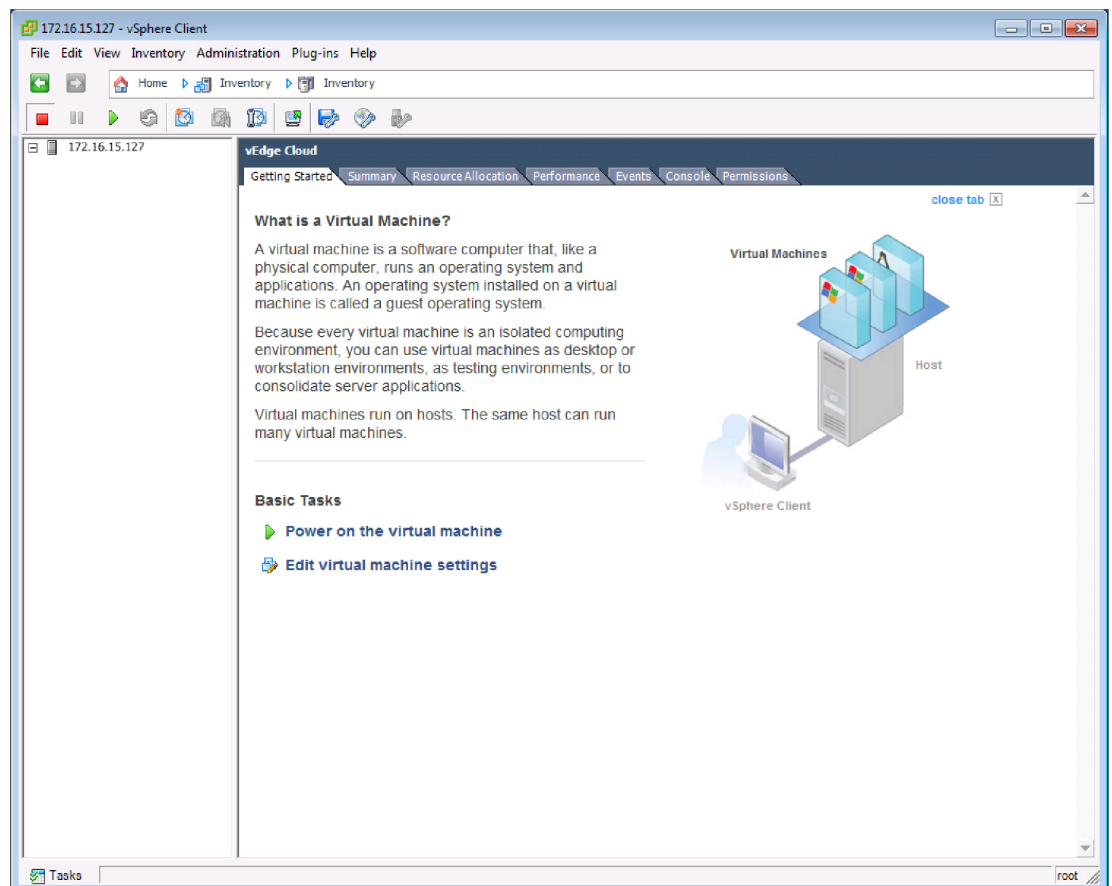
6. The vEdge Cloud – Virtual Machine Properties screen opens showing that the new vNIC is being added. Click **OK** to return to the vSphere Client screen.

Create vBond VM Instance on ESXi

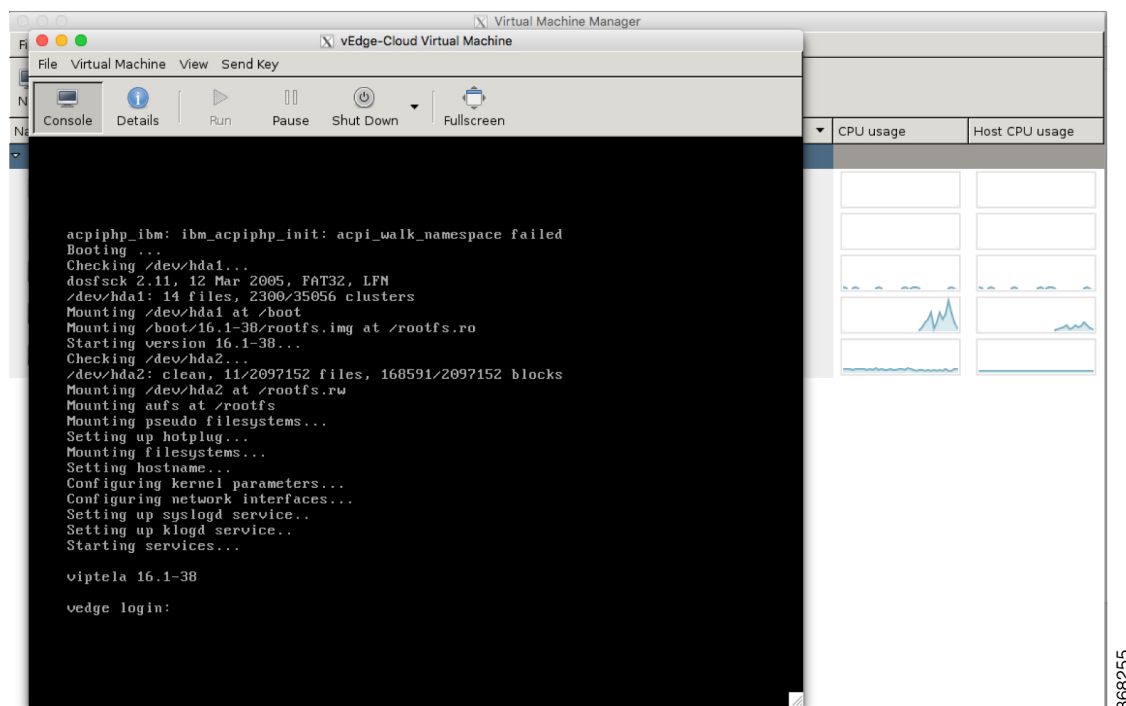


Start the vBond VM Instance and Connect to the Console

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*.

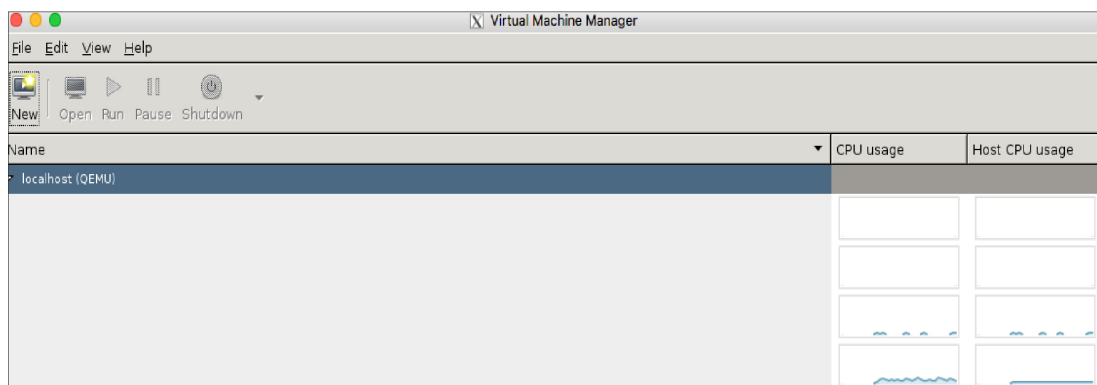
Create vBond VM Instance on KVM

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*.

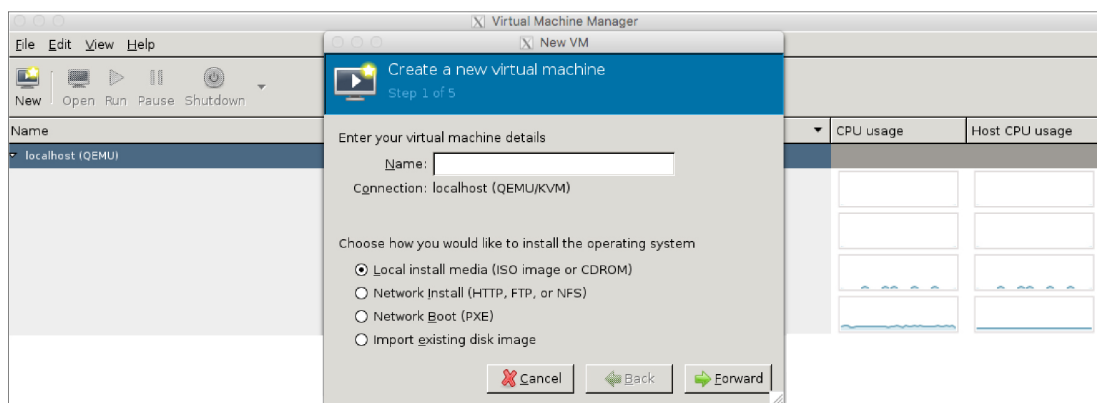
To create a vBond VM instance on the KVM hypervisor:

1. Launch the Virtual Machine Manager (virt-manager) client application. The system displays the Virtual Machine Manager screen.



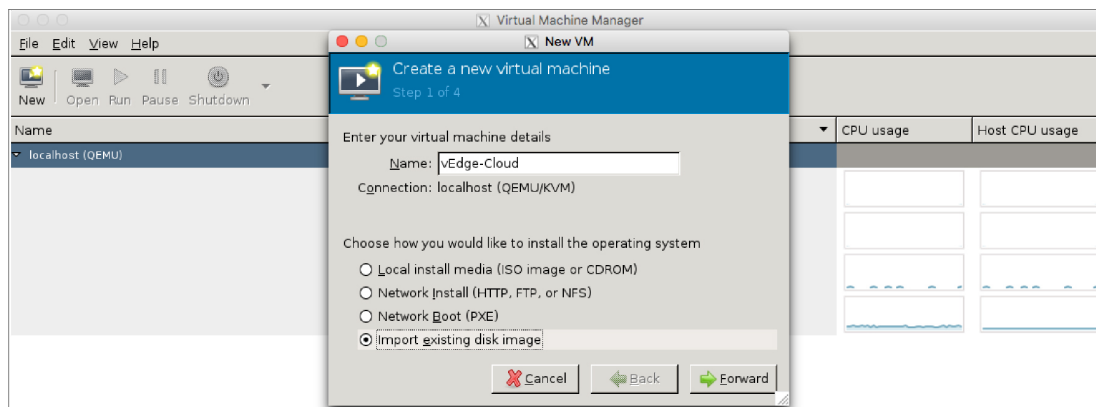
368248

2. Click **New** to deploy the virtual machine. The system opens the Create a new virtual machine screen.



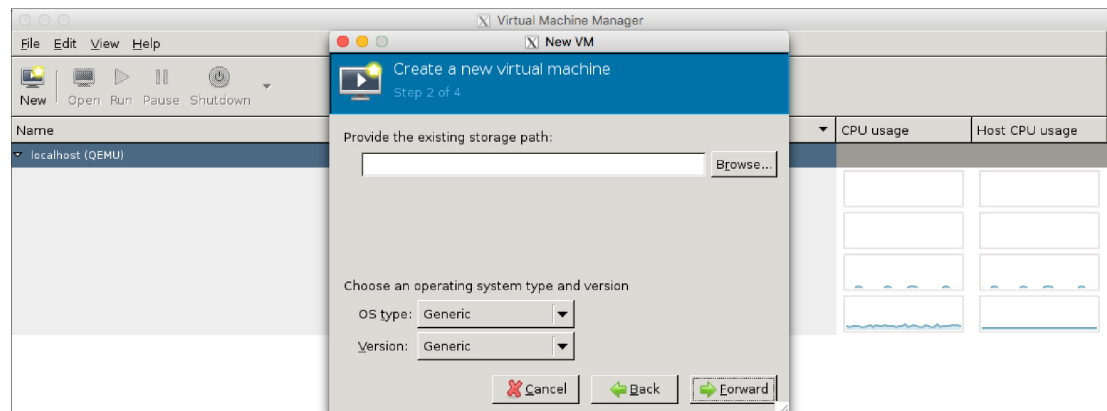
368249

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**.

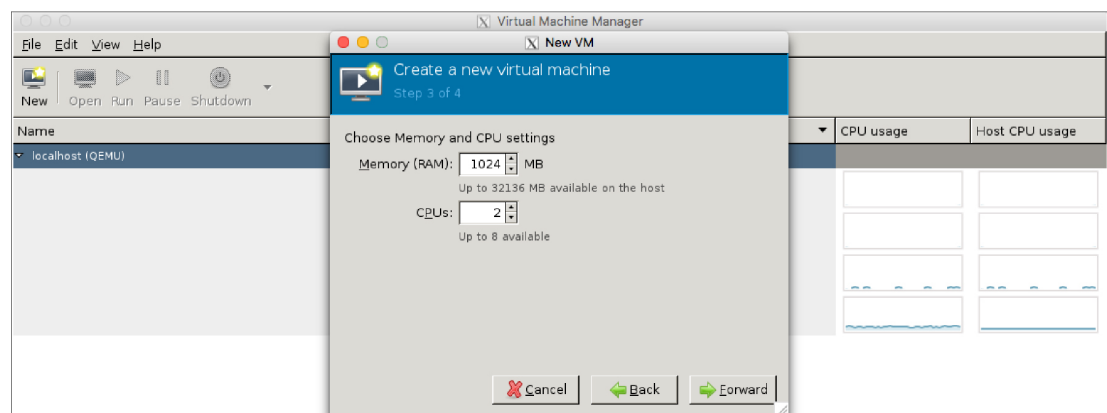


368250

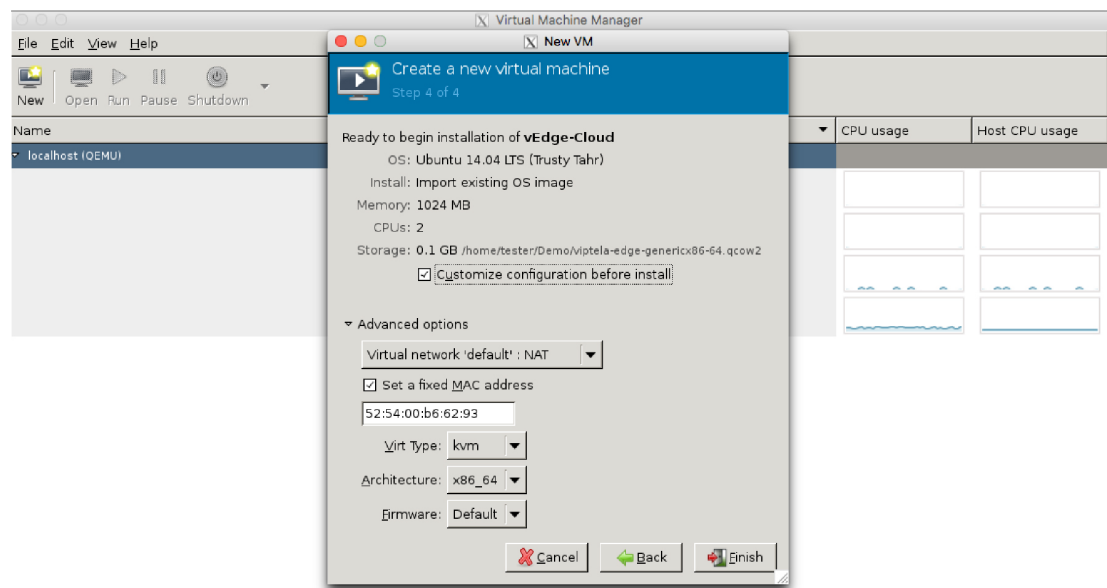
4. For **Provide the existing storage path** field, click **Browse** to find the vBond software image.
 - a. In the **OS Type** field, choose **Linux**.
 - b. In the **Version** field, choose the Linux version that you are running.

c. Click **Forward**.

368252

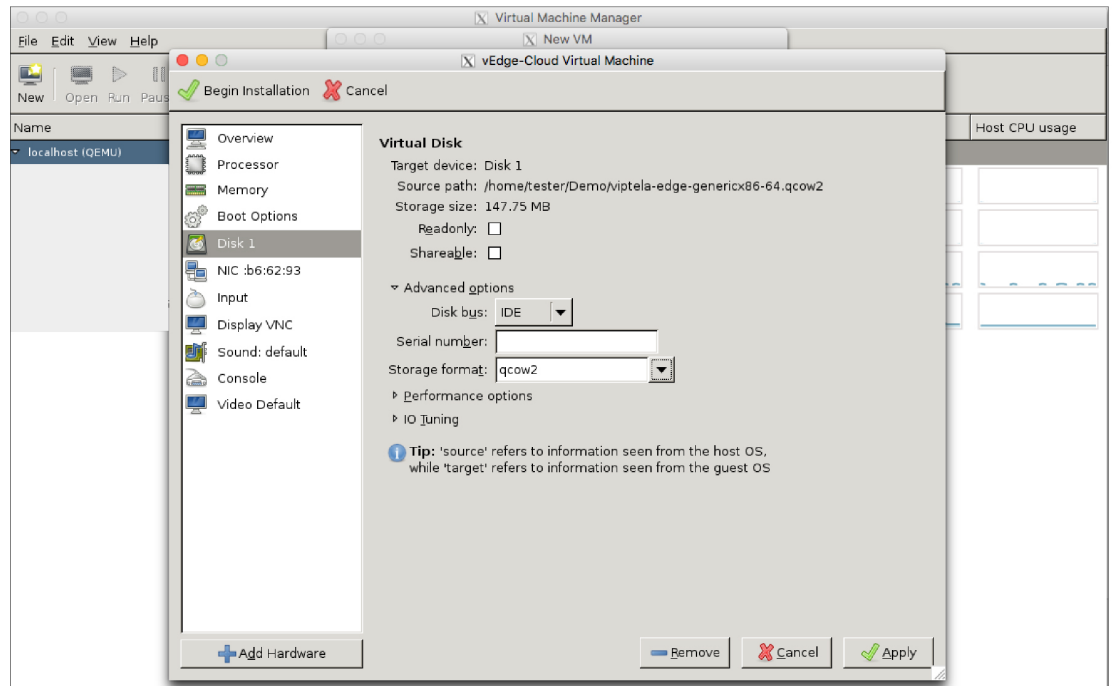
5. Specify Memory and CPU based on your network topology and the number of sites, and click **Forward**.

368251

6. Check **Customize configuration before install**. Then click **Finish**.

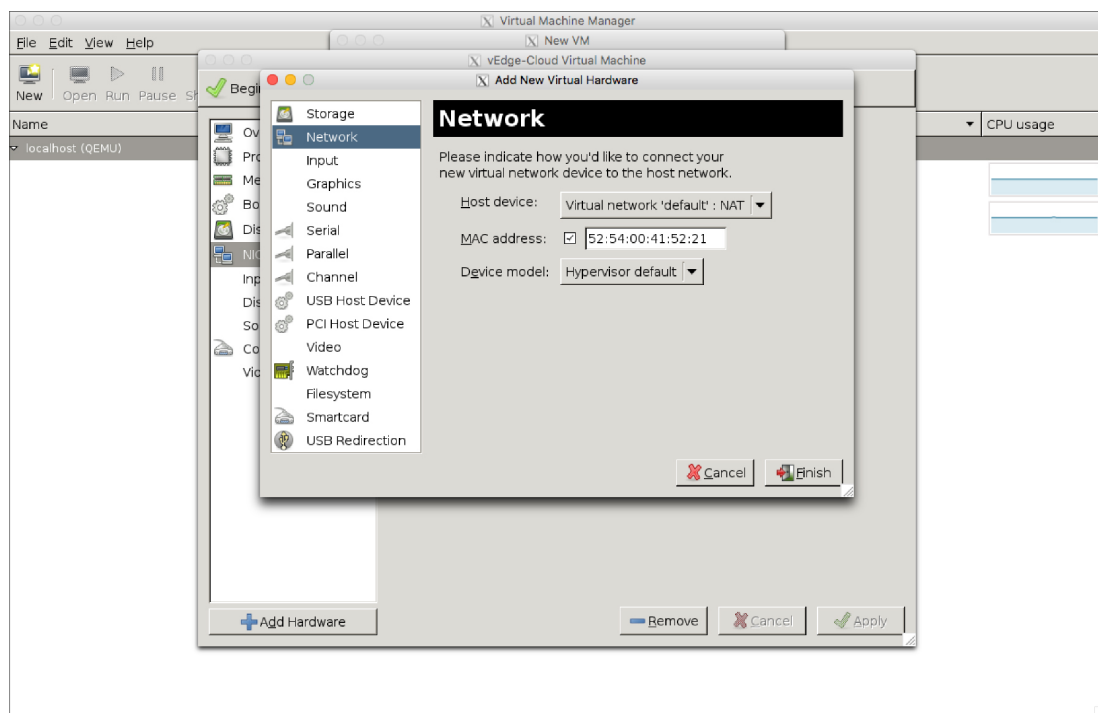
368254

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.



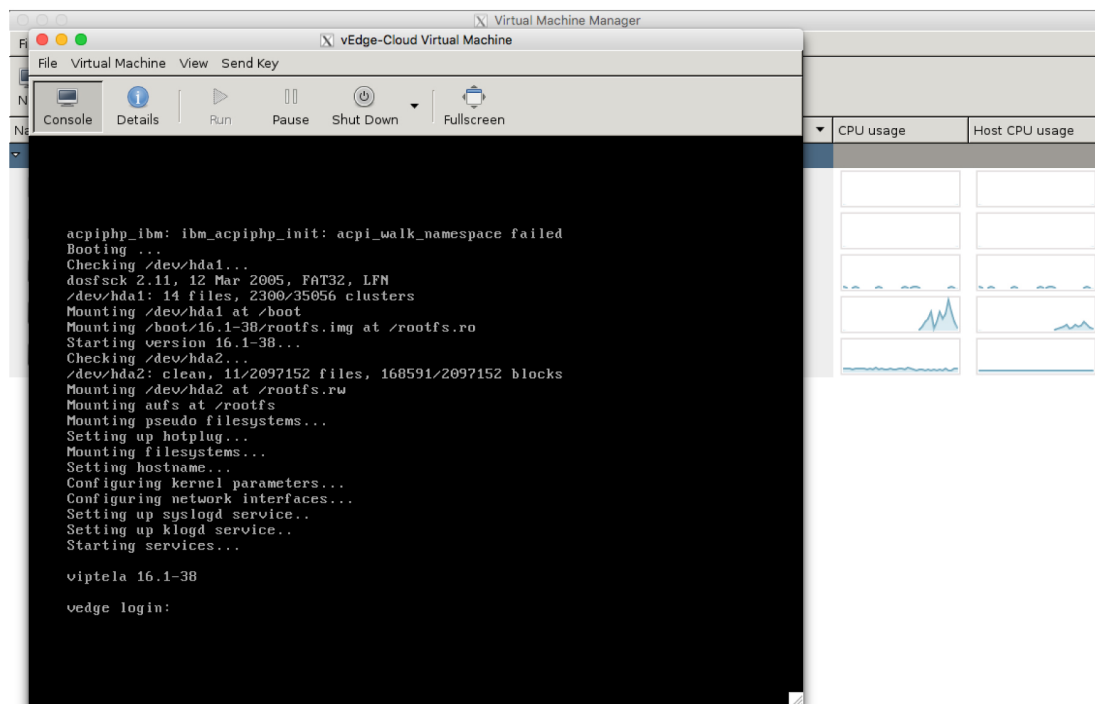
Note The software supports only VMXNET3 vNICs.

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.



12. 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 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 received 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
```



Note

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
vBond#
```

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
```

!

!

What's Next

See *Add Cisco vBond Orchestrator to the Overlay Network*.

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 5:

Feature	Template Name
Authentication, Authorization, and Accounting (AAA)	AAA
Security	Security

Feature	Template Name
System-wide parameters	System
Transport VPN (VPN 0)	VPN, with the VPN ID set to 0
Management VPN (for out-of-band management traffic)	VPN, with the VPN ID set to 512

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

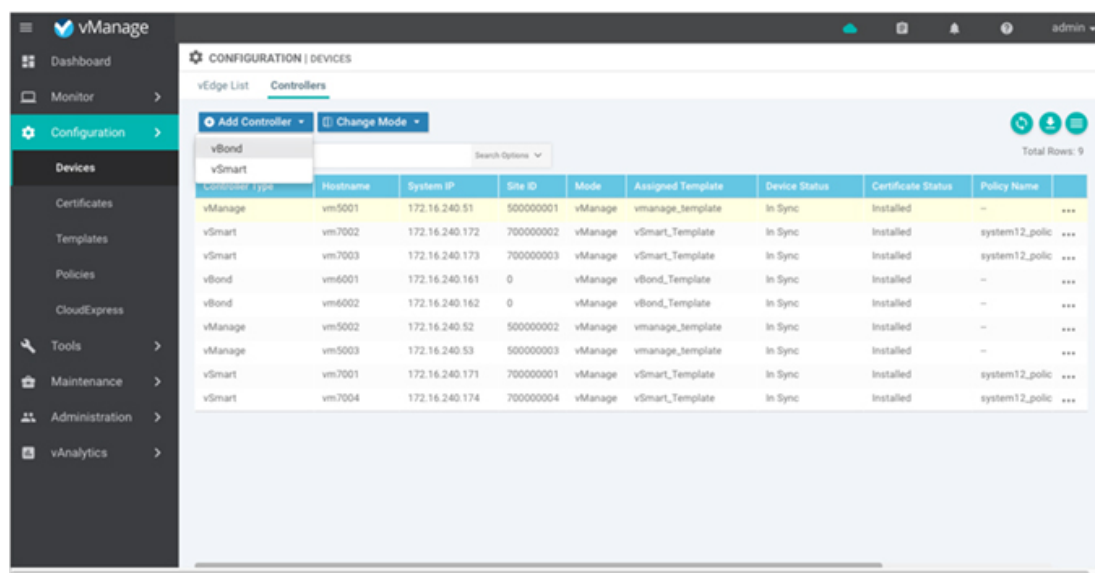
After you create a minimal configuration for Cisco vBond Orchestrator, you must add it to overlay network by making Cisco vManage aware of Cisco vBond Orchestrator. When you add Cisco vBond Orchestrator, a signed certificate is generated and is used to validate and authenticate the orchestrator.

Add Cisco vBond Orchestrator and Generate Certificate

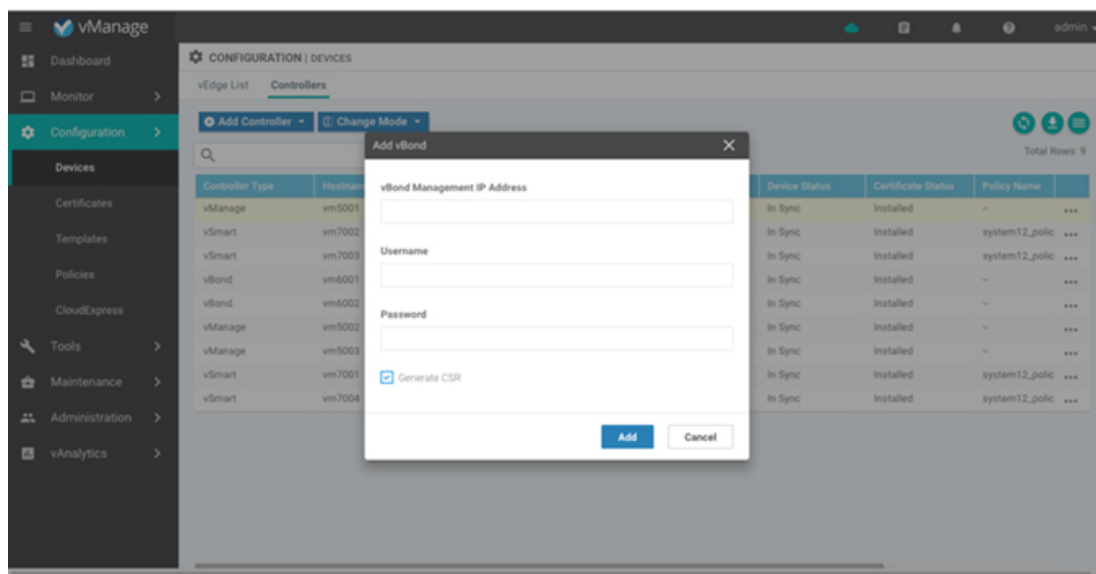
To add Cisco vBond Orchestrator to the network, automatically generate the CSR, and install the signed certificate:

1. In Cisco vManage, select **Configuration > Devices**.
2. In the **Controllers** tab, click **Add Controller** and select **vBond**.

Add Cisco vBond Orchestrator to the Overlay Network

3. In the **Add vBond** dialog box:

- Enter the vBond management IP address.
- Enter the username and password to access Cisco vBond Orchestrator.
- Select the **Generate CSR** checkbox to allow the certificate-generation process to occur automatically.
- Click **Add**.

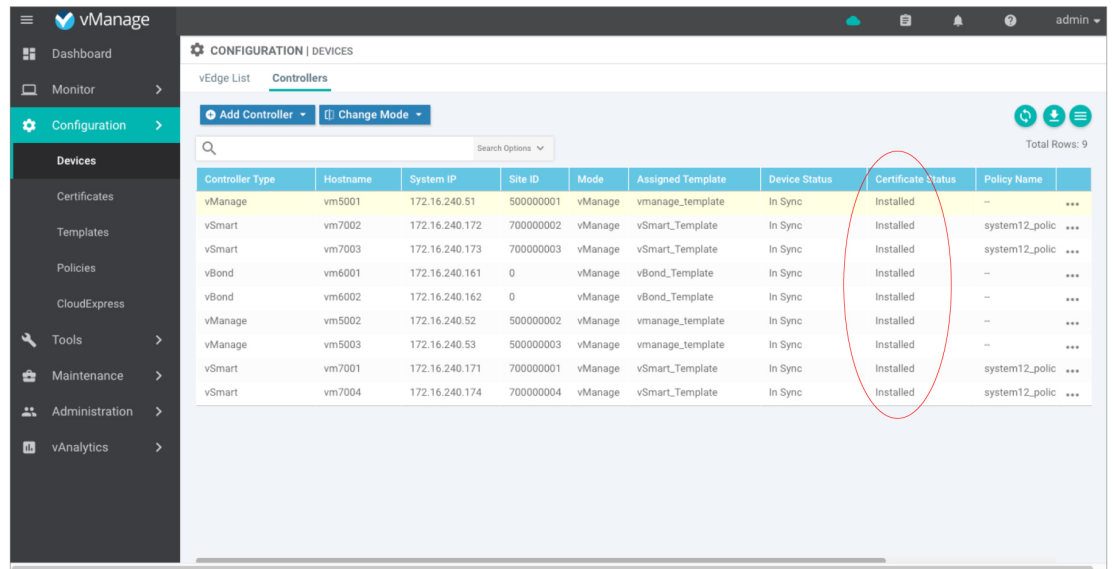


Cisco vManage generates the CSR, retrieves the generated certificate, and automatically installs it on Cisco vBond Orchestrator. The new controller device is listed in the Controller table with the controller type, hostname of the controller, IP address, site ID, and other details.

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.



The screenshot shows the Cisco vManage interface. On the left is a navigation menu with options like Dashboard, Monitor, Configuration, and Devices. The main area is titled 'CONFIGURATION | DEVICES' and shows a table of controllers. The table has columns for Controller Type, Hostname, System IP, Site ID, Mode, Assigned Template, Device Status, Certificate Status, and Policy Name. A red circle highlights the 'Certificate Status' column, showing that all devices have a status of 'Installed'.

Controller Type	Hostname	System IP	Site ID	Mode	Assigned Template	Device Status	Certificate Status	Policy Name
vManage	vm5001	172.16.240.51	500000001	vManage	vmanage_template	In Sync	Installed	---
vSmart	vm7002	172.16.240.172	700000002	vManage	vSmart_Template	In Sync	Installed	system12_polic
vSmart	vm7003	172.16.240.173	700000003	vManage	vSmart_Template	In Sync	Installed	system12_polic
vBond	vm6001	172.16.240.161	0	vManage	vBond_Template	In Sync	Installed	---
vBond	vm6002	172.16.240.162	0	vManage	vBond_Template	In Sync	Installed	---
vManage	vm5002	172.16.240.52	500000002	vManage	vmanage_template	In Sync	Installed	---
vManage	vm5003	172.16.240.53	500000003	vManage	vmanage_template	In Sync	Installed	---
vSmart	vm7001	172.16.240.171	700000001	vManage	vSmart_Template	In Sync	Installed	system12_polic
vSmart	vm7004	172.16.240.174	700000004	vManage	vSmart_Template	In Sync	Installed	system12_polic

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 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 must contain 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)

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:

```
vBond# request device-upload chassis-file JSON-file-name
```

Here is an example of a JSON file:


```

{
    "version": "1.1",
    "organization": "vIPtela Inc Regression",
    "overlay": "vIPtela Inc Regression",
    "root_cert_bundle": "-----BEGIN CERTIFICATE-----
<certificate>
-----END CERTIFICATE-----\n-----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"
}

```

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 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-ge)# ip address prefix/length
vBond(config-ge)# 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
```

file-path can be one of the following:

- *filename*—Path to a file in your home directory on the local Cisco vEdge device.
- **ftp:** *file-path*—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:** *file-path*—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.

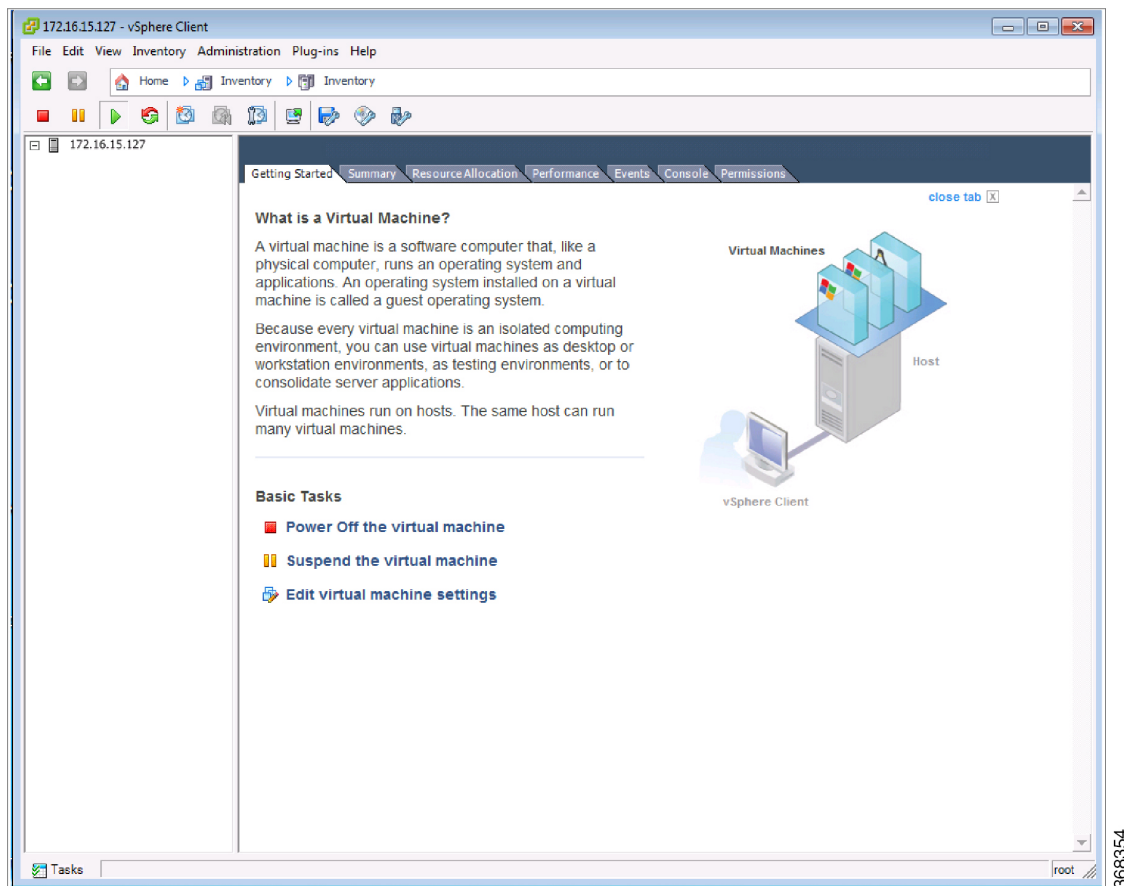
The details of each step are provided below.

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.

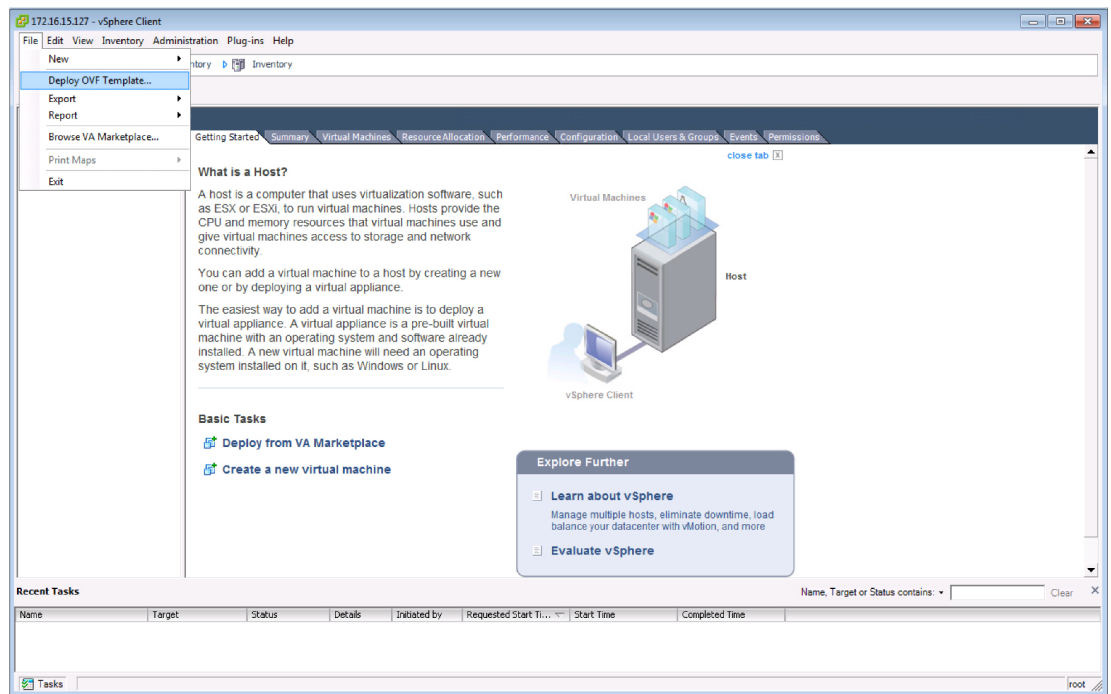
Launch vSphere Client and Create a vSmart VM Instance

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.

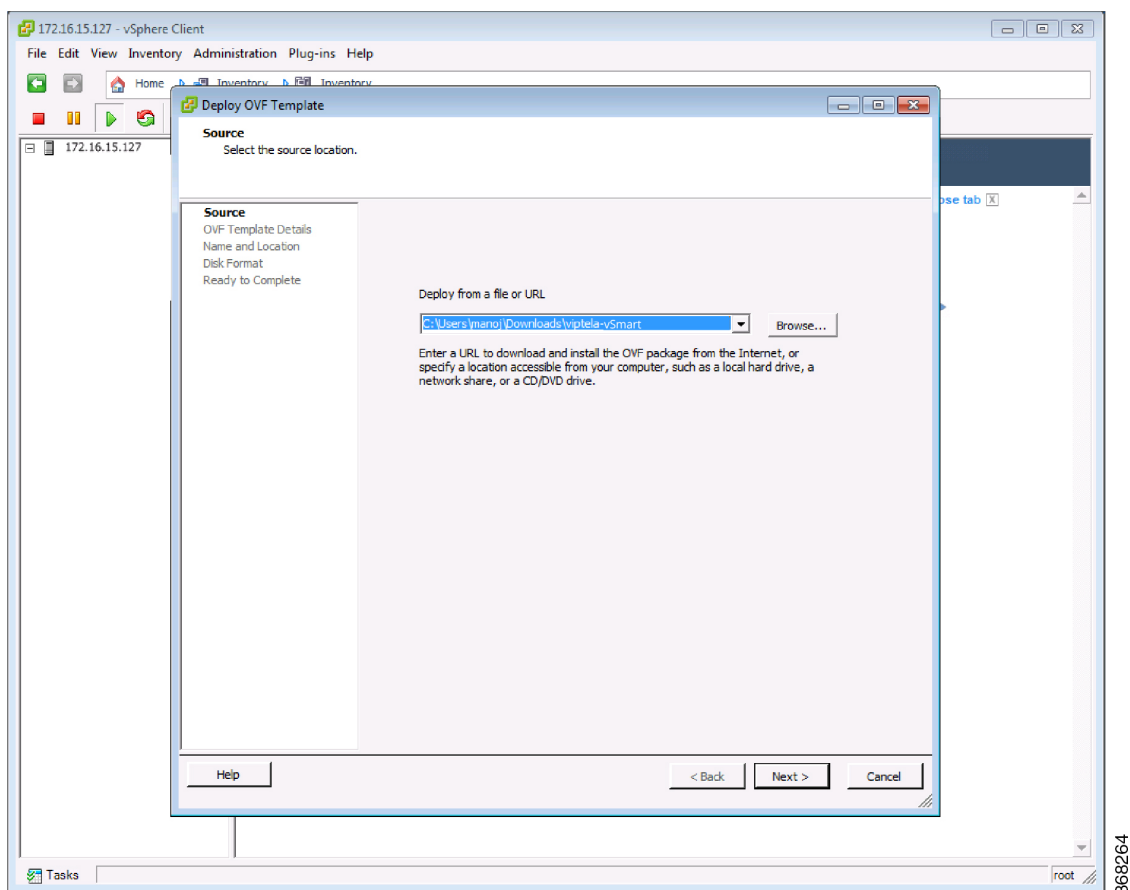
The system displays the ESXi screen.



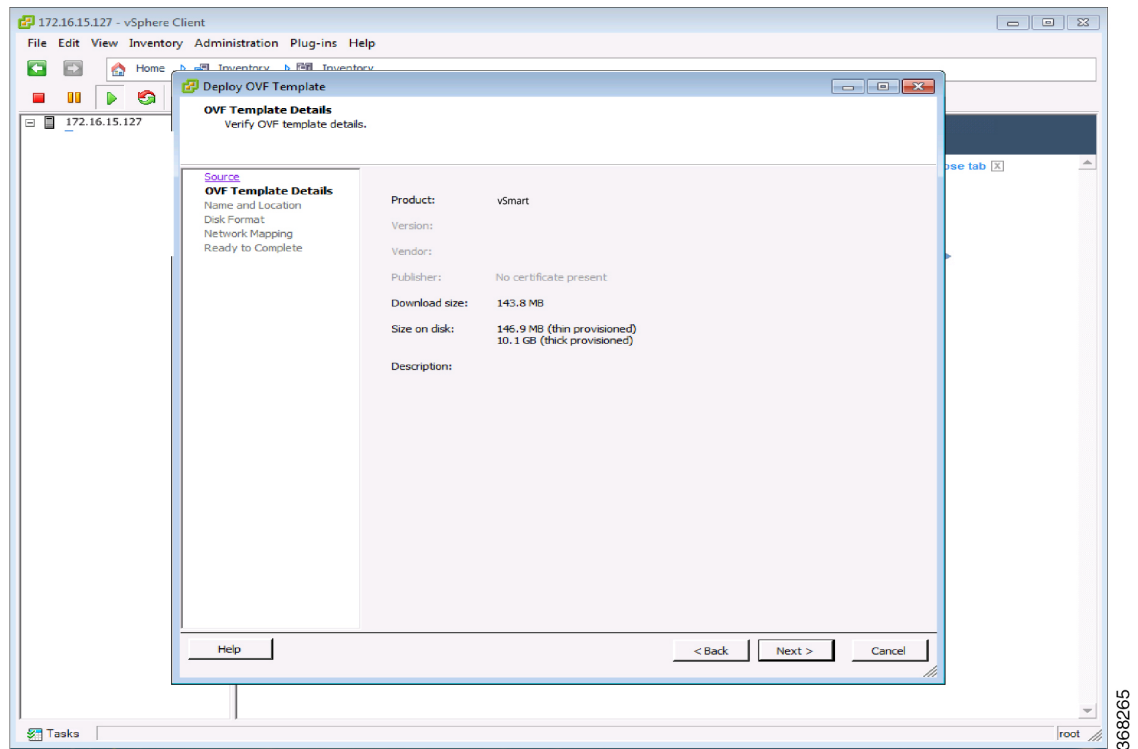
2. Click **File > Deploy OVF Template** to deploy the virtual machine.



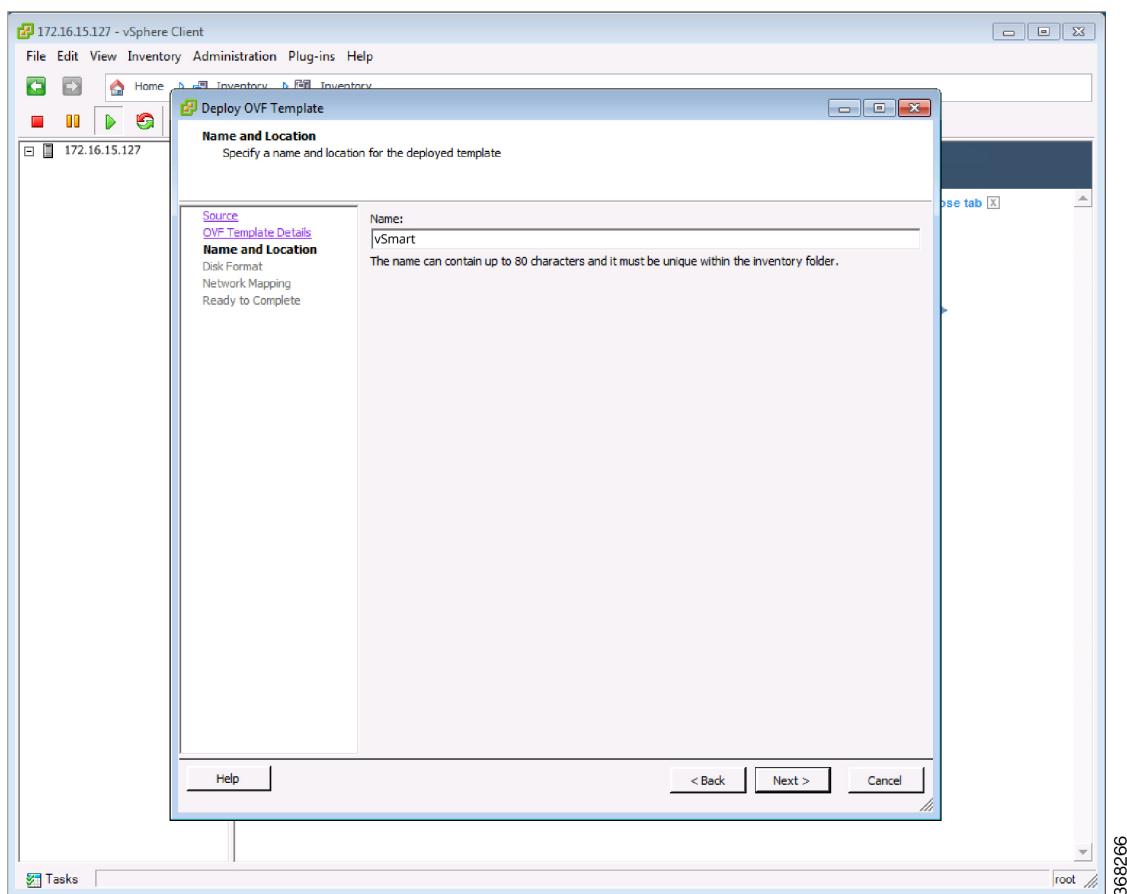
3. In the Deploy OVF Template screen, enter the location to install and download the OVF package. This package is the vsmart.ova file that you downloaded from Cisco. Then click **Next**.



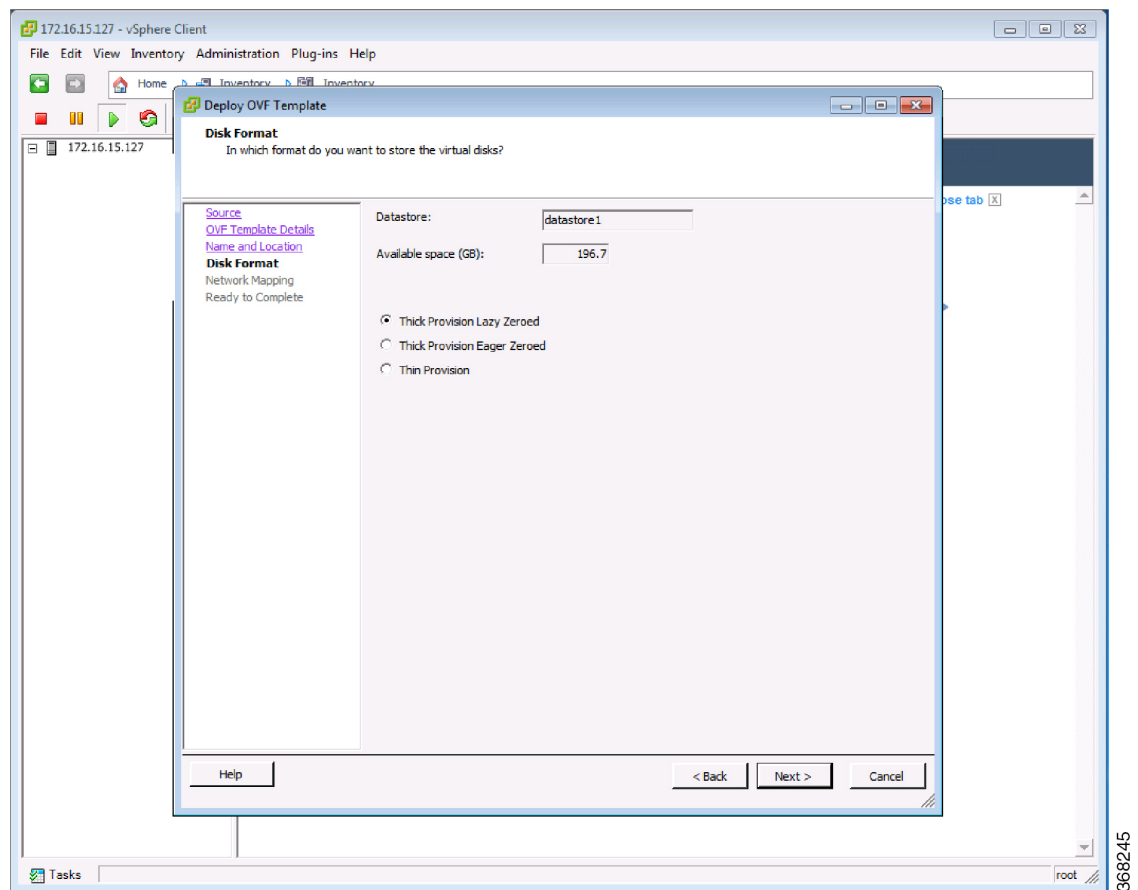
4. Click **Next** to verify OVF template details.



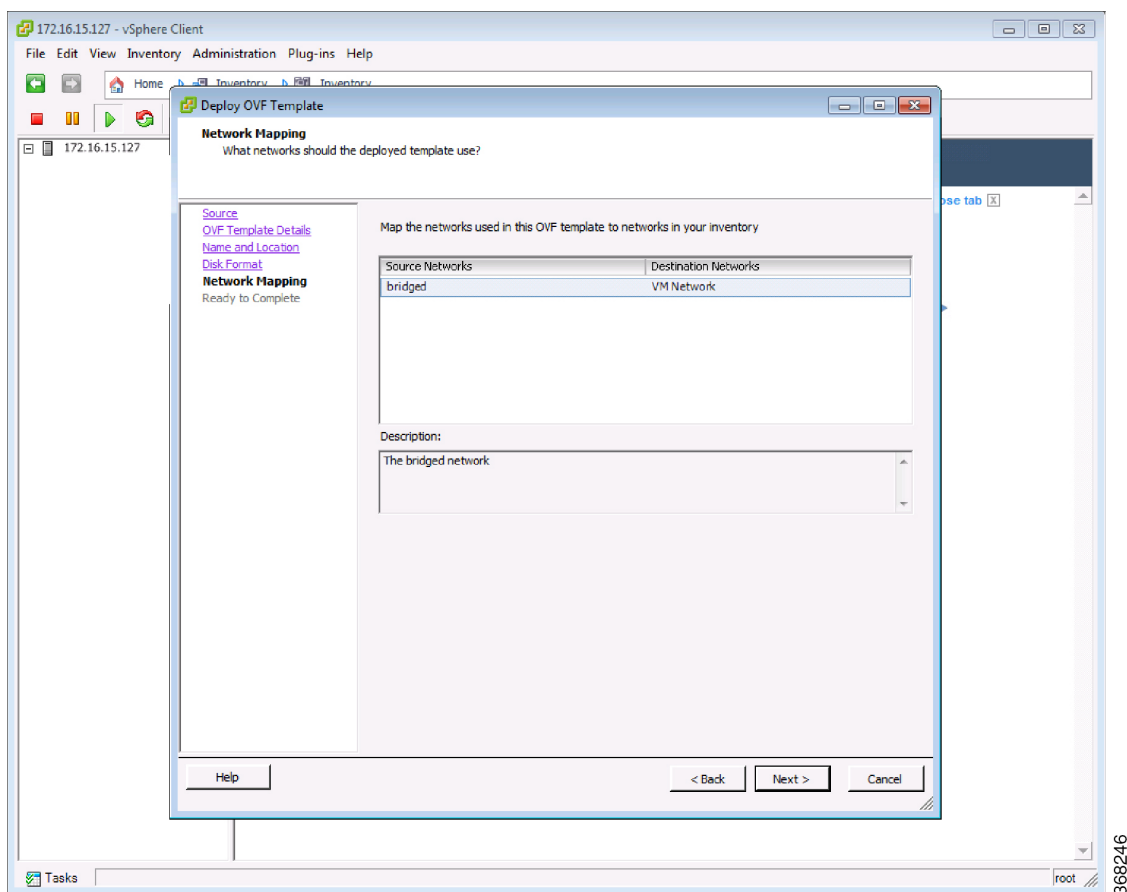
5. Enter a name for the deployed template and click **Next**. The figure below specifies a name for the vSmart instance.



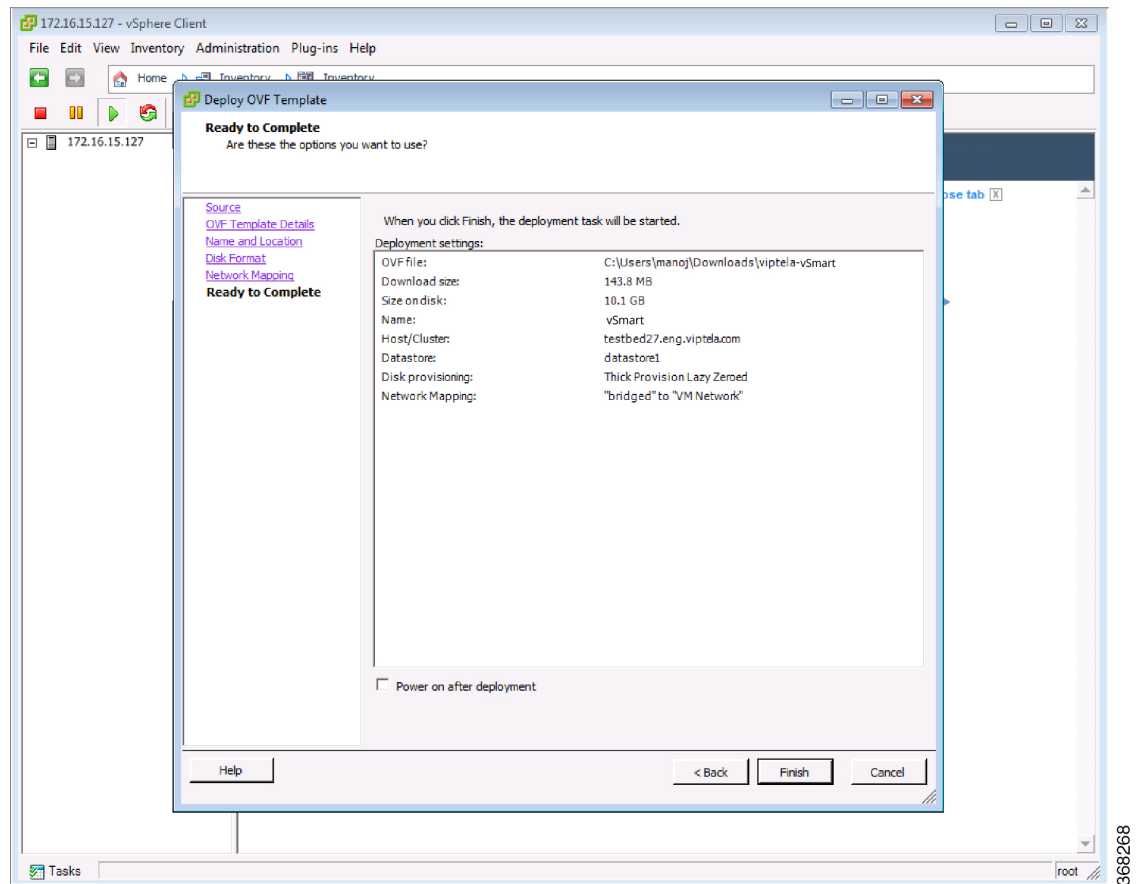
6. Click **Next** to accept the default format for the virtual disks.



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.

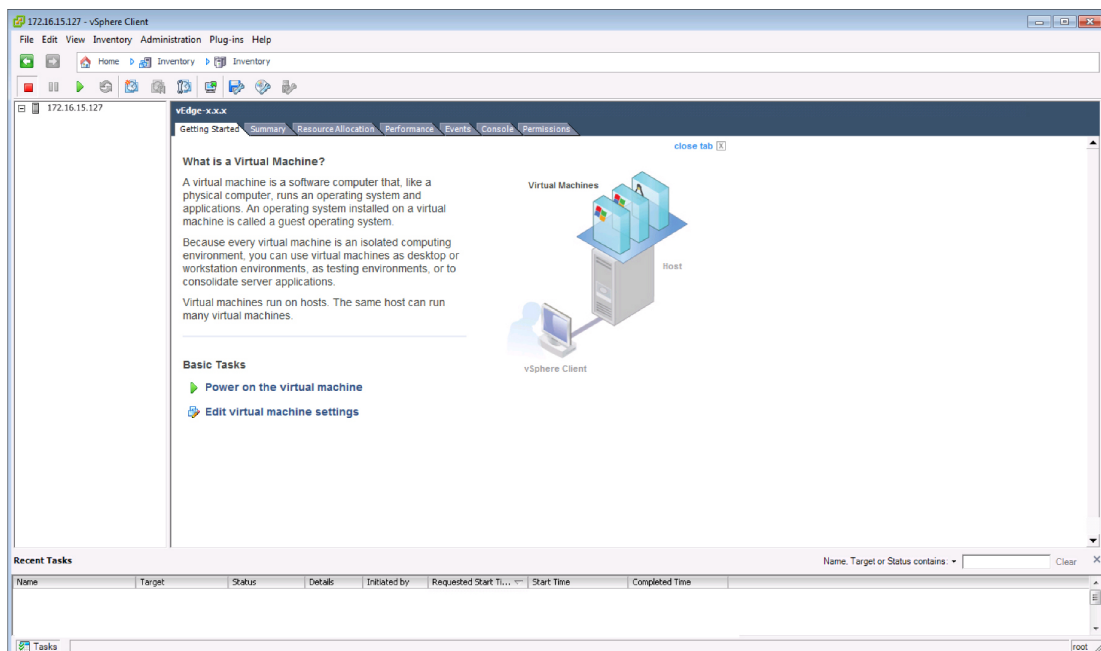


The system has successfully created the VM instance with the parameters you just defined and displays the vSphere Client screen with the **Getting Started** tab selected. By default, this includes one vNIC. This vNIC is used for the tunnel interface.

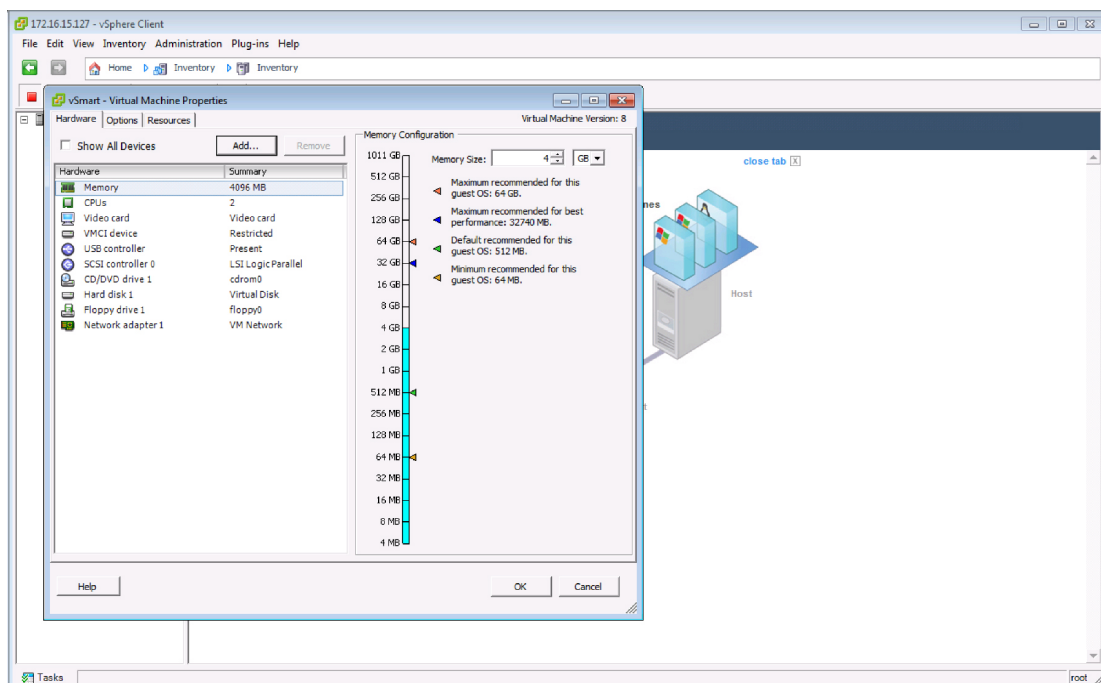
Add a vNIC for the Management Interface

1. In the left navigation bar of the vSphere Client, select the vManage VM instance you just created, and click **Edit virtual machine settings**.

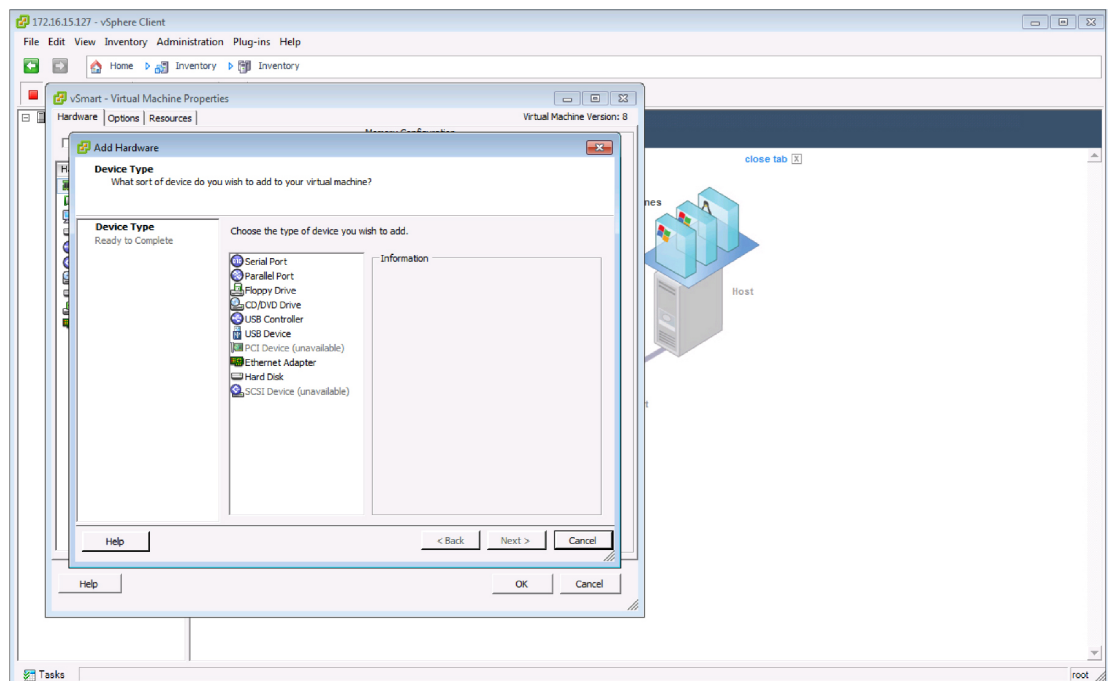
Create vSmart VM Instance on ESXi



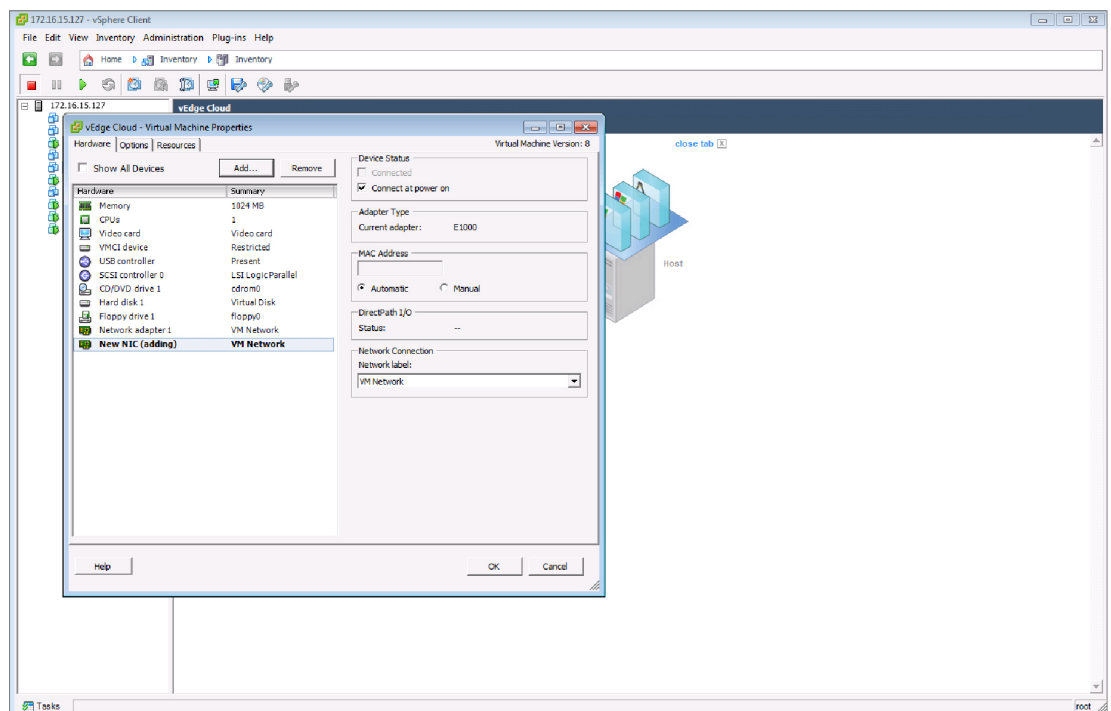
- In the vManage – Virtual Machine Properties screen, click **Add** to add a new vNIC for the management interface. Then click **OK**.



- Click **Ethernet Adapter** for the type of device you wish to add. Then click **Next**.

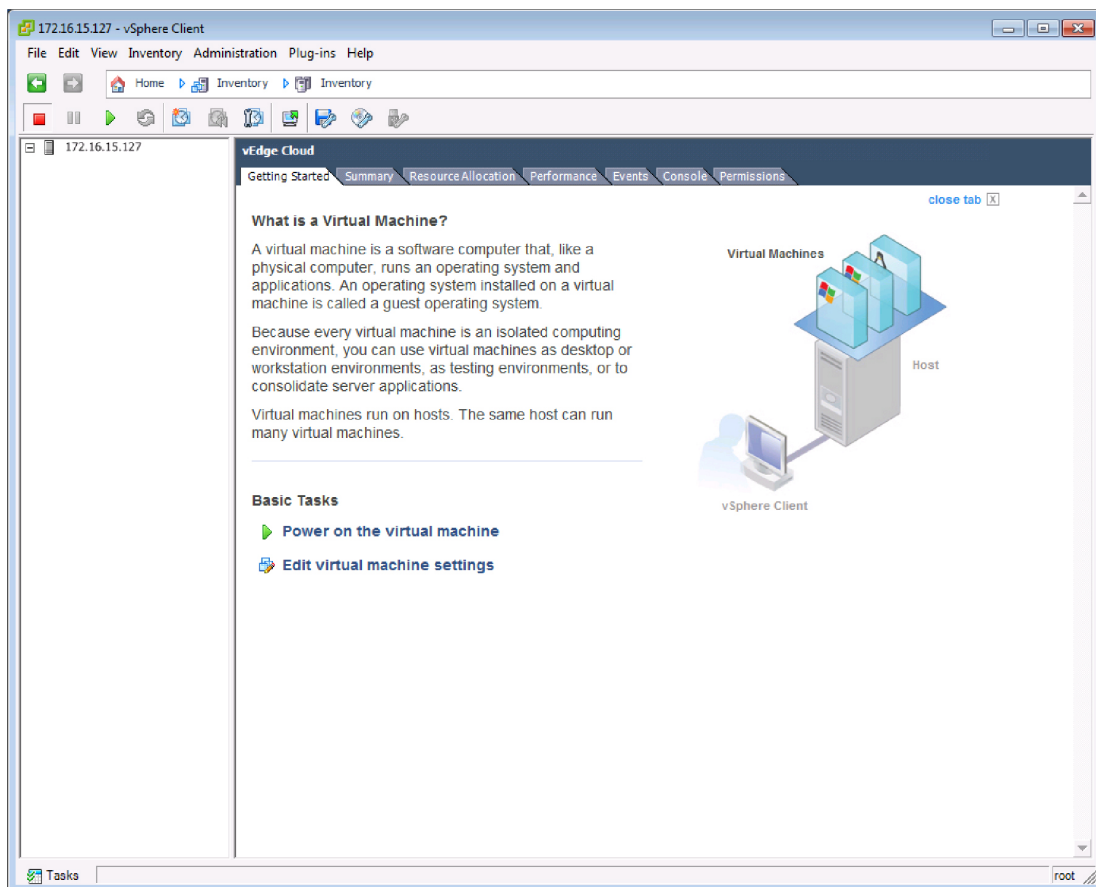


4. In the **Adapter Type** drop-down, select VMXNET3 for the vNIC to add. Then click **Next**.
5. In the Ready to Complete screen, click **Finish**.
6. The vManage – Virtual Machine Properties screen opens showing that the new vNIC is being added. Click **OK** to return to the vSphere Client screen.

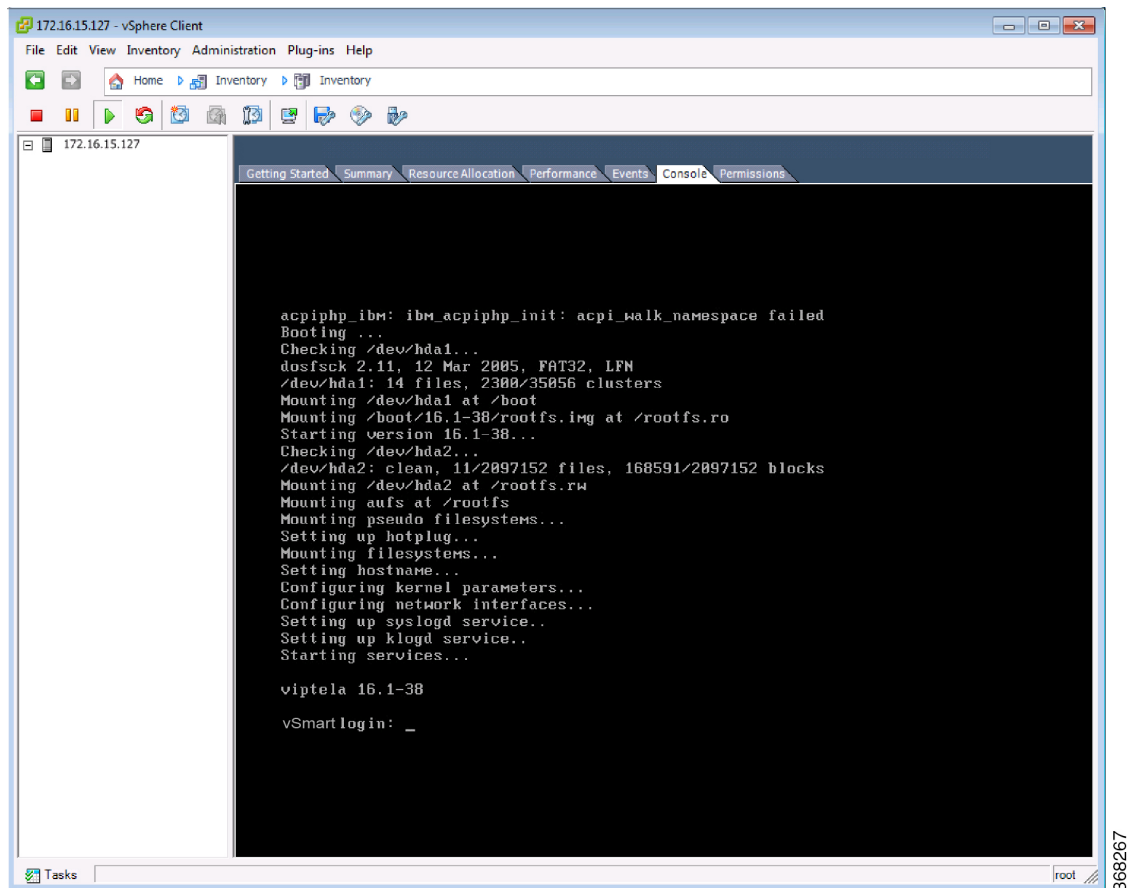


Start the vSmart VM Instance and Connect to the Console

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.



- 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*.

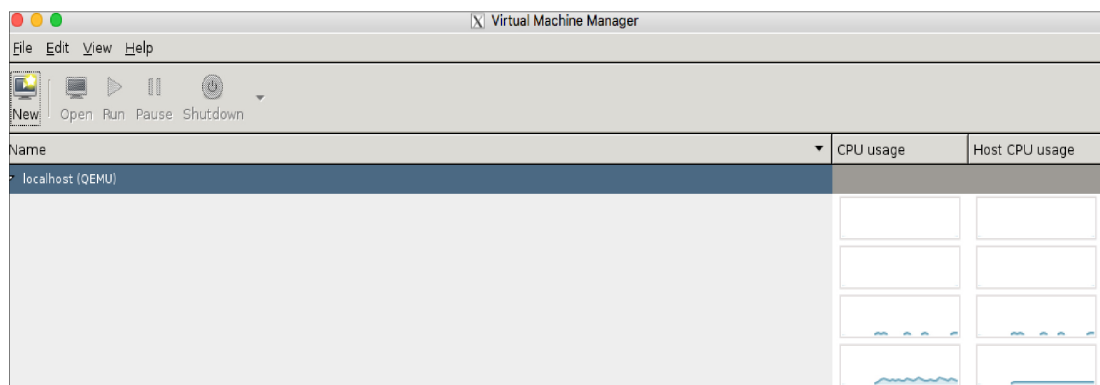
Create vSmart VM Instance on KVM

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*.

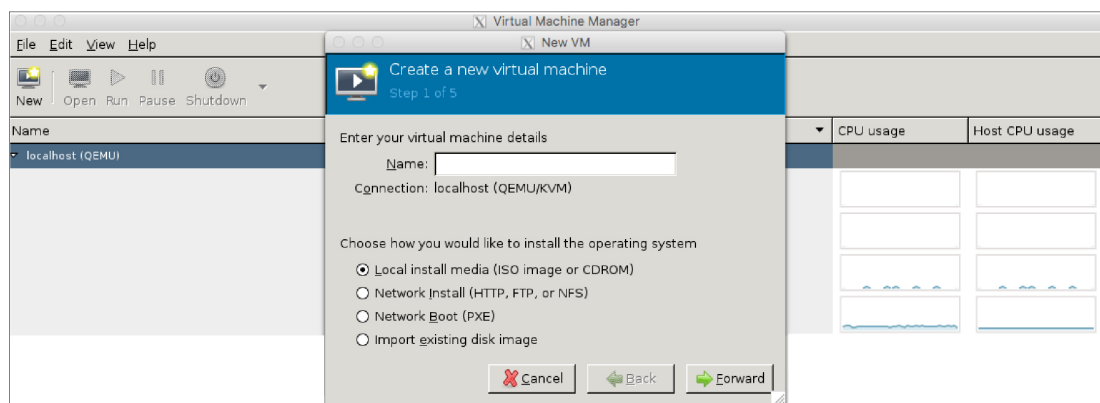
To create a vSmart VM instance on the KVM hypervisor:

- Launch the Virtual Machine Manager (virt-manager) client application. The system displays the Virtual Machine Manager screen.



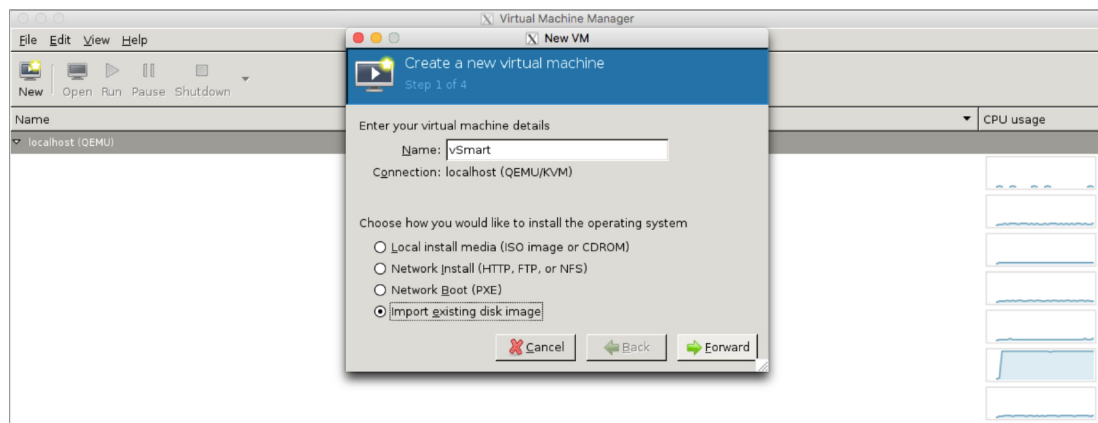
368248

2. Click **New** to deploy the virtual machine. The system opens the Create a new virtual machine screen.



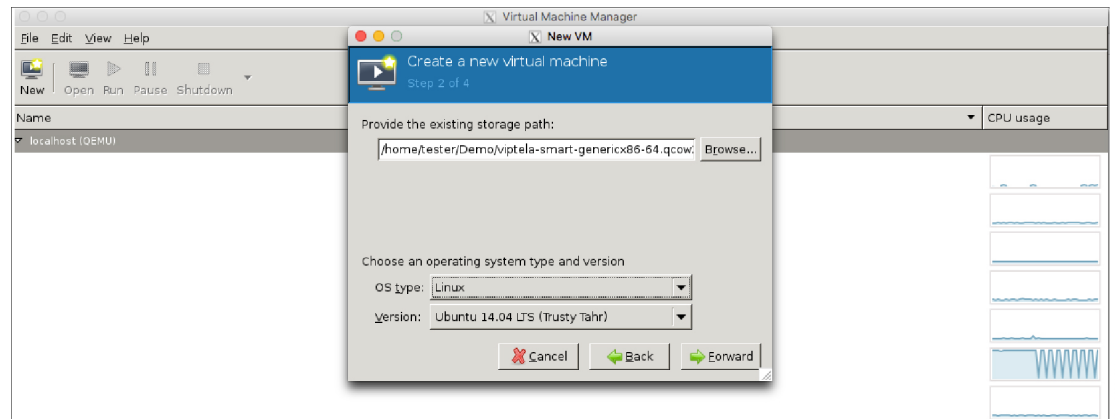
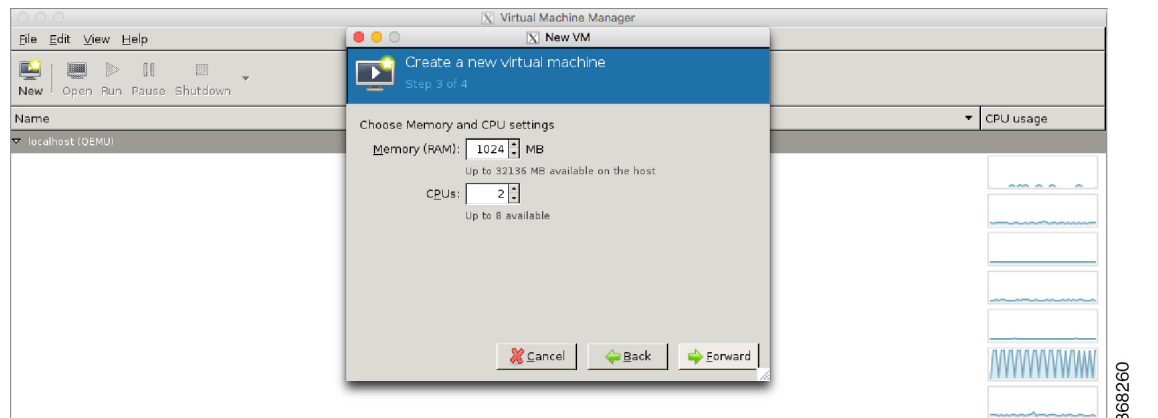
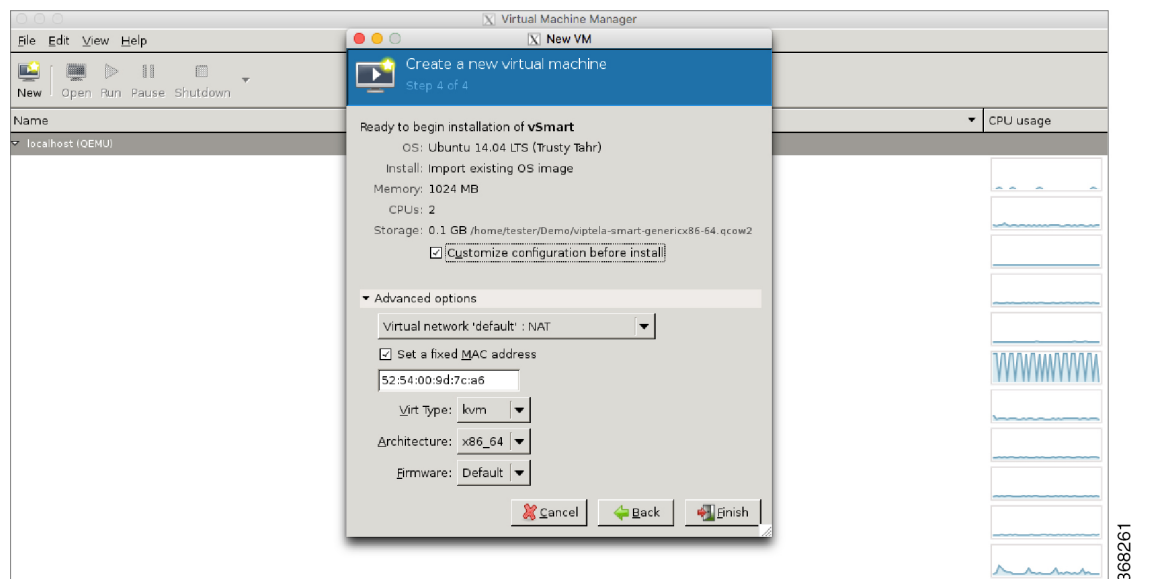
368249

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**.

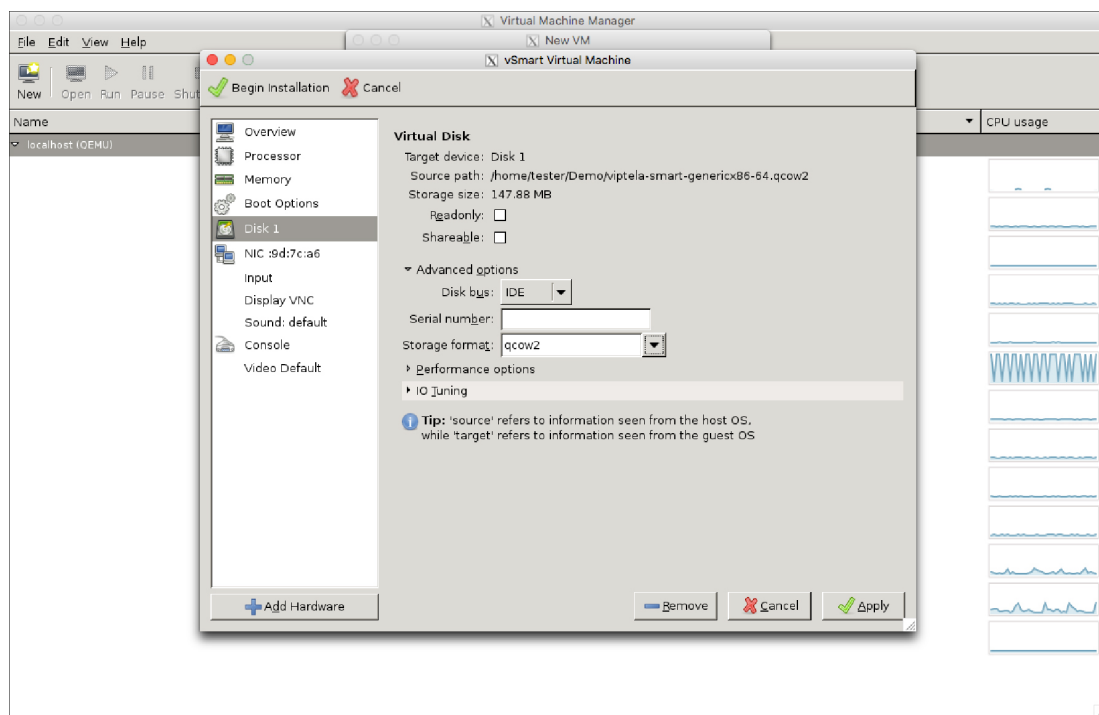


368258

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.

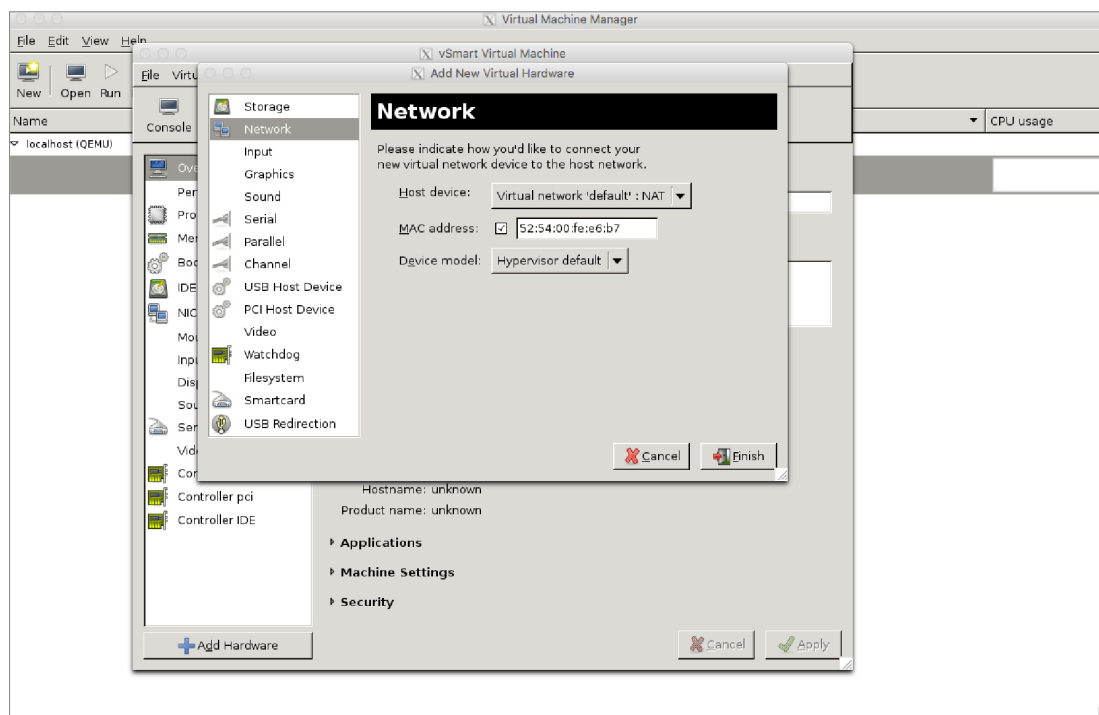
c. Click **Forward**.5. Specify Memory and CPU based on your network topology and the number of sites, and click **Forward**.6. Select **Customize** configuration before install. Then click **Finish**.

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.

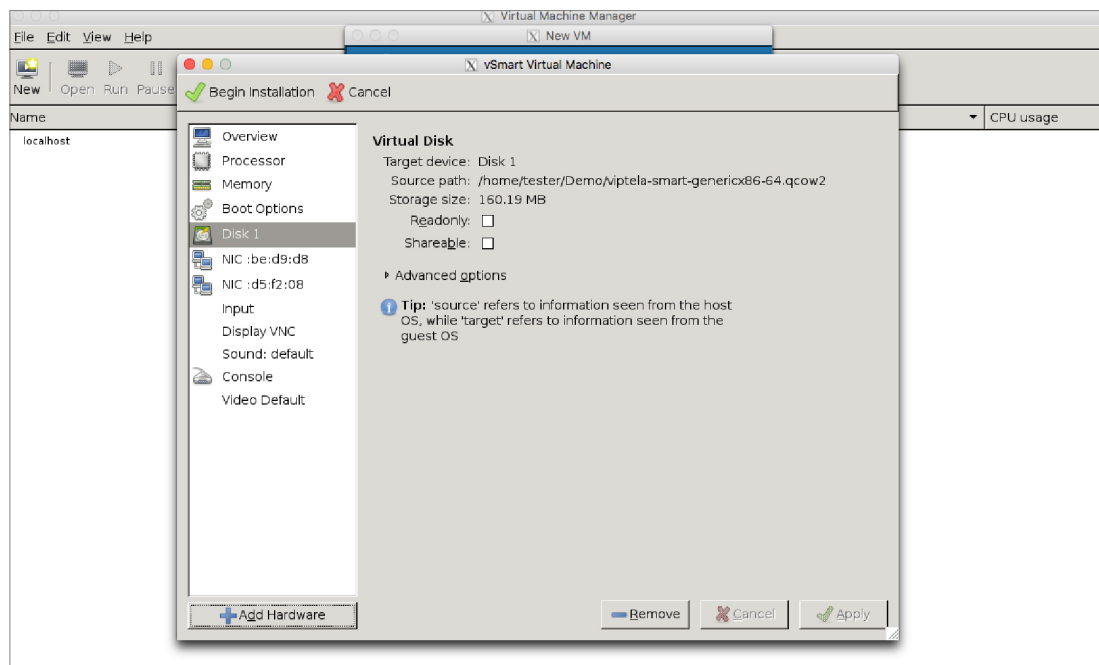


Note The software supports only VMXNET3 vNICs.

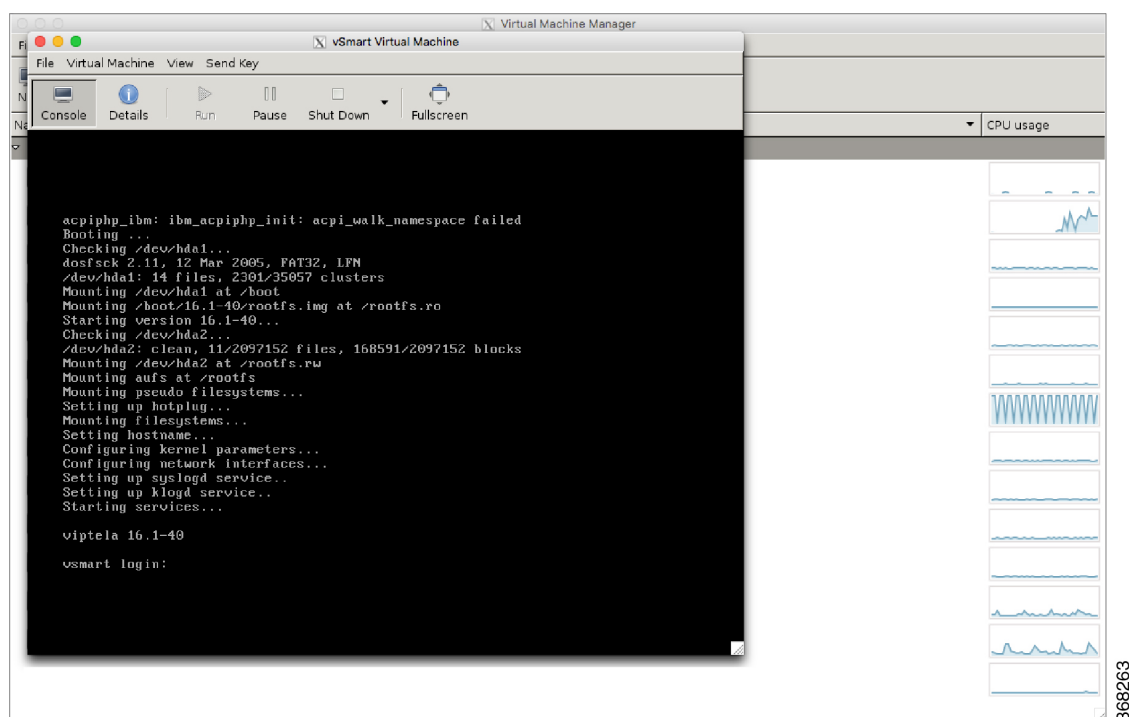
8. In the vSmart Virtual Machine screen, click **Add Hardware** to add a second vNIC for the management interface.
9. In the Add New Virtual Hardware screen, click **Network**.
 - a. In the **Host Device** field, select an appropriate host device.
 - b. Click **Finish**.



The newly created vNIC is listed in the left pane. This vNIC is used for the management interface.



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.



Note 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 received 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:

```
vSmart# show running-config
```

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.

```
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
```

```

        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
    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 6:

Feature	Template Name
Authentication, Authorization, and Accounting (AAA)	AAA
Overlay Management Protocol (OMP)	OMP
Security	Security
System-wide parameters	System
Transport VPN (VPN 0)	VPN with the VPN ID set to 0
Management VPN (for out-of-band management traffic)	VPN with the VPN ID set to 512

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

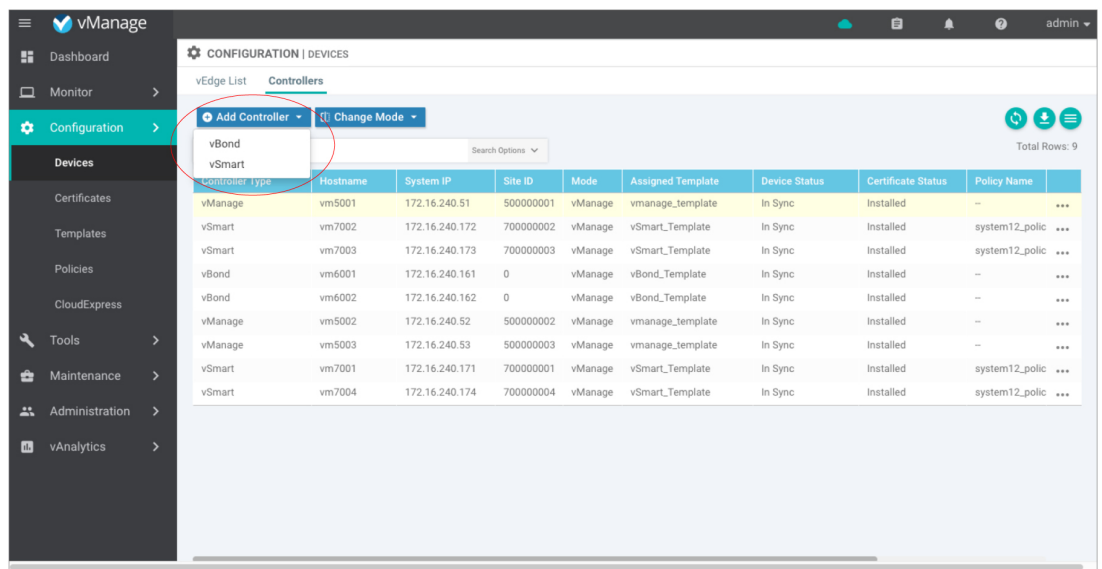
After you create a minimal configuration for Cisco vSmart Controller, you must add it to an overlay network by making Cisco vManage aware of the controller. When you add Cisco vSmart Controller, a signed certificate is generated and is used to validate and authenticate the controller.

Cisco vManage can support up to 20 Cisco vSmart Controllers in the network.

Add a Cisco vSmart Controller and Generate Certificate

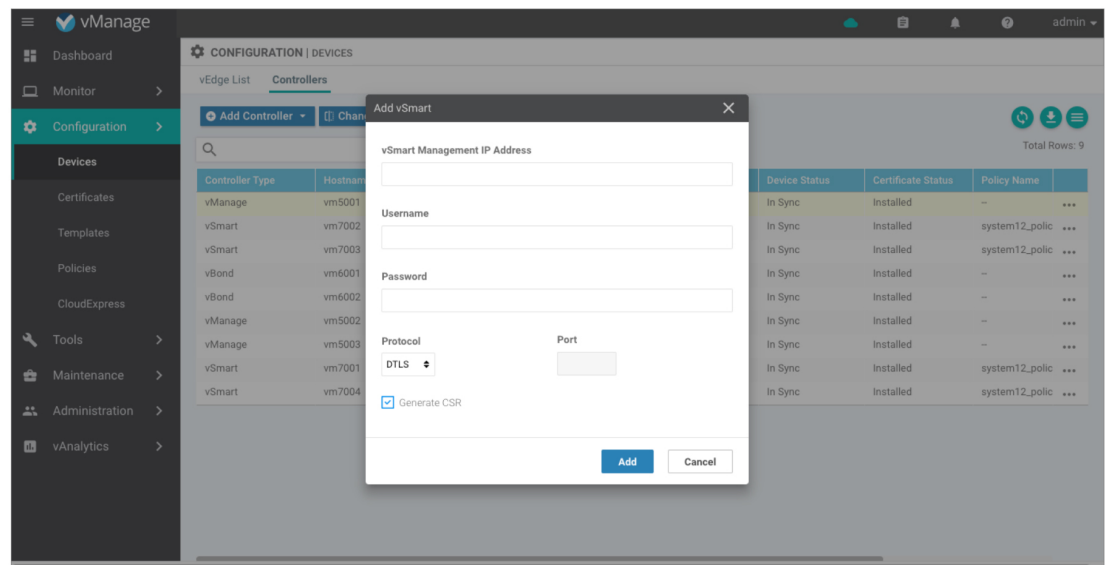
To add a Cisco vSmart Controller to the network, automatically generate the CSR, and install the signed certificate:

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:

- Enter the system IP address of Cisco vSmart Controller.
- Enter the username and password to access Cisco vSmart Controller.
- Select the protocol to use for control-plane connections. The default is DTLS.
- If you select TLS, enter the port number to use for TLS connections. The default is 23456.
- Select the **Generate CSR** check-box to allow the certificate-generation process to occur automatically.
- Click **Add**.

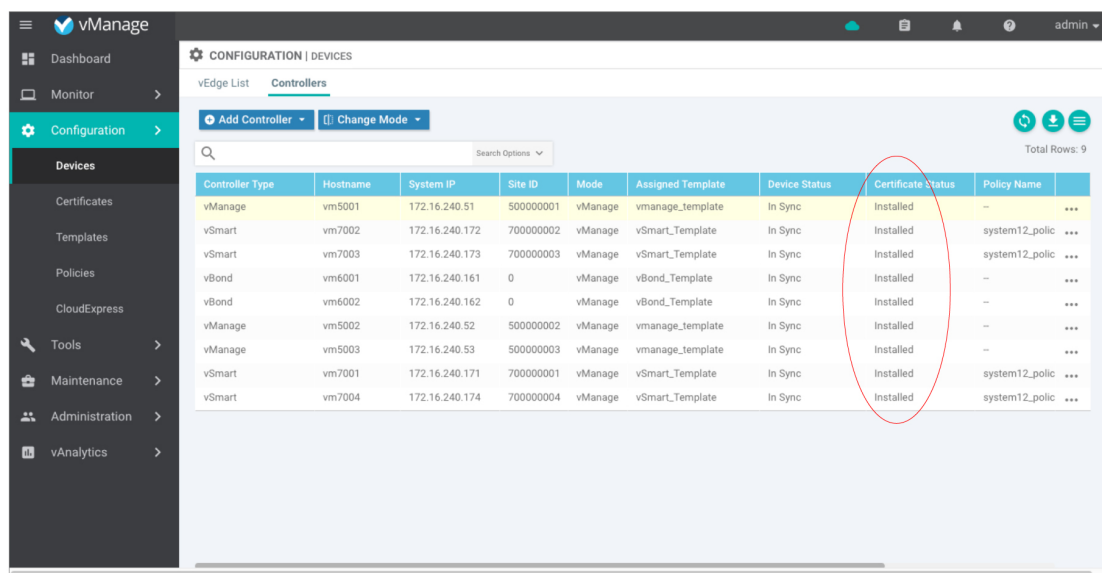


Cisco vManage automatically generates the CSR, retrieves the generated certificate, and installs it on Cisco vSmart Controller. The new controller is listed in the Controller table with the controller type, hostname of the controller, IP address, site ID, and other details.

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.



Controller Type	Hostname	System IP	Site ID	Mode	Assigned Template	Device Status	Certificate Status	Policy Name
vManage	vm5001	172.16.240.51	500000001	vManage	vmanage_template	In Sync	Installed	---
vSmart	vm7002	172.16.240.172	700000002	vManage	vSmart_Template	In Sync	Installed	system12_polic
vSmart	vm7003	172.16.240.173	700000003	vManage	vSmart_Template	In Sync	Installed	system12_polic
vBond	vm6001	172.16.240.161	0	vManage	vBond_Template	In Sync	Installed	---
vBond	vm6002	172.16.240.162	0	vManage	vBond_Template	In Sync	Installed	---
vManage	vm5002	172.16.240.52	500000002	vManage	vmanage_template	In Sync	Installed	---
vManage	vm5003	172.16.240.53	500000003	vManage	vmanage_template	In Sync	Installed	---
vSmart	vm7001	172.16.240.171	700000001	vManage	vSmart_Template	In Sync	Installed	system12_polic
vSmart	vm7004	172.16.240.174	700000004	vManage	vSmart_Template	In Sync	Installed	system12_polic



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 7: Feature History

Feature Name	Release Information	Description
Support for Deploying Cisco Catalyst 8000V Instances for Supported Cloud Services Provider Platforms	Cisco IOS XE Release 17.4.1a	Starting from this release, Cisco Catalyst 8000V instances can be deployed on Cloud Services Provider portals such as Microsoft Azure and Amazon Web Services.

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](#)

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 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.

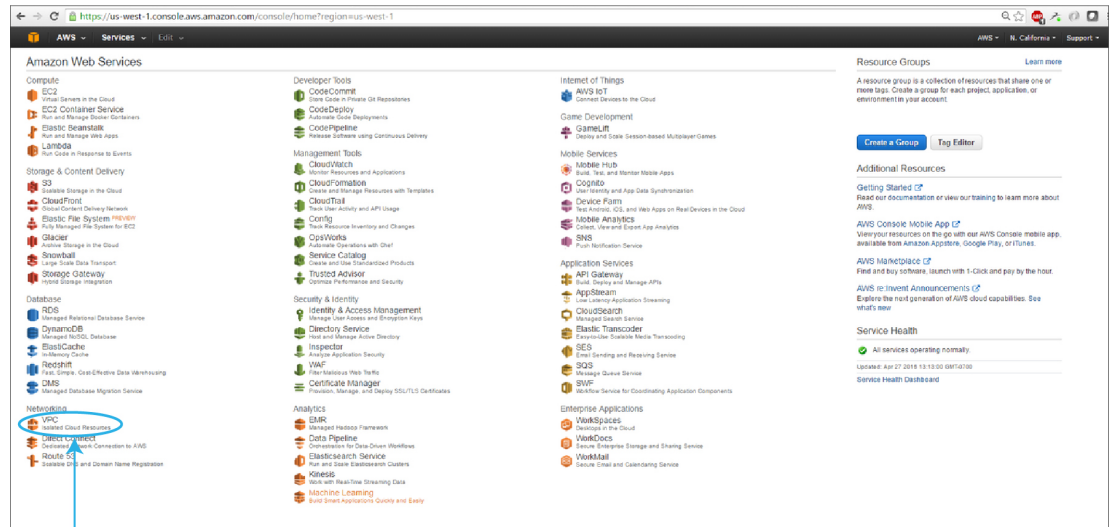
To start a vEdge Cloud router on Amazon AWS:

1. Create a VPC.
2. Set up the vEdge Cloud router VM instance.
3. Define additional interfaces.

Create a VPC

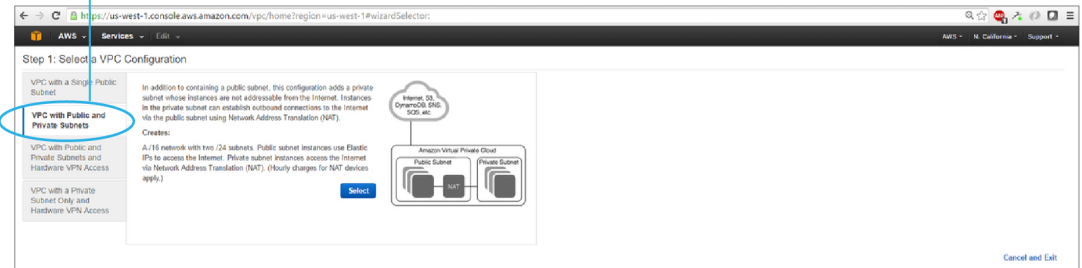
Plan your network address blocks carefully before creating the VPC. Once you create a VPC, you cannot modify it. To make any changes to the network addressing, you must delete the VPC and create a new one.

1. Log in to AWS. In the Networking section of the AWS home page, click **VPC**.



1. On the screen that opens, click **Start VPC wizard**.
2. On the Select a VPC Configuration screen, select **VPC with Public and Private Subnets**.

VPC with Public and Private Subnets



1. 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**.

Create vEdge Cloud router VM Instance on AWS

Create VPC

Step 2: VPC with Public and Private Subnets

IP CIDR block: 10.0.0.0/16 (65531 IP addresses available)

VPC name:

Public subnet: 10.0.0.0/24 (251 IP addresses available)

Availability Zone: No Preference

Public subnet name: Public subnet

Private subnet: 10.0.1.0/24 (251 IP addresses available)

Availability Zone: No Preference

Private subnet name: Private subnet

You can add more subnets after AWS creates the VPC.

Specify the details of your NAT gateway (NAT gateway rules apply).

Elastic IP Allocation ID:

Add endpoints for S3 to your subnets

Subnet: None

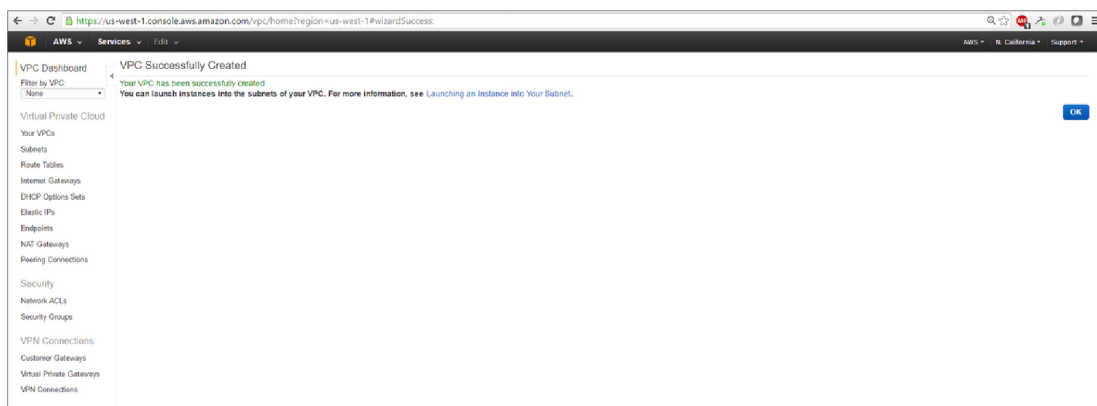
Enable DNS hostnames: Yes No

Hardware tenancy: Default

Cancel and Exit Create VPC

368357

Wait a few minutes until the VPC Dashboard displays the VPC Successfully Created message.



368358

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.

VPC Dashboard

Create Subnet Subnet Actions

Filter by VPC: vpc-b07bda8b (10.0.0.0/16)

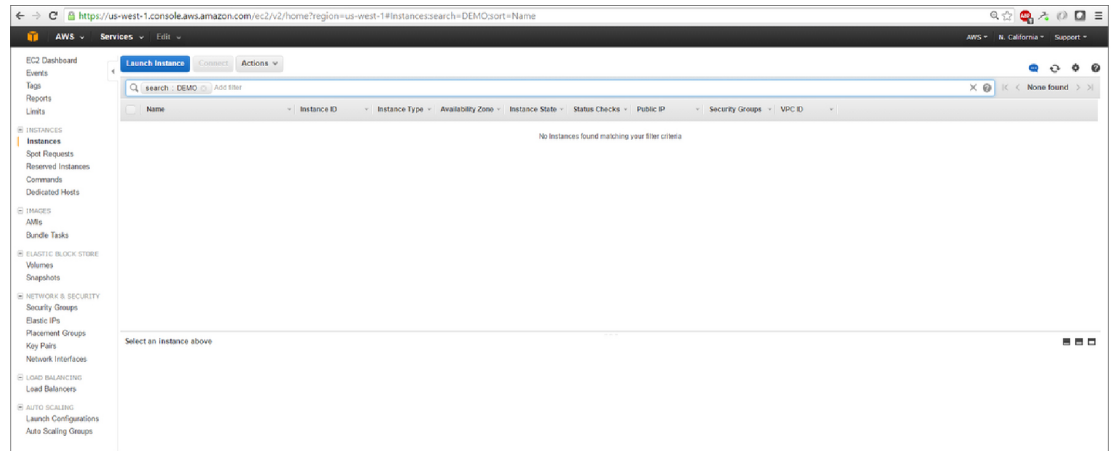
Search Subnets and their pe

Name	Subnet ID	State	VPC	CIDR	Available IPs	Availability Zone	Route Table	Network ACL	Default Subnet	Auto-assign Public IP
PUBLIC_WAN	subnet-77a1e912	available	vpc-b07bda8b (10.0.0.0/16) DE	10.0.0.0/24	250	us-west-1a	rt-c5c8a5d0	acl-95a8a8d0	No	No
PRIVATE_LAN	subnet-7ae1d911	available	vpc-b07bda8b (10.0.0.0/16) DE	10.0.1.0/24	251	us-west-1a	rt-ba6cd59f	acl-95a8a8d0	No	No

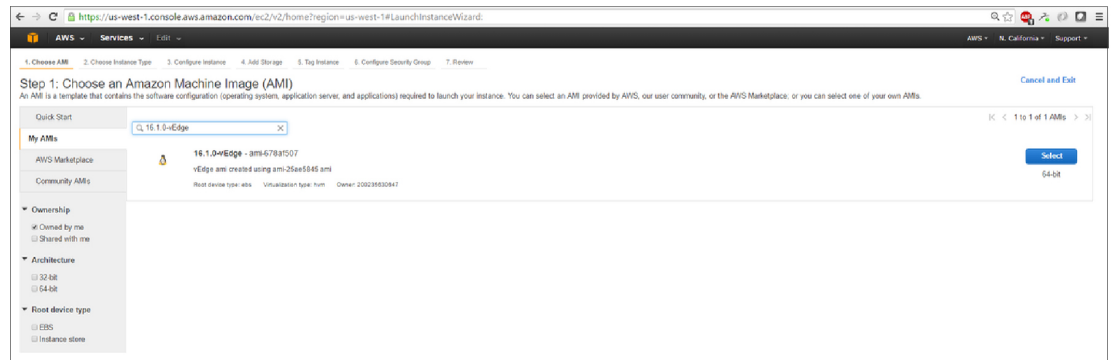
368359

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**.



1. 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 8: Table 1: EC2 Instance Types that Support the vEdge Cloud router

	vCPU	Memory (GB)	Instance Storage (GB)
General Purpose — Current Generation			
m4.large	2	8	EBS only
m4.xlarge	4	16	EBS only
m4.2xlarge	8	32	EBS only
m4.4xlarge	16	64	EBS only
m4.10xlarge	40	160	EBS only

	vCPU	Memory (GB)	Instance Storage (GB)
Compute Optimized — Current Generation			
c4.large	2	3.75	EBS only
c4.xlarge	4	7.5	EBS only
c4.2xlarge	8	15	EBS only
c4.4xlarge	16	30	EBS only
c4.8xlarge	36	60	EBS only
c3.large	2	3.75	2 x 16 SSD
c3.xlarge	4	7.5	2 x 40 SSD
c3.2xlarge	8	15	2 x 80 SSD
c3.4xlarge	16	30	2 x 160 SSD
c3.8xlarge	32	60	2 x 320 SSD

2. Select the preferred instance type, then click **Next: Configure Instance Details**.

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more about instance types and how they can meet your computing needs.](#)

Filter by: **Compute optimized** **Current generation** [Show/Hide Columns](#)

Currently selected: c3.large (7 ECUs, 2 vCPUs, 2.8 GHz Intel Xeon E5-2686v2, 3.75 GB memory, 2 x 16 GB Storage Capacity)

	Family	Type	vCPUs (1)	Memory (GB)	Instance Storage (GB) (1)	EBS Optimized Available (1)	Network Performance (1)
<input type="checkbox"/>	Compute optimized	c4.large	2	3.75	EBS only	Yes	Moderate
<input type="checkbox"/>	Compute optimized	c4.xlarge	4	7.5	EBS only	Yes	High
<input type="checkbox"/>	Compute optimized	c4.2xlarge	8	15	EBS only	Yes	High
<input type="checkbox"/>	Compute optimized	c4.4xlarge	16	30	EBS only	Yes	High
<input type="checkbox"/>	Compute optimized	c4.8xlarge	36	60	EBS only	Yes	15 Gbps
<input checked="" type="checkbox"/>	Compute optimized	c3.large	2	3.75	2 x 16 (SSD)	-	Moderate
<input type="checkbox"/>	Compute optimized	c3.xlarge	4	7.5	2 x 40 (SSD)	Yes	Moderate
<input type="checkbox"/>	Compute optimized	c3.2xlarge	8	15	2 x 80 (SSD)	Yes	High
<input type="checkbox"/>	Compute optimized	c3.4xlarge	16	30	2 x 160 (SSD)	Yes	High
<input type="checkbox"/>	Compute optimized	c3.8xlarge	32	60	2 x 320 (SSD)	-	15 Gbps

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Instance Details](#)

368362

1. On the Configure Instance Details screen:
 - a. In Network, select the VPC you just created.
 - b. In Subnet, select the subnet for your first interface.
 - c. In Network Interfaces, click **Add Device** and select a subnet for each additional interface.
 - d. Click **Next: Add Storage**.

Step 3: Configure Instance Details
Configure the instance to suit your requirements. You can launch multiple instances from the same IAM, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 [Launch into Auto Scaling Group](#)

Purchasing option: ☐ Request Spot instances

Network: ☐ vpc-8f278bde (10.0.0.0/16) DEMO_VEDGE_CLOUD [Create new VPC](#)

Subnet: ☐ subnet-77a4b121 (10.0.0.0/24) PUBLIC_WAN [Create new subnet](#)
256 IP addresses available

Auto-assign Public IP: ☐ Disable

Placement group: ☐ No placement group

IAM role: ☐ ADPS-PUM [Create new IAM role](#)

Shutdown behavior: ☐ Terminate

Enable termination protection: ☐ Protect against accidental termination

Monitoring: ☐ Enable CloudWatch detailed monitoring
Additional charges apply

Tenancy: ☐ Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy

Network interfaces

Device	Network interface	Subnet	Primary IP	Secondary IP addresses
eth0	New network interface	subnet-77a4b121	Auto-assign	Add IP
eth1	New network interface	subnet-77a4b121	Auto-assign	Add IP

[Add device](#)

Warning: We can no longer assign a public IP address to your instance. The auto-assign public IP address feature for this instance is disabled because you specified multiple network interfaces. Public IPs can only be assigned to instances with one network interface. To re-enable the auto-assign public IP address feature, please specify only the eth0 network interface.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

1. The Add Storage screen opens. You do not need to change any settings on this screen. Click **Next: Tag Instance**.

Step 4: Add Storage
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more about storage options in Amazon EC2](#)

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	hdcv1rda	snap-c096229	8	General Purpose SSD (GP2)	24 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted
EBS	hdcv1rdb	snap-47719144	20	General Purpose SSD (GP2)	60 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more about free usage tier eligibility and usage restrictions.](#)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Tag Instance](#)

1. The Tag Instance screen opens. Enter your desired Key and Value, and then click **Next: Configure Security Group**.

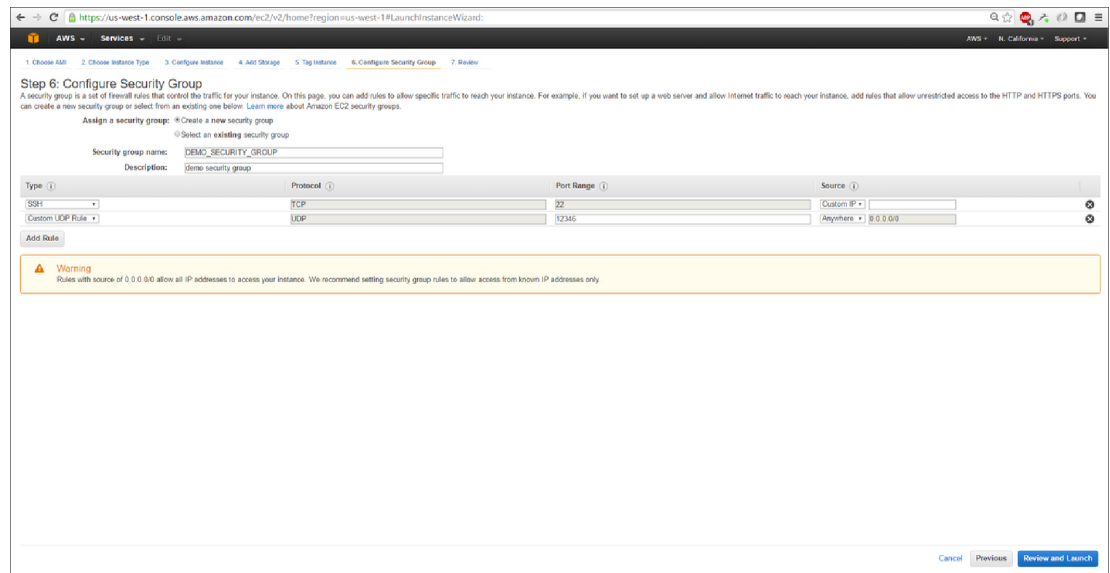
Create vEdge Cloud router VM Instance on AWS

368364

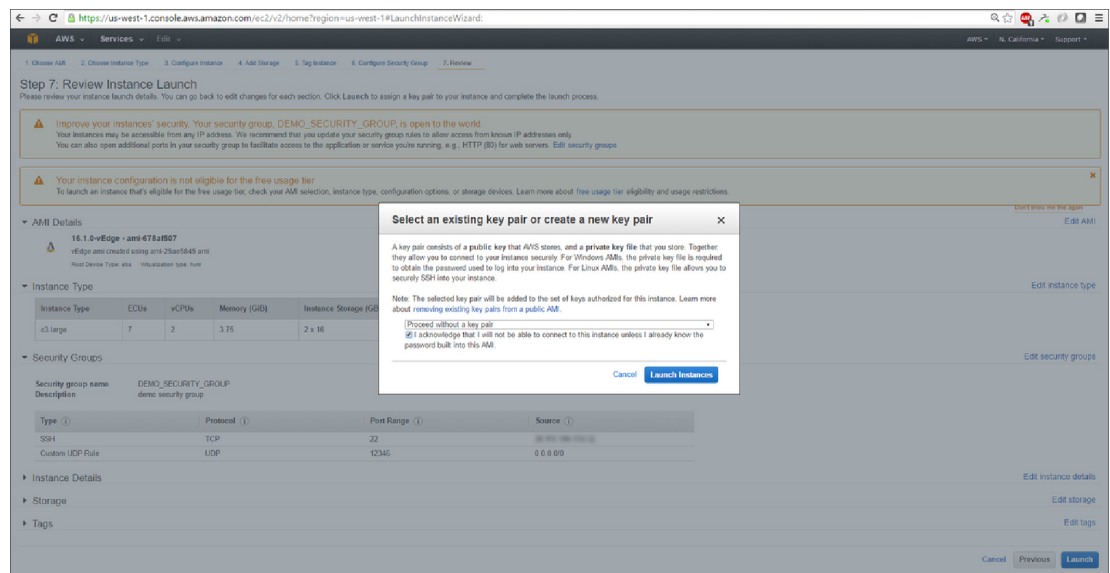
1. The Configure Security Group screen opens. Add rules to configure your firewall settings. These rules apply to outside traffic coming into your vEdge Cloud router.
 - a. Below **Type**, select **SSH**.
 - b. Below **Source**, select **My IP**.

368368

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.

Create vEdge Cloud router VM Instance on AWS

The screenshot shows the AWS Management Console for an EC2 instance named DEMO_VEDGE. The instance is of type c3.large, running in the us-west-1a availability zone. A terminal window is open, displaying the output of the 'vedge show interface | tab' command, which lists network interfaces and their statistics.

VPN	INTERFACE	IP ADDRESS	IF ADMIN STATUS	IF OPER STATUS	ENCP TYPE	PORT	MTU	HWADDR	UP/DN	DUPLX	TCP	UDP	PKT	TX
0	ge0/0	10.0.0.1	up	up	null	transport	1500	02:00:0c:4d:4d:4d	10	Full	1470	0/0	0/0	0/0
1	en0	10.0.0.2	up	up	null	service	1500	02:00:0c:4d:4d:4d	10	Full	1470	0/0	0/0	0/0

368371

Define Additional Interfaces

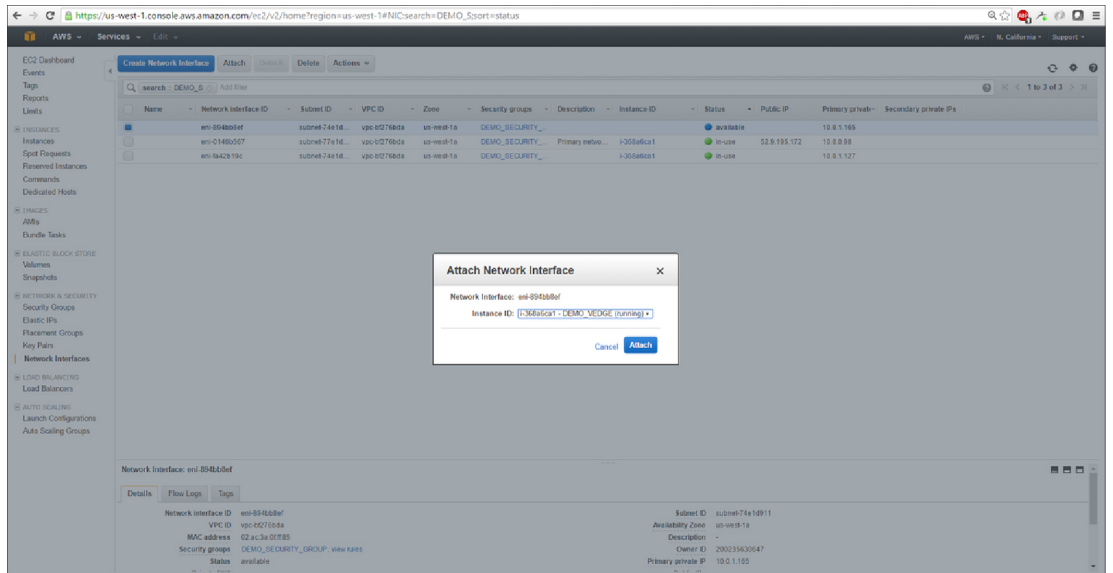
The vEdge Cloud router supports a total of nine interfaces. The first is always the management interface, and the remaining eight are transport and service interfaces. To configure additional interfaces:

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.

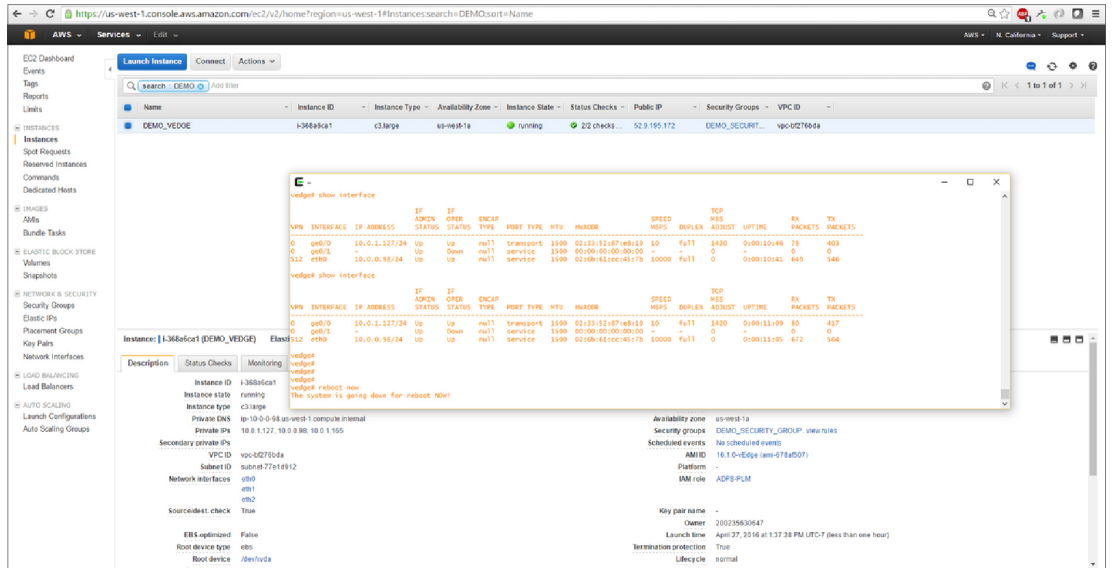
The screenshot shows the 'Create Network Interface' dialog box in the AWS Management Console. The dialog prompts for a description, subnet, private IP, and security group. The 'Subnet' is set to 'Subnet-7a1d9111 (10.0.1.0/24) us-west-1a | PRIVATE_LAN' and the 'Security group' is set to 'sg-3ec3087 - default - default VPC security group'.

38369

3. Select the check box to the left of the new interface, and click **Attach**.
4. Select the vEdge Cloud router, and click **Attach**.



- 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.

Create vEdge Cloud router VM Instance on AWS

The screenshot shows the AWS Management Console with the EC2 instance details for 'DEMO_VEDGE'. A terminal window is open, displaying the output of the 'show interface' command. The output shows statistics for various interfaces, including ge0/0, ge0/1, ge0/2, ge0/3, ge0/6, ge0/7, system, loopback3, ge0/4, ge0/5, and eth0. The MTU for most interfaces is 1500, while for loopback3 and ge0/4, it is 2000.

6. To allow the interface to carry jumbo frames (packets with an MTU of 2000 bytes), configure the MTU from the CLI. For example:

Router# **show interface**

VPN	INTERFACE	SPEED MBPS	AF	IP ADDRESS	TCP MSS	IF STATUS	IF OPER	ENCAP TYPE	PORT	TX PACKETS	MTU	HWADDR
0	ge0/0	1000	ipv4	10.66.15.15/24	full	Up	Up	null	service	545682	1500	
0	ge0/1	1000	ipv4	10.1.17.15/24	full	Up	Up	null	service	545226	1500	
0	ge0/2	1000	ipv4	-	full	Down	Up	null	service	10	1500	
0	ge0/3	1000	ipv4	10.0.20.15/24	full	Up	Up	null	service	0	1500	
0	ge0/6	1000	ipv4	172.17.1.15/24	full	Up	Up	null	service	10	1500	
0	ge0/7	1000	ipv4	10.0.100.15/24	full	Up	Up	null	service	770	1500	
0	system	0	ipv4	172.16.255.15/32	full	Up	Up	null	loopback	0	1500	
0	loopback3	10	ipv4	10.1.15.15/24	full	Up	Up	null	transport	0	2000	
1	ge0/4	1000	ipv4	10.20.24.15/24	full	Up	Up	null	service	52014	2000	
1	ge0/5	1000	ipv4	172.16.1.15/24	full	Up	Up	null	service	8	1500	
512	eth0	0	ipv4	10.0.1.15/24	full	Up	Up	null	service	28826	1500	

Router# **config**

Entering configuration mode terminal

Router(config)# **vpn 0 interface ge0/3 mtu 2000**

Router(config-interface-ge0/3)# **commit**

Commit complete.

vEdge(config-interface-ge0/3)# **end**

```
vEdge# show interface
```

				IF	IF					
				ADMIN	OPER	ENCAP				
					RX	TX				
VPN	INTERFACE	AF	IP ADDRESS	STATUS	STATUS	TYPE	PORT	TYPE	MTU	HWADDR
		SPEED	MSS							
		MBPS	DUPLEX	ADJUST	UPTIME	PACKETS	PACKETS			
0	ge0/0	ipv4	10.66.15.15/24	Up	Up	null	service		1500	
00:0c:29:db:f0:62		1000	full	1420	0:14:05:30	546018	545562			
0	ge0/1	ipv4	10.1.17.15/24	Up	Up	null	service		1500	
00:0c:29:db:f0:6c		1000	full	1420	0:14:21:42	0	10			
0	ge0/2	ipv4	-	Down	Up	null	service		1500	
00:0c:29:db:f0:76		1000	full	1420	0:14:22:10	0	0			
0	ge0/3	ipv4	10.0.20.15/24	Up	Up	null	service		2000	
00:0c:29:db:f0:80		1000	full	1920	0:14:21:42	0	10			
0	ge0/6	ipv4	172.17.1.15/24	Up	Up	null	service		1500	
00:0c:29:db:f0:9e		1000	full	1420	0:14:21:42	0	10			
0	ge0/7	ipv4	10.0.100.15/24	Up	Up	null	service		1500	
00:0c:29:db:f0:a8		1000	full	1420	0:14:21:42	773	708			
0	system	ipv4	172.16.255.15/32	Up	Up	null	loopback		1500	
00:00:00:00:00:00	0		full	1420	0:14:21:54	0	0			
0	loopback3	ipv4	10.1.15.15/24	Up	Up	null	transport		2000	
00:00:00:00:00:00	10		full	1920	0:14:21:46	0	0			
1	ge0/4	ipv4	10.20.24.15/24	Up	Up	null	service		2000	
00:0c:29:db:f0:8a		1000	full	1920	0:14:21:38	52038	52079			
1	ge0/5	ipv4	172.16.1.15/24	Up	Up	null	service		1500	
00:0c:29:db:f0:94		1000	full	1420	0:14:21:38	0	8			
512	eth0	ipv4	10.0.1.15/24	Up	Up	null	service		1500	
00:50:56:00:01:05	0		full	0	0:14:21:39	28926	29663			

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.

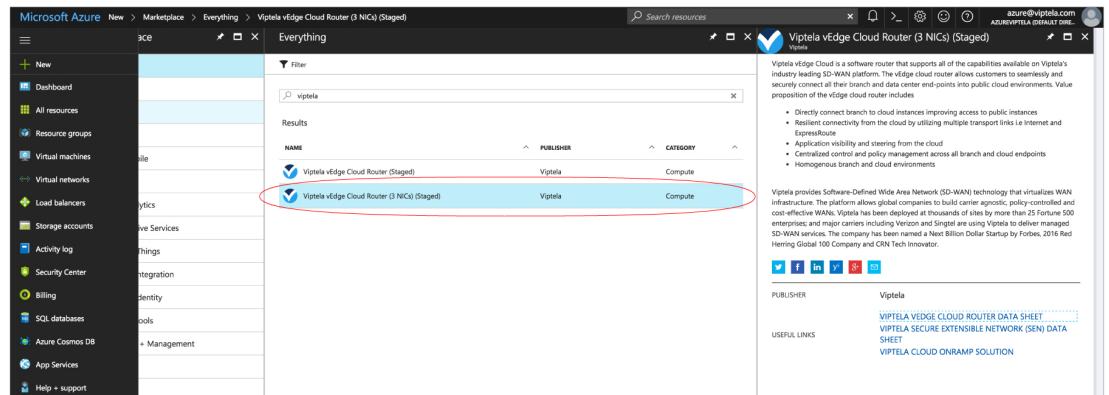
Note: Cisco SD-WAN offers only a Bring Your Own License (BYOL) for the vEdge Cloud router, so you are not actually purchasing the Cisco SD-WAN product. You are charged hourly for the VNET instance.

For server requirements, see *Server Hardware Recommendations*.

Launch Azure Marketplace and Create a vEdge Cloud router VM Instance

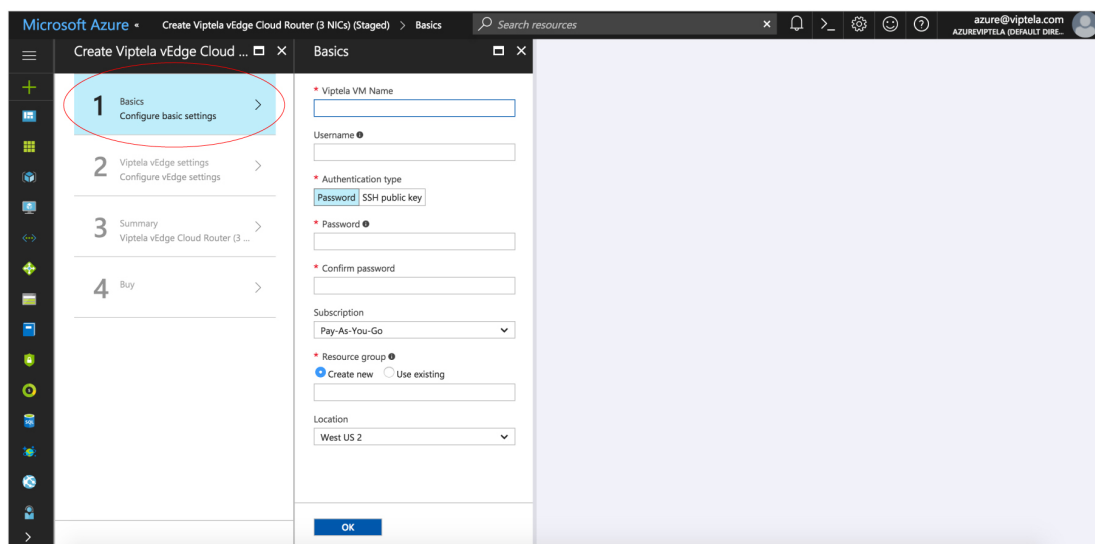
1. Launch the Azure Marketplace application:
 - a. In the left pane, click **New** to create a new vEdge Cloud router VM instance.
 - b. In the **Search** box, search for **Cisco**.

2. In the right pane, select Cisco vEdge Cloud router (3 NICs) (Staged).



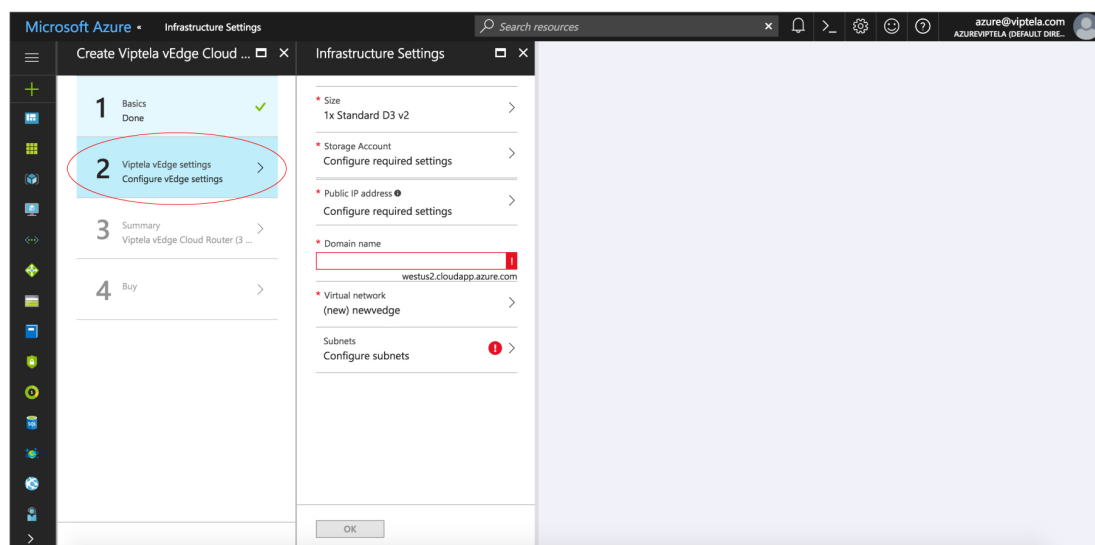
3. In the Cisco vEdge Cloud router (3 NICs) (Staged) screen, click **Basics** in the left pane to configure basic settings for the vEdge Cloud router VM:
- In the **VM Name** field, enter a name for the vEdge Cloud router VM instance.
 - In the **Username** field, enter the name of a user who can access the VM instance.
 - In the **Authentication type** field, select either **Password** or **SSH public key**.
 - If you selected password, enter, and then confirm, your password. You use the username and password to open SSH session to the VM instance.
 - If you selected SSH public key, see <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/create-ssh-key-pair-tutorial> for instructions about how to generate an SSH key pair for Linux VMs.
 - In the **Subscription** field, select **Pay-As-You-Go** from the drop-down menu.
 - 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.
 - In the **Location** field, select the location in which you wish to bring up the vEdge Cloud router VM instance.
 - Click **OK**.

Create vEdge Cloud router VM Instance on Azure



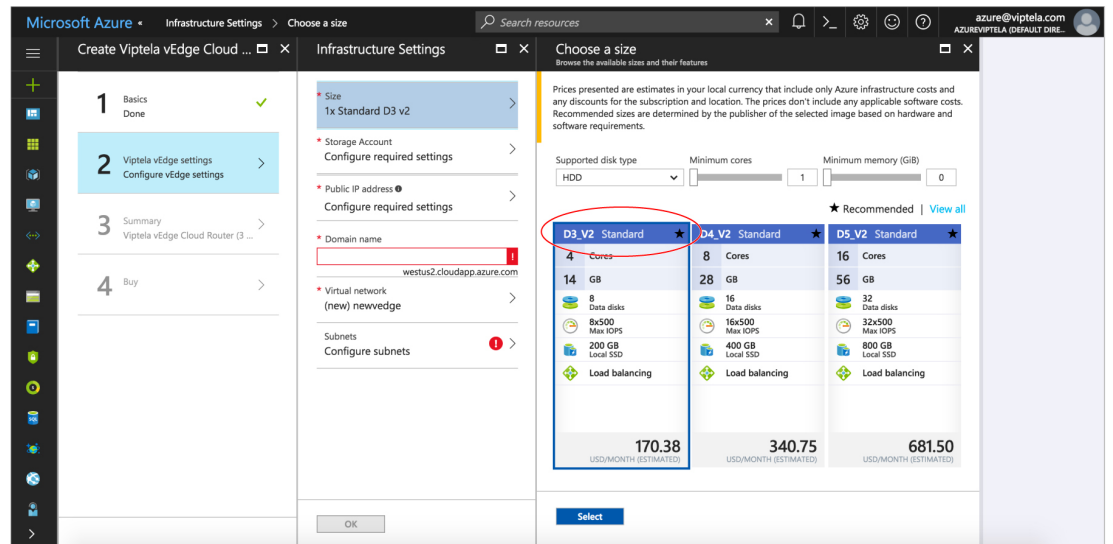
368380

4. In the left pane, click **vEdge Settings** to configure the vEdge Cloud router infrastructure settings.

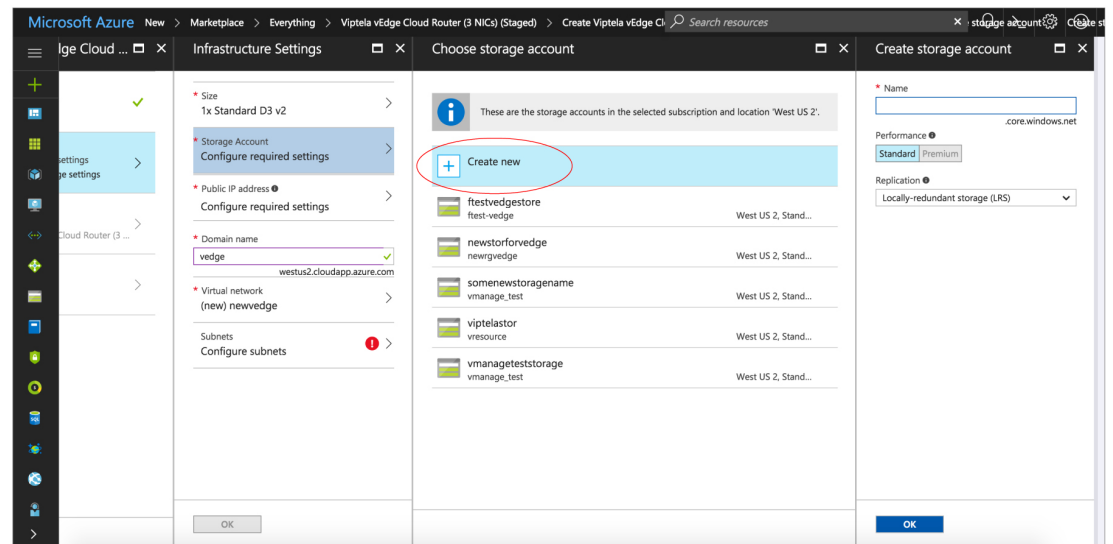


368381

5. In the Infrastructure Settings pane:
- 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.

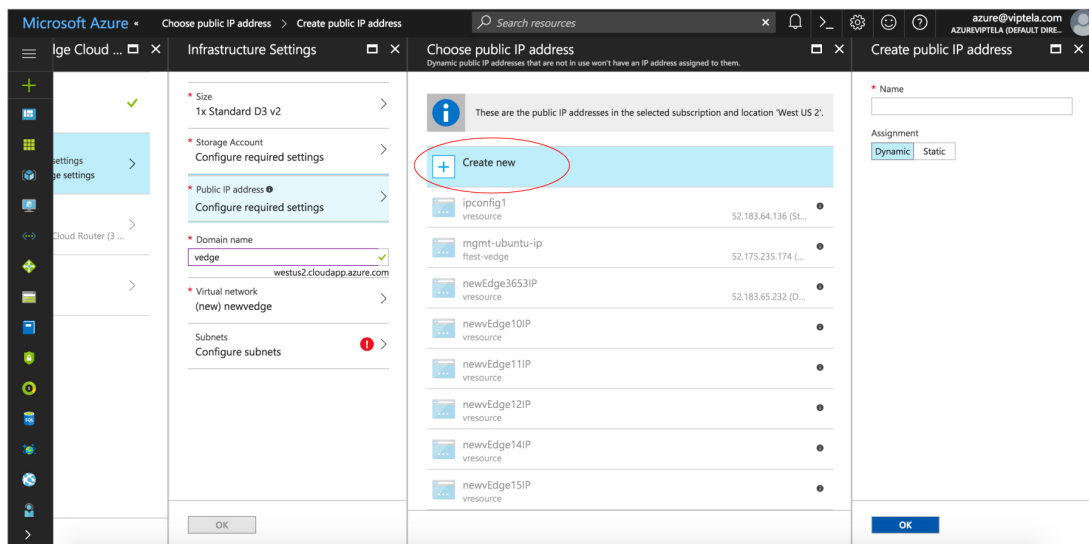


- b. Click **Storage Account**. In the **Choose storage account** pane, click **Create New** to create a new storage account or select one of the listed storage accounts. Then click **OK**.

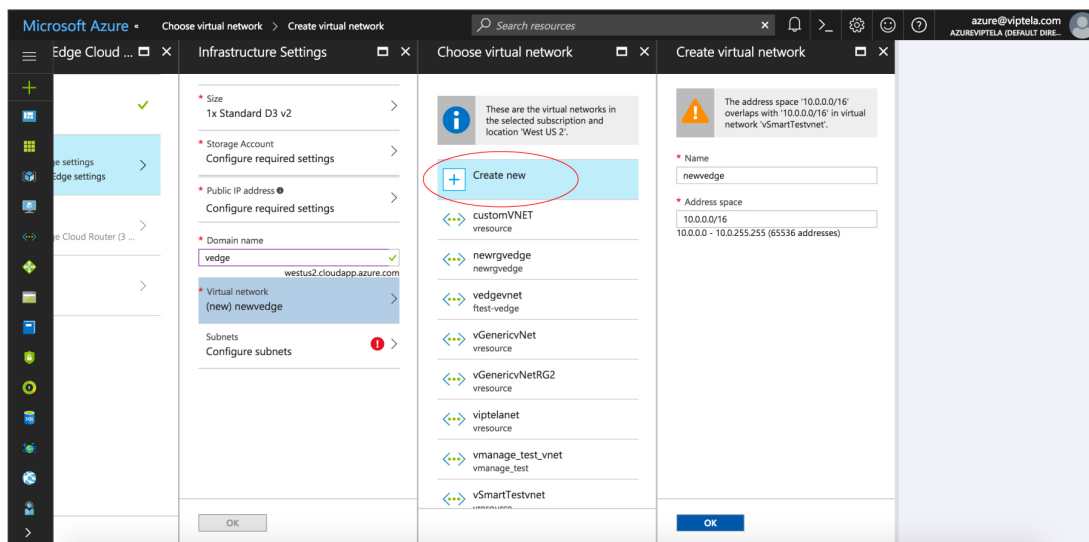


- c. Click **Public IP Address**. In the **Choose public IP address** pane, click **Create New** to create a new public IP address, or select one of the listed public IP address to use for the public IP subnet. Then click **OK**.

Create vEdge Cloud router VM Instance on Azure

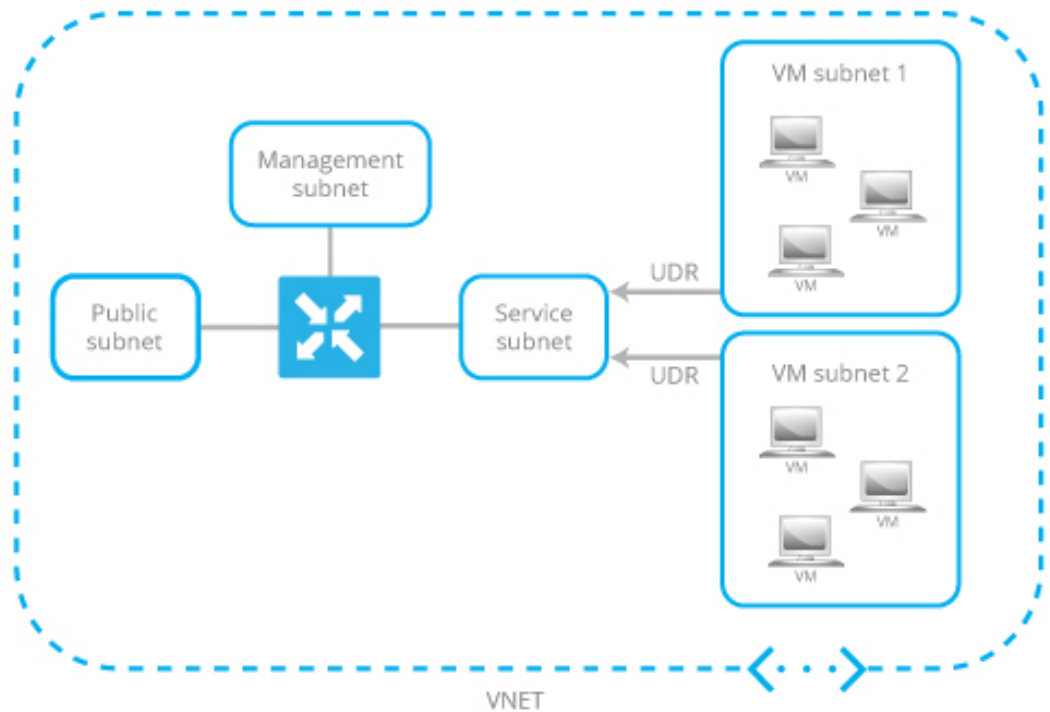


- d. In the **Domain Name** field, select **vedge** from the drop-down menu.
- e. Click **Virtual Network**. In the **Choose virtual network** pane, click **Create New** to create a new virtual network (VNET), or select an existing VNET to launch the vEdge Cloud instance in. Then click **OK**.



- f. If you selected an existing VNET, use the drop-down menu to choose available subnets within the VNET. Then click **OK**.

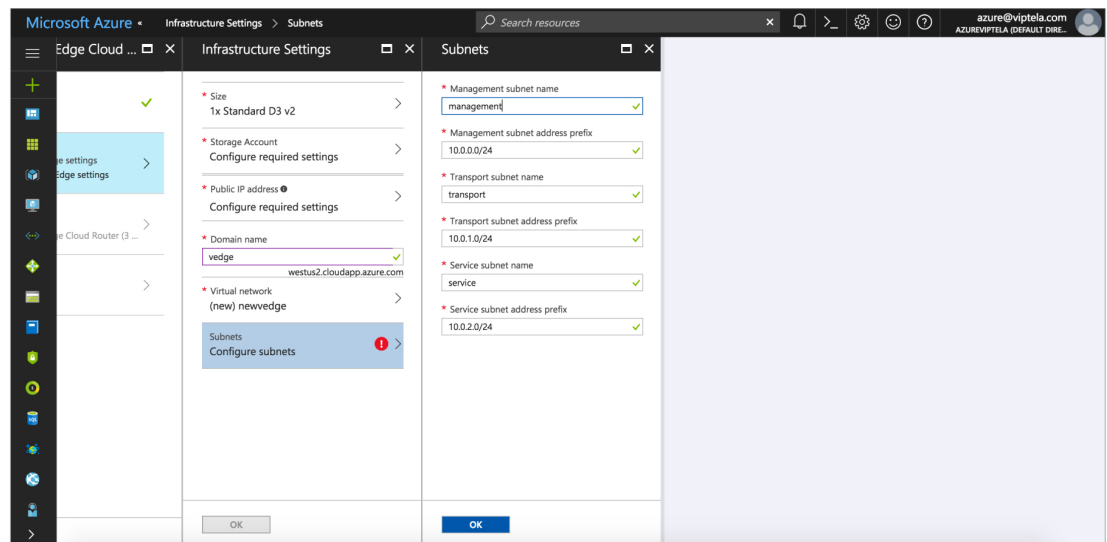
You must have three subnets available within the VNET; otherwise, the vEdge Cloud router VM instance will fail to launch. Also, ensure that route tables associated with your VM subnets have a user-defined route (UDR) towards the service subnet of the vEdge Cloud router. The UDR ensures that the VM subnets use the vEdge Cloud router as the gateway. See the example topology below.



368532

- g. If you created a new VNET, define the address space within that VNET. Then click **OK** in the Subnets pane.

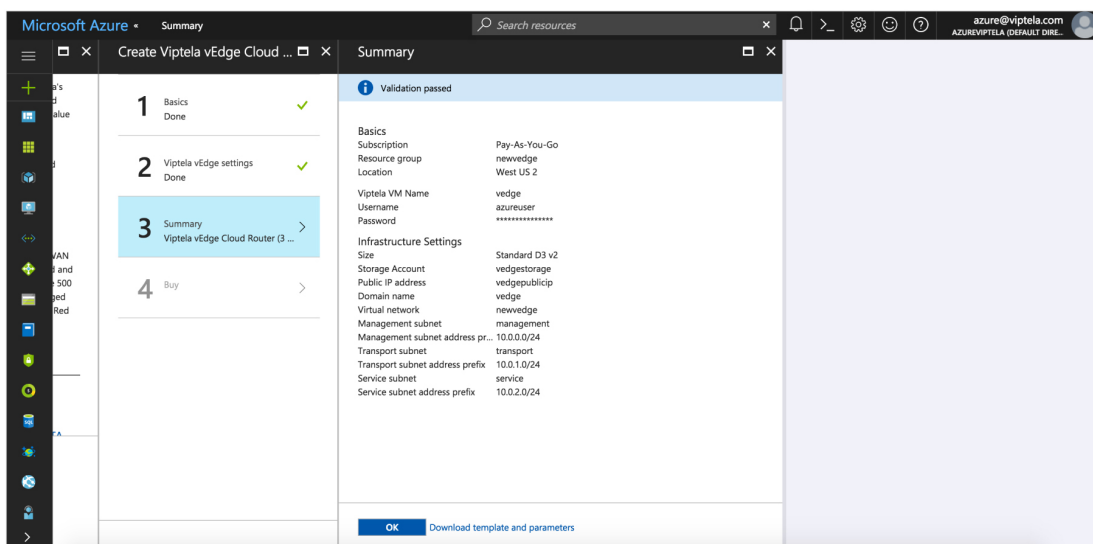
Cisco SD-WAN prepopulates subnet names and assigns IP addresses per subnet from the VNET address space you defined. If you plan to connect your VNET instances through the service subnet associated to the vEdge Cloud router, you do not need to make updates to the route table.



368386

6. In the Summary pane, click **OK**. The Summary pane validates and displays the configuration you defined for the vEdge Cloud router VM instance.

Create vEdge Cloud router VM Instance on Azure

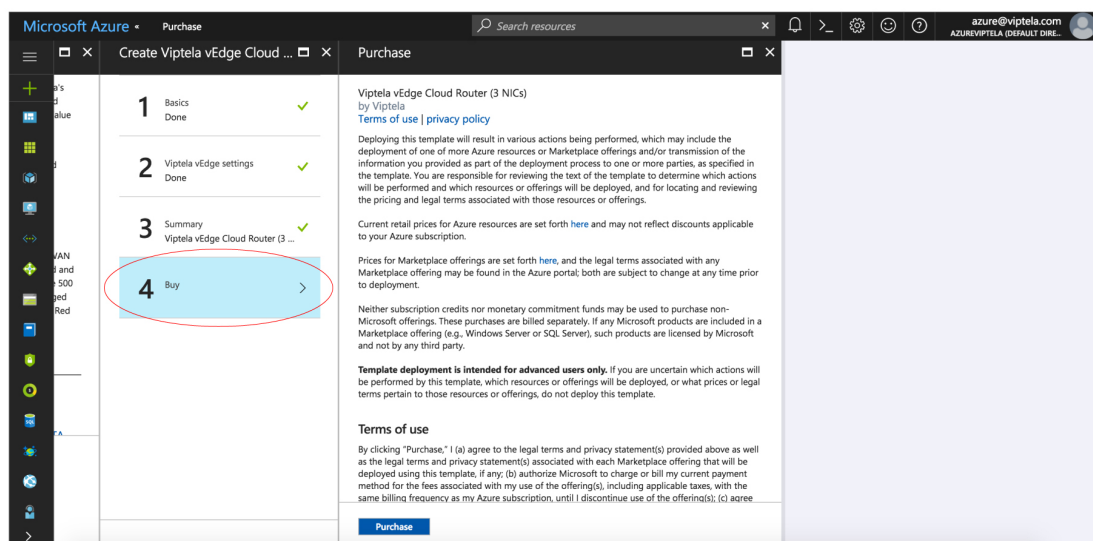


368387

7. Click **Buy** to purchase. Then click **Purchase** in the **Purchase** pane.

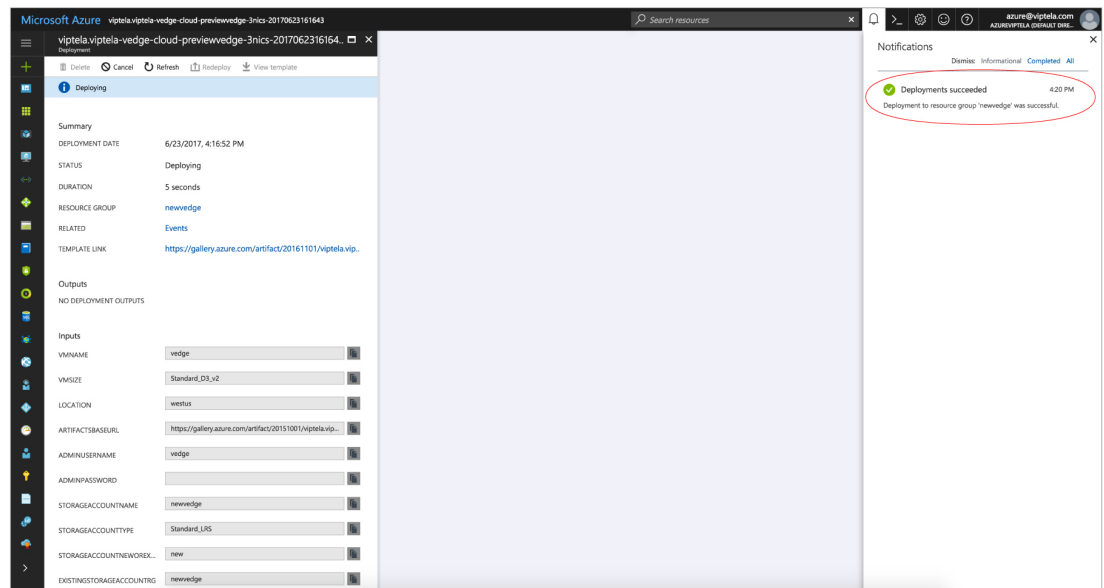
**Note**

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.

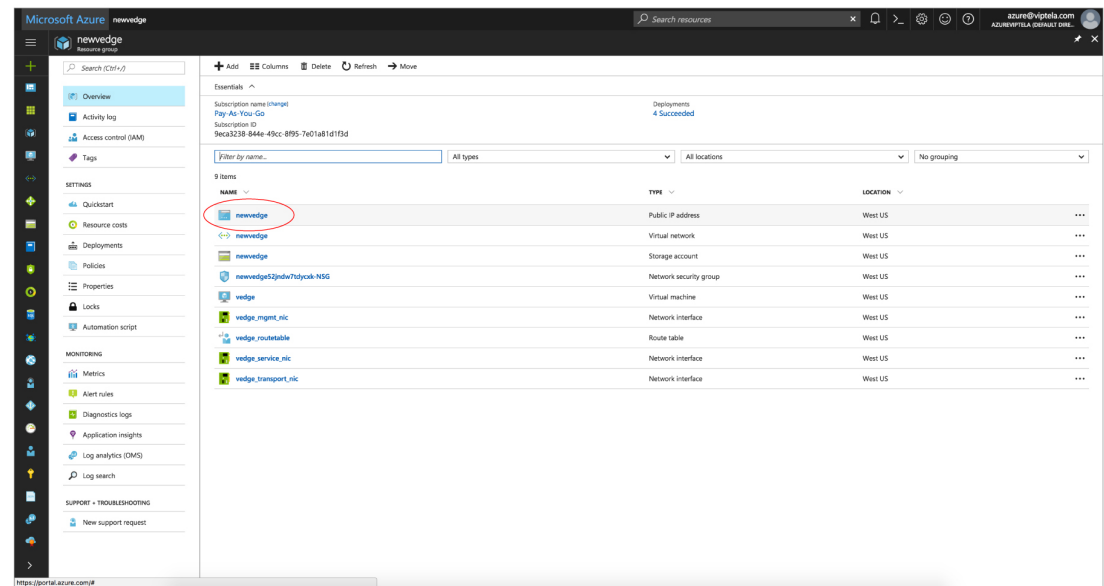


368388

The system creates the vEdge Cloud router VM instance and notifies you that the deployment has succeeded.

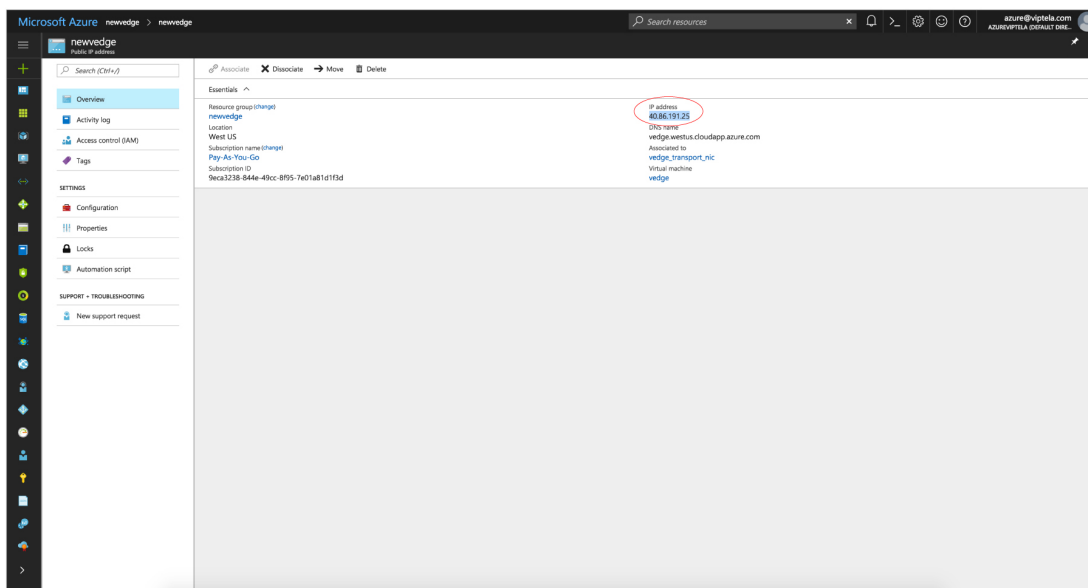


8. Click the **vEdge VM** instance you just created.



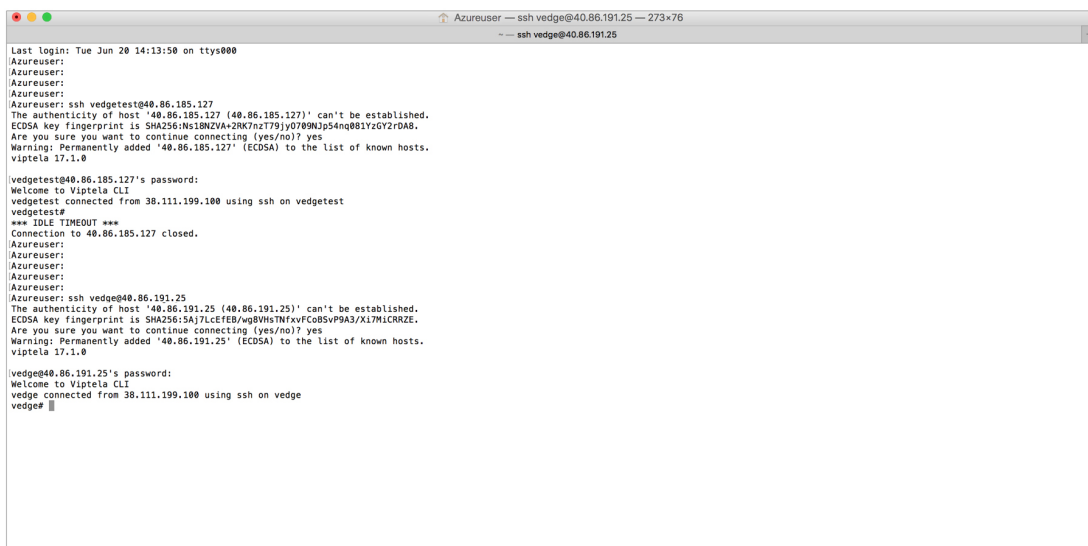
The system displays the public IP address and DNS name of the vEdge Cloud router VM instance.

Create vEdge Cloud router VM Instance on Azure



368391

9. SSH into the public IP address of the vEdge Cloud router VM instance.

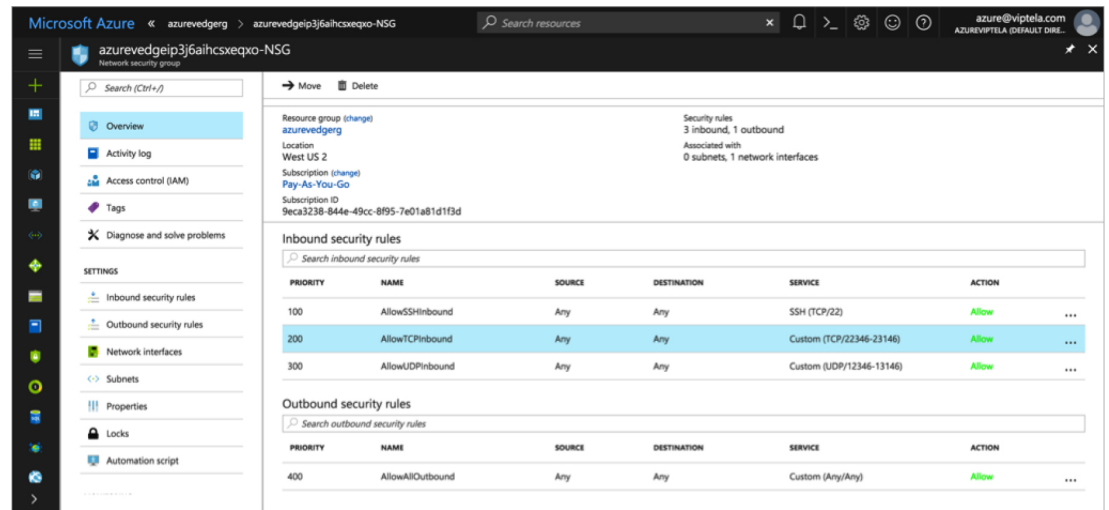


368393

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.



368392

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.

vEdge Cloud Router Interface	Subnet	Description
eth0	Management subnet	In-band management
ge0/1	Service subnet	Connects the vEdge Cloud router as a gateway device
ge0/0	Transport subnet	Transport/WAN link

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 VMware 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 9:

vNIC	Interface on VM Host	Interface in vEdge Cloud Configuration
vNIC 1	eth0	mgmt0 in VPN 512
vNIC 2	eth1	ge0/0
vNIC 3 through 7	eth2 through eth7	ge0/1 through ge0/7

**Note**

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

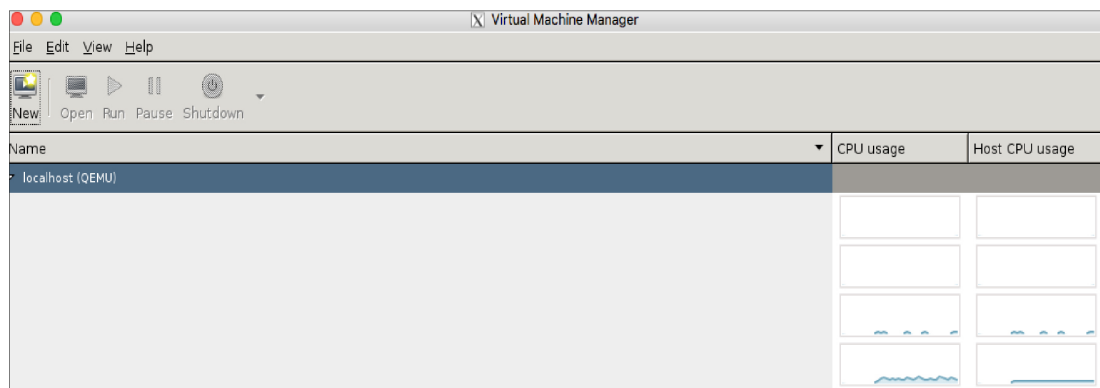
To start a software vEdge Cloud router, you must create a virtual machine (VM) instance for it. This article describes how to create a VM instance on a server running the Kernel-based Virtual Machine (KVM) Hypervisor software. You can also create the VM on Amazon AWS or on a server running the vSphere ESXi Hypervisor software.

For server requirements, see *Server Hardware Recommendations*.

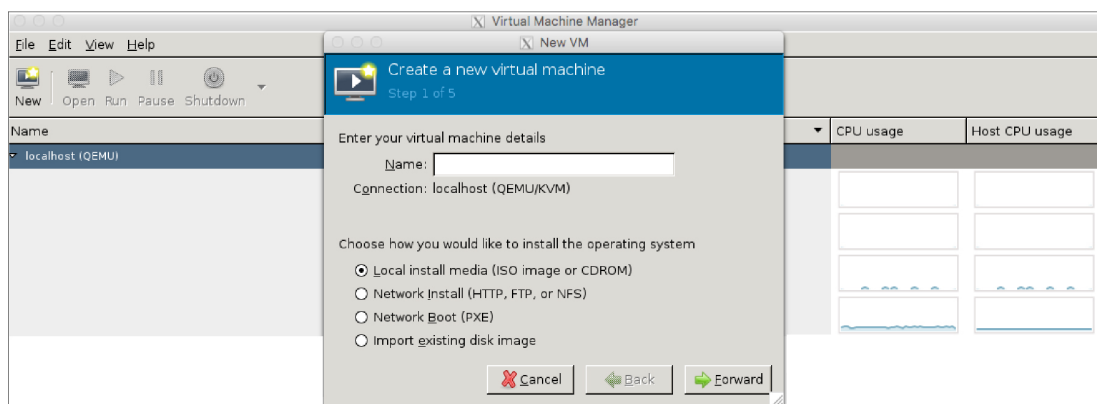
Create vEdge Cloud VM Instance on the KVM Hypervisor

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.

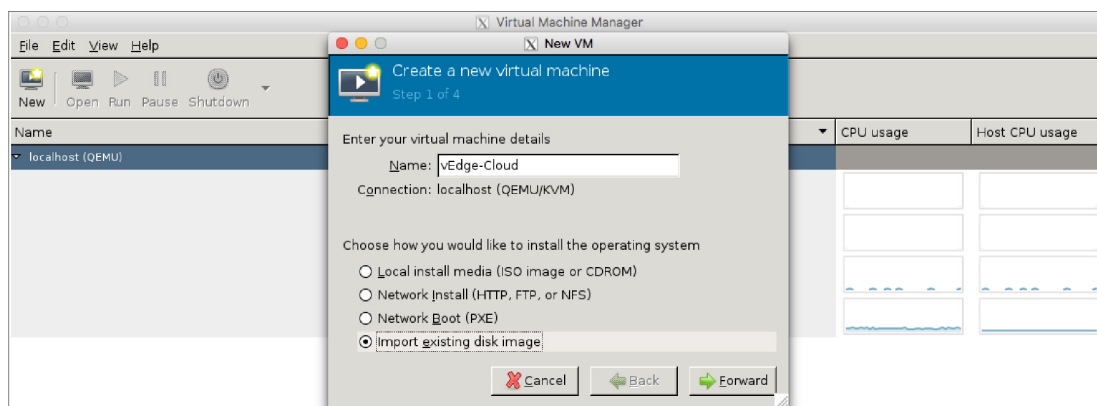


2. Click **New** to deploy the virtual machine. The system opens the Create a new virtual machine screen.



368249

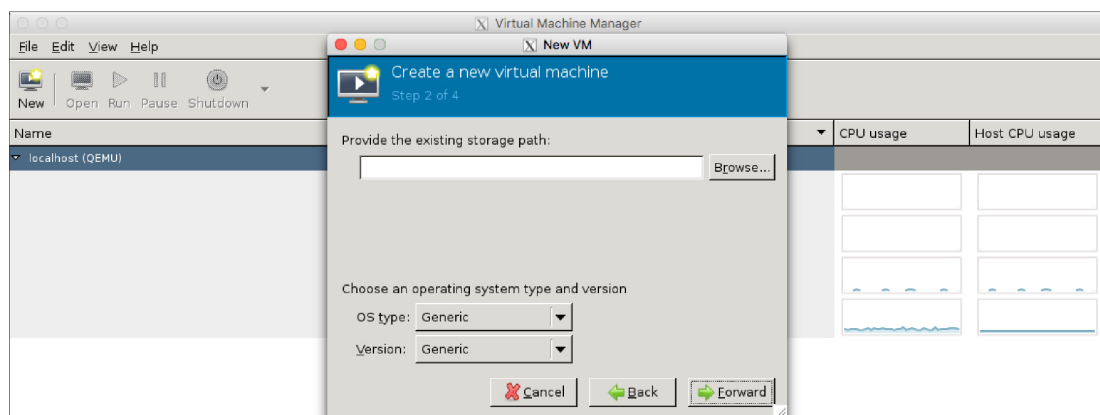
3. Enter the name of the virtual machine. The figure below specifies a name for the vEdge Cloud instance.
 - a. Select **Import existing disk image**.
 - b. Click **Forward**.



368250

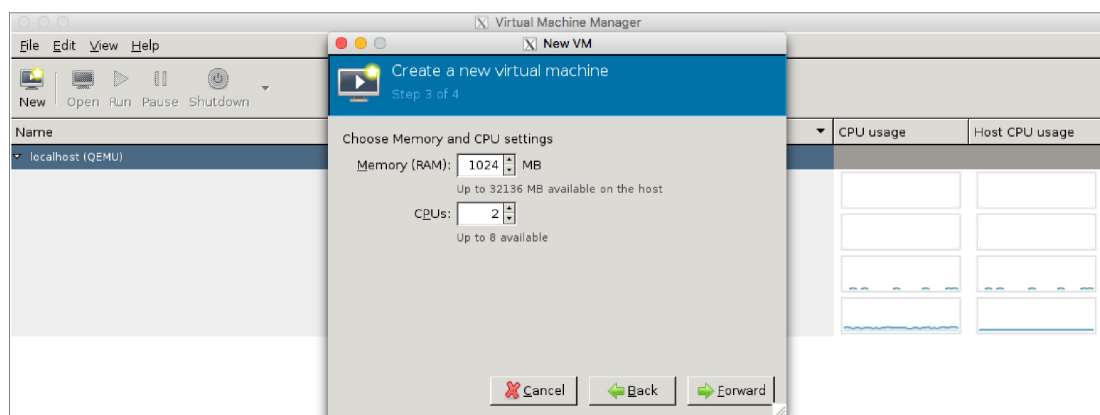
4. In **Provide the existing storage path** field, click **Browse** to find the vEdge Cloud software image.
 - a. In the **OS Type** field, select **Linux**.
 - b. In the **Version** field, select the Linux version you are running.
 - c. Click **Forward**.

Create vEdge Cloud VM Instance on KVM



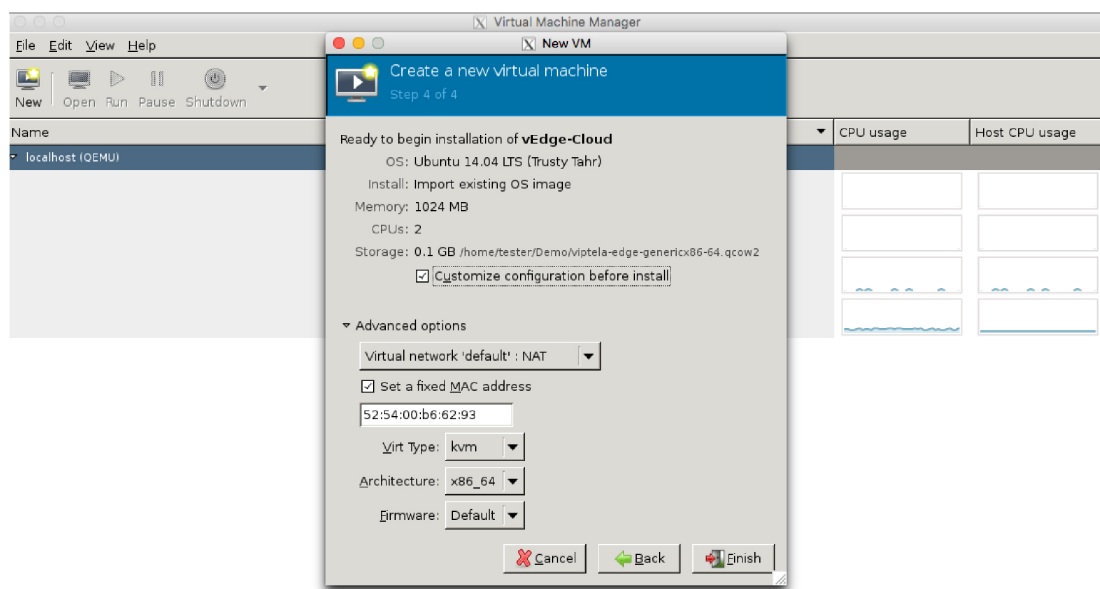
368252

5. Specify Memory and CPU based on your network topology and the number of sites. Click **Forward**.



368251

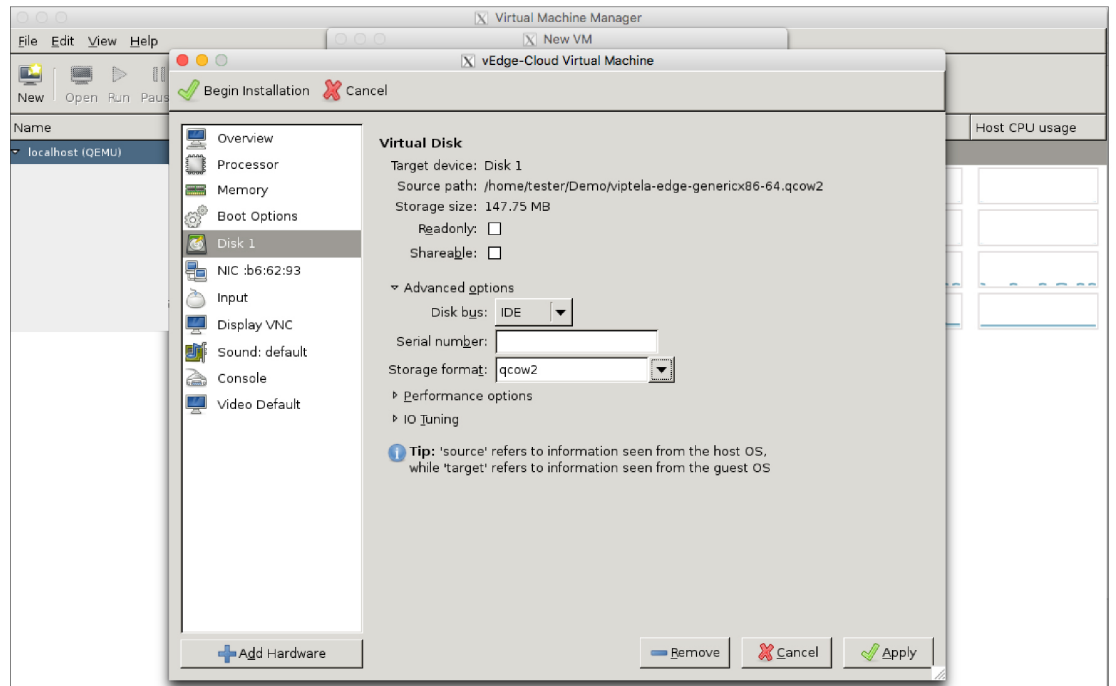
6. Select **Customize configuration before install**. Then click **Finish**.



368254

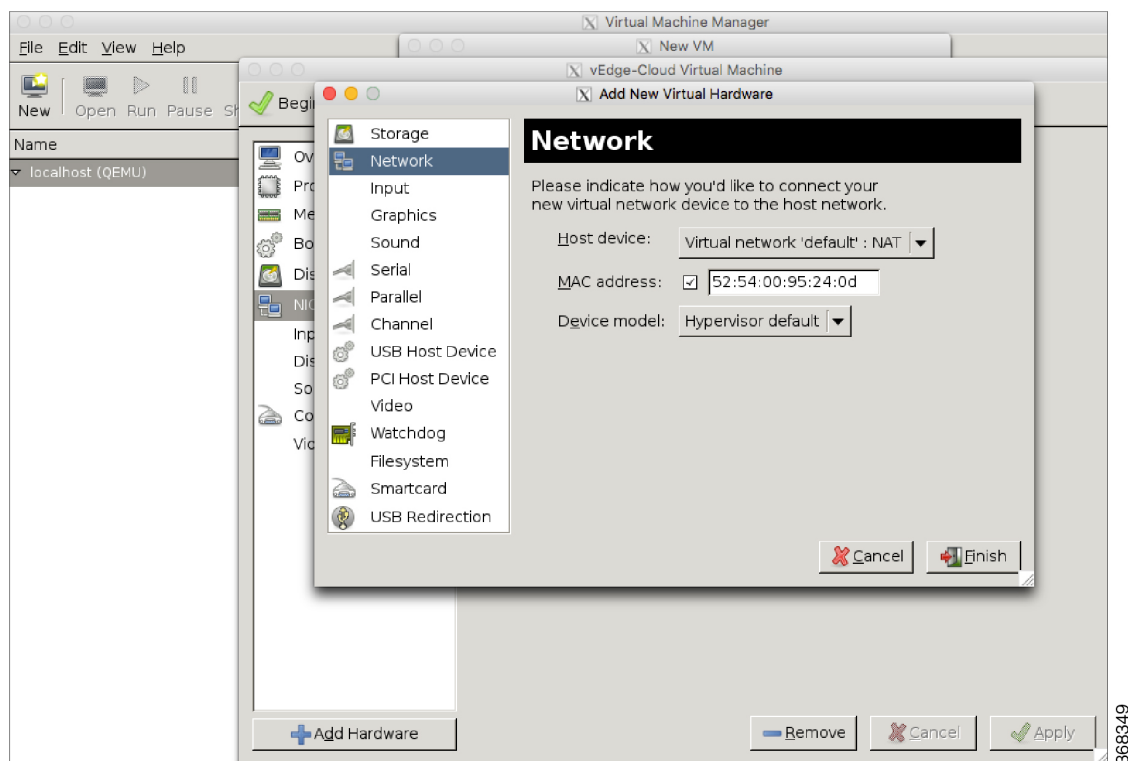
7. Select **Disk 1** in the left navigation bar. Then:

- 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.

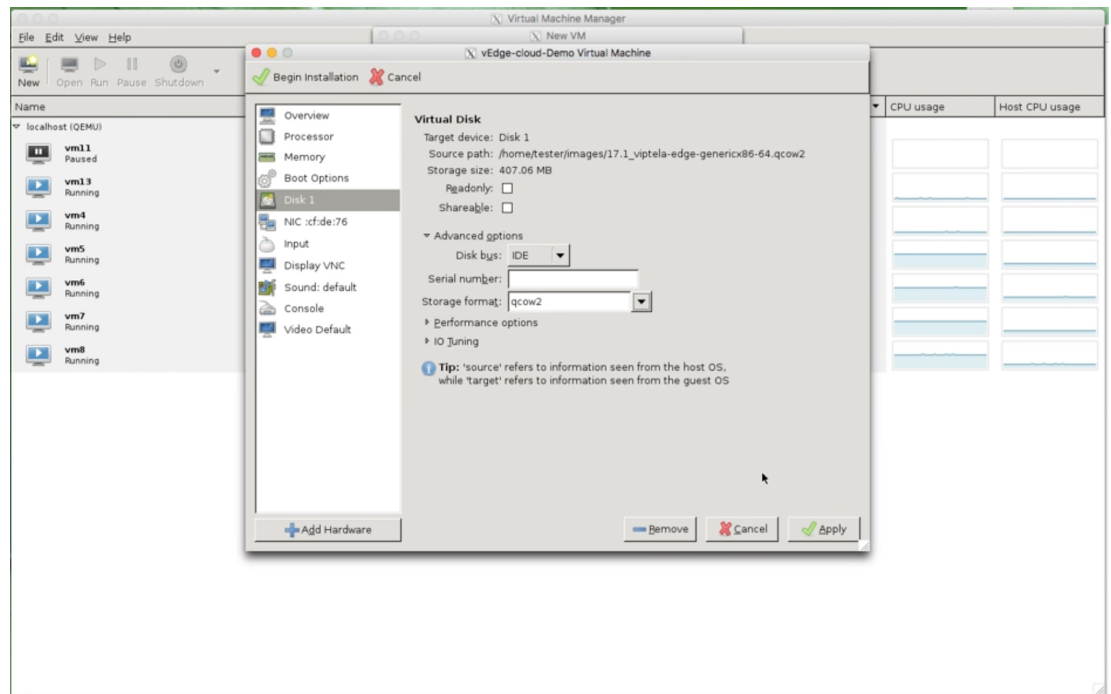


The newly created vNIC is listed in the left pane. This vNIC is used for the tunnel interface.

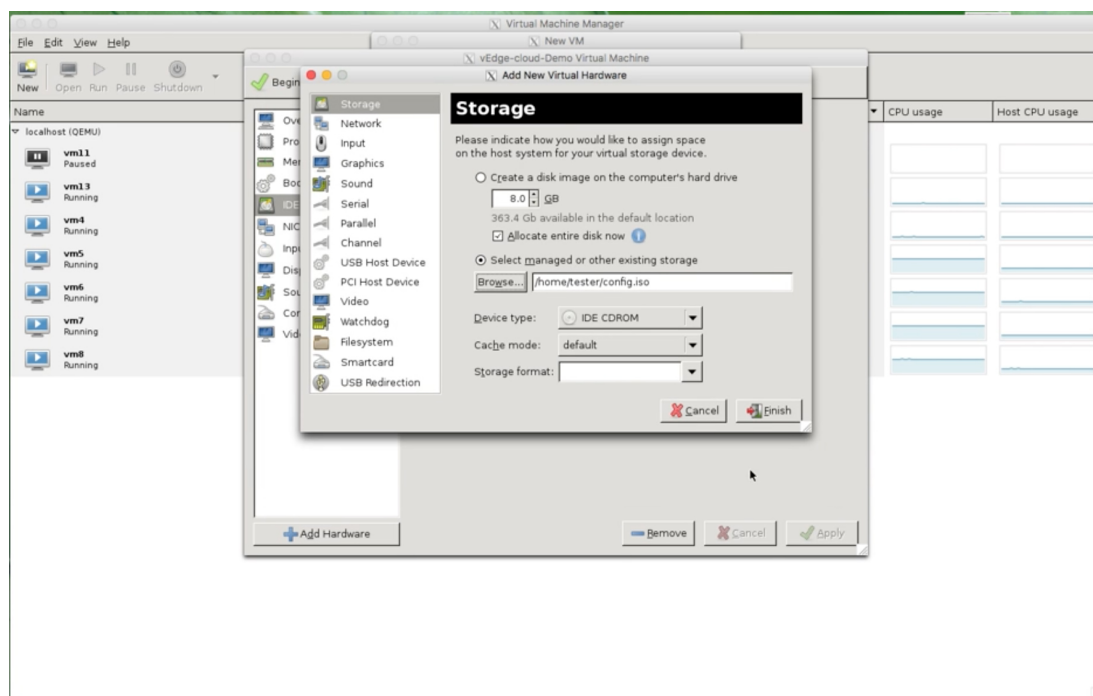
10. Create an ISO file to include a cloud-init configuration for the vEdge Cloud router.

```
tester@testbed46:/tmp/demo$ more meta-data
instance-id: Demo
local-hostname: vm4
tester@testbed46:/tmp/demo$ more user-data
#cloud-config
vinitparam:
- otp : f862ddf0d59f4ab9248da70951388767
- vbond : 172.22.1.2
- uuid : 7b271b64-8c48-453e-a690-ec190cc7d5ef
- org : vIPTela System TB
tester@testbed46:/tmp/demo$
tester@testbed46:/tmp/demo$ genisoimage -o config.iso -V cidata -r -J meta-data user-data
I: -input-charset not specified, using utf-8 (detected in locale settings)
Total translation table size: 0
Total rockridge attributes bytes: 331
Total directory bytes: 0
Path table size(bytes): 10
Max brk space used 0
183 extents written (0 MB)
tester@testbed46:/tmp/demo$
```

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.



368536

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
```

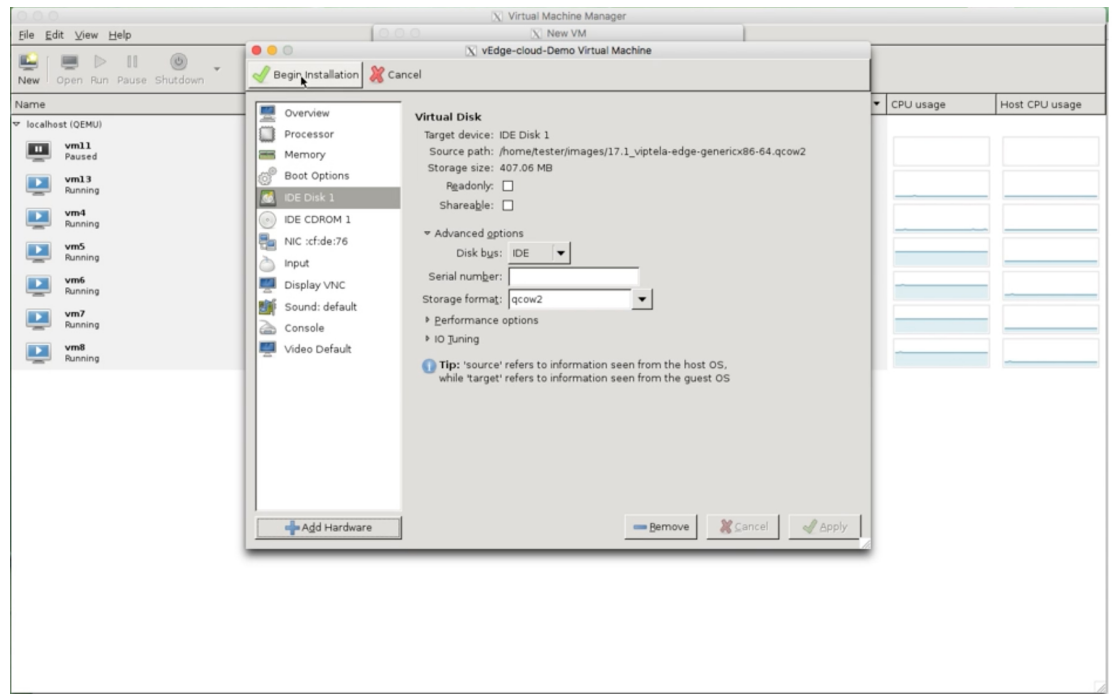
- c. Change the MTU of each virbr-nic:

```
user@vm:~$ sudo ifconfig virbr-nic number mtu 2000
```

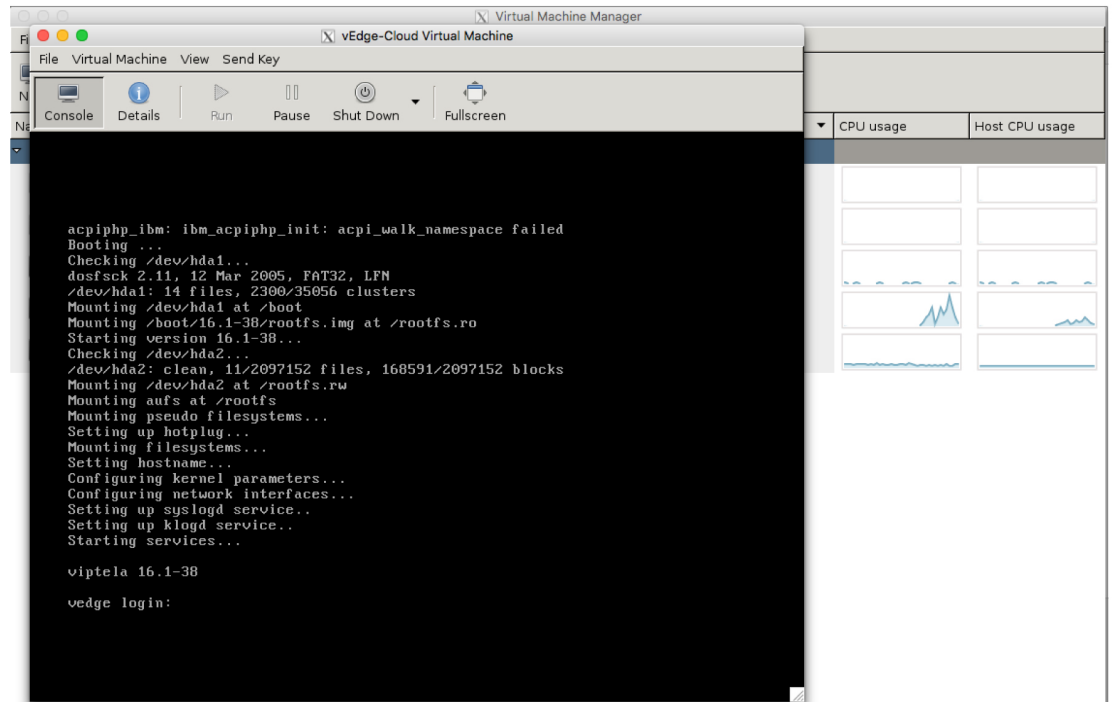
- d. Verify the MTU value:

```
user@vm:~$ ifconfig -a
```

14. In the vEdge Cloud Virtual Machine screen, click Begin Installation in the top upper-left corner of the screen.



15. The system creates the virtual machine instance and displays the vEdge Cloud console.



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 10:

vNIC	Interface on VM Host	Interface in vEdge Cloud Configuration
vNIC 1	eth0	mgmt0 in VPN 512
vNIC 2	eth1	ge0/0
vNIC 3 through 7	eth2 through eth7	ge0/1 through ge0/7

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

1. Go to <http://viptela.com/support/> and log in.
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.
2. In the vEdge Cloud Certificate Authorization bar, select Manual.
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/mcp/enroll/index?jur_hash=422d7cb508a24e32ea7de4f78d37f8



Help

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.

368889

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 11: Feature History

Feature Name	Release Information	Description
Device Onboarding Enhancement	Cisco IOS XE Release 17.3.1a Cisco vManage Release 20.3.1	This feature provides an enhancement to onboard your device to Cisco vManage by directly uploading a .csv file.

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.



Note **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.



Note 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 $20 \times 8 = 160$ 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 or 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.
6. Save the VPN-Interface-Cellular feature template.
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.



Note

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 / 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
```




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 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 -74.00594130000002
system-ip 172.16.251.20
site-id 200
max-controllers 1
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
    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
graceful-restart
advertise bgp
advertise connected
advertise static
!
security
ipsec
authentication-type ah-sha1-hmac sha1-hmac
!
!
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
```

```

remote-as 111000
password $4$LzLwZj1ApK4zj4BgLEFXKw==
!
!
ospf
timers spf 200 1000 10000
area 0
interface ge0/1
authentication type message-direct
authentication message-digest message-digest-key 1 md5 $4$LzLwZj1ApK4zj4BgLEFXKw==
exit
exit
!
!

```

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

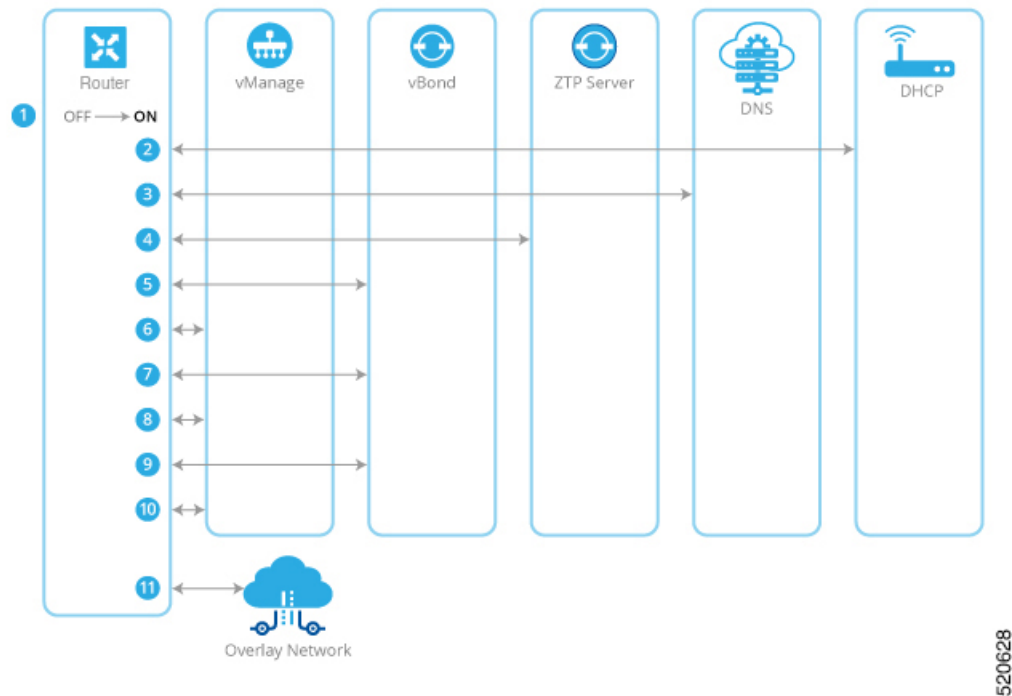
Cisco SD-WAN provides an automatic provisioning software as a service (SaaS) called zero-touch provisioning (ZTP), which allows hardware vEdge routers to join the overlay network automatically. The ZTP process begins when you power on a hardware vEdge router for the first time.

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 reestablishes 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".

Templates Device **Feature**

Feature Template: VPN-Interface-Cellular

Template Name: cellint Device Type: vEdge 100 M

Description: cellint

Shutdown: ☐ Yes ☒ No Technology: ☐ It

Interface name: cellular0 Profile ID: 0

Description:

IPv4 Configuration: ☒ Dynamic ☐ Static DHCP distance:

IPv6 Configuration: ☐ Dynamic ☒ Static IPv6 address:

DHCP Helper:

Bandwidth Upstream: Bandwidth Downstream:

Tunnel Interface: NAT ACL/QoS ARP **Advanced**

Tunnel Interface: ☒ On ☐ Off

Color: ☐ It Restrict: ☐ On ☒ Off

368376

The following figure shows, in the Advanced tab, that the default cellular MTU configuration is 1428 bytes:

Templates Device **Feature**

Feature Template: VPN-Interface-Cellular

Template Name: cellint Device Type: vEdge 100 M

Description: cellint

Shutdown: ☐ Yes ☒ No

Interface name: cellular0 Profile ID: 0

Description:

IPv4 Configuration: ☒ Dynamic ☐ Static DHCP distance:

IPv6 Configuration: ☐ Dynamic ☒ Static IPv6 address:

DHCP Helper:

Bandwidth Upstream: Bandwidth Downstream:

Tunnel Interface: NAT ACL/QoS ARP **Advanced**

IP MTU: 1428 PMTU discovery: ☐ On ☒ Off

Clear-Don't-Fragment: ☐ On ☒ Off Static Ingress QoS: ARP timeout: 1200

Autonegotiate: ☒ On ☐ Off TLLOC Extension:

368375

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.

