Installation Tasks

This section contains the following topics:

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 Cloud). It can be geographically separate from the controller running inside Crosswork Cloud.

Based on the size of your network, you can deploy more than one Cisco Crosswork Data Gateway instances. Crosswork Cloud orchestrates the collection from the distributed Cisco Crosswork Data Gateway instances.

The Cisco Crosswork Data Gateway VM is delivered as an OVA file and the additional functional/collection images are delivered as Docker images from the controller running inside Crosswork Cloud.

Before installing Cisco Crosswork Data Gateway, it is helpful to be familiar with Cisco Crosswork Data Gateway OVF Parameters and Deployment Scenarios, on page 2.

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

- Install Cisco Crosswork Data Gateway Via vCenter, on page 8
- Install Cisco Crosswork Data Gateway Via OVF Tool, on page 17

Base VM Contents

The Base VM (OVA) is pre-packaged with basic functionality required to reach the controller.

The Cisco Crosswork Data Gateway VM (OVA) contains the following pre-packaged contents:

- Cisco hardened Ubuntu distribution of Linux
- Cisco Crosswork Data Gateway services:

1. Vitals Monitor - Monitors the start and stop status of the container services running on the Cisco Crosswork Data Gateway VM.
2. Controller Gateway – Establishes trusted connection with the controller application via the Controller Gateway and downloads functional images and configuration files.
3. Image Manager – Coordinates between the Cisco Crosswork Data Gateway and the controller application to download functional images and configuration files.
4. Route Manager – Allows functional/collection images to program routes, so the traffic to devices can directed on different south-bound network.
5. Docker IPv6nat - Programs IPv6 routes for docker containers.

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 * Denotes the mandatory parameters. Others are optional. You might choose them based on the kind of deployment scenrio you require. Deployment scenarios are explained wherever applicable.

** Denotes parameters that can be entered during install or addressed using additional procedures.

Table 1: Cisco Crosswork Data Gateway OVF Parameters and Deployment Scenarios

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.	

OVF Parameter	Description	Deployment Scenario
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.	
Active vNICs*	Number of vNICs to use for sending traffic.	You can choose to use either 1 or 2 vNICs as per the following combinations: • **1** - sends all traffic through vNIC0. • **2** - sends management traffic through vNIC0 and all data traffic through vNIC1.
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 (from the vNIC0 interface via SCP) 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.	**Note** Keep a note of these usernames and passwords as they will be required to login.
dg-oper Password*	The password you have chosen for the dg-oper user.	
Note • Cisco Crosswork Data Gateway supports either IPv4 or IPv6 for vNIC0, vNIC1, and vNIC2 interfaces. For the interface(s) and protocol you choose to use, select **Method** as **Static** and enter information in **Address**, **Netmask**, and **Gateway** fields. The default value is **None**.		
[1]**vNIC0 IPv4 Address**		

OVF Parameter	Description	Deployment Scenario
vNIC0 IPv4 Method*	How the vNIC0 interface gets its IPv4 address.	
vNIC0 IPv4 Address	IPv4 address of the vNIC0 interface.	
vNIC0 IPv4 Netmask	IPv4 netmask of the vNIC0 interface in dotted quad format.	
vNIC0 IPv4 Gateway	IPv4 address of the vNIC0 gateway.	
[1]**vNIC0 IPv6 Address**		
vNIC0 IPv6 Method*	How the vNIC0 interface gets its IPv6 address.	
vNIC0 IPv6 Address	IPv6 address of the vNIC0 interface.	
vNIC0 IPv6 Netmask	IPv6 prefix of the vNIC0 interface.	
vNIC0 IPv6 Gateway	IPv6 address of the vNIC0 gateway.	
[1]**vNIC1 IPv4 Address**		
vNIC1 IPv4 Method*	How the vNIC1 interface gets its IPv4 address.	
vNIC1 IPv4 Address	IPv4 address of the vNIC1 interface.	
vNIC1 IPv4 Netmask	IPv4 netmask of the vNIC1 interface in dotted quad format.	
vNIC1 IPv4 Gateway	IPv4 address of the vNIC1 gateway.	
[1]**vNIC1 IPv6 Address**		
vNIC1 IPv6 Method*	How the vNIC1 interface gets its IPv6 address.	
vNIC1 IPv6 Address	IPv6 address of the vNIC1 interface.	
vNIC1 IPv6 Netmask	IPv6 netmask of the vNIC1 interface in dotted quad format.	
vNIC1 IPv6 Gateway	IPv6 address of the vNIC1 gateway.	

OVF Parameter	Description	Deployment Scenario
[1]**vNIC2 IPv4 Address** **Note** vNIC2 interface is not applicable to Cloud Deployment.		
vNIC2 IPv4 Method*	How the vNIC2 interface gets its IPv4 address.	
vNIC2 IPv4 Address	IPv4 address of the vNIC2 interface.	
vNIC2 IPv4 Netmask	IPv4 netmask of the vNIC2 interface in dotted quad format.	
vNIC2 IPv4 Gateway	IPv4 address of the vNIC2 gateway.	
[1]**vNIC2 IPv6 Address** **Note** vNIC2 interface is not applicable to Cloud Deployment.		
vNIC2 IPv6 Method*	How the vNIC2 interface gets its IPv6 address.	
vNIC2 IPv6 Address	IPv6 address of the vNIC2 interface.	
vNIC2 IPv6 Netmask	IPv6 netmask of the vNIC2 interface in dotted quad format.	
vNIC2 IPv6 Gateway	IPv6 address of the vNIC2 gateway.	
DNS and NTP		
DNS Address*	Space-delimited list of IPv4/IPv6 addresses of the DNS server accessible from the management interface.	
DNS Search Domain*	DNS search domain	

OVF Parameter	Description	Deployment Scenario
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 critical for time synchronization between Cisco Crosswork Data Gateway VM, Cisco Crosswork Cloud, and devices. 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 Cloud is not more than 24 hours. Else, Cisco Crosswork Data Gateway will fail to connect.
Syslog Servers		
Server Address	IPv4 or IPv6 address of a syslog server accessible from the management interface. **Note** If you are using an IPv6 address, 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 only to the Cisco Crosswork Data Gateway VM. To obtain logs, from the main menu, go to **5 Troubleshooting** > **Run show-tech**. **Note** The host with the URI files must be reachable on the network (from vNIC0 interface via SCP) 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		

OVF Parameter	Description	Deployment Scenario
Proxy Server URL	URL of management network proxy server.	If you want to use a proxy server, you must specify these parameters. In Cloud deployment, Cisco Crosswork Data Gateway must connect to the Internet via TLS, and a proxy server may be required if present in your environment. A symptom of missing proxy server is that the Cisco Crosswork Data Gateway will fail to connect to Crosswork Cloud correctly. If a proxy server is required, then additional configuration may be required and will vary based on the environment.
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		
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 by following the procedure Export Enrollment Package, on page 22.
Enrollment Passphrase**	SCP user passphrase to transfer enrollment package.	

[1]Either an IPv4 or IPv6 address must be specified for the interface(s) you choose to use. Selecting **None** for both will result in a non-functional deployment.

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.

Install Cisco Crosswork Data Gateway Via vCenter

Before you begin

Ensure the following:

- You are creating the Cisco Crosswork Data Gateway VM on a recommended VMware version (See Virtual Machine (VM) Requirements 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 70 GB of hard drive space.

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 Chapter *Manage Users*.

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.

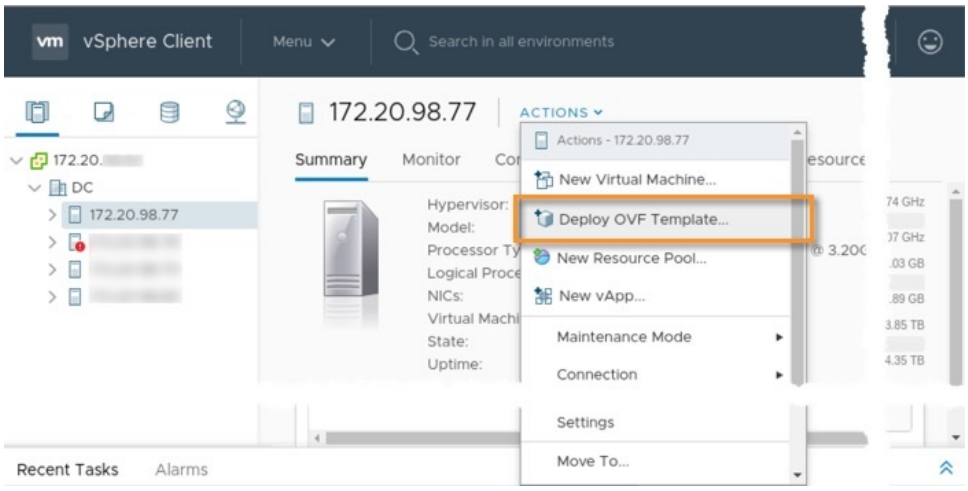
In case of lost or forgotten passwords, the user would have to create a new VM, destroy the current VM, and re-enroll the new one on the Crosswork Cloud.

Step 1 Download the Cisco Crosswork Data Gateway 1.1.4 image file (*.ova) from CCO.

Note If you have trouble downloading the software, please reach out to your Cisco representative.

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**.

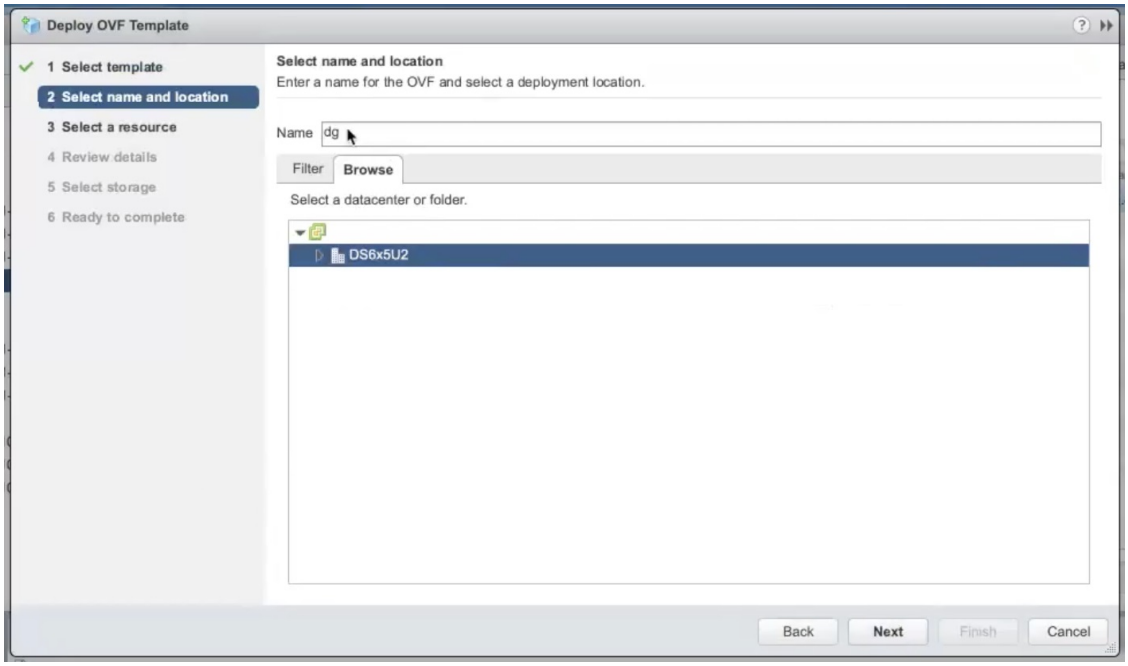
a) Click **Browse** to navigate to the location where you downloaded the OVA image file and select it.

Once selected, the filename is displayed in the window.

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

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

b) In the **Select a location for the virtual machine** list, choose the datacenter under which the Cisco Crosswork Data Gateway VM will reside.



Step 5 Click **Next** to go to **3 Select a resource**. Choose the VM's host.

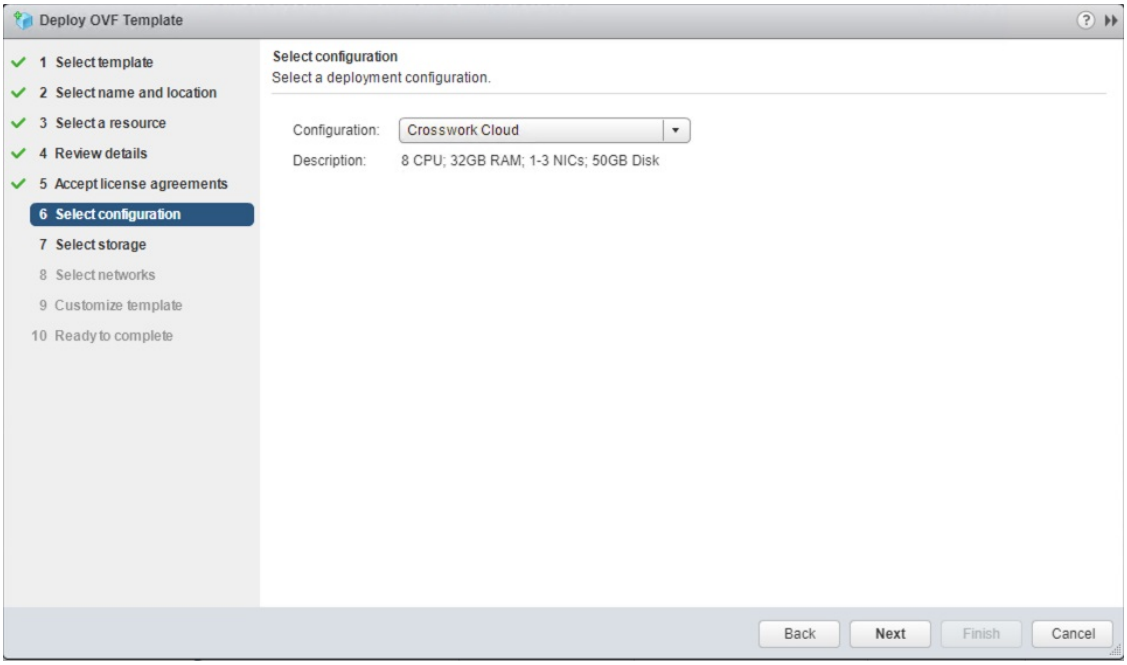
Step 6 Click **Next**. The VMware vCenter Server validates the OVA. Network speed will determine how long validation takes. When the validation is complete, the wizard moves to **4 Review details**. Review the OVA's information and then click **Next**.

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

Note This information is gathered from the OVF and cannot be modified.

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

Step 8 Click **Next** to go to **6 Select configuration**, as shown in the following figure. To install Cisco Crosswork Data Gateway for Crosswork Cloud, you must select **Crosswork Cloud** from the **Configuration** dropdown.

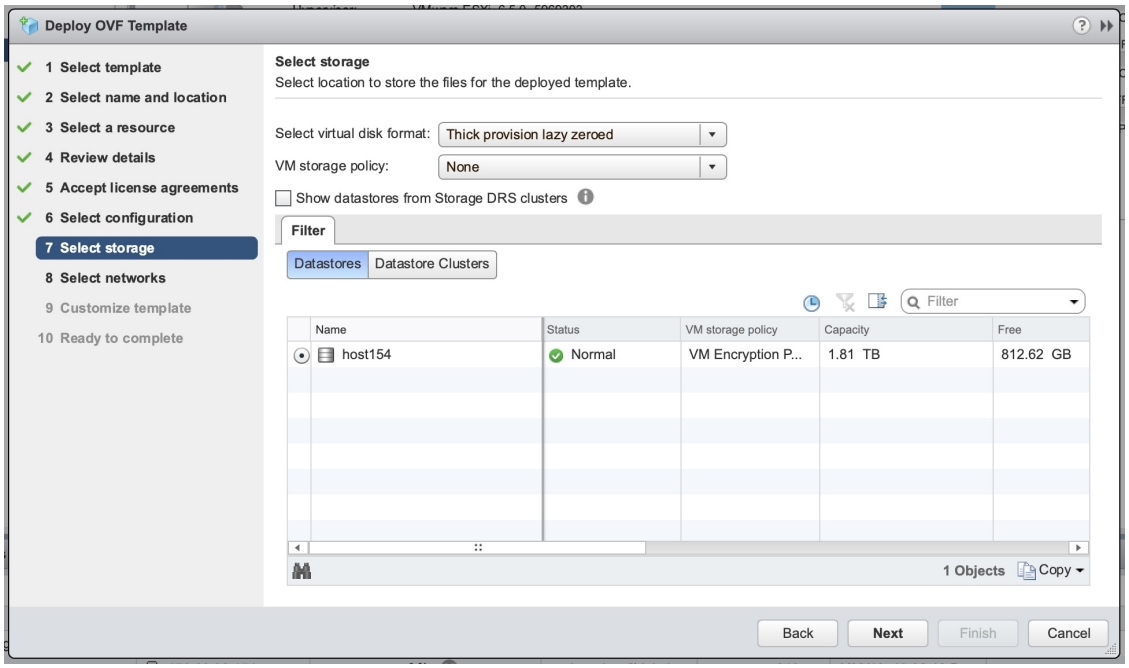


Step 9 Click **Next** to go to **7 Select storage**, as shown in the following figure.

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

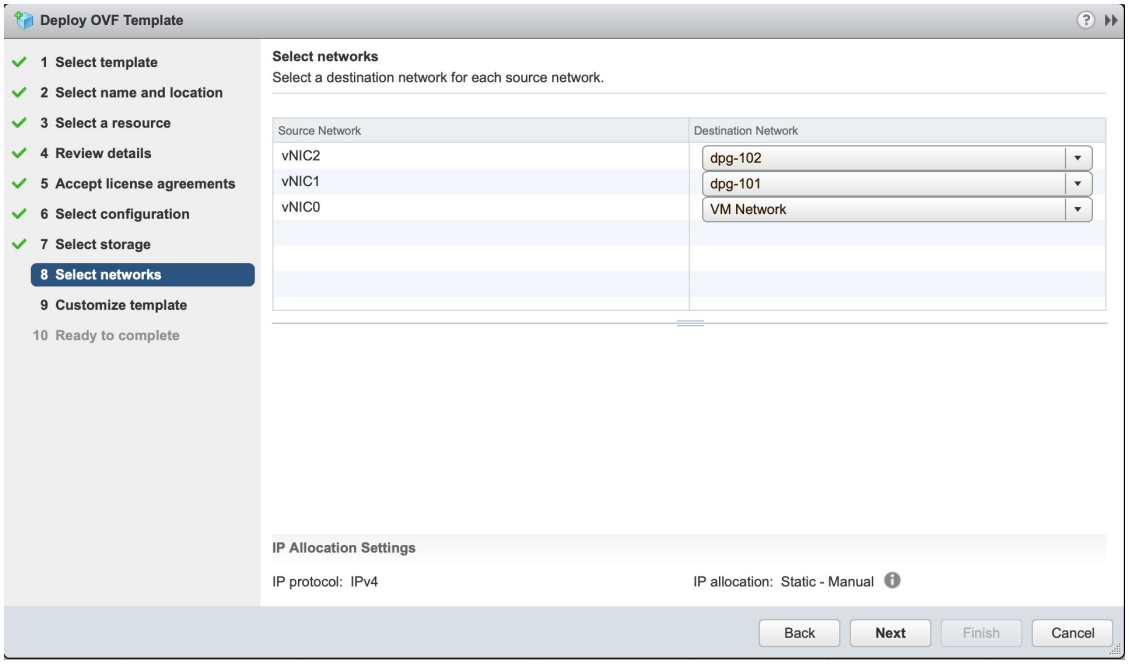
b) From the **Datastores** table, choose the datastore you want to use and review its properties to ensure there is enough available storage.

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



Step 10 Click **Next** to go to **8 Select networks**, as shown in the following figure. In the dropdown table at the top of the page, choose the appropriate destination network for each source network, **vNIC1** and **vNIC0** respectively.

Note vNIC2 is not applicable to cloud deployment.



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 2, 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).

01. Host Information

a. 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.

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

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

d. Active vNICs: Number of vNICs to use for sending traffic. You can choose to use either 1 or 2 vNICs as per the following combinations:

- **1** - sends all traffic through vNIC0.
- **2** - sends management traffic through vNIC0 and all data traffic through vNIC1.

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

f. 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).

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

02. Passphrases

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

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

Note
- Cisco Crosswork Data Gateway supports either IPv4 or IPv6 for vNIC0, vNIC1, and vNIC2 interfaces. For the interface(s) and protocol you choose to use, select **Method** as **Static** and enter information in **Address**, **Netmask**, and **Gateway** fields. The default value is **None**.

03. vNIC0 IPv4 Address

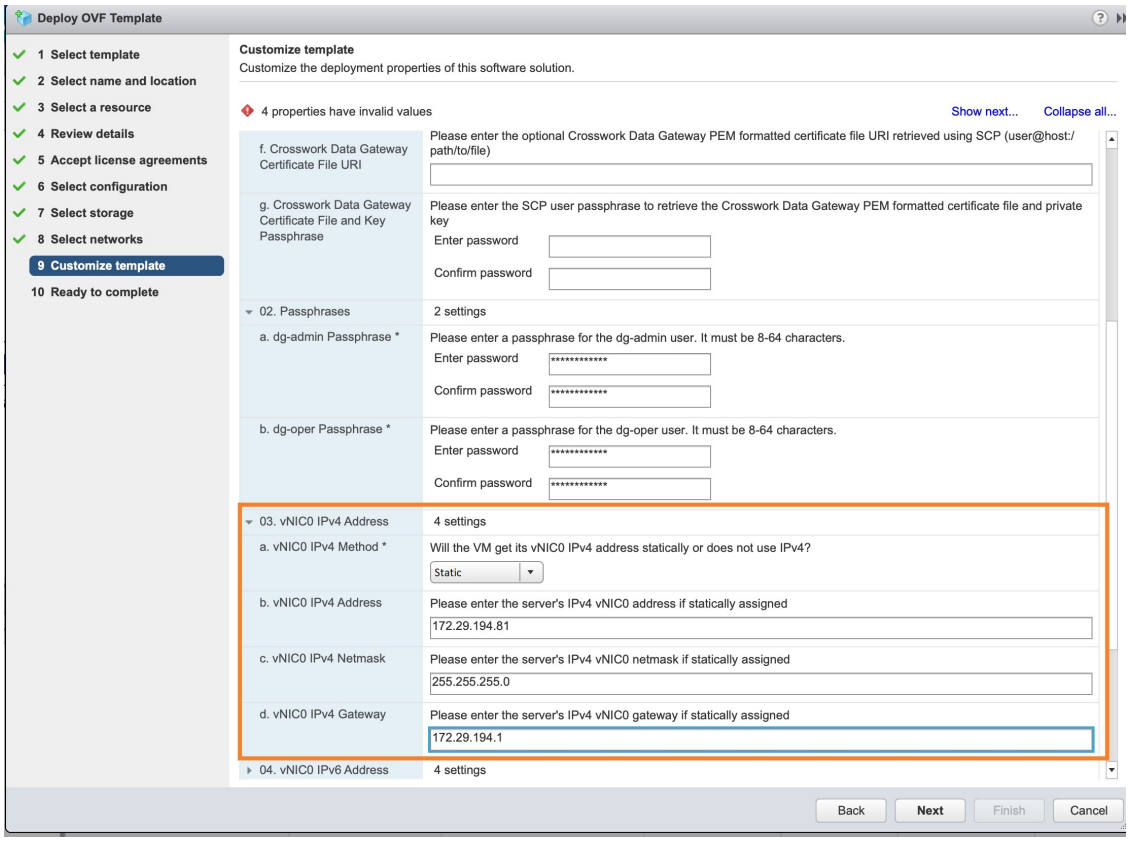
a. vNIC0 IPv4 Method: How the vNIC0 interface gets its IPv4 address.

b. vNIC0 IPv4 Address: IPv4 address of the vNIC0 interface.

c. vNIC0 IPv4 Netmask: IPv4 netmask of the vNIC0 interface in dotted quad format.

d. vNIC0 IPv4 Gateway: IPv4 address of the vNIC0 gateway.

An example is shown below:



04. vNIC0 IPv6 Address

a. vNIC0 IPv6 Method: How the vNIC0 interface gets its IPv6 address.

b. vNIC0 IPv6 Address: IPv6 address of the vNIC0 interface.

c. vNIC0 IPv6 Netmask: IPv6 netmask of the vNIC0 interface in dotted quad format.

d. vNIC0 IPv6 Gateway: IPv6 address of the vNIC0 gateway.

05. vNIC1 IPv4 Address

a. vNIC1 IPv4 Method: How the vNIC1 interface gets its IPv4 address.

b. vNIC1 IPv4 Address: IPv4 address of the vNIC1 interface.

c. vNIC1 IPv4 Netmask: IPv4 netmask of the vNIC1 interface in dotted quad format.

d. vNIC1 IPv4 Gateway: IPv4 address of the vNIC1 gateway.

06. vNIC1 IPv6 Address

a. vNIC1 IPv6 Method: How the vNIC1 interface gets its IPv6 address.

b. vNIC1 IPv6 Address: IPv6 address of the vNIC1 interface.

c. vNIC1 IPv6 Netmask: IPv6 netmask of the vNIC1 interface in dotted quad format.

d. vNIC1 IPv6 Gateway: IPv6 address of the vNIC1 gateway.

07. vNIC2 IPv4 Address

Not applicable to cloud deployment.

08. vNIC2 IPv6 Address

Not applicable to cloud deployment.

09. DNS and NTP

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

b. DNS Search Domain: DNS search domain

c. 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 critical for time synchronization between Cisco Crosswork Data Gateway VM, Cisco Crosswork Cloud, and devices. 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 Cloud is not more than 24 hours. Else, Cisco Crosswork Data Gateway will fail to connect.

10. Syslog Servers

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

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

b. Syslog Port: Port number of the syslog server.

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

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

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

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

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

11. Controller Settings

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

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

h. Authenticated Proxy Username: Username for authenticated proxy servers.

i. Authenticated Proxy Passphrase: Passphrase for authenticated proxy servers.

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

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

12. Auto Enrollment Package

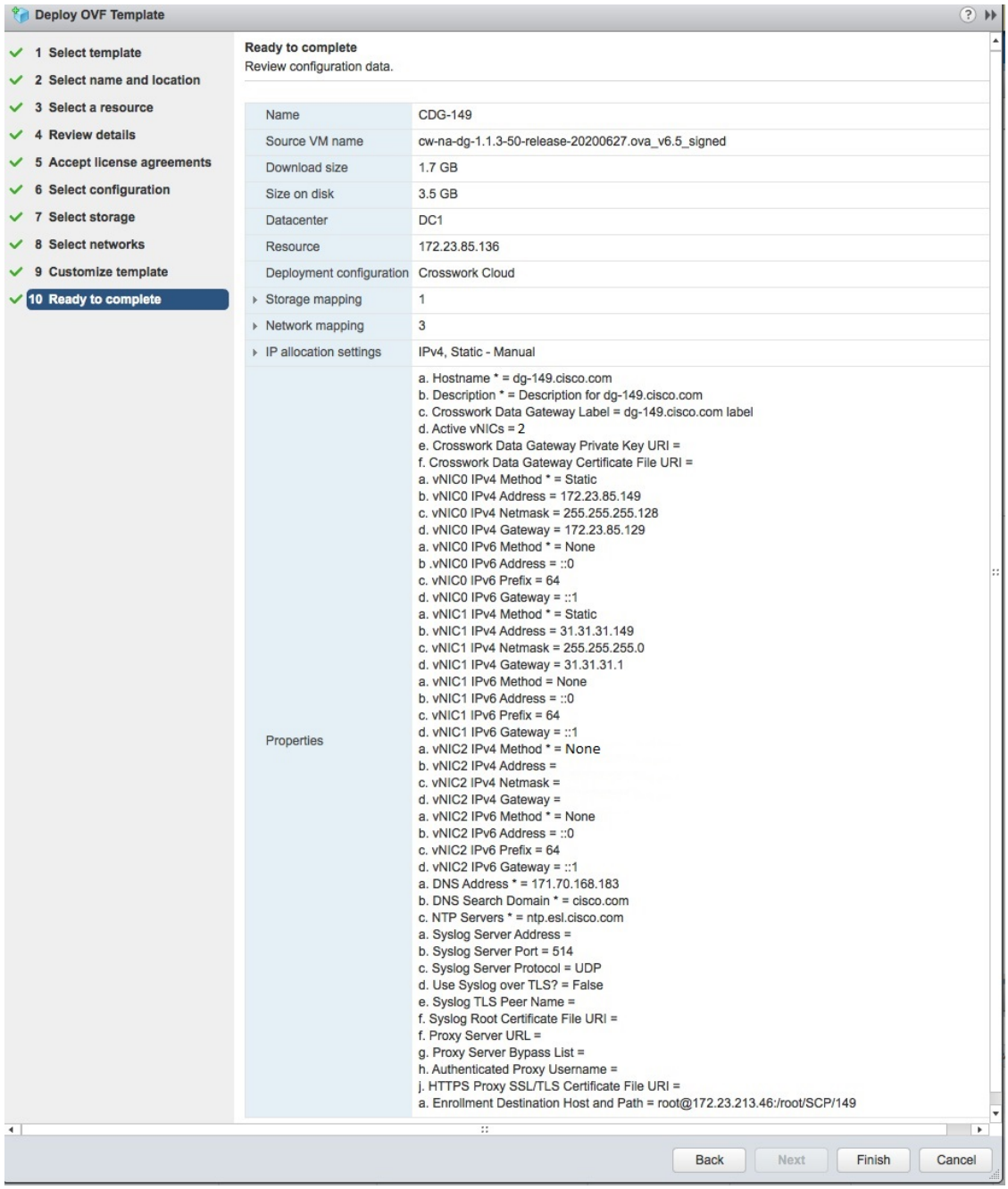
Note Enrollment package is required for enrolling Cisco Crosswork Data Gateway with Crosswork. The enrollment package is automatically transferred once Cisco Crosswork Data Gateway boots up for the first time if you specify these parameters during the installation.

If you do not specify these parameters during installation, then you must export enrollment package manually by following the procedure Export Enrollment Package, on page 22.

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

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

Step 12 Click **Next** to go to **10 Ready to complete**, as shown in the following figure. Review your settings and then click **Finish** if you are ready to begin deployment.



Step 13 Wait for the deployment to finish before continuing. To check the deployment status:

a) Open the vCenter vSphere client.

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

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:

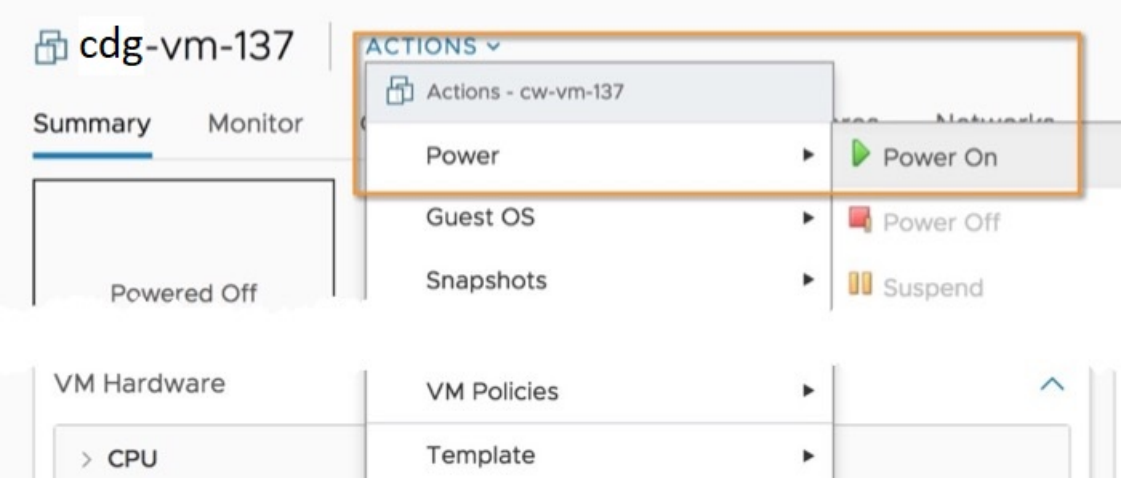
a. On the host VM **Summary** tab, below the **VM Hardware** table, click **Edit Settings**.

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 20.

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>"

VM_NAME="dg-141"
DM="thin"
Deployment="cloud"

ActiveVnics="2"
```

```
Hostname="Hostname"
Vnic0IPv4Address="<Vnic0_ipv4_address>"
Vnic0IPv4Gateway="<Vnic0_ipv4_gateway>"
Vnic0IPv4Netmask="<Vnic0_ipv4_netmask>"
Vnic0IPv4Method="Static"
Vnic1IPv4Address="<Vnic1_ipv4_address>"
Vnic1IPv4Gateway="<Vnic1_ipv4_gateway>"
Vnic1IPv4Netmask="<Vnic1_ipv4_netmask>"
Vnic1IPv4Method="Static"

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


Description="Description for Cisco Crosswork Data Gatewayi : "dg-141""
Label="Label for Cisco Crosswork Data Gateway dg-141"

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

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

ProxyUsername="<username_for_proxy>"
ProxyPassphrase="<password_for_proxy>"

SyslogAddress="<syslog_server_address>"
SyslogPort=<syslog_server_port>
SyslogProtocol="<syslog_server_protocol>"
SyslogTLS=False
SyslogPeerName="<syslog_server_peer_name>"
SyslogCertChain="<syslog_server_root_certificate>"
SyslogCertChainPwd="<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=$VM_NAME \
--net:"vNIC0=VM Network" \
--net:"vNIC1=DPortGroupVC-1" \
--deploymentOption=$Deployment \
--prop:"EnrollmentURI=$EnrollmentURI" \
--prop:"EnrollmentPassphrase=$EnrollmentPassphrase" \
--prop:"Hostname=$Hostname" \
--prop:"Description=$Description" \
--prop:"Label=$Label" \
--prop:"ActiveVnics=$ActiveVnics" \
--prop:"Vnic0IPv4Address=$Vnic0IPv4Address" \
--prop:"Vnic0IPv4Gateway=$Vnic0IPv4Gateway" \
--prop:"Vnic0IPv4Netmask=$Vnic0IPv4Netmask" \
--prop:"Vnic0IPv4Method=$Vnic0IPv4Method" \
--prop:"Vnic1IPv4Address=$Vnic1IPv4Address" \
--prop:"Vnic1IPv4Gateway=$Vnic1IPv4Gateway" \
--prop:"Vnic1IPv4Netmask=$Vnic1IPv4Netmask" \
--prop:"Vnic1IPv4Method=$Vnic1IPv4Method" \
--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,

```
ovftool --noSSLVerify --overwrite --powerOffTarget --powerOn --acceptAllEulas --skipManifestCheck
--X:injectOvfEnv --allowExtraConfig \
--extraConfig:firmware=efi --extraConfig:uefi.secureBoot.enabled=true \
--net:"vNIC0=VM Network" -ds="datastore-<data_store>-ssd" --diskMode="thin" \
--deploymentOption="cloud" --prop:"Description=CDG VM Single Interface" \
--name="cdg1.cisco.local" --prop:"Hostname=cdg1.cisco.local" --prop:"ActiveVnics=1" \
--prop:"Vnic0IPv4Method=Static" \
--prop:"Vnic0IPv4Address=<Vnic0_ipv4_address>" --prop:"Vnic0IPv4Netmask=<Vnic0_ipv4_netmask>"
--prop:"Vnic0IPv4Gateway=<Vnic0_ipv4_gateway>" \
--prop:'dg-adminPassword=<dg-admin_password>' --prop:'dg-operPassword=<dg-oper_password>' \
--prop:"DNS=<DNS_ip_address>" --prop:"NTP=<NTP Server>" --prop:"Domain=cisco.com" \
cw-na-dg-1.1.3-14-TESTONLY-20200501.ova
vi://'administrator@ai.local:<vcenter_password>'@<vcenter_ip_address>/ai/host/172.25.126.21
```

OR

if you want to execute a file containing the command and arguments, run the following command:

```
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:

1. Log In and Log Out, on page 20
2. Generate Enrollment Package, on page 21
3. Export Enrollment Package, on page 22

Note Steps 4 and 5 are applicable only if you are going to use Cisco Crosswork Data Gateway with Cisco Crosswork Trust Insights.

4. Configure Control Proxy
5. Verify the Cisco Crosswork Data Gateway Connectivity
6. Enroll Cisco Crosswork Data Gateway with Crosswork Trust Insights

Note For procedure to enroll Cisco Crosswork Data Gateway with Crosswork Trust Insights, refer Section: **Add Crosswork Data Gateway Information** in *Cisco Crosswork Trust Insights User Guide*.

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 20
- Access Cisco Crosswork Data Gateway Via SSH, on page 20

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**.

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>**

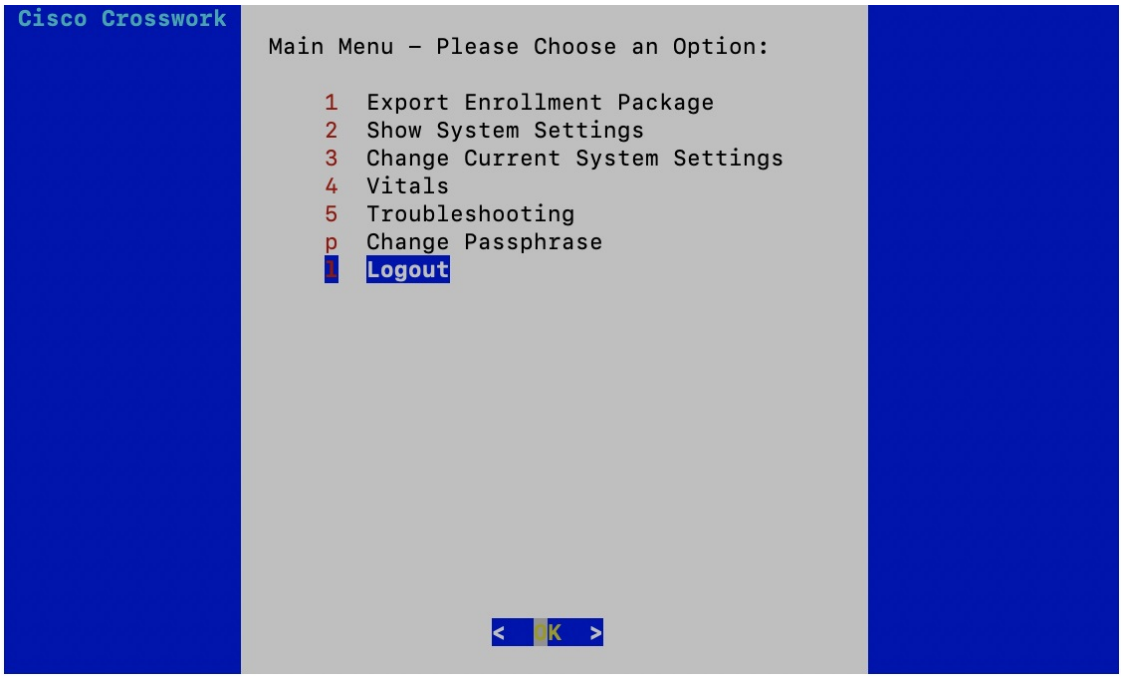
To login as operator user: **ssh dg-oper@<ManagementNetworkIP>**

The Cisco Crosswork Data Gateway flash screen opens prompting for 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**.



Generate 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 using any of the following two methods:

- By supplying **Auto Enrollment Package** OVF parameters during installation process (see Auto Enrollment Package under OVF deployment scenarios and Step 11 Auto Enrollment Package of *Install Crosswork Data Gateway via vCenter*)
- By using the **Export Enrollment Package** option from the interactive menu (see Export Enrollment Package, on page 22)

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, etc.

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 Cloud. The steps to do so are described in Export Enrollment Package, on page 22.

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

A sample enrollment package JSON 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": [
    "<cert_chain>"
  ],
  "version": "1.1.0 (branch dg110dev - build number 152)",
  "duuid": "d58fe482-fdca-468b-a7ad-dfbfa916e58b"
}
```

Note The value shown for *memory* represents the usable amount for user processes, not the total VM amount. The Cisco Crosswork Data Gateway operating system reserves about 700MB from the total VM memory for itself, which is excluded from memory reporting tools. It is expected for the *memory* value reported here to be 1GB less than the full amount allocated to the VM due to operating system reservation and rounding.

Export Enrollment Package

To enroll the Cisco Crosswork Data Gateway with Crosswork Cloud, you must have a copy of the enrollment package on your local computer.

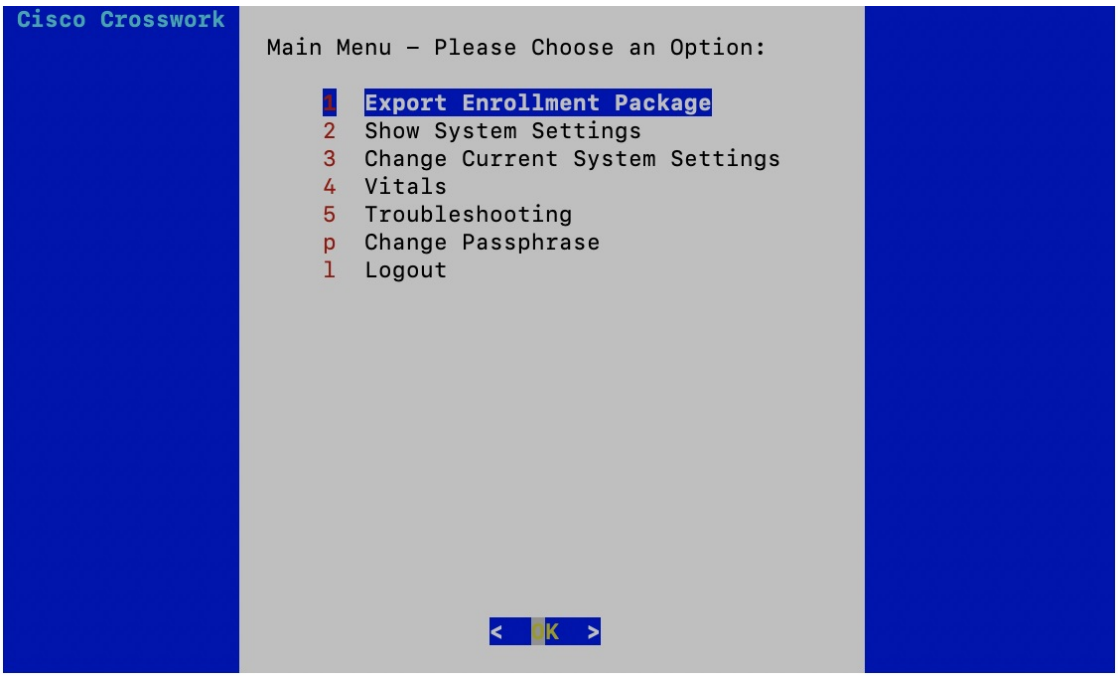
Note This is needed only if you have not specified **Auto Enrollment Package Transfer** settings in the OVF template. Otherwise, the file will be copied to the SCP URI destination you selected after the VM boots.

Cisco Crosswork Data Gateway uses SCP (via SSH) protocol to preserve formatting and eliminate common errors when transferring text-based files.

Follow these steps:

Step 1 Log in to the Cisco Crosswork Data Gateway Base VM as explained in Section Log In and Log Out, on page 20.

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

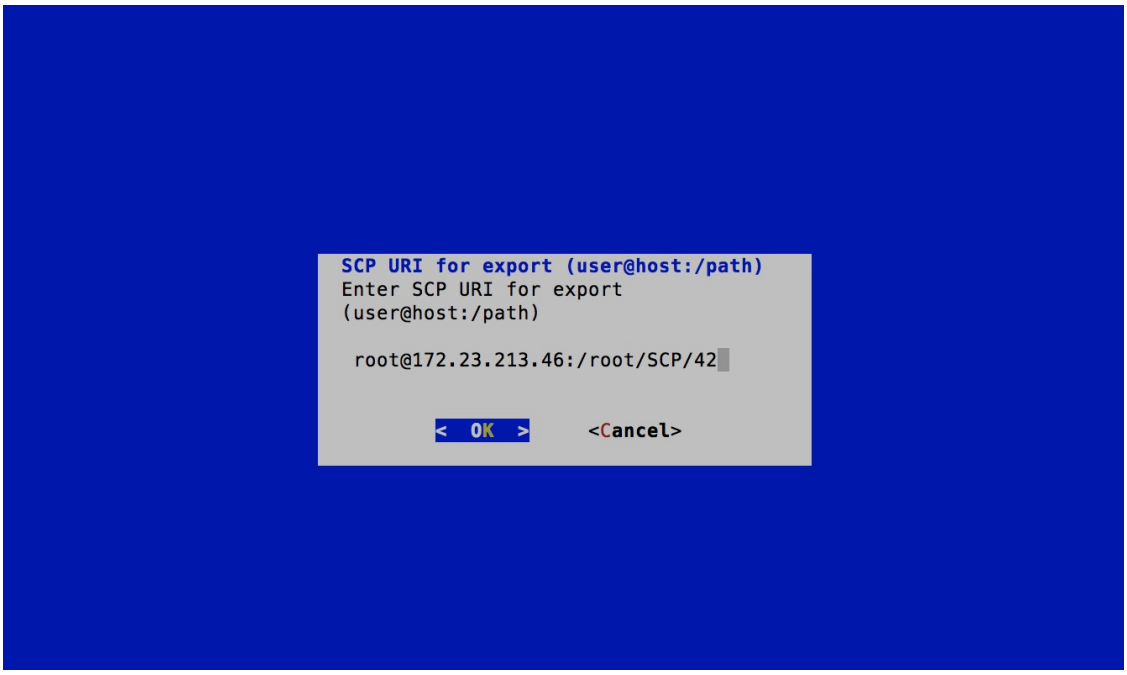


Step 3 Enter the SCP URI for exporting the enrollment package and click **OK**.

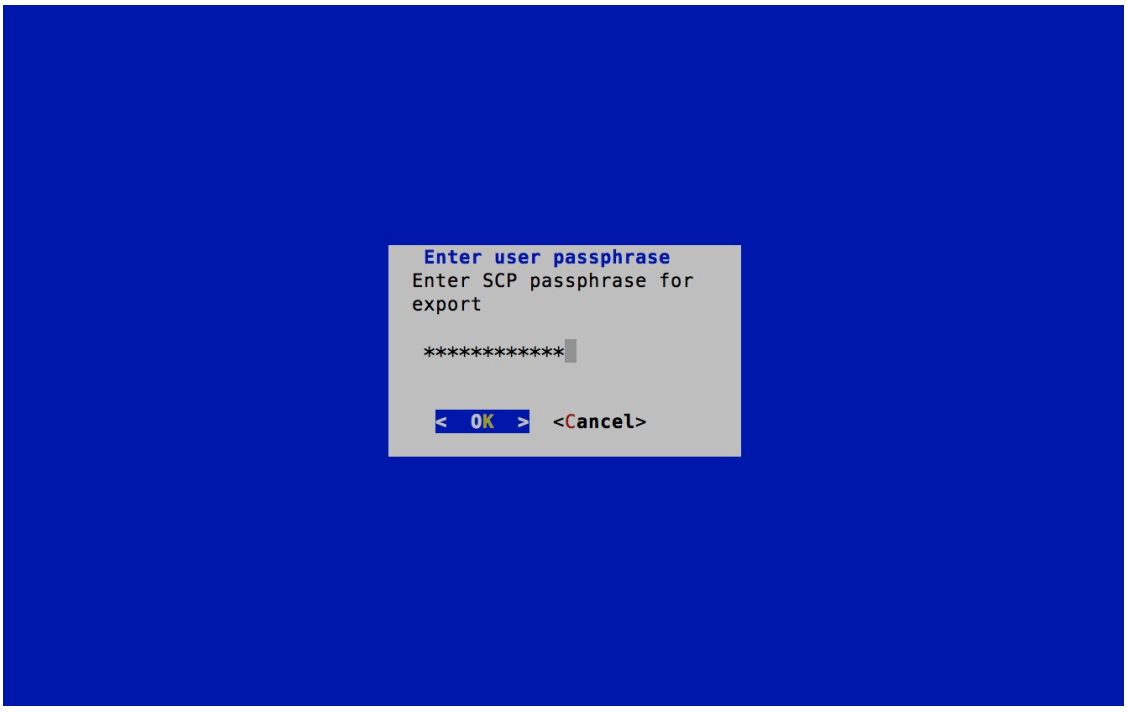
Note

- 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 you are not using the default port 22, you can specify the port as a part of the SCP command. For example, to export the enrollment package to another host that has SCP server listening on port 4000, you can give the following command:

```
-P4000 admin@<ip_address>:/home/admin
```



Step 4 Enter the SCP passphrase (the SCP user password) and click **OK**.



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 the Cisco Crosswork Data Gateway with Crosswork Cloud.

Note Before enrolling Cisco Crosswork Data Gateway with Cisco Crosswork Trust Insights, the following two additional steps must also be performed:

a. Configure Control Proxy

b. Verify the Cisco Crosswork Data Gateway Connectivity