Cisco Crosswork Change Automation and Health Insights 3.2 Installation Guide

First Published: 2020-04-03

Last Modified: 2020-04-03

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

Overview

This section contains the following topics:

Overview of Cisco Crosswork Change Automation and Health Insights

Cisco Crosswork Change Automation and Health Insights is part of the Cisco Crosswork Network Automation suite of products. Cisco Crosswork Network Automation is a microservices-based platform that brings together streaming telemetry, big data and application programming interfaces (APIs) to redefine service provider network operations.

Cisco Crosswork Change Automation and Health Insights provides the following:

- Continuous real-time monitoring of key performance indicators (KPIs)
- Routinizing scheduled network maintenance and network reconfiguration tasks
- Linking optimization and remediation playbooks to KPIs in order to streamline response to network events

The data collection functionality has been separated out into its own VM and software package called Cisco Crosswork Data Gateway. Cisco Crosswork Data Gateway gathers all the information from the monitored devices and forwards it to Cisco Crosswork Change Automation and Health Insights for analysis and processing. Cisco Crosswork Change Automation and Health Insights can then be used by the operator to manage the network or respond to changes in the network. Apart from Cisco Crosswork Change Automation and Health Insights, Cisco Crosswork Data Gateway can also be used for external data collection integration. Cisco Crosswork Change Automation and Health Insights uses Cisco Network Services Orchestrator (Cisco NSO) as the default provider to manage the devices according to their expected functions, including configuring any required model-driven telemetry (MDT) sensor paths for data collection. Cisco NSO is vital in supplying device management and configuration-maintenance services

Note Cisco recommends using Cisco Crosswork Data Gateway 1.1.2 with Cisco Crosswork Change Automation and Health Insights 3.2.

For more information about the Cisco Crosswork Network Automation platform and Cisco Crosswork Change Automation and Health Insights, see the Cisco Crosswork Network Automation Product page on Cisco.com.

Audience

This guide is for experienced network administrators who install Cisco Crosswork Change Automation and Health Insights 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
- Deploying OVF templates using VMware vCenter or OVF Tool

Note Unless otherwise noted, all commands and examples in this guide use IPv4 address formatting.

CHAPTER 2

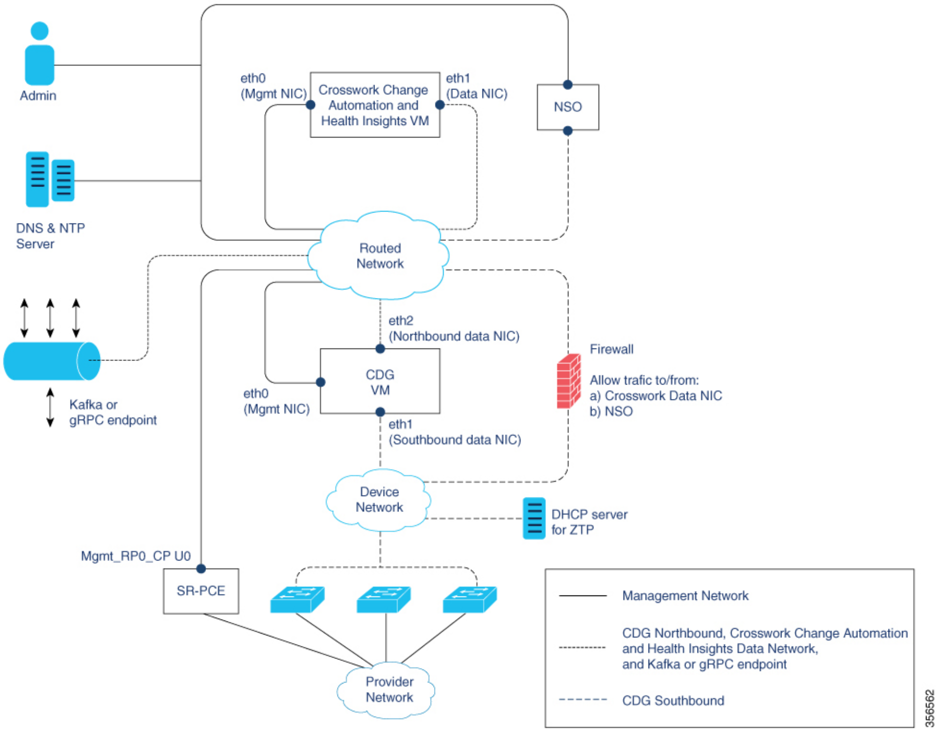
Installation Requirements

This section contains the following topics:

Network Requirements

This figure shows the network components and connections needed to install and use Cisco Crosswork Change Automation and Health Insights.

Figure 1: Crosswork Change Automation and Health Insights Network



Cisco Crosswork Change Automation and Health Insights Virtual Machine (VM)

The Cisco Crosswork Change Automation and Health Insights 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 Multiple NICs are not required for any of the VMs. However, it is recommended to have separate vNICs so that security policies can be applied (virtually or physically on the switch) if needed.

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`.

If you plan to use Zero Touch Provisioning, the device network needs to be equipped with a DHCP server.

Cisco Crosswork Change Automation and Health Insights Installation Requirements

Cisco Crosswork Change Automation and Health Insights 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 Change Automation and Health Insights on a single host, unless otherwise specified.

This section contains the following topics:

Virtual Machine (VM) Requirements

You can deploy Cisco Crosswork Change Automation and Health Insights as a VM on a host that meets the following minimum requirements.

Note Upgrading Cisco Crosswork Change Automation and Health Insights generally requires additional storage apart from the following minimum requirements. For more information, see Upgrade Cisco Crosswork Change Automation and Health Insights, on page 74.

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)
Memory	96 GB
Storage	Storage requirements vary based on factors such as the number of devices being supported, amount of KPI data being collected, 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 Change Automation and Health Insights Via vCenter, on page 16.
vCPU	16 vCPUs
Network Connections	For live deployments, Cisco recommends using dual interfaces, one for the management network and one for the data network between Cisco Crosswork Change Automation and Health Insights and Cisco Crosswork Data Gateway. For demos and lab deployments you can choose between using a single interface or dual interfaces.
IP Addresses	Two IP addresses (IPv4 or IPv6): One public IP for the Management Network virtual interface and one public or private IP for the Data Network virtual interface.

Requirement	Description
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 servers are reachable on the network before attempting the install. The install will fail if the servers cannot be reached.
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. 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 Change Automation and Health Insights VM and uses Docker for containerization. The number of containers varies as applications are added or deleted.

Platform Support for Telemetry

Cisco Crosswork Change Automation and Health Insights supports model-driven telemetry (MDT), SNMP and CLI protocols on the following platforms.

OS	Platform	Software Version[1]	Collection Protocol	Encoding	Transport
Cisco IOS-XR	Cisco ASR 9K (ASR 9001, ASR 9004)	6.4.1, 6.5.1, 6.5.2, 6.5.3, 6.6.2	MDT	KVGPB	TCP
	Cisco NCS 5500	6.4.1, 6.5.3, 6.6.2			
	Cisco XRV9K	6.5.1, 6.5.2, 6.5.3, 6.6.2			
	Cisco NCS 6000	6.4.1, 6.4.2			
	Cisco NCS 1K (NCS 1004)	7.0.1			
	Cisco CRS (CRS 1K, CRS 3K)	6.4.2			
Cisco IOS-XE	Cisco CSR 1Kv	16.10	SNMP CLI		
	Cisco ASR 1K (ASR 1006)	16.9.2, 16.10			
Cisco NX-OS	Cisco Nexus 9K	7.0(3).7(2)			
	Cisco Nexus 7K	8.4(0).SK(1)			

[1] Includes any later version that is backward-compatible with the 6.2.1 (device-native) or 6.1.4 XR CLI YANG model (as appropriate). Before attempting to deploy with a particular later version, please check for compatibility with your Cisco Customer Experience team.

Note Cisco Crosswork Change Automation and Health Insights version 3.2 does not support ASR 9901 version 7.0.1 due to platform issues.

Note The platform support information is provided with the assumption that you plan to stream telemetry in band with other traffic. If you want to stream telemetry via a separate management VRF, you must use Cisco IOS XR version 6.2.1 or later.

Cisco NSO and NED Requirements

Software/Driver	Version
Cisco Network Services Orchestrator (Cisco NSO)	5.2.03
Cisco IOS XR Network Element Driver (NED)	7.13.9
Cisco IOS Network Element Driver	6.36

Supported Web Browsers

This version of Cisco Crosswork Change Automation and Health Insights 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	70 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 Change Automation and Health Insights 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 Change Automation and Health Insights 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 Change Automation and Health Insights VM.

Table 2: 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 Change Automation and Health Insights uses these ports to connect to network devices. You must open the required ports to allow Cisco Crosswork Change Automation and Health Insights to connect to these devices.

Table 3: Destination Ports Used by Cisco Crosswork Change Automation and Health Insights

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

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, on page 10
- Supported Cisco OS, on page 12
- Ports Used, on page 13

Virtual Machine (VM) Requirements

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

Requirement	
Hypervisor	• 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)
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.
vCPU	8 vCPUs

Requirement	
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 Change Automation and Health Insights 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 Change Automation and Health Insights. • 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 Change Automation and Health Insights 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 Change Automation and Health Insights 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 1.1.2 was tested. Cisco Crosswork Data Gateway allows you to expand device coverage by means of custom packages. See Section *Manage Custom Software Packages* in *Cisco Crosswork Change Automation and Health Insights 3.2 User Guide* for information on how to expand the device coverage.

OS	Software Version	Collection Protocols	MDT Encoding
IOS-XR*	6.4.1, 6.4.2 6.5.1, 6.5.2, 6.5.3 6.6.2, 6.6.3 7.0.1	MDT CLI SNMP	KVGPB/TCP
IOS-XE	16.9.2, 16.10 17.1.1	SNMP CLI	NA

NX-OS	7.0(3).7(2)
	8.4(0).SK(1)
			NA

***For MDT configuration via NSO on IOS-XR, use NSO XR NED 7.13.9.**

Note All collection types support IPv4 and IPv6. For any IPv4/IPv6 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.

Note SCP port can be tuned.

Table 4: 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 5: 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 6: 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

CHAPTER 3

Installation Tasks

This section contains the following topics:

Installation Workflow

To set up Cisco Crosswork Change Automation and Health Insights and Cisco Crosswork Data Gateway complete the below installation tasks in the order of their listing:

1. Install Cisco Crosswork Change Automation and Health Insights, on page 16
   a. Verify the VM Configuration, on page 34
   b. Log In to the UI From a Browser, on page 34
   c. Troubleshoot the Installation, on page 35
2. Install Cisco Crosswork Data Gateway, on page 38
   a. Log In and Log Out, on page 58
   b. Generate An Enrollment Package, on page 60
   c. Export Enrollment Package, on page 61
3. Enroll Cisco Crosswork Data Gateway With Cisco Crosswork Change Automation and Health Insights, on page 63
   a. Enroll Cisco Crosswork Data Gateway, on page 63
   b. Cisco Crosswork Data Gateway Authentication and Bootstrap, on page 67
   c. Troubleshoot the Cisco Crosswork Data Gateway Installation and Enrollment, on page 68

Install Cisco Crosswork Change Automation and Health Insights

This section explains the procedure to install Cisco Crosswork Change Automation and Health Insights for the first time. You can install Cisco Crosswork Change Automation and Health Insights using one of the following methods:

- Install Cisco Crosswork Change Automation and Health Insights Via vCenter, on page 16
- Install Cisco Crosswork Change Automation and Health Insights Via OVF Tool, on page 31

For details on upgrading Cisco Crosswork Change Automation and Health Insights to a newer version, see Upgrade Cisco Crosswork Change Automation and Health Insights, on page 74.

During installation, Cisco Crosswork Change Automation and Health Insights 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 Change Automation and Health Insights VM. You will use it to verify that the VM has been properly set up (see Verify the VM Configuration, on page 34).
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 Change Automation and Health Insights user interface, and to perform special operations, such as stopping and restarting services.

Note These two administrative usernames are reserved and cannot be changed. The first time you log in using either of these administrative IDs, you will be prompted to change that ID's password.

Install Cisco Crosswork Change Automation and Health Insights Via vCenter

This section explains the procedure to install Cisco Crosswork Change Automation and Health Insights using vCenter.

Before you begin, ensure that:

- You are creating the Cisco Crosswork Change Automation and Health Insights VM on VMware vCenter
  - Server 6.7 Update 3b or later (ESXi 6.7 Update 1 installed on hosts), OR
  - Server 6.5 Update 2d or later (ESXi 6.5 Update 2 installed on hosts)

  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 Change Automation and Health Insights 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 or IPv6) to assign to the Cisco Crosswork Change Automation and Health Insights 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 or IPv6) to assign to the Cisco Crosswork Change Automation and Health Insights 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 Change Automation and Health Insights VM clock is reachable on the network.

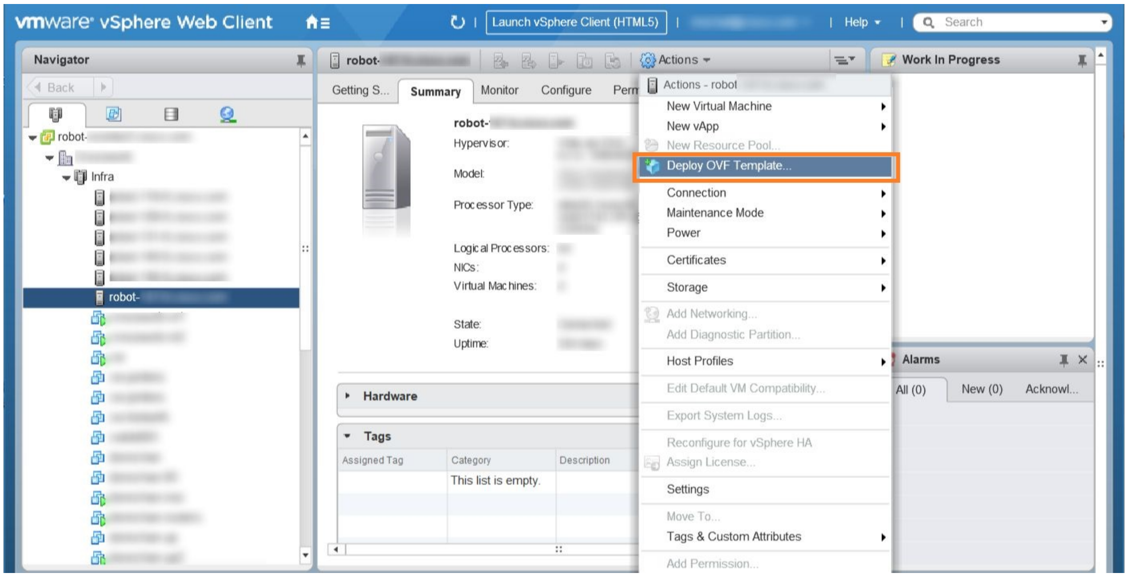
Note Only single stack deployment modes are supported in Cisco Crosswork Change Automation and Health Insights version 3.2. For more information, see Supported TCP/IP Stack, on page 95

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.

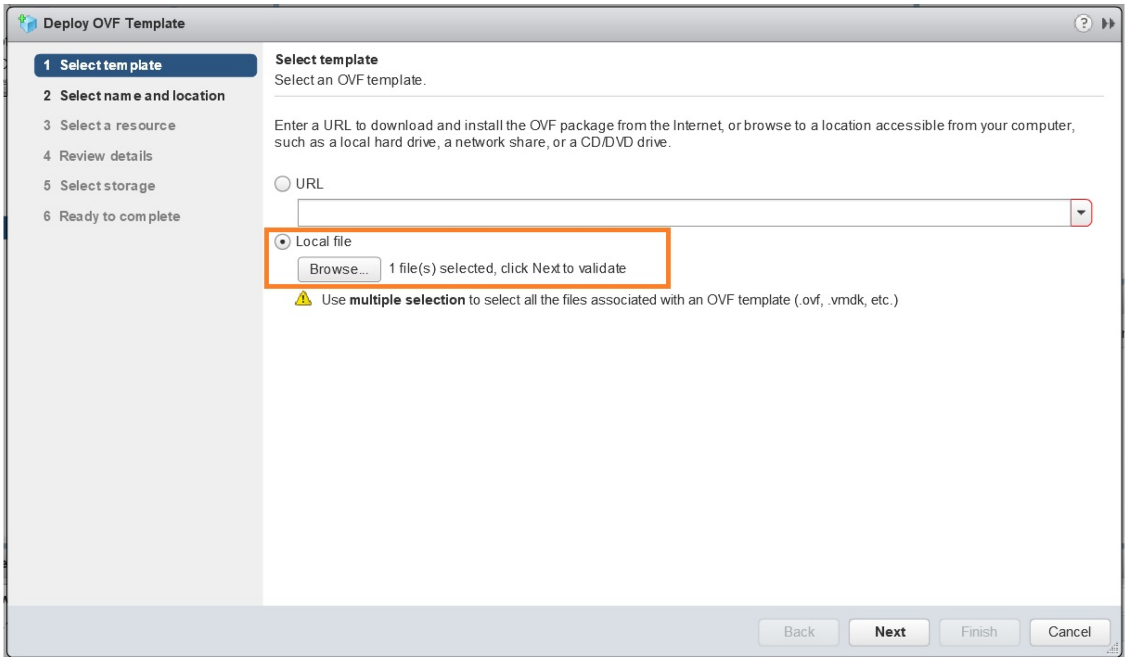
Step 1 Download the latest available Cisco Crosswork Change Automation and Health Insights image file (*.ova) to your system.

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.



Select template

Select an OVF template.

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

○ URL

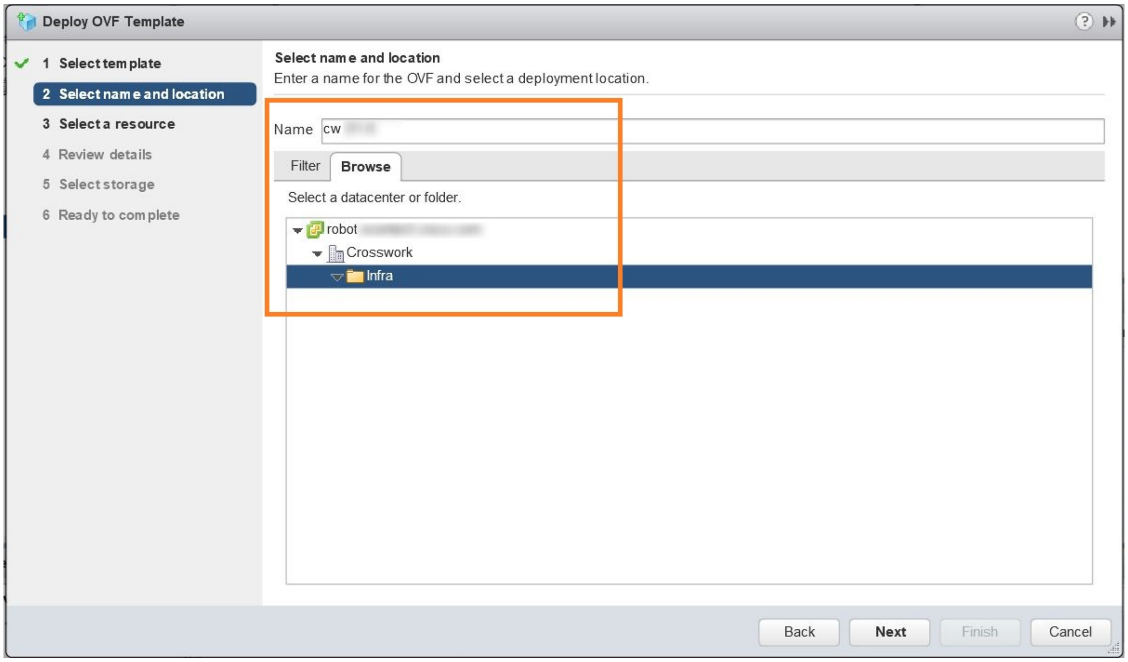
● Local file

Browse... 1 file(s) selected, click Next to validate

Use **multiple selection** to select all the files associated with an OVF template (.ovf, .vmdk, etc.)

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 Change Automation and Health Insights VM you are creating.

Cisco recommends that you include the Cisco Crosswork Change Automation and Health Insights version and build number in the name (for example: `Crosswork CA/HI 3.2 Build 283`).



Deploy OVF Template

1 Select template

2 Select name and location

3 Select a resource

4 Review details

5 Select storage

6 Ready to complete

Select name and location

Enter a name for the OVF and select a deployment location.

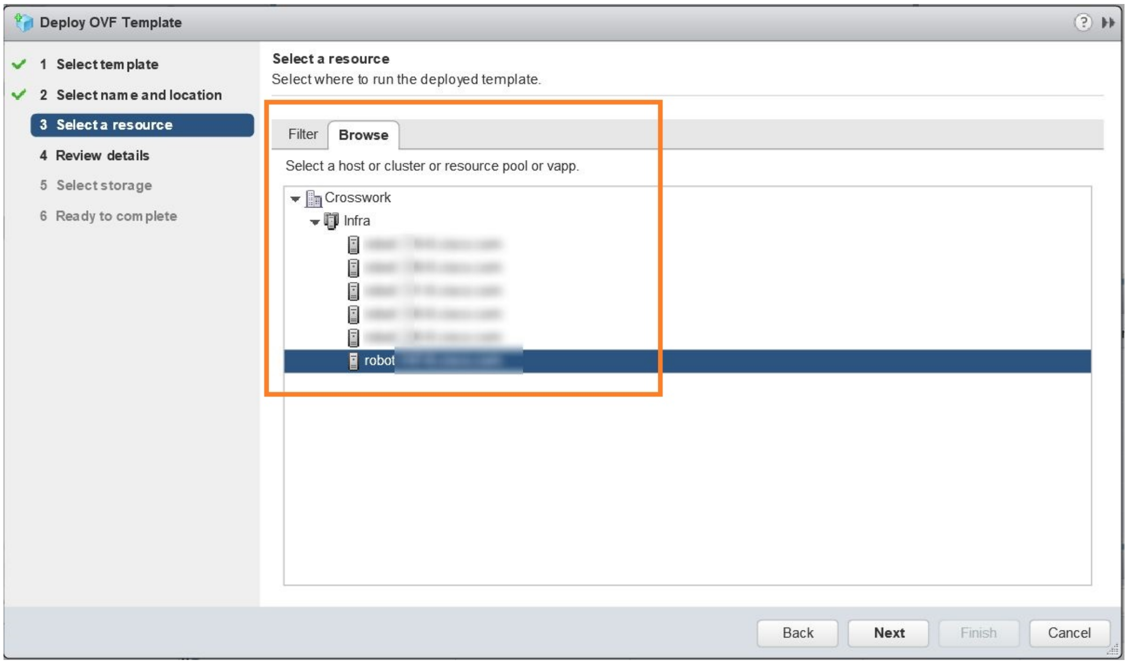
Name: cw [redacted]

Filter | Browse

Select a datacenter or folder.

- robot [redacted]
  - Crosswork
    - Infra

Step 5 Click **Next** to go to **3 - Select a resource**, similar to the following figure. Choose the Cisco Crosswork Change Automation and Health Insights VM's host.



Deploy OVF Template

1 Select template

2 Select name and location

3 Select a resource

4 Review details

5 Select storage

6 Ready to complete

Select a resource

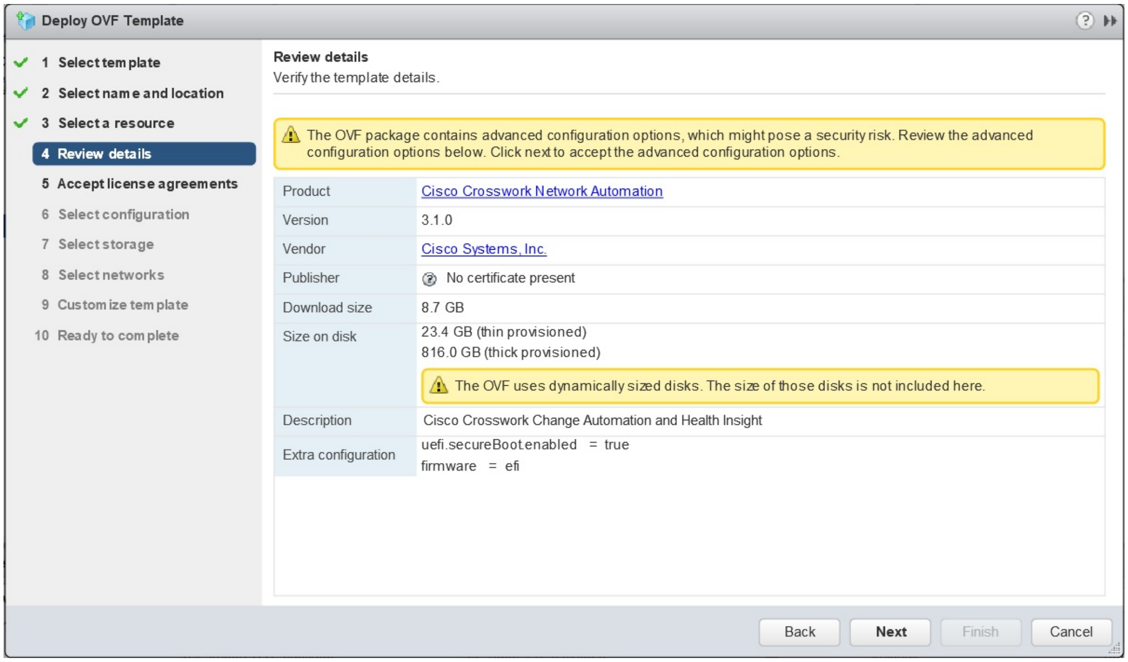
Select where to run the deployed template.

Filter | Browse

Select a host or cluster or resource pool or vapp.

- Crosswork
  - Infra
    - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]
    - robot [redacted]

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.



Review details
Verify the template details.

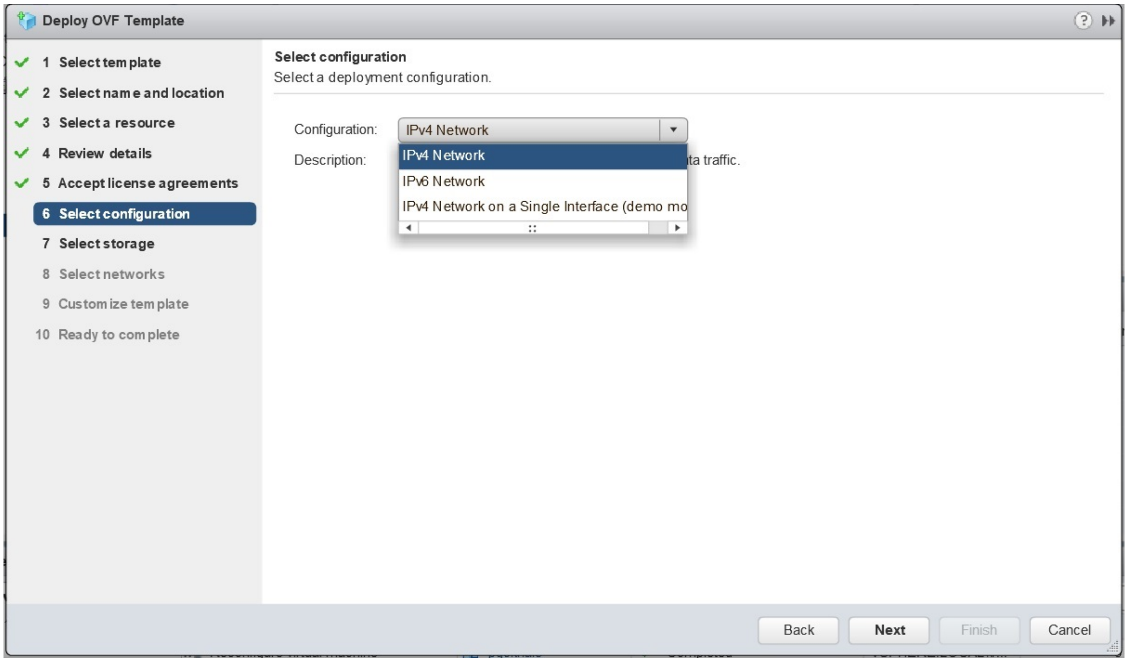
The OVF package contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below. Click next to accept the advanced configuration options.

Product	Cisco Crosswork Network Automation
Version	3.1.0
Vendor	Cisco Systems, Inc.
Publisher	No certificate present
Download size	8.7 GB
Size on disk	23.4 GB (thin provisioned) 816.0 GB (thick provisioned) The OVF uses dynamically sized disks. The size of those disks is not included here.
Description	Cisco Crosswork Change Automation and Health Insight

Extra configuration	uefi.secureBoot.enabled = true
	firmware = efi

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 **Note** The IPv4 on a Single Interface should only be used for demonstrations and lab installations.



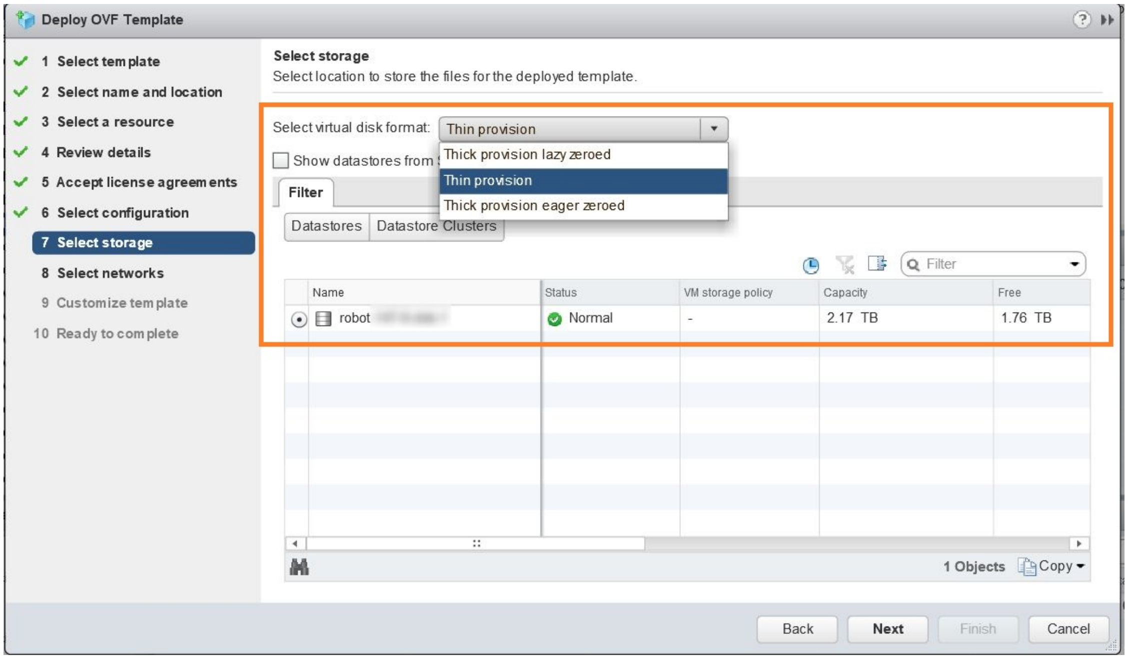
Select configuration
Select a deployment configuration.

Configuration: IPv4 Network

Description: ta traffic.

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.



Select storage

Select location to store the files for the deployed template.

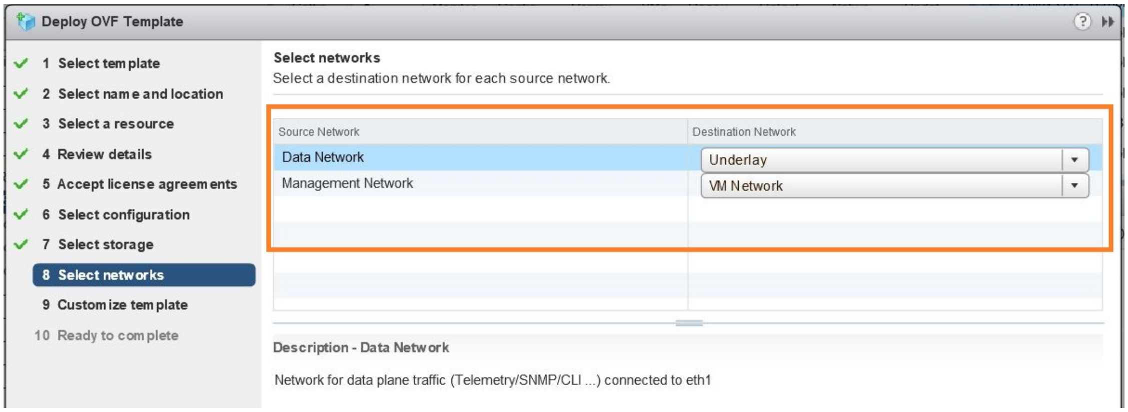
Select virtual disk format: Thin provision

- Thick provision lazy zeroed
- Thin provision
- Thick provision eager zeroed

□ Show datastores from

Name	Status	VM storage policy	Capacity	Free
● robot [redacted]	Normal	-	2.17 TB	1.76 TB

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.



Select networks

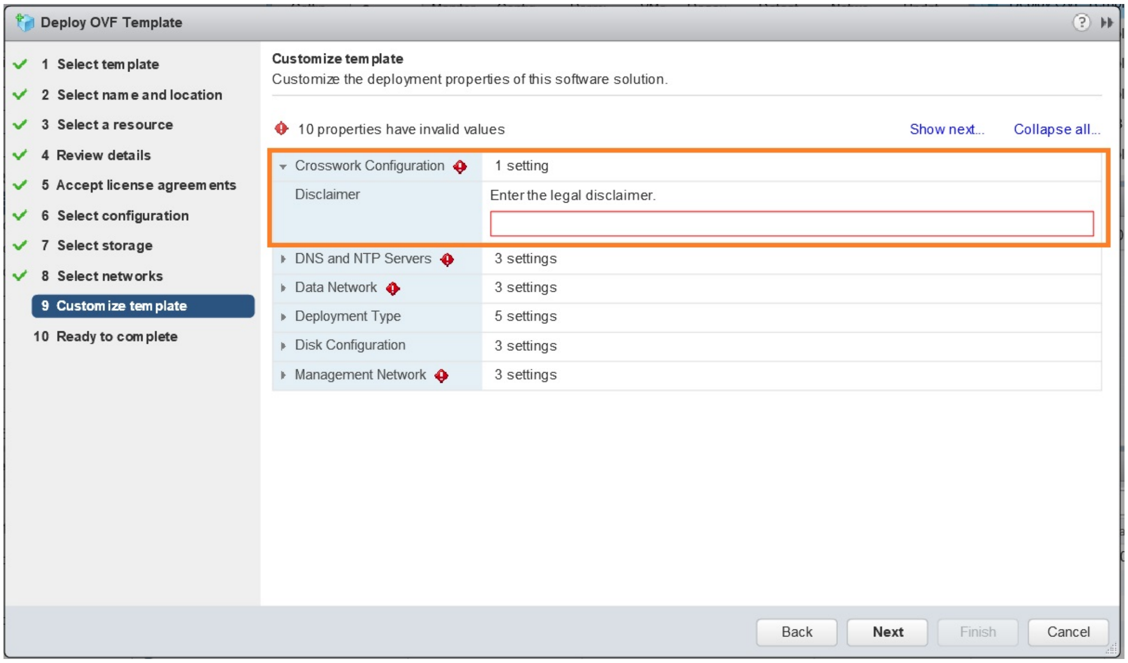
Select a destination network for each source network.

Source Network	Destination Network
Data Network	Underlay
Management Network	VM Network

Description - Data Network

Network for data plane traffic (Telemetry/SNMP/CLI ...) connected to eth1

Step 11 Click **Next** to go to **9 - Customize template**, with the **Crosswork Configuration** settings already expanded, similar to the following figure. Make entry in the **Disclaimer** field.



Deploy OVF Template

- ✓ 1 Select template
- ✓ 2 Select name and location
- ✓ 3 Select a resource
- ✓ 4 Review details
- ✓ 5 Accept license agreements
- ✓ 6 Select configuration
- ✓ 7 Select storage
- ✓ 8 Select networks
- 9 Customize template
- 10 Ready to complete

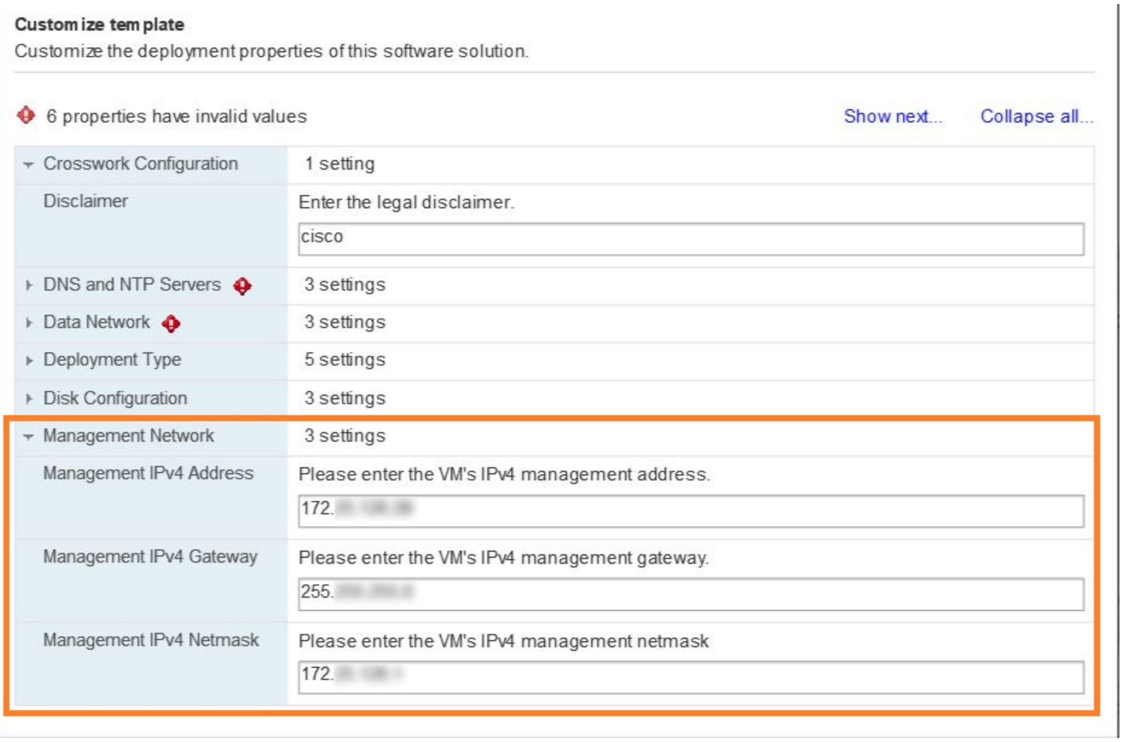
Customize template

Customize the deployment properties of this software solution.

10 properties have invalid values

Crosswork Configuration	1 setting
Disclaimer	Enter the legal disclaimer.
DNS and NTP Servers	3 settings
Data Network	3 settings
Deployment Type	5 settings
Disk Configuration	3 settings
Management Network	3 settings

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) or IPv6 deployment (**Management IPv6 Address**, **Management IPv6 Gateway**, and **Management IPv6 Prefix** fields) respectively.

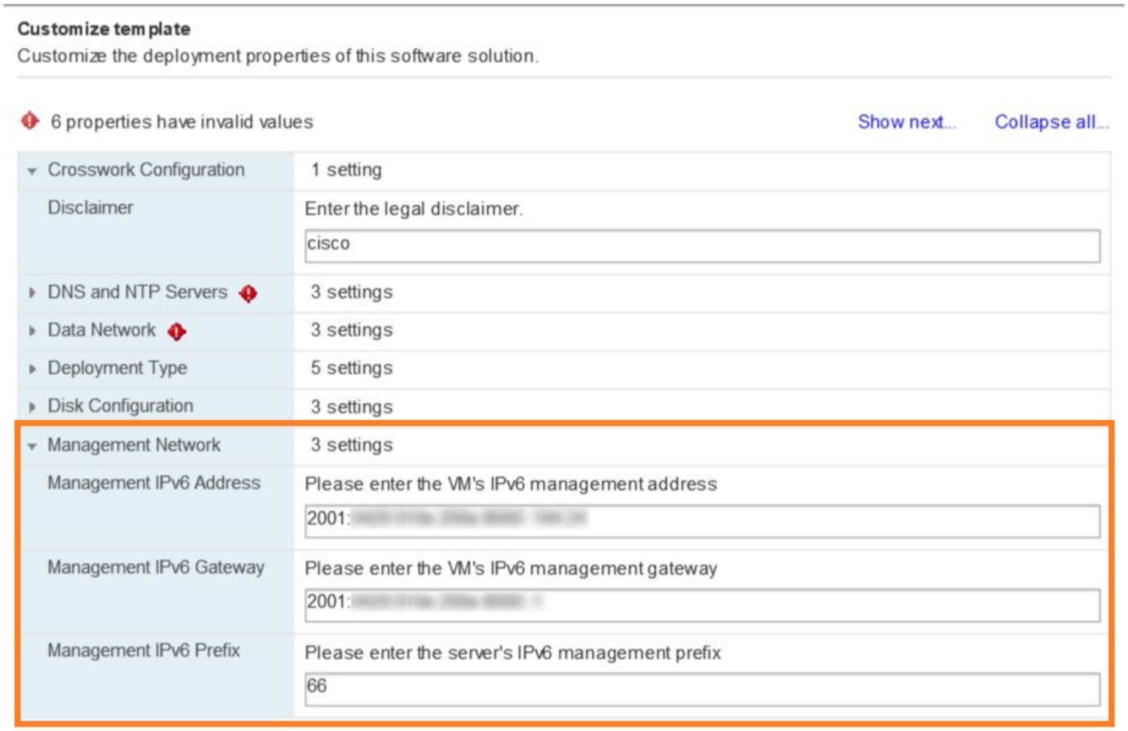


Customize template

Customize the deployment properties of this software solution.

6 properties have invalid values

Crosswork Configuration	1 setting
Disclaimer	Enter the legal disclaimer. cisco
DNS and NTP Servers	3 settings
Data Network	3 settings
Deployment Type	5 settings
Disk Configuration	3 settings
Management Network	3 settings
Management IPv4 Address	Please enter the VM's IPv4 management address. 172.[redacted]
Management IPv4 Gateway	Please enter the VM's IPv4 management gateway. 255.[redacted]
Management IPv4 Netmask	Please enter the VM's IPv4 management netmask 172.[redacted]



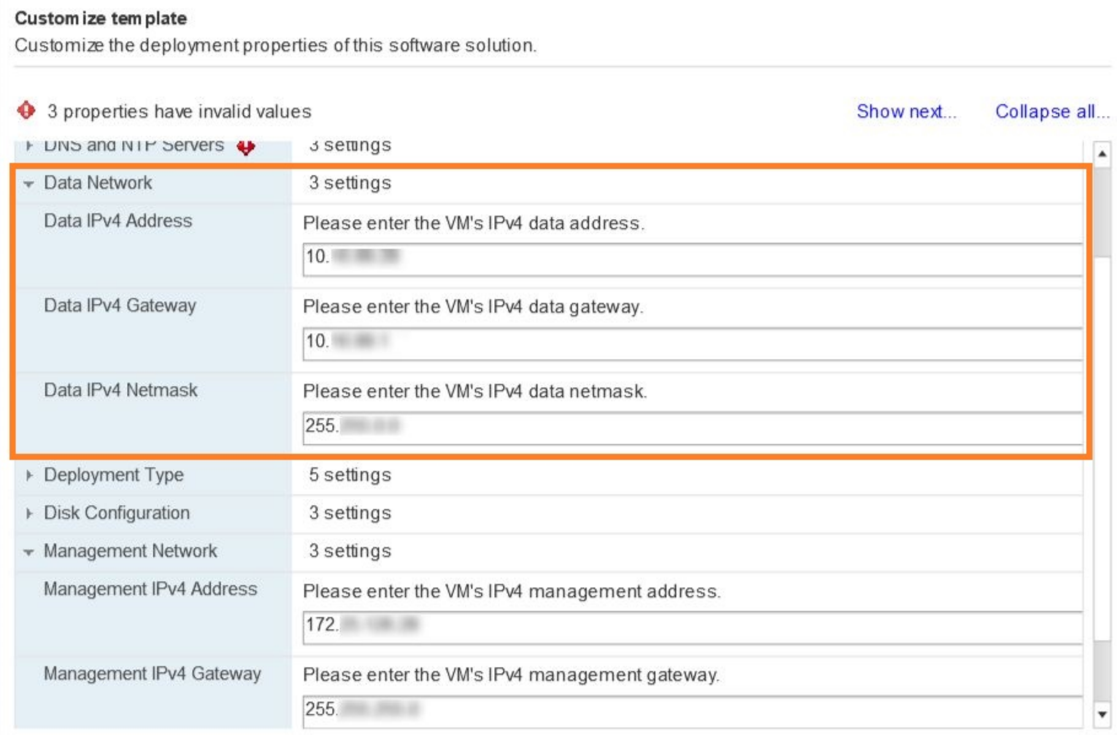
Customize template

Customize the deployment properties of this software solution.

6 properties have invalid values

▾ Crosswork Configuration	1 setting
Disclaimer	Enter the legal disclaimer. cisco
▸ DNS and NTP Servers	3 settings
▸ Data Network	3 settings
▸ Deployment Type	5 settings
▸ Disk Configuration	3 settings
▾ Management Network	3 settings
Management IPv6 Address	Please enter the VM's IPv6 management address 2001:[redacted]
Management IPv6 Gateway	Please enter the VM's IPv6 management gateway 2001:[redacted]
Management IPv6 Prefix	Please enter the server's IPv6 management prefix 66

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) or IPv6 deployment (**Data IPv6 Address**, **Data IPv6 Gateway**, and **Data IPv6 Prefix** fields) respectively.

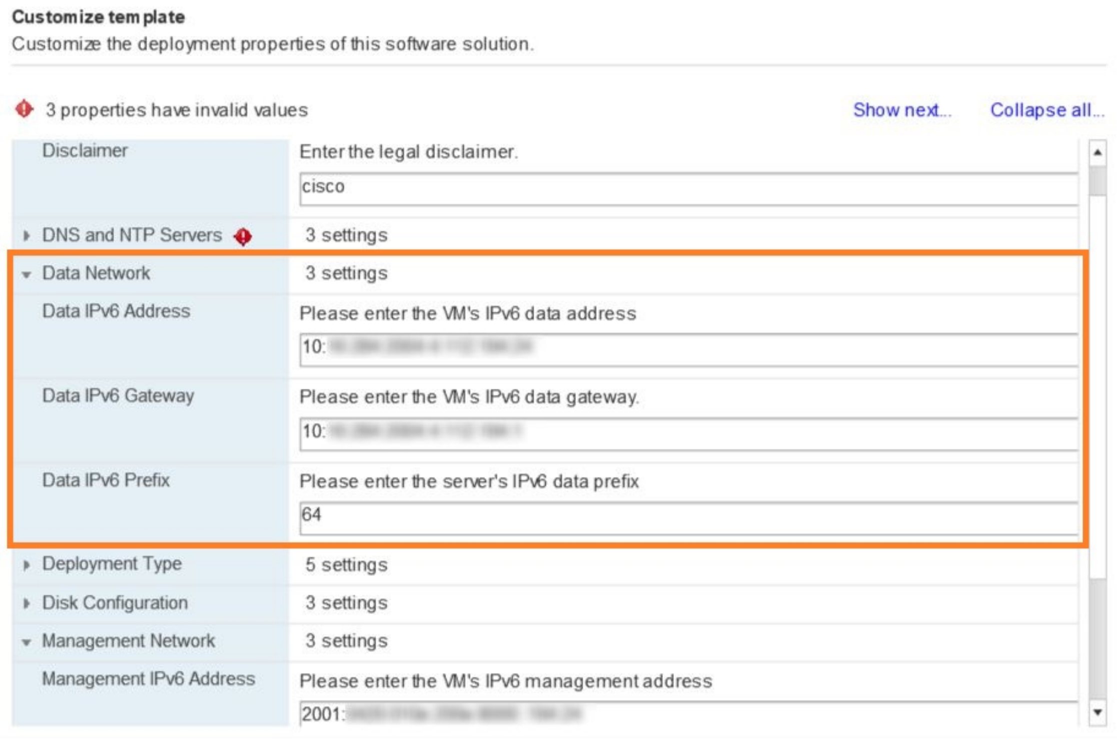


Customize template

Customize the deployment properties of this software solution.

3 properties have invalid values

DNS and NTP Servers	3 settings	
Data Network	3 settings	
Data IPv4 Address	Please enter the VM's IPv4 data address.	10.[redacted]
Data IPv4 Gateway	Please enter the VM's IPv4 data gateway.	10.[redacted]
Data IPv4 Netmask	Please enter the VM's IPv4 data netmask.	255.[redacted]
Deployment Type	5 settings	
Disk Configuration	3 settings	
Management Network	3 settings	
Management IPv4 Address	Please enter the VM's IPv4 management address.	172.[redacted]
Management IPv4 Gateway	Please enter the VM's IPv4 management gateway.	255.[redacted]



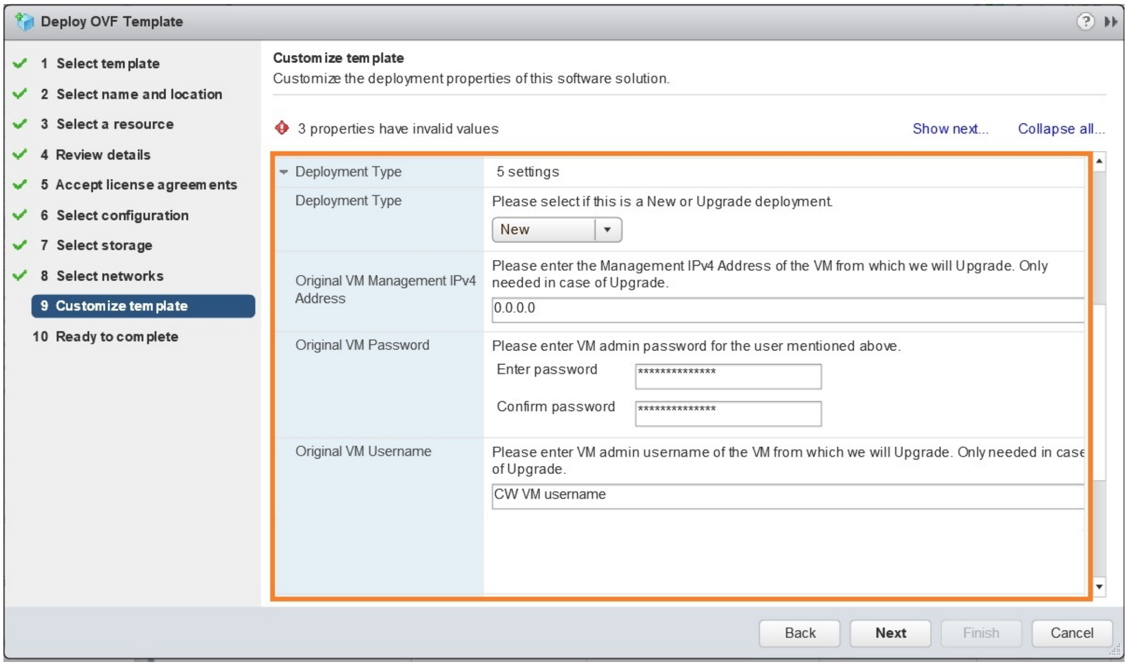
Customize template

Customize the deployment properties of this software solution.

3 properties have invalid values

Disclaimer	Enter the legal disclaimer.	cisco
DNS and NTP Servers	3 settings	
Data Network	3 settings	
Data IPv6 Address	Please enter the VM's IPv6 data address	10:[redacted]
Data IPv6 Gateway	Please enter the VM's IPv6 data gateway.	10:[redacted]
Data IPv6 Prefix	Please enter the server's IPv6 data prefix	64
Deployment Type	5 settings	
Disk Configuration	3 settings	
Management Network	3 settings	
Management IPv6 Address	Please enter the VM's IPv6 management address	2001:[redacted]

Step 14 Expand the **Deployment Type** settings, similar to the following figure. In the **Deployment Type** drop-down list, select **New**. You can leave the remaining fields blank or with the default values.



Customize template

Customize the deployment properties of this software solution.

3 properties have invalid values

Deployment Type: 5 settings

Deployment Type: Please select if this is a New or Upgrade deployment. New

Original VM Management IPv4 Address: Please enter the Management IPv4 Address of the VM from which we will Upgrade. Only needed in case of Upgrade. 0.0.0.0

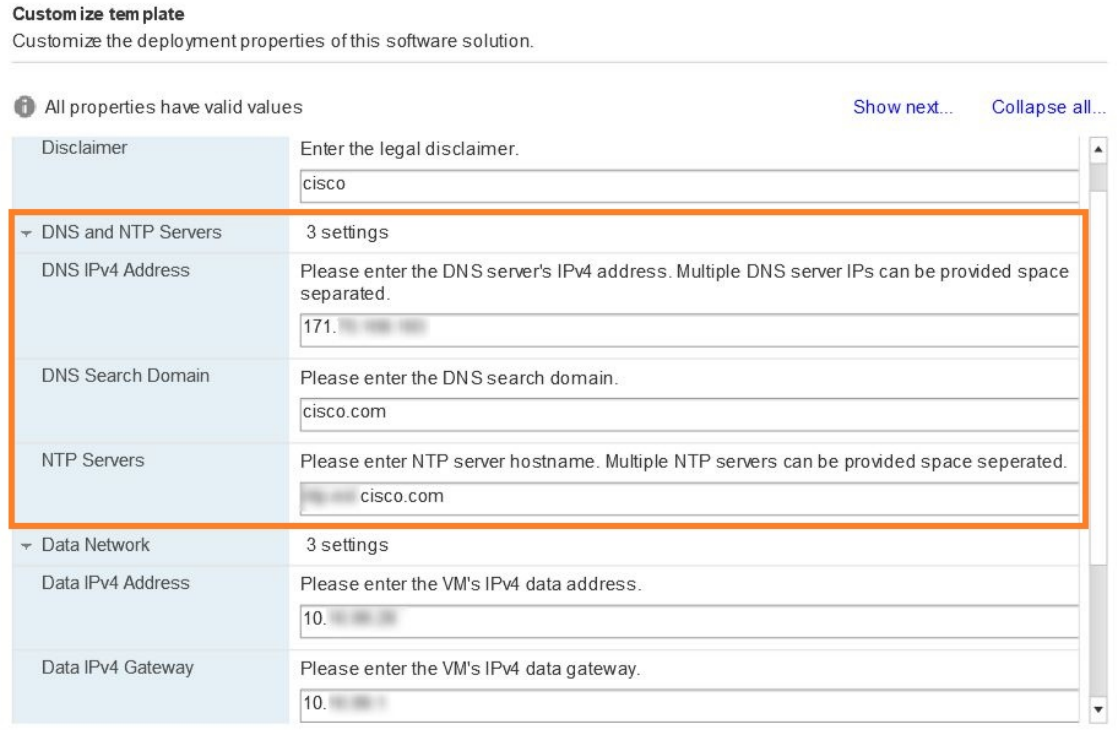
Original VM Password: Please enter VM admin password for the user mentioned above.
Enter password: **************
Confirm password: **************

Original VM Username: Please enter VM admin username of the VM from which we will Upgrade. Only needed in case of Upgrade. CW VM username

Step 15 Expand the **DNS and NTP Servers** settings, similar to the following figure. According to your deployment configuration (IPv4 or IPv6), 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 Change Automation and Health Insights 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.



Customize template
Customize the deployment properties of this software solution.

All properties have valid values

Disclaimer: Enter the legal disclaimer.
cisco

DNS and NTP Servers: 3 settings

DNS IPv4 Address: Please enter the DNS server's IPv4 address. Multiple DNS server IPs can be provided space separated.
171.[redacted]

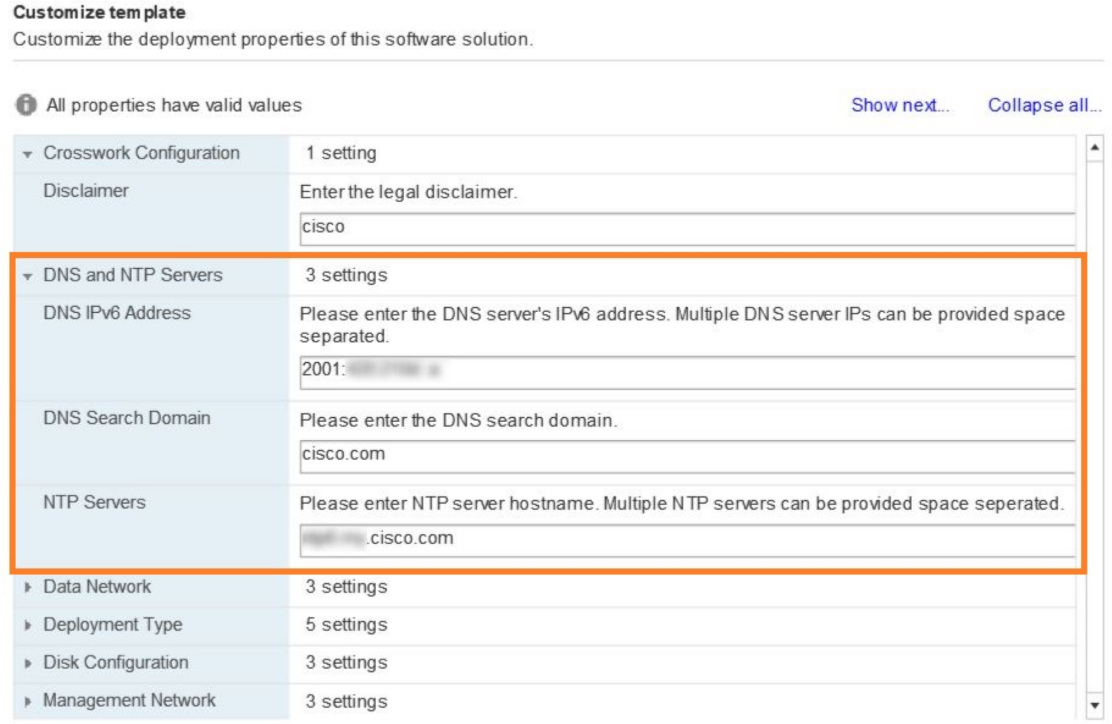
DNS Search Domain: Please enter the DNS search domain.
cisco.com

NTP Servers: Please enter NTP server hostname. Multiple NTP servers can be provided space seperated.
[redacted]cisco.com

Data Network: 3 settings

Data IPv4 Address: Please enter the VM's IPv4 data address.
10.[redacted]

Data IPv4 Gateway: Please enter the VM's IPv4 data gateway.
10.[redacted]



Customize template
Customize the deployment properties of this software solution.

All properties have valid values

Crosswork Configuration: 1 setting

Disclaimer: Enter the legal disclaimer.
cisco

DNS and NTP Servers: 3 settings

DNS IPv6 Address: Please enter the DNS server's IPv6 address. Multiple DNS server IPs can be provided space separated.
2001:[redacted]

DNS Search Domain: Please enter the DNS search domain.
cisco.com

NTP Servers: Please enter NTP server hostname. Multiple NTP servers can be provided space seperated.
[redacted].cisco.com

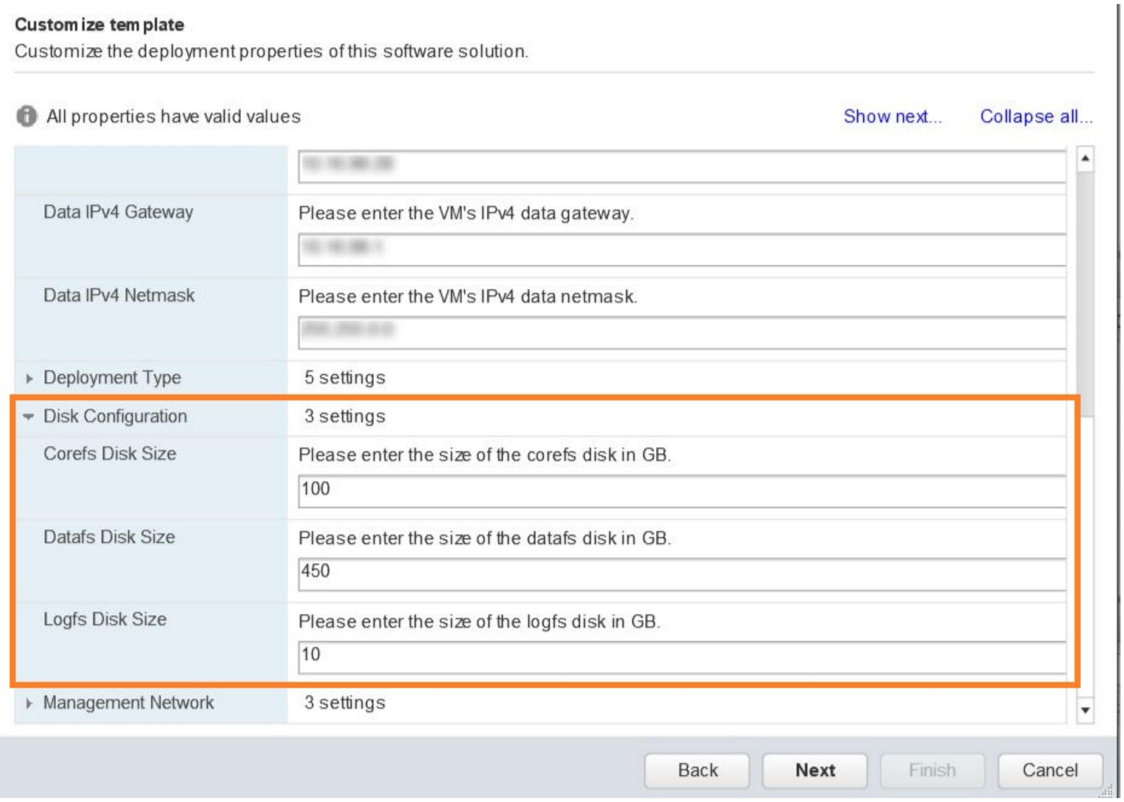
Data Network: 3 settings

Deployment Type: 5 settings

Disk Configuration: 3 settings

Management Network: 3 settings

Step 16 **Disk Configuration** settings allows you to adjust the amount of storage space available to Cisco Crosswork Change Automation and Health Insights. The default settings should work for most environments. For assistance in adding additional storage, contact the Cisco Customer Experience team.



Customize template
Customize the deployment properties of this software solution.
All properties have valid values
Show next...
Collapse all...
Back
Next
Finish
Cancel

[redacted]

Data IPv4 Gateway — Please enter the VM's IPv4 data gateway. [redacted]

Data IPv4 Netmask — Please enter the VM's IPv4 data netmask. [redacted]

Deployment Type — 5 settings

Disk Configuration — 3 settings

Corefs Disk Size — Please enter the size of the corefs disk in GB. 100

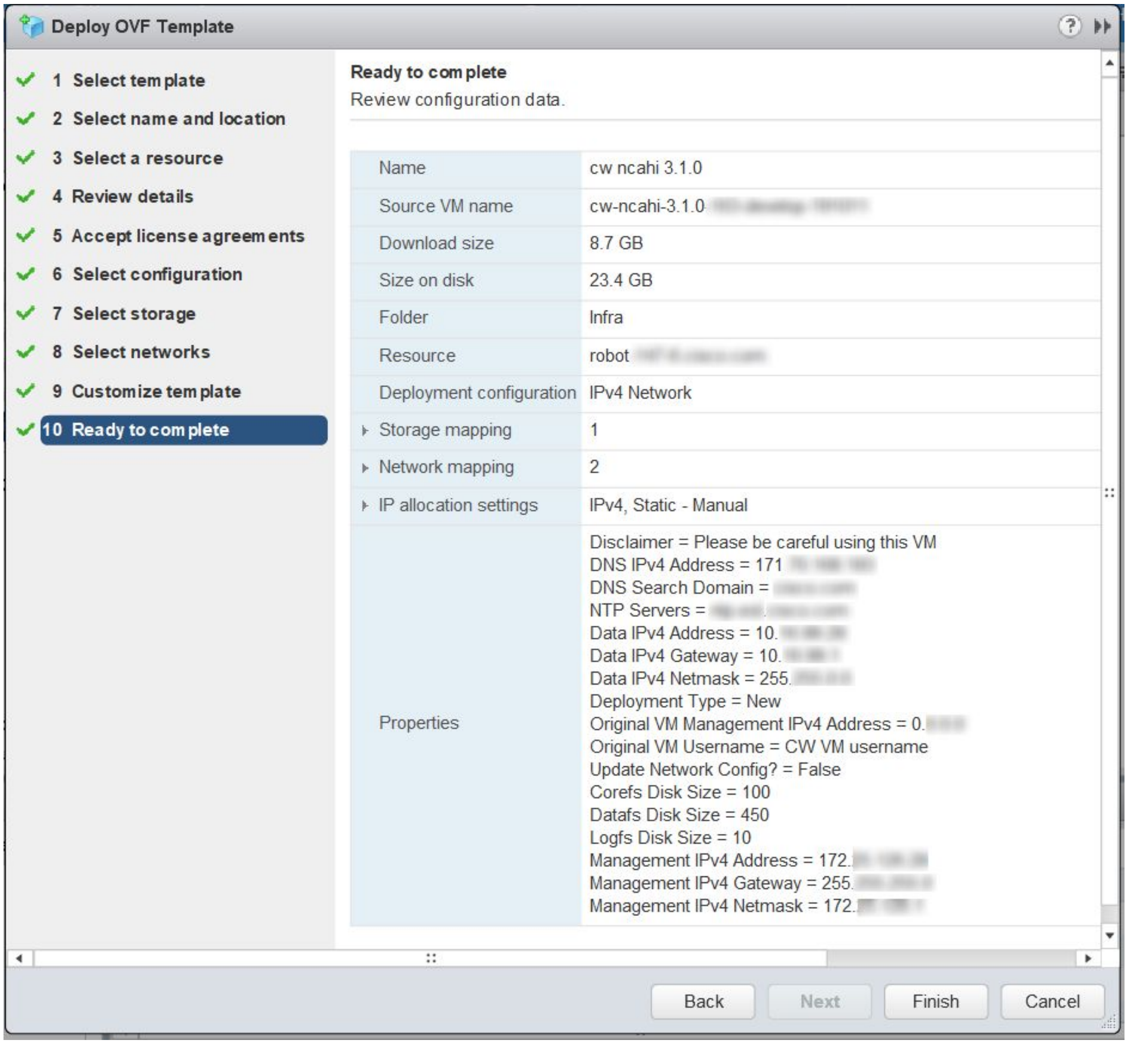
Datafs Disk Size — Please enter the size of the datafs disk in GB. 450

Logfs Disk Size — Please enter the size of the logfs disk in GB. 10

Management Network — 3 settings

Step 17 Expand the **Crosswork Configuration** and enter any legal disclaimer text (users will see this text if they log into the CLI).

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.



Ready to complete

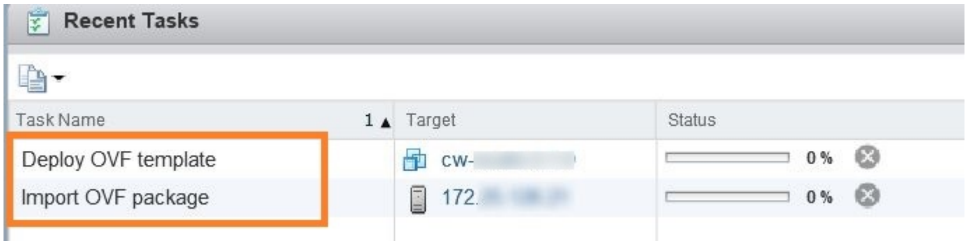
Review configuration data.

Name	cw ncahi 3.1.0
Source VM name	cw-ncahi-3.1.0 [redacted]
Download size	8.7 GB
Size on disk	23.4 GB
Folder	Infra
Resource	robot [redacted]
Deployment configuration	IPv4 Network
Storage mapping	1
Network mapping	2
IP allocation settings	IPv4, Static - Manual
Properties	Disclaimer = Please be careful using this VM DNS IPv4 Address = 171 [redacted] DNS Search Domain = [redacted] NTP Servers = [redacted] Data IPv4 Address = 10. [redacted] Data IPv4 Gateway = 10. [redacted] Data IPv4 Netmask = 255. [redacted] Deployment Type = New Original VM Management IPv4 Address = 0. [redacted] Original VM Username = CW VM username Update Network Config? = False Corefs Disk Size = 100 Datafs Disk Size = 450 Logfs Disk Size = 10 Management IPv4 Address = 172. [redacted] Management IPv4 Gateway = 255. [redacted] Management IPv4 Netmask = 172. [redacted]

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.

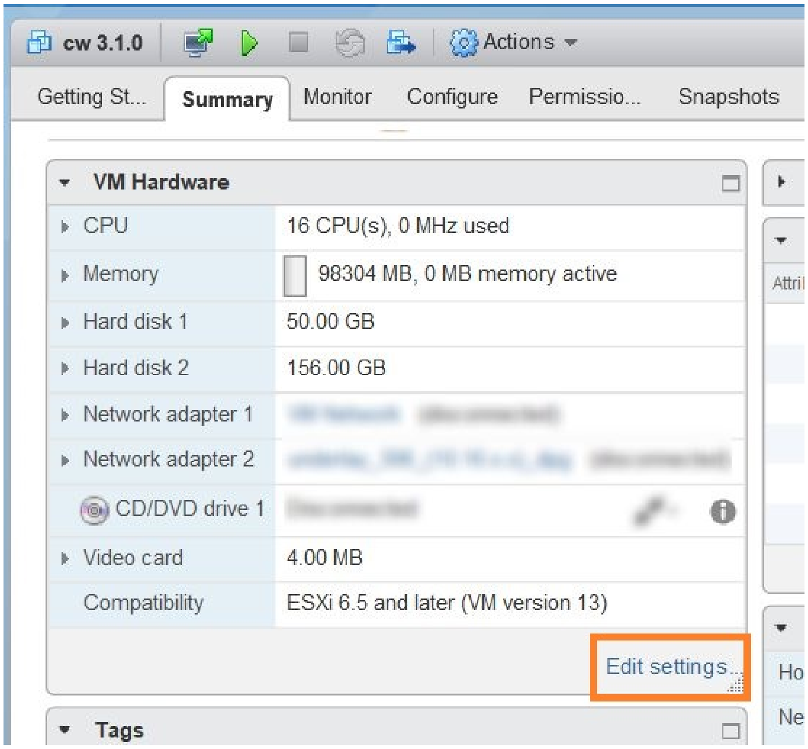


Recent Tasks

Task Name 1 ▲	Target	Status
Deploy OVF template	cw- [redacted]	0 %
Import OVF package	172. [redacted]	0 %

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

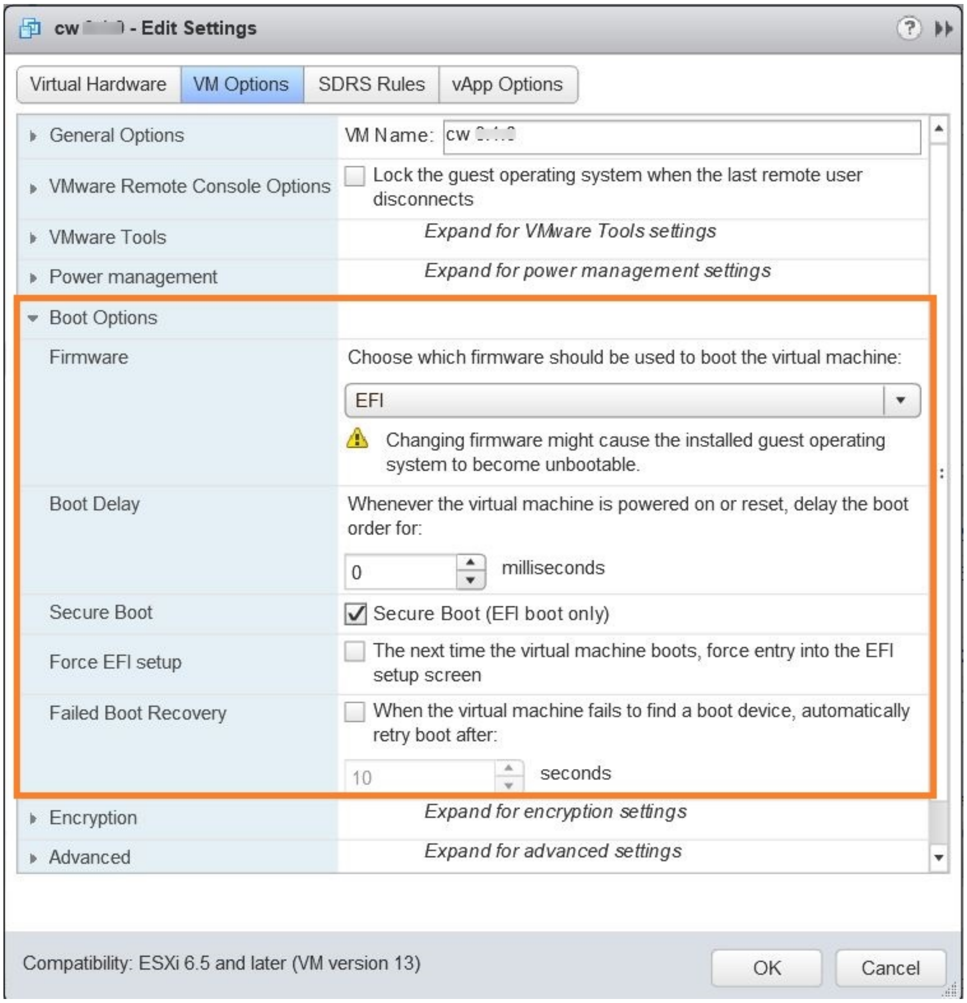
a) On the host VM **Summary** tab, below the **VM Hardware** table, click **Edit Settings**, similar to the following figure.



CPU	16 CPU(s), 0 MHz used
Memory	98304 MB, 0 MB memory active
Hard disk 1	50.00 GB
Hard disk 2	156.00 GB
Network adapter 1	[redacted]
Network adapter 2	[redacted]
CD/DVD drive 1	[redacted]
Video card	4.00 MB
Compatibility	ESXi 6.5 and later (VM version 13)

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.



cw [redacted] - Edit Settings

General Options — VM Name: cw [redacted]

VMware Remote Console Options — □ Lock the guest operating system when the last remote user disconnects

VMware Tools — *Expand for VMware Tools settings*

Power management — *Expand for power management settings*

Boot Options

Firmware — Choose which firmware should be used to boot the virtual machine: EFI

Changing firmware might cause the installed guest operating system to become unbootable.

Boot Delay — Whenever the virtual machine is powered on or reset, delay the boot order for: 0 milliseconds

Secure Boot — ☑ Secure Boot (EFI boot only)

Force EFI setup — □ The next time the virtual machine boots, force entry into the EFI setup screen

Failed Boot Recovery — □ When the virtual machine fails to find a boot device, automatically retry boot after: 10 seconds

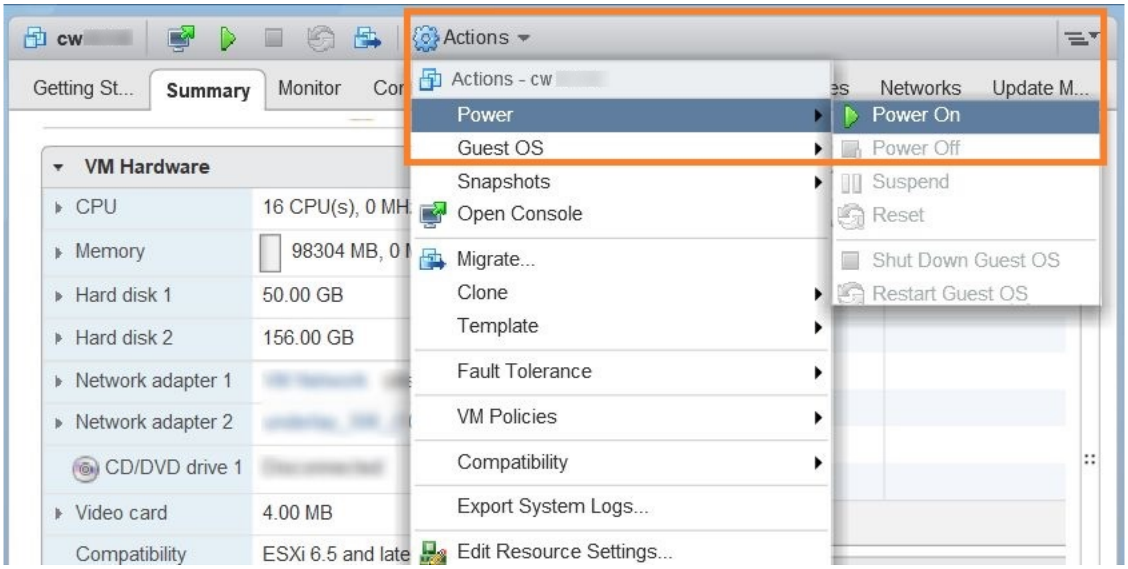
Encryption — *Expand for encryption settings*

Advanced — *Expand for advanced settings*

Compatibility: ESXi 6.5 and later (VM version 13)

Step 21 You can now power on the Cisco Crosswork Change Automation and Health Insights VM to complete the deployment process. Expand the host’s entry so you can click the Cisco Crosswork Change Automation and Health Insights 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 Change Automation and Health Insights VM to become operational. Please wait for the process to finish before continuing.

Install Cisco Crosswork Change Automation and Health Insights Via OVF Tool

Note

- Use vCenter UI to start the VM or the OVF tool command line.
- VMware OVF tool version 4.3 is required for this procedure.

Sample script for IPv4 deployment:

```
#!/bin/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}
cd..
```

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

# This deployment is for IPv4.
Deployment="cw_ipv4"
DM="thin"

corefs="100"
datafs="450"
logfs="10"

VM_NAME=<mention the VM name>

ManagementIPv4Address=<Management IPv4 Address>
ManagementIPv4Netmask=<Management IPv4 Netmask>
ManagementIPv4Gateway=<Management IPv4 Gateway>
RouterIPv4Address=<Router IPv4 Address>
RouterIPv4Netmask=<Router IPv4 Netmask>
RouterIPv4Gateway=<Router IPv4 Gateway>
DNSv4=<DNS>
NTP=<NTP>
Domain=<Domain Name>

Disclaimer=<add a relevant disclaimer>

# Please replace this information according to your vcenter setup
VCENTER_LOGIN=<vCenter login details>
VCENTER_PATH=<vCenter path>
DS=<DS details>

ovftool --acceptAllEulas --skipManifestCheck --X:injectOvfEnv -ds=$DS --diskMode=$DM \
--overwrite --powerOffTarget --powerOn --noSSLVerify \
--allowExtraConfig \
--name="$VM_NAME" \
--net:"Data Network=Change Me" \
--deploymentOption="${Deployment}" \
--prop:"ManagementIPv4Address=${ManagementIPv4Address}" \
--prop:"ManagementIPv4Netmask=${ManagementIPv4Netmask}" \
--prop:"ManagementIPv4Gateway=${ManagementIPv4Gateway}" \
--prop:"DataIPv4Address=${RouterIPv4Address}" \
--prop:"DataIPv4Netmask=${RouterIPv4Netmask}" \
--prop:"DataIPv4Gateway=${RouterIPv4Gateway}" \
--prop:"DNSv4=${DNSv4}" \
--net:"Management Network=VM Network" \
--prop:"NTP=${NTP}" \
--prop:"Domain=${Domain}" \
--prop:corefs=${corefs} \
--prop:ddatafs=${datafs} \
--prop:logfs=${logfs} \
--prop:"Disclaimer=${Disclaimer}" \
--sourceType=OVA \
"$filename" \
vi://$VCENTER_LOGIN/$VCENTER_PATH
```

Sample script for IPv6 deployment:

```
#!/bin/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}
cd..
filename=`find $ova_path -name \*.ova`

# This deployment is for IPv6.
Deployment="cw_ipv6"
DM="thin"

corefs="100"
datafs="450"
logfs="10"

VM_NAME=<mention the VM name>

ManagementIPv6Address=<Management IPv6 Address>
ManagementIPv6Netmask=<Management IPv6 Netmask>
ManagementIPv6Gateway=<Management IPv6 Gateway>
RouterIPv6Address=<Router IPv6 Address>
RouterIPv6Netmask=<Router IPv6 Netmask>
RouterIPv6Gateway=<Router IPv6 Gateway>
DNSv6=<DNS>
NTP=<NTP>
Domain=<Domain Name>

Disclaimer=<add a relevant disclaimer>

# Please replace this information according to your vcenter setup
VCENTER_LOGIN=<vCenter login details>
VCENTER_PATH=<vCenter path>
DS=<DS details>

ovftool --acceptAllEulas --skipManifestCheck --X:injectOvfEnv -ds=$DS --diskMode=$DM \
--overwrite --powerOffTarget --powerOn --noSSLVerify \
--allowExtraConfig \
--name="$VM_NAME" \
--net:"Data Network=Change Me" \
--deploymentOption="${Deployment}" \
--prop:"ManagementIPv6Address=${ManagementIPv6Address}" \
--prop:"ManagementIPv6Netmask=${ManagementIPv6Netmask}" \
--prop:"ManagementIPv6Gateway=${ManagementIPv6Gateway}" \
--prop:"DataIPv6Address=${RouterIPv6Address}" \
--prop:"DataIPv6Netmask=${RouterIPv6Netmask}" \
--prop:"DataIPv6Gateway=${RouterIPv6Gateway}" \
--prop:"DNSv6=${DNSv6}" \
--net:"Management Network=VM Network" \
--prop:"NTP=${NTP}" \
--prop:"Domain=${Domain}" \
--prop:corefs=${corefs} \
--prop:ddatafs=${datafs} \
--prop:logfs=${logfs} \
--prop:"Disclaimer=${Disclaimer}" \
--sourceType=OVA \
"$filename" \
vi://$VCENTER_LOGIN/$VCENTER_PATH
```

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 Cisco Crosswork Change Automation and Health Insights 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 35. After you have identified the error, perform the following:

a) Power off the Cisco Crosswork Change Automation and Health Insights VM.

b) Delete the Cisco Crosswork Change Automation and Health Insights 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 Change Automation and Health Insights 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 35.

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

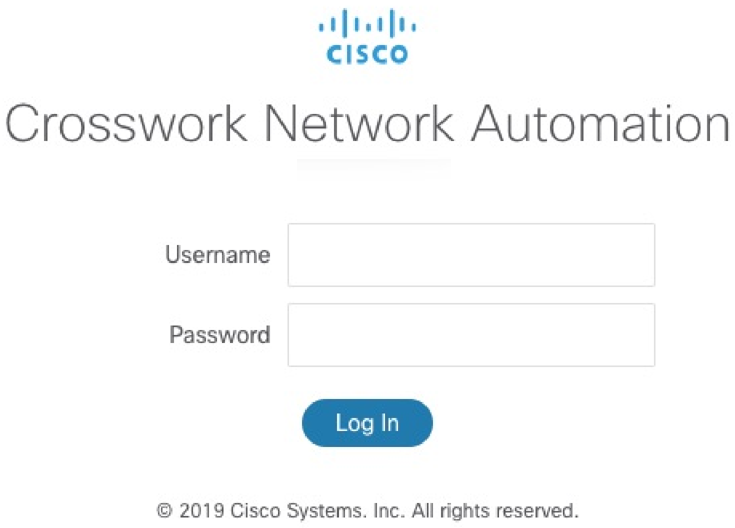
Step 2 In the browser's address bar, enter:

```
https://<Crosswork_VM_management_IP_adddress>:30603/
```

The **Log In** window opens, as shown in the following figure.

When you access Cisco Crosswork Change Automation and Health Insights 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 Change Automation and Health Insights 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 Change Automation and Health Insights User Guide.

Figure 3: Cisco Crosswork Network Change Automation and Health Insights Log In Window



© 2019 Cisco Systems. Inc. All rights reserved.

Step 3 Log into Cisco Crosswork Change Automation and Health Insights as follows:

a) Enter the Cisco Crosswork Change Automation and Health Insights administrator username **`admin`** and the default password **`admin`**.

b) Click **Log In**.

c) When prompted to change the Cisco Crosswork Change Automation and Health Insights 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 Change Automation and Health Insights, 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 7: Troubleshoot the Installation

Issue	Action
Cannot Connect to the VM	

Issue	Action
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 34. 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	
Browser does not display the login screen.	1. Make sure you are using a supported browser (see Supported Web Browsers, on page 9 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 34. 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.

Issue	Action
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	
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 Change Automation and Health Insights User Guide* topic "Monitor Cisco Crosswork Infrastructure and Resources".

Issue	Action
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 Change Automation and Health Insights 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 (for example, Cisco Crosswork Change Automation and Health Insights) 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. The Cisco Crosswork Change Automation and Health Insights VM does not come with a CPU or Memory set, allowing for a flexibility in deployment.

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.

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

OVF Parameter	Description	Deployment Scenario
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. However, if you want to use third-party or your own certificate files, then you must input these three parameters. **Note** The host with the URI files must be reachable on the network and files must be present at the time of install.
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.	
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**		
Management IPv6 Method*	How the Management interface gets its IPv6 address.	
Management IPv6 Address	IPv6 address of the management interface.	

OVF Parameter	Description	Deployment Scenario
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.	
Northbound Data IPv4 Gateway	IPv4 address of the Northbound data gateway.	
[1]**Northbound Data IPv6 Address**		

OVF Parameter	Description	Deployment Scenario
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 Change Automation and Health Insights. 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 Change Automation and Health Insights 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 Change Automation and Health Insights. **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 Change Automation and Health Insights.	

OVF Parameter	Description	Deployment Scenario
Controller Signing Certificate File URI	PEM formatted root cert of Cisco Crosswork Change Automation and Health Insights 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 Change Automation and Health Insights 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. 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`
Enrollment Passphrase	SCP user passphrase to transfer enrollment package.	

[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 If you are not using the default SCP port 22, you can specify the port as a part of the SCP command. For example,

```
-P55 user@host:path/to/file
```

where 55 is a custom port.

Ensure the following:

- You are creating the Cisco Crosswork Data Gateway VM on a recommended VMware version (See Virtual Machine (VM) Requirements, on page 10 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 Change Automation and Health Insights 3.2 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.

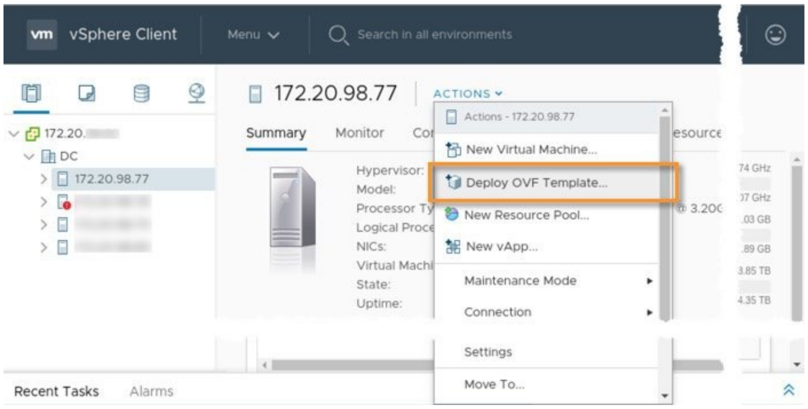
In case of lost or forgotten passwords, the user would have to create a new VM, destroy the current VM, and re-enroll the new one on the Cisco Crosswork Change Automation and Health Insights.

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

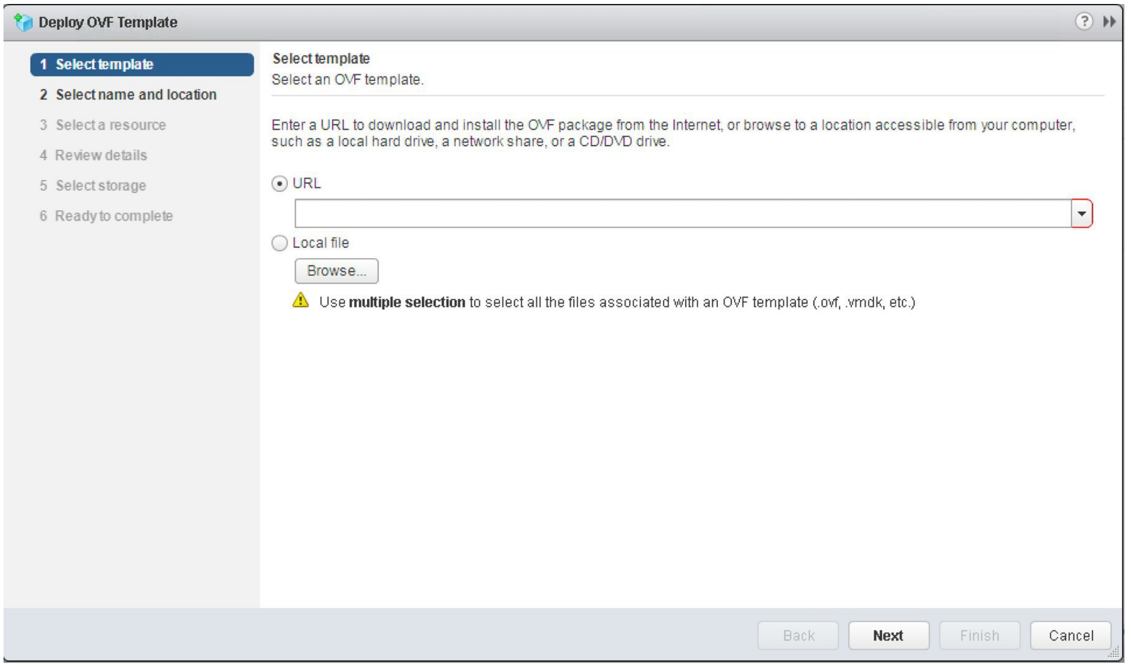
Note Cisco recommends using Cisco Crosswork Data Gateway 1.1.2 with Cisco Crosswork Change Automation and Health Insights 3.2.

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.


Deploy OVF Template

1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Select storage
6 Ready to complete

Select template
Select an OVF template.

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

● URL

○ Local file

Browse...

Use **multiple selection** to select all the files associated with an OVF template (.ovf, .vmdk, etc.)

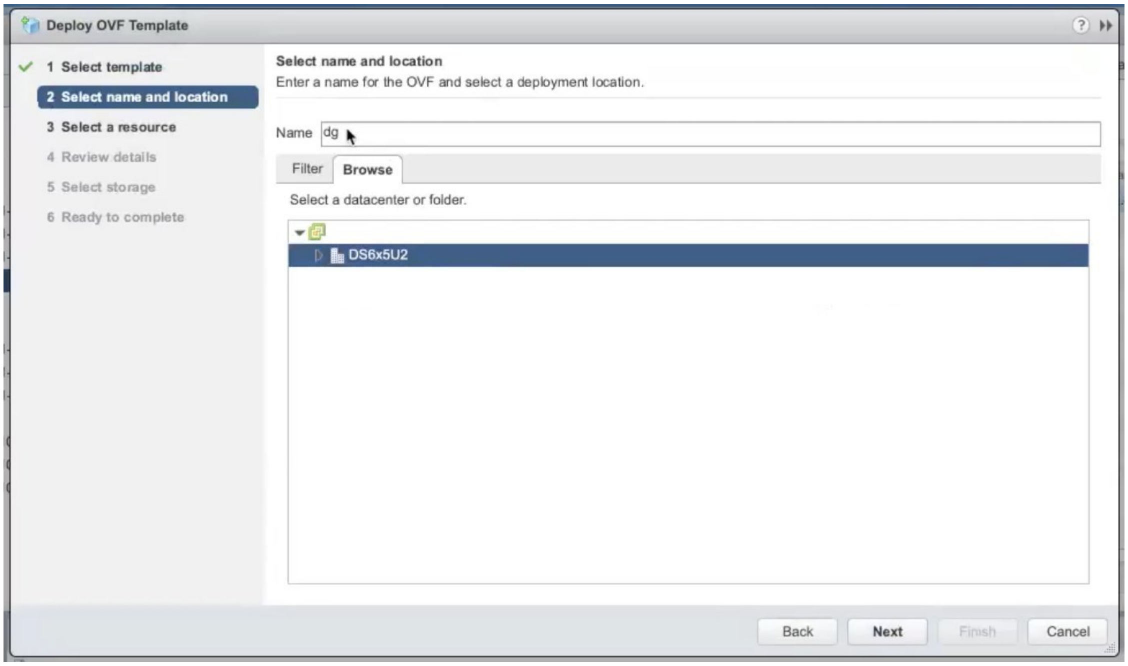
Back | Next | Finish | Cancel

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.



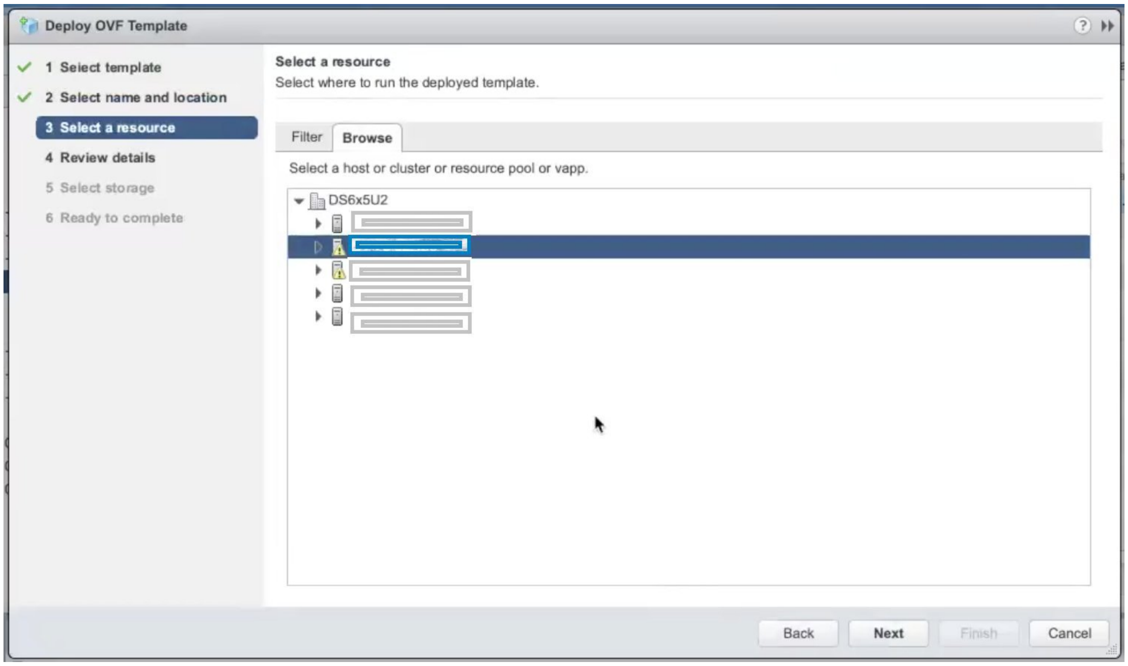
Select name and location

Enter a name for the OVF and select a deployment location.

Name: dg

Select a datacenter or folder.

Step 5 Click **Next** to go to **3 Select a resource**, as shown in the following figure. Choose the VM’s host.



Select a resource

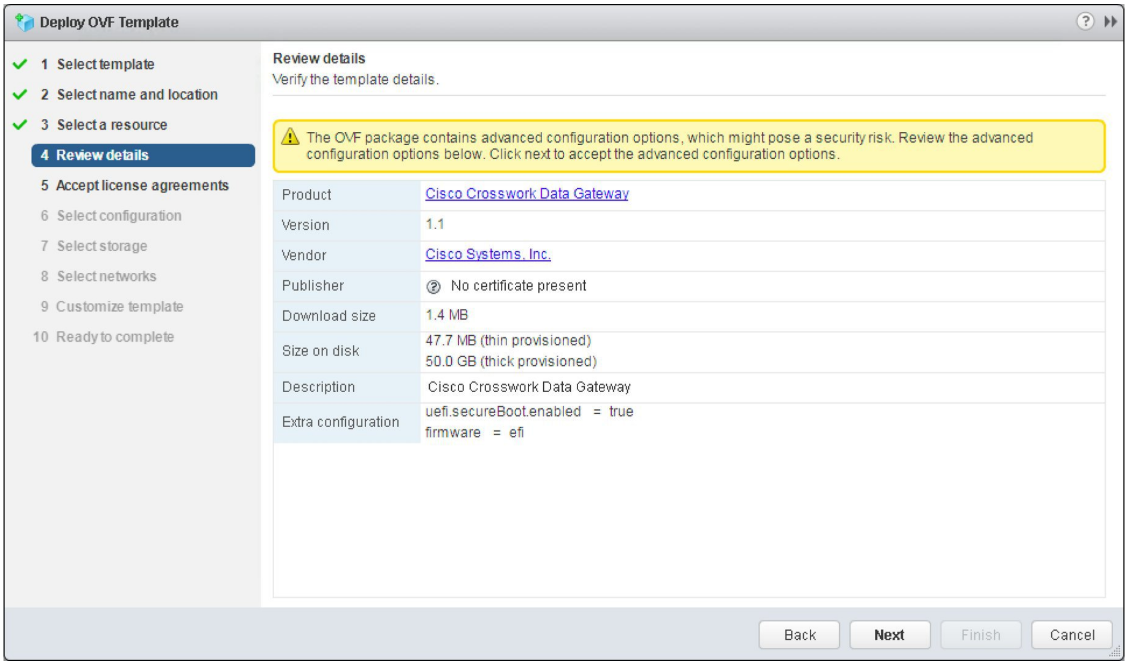
Select where to run the deployed template.

Select a host or cluster or resource pool or vapp.

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.



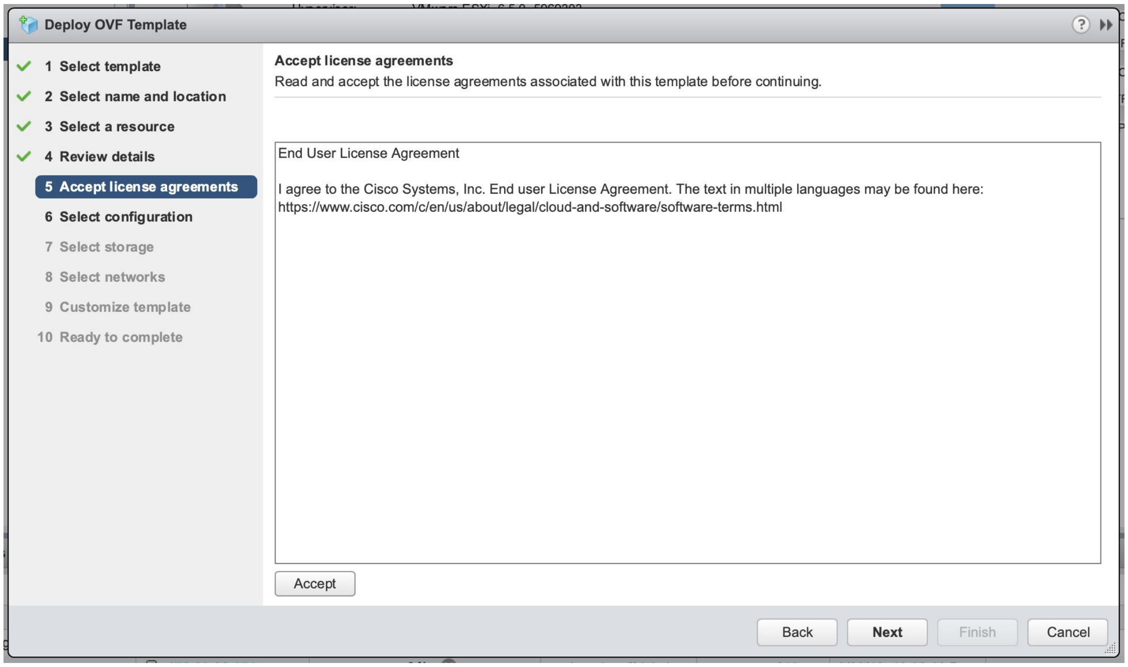
Review details
Verify the template details.

⚠ The OVF package contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below. Click next to accept the advanced configuration options.

Product	Cisco Crosswork Data Gateway
Version	1.1
Vendor	Cisco Systems, Inc.
Publisher	No certificate present
Download size	1.4 MB
Size on disk	47.7 MB (thin provisioned) 50.0 GB (thick provisioned)
Description	Cisco Crosswork Data Gateway

Extra configuration	uefi.secureBoot.enabled = true
	firmware = efi

Step 7 Click **Next** to go to **5 accept license agreements**. Review the End User License Agreement and click **Accept**.

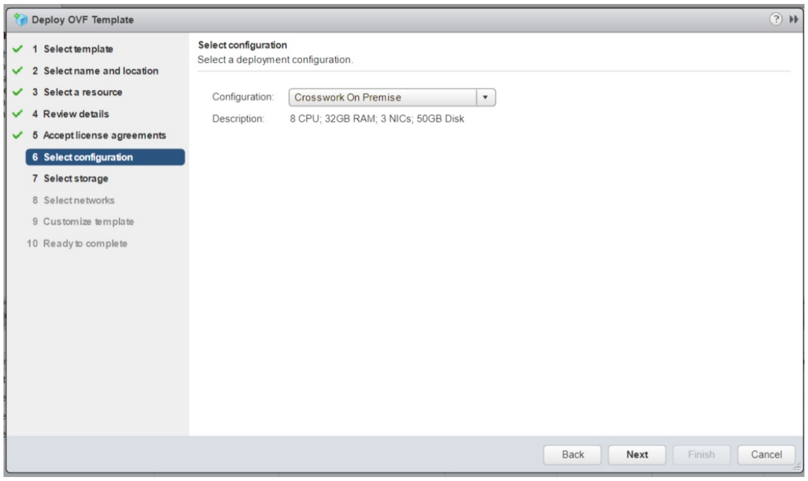


Accept license agreements
Read and accept the license agreements associated with this template before continuing.

End User License Agreement

I agree to the Cisco Systems, Inc. End user License Agreement. The text in multiple languages may be found here: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html

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 Change Automation and Health Insights, you must select **Crosswork On Premise** from the **Configuration** dropdown.



Select configuration

Select a deployment configuration.

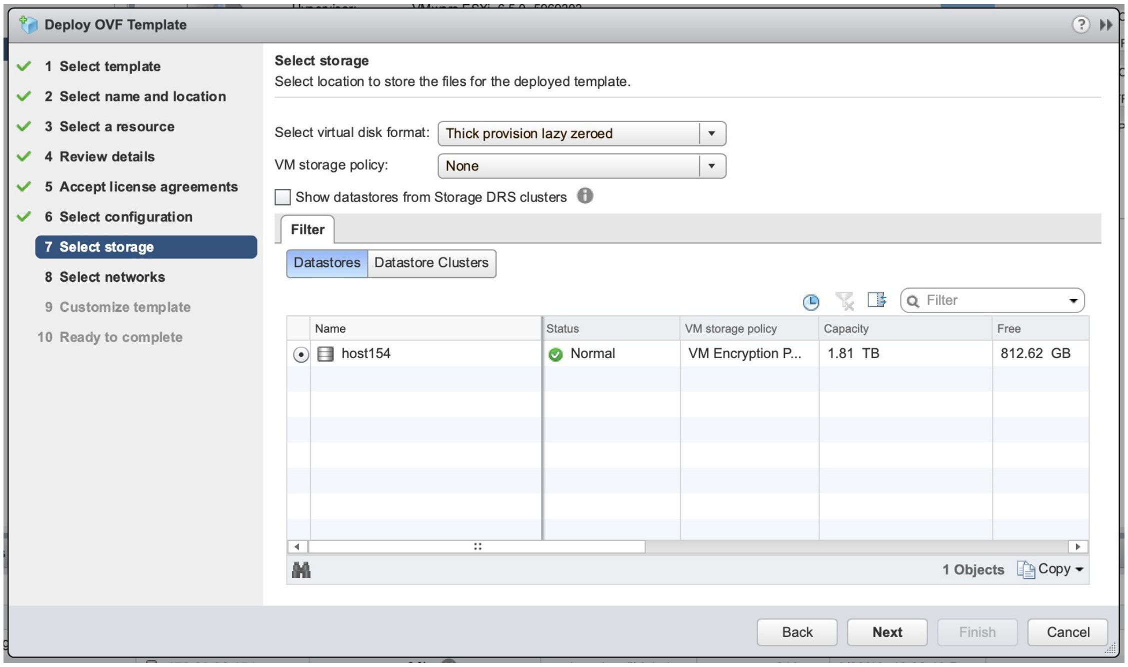
Configuration: Crosswork On Premise

Description: 8 CPU; 32GB RAM; 3 NICs; 50GB Disk

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.



Select storage

Select location to store the files for the deployed template.

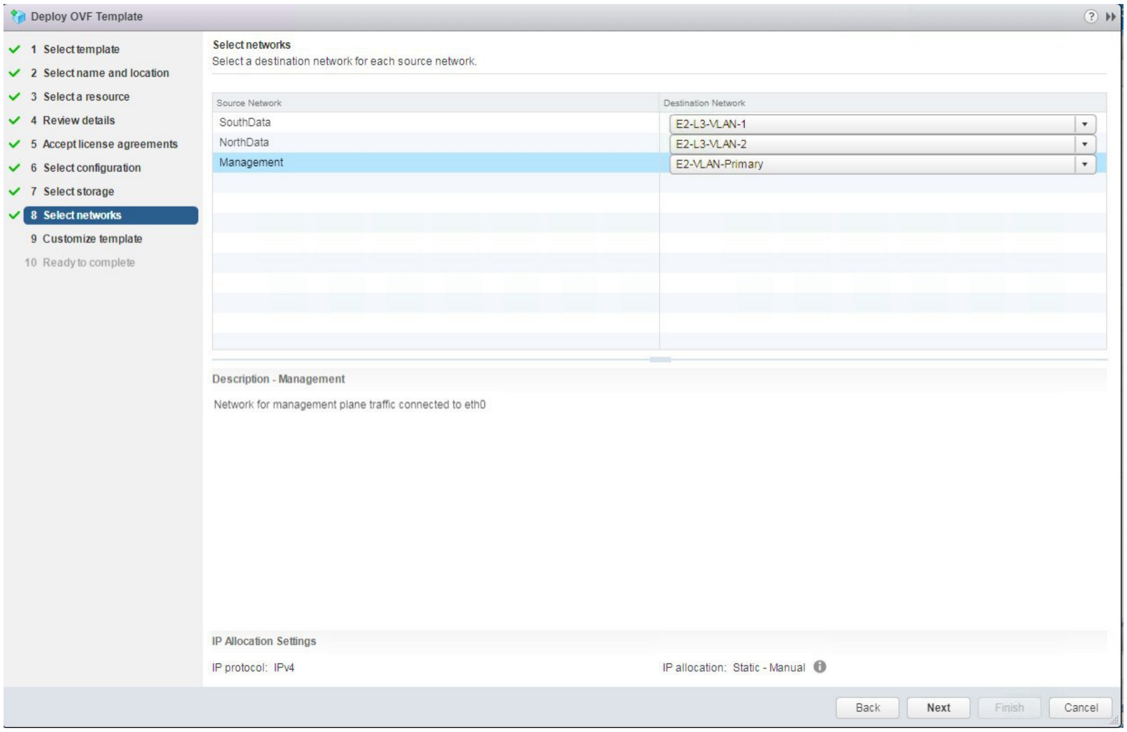
Select virtual disk format: Thick provision lazy zeroed

VM storage policy: None

☐ Show datastores from Storage DRS clusters

Name	Status	VM storage policy	Capacity	Free
● host154	Normal	VM Encryption P...	1.81 TB	812.62 GB

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.



Deploy OVF Template

- ✓ 1 Select template
- ✓ 2 Select name and location
- ✓ 3 Select a resource
- ✓ 4 Review details
- ✓ 5 Accept license agreements
- ✓ 6 Select 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
SouthData	E2-L3-VLAN-1
NorthData	E2-L3-VLAN-2
Management	E2-VLAN-Primary

Description - Management

Network for management plane traffic connected to eth0

IP Allocation Settings

IP protocol: IPv4 IP allocation: Static - Manual

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 Change Automation and Health Insights. 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 Change Automation and Health Insights 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**

Note If you are not using the default SCP port 22, you can specify the port as a part of the SCP command. For example,

```
-P55 user@host:path/to/file
```

where 55 is a custom port.

- Controller IP: IP address of the Crosswork controller i.e., Cisco Crosswork Change Automation and Health Insights.

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

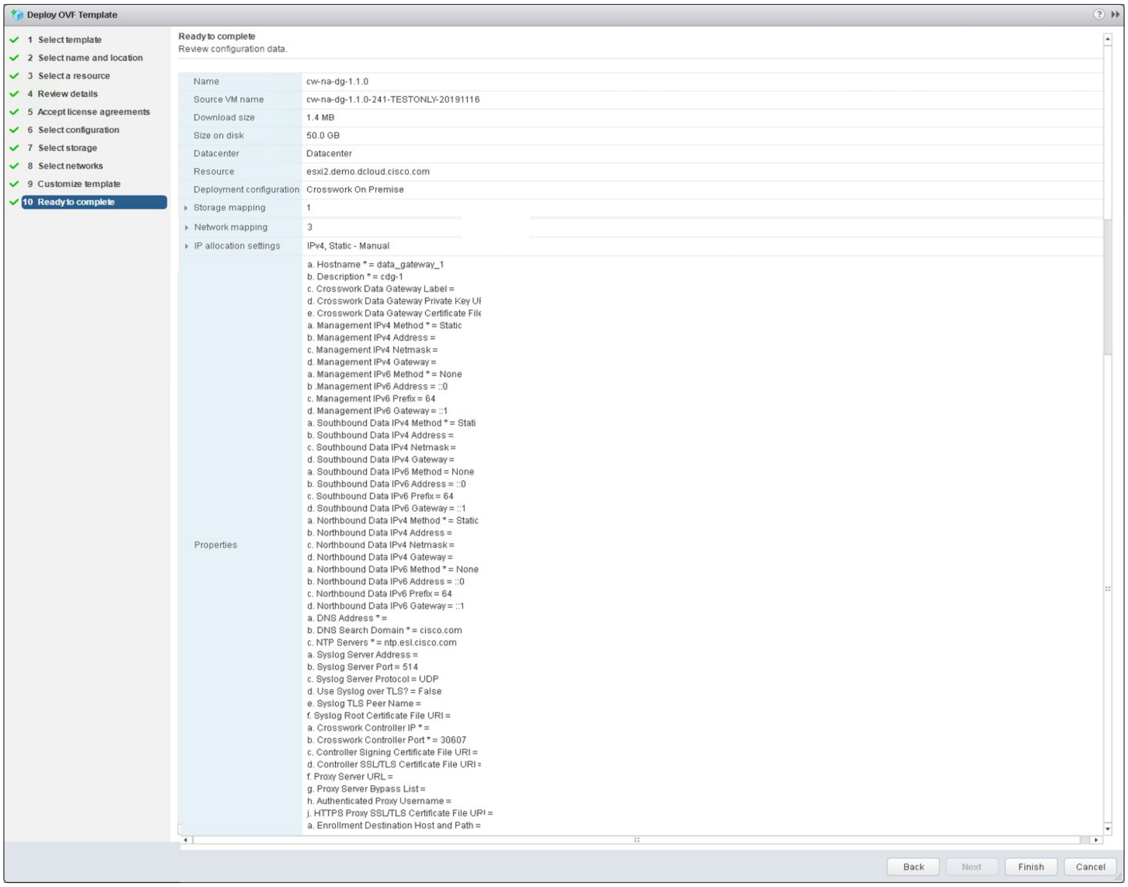
  ```
  cw-admin@<Crosswork_VM_ Management_IP_Address>:/home/cw-admin/controller.pem
  ```

- 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 Change Automation and Health Insights 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.



Deploy OVF Template

- ✓ 1 Select template
- ✓ 2 Select name and location
- ✓ 3 Select a resource
- ✓ 4 Review details
- ✓ 5 Accept license agreements
- ✓ 6 Select configuration
- ✓ 7 Select storage
- ✓ 8 Select networks
- ✓ 9 Customize template
- ✓ 10 Ready to complete

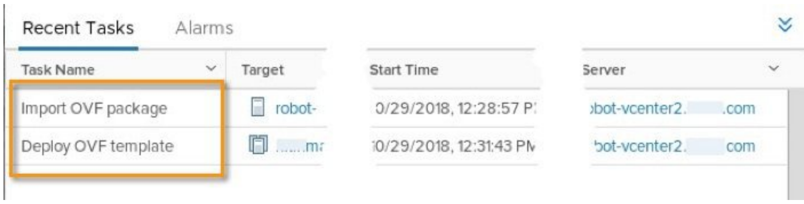
Ready to complete
Review configuration data.

Name	cw-na-dg-1.1.0
Source VM name	cw-na-dg-1.1.0-241-TESTONLY-20191116
Download size	1.4 MB
Size on disk	50.0 GB
Datacenter	Datacenter
Resource	esxi2.demo.dcloud.cisco.com
Deployment configuration	Crosswork On Premise
Storage mapping	1
Network mapping	3
IP allocation settings	IPv4, Static - Manual
Properties	a. Hostname * = data_gateway_1 b. Description * = cdg-1 c. Crosswork Data Gateway Label = d. Crosswork Data Gateway Private Key UI e. Crosswork Data Gateway Certificate File a. Management IPv4 Method * = Static b. Management IPv4 Address = c. Management IPv4 Netmask = d. Management IPv4 Gateway = a. Management IPv6 Method * = None b .Management IPv6 Address = ::0 c. Management IPv6 Prefix = 64 d. Management IPv6 Gateway = ::1 a. Southbound Data IPv4 Method * = Stati b. Southbound Data IPv4 Address = c. Southbound Data IPv4 Netmask = d. Southbound Data IPv4 Gateway = a. Southbound Data IPv6 Method = None b. Southbound Data IPv6 Address = ::0 c. Southbound Data IPv6 Prefix = 64 d. Southbound Data IPv6 Gateway = ::1 a. Northbound Data IPv4 Method * = Static b. Northbound Data IPv4 Address = c. Northbound Data IPv4 Netmask = d. Northbound Data IPv4 Gateway = a. Northbound Data IPv6 Method * = None b. Northbound Data IPv6 Address = ::0 c. Northbound Data IPv6 Prefix = 64 d. Northbound Data IPv6 Gateway = ::1 a. DNS Address * = b. DNS Search Domain * = cisco.com c. NTP Servers * = ntp.esl.cisco.com a. Syslog Server Address = b. Syslog Server Port = 514 c. Syslog Server Protocol = UDP d. Use Syslog over TLS? = False e. Syslog TLS Peer Name = f. Syslog Root Certificate File URI = a. Crosswork Controller IP * = b. Crosswork Controller Port * = 30607 c. Controller Signing Certificate File URI = d. Controller SSL/TLS Certificate File URI = f. Proxy Server URL = g. Proxy Server Bypass List = h. Authenticated Proxy Username = j. HTTPS Proxy SSL/TLS Certificate File URI = a. Enrollment Destination Host and Path =

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:



Task Name	Target	Start Time	Server
Import OVF package	robot-	0/29/2018, 12:28:57 P	›bot-vcenter2. .com
Deploy OVF template	......m	0/29/2018, 12:31:43 PM	bot-vcenter2. com

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:

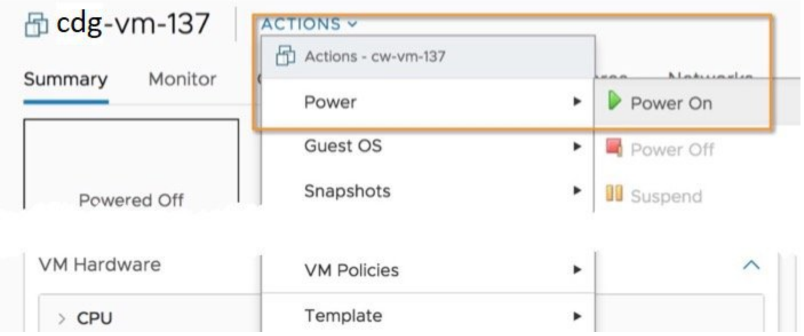
a. On the host VM **Summary** tab, below the **VM Hardware** table, click **Edit Settings**.

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, on page 61

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

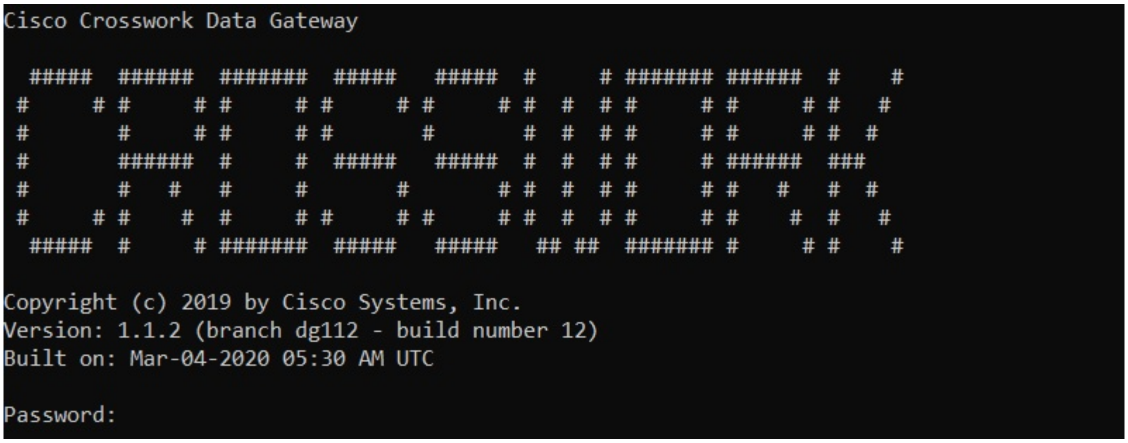
Access Cisco Crosswork Data Gateway Through vCenter

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: 1.1.2 (branch dg112 - build number 12)
Built on: Mar-04-2020 05:30 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>

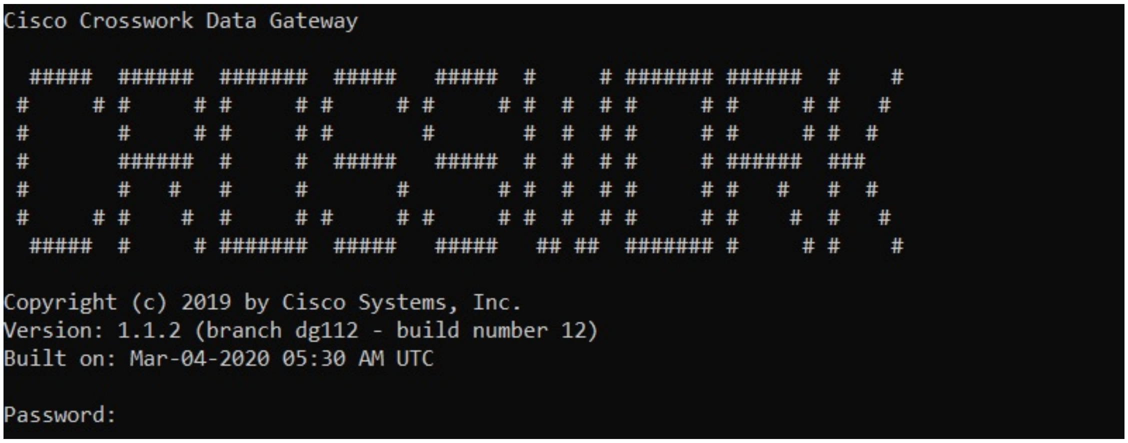
where **ManagementNetworkIP** is the management network IP address.

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:

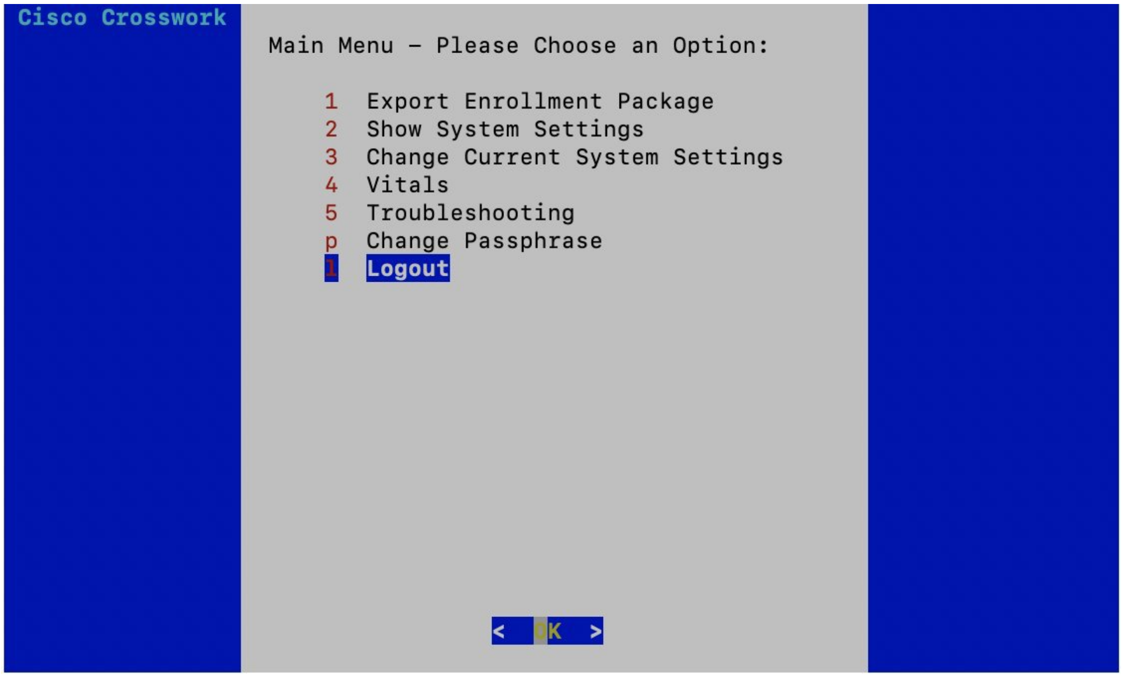


```
Cisco Crosswork Data Gateway

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

Copyright (c) 2019 by Cisco Systems, Inc.
Version: 1.1.2 (branch dg112 - build number 12)
Built on: Mar-04-2020 05:30 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": [

[illegible]

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

Export Enrollment Package

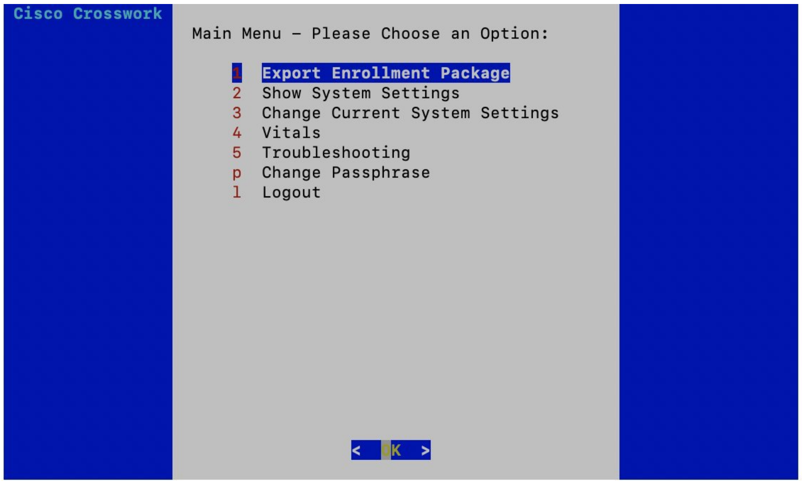
To enroll the Cisco Crosswork Data Gateway with Cisco Crosswork Change Automation and Health Insights, you must have a copy of the enrollment package on your local computer.

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

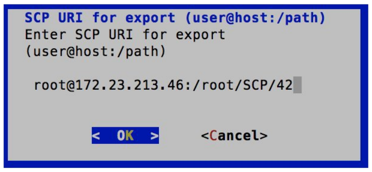


```
Cisco Crosswork
                 Main Menu - Please Choose an Option:

                    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**.

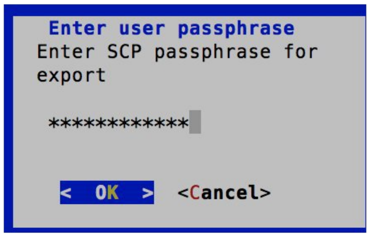
Note The host must run an SCP server. Ideally, you should export the enrollment package to the local computer you will use to access the Crosswork server. If no alternative SCP server is available, then Crosswork server can be used. An example URI is given below:

```
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**.



```
 Enter user passphrase
Enter SCP passphrase for
export

 ************

   <  OK  >  <Cancel>
```

The enrollment package is exported.

Step 5 If you could not copy the enrollment package directly to your local computer, manually copy the enrollment package from the SCP server to your local computer.

Step 6 Proceed with enrolling Cisco Crosswork Data Gateway with Cisco Crosswork Change Automation and Health Insights.

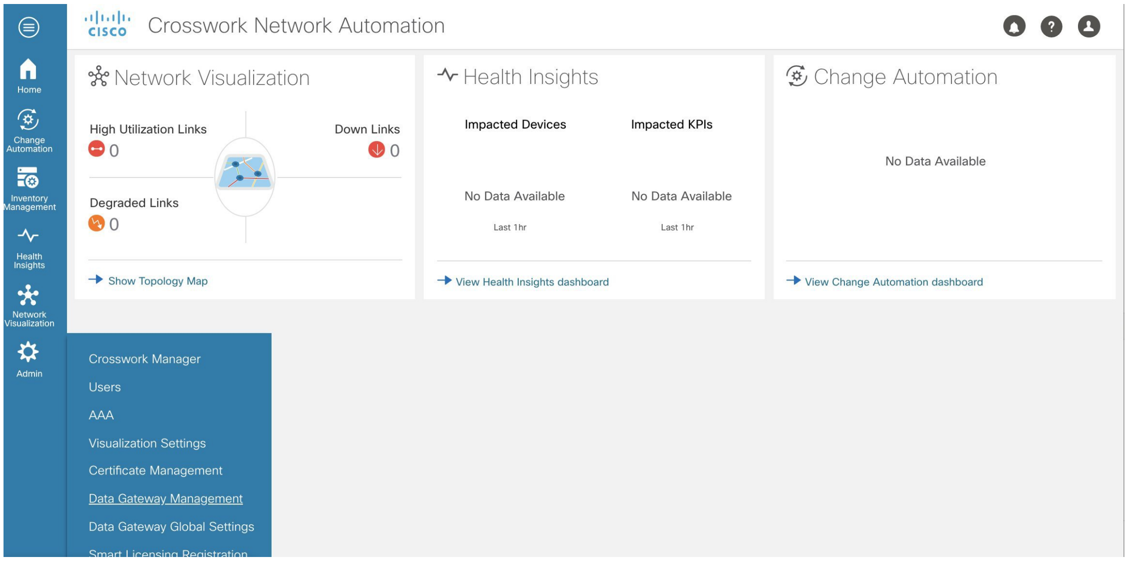
Enroll Cisco Crosswork Data Gateway With Cisco Crosswork Change Automation and Health Insights

Enroll Cisco Crosswork Data Gateway

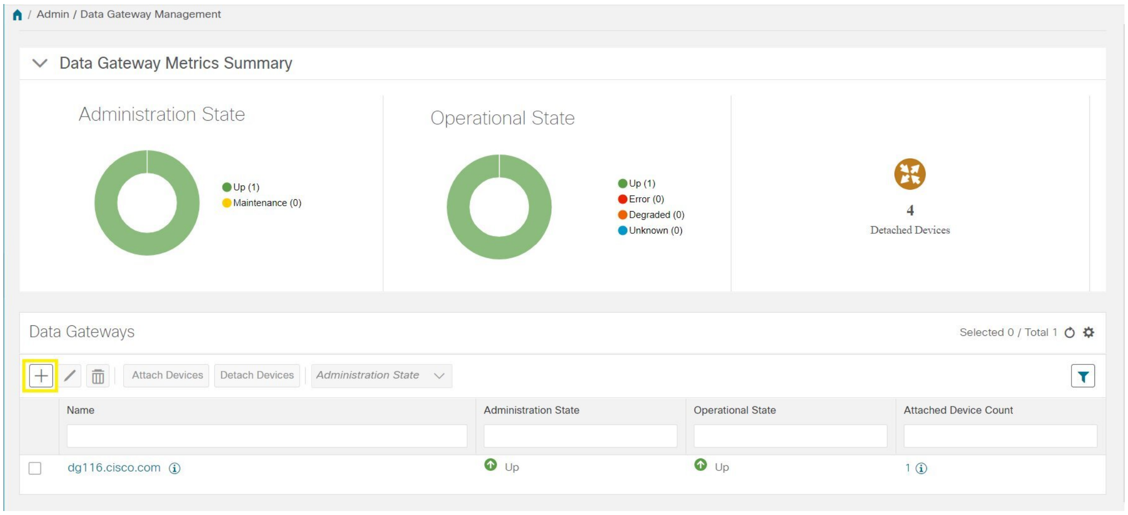
Step 1 Log into Cisco Crosswork Change Automation and Health Insights as described in Section Log In to the UI From a Browser, on page 34.

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

The **Data Gateway Management** page opens.



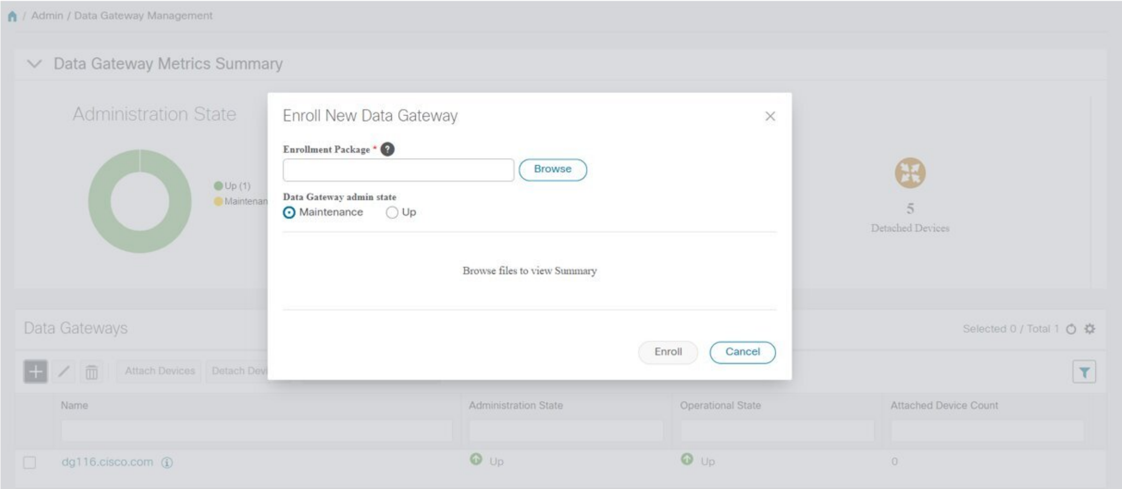
Step 3 Click the **Add** button.



	Name	Administration State	Operational State	Attached Device Count
□	dg116.cisco.com	Up	Up	1

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.



Enroll New Data Gateway

Enrollment Package * [Browse]

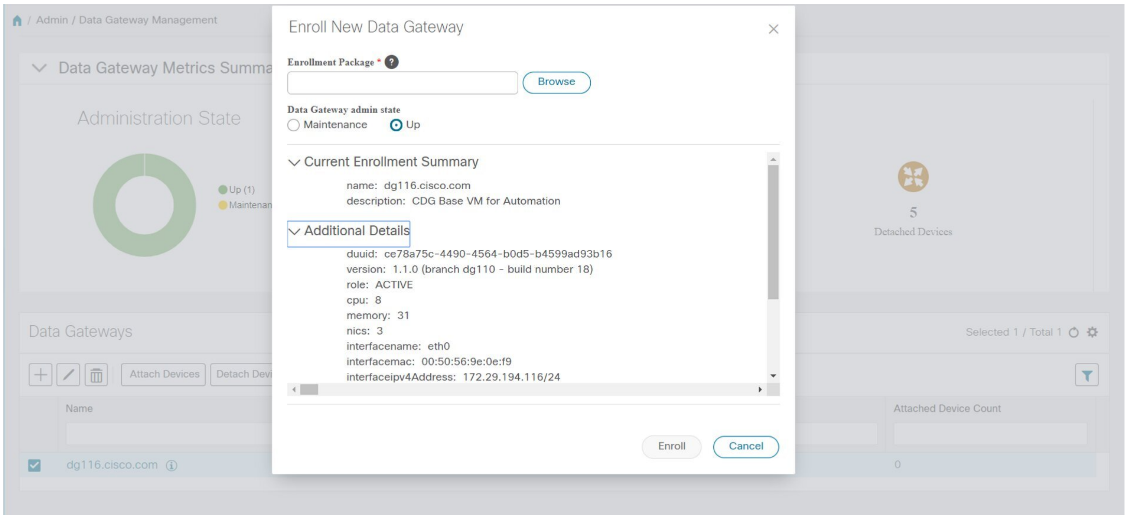
Data Gateway admin state
● Maintenance ○ Up

Browse files to view Summary

[Enroll] [Cancel]

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.



Enroll New Data Gateway

Enrollment Package * [Browse]

Data Gateway admin state
○ Maintenance ● Up

Current Enrollment Summary

name: dg116.cisco.com
description: CDG Base VM for Automation

Additional Details

duuid: ce78a75c-4490-4564-b0d5-b4599ad93b16
version: 1.1.0 (branch dg110 - build number 18)
role: ACTIVE
cpu: 8
memory: 31
nics: 3
interfacename: eth0
interfacemac: 00:50:56:9e:0e:f9
interfaceipv4Address: 172.29.194.116/24

[Enroll] [Cancel]

The **Enroll New Data Gateway** dialog displays a summary of the selected enrollment package:

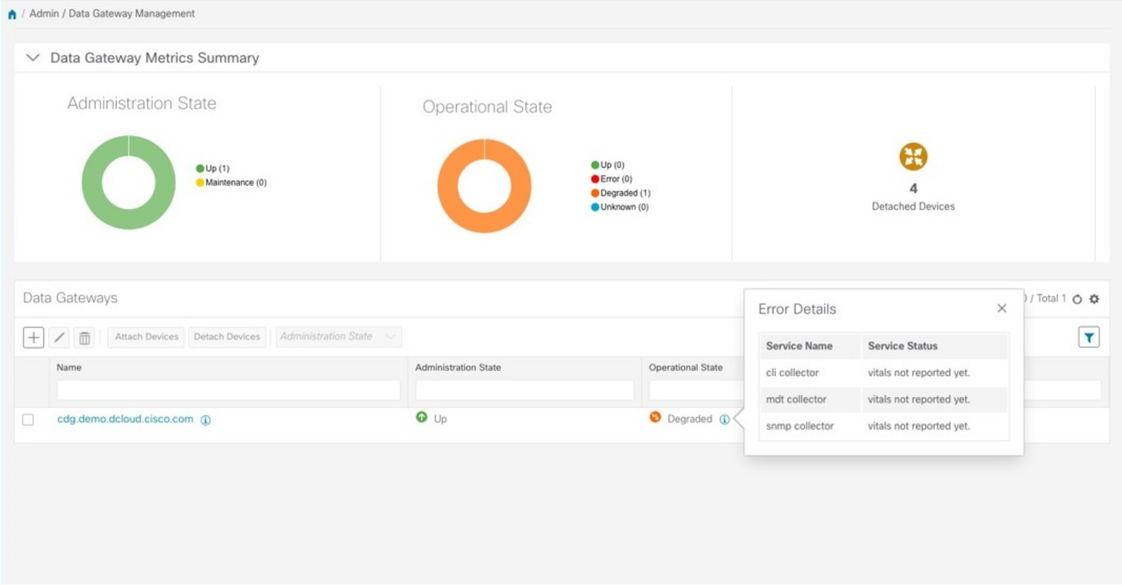
- Name of the Cisco Crosswork Data Gateway instance
- Description of the Cisco Crosswork Data Gateway instance
- Labels associated with the Cisco Crosswork Data Gateway instance

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:



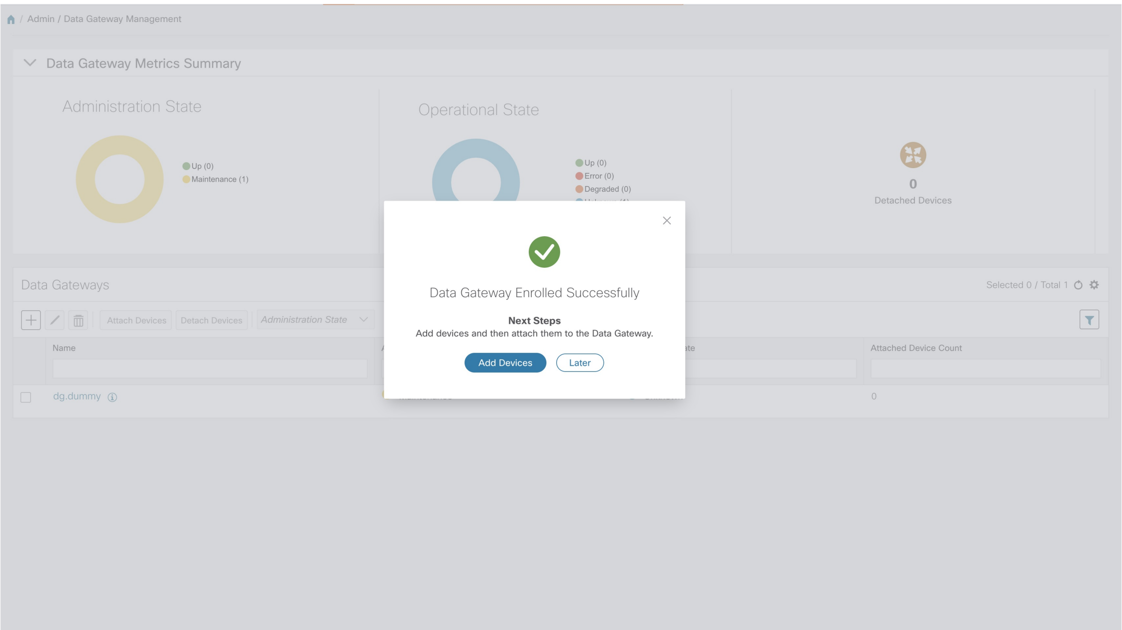
Name	Administration State	Operational State
cdg.demo.dcloud.cisco.com	Up	Degraded

Error Details

Service Name	Service Status
cli collector	vitals not reported yet.
mdt collector	vitals not reported yet.
snmp collector	vitals not reported yet.

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 3.2 User Guide*.



Data Gateway Enrolled Successfully

Next Steps
Add devices and then attach them to the Data Gateway.

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 Change Automation and Health Insights and downloads collector binary files. While it depends on the bandwidth between the Cisco Crosswork Data Gateway instance and Cisco Crosswork Change Automation and Health Insights, 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 Change Automation and Health Insights, 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 8: 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 9: 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 10: Troubleshooting the Installation/Enrollment

Issue	Action
1. Cannot enroll Cisco Crosswork Data Gateway with Crosswork	

Issue	Action
Cisco Crosswork Data Gateway cannot be enrolled with Crosswork 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 Change Automation and Health Insights. Also, on the NTP servers for Cisco Crosswork Change Automation and Health Insights 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 Crosswork. 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 Crosswork server and try re-enrolling Cisco Crosswork Data Gateway. It is also possible that the Cisco Crosswork Change Automation and Health Insights's NTP server might be down or its address might be incorrect. To configure NTP on the Cisco Crosswork Change Automation and Health Insights 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"	
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**.

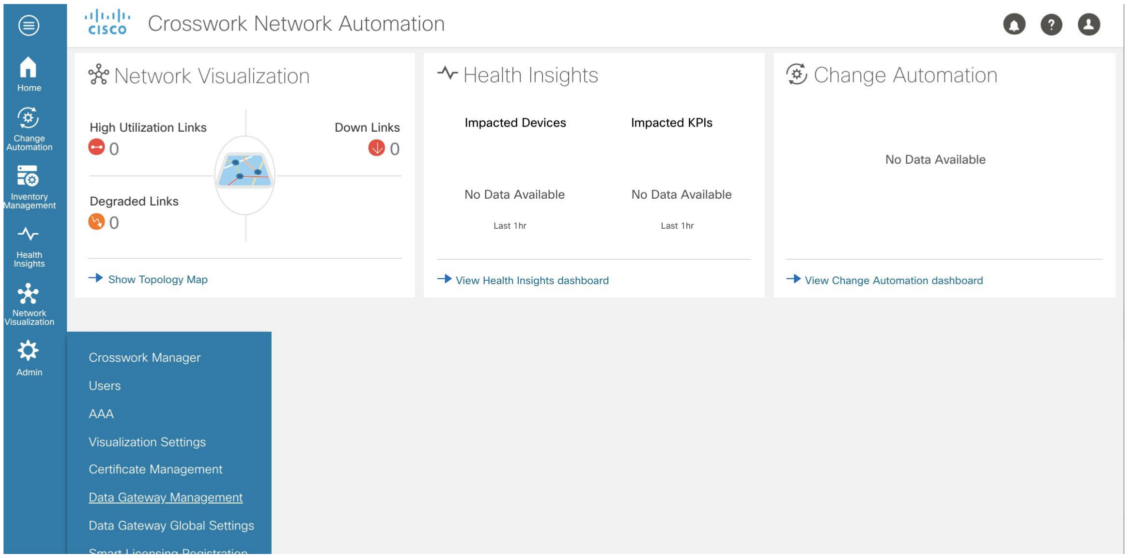
Issue	Action
3. Cisco Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "gRPC connection cannot be established"	
Cisco Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "gRPC connection cannot be established" 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

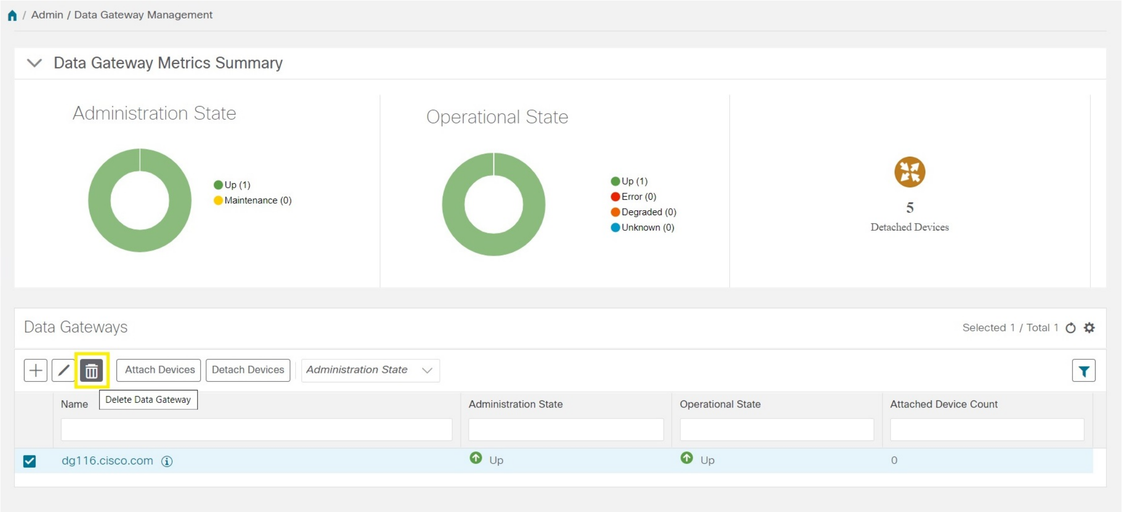
Step 1 Log in to Crosswork UI as desribed in Log In to the UI From a Browser, on page 34.

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

The **Data Gateway Management** page opens.

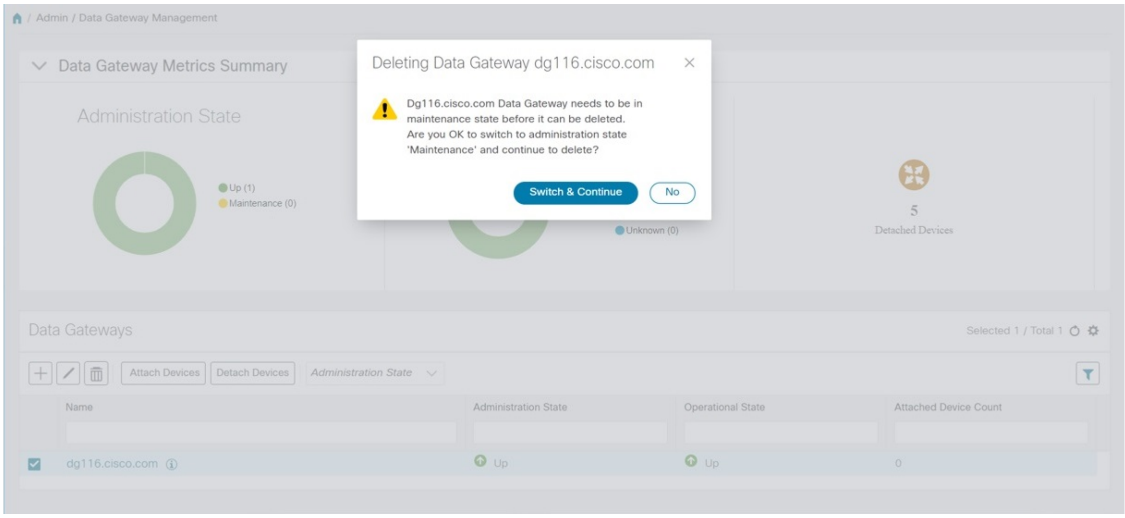


Step 3 In the **Data Gateways** panel, select the Cisco Crosswork Data Gateway VM you want to remove and click **Delete** button.



Name	Administration State	Operational State	Attached Device Count
dg116.cisco.com	Up	Up	0

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.

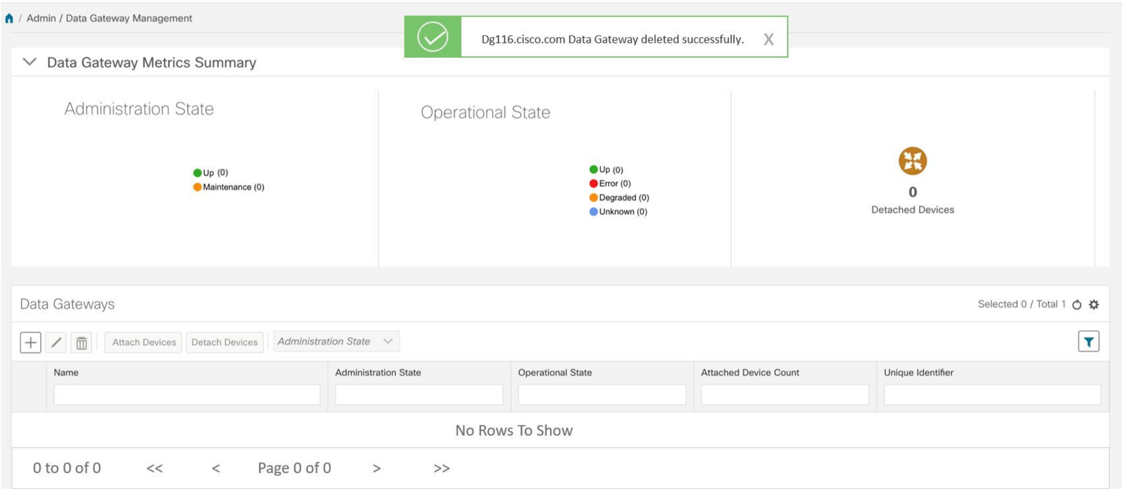


Deleting Data Gateway dg116.cisco.com

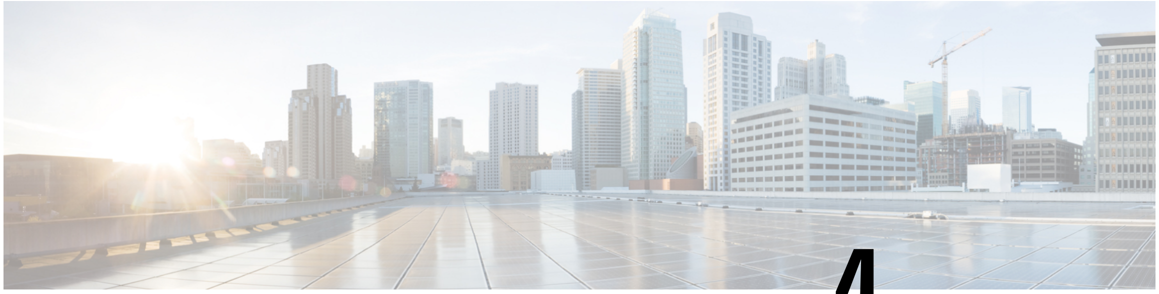
Dg116.cisco.com Data Gateway needs to be in maintenance state before it can be deleted. Are you OK to switch to administration state 'Maintenance' and continue to delete?

Name	Administration State	Operational State	Attached Device Count
dg116.cisco.com	Up	Up	0

The selected Cisco Crosswork Data Gateway VM is deleted.



Dg116.cisco.com Data Gateway deleted successfully.



CHAPTER 4

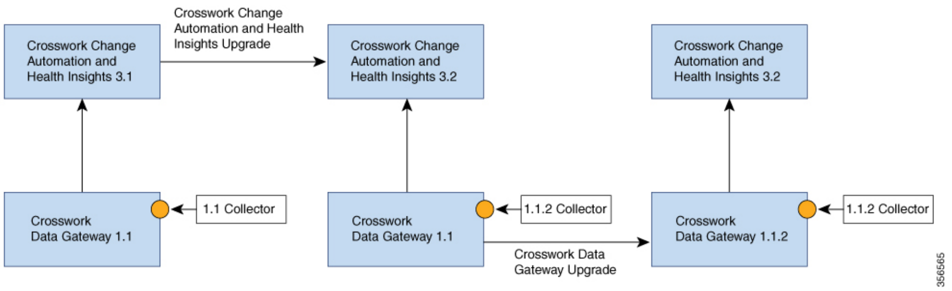
Upgrade

This section contains the following topics:

Upgrade Workflow

This section explains the upgrade workflow from Cisco Crosswork Change Automation and Health Insights version 3.1 to version 3.2. Cisco Crosswork Change Automation and Health Insights version 3.2 introduces secure Kafka to the Crosswork platform.

Figure 4: Upgrade Workflow



Crosswork Change Automation and Health Insights 3.1
Crosswork Change Automation and Health Insights Upgrade
Crosswork Change Automation and Health Insights 3.2
Crosswork Change Automation and Health Insights 3.2
Crosswork Data Gateway 1.1
1.1 Collector
Crosswork Data Gateway 1.1
1.1.2 Collector
Crosswork Data Gateway Upgrade
Crosswork Data Gateway 1.1.2
1.1.2 Collector
356565

The upgrade workflow has two stages:

1. **Cisco Crosswork Change Automation and Health Insights Upgrade:**

    - Cisco Crosswork Change Automation and Health Insights is upgraded by following the instructions in Upgrade Cisco Crosswork Change Automation and Health Insights, on page 74 (Kafka security should be seamless).

    - Post upgrade, the same Cisco Crosswork Data Gateway version 1.1 continues to work with Cisco Crosswork Change Automation and Health Insights version 3.2 while using the latest collector images (version 1.1.2) for secure Kafka.

2. **Cisco Crosswork Data Gateway Upgrade:**

- The new Cisco Crosswork Data Gateway VM is installed.
- Cisco Crosswork Data Gateway version 1.1.2 is enrolled on Cisco Crosswork Change Automation and Health Insights version 3.2.
- All devices are detached from the old Cisco Crosswork Data Gateway VM (version 1.1) and attached to the new Cisco Crosswork Data Gateway VM (version 1.1.2).
- Jobs start again automatically from the new Cisco Crosswork Data Gateway. At this point, the old Cisco Crosswork Data Gateway VM can be discarded.

Note It is not mandatory to upgrade Cisco Crosswork Data Gateway after upgrading Cisco Crosswork Change Automation and Health Insights. It can be performed later.

Upgrade Cisco Crosswork Change Automation and Health Insights

This section explains the procedure to upgrade Cisco Crosswork Change Automation and Health Insights from version 3.1 to version 3.2.

The upgrade process retains the following:

- User uploaded inventory (devices, providers, credential profiles, and tags).
- Platform details (database credentials).
- User configurations (Playbooks, Topology).
- AAA server integration data, custom local roles and custom roles
- Cisco Crosswork Change Automation and Health Insights VM version 3.1 settings for any rollback scenario.

Note The upgrade process for Cisco Crosswork Change Automation and Health Insights VM requires two instances (old and new) to exist at the same time. As a result you should plan to have resources (storage, disk and memory) within your data center (even if only temporarily) to support two VMs.

Without adequate resources, the upgrade operation will be unable to load the services successfully, and will fail in the first boot.

Before you begin, ensure that:

- You meet the system requirements to install Cisco Crosswork Change Automation and Health Insights and Cisco Crosswork Data Gateway. For more information, see Install Cisco Crosswork Change Automation and Health Insights Via vCenter, on page 16 and Install Cisco Crosswork Data Gateway, on page 38.

- You have details of the Cisco Crosswork Change Automation and Health Insights VM version 3.1 including the Management IPv4 address, username and password.
- You have a public IPv4 address to assign to the Cisco Crosswork Change Automation and Health Insights VM version 3.2 management network virtual interface. This is a temporary address as the Management IPv4 address from Cisco Crosswork Change Automation and Health Insights VM version 3.1 is retained.

  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 IPv4 to assign to the Cisco Crosswork Change Automation and Health Insights VM's data network virtual interface. This IP address must be able to reach your managed devices, Cisco Crosswork Data Gateway network, and be reachable by Cisco Network Services Orchestrator (NSO).

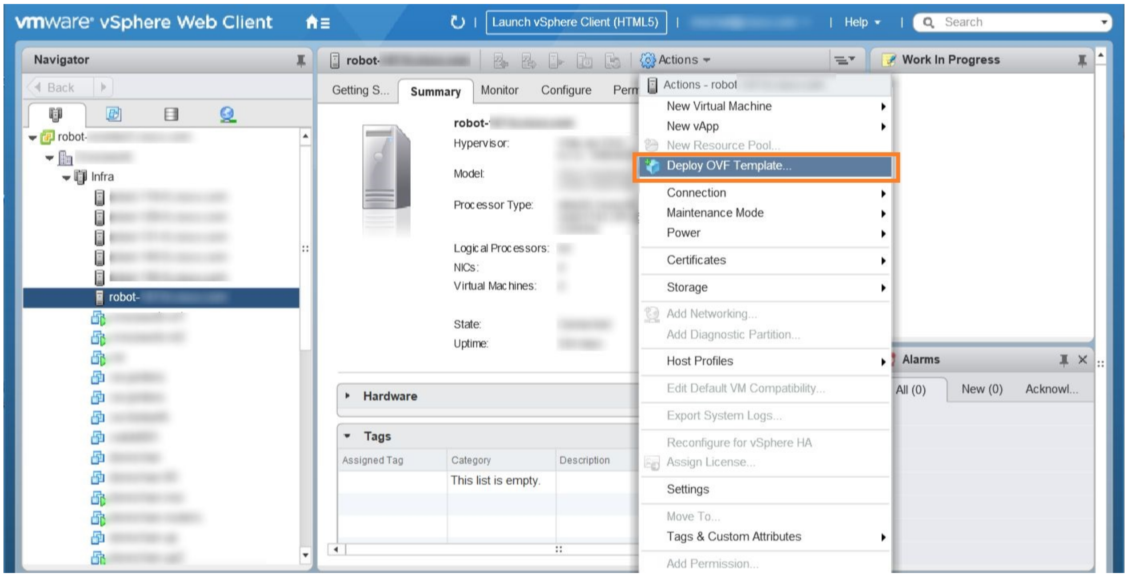
Note Before upgrading, it is recommended to move the Cisco Crosswork Change Automation and Health Insights VM version 3.1 to maintenance mode. The Health Insights KPIs and scheduled playbooks must be deactivated to stop any active collection on Cisco Crosswork Data Gateway.

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 Change Automation and Health Insights VM deployment and is explained in this procedure. The vSphere Client (HTML5 mode) is supported only on VMware vCenter Server 6.7 Update 3b.

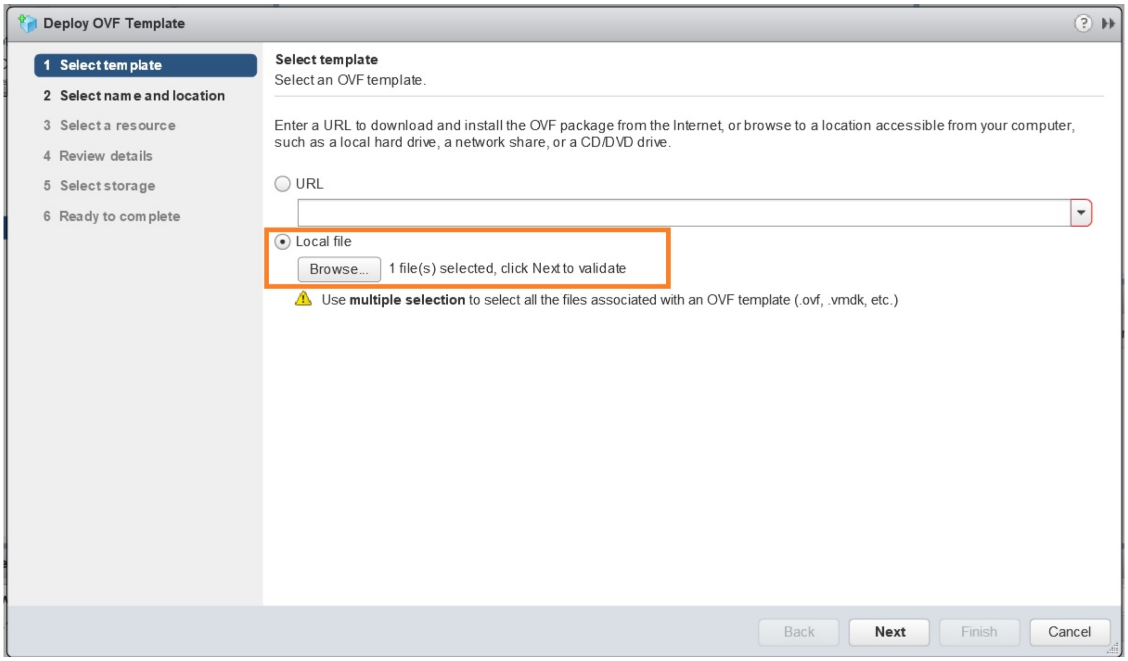
Step 1 Download the latest available Cisco Crosswork Change Automation and Health Insights image file (*.ova) to your system.

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 three separate Open Virtualization Format and Virtual Machine Disk component files: `cw.ovf`, `cw_rootfs.vmdk`, and `cw_dockerfs`.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**, 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. 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.



Select template

Select an OVF template.

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

○ URL

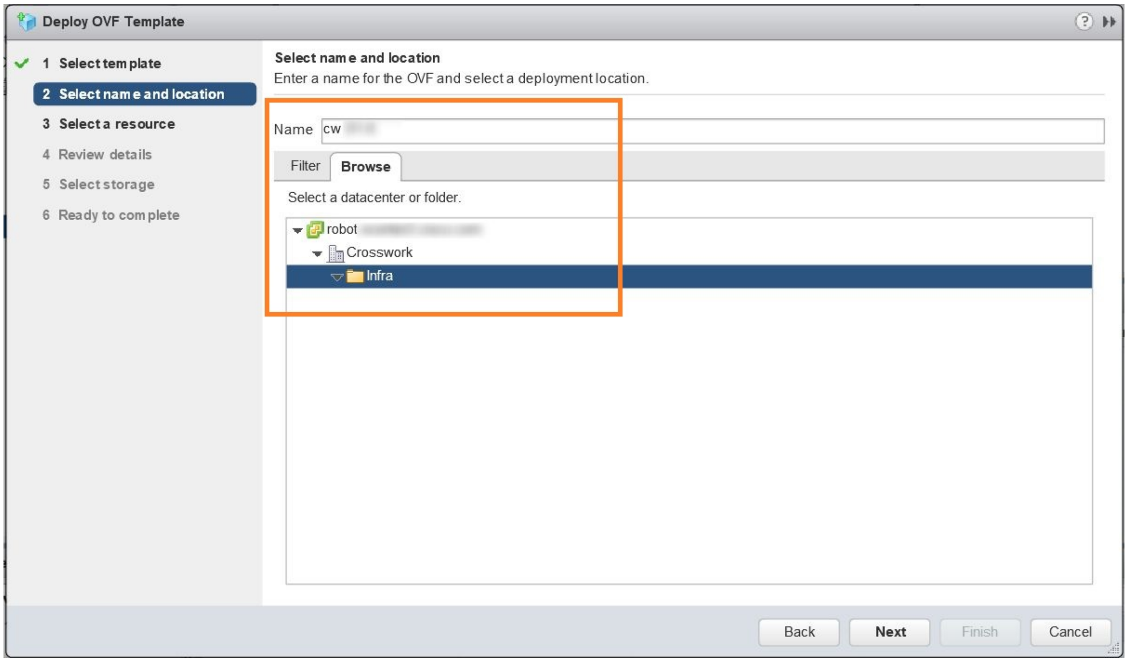
● Local file

Browse... 1 file(s) selected, click Next to validate

Use **multiple selection** to select all the files associated with an OVF template (.ovf, .vmdk, etc.)

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 Change Automation and Health Insights VM you are creating.

Cisco recommends that you include the Cisco Crosswork Change Automation and Health Insights version and build number in the name (for example: `Crosswork CA/HI 3.2 Build 283`).



Deploy OVF Template

- ✓ 1 Select template
- 2 Select name and location
- 3 Select a resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select name and location

Enter a name for the OVF and select a deployment location.

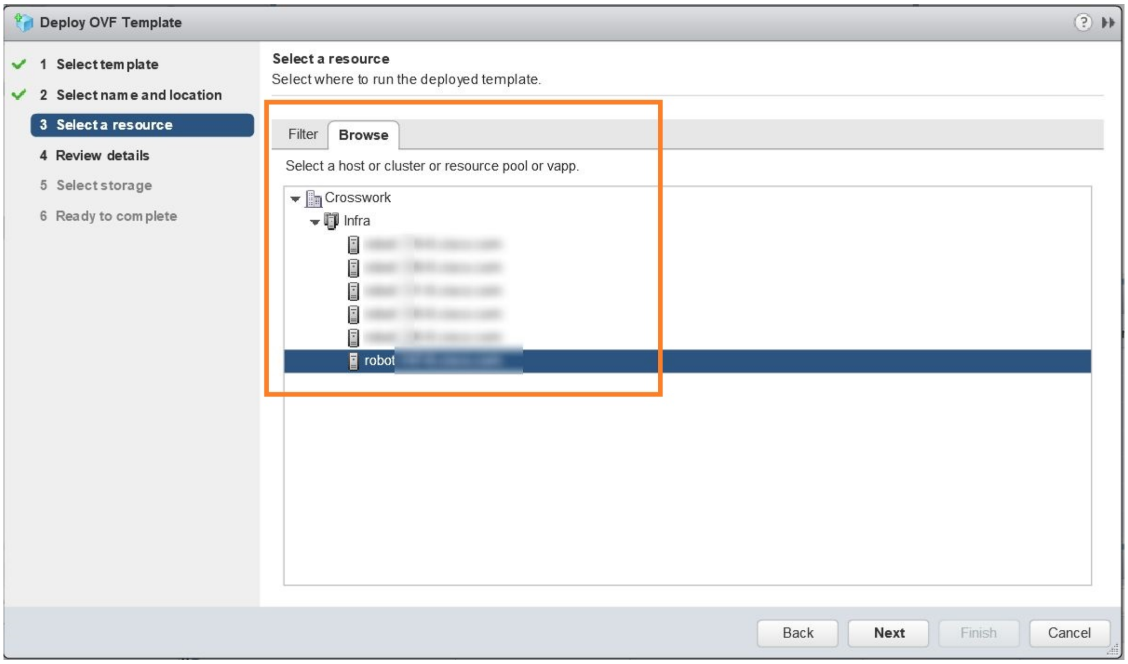
Name: cw [redacted]

Filter | Browse

Select a datacenter or folder.

- robot [redacted]
  - Crosswork
    - Infra

Step 5 Click **Next** to go to **3 - Select a resource**, as shown in the following figure. Choose the Cisco Crosswork Change Automation and Health Insights VM’s host.



Deploy OVF Template

- ✓ 1 Select template
- ✓ 2 Select name and location
- 3 Select a resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select a resource

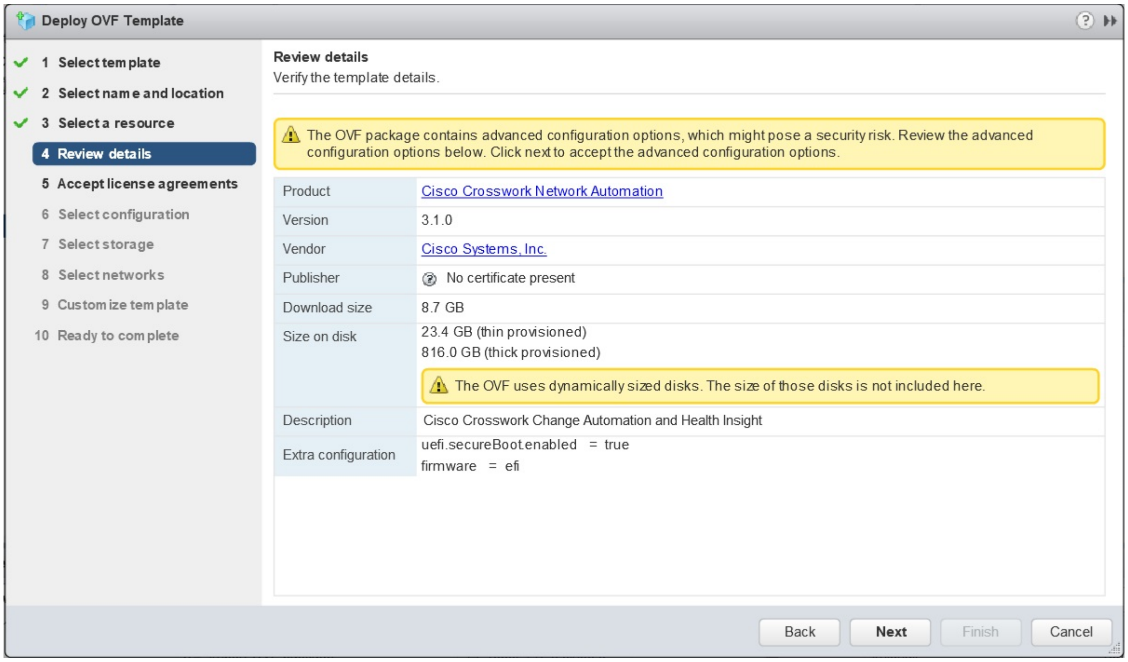
Select where to run the deployed template.

Filter | Browse

Select a host or cluster or resource pool or vapp.

- Crosswork
  - Infra
    - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]
    - robot [redacted]

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**, as shown in 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.



Review details

Verify the template details.

⚠ The OVF package contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below. Click next to accept the advanced configuration options.

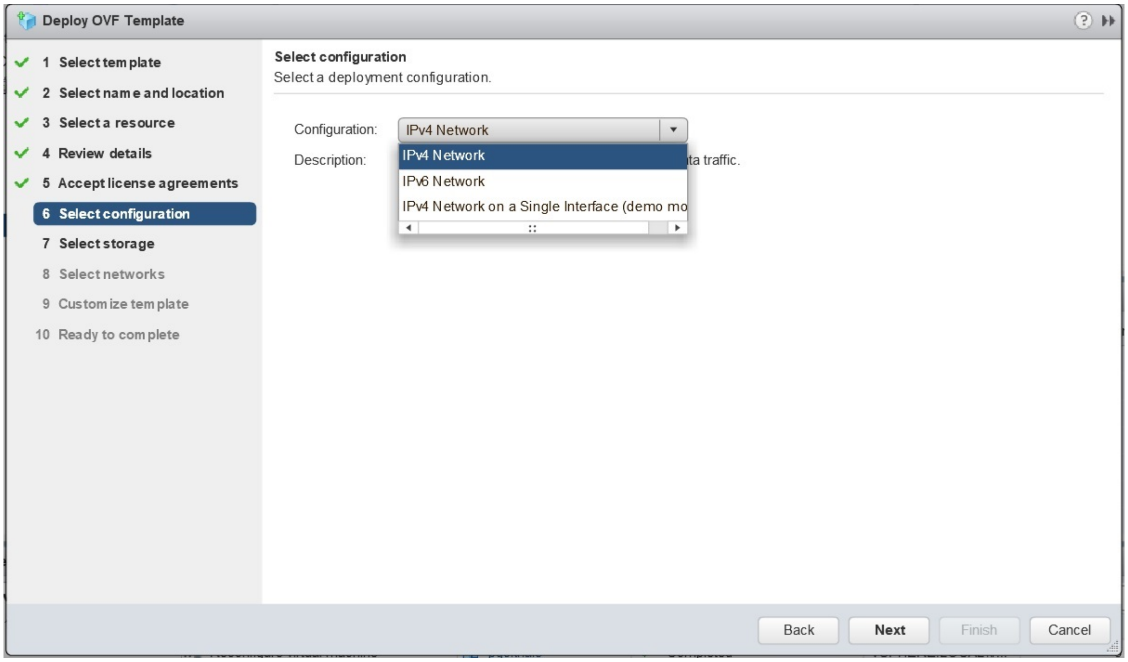
Product	Cisco Crosswork Network Automation
Version	3.1.0
Vendor	Cisco Systems, Inc.
Publisher	No certificate present
Download size	8.7 GB
Size on disk	23.4 GB (thin provisioned) 816.0 GB (thick provisioned) ⚠ The OVF uses dynamically sized disks. The size of those disks is not included here.
Description	Cisco Crosswork Change Automation and Health Insight

Extra configuration	uefi.secureBoot.enabled = true
	firmware = efi

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**, as shown in the following figure. Select the desired deployment configuration (IPv4 or IPv4 Network on a Single Interface).

Note As indicated, the IPv4 on a Single Interface should only be used for demonstrations and lab installations.



Select configuration

Select a deployment configuration.

Configuration: IPv4 Network

Description: ta traffic.

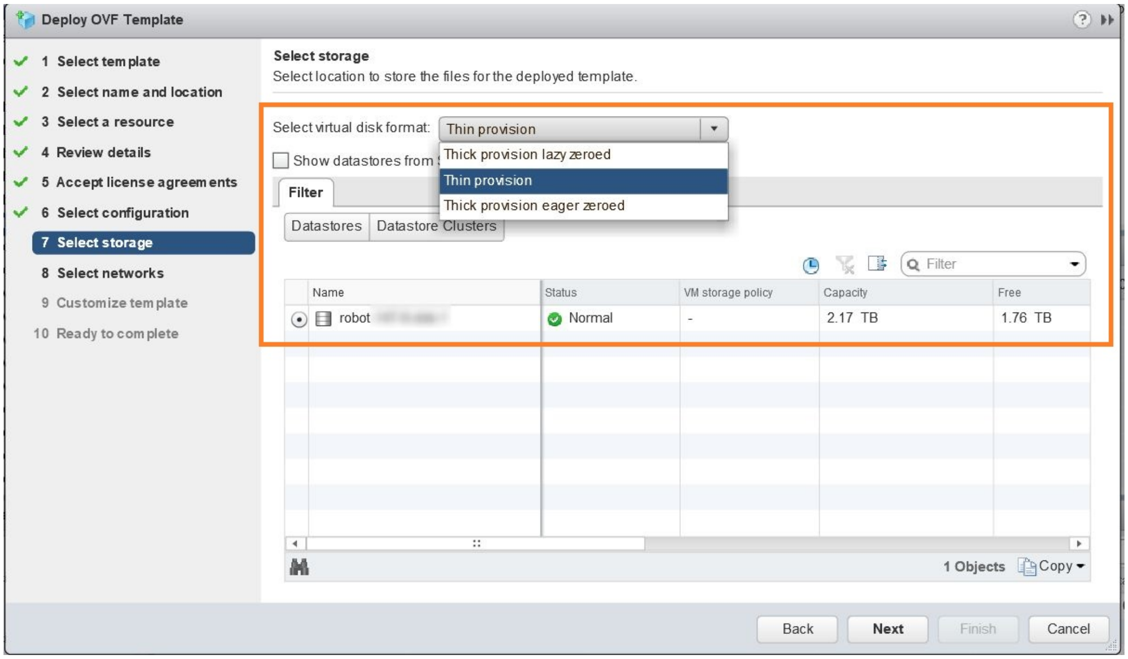
IPv4 Network

IPv6 Network

IPv4 Network on a Single Interface (demo mo

Step 9 Click **Next** to go to **7 - Select Storage**, as shown in 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, consider choosing **Thick provision eager zeroed** as it will not have a penalty of allocating and initializing disk space at runtime. For demo or testing purposes, **Thin provision** is recommended as it saves disk space.



Deploy OVF Template

- ✓ 1 Select template
- ✓ 2 Select name and location
- ✓ 3 Select a resource
- ✓ 4 Review details
- ✓ 5 Accept license agreements
- ✓ 6 Select configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Select storage

Select location to store the files for the deployed template.

Select virtual disk format: Thin provision ▾

- Thick provision lazy zeroed
- Thin provision
- Thick provision eager zeroed

□ Show datastores from

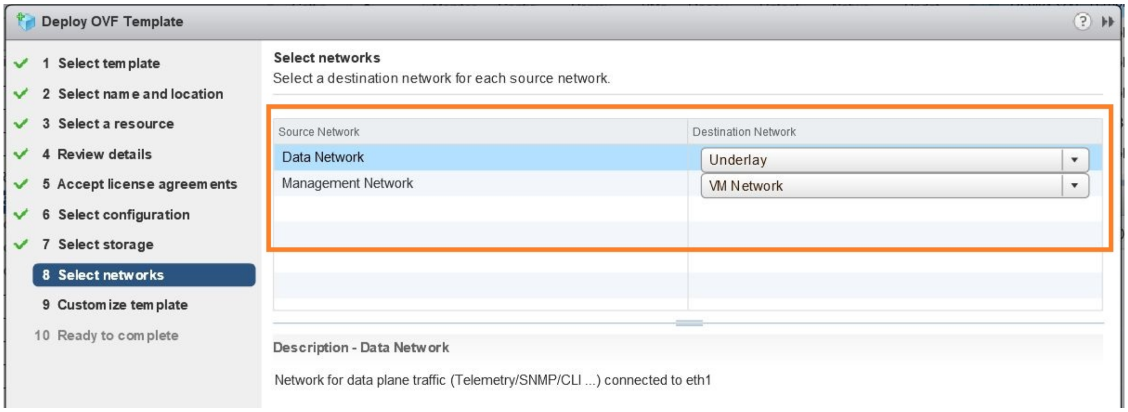
Filter

Datastores | Datastore Clusters

	Name	Status	VM storage policy	Capacity	Free
●	robot [redacted]	✓ Normal	-	2.17 TB	1.76 TB

1 Objects Copy ▾

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 **Data Network** and **Management Network**, respectively.



Deploy OVF Template

- ✓ 1 Select template
- ✓ 2 Select name and location
- ✓ 3 Select a resource
- ✓ 4 Review details
- ✓ 5 Accept license agreements
- ✓ 6 Select configuration
- ✓ 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Select networks

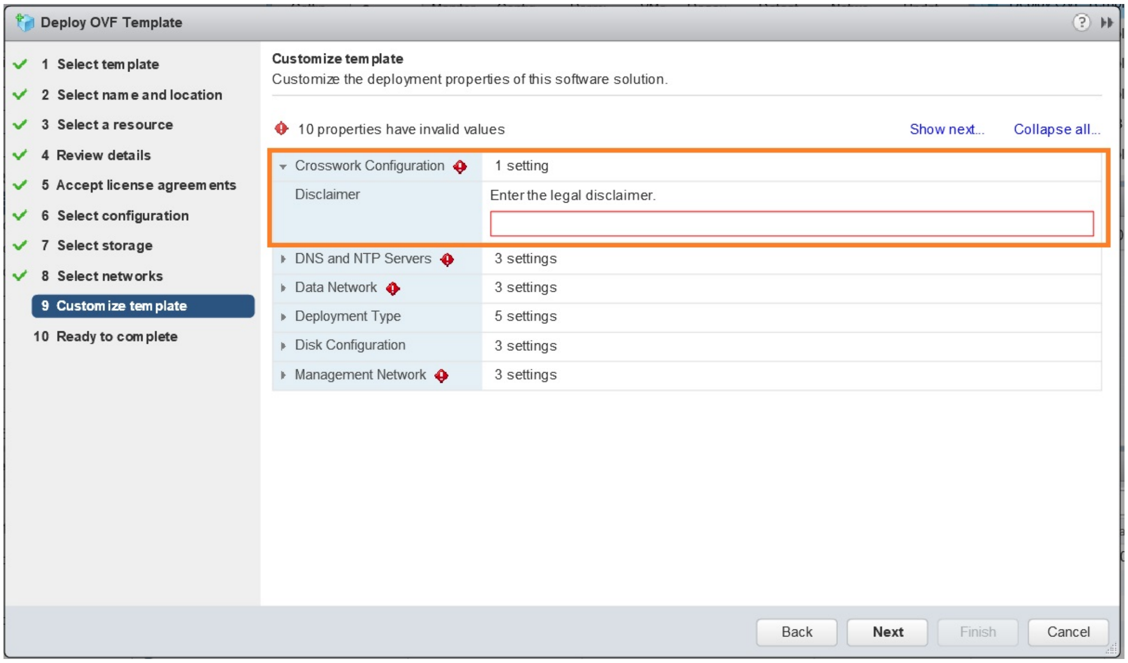
Select a destination network for each source network.

Source Network	Destination Network
Data Network	Underlay ▾
Management Network	VM Network ▾

Description - Data Network

Network for data plane traffic (Telemetry/SNMP/CLI ...) connected to eth1

Step 11 Click **Next** to go to **9 - Customize template**, with the **Crosswork Configuration** settings already expanded, as shown in the following figure. Make entry in the **Disclaimer** field.



Deploy OVF Template

- ✓ 1 Select template
- ✓ 2 Select name and location
- ✓ 3 Select a resource
- ✓ 4 Review details
- ✓ 5 Accept license agreements
- ✓ 6 Select configuration
- ✓ 7 Select storage
- ✓ 8 Select networks
- 9 Customize template
- 10 Ready to complete

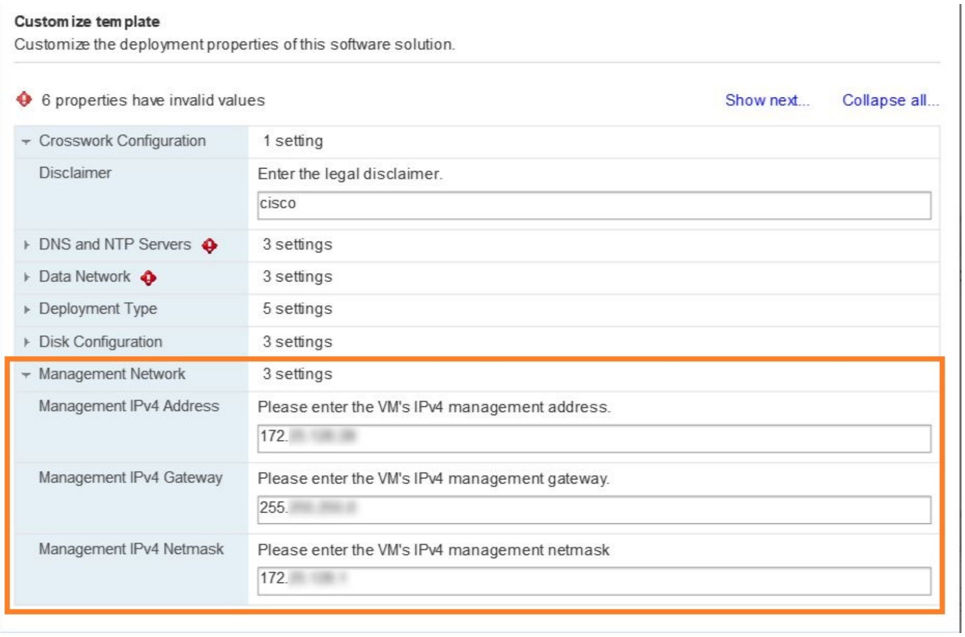
Customize template

Customize the deployment properties of this software solution.

10 properties have invalid values

Crosswork Configuration	1 setting
Disclaimer	Enter the legal disclaimer.
DNS and NTP Servers	3 settings
Data Network	3 settings
Deployment Type	5 settings
Disk Configuration	3 settings
Management Network	3 settings

Step 12 Expand the **Management Network** settings. According to your deployment configuration, the fields displayed are different. Enter the temporary IP address you want to be associated with the VM during the upgrade. If as part of the upgrade you want to keep this address associated with the VM you can select this option later in the upgrade process. See how to customize the template (step 11).



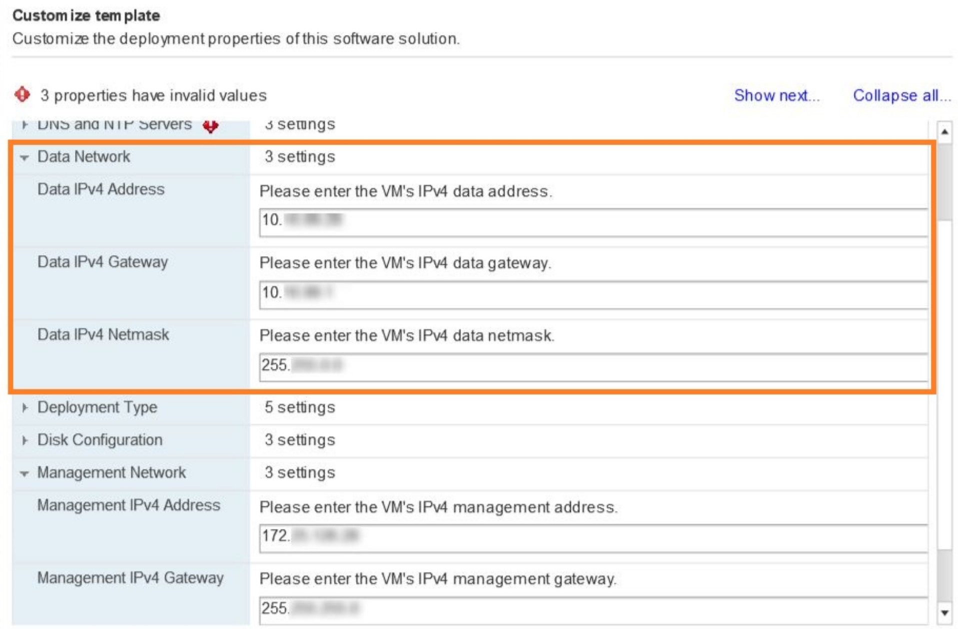
Customize template

Customize the deployment properties of this software solution.

6 properties have invalid values

Crosswork Configuration	1 setting
Disclaimer	Enter the legal disclaimer. cisco
DNS and NTP Servers	3 settings
Data Network	3 settings
Deployment Type	5 settings
Disk Configuration	3 settings
Management Network	3 settings
Management IPv4 Address	Please enter the VM's IPv4 management address. 172.[redacted]
Management IPv4 Gateway	Please enter the VM's IPv4 management gateway. 255.[redacted]
Management IPv4 Netmask	Please enter the VM's IPv4 management netmask 172.[redacted]

Step 13 Expand the **Data Network** settings. According to your deployment configuration, the fields displayed are different. Enter a temporary IP address and other information for the data network. If you want to change the IP to this value you can choose to do that in the customizing template section (step 11).



Customize template

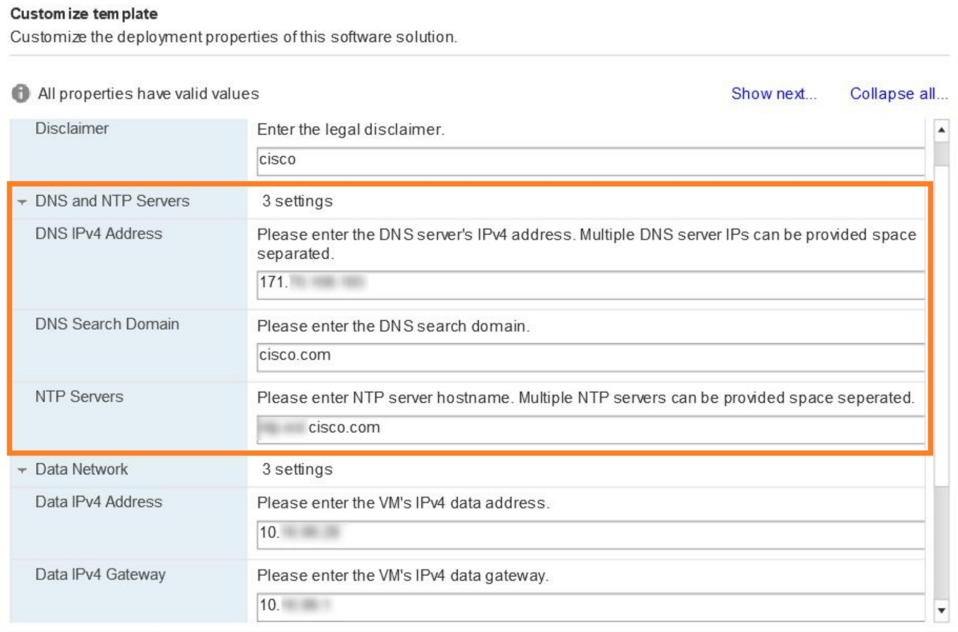
Customize the deployment properties of this software solution.

3 properties have invalid values

DNS and NTP Servers	3 settings
Data Network	3 settings
Data IPv4 Address	Please enter the VM's IPv4 data address. 10.[redacted]
Data IPv4 Gateway	Please enter the VM's IPv4 data gateway. 10.[redacted]
Data IPv4 Netmask	Please enter the VM's IPv4 data netmask. 255.[redacted]
Deployment Type	5 settings
Disk Configuration	3 settings
Management Network	3 settings
Management IPv4 Address	Please enter the VM's IPv4 management address. 172.[redacted]
Management IPv4 Gateway	Please enter the VM's IPv4 management gateway. 255.[redacted]

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

- **DNS IP Address**: The IPv4 addresses of the DNS servers you want the Cisco Crosswork Change Automation and Health Insights 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.



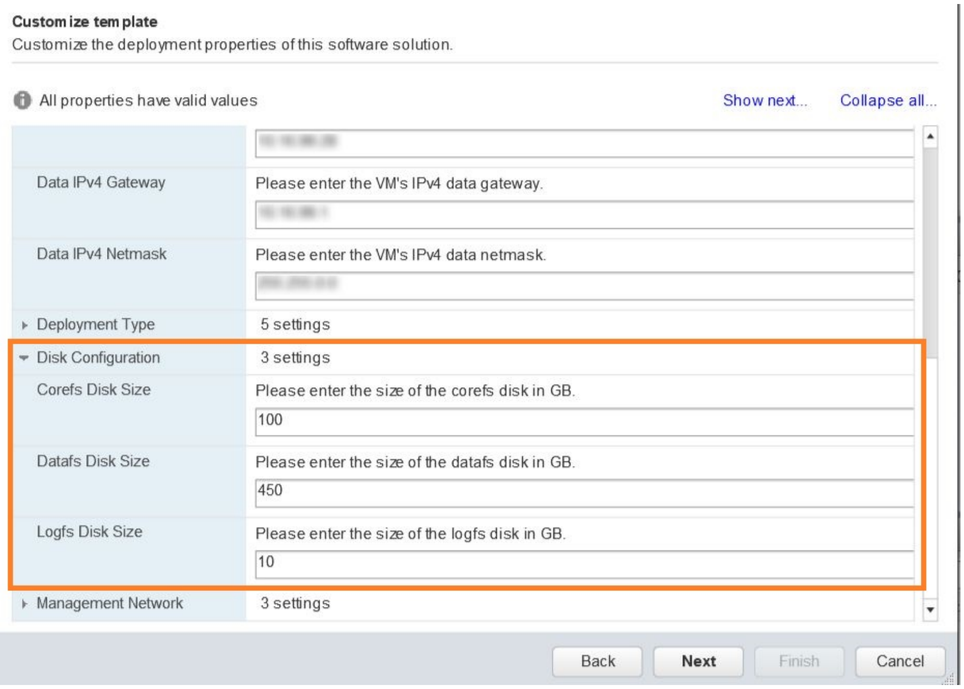
Customize template

Customize the deployment properties of this software solution.

All properties have valid values

Disclaimer	Enter the legal disclaimer. cisco
DNS and NTP Servers	3 settings
DNS IPv4 Address	Please enter the DNS server's IPv4 address. Multiple DNS server IPs can be provided space separated. 171.[redacted]
DNS Search Domain	Please enter the DNS search domain. cisco.com
NTP Servers	Please enter NTP server hostname. Multiple NTP servers can be provided space seperated. [redacted]cisco.com
Data Network	3 settings
Data IPv4 Address	Please enter the VM's IPv4 data address. 10.[redacted]
Data IPv4 Gateway	Please enter the VM's IPv4 data gateway. 10.[redacted]

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



Customize template
Customize the deployment properties of this software solution.

All properties have valid values

	[redacted]
Data IPv4 Gateway	Please enter the VM's IPv4 data gateway. [redacted]
Data IPv4 Netmask	Please enter the VM's IPv4 data netmask. [redacted]
▸ Deployment Type	5 settings
▾ Disk Configuration	3 settings
Corefs Disk Size	Please enter the size of the corefs disk in GB. 100
Datafs Disk Size	Please enter the size of the datafs disk in GB. 450
Logfs Disk Size	Please enter the size of the logfs disk in GB. 10
▸ Management Network	3 settings

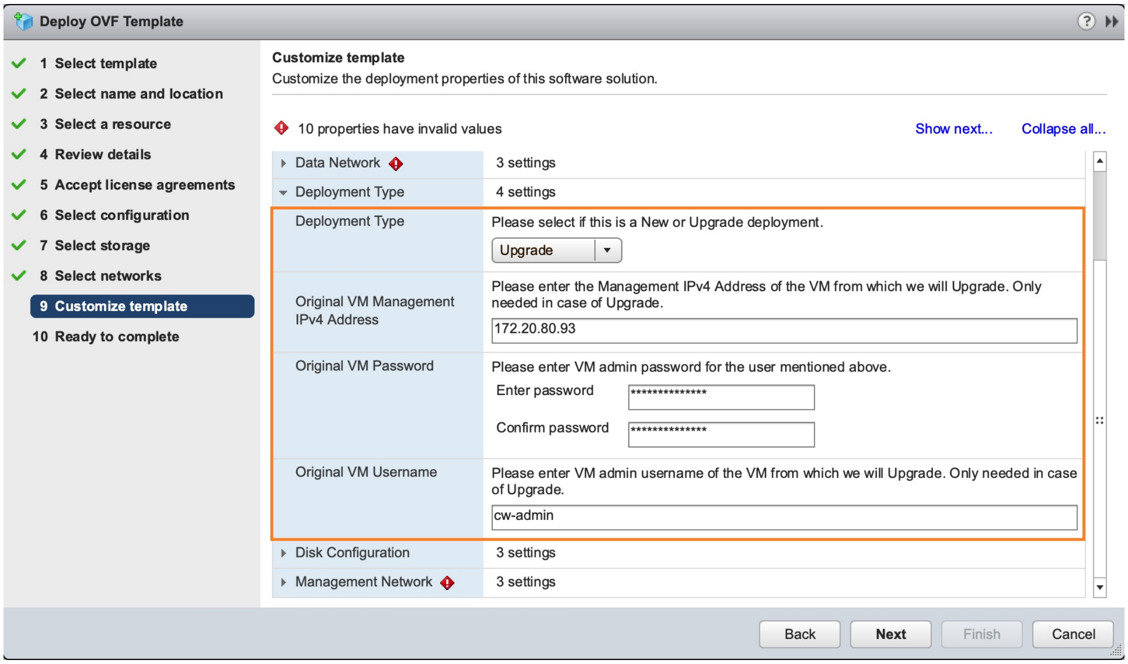
Step 16 Expand the **Deployment Type** settings, as shown in the following figure. In the **Deployment Type** dropdown, select **Upgrade**, and make relevant entries for the following fields:

a) **Original VM Management IPv4 Address**: Management IPv4 address of Cisco Crosswork Change Automation and Health Insights VM version 3.1.

b) **Original VM Password**: Provide the Cisco Crosswork Change Automation and Health Insights VM version 3.1 password in the **Enter Password** and **Confirm Password** fields.

c) **Original VM Username**: Username of Cisco Crosswork Change Automation and Health Insights VM version 3.1. Typically, it is **`cw-admin`** unless it has been changed by your system administrator.

Note Switching the Management or Data IPv4 address, or changing the IP stack from IPv4 to IPv6 is not supported during upgrade owing to restrictions in Cisco Crosswork Change Automation and Health Insights and Cisco Crosswork Data Gateway certificates. For more information, see Supported TCP/IP Stack, on page 95



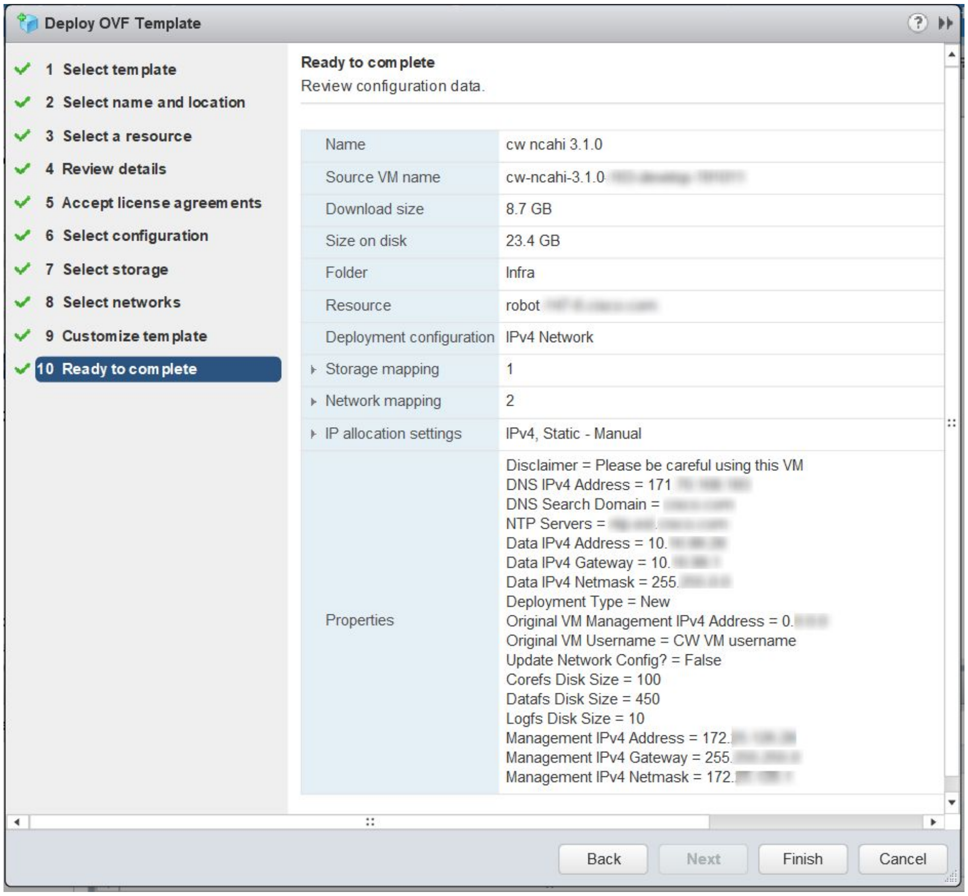
Customize template

Customize the deployment properties of this software solution.

10 properties have invalid values Show next... Collapse all...

Data Network	3 settings
Deployment Type	4 settings
Deployment Type	Please select if this is a New or Upgrade deployment. Upgrade
Original VM Management IPv4 Address	Please enter the Management IPv4 Address of the VM from which we will Upgrade. Only needed in case of Upgrade. 172.20.80.93
Original VM Password	Please enter VM admin password for the user mentioned above. Enter password ************** Confirm password **************
Original VM Username	Please enter VM admin username of the VM from which we will Upgrade. Only needed in case of Upgrade. cw-admin
Disk Configuration	3 settings
Management Network	3 settings

Step 17 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.



Ready to complete

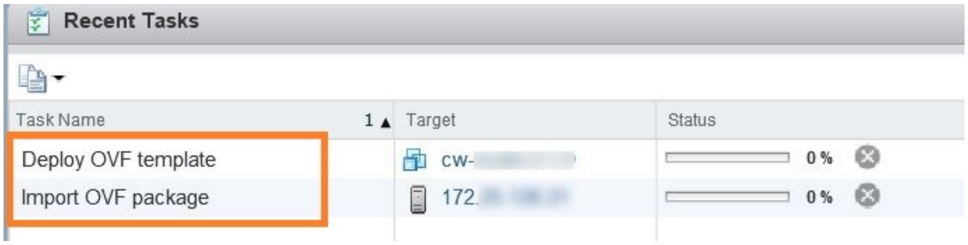
Review configuration data.

Name	cw ncahi 3.1.0
Source VM name	cw-ncahi-3.1.0 [redacted]
Download size	8.7 GB
Size on disk	23.4 GB
Folder	Infra
Resource	robot [redacted]
Deployment configuration	IPv4 Network
Storage mapping	1
Network mapping	2
IP allocation settings	IPv4, Static - Manual
Properties	Disclaimer = Please be careful using this VM DNS IPv4 Address = 171 [redacted] DNS Search Domain = [redacted] NTP Servers = [redacted] Data IPv4 Address = 10. [redacted] Data IPv4 Gateway = 10. [redacted] Data IPv4 Netmask = 255. [redacted] Deployment Type = New Original VM Management IPv4 Address = 0. [redacted] Original VM Username = CW VM username Update Network Config? = False Corefs Disk Size = 100 Datafs Disk Size = 450 Logfs Disk Size = 10 Management IPv4 Address = 172. [redacted] Management IPv4 Gateway = 255. [redacted] Management IPv4 Netmask = 172. [redacted]

Step 18 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, as shown in the following figure.

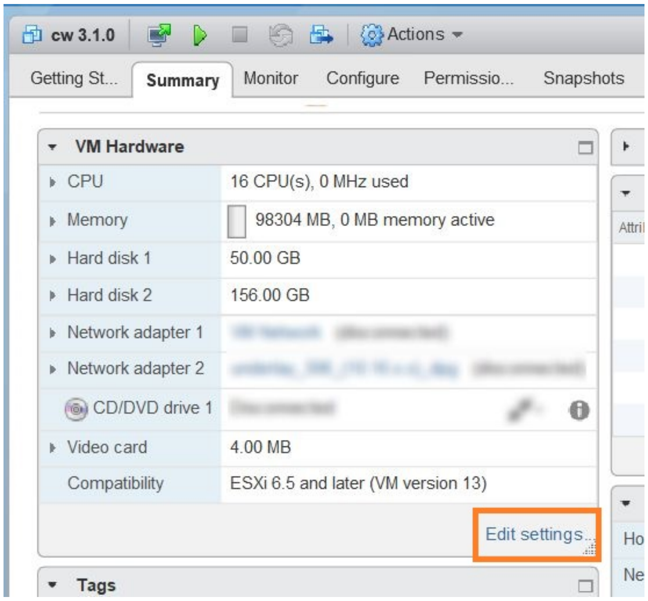


Recent Tasks

Task Name	1 ▲	Target	Status
Deploy OVF template		cw-[redacted]	0 % ⊗
Import OVF package		172.[redacted]	0 % ⊗

Step 19 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**, as shown in the following figure.

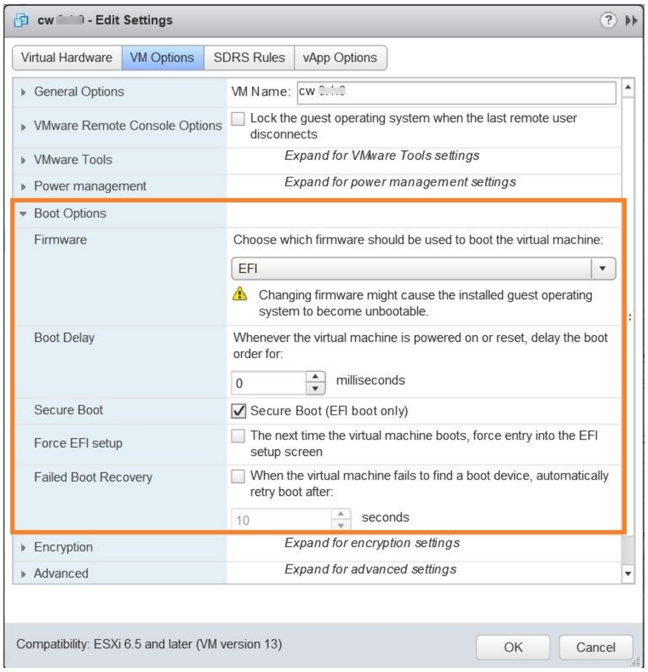


VM Hardware

CPU	16 CPU(s), 0 MHz used
Memory	98304 MB, 0 MB memory active
Hard disk 1	50.00 GB
Hard disk 2	156.00 GB
Network adapter 1	[redacted]
Network adapter 2	[redacted]
CD/DVD drive 1	[redacted]
Video card	4.00 MB
Compatibility	ESXi 6.5 and later (VM version 13)

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.



cw [redacted] - Edit Settings

Virtual Hardware | VM Options | SDRS Rules | vApp Options

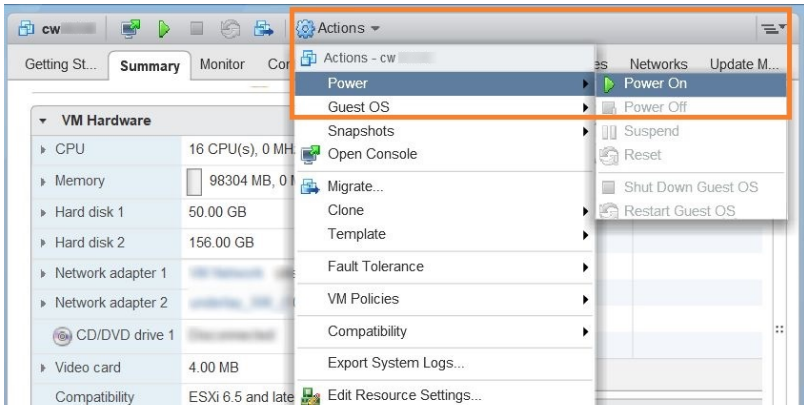
- General Options — VM Name: cw [redacted]
- VMware Remote Console Options — ☐ Lock the guest operating system when the last remote user disconnects
- VMware Tools — Expand for VMware Tools settings
- Power management — Expand for power management settings
- Boot Options
  - Firmware — Choose which firmware should be used to boot the virtual machine: EFI
    Changing firmware might cause the installed guest operating system to become unbootable.
  - Boot Delay — Whenever the virtual machine is powered on or reset, delay the boot order for: 0 milliseconds
  - Secure Boot — ☑ Secure Boot (EFI boot only)
  - Force EFI setup — ☐ The next time the virtual machine boots, force entry into the EFI setup screen
  - Failed Boot Recovery — ☐ When the virtual machine fails to find a boot device, automatically retry boot after: 10 seconds
- Encryption — Expand for encryption settings
- Advanced — Expand for advanced settings

Compatibility: ESXi 6.5 and later (VM version 13)

OK Cancel

Step 20 You can now power on the Cisco Crosswork Change Automation and Health Insights VM to complete the deployment process. Expand the host's entry so you can click the Cisco Crosswork Change Automation and Health Insights VM and then choose **Actions** > **Power** > **Power On**, as shown in the following figure.

Figure 5: Power On



From this point, the upgrade is automatically triggered. The Data and IP configurations are transferred from Cisco Crosswork Change Automation and Health Insights VM version 3.1 to version 3.2. Once the transfer is completed, Cisco Crosswork Change Automation and Health Insights VM version 3.1 will shut down. It will take 30 minutes or more for the Cisco Crosswork Change Automation and Health Insights VM version 3.2 to become operational. Please wait for the process to finish before continuing.

To get the current status of the upgrade, login as the super user and use the cli `upgrade status` command on the VM.

Note

- Each time the Cisco Crosswork Change Automation and Health Insights VM is re-imaged, you need to refresh the Cisco Crosswork Change Automation and Health Insights login page to accept the new certificate. Otherwise, the error message *Http failure response for /crosswork/sso/v1/tickets: 0 Unknown Error* is displayed on the login page.
- Each time the Cisco Crosswork Change Automation and Health Insights VM is re-imaged, Cisco Crosswork Data Gateway must be restarted to re-initialize the certificates. Otherwise, the devices become unreachable and collection stops.

Step 21 Install Cisco Crosswork Data Gateway and complete the post-installation tasks using the instructions in Install Cisco Crosswork Data Gateway, on page 38 and Post-installation Tasks, on page 58 respectively.

Step 22 Enroll the Cisco Crosswork Data Gateway with Cisco Crosswork Change Automation and Health Insights as instructed in Enroll Cisco Crosswork Data Gateway, on page 63. For information on adding devices to the Cisco Crosswork Data Gateway, see the *Manage Crosswork Data Gateway Instances* section in the *Cisco Crosswork Change Automation and Health Insights User Guide*

What to do next

- Verify that you are able to login to Cisco Crosswork Change Automation and Health Insights VM version 3.2 using the 3.1 credentials (**`cw-admin`** as username and password).
- Verify if the inventory data, application configurations, and AAA user configurations from Cisco Crosswork Change Automation and Health Insights VM version 3.1 have been retained in version 3.2.

Note While managing inventory in Cisco Crosswork Change Automation and Health Insights version 3.2:

- Make sure to use the latest CSV template for managing inventory.
- Configured state of devices being onboarded needs to be marked as DOWN.

- Verify if the device details are visible in the Topology page.
- Verify if Cisco Crosswork Data Gateway is onboarded and functioning properly.

Note

- After upgrade to version 3.2, all historical alerts will be available only for an hour. Future alerts will be available once devices are mapped to Cisco Crosswork Data Gateway for the enabled KPIs.
- Post upgrade, if helios fails to cleanup some of the nodes there will not be any impact, as the devices will be remapped to the new Cisco Crosswork Data Gateway VM.

- Check the health status of Cisco Crosswork Change Automation and Health Insights version 3.2 and Cisco Crosswork Data Gateway using the **Crosswork Manager** and **Data Gateway Management**windows in the UI respectively.

For more information, see the *Perform Administrative Tasks* chapter in the *Cisco Crosswork Change Automation and Health Insights User Guide*.

- Check if you are able to configure and use the applications in Cisco Crosswork Change Automation and Health Insights version 3.2. For more information on the UI workflow, see the *Cisco Crosswork Change Automation and Health Insights User Guide*.

Upgrade Cisco Crosswork Data Gateway

Note This procedure is required only for a Cisco Crosswork Data Gateway Base VM upgrade. Upgrade of other components, such as collectors, is performed by Crosswork as explained is Section Crosswork Patch Framework, on page 87.

Cisco Crosswork Data Gateway functions as a passive device in the network. As such, the upgrade process consists of stopping the active Cisco Crosswork Data Gateway instance and replacing it with a Cisco Crosswork Data Gateway instance that is running the new version of Cisco Crosswork Data Gateway software, essentially exchanging one Cisco Crosswork Data Gateway instance for another.

Follow the below steps.

Step 1 Put the current Cisco Crosswork Data Gateway instance in maintenance mode.

Steps to put a Cisco Crosswork Data Gateway instance in maintenance mode are described in Section: **Change the Administration State of a Cisco Crosswork Data Gateway VM** of *Cisco Crosswork Change Automation and Health Insights 3.2 User Guide*.

Step 2 Deploy the new upgraded Cisco Crosswork Data Gateway instance. See Install Cisco Crosswork Data Gateway, on page 38.

Step 3 Enroll the new Cisco Crosswork Data Gateway instance with Crosswork. See Enroll Cisco Crosswork Data Gateway With Cisco Crosswork Change Automation and Health Insights, on page 63.

Step 4 Uninstall the old Cisco Crosswork Data Gateway instance.

Crosswork Patch Framework

There are three types of patches in Cisco Crosswork Change Automation and Health Insights:

- **Crosswork Application Patching (PATCH_IMAGE)**: This is a patch on the Crosswork applications such as Change Automation and Health Insights, and the configuration packages within the application layer. One or more applications can be patched simultaneously.
- **Crosswork Data Gateway Patching (PATCH_CDG)**: This is a patch on the collector images for Cisco Crosswork Data Gateway VM.
- **Crosswork Data Patching (PATCH_DATA)**: This is a patch to dynamically update the pre-built set of fundamental data such as YANG models and system MIB packages used by the Crosswork applications.

The patch versioning is done in the [MAJOR: MINOR: PATCH] format, where MAJOR corresponds to every major release of the Cisco Crosswork Change Automation and Health Insights, MINOR corresponds to every critical (backward incompatible) change made during a release, and PATCH corresponds to every patch created in a release.

The unit of a patch is a TAR file. The TAR file consists of the patch metadata, list of docker images, checksum and signature. The metadata contains platform and product details, patch version, type of patch and other creation details. Signature is a security requirement in order to safeguard the patch; the signature is verified by the patch framework. It also helps to perform error correction mechanisms and detect if the patch is corrupted or not.

The platform orchestrator (such as Robot orchestrator) maintains and manages the lifecycle of all applications in the Crosswork platform. Each Crosswork product has its own centralized manifest file `<orchmanifest.json>` which contains the list of applications and the corresponding configurations. When the orchestrator is up, it goes through the manifest. Along with the manifest, the dependency diagram `<orch.yaml>` explains the logical grouping of applications and their dependencies. Currently, simultaneous application patching is possible as the applications are independent of each other. Patching the Collection Infra is a system-wide change and requires shutting down other dependent applications. A patch on the Core Infra is not allowed and is considered as a VM upgrade. Schema changes are not allowed during patching. Users are recommended to take backup of the system before patching, to restore in case of any error.

Patching Activation workflow:

Each stage of the patching workflow, performed using APIs, are explained below:

1. **Validate**
    - API: **/crosswork/platform/v1/patch/validate**
    - User downloads the patch to any reachable host from the Crosswork VM. After the download, the patch is validated for accuracy and compatibility to the product version.

2. **Add**
    - API: **/crosswork/platform/v1/patch/add**
    - After the patch is validated, it is added to the corresponding registry in the system, such as updating the IMAGE registry in case of an IMAGE patch. The *add* operation prepares the system for the patch to be activated. It is an asynchronous operation and may take around 15 mins. Once *add* is initiated, user receives a corresponding job ID and the operation is performed in the background.

3. **Status**
    - There are 2 status APIs:
    - *Status* - which displays the current status of the Patch framework.
        - API: **/crosswork/platform/v1/patch/status**
        - This API displays the current status of the patch framework, such as if *add* is successful or ongoing, or if *activate* has been triggered.
    - *Job Status* - which displays the specific job status.
        - API: **/crosswork/platform/v1/patch/jobstatus**
        - This API return the status of a specific job based on the Job ID.

4. **Activate**

   - API: **/crosswork/platform/v1/patch/activate**
   - After successful addition, the patching is locked. If a patch is added, it needs to be activated before another patch can be added to the application. *Activate*, like *add*, is an asynchronous operation that generates a job ID for the user and continues the process in the background. Activation takes the backup of the current state and updates the configuration. If the patch fails, the auto-roll back functionality rolls back to the previous version and the status is updated with the failure details.

5. **Summary**

   - API: **/crosswork/platform/v1/patch/summary**
   - *Summary* provides the overall summary of the Patch framework, and summary of the different patch types including patch version. This information changes each time a new patch is added and activated:
     - PATCH_IMAGE - Patch version and the applications changed as part of the patch.
     - PATCH_CDG - Patch version
     - PATCH_DATA - Patch version and the applications to which the new data has been uploaded.

6. **Remove**

   - API: **/crosswork/platform/v1/patch/remove**
   - A patch can be removed in 2 ways:
     - Flow 1: A patch can be removed after it is validated and added. For example, if user chooses to cancels after the *add* is successful, *remove* can be used.
     - Flow 2: A patch can be removed after it is validated, added and activated. For example, if user chooses to go back to a previous version after a patch is applied successfully, *remove* can be used.

For more information, refer the Swagger file for Payload https://github3.cisco.com/ROBOT/k8s-orchestrator/blob/develop/robotctl_api/robotctl_api.swagger.json

Upon successful activation of a patch, user can verify the health of the application using the **Crosswork Manager** or **Data Gateway Management** feature in Cisco Crosswork Change Automation and Health Insights, depending on the type of the patch. For more information, see the *Perform Administrative Tasks* chapter in *Cisco Crosswork Change Automation and Health Insights User Guide*.

CHAPTER 5

Deleting the Virtual Machine

This section contains the following topics:

Deleting Cisco Crosswork Change Automation and Health Insights and Cisco Crosswork Data Gateway

The procedure to delete a Cisco Crosswork Change Automation and Health Insights VM and Cisco Crosswork Data Gateway VM is the same.

Note

- Be aware that this procedure deletes all your Cisco Crosswork Change Automation and Health Insights 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 Change Automation and Health Insights 3.2 User Guide*.
  - De-enroll the Cisco Crosswork Data Gateway from Cisco Crosswork Change Automation and Health Insights as described in De-enroll Cisco Crosswork Data Gateway, on page 70.

Step 1 Log in to the VMware vSphere Web Client.

Step 2 In the **Navigator** pane, right-click the Cisco Crosswork Change Automation and Health Insights 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.

APPENDIX A

Device Configurations

This section provides device configurations that are necessary for device onboarding and the supported deployment modes. For more information on adding devices, see the "Manage Inventory" chapter in the Cisco Crosswork Change Automation and Health Insights User Guide.

- Prerequisites for Onboarding Devices, on page 93
- Supported TCP/IP Stack, on page 95

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 Change Automation and Health Insights. 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 Change Automation and Health Insights.

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>
```

Pre-Onboarding SNMPv2 and SNMPv3 Trap Configuration

If you want the device to send SNMP traps to Cisco Crosswork Change Automation and Health Insights, use the following commands to perform a pre-onboarding device configuration and test for the trap version you want.

For SNMP v2 traps:

```
snmp-server trap link ietf

snmp-server host <CrossworkDataGatewaysouthboundIPAddress> traps version 2c cisco123 udp-port
 1062

snmp-server community cisco123

snmp-server traps snmp linkup

snmp-server traps snmp linkdown
```

For SNMP v3 traps:

```
snmp-server trap link ietf

snmp-server host < CrossworkDataGatewaysouthboundIPAddress> traps version 3 cisco123 udp-port
 1062

snmp-server community cisco123

snmp-server traps snmp linkup
```

```
snmp-server traps snmp linkdown
```

Please note that, for traps to be received, the node_ip field for the device as listed in the Cisco Crosswork Change Automation and Health Insights inventory must match the IP address of the device interface from which the traps are sent. If they do not, Cisco Crosswork Change Automation and Health Insights will reject the traps. Also, the device needs to be in ADMIN_UP state for traps to be received.

Supported TCP/IP Stack

Cisco Crosswork Change Automation and Health Insights version 3.2 supports only single stack deployments (IPv4 or IPv6).

Table 11: Single stack deployment modes

Stack/Deployment mode	IPv4 only	IPv6 only
Cisco Crosswork Change Automation and Health Insights interfaces (two interfaces)	• IPv4 (mandatory) • IPv6 (optional)	• IPv4 (optional) • IPv6 (mandatory)
Cisco Crosswork Data Gateway	• IPv4 (mandatory) • IPv6 (optional)	• IPv4 (optional) • IPv6 (mandatory)
Providers	• IPv4 (mandatory) • IPv6 (optional)	• IPv4 (optional) • IPv6 (mandatory)
External Destinations	• IPv4 (mandatory) • IPv6 (optional)	• IPv4 (optional) • IPv6 (mandatory)
Devices	• IPv4 (mandatory) Device can be onboarded to Device Management only with IPv4 address.	• IPv6 (mandatory) Device can be onboarded to Device Management only with IPv6 address.
Restrictions	• Provider/Destination configuration and CDG Enrollment is prevented if interface connectivity information does not include an IPv4 address. • Device onboarding is prevented if IPv6 address is included.	• Provider/Destination configuration and CDG Enrollment is prevented if interface connectivity information does not include an IPv6 address. • Device onboarding is prevented if IPv4 address is included.