Cisco Crosswork Optimization Engine 1.1 Installation Guide

First Published: 2020-04-03

Last Modified: 2020-04-22

CONTENTS

Overview of Cisco Crosswork Optimization Engine

This section provides the following topics:

Overview of Cisco Crosswork Optimization Engine

Cisco Crosswork Optimization Engine is part of the Cisco Crosswork Network Automation suite of products. Cisco Crosswork Optimization Engine provides real-time network optimization allowing operators to effectively maximize network utilization as well as increase service velocity.

Crosswork Optimization Engine provides the following:

- A topology map that gives valuable real-time visualization of devices, links, link utilization, and TE tunnels (Segment Routing policies and RSVP-TE tunnels) in the network.

  Note Throughout this document *TE tunnels* refer to both SR policies and RSVP-TE tunnels.

- A UI that allows for easy manageability of TE tunnels. Crosswork Optimization Engine enables the network operator to perform the following tasks:

  - Provision TE tunnels and modify or remove them using an intuitive workflow

  - Continuously track TE tunnel dynamic path computations to maintain SLA objectives

  - Preview TE tunnels before deploying it to the network

- Crosswork Optimization Engine function packs (with correct licensing) that provide closed-loop optimization to define the optimization intent, implement the intent, and continuously monitor, track, and react to maintain the original intent. For more information, see the *Cisco Crosswork Optimization Engine Function Packs* document.

Cisco Crosswork Optimization Engine Architecture

In order to provide for better scalability and improved performance the data collection functionality has been separated out into its own VM and software package called Cisco Crosswork Data Gateway. The license to use Cisco Crosswork Data Gateway is included with the Crosswork Optimization Engine license. Cisco Crosswork Data Gateway gathers all the information from the monitored devices and forwards it to Crosswork Optimization Engine for analysis and processing. Crosswork Optimization Engine can then be used by the operator to manage the network or respond to changes in the network.

Apart from Crosswork Optimization Engine, Cisco Crosswork Data Gateway is required for external data collection, such as interface statistics via SNMP and model-driven telemetry sensor paths. Crosswork Optimization Engine can use Cisco Network Services Orchestrator (Cisco NSO) as a provider to manage the devices for any required model-driven telemetry (MDT) sensor paths for data collection. Cisco NSO then supplies the device management and configuration-maintenance services.

If you do not plan to use to use Cisco NSO, you must apply the telemetry configuration on your devices. See the "Prerequisites for Device Telemetry" topic in the *Cisco Crosswork Optimization Engine User Guide*.

.

Note Crosswork Optimization Engine is designed and tested to be used with the Cisco Crosswork Data Gateway 1.1 release.

This guide explains the installation process to set up both Crosswork Optimization Engine and Cisco Crosswork Data Gateway for use. For information on how to use Crosswork Optimization Engine, refer to the *Cisco Crosswork Optimization Engine User Guide*.

For more information about the Cisco Crosswork Network Automation platform and Cisco Crosswork Optimization Engine, see the Cisco Crosswork Network Automation Product page on Cisco.com.

Segment Routing Path Computation Element (SR-PCE)

Crosswork Optimization Engine uses the combination of telemetry and Cisco Segment Routing Path Computation Element (SR-PCE) to analyze and compute optimal TE tunnels.

Cisco SR-PCE (formerly Cisco XR Traffic Controller (XTC)) runs on the Cisco IOS XR operating system. SR-PCE provides stateful PCE functionality that helps control and move TE tunnels to optimize the network. PCE describes a set of procedures by which a Path Computation Client (PCC) can report and delegate control of head-end tunnels sourced from the PCC to a PCE peer. The PCC and PCE establish a Path Computation Element Communication Protocol (PCEP) connection that SR-PCE uses to push updates to the network.

Crosswork Optimization Engine discovers all devices that are part of the IGP domain including those that do not establish PCEP peering with SR-PCE. However, PCEP peering is required to deploy TE tunnels to the device.

Audience

This guide is for experienced network administrators who install Cisco Crosswork Optimization Engine and Cisco Crosswork Data Gateway in their network. This guide assumes that you are familiar with the following:

- Linux system administration

- Routing and switching terminology and concepts

- Configuration of SR policies and RSVP-TE tunnels

- Deploying OVF templates using VMware vCenter

Installation Requirements

This section provides general guidelines and minimum requirements for individual components installed on a single server.

This section contains the following topics:

Cisco Crosswork Optimization Engine Installation Requirements

Cisco Crosswork Optimization Engine deployment requirements vary, depending on which of the platform's components are installed together and the number of hosts. This section provides general guidelines and minimum requirements for installing Cisco Crosswork Optimization Engine on a single host, unless otherwise specified.

Network Requirements

This figure shows the network components and connections needed to install and use Cisco Crosswork Optimization Engine.

Figure 1: Crosswork Optimization Engine Network
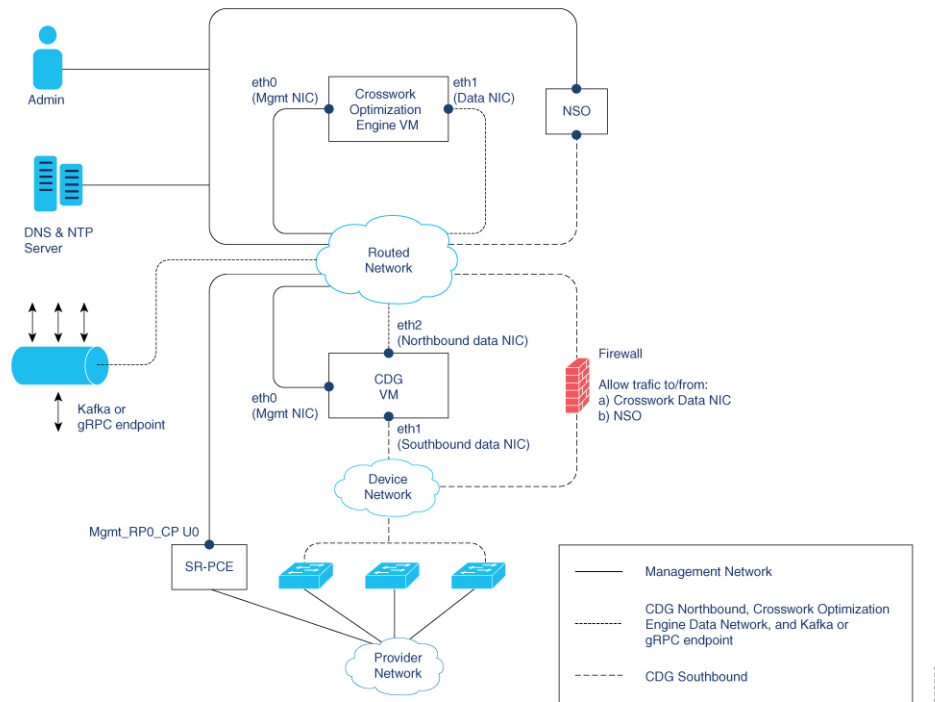
Cisco Crosswork Optimization Engine Virtual Machine (VM)

The Cisco Crosswork Optimization Engine VM has the following vNICs:

- Management NIC (eth0)—Used for traffic management to all Crosswork applications via the API or UI.

- Data NIC (eth1)—Used for Crosswork applications to reach devices and Cisco Crosswork Data Gateway (northbound).

Cisco Crosswork Data Gateway VM

The Cisco Crosswork Data Gateway VM has the following vNICs:

- Management NIC (eth0)—Provides control plane communication between Cisco Crosswork Data Gateway and Crosswork VM.

- Southbound Data NIC (eth1)—Used for Cisco Crosswork Data Gateway collectors to reach devices.

- Northbound Data NIC (eth2)—Sends data collected from devices to Crosswork applications or external data sinks (Kafka or gRPC receiver).

Cisco Network Services Orchestrator (NSO) VM

The NSO VM has the following vNICs:

- Management NIC (eth0): Used for Crosswork applications to reach NSO.

- Southbound data NIC (eth1): Used for NSO to reach devices (southbound) or RFS NSO.

Note Single interface deployment is not supported for Cisco Crosswork Optimization Engine and Cisco Crosswork Data Gateway.

Routed and Device Networks

Connectivity between the various components should be accomplished via an external routing entity (shown as 'Routed Network' in the figure). The figure shows various line styles suggesting possible routing domains within the Routed Network.

- Solid—Management routing domain.

- Dotted—Cisco Crosswork Data Gateway northbound data routing domain (towards Crosswork/External data sink).

- Dashes—Device access routing domain (from Cisco Crosswork Data Gateway and NSO).

The IP/subnet addressing scheme on each of these domains depend on the type of deployment.

Routing between domains is needed for Crosswork and NSO to reach the devices. However, proper firewall rules need to be in place to allow only select sources (for example, Crosswork and NSO) to reach the devices.

If you plan to access devices via host name, be sure that host names are registered with your deployment's DNS server.

On the Device network, devices may be reached in-band or via out-of-band management interfaces depending on the local security policies of each deployment.

An SR-PCE is both a device and an SDN controller. Some deployments may want to treat an SR-PCE as a device, in which case they would need access via the device network. Some deployments may want to treat an SR-PCE as an SDN controller and access it on the Management routing domain. Both of these models are supported.

To enable Crosswork access to an SR-PCE as an SDN controller on the management domain (shown in the figure), just add an SR-PCE as a provider.

To enable Crosswork access to an SR-PCE as a device on the device network (not shown in figure), add an SR-PCE as a provider with an additional property: `outgoing-interface`:eth1.

Virtual Machine (VM) Requirements

You can deploy Cisco Crosswork Optimization Engine as a VM on a host that meets the following minimum requirements.

Note Although installation shows an option for IPv6, Cisco Crosswork Optimization Engine does not currently support IPv6 deployments at this time.

Table 1:

Requirement	Description
Hypervisor and vCenter	• VMware vCenter Server 6.7 Update 3b or later (ESXi 6.7 Update 1 installed on hosts). • VMware vCenter Server 6.5 Update 2d or later (ESXi 6.5 Update 2 installed on hosts) **Note** Installation should be done only from vCenter. Installation is not supported on ESXi directly.
Memory	96 GB
Storage	Storage requirements vary based on factors such as the number of devices being supported, and the type of deployment selected. For demos and lab environments, Cisco recommends the **thin provision** format as it requires the least amount of storage on the host machine. This deployment configuration uses roughly 23 GB of storage. For live systems, Cisco recommends the **Thick provision eager zeroed** format which allocates 1 TB of storage by default. This should be sufficient for most customer use cases. Due to their performance, solid state drives (SSD) are preferred over traditional hard disk drives (HDD). If you are using HDD, the minimum speed should be 10,000 RPM. For more information, see the volume requirements displayed in the VMware GUI when configuring disk space, as shown in Install Cisco Crosswork Optimization Engine , on page 20.
vCPU	16 vCPUs
CPU Planning (avoid overcommittment)	CPU/memory overcommitment occurs when the vCPUs are running on a host are more than the total number of physical processor cores in that host. VMware vCenter/ESXi allows this for the flexibility in deploying and running the VMs on physical hosts. It is natural to assume that the vCenter users will try to maximize the physical resources usage by deploying and running a reasonably high amount of VMs on a specific ESXi host. However, it can lead to a problem manifested in a "soft lockup" situation, where a VM will not be able to get a vCPU allocated in a reasonable amount of time.

Requirement	Description
Network Connections	For live deployments, Cisco recommends using dual interfaces, one for the management network and one for the data network between Cisco Crosswork Optimization Engine and Cisco Crosswork Data Gateway.
IP Addresses	Two IP addresses (IPv4): One public IP for the Management Network virtual interface and one public or private IP for the Data Network virtual interface.
NTP Servers	The IPv4 addresses or host names of the NTP servers you plan to use. If you want to enter multiple NTP servers, separate them with spaces. These should be the same NTP servers you use to synchronize devices, clients, and servers across your network. Confirm that the NTP servers are reachable on the network before attempting the install. The install will fail if the servers cannot be reached.
DNS Servers	The IPv4 addresses of the DNS servers you plan to use. These should be the same DNS servers you use to resolve host names across your network. Confirm that the DNS servers are reachable on the network before attempting the install. The install will fail if the servers cannot be reached.
DNS Search Domain	The search domain you want to use with the DNS servers (for example, `cisco.com`). You can only have one search domain.
Disclaimer	The text of the legal disclaimer displayed to clients accessing the VM via the command line. Consult your organization's IT or legal department for the content of this text.

Important Notes

- The VM runs Ubuntu Server 18.04.1 (ubuntu-18.04.1-server).

- Kubernetes runs within the Cisco Crosswork Optimization Engine VM and uses Docker for containerization. The number of containers varies as applications are added or deleted.

Cisco IOS XR Software Version Support

Cisco Crosswork Optimization Engine supports the following Cisco IOS XR software versions.

Table 2: Cisco IOS XR Software Versions

SR-PCE Software Version	PCC Software Version (Headend Routers)				
	Cisco ASR 9000	**Cisco NCS 5500 series**	**Cisco NCS 540 series**	**Cisco NCS 560 series**	**Cisco XRv 9000**
6.6.3 + SMU[1]	• 6.5.3 + SMU (CSCvp83001) • 6.6.3 + SMU See footnote 1	• 6.5.3 + SMU (CSCvp83001)[2] • 6.6.3 + SMU See footnote 1 and 2	6.6.3 + SMU [3] See footnote 1	6.6.3 + SMU See footnote 1	• 6.5.3 + SMU (CSCvp83001) • 6.6.3 + SMU See footnote 1

[1] 6.6.3 + SMU is needed to support RSVP-TE tunnel and updated SR policy features. SMU file is <platform-name>-6.6.3-Optima.tar.

[2] This SMU is available via the Cisco NCS 5508 Software Download Center.

[3] This SMU is available via the Cisco NCS 540-ACC-SYS Router or Cisco NCS 540x-ACC-SYS Router Software Download Center.

Note   Segment Routing Traffic Matrix (SRTM) is only available in Cisco ASR 9000 devices.

Software Maintenance Updates (SMUs) are required for both PCC/Headend and SR-PCE versions indicated in the table. To download the Cisco IOS XR versions and updates, see the IOS XR Software Maintenance Updates (SMUs) document. The correct SMUs to download will have "Optima" or the bug ID appended to the filename. For example:

- `asr9k-x64-6.6.3.Optima.tar`

- `asr9k-x64-6.5.3.CSCvp83001.tar`

Cisco NSO and NED Requirements

This is only applicable if Cisco Network Services Orchestrator is going to be used.

Software/Driver	Version
Cisco Network Services Orchestrator (Cisco NSO)	4.4.5.3
Cisco IOS XR Network Element Driver (NED)	6.6.1
Cisco IOS Network Element Driver	5.9.2

Device and TE Tunnel Scale Support

The following number of devices and TE tunnels (SR policies and RSVP-TE tunnels) are supported.

Table 3: Device and TE Tunnel (SR Policies and RSVP-TE Tunnels) Scale Support

Feature	Devices	TE Tunnels
SR Policy Visualization and Provisioning	• 5,000 nodes • 50,000 interfaces	2,000 SR Policies
RSVP-TE Tunnel (PCE initiated) Visualization and Provisioning	• 5,000 nodes • 50,000 interfaces	2,000 RSVP-TE Tunnels
RSVP-TE Tunnel (PCC initiated) Visualization only	• 5,000 nodes • 50,000 interfaces	2,000 RSVP-TE Tunnels
Bandwidth Optimization Function Pack	• 2,000 nodes • 20,000 interfaces	—
Bandwidth On Demand Function Pack (with Priority Mode)	• 5,000 nodes • 50,000 interfaces	—
Bandwidth On Demand Function Pack (without Priority Mode)	• 2,000 nodes • 20,000 interfaces	—
Demand Deduction Function Pack	500 nodes	—

IGP and Inter-AS

The following table captures the IGP and inter-AS features that Cisco Crosswork Optimization Engine supports.

Table 4: IGP and Inter-AS Support

Feature	OSPF	IS-IS	Inter-AS
Topology Visualization (including SR Policies)	Supported	Supported	Egress Peer Engineering (EPE) is limited to EPE adjacency segment IDs (SIDs)
SR Policy Creation, Modification, and Deletion	Supported	Supported	EPE is limited to EPE adjacency SIDs

Feature	OSPF	IS-IS	Inter-AS
Bandwidth on Demand Function Pack	Supported	Supported	Not Supported
Bandwidth Optimization Function Pack	Only single area is supported	Only single level is supported	Not Supported
RSVP TE	Supported	Supported	Supported with IGP between ASes but not EPE.

Table 5: RSVP-TE Tunnel Traffic Steering Configuration

Feature	Intra Area/Level	Inter Area/Level, Multiple IGP, Inter-AS
PCC Initiatied	Requires Autoroute Announce configuration in individual tunnel interface: `int tunnel-te <id> autoroute-announce exclude-traffic segment-routing`	Requires Static Route configuration pointing to the tunnel interface: `router static address-family ipv4 unicast <destination-ip> <tunnel-interface>`
PCE Initiatied	Requires Autoroute Announce configuration under MPLS TE: `mpls traffic-eng pcc stateful-client autoroute-announce`	

Supported Web Browsers

This version of Cisco Crosswork Optimization Engine supports the web browsers shown in the table below.

Recommended display resolution: 1600 x 900 pixels or higher (minimum: 1366 x 768).

Browser	Version
Google Chrome (recommended)	75 or later
Mozilla Firefox	70 or later

In addition to using a supported browser, all client desktops accessing geographical map information in the Cisco Crosswork Optimization Engine topology maps must be able to reach the mapbox.com map data URL directly, via the standard HTTPS port 443. Similar guidance may apply if you choose a different map data provider, as explained in "Configure Geographical Map Settings" in the *Cisco Crosswork Optimization Engine User Guide* .

Ports Used

As a general policy, any ports that are not needed should be disabled. To view a list of all open listening ports, log in as a Linux CLI admin user and run the **netstat -aln** command.

The following table lists the external ports that are open on the Cisco Crosswork Optimization Engine VM.

Table 6: External Ports That Are Open on the VM

Port	Protocol	Usage
22	TCP	Remote SSH traffic
323	UDP	Network Time Protocol (NTP) listener
30603	TCP	User interface (NGINX server listens for secure connections on port 443)
30607	TCP	To collect vitals from and download images to Cisco Crosswork Data Gateway
30649	TCP	To monitor Cisco Crosswork Data Gateway status.
30993	TCP	Cisco Crosswork Data Gateway sends the collected data to Crosswork Kafka destination.

The following table lists the destination ports on external devices that may be protected by a firewall. Cisco Crosswork Optimization Engine uses these ports to connect to network devices. You must open the required ports to allow Cisco Crosswork Optimization Engine to connect to these devices.

Table 7: Destination Ports Used by Cisco Crosswork Optimization Engine

Port	Protocol	Usage
7	TCP/UDP	Discover endpoints using ICMP
53	TCP/UDP	Connect to DNS
123	UDP	Network Time Protocol (NTP)
830	TCP	Initiate NETCONF

Collection Considerations

MDT Collection

When Cisco NSO is used in conjunction with Cisco Crosswork Optimization Engine, the telemetry configurations are pushed to the devices by Cisco NSO. To use Cisco NSO, it is important during installation to check the "Is NSO used as the provider for device management?" checkbox under Crosswork Collection Configuration (see Install Cisco Crosswork Optimization Engine , on page 20).

If you do not plan to use to use Cisco NSO, you must apply the telemetry configuration on your devices. See the "Prerequisites for Device Telemetry" topic in the *Cisco Crosswork Optimization Engine User Guide*.

> ✎
>
> **Note** The default MDT collector port is 9010.

Device Limits

Cisco Data Gateway collection supports 1000 devices. If your network requires collection of more than 1000 devices, multiple Cisco Data Gateways must be deployed.

Cisco Crosswork Data Gateway Installation Requirements

This section provides general guidelines and minimum requirements for installing Cisco Crosswork Data Gateway.

This section contains the following topics:

Virtual Machine (VM) Requirements

You can deploy Cisco Crosswork Data Gateway as a VM on a host that meets the following minimum requirements:

> ✎
>
> **Note**
> - Although Cisco Crosswork Data Gateway supports both IPv6 and IPv4, it is recommended to use IPv4 as Cisco Crosswork Optimization Engine supports only IPv4.
> - IPv4 on a single interface (demo mode) is not supported.

Requirement	
Hypervisor	• VMware vCenter 6.5 Update2d • VMware ESX 6.5 Update2 • VMware vCenter 6.7 Update1 • VMware ESX 6.7 Update1
Memory	32 GB
Disk space	50 GB **Note** This is the deployment size only. Once started, VM disk space will increase based on the VMware overhead.

Requirement	
vCPU	8 vCPUs

Interfaces	Three virtual interfaces in the VM:
	
	• One virtual interface for management network traffic, including SSH access to the VM. The DNS and NTP servers, and the default gateway, must be reachable via this interface.
	
	• One virtual interface for Northbound data traffic:
	
	    • The Cisco Crosswork Optimization Engine data interface must be reachable from this interface (routable) to be able to connect to Kafka data destinations.
	
	    • Cisco Crosswork Data Gateway uses this interface to receive collection jobs and send back their statuses to Crosswork.
	
	    • This interface is also used by external applications other than Cisco Crosswork Optimization Engine.
	
	• One virtual interface for Southbound data traffic. The devices must be reachable via this interface (routable).

IP Addresses	Three IPv4 or IPv6 addresses: One public IP for the management network virtual interface and two public or private IPs for the Northbound and Southbound data network virtual interfaces. The DNS and NTP servers, and the default gateway, must be reachable via the management network IP address. The data destinations must be reachable via Northbound data network IP address. The managed devices and providers must be reachable via Southbound data network IP address.
NTP Servers	The IPv4/IPv6 addresses or host names of the NTP servers you plan to use. If you want to enter multiple NTP servers, separate them with spaces. These should be the same NTP servers you use to synchronize devices, clients, and servers across your network. Confirm that the NTP IP address or host name is reachable on the network or installation will fail. Also, the ESXi hosts that will run the Cisco Crosswork Optimization Engine and Cisco Crosswork Data Gateway VM must have NTP configured, or the initial handshake may fail with "certificate not valid" errors.

Requirement	
DNS Servers	The IPv4/IPv6 addresses of the DNS servers you plan to use. These should be the same DNS servers you use to resolve host names across your network.
DNS Search Domain	The search domain you want to use with the DNS servers (for example, cisco.com). You can only have one search domain.
Destination Networks	For live deployments, we recommend one virtual switch for the Data Network (connection between the Cisco Crosswork Optimization Engine VM and the Cisco Crosswork Data Gateway VM) and second virtual switch for all the management traffic (vms to dns, ntp and the network you will use to access and manage the applications).

Note The VM runs Ubuntu Server 18.04.1 (ubuntu-18.04.1-server).

Supported Cisco OS

Note The below table lists only the software versions on which Cisco Crosswork Data Gateway 1.1 was tested. For OS software versions that only Cisco Crosswork Optimization Engine supports, please refer to Cisco IOS XR Software Version Support, on page 9. Cisco Crosswork Data Gateway allows you to expand device coverage by means of custom packages.

OS	Software Version	Config Mode	Protocol	Encoding	Transport
IOS-XR	6.4.1, 6.5.1, 6.5.2, 6.5.3, 6.6.2	NSO	MDT	KVGPB	TCP
	6.4.1, 6.5.3, 6.6.2	XR NED			
	6.5.1, 6.5.2, 6.5.3, 6.6.2	CLI 7.13.9			
	6.4.1, 6.4.2				
	7.0.1				
	6.4.2				
IOS-XE	16.10,		SNMP, CLI		
	16.9.2, 16.10				
NX-OS	7.0(3).7(2)				
	8.4(0).SK(1)				

Note
All collection types support IPv4. For any IPv4 and Day0 configs and limitations for different device platforms, please refer your network administrator and platform configuration guide.

Ports Used

As a general policy, any ports that are not needed should be disabled.

The following table shows the minimum set of ports needed for Cisco Crosswork Data Gateway to operate correctly.

Table 8: Ports to be Opened on Cisco Crosswork Data Gateway Management Interface

Port	Protocol	Used for...	Direction
22	TCP	SSH server	Inbound
22	TCP	SCP client	Outbound
123	UDP	NTP Client	Outbound
53	UDP	DNS Client	Outbound
30607	TCP	Crosswork Controller	Outbound

Table 9: Ports to be Opened on Cisco Crosswork Data Gateway Northbound Interface

Port	Protocol	Used for...	Direction
30649	TCP	Crosswork Controller	Outbound
30993	TCP	Crosswork Kafka	Outbound
Site Specific	Site Specific	Kafka and gRPC Destination	Outbound

Table 10: Ports to be Opened on Cisco Crosswork Data Gateway Southbound Interface

Port	Protocol	Used for...	Direction
161	UDP	SNMP Collector	Inbound
1062	UDP	SNMP TrapCollector	Inbound
9010	TCP	MDT Collector	Inbound
22	TCP	CLI Collector	Outbound

The Interface role to physical name mapping is:

- Management Interface: eth0

- Southbound Data Interface: eth1

- Northbound Data Interface: eth2

C H A P T E R 3

Installation Tasks

This section contains the following topics:

Installation Workflow

To set up Cisco Crosswork Optimization Engine and Cisco Crosswork Data Gateway complete the below installation tasks in the order of their listing:

Install Cisco Crosswork Optimization Engine

This section explains the procedure to install using vCenter.

Before you begin, ensure that:

- You are creating the Cisco Crosswork Optimization Engine VM on VMware ESXi 6.5 (Update 2 or later), and using the VMware vCenter Server 6.5 (Update 2d or later) or 6.7 (Update 3b).

  > **Note** VMware vCenter supports vSphere Web Client (flash mode) and vSphere Client (HTML5 mode), however vSphere Web Client (flash mode) is recommended for the Cisco Crosswork Optimization Engine VM deployment and is explained in this procedure. The vSphere Client (HTML5 mode) is supported only on VMware vCenter Server 6.7 Update 3b.

- You have a public IP address (IPv4) to assign to the Cisco Crosswork Optimization Engine VM's management network virtual interface. The default gateway must be reachable via this IP address.

  > **Note** It is preferred that the DNS and NTP servers are reachable via the Management Network Interface. However, it is not mandatory. The only requirement is that they are reachable on one of the network interfaces connected to the server.

- You have a public or private IP address (IPv4) to assign to the Cisco Crosswork Optimization Engine VM's data network virtual interface. This IP address must be able to reach the gateway address for the network where Cisco Crosswork Data Gateway will be installed.

- The NTP server you will use to synchronize the Cisco Crosswork Optimization Engine VM clock is reachable on the network.

> **Note** During the installation and first-time booting of the VM, the links to the specified gateways will be validated. VM configuration will fail if the links are inaccessible.

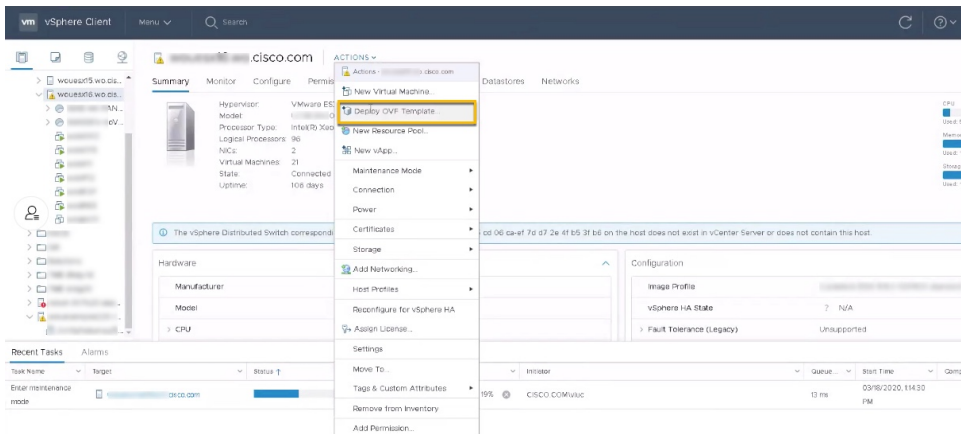Also during installation, Cisco Crosswork Optimization Engine creates two special administrative IDs:

1. The **virtual machine (VM) administrator**, with the username `cw-admin`, and the default password `cw-admin`. Data center administrators use this ID to log in to and troubleshoot the Cisco Crosswork Optimization Engine VM. You will use it to verify that the VM has been properly set up (see Verify the VM Configuration, on page 35).

2. The **Crosswork administrator**, with the username `admin` and the default password `admin`. Product administrators use this ID to log in to and configure the Cisco Crosswork Optimization Engine user interface, and to perform special operations, such as stopping and restarting services.

While this section describes installation, you must also set up Cisco SR-PCE in order to use Cisco Crosswork Optimization Engine. Refer to the appropriate device configuration guide (for example, Segment Routing Configuration Guide for Cisco ASR 9000 Series Routers).

Step 1   Download the latest available Cisco Crosswork Optimization Engine image file (*.ova) to your system.

> **Warning**   The default VMware vCenter deployment timeout is 15 minutes. The total time needed to deploy the OVA image file may take much longer than 15 minutes, depending on your network speed and other factors. If vCenter times out during deployment, the resulting VM will be unbootable. To prevent this, Cisco recommends that you either set the vCenter deployment timeout to a much longer period (such as one hour), or unTAR the OVA file before continuing and then deploy using the OVA's four separate Open Virtualization Format and Virtual Machine Disk component files: `cw.ovf`, `cw_rootfs.vmdk`, `cw_dockerfs.vmdk`, and `cw_extrafs.vmdk`.

Step 2   With VMware ESXi running, log in to the VMware vSphere Web Client. On the left side, choose the ESXi host on which you want to deploy the VM, then select **Actions** > **Deploy OVF Template**, similar to the following figure.

Step 3   The VMware **Deploy OVF Template** wizard appears and highlights the first step, **1 - Select template**, similar to the following figure. Click **Browse** to navigate to the location where you downloaded the OVA image file and select it. Once selected, the file name is displayed in the window.

Step 4   Click **Next** to go to **2 - Select name and location**, as shown in the following figure. Enter a name for the Cisco Crosswork Optimization Engine VM you are creating.

Cisco recommends that you include the Cisco Crosswork Optimization Engine version and build number in the name (for example: `CW Optimization Engine 1.1 Build 123`).

Step 5   Click **Next** to go to **3 - Select a resource**, similar to the following figure. Choose the Cisco Crosswork Optimization Engine VM's host.

Step 6   Click **Next**. The VMware vCenter Server validates the OVA. Network speed will determine how long validation takes. When validation is complete, the wizard moves to **4 - Review details**, similar to the following figure. Take a moment to review the OVF template you are deploying. Note that this information is gathered from the OVF and cannot be modified.

Step 7   Click **Next** to go to **5 - Accept license agreements**. Review the End User License Agreement and click on **Accept** before you continue.

Step 8   Click **Next** to go to **6 - Select configuration**, similar to the following figure. Select the desired deployment configuration (IPv4). IPv6 or an IPv4 network on a single interface is not currently supported.

Step 9   Click **Next** to go to **7 - Select Storage**, similar to the following figure. Select the relevant option from the **Select virtual disk format** drop-down list. From the table, choose the datastore you want to use and review its properties to ensure there is enough available storage.

> **Note**   For production deployment, choose **Thick provision eager zeroed** as it will preallocate disk space and provide the best performance. For development purposes, **Thin provision** is recommended as it saves disk space.

Step 10   Click **Next** to go to **8 - Select networks**, similar to the following figure. In the dropdown table at the top of the page, choose the appropriate destination network for the source **Data Network** and **Management Network**, respectively.

Deploy OVF Template

✔ 1 Select an OVF template
✔ 2 Select a name and folder
✔ 3 Select a compute resource
✔ 4 Review details
✔ 5 License agreements
✔ 6 Configuration
✔ 7 Select storage
8 Select networks
9 Customize template
10 Ready to complete

Select networks
Select a destination network for each source network.

Source Network	▼	Destination Network	▼
Data Network		VM Network	⌄
Management Network		VM Network	⌄

2 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL   BACK   NEXT

Step 11   Click **Next** to go to **9 - Customize template**.

Step 12   Expand the **Management Network** settings. According to your deployment configuration, the fields displayed are different, similar to the following figures. Make relevant entries for IPv4 deployment (**Management IPv4 Address**, **Management IPv4 Gateway**, and **Management IPv4 Netmask** fields).

Step 13   Expand the **Data Network** settings. According to your deployment configuration, the fields displayed are different, similar to the following figures. Make relevant entries for IPv4 deployment (**Data IPv4 Address**, **Data IPv4 Gateway**, and **Data IPv4 Netmask** fields) respectively.

Step 14 Expand the **DNS and NTP Servers** settings, similar to the following figure. According to your deployment configuration (IPv4), the fields displayed are different. Make entries in three fields:

- **DNS IP Address**: The IP addresses of the DNS servers you want the Cisco Crosswork Optimization Engine server to use. Separate multiple IP addresses with spaces.

- **DNS Search Domain**: The name of the DNS search domain.

- **NTP Servers**: The IP addresses or host names of the NTP servers you want to use. Separate multiple IPs or host names with spaces.

Note The DNS and NTP servers must be reachable via the network interfaces you have mapped on the host or the configuration of the VM will fail.

Step 15 **Disk Configuration** settings allows you to adjust the amount of storage space available to Cisco Crosswork Optimization Engine. The default settings should work for most environments. For assistance in adding additional storage, contact the Cisco Customer Experience team.

Step 16   Expand the **Crosswork Configuration** and enter any legal disclaimer text (users will see this text if they log into the CLI).

Step 17   Expand the **Crosswork Collection Configuration** settings, similar to the following figure.

Check this option if you plan to use Cisco NSO. For more guidance and information on which mode to select, see Collection Considerations, on page 13).

Step 18 Click **Next** to go to **10 - Ready to Complete**, similar to the following figure (template name will depend on the version you are installing). Review your settings and then click **Finish** if you are ready to begin deployment.

Step 19   Wait for the deployment to finish before continuing. To check on the deployment status:

a)   Open a VMware vCenter client.

b)   In the **Recent Tasks** tab for the host VM, view the status for the **Deploy OVF template** and **Import OVF package** jobs.

Step 20   After the deployment tasks are complete, check the host's VM settings to permit boot from EFI Firmware:

a)   On the host VM **Summary** tab, below the **VM Hardware** table, click **Edit Settings**, similar to the following figure.
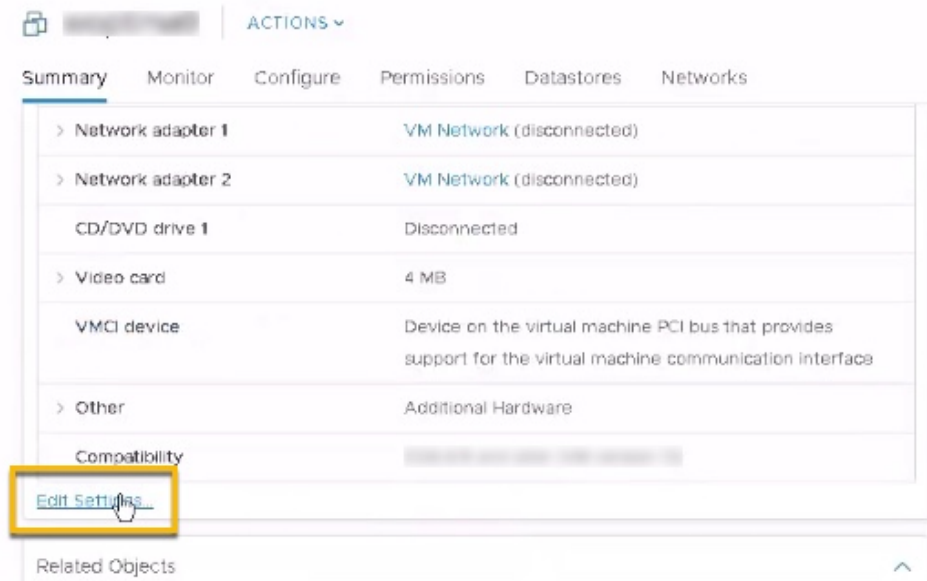
b)   On the **Edit Settings** page, click the **VM Options** tab.

c)   Expand the **Boot Options** dropdown list and change the **Firmware** setting to **EFI**, if it not set by default. When you are finished, click **OK**. You may want to take a snapshot of the VM at this point.
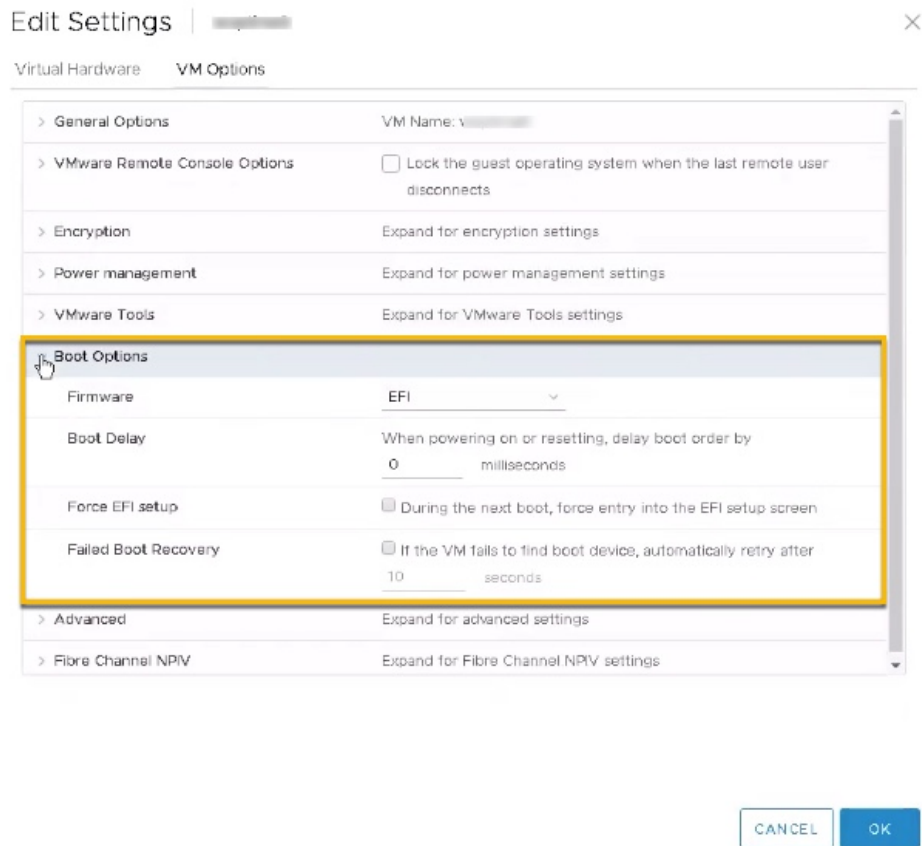
Step 21   You can now power on the Cisco Crosswork Optimization Engine VM to complete the deployment process. Expand the host's entry so you can click the Cisco Crosswork Optimization Engine VM and then choose **Actions** > **Power** > **Power On**, similar to the following figure.

Figure 2: Power On
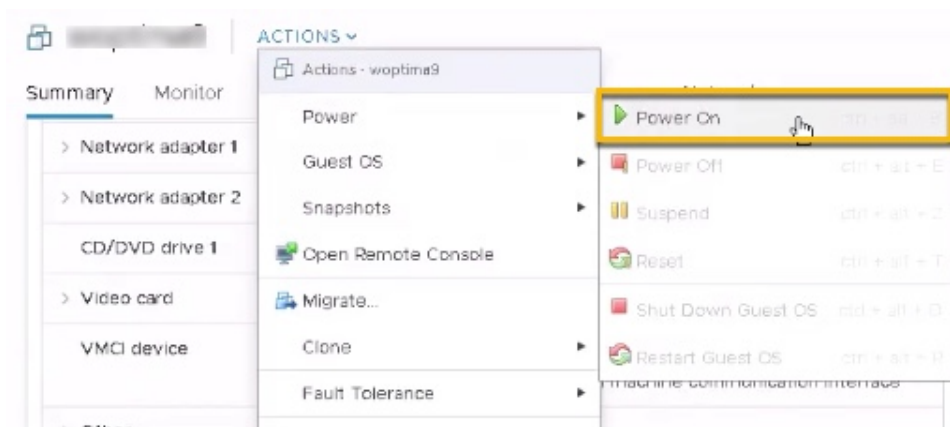
From this point, it will take 20 minutes for the Cisco Crosswork Optimization Engine VM to become operational. Please wait for the process to finish before continuing.

Verify the VM Configuration

Before trying to log in to the new installation, verify that the VM is properly configured. You will be prompted to change the VM administrator's password during first login via the console.

Step 1   After the VM is powered on, wait for 20 minutes, and then launch the console.

Step 2   In the password prompt, enter the default cw-admin user password, **cw-admin**. When prompted to change the cw-admin user's password, enter the default password again for verification. Then enter and confirm the new password as prompted.

Step 3   If you see instructions to check `firstBoot.log`, use the command `sudo cat /var/log/firstBoot.log` to view the log file. If you find any discrepancy and want to investigate further, refer to Troubleshoot the Installation, on page 36. After you have identified the error, perform the following:

a) Power off the Cisco Crosswork Optimization Engine VM.

b) Delete the Cisco Crosswork Optimization Engine VM from the disk.

c) Repeat the installation procedure, while rectifying the error(s) that prevented the installation from completing.

d) Launch the console (go to step 1).

Log In to the UI From a Browser

To log in to the Cisco Crosswork Optimization Engine web-based user interface from a browser, perform these steps. If you are unable to display the user interface, see Troubleshoot the Installation, on page 36.

Step 1   Launch one of the supported browsers (see Supported Web Browsers).

Step 2   In the browser's address bar, enter:

https://<Crosswork_VM_management_IP_adddress>:30603/

The **Log In** window opens.

When you access Cisco Crosswork Optimization Engine for the first time, some browsers display a warning that the site is untrusted. When this happens, follow the prompts to add a security exception and download the self-signed certificate from the Cisco Crosswork Optimization Engine server. After you add a security exception, the browser accepts the server as a trusted site in all future login attempts. If you want to use a CA signed certificate, see the "Manage Certificates"section in the *Cisco Crosswork Optimization Engine User Guide*.

Step 3   Log into Cisco Crosswork Optimization Engine as follows:

a) Enter the Cisco Crosswork Optimization Engine administrator username **admin** and the default password **admin**.

b) Click **Log In**.

c) When prompted to change the Cisco Crosswork Optimization Engine administrator's default password, enter the new password in the fields provided and then click **OK**.

Step 4 To exit the web GUI, close the browser window or click ● at the top right of the home page and choose **Log out**.

Troubleshoot the Installation

The following table lists common problems experienced while installing Cisco Crosswork Optimization Engine, and approaches to identifying the source of the problem and solving it.

Note You need to login as a super user to perform the troubleshooting.

Table 11: Troubleshoot the Installation

Issue	Action
Cannot Connect to the VM	
VM cannot be reached by the provided gateways due to IP misconfiguration	1. You will see error messages in the login banner indicating this problem when you try to connect to the VM via SSH following the steps in as explained in Verify the VM Configuration, on page 35.
	2. Redeploy the VM from scratch, using the correct IP configuration.
Configure NTP after installation	

User wants to configure NTP after the VM deployment, in the scenario of giving the wrong NTP address, or the server being down.	1. You need to edit the `/etc/chrony/chrony.conf` file. Add the pool line at the bottom of the file with relevant NTP server details.
	
	```keyfile /etc/chrony/chrony.keys```
	```driftfile /var/lib/chrony/chrony.drift```
	```logdir /var/log/chrony```
	```maxupdateskew 100.0```
	```rtcsync```
	```makestep 1 -1```
	```pool <ntp address> iburst maxsources 1```
	
	2. Restart the `chronyd` service (`systemctl restart chronyd`).
	
	3. Please verify that the NTP server has been configured (`chronyc sources`).

Cannot Display the User Interface	

Issue	Action
Browser does not display the login screen.	1. Make sure you are using a supported browser (see Supported Web Browsers, on page 12 and that you entered the correct IP address in the browser (this should be the same as the management IP4 address and port number (30603) you entered during installation).
	2. Log in to the VM using SSH, as explained in Verify the VM Configuration, on page 35.
	3. At the prompt, enter the command **collect**. This generates a file.
	4. Open a ticket with the Cisco Customer Experience team and attach the file to the ticket.
Unable to resolve other network addresses on the local network.	1. While connected to the VM, open the file `/etc/resolv.conf` file and check that it contains the correct DNS name server and search domain.
	2. If it does not, redeploy the VM using the correct DNS name server and search domain configuration.
Running `kubectl get nodes` does not display the correct VM management IP address.	1. While connected to the VM, open the file `/etc/hosts` file and check if the IP address assigned to the VM is correct.
	2. If the address is wrong, redeploy the VM using the correct management IP address.
Running `kubectl get nodes` does not display a `Ready` status for the VM IPv4 address.	1. While connected to the VM, check the login banner for any error messages.
	2. If there are error messages in the login banner, they will be recorded in `/var/log/firstBoot.log` file, along with recommended remediation steps. Open the log and follow the steps given for the error message found in the banner.
	3. If this does not help, run `kubectl get pods --namespace kube-system` and look for mismatched `Ready` counts.
Running `kubectl get pods --namespace kube-system` displays one or more system containers that are not in `Running` status.	1. Check for user input errors in the `/var/log/boot.log` file and perform the log's recommended remediation steps.
	2. If this does not help, please contact the Cisco Customer Experience team.
Running `kubectl get pods` displays one or more system containers that are not launched properly.	Please contact the Cisco Customer Experience team.
Able to Display the User Interface	

Issue	Action
I cannot log in.	1. Make sure you are using the Crosswork administrator default user ID and password (**admin** and **admin**). 2. If the Crosswork administrator default password has already been changed, use the new password.
I can log in but cannot access some features.	Make sure all the applications and their underlying services are up and running by selecting **Admin** > **Crosswork Manager** and checking the status of the applications and services. See the *Cisco Crosswork Optimization Engine User Guide* topic "Monitor Cisco Crosswork Infrastructure and Resources".
Crosswork Manager shows one or more applications or their underlying services are not running.	1. In Crosswork Manager, check the description of the application or service issue and, if possible, try restarting the application or service. See the *Cisco Crosswork Optimization Engine User Guide* topic "Monitor Cisco Crosswork Infrastructure and Resources". 2. Gather log and metric information about the application or service with issues. See the *User Guide* topic "View, Control and Log Cisco Crosswork Applications and Services". 3. Contact Cisco Customer Experience team.
CPU Overcommitment	
CPU/memory overcommitment occurs when the vCPUs are running on a host are more than the total number of physical processor cores in that host. VMware vCenter/ESXi allows this for the flexibility in deploying and running the VMs on physical hosts. It is natural to assume that the vCenter users will try to maximize the physical resources usage by deploying and running a reasonably high amount of VMs on a specific ESXi host. However, it can lead to a problem manifested in a "soft lockup" situation, where a VM will not be able to get a vCPU allocated in a reasonable amount of time.	1. Perform an analysis to confirm that an overcommitment has led to the manifested problem. The vSphere ESXi host Monitor screens have a **Performance** > **Advanced** tab which can display several views and performance counters to illustrate. For example, CPU usage in MHz displays the spike in CPU usage at a particular date and time compared to the average usage. 2. After you confirm the analysis, use a CPU or Memory reservation to resolve an overcommitment. The CPU reservation specifies the CPU allocation (in MHz) for your VM, while Memory reservation specifies the guaranteed minimum allocation for a VM (in MB). If the reservation is not met, the VM cannot be turned on.

Install Cisco Crosswork Data Gateway

Cisco Crosswork Data Gateway is initially deployed as a VM called Base VM (containing only enough software to register itself with Crosswork).

Before installing Cisco Crosswork Data Gateway, it is helpful to be familiar with Cisco Crosswork Data Gateway OVF Parameters and Deployment Scenarios, on page 39.

You can use either of the following two ways to install Cisco Crosswork Data Gateway:

- Install Cisco Crosswork Data Gateway Via vCenter, on page 45
- Install Cisco Crosswork Data Gateway Via OVF Tool, on page 56

Cisco Crosswork Data Gateway OVF Parameters and Deployment Scenarios

Before you begin installing Cisco Crosswork Data Gateway, read below about OVF parameters and possible deployment scenarios.

Note
- Mandatory parameters are denoted by an *. Others are optional. You might choose them based on the kind of deployment scenrio you require. Deployment scenarios are explained wherever applicable.

- Although Cisco Crosswork Data Gateway supports both IPv6 and IPv4, it is recommended to use IPv4 as Cisco Crosswork Optimization Engine supports only IPv4.

OVF Parameter	Description	Deployment Scenario
Host Information		
Hostname*	Hostname of the server specified as a fully qualified domain name (FQDN). **Note** For larger systems it is likely that you will have more than one Cisco Crosswork Data Gateway instance. The Cisco Crosswork Data Gateway hostname should, therefore, be unique and created in a way that makes identifying a specific instance easy.	
Description*	A detailed description of the Cisco Crosswork Data Gateway instance.	

OVF Parameter	Description	Deployment Scenario
Label	Label used by Crosswork to categorize and group multiple Cisco Crosswork Data Gateway instances.	
Private Key URI	SCP URI to private key file for session key signing. You can retrieve this using SCP (user@host:path/to/file).	Crosswork uses self-signed certificates for handshake with Cisco Crosswork Data Gateway. These certificates are generated upon installation.
Certificate File URI	SCP URI to PEM formatted signing certificate chain for this VM. You can retrieve this using SCP (user@host:path/to/file).	However, if you want to use third-party or your own certificate files, then you must input these three parameters.
Certificate File and Key Passphrase	SCP user passphrase to retrieve the Cisco Crosswork Data Gateway PEM formatted certificate file and private key.	**Note** The host with the URI files must be reachable on the network and files must be present at the time of install.
Passphrases		
dg-admin Password[*]	The password you have chosen for the dg-admin user.	
dg-oper Password[*]	The password you have chosen for the dg-oper user.	
Note *For Management, Southbound, and Northbound interfaces, Cisco Crosswork Data Gateway supports both IPv4 and IPv6. For the protocol you choose to use, select **Method** as **Static** and enter information in **Address**, **Netmask**, and **Gateway** fields. Also, for the protocol you are not using, set **Method** as **none** and leave **Address**, **Netmask**, and **Gateway** fields blank.*		
[1]**Management IPv4 Address**		
Management IPv4 Method[*]	How the management interface gets its IPv4 address.	
Management IPv4 Address	IPv4 address of the management interface.	
Management IPv4 Netmask	IPv4 netmask of the management interface in dotted quad format.	
Management IPv4 Gateway	IPv4 address of the management gateway.	
[1]**Management IPv6 Address**		

OVF Parameter	Description	Deployment Scenario
Management IPv6 Method[*]	How the Management interface gets its IPv6 address.	
Management IPv6 Address	IPv6 address of the management interface.	
Management IPv6 Netmask	IPv6 prefix of the management interface.	
Management IPv6 Gateway	IPv6 address of the management gateway.	
[1]**Southbound Data IPv4 Address**		
Southbound Data IPv4 Method[*]	How the southbound data interface gets its IPv4 address.	
Southbound Data IPv4 Address	IPv4 address of the southbound data interface.	
Southbound Data IPv4 Netmask	IPv4 netmask of the southbound data interface in dotted quad format.	
Southbound Data IPv4 Gateway	IPv4 address of the southbound Cisco Crosswork Data Gateway.	
[1]**Southbound Data IPv6 Address**		
Southbound Data IPv6 Method[*]	How the southbound data interface gets its IPv6 address.	
Southbound Data IPv6 Address	IPv6 address of the southbound data interface.	
Southbound Data IPv6 Netmask	IPv6 netmask of the southbound data interface in dotted quad format.	
Southbound Data IPv6 Gateway	IPv6 address of the southbound data gateway.	
[1]**Northbound Data IPv4 Address**		
Northbound Data IPv4 Method[*]	How the Northbound data interface gets its IPv4 address.	
Northbound Data IPv4 Address	IPv4 address of the Northbound data interface.	
Northbound Data IPv4 Netmask	IPv4 netmask of the Northbound data interface in dotted quad format.	

OVF Parameter	Description	Deployment Scenario
Northbound Data IPv4 Gateway	IPv4 address of the Northbound data gateway.	
[1]**Northbound Data IPv6 Address**		
Northbound Data IPv6 Method[*]	How the Northbound data interface gets its IPv6 address.	
Northbound Data IPv6 Address	IPv6 address of the Northbound data interface.	
Northbound Data IPv6 Netmask	IPv6 netmask of the Northbound data interface in dotted quad format.	
Northbound Data IPv6 Gateway	IPv6 address of the Northbound data gateway.	
DNS and NTP		
DNS Address[*]	Space-delimited list of IPv4/IPv6 addresses of the DNS server accesible from the management interface.	
DNS Search Domain[*]	DNS search domain	
NTP Servers[*]	Space-delimited list of IPv4/IPv6 addresses or hostnames of the NTP servers accessible from the management interface.	You must enter a value here, such as pool.ntp.org. NTP server is important for time synchronization between Cisco Crosswork Data Gateway VM and Cisco Crosswork Optimization Engine. Using a non-functional or dummy address may cause issues when Crosswork and Cisco Crosswork Data Gateway try to communicate with each other. If you are not using an NTP server, ensure that time gap between Cisco Crosswork Data Gateway and Cisco Crosswork Optimization Engine is not more than 10 minutes. Else, Cisco Crosswork Data Gateway will fail to pull images.
Syslog Servers		

OVF Parameter	Description	Deployment Scenario
Server Address	IPv4 or IPv6 address of a syslog server accessible from the management interface. **Note** If you are using an IPv6 addres, it must be surrounded by square brackets ([1::1]).	If you want to use an external syslog server, you must specify these 7 settings. **Note** If you have configured an external syslog server, the service (CLI/MDT/SNMP) events are sent to that external syslog server. Otherwise, they are logged in `/optdg/log` in Cisco Crosswork Data Gateway VM. **Note** The host with the URI files must be reachable on the network and files must be present at the time of install.
Syslog Port	Port number of the syslog server.	
Syslog Protocol	Use UDP, TCP, or RELP when sending syslog.	
Use Syslog over TLS?	Use TLS to encrypt syslog traffic.	
TLS Peer Name	Syslog server's hostname exactly as entered in the server certificate SubjectAltName or subject common name.	
Syslog Root Certificate File URI	PEM formatted root cert of syslog server retrieved using SCP.	
Syslog Certificate File Passphrase	Password of SCP user to retrieve Syslog certificate chain.	
Controller Settings		
Controller IP[*]	IP address of the Crosswork controller i.e., Cisco Crosswork Optimization Engine. **Note** If you are using an IPv6 address, it must be surrounded by square brackets ([1::1]).	
Controller Port[*]	Port of the Crosswork controller i.e., Cisco Crosswork Optimization Engine.	

OVF Parameter	Description	Deployment Scenario

Controller Signing Certificate File URI	PEM formatted root cert of Cisco Crosswork Optimization Engine to validate signing certs retrived using SCP. PEM file is generated by Crosswork and is available at the following location:
	
	`cw-admin@<Crosswork_VM_Management_IP_Address>`
	`:/home/cw-admin/controller.pem`
	
	Note Theoretically, it can be placed on any host where the SCP server is running but best practice is uploading from Crosswork, directly.	

SSL/TLS Certificate File URI	Crosswork controller PEM formatted SSL/TLS certificate file retrieved using SCP.	
Controller Certificate File Passphrase	Password of SCP user to retrieve Cisco Crosswork Optimization Engine certificate chain.	
Proxy Server URL	URL of management network proxy server.	If you want to use a proxy server, you must specify these parameters.
Proxy Server Bypass List	Space-delimited list of subnets and domains that will not be sent to the proxy server.	
Authenticated Proxy Username	Username for authenticated proxy servers.	
Authenticated Proxy Passphrase	Passphrase for authenticated proxy servers.	
HTTPS Proxy SSL/TLS Certificate File URI	HTTPS proxy PEM formatted SSL/TLS certificate file retrieved using SCP.	
HTTPS Proxy SSL/TLS Certificate File passphrase	Password of SCP user to retrieve proxy certificate chain.	
Auto Enrollment Package		

OVF Parameter	Description	Deployment Scenario
Enrollment Destination Host and Path	SCP host and path to transfer the enrollment package using SCP (`user@host:/path/to/file`).	Enrollment package is required for enrolling Cisco Crosswork Data Gateway with Crosswork. The enrollment package is automatically transferred once Cisco Crosswork Data Gateway boots up for the first time if you specify these parameters during the installation.
Enrollment Passphrase	SCP user passphrase to transfer enrollment package.	If you do not specify these parameters during installation, then you must export enrollment package manually following the procedure Export Enrollment Package, on page 61. **Note:** • The host must run SCP server. If no alternative SCP server is available, then Crosswork can be used. An example URI is given below: `cw-admin@<Crosswork_VM_ Management_IP_ Address> :/home/cw-admin`

[1]Either an IPv4 or IPv6 address must be specified. Selecting None for both will result in a non-functional deployment.

Install Cisco Crosswork Data Gateway Via vCenter

Before you begin

✎ **Note** Although Cisco Crosswork Data Gateway supports both IPv6 and IPv4, it is recommended to use IPv4 as Cisco Crosswork Optimization Engine supports only IPv4.

Ensure the following:

- You are creating the Cisco Crosswork Data Gateway VM on a recommended VMware version (See Virtual Machine (VM) Requirements, on page 14 for supported versions). To know which vCenter build you have, check on the vSphere web client under **Help** menu.

- The Cisco Crosswork Data Gateway VM has allocated to it a minimum of 32 GB of RAM, 8 vCPUs, and 50 GB of hard drive space.

- You have a public/private IPv4/IPv6 address to assign to the Cisco Crosswork Data Gateway VM's management network virtual interface. The DNS servers, NTP servers, and the Crosswork application must be reachable via this IP address.

- You have two public or private IPv4/IPv6 addresses to assign to the Cisco Crosswork Data Gateway VM's Northbound and Southbound data network virtual interfaces. Your managed devices must be reachable via the Southbound data network interface and your output destinations (either Crosswork, external Kafka, or gRPC server) must be reachable via the Northbound data network interface.

During installation, Cisco Crosswork Data Gateway creates two default accounts:

1. A **Cisco Crosswork Data Gateway administrator**, with the username **dg-admin** and password set during installation. The product administrator uses this ID to log in to and troubleshoot the Cisco Crosswork Data Gateway.

2. A **Cisco Crosswork Data Gateway operator**, with the username **dg-oper** and password set during installation. This is a read-only user and has permissions to perform all 'read' operations and some limited 'action' commands. To know what operations can an operator perform, see *Table: Permissions Per Role* in the *Cisco Crosswork Optimization Engine 1.1 User Guide*.

Note These two pre-defined usernames are reserved and cannot be changed.

Change of password would be allowed from the console for both the accounts.

In case of lost or forgotten passwords, the user would have to create a new VM, destroy the current VM, and re-enroll the new one on the Cisco Crosswork Optimization Engine.

Step 1 Download the Cisco Crosswork Data Gateway 1.1.0 image file from CCO (*.ova).

Note Crosswork Optimization Engine is designed and tested to be used with only the Cisco Crosswork Data Gateway 1.1.0 release.

Warning The default VMware vCenter deployment timeout is 15 minutes. If the time taken to fill the OVF template exceeds 15 minutes, vCenter times out and you will have to start over again. To prevent this, Cisco recommends that you set the vCenter deployment timeout to a much longer period (such as one hour). Refer your vCenter guide.

Step 2 Connect to vCenter vSphere Client. Then select **Actions** > **Deploy OVF Template**, as shown in the following figure:
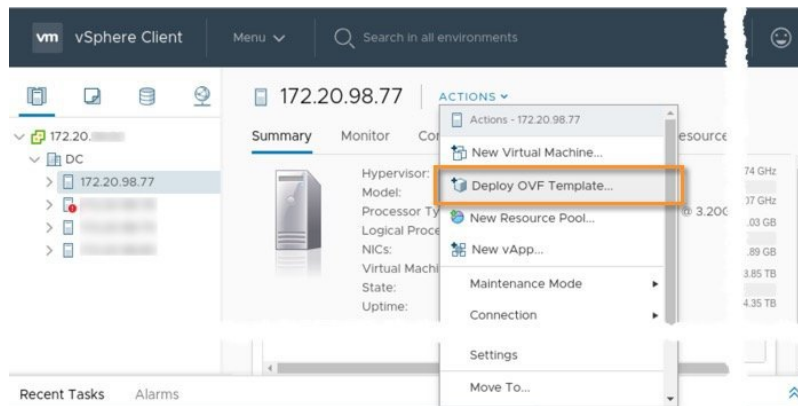
Step 3   The VMware **Deploy OVF Template** wizard appears and highlights the first step, **1 Select template**, as shown in the following figure.
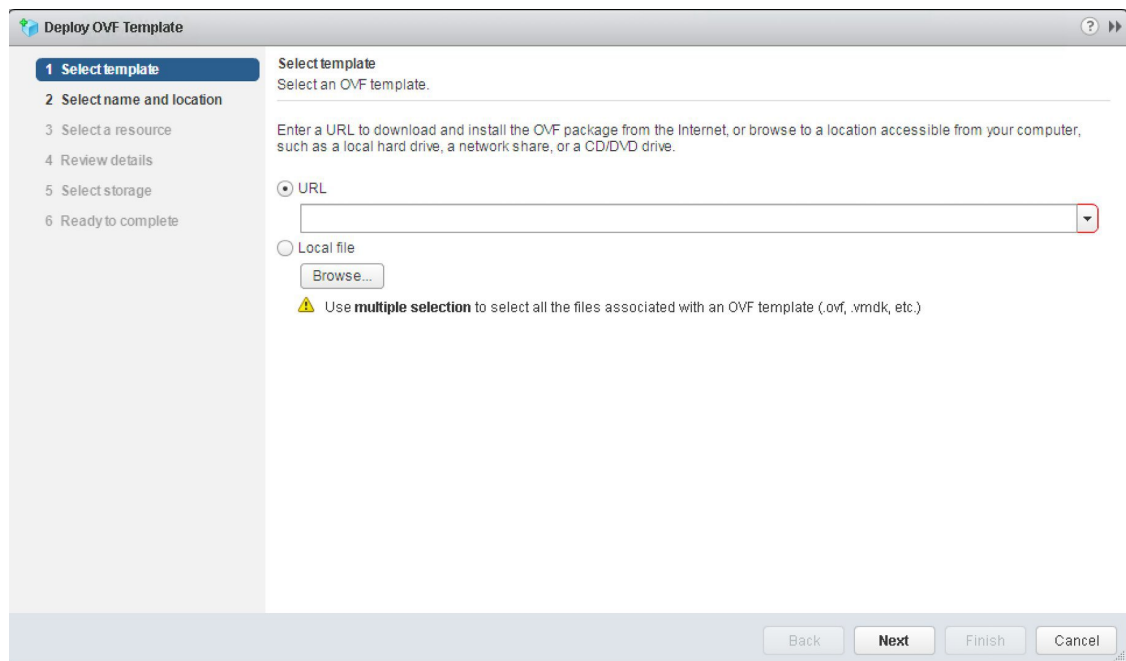
a) Click **Browse** to navigate to the location where you downloaded the OVA image file and select it.

Once selected, the filename is displayed in the window.

Step 4   Click **Next** to go to **2 Select name and location**, as shown in the following figure.

a) Enter a name for the Cisco Crosswork Data Gateway VM you are creating.

b) In the **Select a location for the virtual machine** list, choose the datacenter under which the Cisco Crosswork Data Gateway VM will reside.
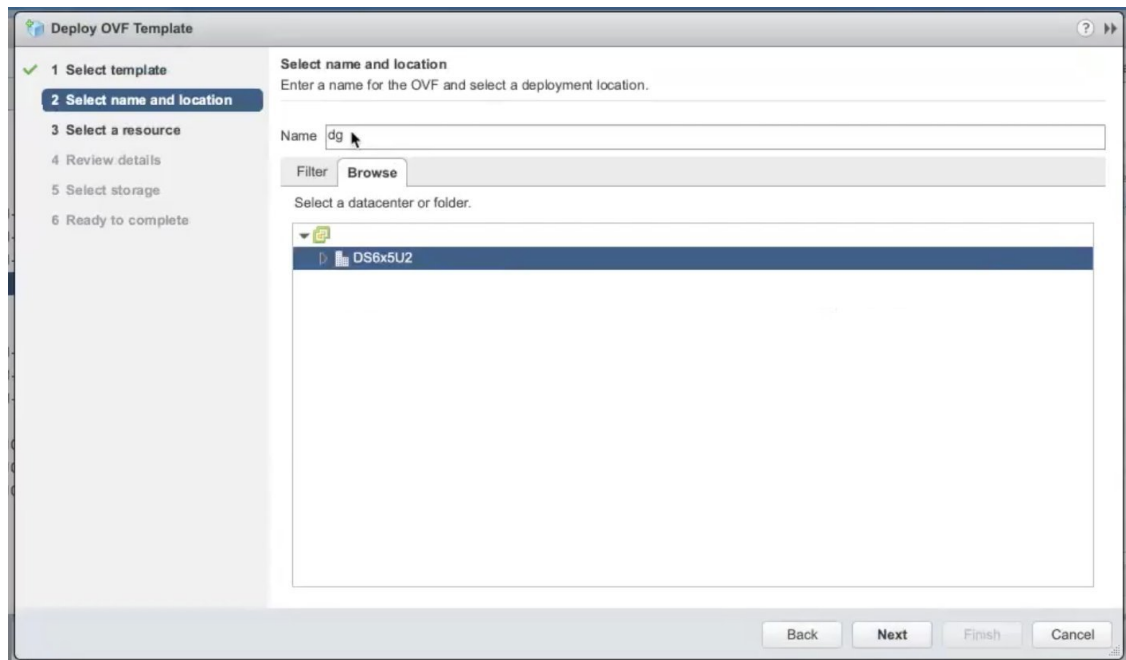
Step 5   Click **Next** to go to **3 Select a resource**, as shown in the following figure. Choose the VM's host.
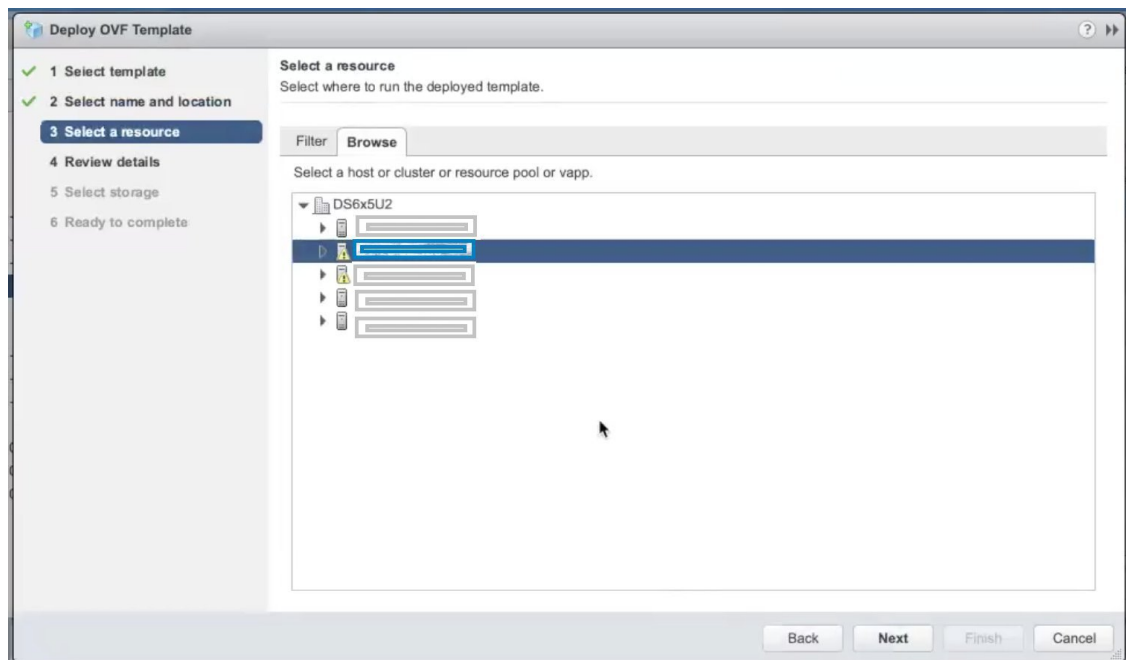
Step 6   Click **Next**. The VMware vCenter Server validates the OVA. Network speed will determine how long validation takes. When the validation is complete, the wizard moves to **4 Review details**, as shown in the following figure. Review the OVA's information and then click **Next**.

Take a moment to review the OVF template you are deploying.

Note   This information is gathered from the OVF and cannot be modified.
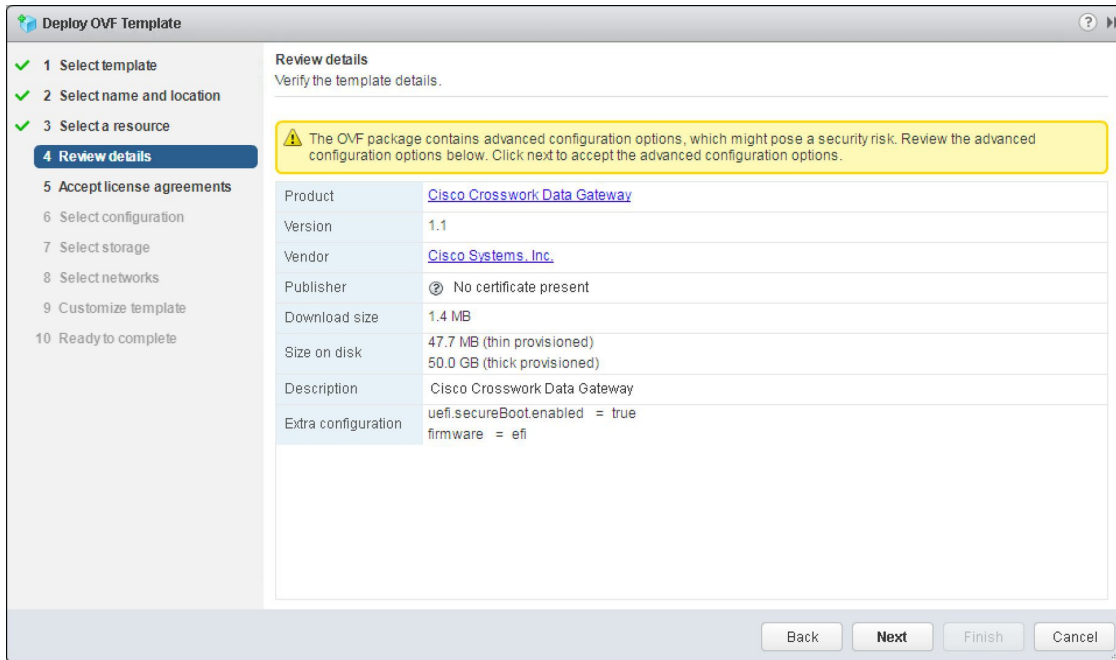
Step 7   Click **Next** to go to **5 accept license agreements**. Review the End User License Agreement and click **Accept**.
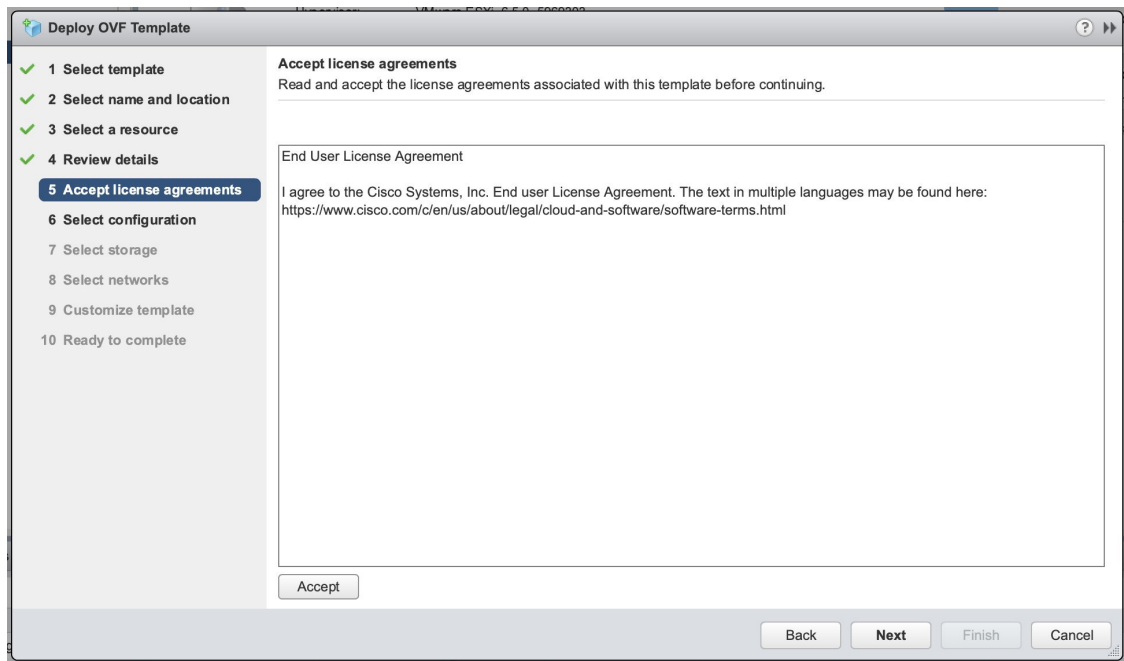
Step 8   Click **Next** to go to **6 Select configuration**, as shown in the following figure. To install Cisco Crosswork Data Gateway for Cisco Crosswork Optimization Engine, you must select **Crosswork On Premise** from the **Configuration** dropdown.
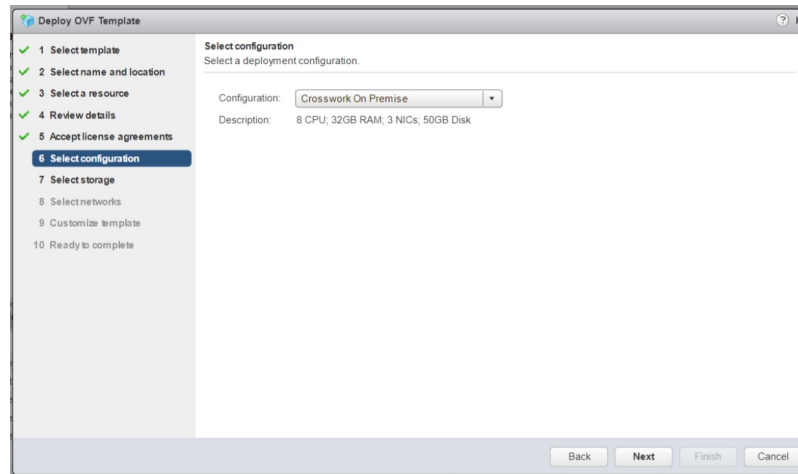
Step 9   Click **Next** to go to **7 Select storage**, as shown in the following figure.

a) Cisco recommends that you select **Thick provision lazy zeroed** from the **Select virtual disk format** drop-down list.

b) From the **Datastores** table, choose the datastore you want to use and review its properties to ensure there is enough available storage.
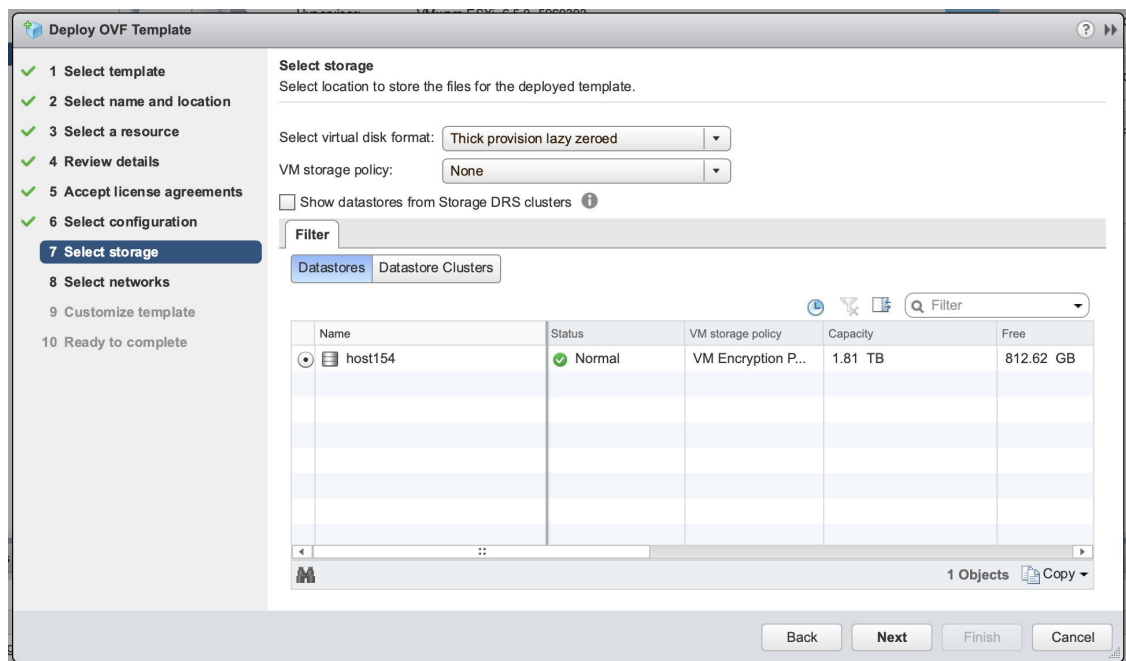
Step 10   Click **Next** to go to **8 Select networks**, as shown in the following figure. In the dropdown table at the top of the page, choose the appropriate destination network for the source **Management Network**, **Northbound Data Network**, and **Southbound Data Network** respectively.
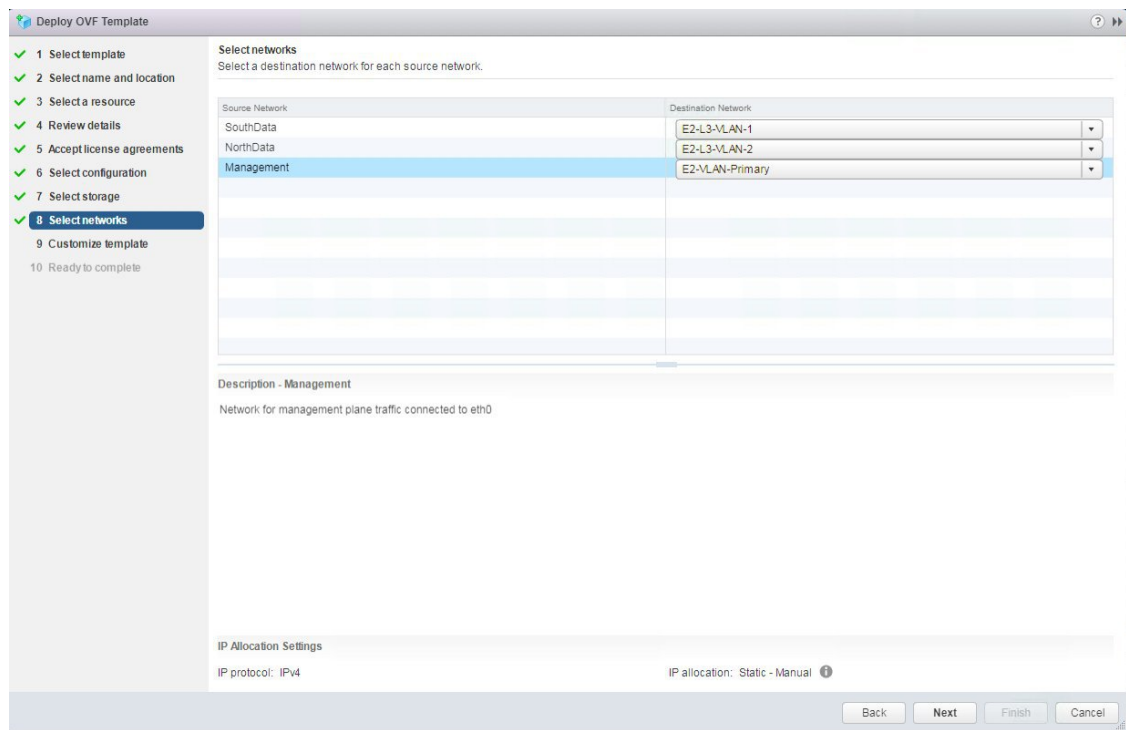
Step 11 Click **Next** to go to **9 Customize template**, with the **Host Information Settings** already expanded. As per the deployment scenario chosen by you in Section: Cisco Crosswork Data Gateway OVF Parameters and Deployment Scenarios, on page 39, enter the information for the parameters:

Note • Certificate chains override any preset or generated certificates in the VM and are given as an SCP URI (user:host:/path/to/file).

a) **Host Information**

- Hostname: Hostname of the server specified as a fully qualified domain name (FQDN).

  Note For larger systems it is likely that you will have more than one Cisco Crosswork Data Gateway instance. The Cisco Crosswork Data Gateway hostname should, therefore, be unique and created in a way that makes identifying a specific instance easy.

- Description:A detailed description of the Cisco Crosswork Data Gateway instance.

- Label: Label used by Crosswork to categorize and group multiple Cisco Crosswork Data Gateway instances.

- Private Key URI: SCP URI to private key file for session key signing. You can retrieve this using SCP (user@host:path/to/file).

- Certificate File URI: SCP URI to PEM formatted signing certificate chain for this VM. You can retrieve this using SCP (user@host:path/to/file).

- Certificate File and Key Passphrase: SCP user passphrase to retrieve the Cisco Crosswork Data Gateway PEM formatted certificate file and private key.

b) **Passphrases**

- dg-admin Password: The password you have chosen for the dg-admin user.

- dg-oper Password: The password you have chosen for the dg-oper user.

Note *For Management, Southbound, and Northbound interfaces, Cisco Crosswork Data Gateway supports both IPv4 and IPv6. For the protocol you choose to use, select **Method** as **Static** and enter information in **Address**, **Netmask**, and **Gateway** fields. Also, for the protocol you are not using, set **Method** as **none** and leave **Address**, **Netmask**, and **Gateway** fields blank.*

c) **Management IPv4 Address**

- Management IPv4 Method: How the Management interface gets its IPv4 address.

- Management IPv4 Address: IPv4 address of the Management interface.

- Management IPv4 Netmask: IPv4 netmask of the Management interface in dotted quad format.

- Management IPv4 Gateway: IPv4 address of the Management gateway.

d) **Management IPv6 Address**

- Management IPv6 Method: How the Management interface gets its IPv6 address.

- Management IPv6 Address: IPv6 address of the Management interface.

- Management IPv6 Netmask: IPv6 netmask of the Management interface in dotted quad format.

- Management IPv6 Gateway: IPv6 address of the Management gateway.

e) **Southbound Data IPv4 Address**

- Southbound Data IPv4 Method: How the Southbound data interface gets its IPv4 address.

- Southbound Data IPv4 Address: IPv4 address of the Southbound data interface.

- Southbound Data IPv4 Netmask: IPv4 netmask of the Southbound data interface in dotted quad format.

- Southbound Data IPv4 Gateway: IPv4 address of the Southbound data gateway.

f) **Southbound Data IPv6 Address**

- Southbound Data IPv6 Method: How the Southbound data interface gets its IPv6 address.

- Southbound Data IPv6 Address: IPv6 address of the Southbound data interface.

- Southbound Data IPv6 Netmask: IPv6 netmask of the Southbound data interface in dotted quad format.

- Southbound Data IPv6 Gateway: IPv6 address of the Southbound data gateway.

g) **Northbound Data IPv4 Address**

- Northbound Data IPv4 Method: How the Northbound data interface gets its IPv4 address.

- Northbound Data IPv4 Address: IPv4 address of the Northbound data interface.

- Northbound Data IPv4 Netmask: IPv4 netmask of the Northbound data interface in dotted quad format.

- Northbound Data IPv4 Gateway: IPv4 address of the Northbound data gateway.

h) **Northbound Data IPv6 Address**

- Northbound Data IPv6 Method: How the Northbound data interface gets its IPv6 address.

- Northbound Data IPv6 Address: IPv6 address of the Northbound data interface.

- Northbound Data IPv6 Netmask: IPv6 netmask of the Northbound data interface in dotted quad format.

- Northbound Data IPv6 Gateway: IPv6 address of the Northbound data gateway.

i) **DNS and NTP**

- DNS Address: Space-delimited list of IPv4/IPv6 addresses of the DNS server accesible from the management interface.

- DNS Search Domain: DNS search domain

- NTP Servers: Space-delimited list of IPv4/IPv6 addresses or hostnames of the NTP servers accessible from the management interface.

  Note   You must enter a value here, such as pool.ntp.org. NTP server is important for time synchronization between Cisco Crosswork Data Gateway VM and Cisco Crosswork Optimization Engine. Using a non-functional or dummy address may cause issues when Crosswork and Cisco Crosswork Data Gateway try to communicate with each other. If you are not using an NTP server, ensure that time gap between Cisco Crosswork Data Gateway and Cisco Crosswork Optimization Engine is not more than 10 minutes. Else, Cisco Crosswork Data Gateway will fail to pull images.

j) **Syslog Servers**

- Server Address: IPv4 or IPv6 address of a syslog server accessible from the management interface.

  Note   If you are using an IPv6 addres, it must be surrounded by square brackets ([1::1]).

- Syslog Port: Port number of the syslog server.

- Syslog Protocol: Use UDP, TCP, or RELP when sending syslog.

- Use Syslog over TLS?: Use TLS to encrypt syslog traffic.

- TLS Peer Name: Syslog server's hostname exactly as entered in the server certificate SubjectAltName or subject common name.

- Syslog Root Certificate File URI: PEM formatted root cert of syslog server retrieved using SCP.

- Syslog Certificate File Passphrase: Password of SCP user to retrieve Syslog certificate chain.

k) **Controller Settings**

- Controller IP: IP address of the Crosswork controller i.e., Cisco Crosswork Optimization Engine.

  Note   If you are using an IPv6 address, it must be surrounded by square brackets ([1::1]).

- Controller Port: Port of the Crosswork controller i.e., Cisco Crosswork Optimization Engine.

- Controller Signing Certificate File URI: PEM formatted root cert of Cisco Crosswork Optimization Engine to validate signing certs retrived using SCP. PEM file is generated by Crosswork and is available at the following location:

```
cw-admin@<Crosswork_VM_ Management_IP_Address>:/home/cw-admin/controller.pem
```

- SSL/TLS Certificate File URI: Crosswork controller PEM formatted SSL/TLS certificate file retrieved using SCP.

- Controller Certificate File Passphrase: Password of SCP user to retrieve Cisco Crosswork Optimization Engine certificate chain.

- Proxy Server URL: URL of management network proxy server.

- Proxy Server Bypass List: Space-delimited list of subnets and domains that will not be sent to the proxy server.

- Authenticated Proxy Username: Username for authenticated proxy servers.

- Authenticated Proxy Passphrase: Passphrase for authenticated proxy servers.

- HTTPS Proxy SSL/TLS Certificate File URI: HTTPS proxy PEM formatted SSL/TLS certificate file retrieved using SCP.

- HTTPS Proxy SSL/TLS Certificate File passphrase: Password of SCP user to retrieve proxy certificate chain.

l) **Auto Enrollment Package**

- Enrollment Passphrase: SCP user passphrase to transfer enrollment package.

- Enrollment Destination Host and Path: SCP host and path to transfer the enrollment package using SCP (`user@host:/path/to/file`).

Step 12   Click **Next** to go to **10 Ready to complete**, as shown in the following figure. Review your settings and then click **Finish** if you are ready to begin deployment.
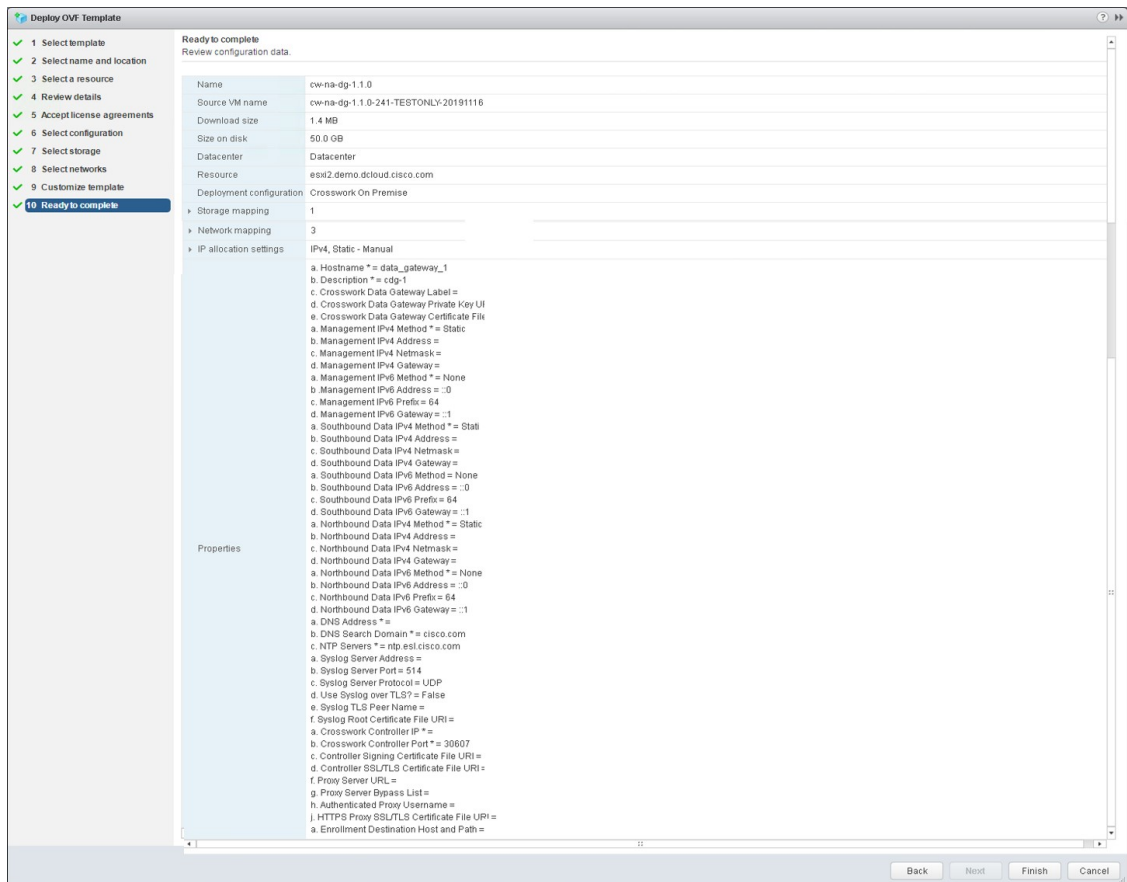
Step 13 Wait for the deployment to finish before continuing. To check the deployment status:

a) Open the vCenter vSphere client.

b) In the **Recent Tasks** tab for the host VM, view the status for the **Deploy OVF template** and **Import OVF package** jobs, as shown in the following figure:
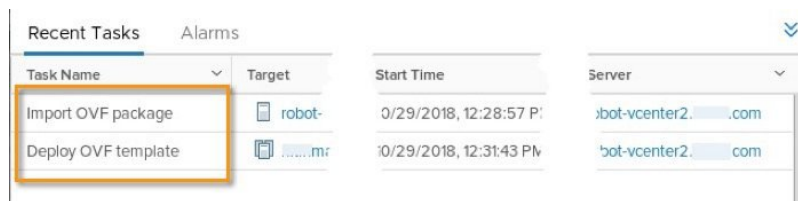
Wait for the deployment status to become 100%.

Note If you are deploying Cisco Crosswork Data Gateway on VCenter 6.7U1 and above, you also need to set boot option to EFI before powering on the VM. Follow these steps:

a. On the host VM **Summary** tab, below the **VM Hardware** table, click **Edit Settings**.

b. On the **Edit Settings** page, click the **VM Options** tab.

c. Expand the **Boot Options** dropdown list and change the **Firmware** setting to **EFI**, if it not set by default. When you are finished, click **OK**. You may want to take a snapshot of the VM at this point.

You can now proceed to power on the VM.

Step 14   Once the deployment status is 100%, power on the VM to complete the deployment process. Expand the host's entry so you can click the VM and then choose **Actions** > **Power** > **Power On**, as shown in the following figure:
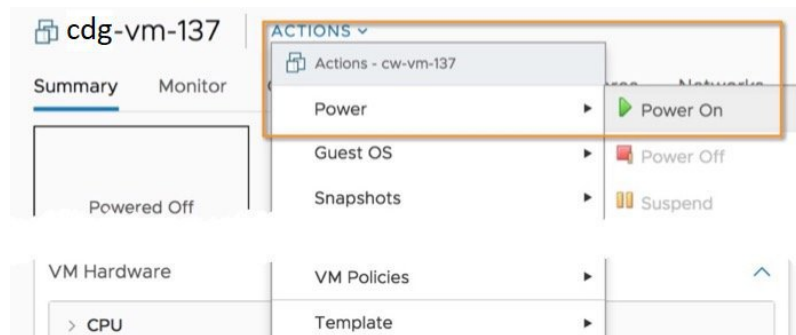
Wait for at least 5 minutes for the Cisco Crosswork Data Gateway VM to come up and then login via vCenter or SSH as explained in the Section Log In and Log Out, on page 58.

Install Cisco Crosswork Data Gateway Via OVF Tool

This is an alternative way to install Cisco Crosswork Data Gateway. You can modify mandatory/optional parameters in the script as per your requirement and run the OVF Tool.

Below is a sample script for installing using this method:

```
#!/usr/bin/env bash

# robot.ova path
ROBOT_OVA_PATH="<mention the orchestrator path>"

# Download robot.ova
# Change the path to a convenient location for download
ova_path=<mention the ova path>

mkdir -p $ova_path

echo "Delete ova image if exists"
rm -rf $ova_path/*.ova

# Download robot.ova
cd $ova_path
echo "Downloading ova image"
wget -d --proxy=off -r -l1 -H -t1 -nd -N -np -A.ova -erobots=off ${ROBOT_OVA_PATH}

filename=`find $ova_path -name \*.ova`

VM_NAME="dg-42"
DM="thin"
Deployment="onpremise"


Hostname="Hostname"
ManagementIPv4Address="<management_ipv4_address>"
ManagementIPv4Gateway="<management_ipv4_gateway>"
ManagementIPv4Netmask="<management_ipv4_netmask>"
ManagementIPv4Method="Static"
SouthDataIPv4Address="<southdata_ipv4_address>"
```

```
SouthDataIPv4Gateway="<southdata_ipv4_gateway>"
SouthDataIPv4Netmask="<southdata_ipv4_netmask>"
SouthDataIPv4Method="Static"
NorthDataIPv4Address="<northdata_ipv4_address>"
NorthDataIPv4Gateway="<northdata_ipv4_gateway>"
NorthDataIPv4Netmask="<northdata_ipv4_netmask>"
NorthDataIPv4Method="Static"

DNS="<DNS_ip_address>"
NTP="<NTP Server>"
Domain="cisco.com"

ControllerIP="<controller_ipv4_address>"
ControllerPort="<controller_port>"
ControllerSignCertChain="cw-admin@<management_ip_address>:/home/cw-admin/controller.pem"
ControllerCertChainPwd="<Password>"


Description="Description for Cisco Crosswork Data Gateway for 42"
Label="Label for Cisco Crosswork Data Gateway dg-42"

dg_adminPassword="<dg-admin_password>"
dg_operPassword="<dg-oper_password>"

EnrollmentURI="<enrollment_package_URI>"
EnrollmentPassphrase="<password>"

# Please replace this information according to your vcenter setup

VCENTER_LOGIN="<vCenter login details>"
VCENTER_PATH="<vCenter path>"
DS="<DS details>"

ovftool --acceptAllEulas --X:injectOvfEnv --skipManifestCheck --overwrite --noSSLVerify
--powerOffTarget --powerOn \
--allowExtraConfig --extraConfig:firmware=efi --extraConfig:uefi.secureBoot.enabled=true \
--datastore="$DS" --diskMode="$DM" \
--name=$VM_NAME \
--net:"Management=VM Network" \
--net:"SouthData=DPortGroupVC-1" \
--net:"NorthData=DPortGroupVC-2" \
--deploymentOption=$Deployment \
--prop:"ControllerIP=$ControllerIP" \
--prop:"ControllerPort=$ControllerPort" \
--prop:"ControllerSignCertChain=$ControllerSignCertChain" \
--prop:"ControllerCertChainPwd=$ControllerCertChainPwd" \
--prop:"EnrollmentURI=$EnrollmentURI" \
--prop:"EnrollmentPassphrase=$EnrollmentPassphrase" \
--prop:"Hostname=$Hostname" \
--prop:"Description=$Description" \
--prop:"Label=$Label" \
--prop:"ManagementIPv4Address=$ManagementIPv4Address" \
--prop:"ManagementIPv4Gateway=$ManagementIPv4Gateway" \
--prop:"ManagementIPv4Netmask=$ManagementIPv4Netmask" \
--prop:"ManagementIPv4Method=$ManagementIPv4Method" \
--prop:"SouthDataIPv4Address=$SouthDataIPv4Address" \
--prop:"SouthDataIPv4Gateway=$SouthDataIPv4Gateway" \
--prop:"SouthDataIPv4Netmask=$SouthDataIPv4Netmask" \
--prop:"SouthDataIPv4Method=$SouthDataIPv4Method" \
--prop:"NorthDataIPv4Address=$NorthDataIPv4Address" \
--prop:"NorthDataIPv4Gateway=$NorthDataIPv4Gateway" \
--prop:"NorthDataIPv4Netmask=$NorthDataIPv4Netmask" \
--prop:"NorthDataIPv4Method=$NorthDataIPv4Method" \
--prop:"DNS=$DNS" \
```

```
        --prop:"NTP=$NTP" \
        --prop:"dg-adminPassword=$dg_adminPassword" \
        --prop:"dg-operPassword=$dg_operPassword" \
        --prop:"Domain=$Domain" $ROBOT_OVA_PATH "vi://$VCENTER_LOGIN/$VCENTER_PATH"
```

Step 1   Open a command prompt.

Step 2   Navigate to the location where you installed the OVF Tool.

Step 3   Run the OVF Tool using the following command:

The command contains the location of the source OVF file and location of the vmx file that will be created as a result of executing the command:

```
ovftool <location_of_source_ovf_file> <location_of_vmx_file>
```

For example,

```
root@cxcloudctrl:/opt# ./cdgovfdeployVM197
```

Post-installation Tasks

Once the Cisco Crosswork Data Gateway is installed, complete the following tasks in the order of their listing:

- Log In and Log Out, on page 58
- Generate An Enrollment Package, on page 60
- Export Enrollment Package

Log In and Log Out

You can use either of the following two ways to access Cisco Crosswork Data Gateway:

- Access Cisco Crosswork Data Gateway Through vCenter, on page 58
- Access Cisco Crosswork Data Gateway Via SSH, on page 59

Access Cisco Crosswork Data Gateway Through vCenter

Follow these steps to log in via vCenter:

Step 1   Locate the VM in vCenter and then right click and select **Open Console**.

The Cisco Crosswork Data Gateway flash screen comes up.

Step 2   Enter username (dg-admin or dg-oper as per the role assigned to you) and the corresponding password (the one that you created during installation process) and press **Enter**.

```
Cisco Crosswork Data Gateway

  #####  ######  #######  #####   #####  #     # ####### ######  #    #
 #     # #     # #       #     # #     # #  #  #    #    #     # #   #
 #       #     # #       #       #       #  #  #    #    #     # #  #
 #       ######  #       #  #### #       #  #  #    #    ######  ###
 #       #   #   #       #     # #       #  #  #    #    #   #   #  #
 #     # #    #  #       #     # #     # #  #  #    #    #    #  #   #
  #####  #     # #######  #####   #####   ## ##     #    #     # #    #

Copyright (c) 2019 by Cisco Systems, Inc.
Version: 1.1.0 (branch dg110dev - build number 245)
Built on: Nov-20-2019 00:06 AM UTC

[Password:
```

Access Cisco Crosswork Data Gateway Via SSH

Note   The SSH process is protected from brute force attacks by blocking the client IP after a number of login failures. Failures such as incorrect username or password, connection disconnect, or algorithm mismatch are counted against the IP. Up to 4 failures within a 20 minute window will cause the client IP to be blocked for at least 7 minutes. Continuing to accumulate failures will cause the blocked time to be increased. Each client IP is tracked separately.

Follow these steps to login via SSH.

Step 1   Run the following command:

ssh <username>@<ManagementNetworkIP>

where **ManagementNetworkIP** is the management network IP address.

For example,

To login as adminstrator user: **ssh dg-admin@<ManagementNetworkIP>**

To login as operator user: **ssh dg-oper@<ManagementNetworkIP>**

The following Cisco Crosswork Data Gateway flash screen opens prompting for password:

```
Cisco Crosswork Data Gateway

  #####  ######  #######  #####   #####  #      # ####### ######  #    #
 #     # #     # #       #     # #     # #      # #       #     # #    #
 #       #     # #       #             #        #   #   # #       #     # #  #  #
 #       ######  #       # #####   #####  #   #   #   #   # ######  ###
 #       #     # #       #     #       #   #   #   #   #   # #     # #   #   #
 #     # #     # #       #     # #     # #   #   #   #   #   # #     # #    #   #
  #####  #       # ####### #####   #####   ## ## ####### #     # #    #
```

Copyright (c) 2019 by Cisco Systems, Inc.
Version: 1.1.0 (branch dg110dev – build number 245)
Built on: Nov-20-2019 00:06 AM UTC

Password:

Step 2   Input the corresponding password (the one that you created during installation process) and press **Enter**.

Log Out

To log out, select option **l Logout** from the Main Menu and press Enter or click **OK**.

```
Cisco Crosswork

        Main Menu – Please Choose an Option:

            1   Export Enrollment Package
            2   Show System Settings
            3   Change Current System Settings
            4   Vitals
            5   Troubleshooting
            p   Change Passphrase
            l   Logout




                        <  OK  >
```
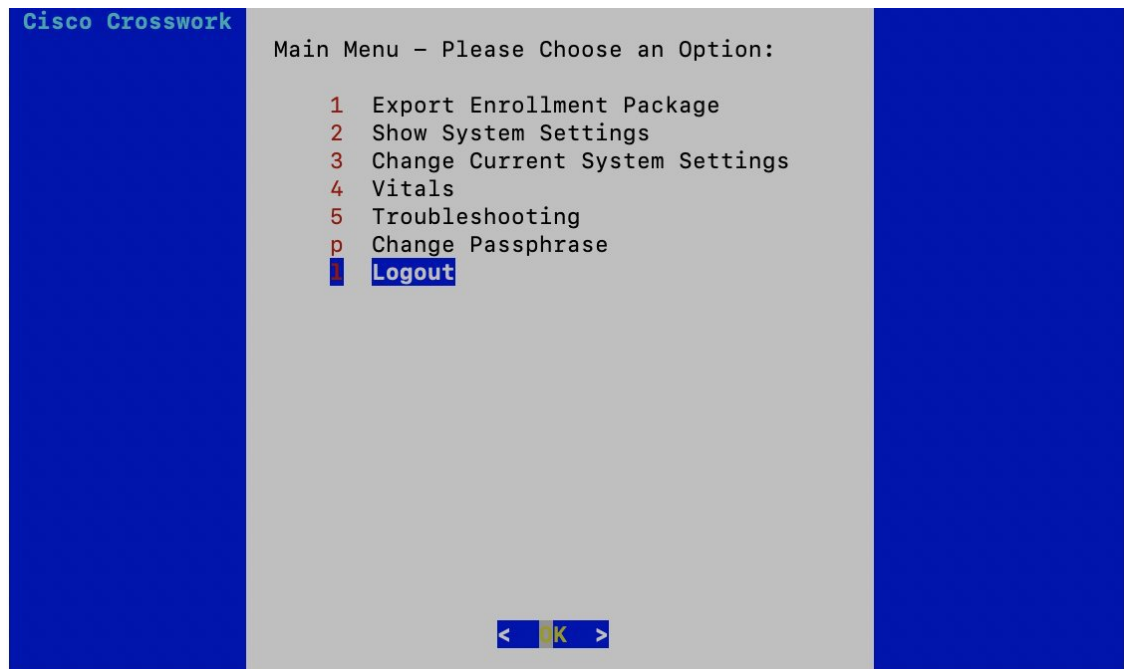
Generate An Enrollment Package

Every Cisco Crosswork Data Gateway instance must be identified by means of an immutable identifier. This requires generation of a Cisco Crosswork Data Gateway enrollment package. The enrollment package can be generated during installation by supplying OVF parameters or by using the **Export Enrollment Package** option from the interactive menu in the console.

The enrollment package is a JSON document created from the information obtained through the OVF template populated by the user during installation. It includes the all necessary information about Cisco Crosswork

Data Gateway required for registering, such as Certificate, UUID of the Cisco Crosswork Data Gateway instance, and metadata like Cisco Crosswork Data Gateway instance name, creation time, version info, and so on.

If you opted not to export the enrollment package during install, then you must export it before you can enroll the Cisco Crosswork Data Gateway instance with Crosswork. The steps to do so are described in Export Enrollment Package, on page 61.

Note The enrollment package is unique to each Cisco Crosswork Data Gateway instance.

A sample enrollment package JSON file is shown below:

```
{
  "name": "dg116.cisco.com",
  "description": "CDG Base VM for Automation",
  "profile": {
    "cpu": 8,
    "memory": 31,
    "nics": 3
  },
  "interfaces": [
    {
      "name": "eth0",
      "mac": "00:50:56:9e:09:7a",
      "ipv4Address": "<ip_address>/24"
    },
    {
      "name": "eth1",
      "mac": "00:50:56:9e:67:c3",
      "ipv4Address": "<ip_address>/16"
    },
    {
      "name": "eth2",
      "mac": "00:50:56:9e:83:83",
      "ipv4Address": "<ip_address>/16"
    }
  ],
  "certChain": [
```

███

```
  ],
  "version": "1.1.0 (branch dg110dev - build number 152)",
  "duuid": "d58fe482-fdca-468b-a7ad-dfbfa916e58b"
}
```

Export Enrollment Package

Before enrolling Cisco Crosswork Data Gateway with Cisco Crosswork Optimization Engine, you must export the enrollment package.

Note This is needed only if you have not specified **Auto Enrollment Package Transfer** settings in the OVF template. Otherwise, the file will be at the SCP URI destination after the VM boots.

Follow these steps:

Step 1   Log into the Cisco Crosswork Data Gateway Base VM as explained in Section Log In and Log Out, on page 58.

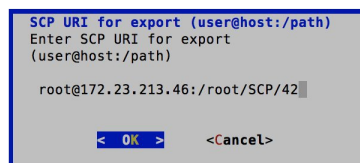**Step 2**   From the Main Menu, select **1 Export Enrollment Package** and click **OK**.

```
Cisco Crosswork
                    Main Menu - Please Choose an Option:

                       1   Export Enrollment Package
                       2   Show System Settings
                       3   Change Current System Settings
                       4   Vitals
                       5   Troubleshooting
                       p   Change Passphrase
                       l   Logout













                                   <  OK  >
```
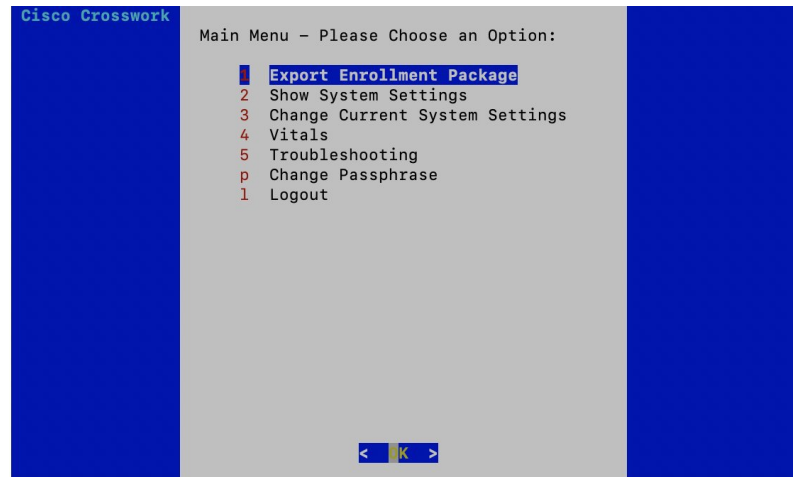
Step 3   Enter the SCP URI for exporting the enrollment package and click **OK**.

> **Note**   The host must run an SCP server. If no alternative SCP server is available, then Crosswork can be used. An example URI is given below:
>
> ```
> cw-admin@<Crosswork_VM_Management_IP_Address>:/home/cw-admin
> ```

```
SCP URI for export (user@host:/path)
Enter SCP URI for export
(user@host:/path)

  root@172.23.213.46:/root/SCP/42

       <  OK  >      <Cancel>
```

Step 4   Enter the SCP passphrase (the SCP user password) and click **OK**.
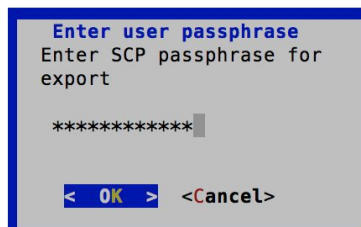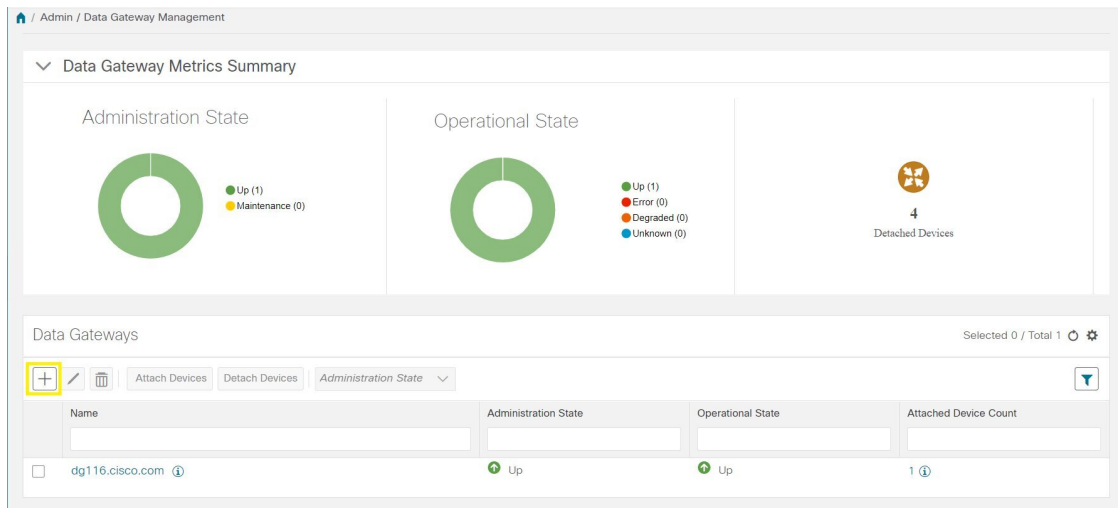
The enrollment package is exported.

Step 5 Manually copy the enrollment package from the above SCP server to your local computer, to be used in the next task to enroll Cisco Crosswork Data Gateway with Cisco Crosswork Optimization Engine.

Enroll Cisco Crosswork Data Gateway With Cisco Crosswork Optimization Engine
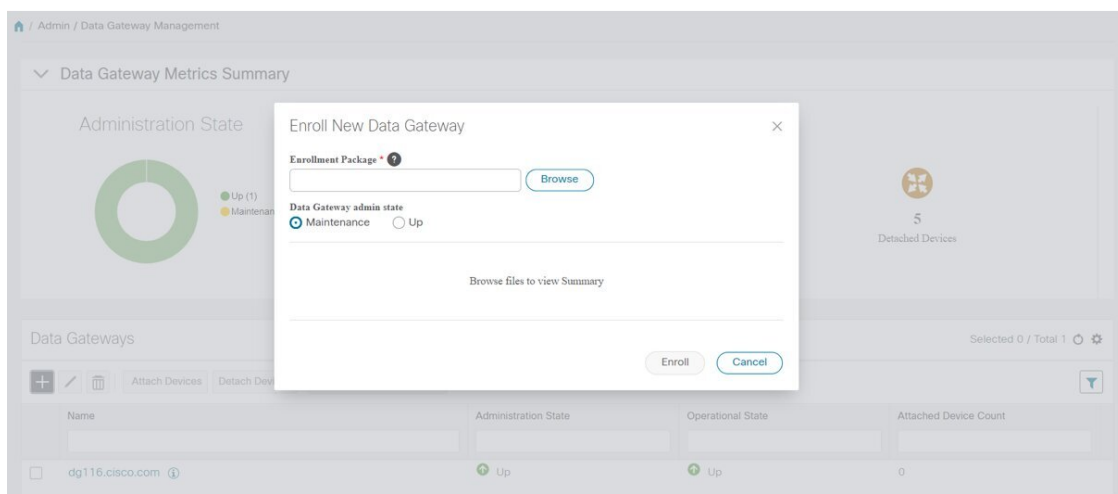
Enroll Cisco Crosswork Data Gateway

Step 1 Log into Cisco Crosswork Optimization Engine as described in Section Log In to the UI From a Browser, on page 35.

Step 2 From the Main Menu, select **Admin** > **Data Gateway Management**.

The **Data Gateway Management** page opens.

Step 3 Click the **Add** button.

The **Enroll New Data Gateway** dialog opens.

Step 4   Click **Browse** and navigate to the folder to which you copied the enrollment package and select it.

Step 5   Select the **Data gateway admin state** in which you want to bring up the Cisco Crosswork Data Gateway:

- **Up** (recommended): Select this state if you want to bring up the Cisco Crosswork Data Gateway in active mode. Up state moves the operational state of the Cisco Crosswork Data Gateway to up with no intermediate step.

- **Maintenance**: Select this state if you want to bring up the Cisco Crosswork Data Gateway in maintenance mode. Maintenance state moves the operational state of the Cisco Crosswork Data Gateway to up. However, it applies an identifying flag to the Cisco Crosswork Data Gateway while you perform any additional testing and setup.
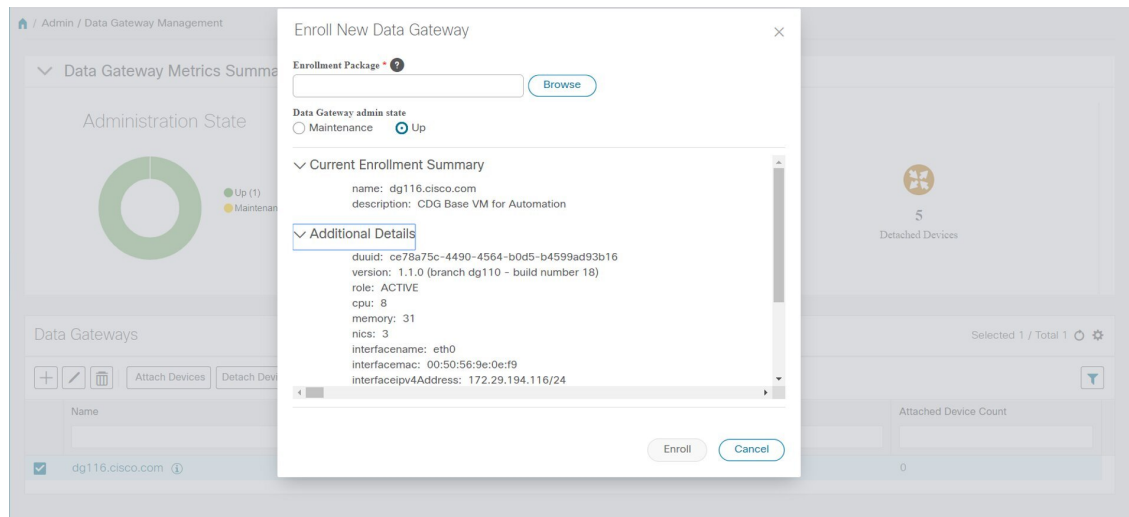
The **Enroll New Data Gateway** dialog displays a summary of the selected enrollment package:

- Name of the Cisco Crosswork Data Gateway instance

- Description of the Cisco Crosswork Data Gateway instance

- Labels associated with the Cisco Crosswork Data Gateway instance

It also displays additional details:

- Number of CPUs

- Memory

- Number of NICs

- Interface name

- Interface MAC address

- Interface IPv4Address

- certChain

- Version

- DUUID

Step 6 Click **Enroll**.Cisco Crosswork Data Gateway displays the following message upon successful enrollment:

Once you click **Enroll**, a dialog pops up asking if you want to attach devices now or later. It is recommended to choose **Later** as devices must only be attached once the operational state of the Cisco Crosswork Data Gateway instance is **Up**.

Note Steps to attach devices to a Cisco Crosswork Data Gateway instance are available in *Cisco Crosswork Change Automation and Health Insights 3.1 User Guide*.

What to do next

The Operational Status of a Cisco Crosswork Data Gateway instance is shown as "**Degraded**" until it establishes a connection with Cisco Crosswork Optimization Engine and downloads collector binary files. While it

depends on the bandwidth between the Cisco Crosswork Data Gateway instance and Cisco Crosswork

Optimization Engine, this operation typically takes less than 5 minutes. Click the ⟳ icon in the **Data Gateways** pane to refresh the pane to reflect the latest operational status of the Cisco Crosswork Data Gateway instance and wait for it to become **Up**. If the Cisco Crosswork Data Gateway instance fails to enroll, contact Cisco CX for assistance.

Cisco Crosswork Data Gateway Authentication and Bootstrap

During the enrollment process, the enrollment package is uploaded to the controller application, i.e., Cisco Crosswork Optimization Engine, which then instantiates a new Cisco Crosswork Data Gateway instance in its database and waits for a "first-sign-of-life" from the Cisco Crosswork Data Gateway.

Session Establishment

Once the connectivity is established, the Cisco Crosswork Data Gateway instance confirms the identity of the controller and offers its own proof of identity via signed certificates during this initial connection.

Download of Configuration Files

Once the session is established, Cisco Crosswork Data Gateway downloads the following configuration files:

Table 12: Configuration Files

boot-config	A json response created by Crosswork that contains a list of services (docker containers) and functional images should be downloaded on that particular Cisco Crosswork Data Gateway instance.
docker-compose	A YAML file that contains instructions and order to start up the right set of services and functional images.

Download of Functional Images

A functional image represents a collection profile for a protocol, i.e., CLI, SNMP, or MDT. Cisco Crosswork Data Gateway downloads the following functional images:

Table 13: Functional Images

CLI Collection	To connect to a device using SSH/Telnet, collect **show** commands output, and send it to the designated output destination.
SNMP Collection	To connect to a device using SNMP protocol, collect SNMP responses, receive SNMP traps, and send them to a designated output destination.
MDT Collection	To connect to a device and collect model-driven telemetry or event-driven telemetry events, and send them to a designated output destination.

After the downloads, Cisco Crosswork Data Gateway boots the containers.

Cisco Crosswork Data Gateway is now ready to collect data.

Troubleshoot the Cisco Crosswork Data Gateway Installation and Enrollment

The following table lists common problems that might be experienced while installing or enrolling Cisco Crosswork Data Gateway, and provides approaches to identifying the source of the problem and solving it.

Table 14: Troubleshooting the Installation/Enrollment

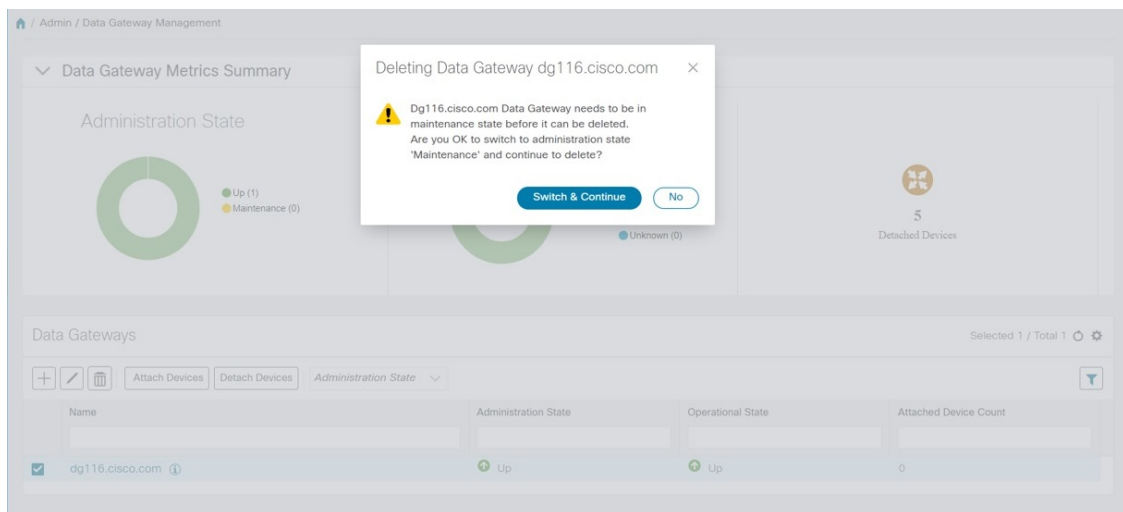| Issue	Action
1. Cannot enroll Cisco Crosswork Data Gateway with Crosswork	
Cisco Crosswork Data Gateway cannot be enrolled with Cisco Crosswork Optimization Engine due to an NTP issue, i.e., there is a clock-drift between the two. The clock-drift might be with either Cisco Crosswork Data Gateway or Cisco Crosswork Optimization Engine. Also, on the NTP servers for Cisco Crosswork Optimization Engine and Cisco Crosswork Data Gateway, the initial time is set to the ESXi server. For this reason, the ESXi server must also have NTP configured. Sync the clock time on the host and retry.	1. Log into the Cisco Crosswork Data Gateway VM. 2. From the main menu, go to **5 Troubleshooting** > **Run show-tech**. Enter the destination to save the tarball containing logs and vitals and click **OK**. In the show-tech logs (in file `session.log` at location `/opt/dg/data/controller-gateway`), if you see the error `UNAUTHENTICATED:invalid certificate. reason: x509: certificate has expired or is not yet valid`, then there is a clock-drift between Cisco Crosswork Data Gateway and . 3. From the main menu, go to **3 Change Current System Settings** > **1 Configure NTP**. Configure NTP to sync with the clock time on the Cisco Crosswork Optimization Engine server and try re-enrolling Cisco Crosswork Data Gateway. It is also possible that the Cisco Crosswork Optimization Engine's NTP server might be down or its address might be incorrect. To configure NTP on the Cisco Crosswork Optimization Engine side, see Configure NTP after installation.
2. Cisco Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "Could not collect vitals"	

Issue	Action
Cisco Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "Could not collect vitals" due to certificate errors.	1. Log into the Cisco Crosswork Data Gateway VM. 2. From the main menu, select **5 Troubleshooting** > **Run show-tech**. Enter the destination to save the tarball containing logs and vitals and click **OK**. In the show-tech logs (in file `gateway.log` at location `/opt/dg/log/controller-gateway/gateway.log`), if you see certificate errors, then re-upload the Controller Signing Certificate, as explained in the steps below: 1. From the main menu, select **3 Change Current System Settings** > **7 Import Certification**. 2. From the **Import Certificates** menu, select **1 Controller Signing Certificate File** and click **OK**. 3. Enter the SCP URI for the certificate file and click **OK**.
3. Cisco Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "gRPC connection cannot be established"	
Cisco Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "gRPC connection cannot be established" due to certificate errors.	1. Re-upload the certificate file as explained in the troubleshooting scenario **2.** above. 2. Reboot the Cisco Crosswork Data Gateway VM following the steps below: a. From the main menu, select **5 Troubleshooting** and click **OK**. b. From the Troubleshooting menu, select **7 Reboot VM** and click **OK**. c. Once the reboot is complete, check if the Cisco Crosswork Data Gateway's operational status is **Up**.

De-enroll Cisco Crosswork Data Gateway

Step 1 Log in to Crosswork UI as desribed in .

Step 2 From the navigation panel, select **Admin** > **Data Gateway Management**.

The **Data Gateway Management** page opens.

Step 3 In the **Data Gateways** panel, select the Cisco Crosswork Data Gateway VM you want to remove and click **Delete** button.
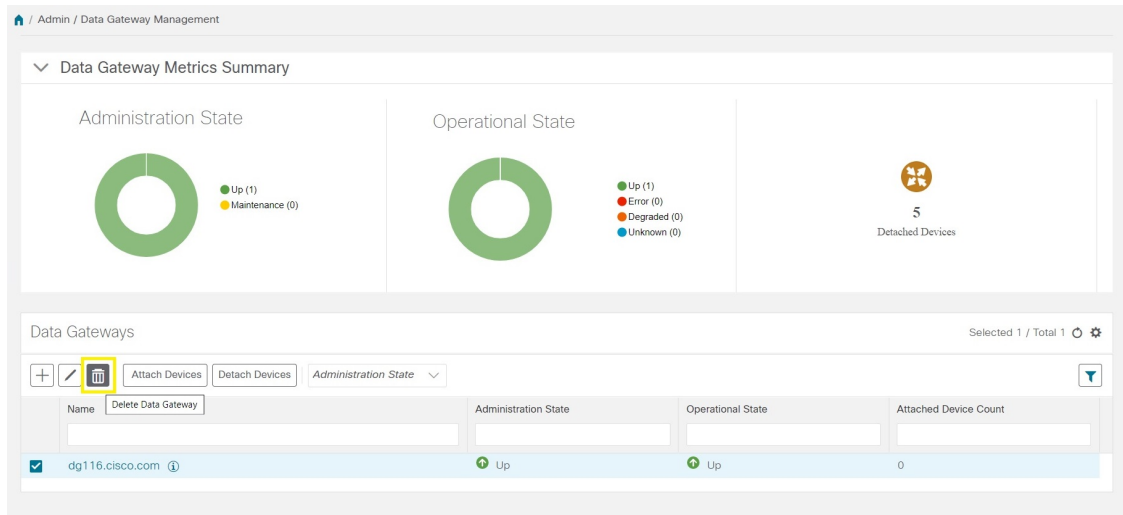
Step 4 A Cisco Crosswork Data Gateway instance must be in maintenance mode to be deleted. Click **Switch & Continue** when prompted to switch to maintenance mode.

The selected Cisco Crosswork Data Gateway VM is deleted.

C H A P T E R 4

Remove Cisco Crosswork Optimization Engine and Cisco Crosswork Data Gateway

This section contains the following topics:

Deleting Cisco Crosswork Optimization Engine and Cisco Crosswork Data Gateway

The procedure to delete a Cisco Crosswork Optimization Engine VM and Cisco Crosswork Data Gateway VM is the same.

Note

- Be aware that this procedure deletes all your Cisco Crosswork Optimization Engine and Cisco Crosswork Data Gateway data.

- **If you want to delete Cisco Crosswork Data Gateway only**, ensure you have done the following:

  - Detach the devices from the Cisco Crosswork Data Gateway VM you want to delete. The procedure to detach devices from a Crosswork Data Gateway is described in *Cisco Crosswork Optimization Engine User Guide*.

  - De-enroll the Cisco Crosswork Data Gateway from Cisco Crosswork Optimization Engine as described in De-enroll Cisco Crosswork Data Gateway, on page 69.

Step 1   Log in to the VMware vSphere Web Client.

Step 2   In the **Navigator** pane, right-click the VM or Cisco Crosswork Data Gateway VM that you want to remove and choose **Power** > **Power Off**.

Step 3   Once the VM is powered off, right-click the VM again and choose **Delete from Disk**.

The VM is deleted.

Device Configurations

This section provides device configurations that are necessary for device onboarding and multiple SR-PCE setup. For more information on adding devices and SR-PCE providers, see the "Manage Inventory" chapter in the *Cisco Crosswork Optimization Engine User Guide*.

Prerequisites for Onboarding Devices

Before adding devices, you must ensure that the devices themselves are configured to collect and transmit telemetry data properly and communicate successfully with Cisco Crosswork Optimization Engine. The following sections provide sample configurations for a variety of communications options. Use them as a guide to configuring the devices you plan to manage using Cisco Crosswork Optimization Engine.

Note Only users configured with privilege level 15 can use the NETCONF APIs. Privilege level 15 can be used to configure the "enable" password option in XE devices. In such cases, NETCONF should not be included as one of the protocols to verify reachability and operational state for the onboarded devices.

Note Only SNMPv2 and SNMPv3 (NoAuth/NoPriv) traps are supported.

Pre-Onboarding SNMP v2 Device Configuration

The following commands provide a sample pre-onboarding device configuration that sets the correct SNMPv2 and NETCONF configuration, and SSH and Telnet rate limits. The NETCONF setting is only needed if the device is MDT-capable (XR 6.5.3/6.6.3 or higher).

```
logging console debugging
logging monitor debugging
telnet vrf default ipv4 server max-servers 100
telnet vrf default ipv6 server max-servers 100
crypto key generate rsa
line default
 exec-timeout 0 0
 width 107
```

```
 length 37
 absolute-timeout 0
!
snmp-server community public RO
snmp-server community robot-demo2 RO
snmp-server ifindex persist
ntp
 server <NTPServerIPAddress>
!
service cli history size 5000
service cli interactive disable
ssh server v2
ssh server vrf default
ssh server netconf vrf default
ssh server logging
ssh server rate-limit 100
ssh server session-limit 100
grpc
 port 57400
!
netconf agent tty
!
netconf-yang agent
 ssh
!
```

Pre-Onboarding SNMPv3 Device Configuration

If you want to enable SNMPv3 data collection, repeat the SNMPv2 configuration commands in the previous section, and add the following commands:

```
snmp-server group grpauthpriv v3 priv notify v1default
snmp-server user <user-ID> grpauthpriv v3 auth md5 <password> priv aes 128 <password>
```

Configure Redundant Cisco SR-PCEs

You can set up two Cisco SR-PCEs to ensure high availability (HA). The two Cisco SR-PCE providers must have matching configurations, supporting the same network topology. In HA, if the primary SR-PCE becomes unreachable, Cisco Crosswork Optimization Engine uses the secondary SR-PCE to discover the network topology. The network topology will continue to be updated correctly and you can view SR-PCE connectivity events in the Events table.

Configure HA

The following configurations must be done to enable HA when two Cisco SR-PCE providers are added in Cisco Crosswork Optimization Engine. To enable HA, both SR-PCEs must have network connectivity between them for communication and syncing purposes.

Issue the following commands on *each* of the Cisco SR-PCE devices:

Enable the interface:

```
# interface <interface><slot>/<port>
ipv4 address <sync-link-interface-ip-address> <subnet-mask>
no shut
```

Enable HA:

```
# pce rest sibling ipv4 <other-node-pce-address>
```

Establish a sync link between the two SR-PCEs:

```
# router static
address-family ipv4 unicast
<other-node-pce-ip-address>/<subnet-mask-length> <remote-sync-link-ip-address>
```

(Optional) `# pce segment-routing traffic-eng peer ipv4 <other-node-pce-ip-address>`

It should be entered for each PCC and not for other PCE nodes.

Issue the following command on the PCC:

For SR Policies: `# segment-routing traffic-eng pcc redundancy pcc-centric`

For RSVP-TE Tunnels: `# mpls traffic-eng pce stateful-client redundancy pcc-centric`

Confirm Sibling SR-PCE Configuration

From the SR-PCE, enter the `show tcp brief` command to verify synchronization between SR-PCEs in HA are intact:

```
#show tcp brief | include <remote-SR-PCE-router-id>
```

Confirm that following information is correct:

Local Address	Foreign Address	State
<local-SR-PCE-router-id>:8080	*<local-SR-PCE-router-id>*:*<any-port-id>*	ESTAB
<local-SR-PCE-router-id>:*<any-port-id>*	*<local-SR-PCE-router-id>*:8080	ESTAB

SR-PCE Delegation

Depending on where an SR policy is created, the following SR-PCE delegation occurs:

- SR-PCE initiated—Policies configured on a PCE. SR policies are delegated back to the source SR-PCE.

  Note
  - The policy can be PCE initiated even if it is created using the UI, but in that case it is not configured explicitly on SR-PCE.
  - RSVP-TE tunnels cannot be configured directly on a PCE.

- PCC initiated—An SR policy or RSVP-TE tunnel that is configured directly on a device. The SR-PCE configured with the lowest precedence is the delegated SR-PCE. If precedence is not set, then SR-PCE with the lowest PCE IP address is the delegated SR-PCE. The following configuration example, shows that **10.0.0.1** is assigned a precedence value of 10 and will be the delegated SR-PCE.

  ```
  segment-routing
    traffic-eng
      pcc
        source-address ipv4 10.0.0.2
        pce address ipv4 10.0.0.1
          precedence 10
         !
        pce address ipv4 10.0.0.8
          precedence 20
         !
  ```

```
            report-all
            redundancy pcc-centric
```

For RSVP-TE Tunnel:

```
mpls traffic-eng
interface GigabitEthernet0/0/0/0
  admin-weight 1
!
interface GigabitEthernet0/0/0/1
  admin-weight 1
!
interface GigabitEthernet0/0/0/2
  admin-weight 1
!
pce
  peer source ipv4 192.168.0.02
  peer ipv4 192.168.0.9
    precedence 10
  !
  peer ipv4 192.168.0.10
    precedence 20
  !
  stateful-client
   instantiation
   report
   redundancy pcc-centric
   autoroute-announce
   !
!
auto-tunnel pcc
  tunnel-id min 990 max 999
```

• Cisco Crosswork Optimization Engine SR-PCE initiated—An SR policy that is configured using Cisco Crosswork Optimization Engine. SR-PCE delegation is random per policy.

> **Note** Only TE tunnels (SR policies or RSVP-TE tunnels) created by Cisco Crosswork Optimization Engine can be modified or deleted by Cisco Crosswork Optimization Engine.

HA Notes and Limitations

• It is assumed that all PCCs are PCEP connected to both SR-PCEs.

• When an SR-PCE is disconnected only from Cisco Crosswork Optimization Engine, the following occur:

  • SR-PCE delegation assignments remain, but the SR-PCE that has been disconnected will not appear in Cisco Crosswork Optimization Engine.

  • You are not able to modify Cisco Crosswork Optimization Engine SR-PCE initiated SR policies if the disconnected SR-PCE is the delegated PCE.

• After an SR-PCE reloads, do the following:

  1. Execute the following command:

     ```
     # process restart pce_server
     ```

2. From the UI, navigate to **Inventory Management** > **Providers** and delete the PCE sibling configuration in both SR-PCEs and then add the sibling configuration back again.

- In some cases, when an SR policy that was created via the UI is automatically deleted (intentional and expected) from Cisco Crosswork Optimization Engine, a warning message does not appear. For example, if the source PCC is reloaded, the UI created SR policy disappears and the user is not informed.

- In an extreme case where one SR-PCE fails on all links (to PCCs/topology devices) except the up-link to Cisco Crosswork Optimization Engine, then topology information will not be accurate in Cisco Crosswork Optimization Engine. When this happens, fix the connectivity issue or delete both SR-PCEs from the Provider page and re-add the one that is reachable.

SR-PCE Configuration Examples

The following configurations are *examples* to guide you in a multiple SR-PCE setup for HA. Please modify accordingly.

Sample redundant SR-PCE configuration (on PCE)

```
pce
 address ipv4 192.168.0.7
 rest
  sibling ipv4 192.168.0.6
```

Sample redundant SR-PCE Configuration (PCC)

```
segment-routing
 traffic-eng
  pcc
   source-address ipv4 192.0.2.1
   pce address ipv4 192.0.2.6
    precedence 200
    !
   pce address ipv4 192.0.2.7
    precedence 100
    !
   report-all
   redundancy pcc-centric
```

Sample redundant SR-PCE Configuration (on PCC) for RSVP-TE

✎

Note `Loopback0` represents the TE router ID.

```
ipv4 unnumbered mpls traffic-eng Loopback0
!
mpls traffic-eng
 pce
  peer source ipv4 209.165.255.1
  peer ipv4 209.165.0.6
   precedence 200
   !
  peer ipv4 209.165.0.7
   precedence 100
   !
  stateful-client
```

```
    instantiation
    report
    redundancy pcc-centric
    autoroute-announce
   !
 !
 auto-tunnel pcc
  tunnel-id min 1000 max 1999
 !
!
```

Sample SR-TM Configuation

```
telemetry model-driven
 destination-group crosswork
  address-family ipv4 198.18.1.219 port 9010
   encoding self-describing-gpb
   protocol tcp
  !
 !
 sensor-group SRTM
  sensor-path Cisco-IOS-XR-infra-tc-oper:traffic-collector/afs/af/counters/tunnels
  sensor-path
Cisco-IOS-XR-infra-tc-oper:traffic-collector/vrf-table/default-vrf/afs/af/counters/prefixes

 !
 subscription OE
  sensor-group-id SRTM sample-interval 60000
  destination-id crosswork
  source-interface Loopback0
!
traffic-collector
 interface GigabitEthernet0/0/0/3
 !
 statistics
  history-size 10
```

Note   The destination address uses the southbound data interface (eth1) address of the Cisco Crosswork Data Gateway
VM.