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 enroll itself with Crosswork Cloud). Once the Crosswork Data Gateway is registered with Crosswork Cloud, Crosswork Cloud pushes the collection job configuration down to the Crosswork Data Gateway, enabling it to gather the data it needs from the network devices.

Based on the size and geography of your network, you can deploy more than one Cisco Crosswork Data Gateway.

Cisco Crosswork Data Gateway Deployment and Set Up Workflow

To deploy and set up Cisco Crosswork Data Gateway for use with Crosswork Cloud, follows these steps:

1. Plan your installation. Refer to the topic Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2 for information on deployment parameters and possible deployment scenarios.

2. Install Cisco Crosswork Data Gateway on your preferred platform:

VMware	Install Crosswork Data Gateway Using vCenter vSphere Client, on page 11
	Install Crosswork Data Gateway Via OVF Tool, on page 17

OpenStack	Install Crosswork Data Gateway on OpenStack from OpenStack CLI, on page 19 Install Crosswork Data Gateway on OpenStack from the OpenStack UI, on page 26

3. Generate and export Enrollment package.
    - Generate Enrollment Package, on page 43
    - Export Enrollment Package, on page 44
4. Enroll Cisco Crosswork Data Gateway with Crosswork Cloud applications. See Register Crosswork Data Gateway with Crosswork Cloud Applications, on page 45.

Cisco Crosswork Data Gateway Deployment Parameters and Scenarios

Before you begin installing the Crosswork Data Gateway, go through this section to read about the deployment parameters and possible deployment scenarios.

Interface addresses

Crosswork Data Gateway supports either IPv4 or IPv6 for all interfaces. Crosswork Cloud does not support dual stack configurations. Therefore, plan ALL addresses for the environment as either IPv4 or IPv6.

User Accounts

During installation, Cisco Crosswork Data Gateway creates three default user accounts:

- Cisco Crosswork Data Gateway administrator, with the username, **dg-admin** and the password set during installation. The administrator uses this ID to log in and troubleshoot Cisco Crosswork Data Gateway.
- Cisco Crosswork Data Gateway operator, with the username, **dg-oper** and the password set during installation. This is a read-only user and has permissions to perform all 'read' operations and limited 'action' commands.
- A **dg-tac** user account that is used to enable Cisco to assist you in troubleshooting issues with the Crosswork Data Gateway. (Enable TAC Shell Access). The temporary password for this account is created when you enable troubleshooting access.

To know what operations an admin and operator can perform, see Section Supported User Roles.

The **dg-admin** and **dg-oper** user accounts are reserved usernames and cannot be changed. You can change the password from the console for both the accounts. See Change Password. In case of lost or forgotten passwords, you have to create a new VM, destroy the current VM, and re-enroll the new VM on Crosswork Cloud.

Installation Parameters and Scenarios

In the following table:

* Denotes the mandatory parameters. Other parameters are optional. You can choose them based on deployment scenario you require. We have explained deployment scenarios wherever applicable in the **Additional Information** column.

** Denotes parameters that you can enter during install or address later using additional procedures.

Table 1: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios

Name	Parameter	Description	Additional Information
Host Information			
Hostname*	`Hostname`	Name of the Cisco Crosswork Data Gateway VM specified as a fully qualified domain name (FQDN). **Note** In larger systems you are likely to have more than one Cisco Crosswork Data Gateway VM. The hostname must, therefore, be unique and created in a way that makes identifying a specific VM easy.	
Description*	`Description`	A detailed description of the Cisco Crosswork Data Gateway.	
Label	`Label`	Label used by Cisco Crosswork Cloud to categorize and group multiple Cisco Crosswork Data Gateways.	
Deployment	`Deployment`	Parameter that conveys the controller type. Specify the value as `Crosswork Cloud`.	

Name	Parameter	Description	Additional Information
Active vNICs*	`ActiveVnics`	Number of vNICs to use for sending traffic.	You can choose to use either 1, 2 or 3 interfaces as per your network requirements. For information on how you can route traffic, see *Interfaces* in the VM Requirements table.
AllowRFC8190 *	`AllowRFC8190`	Automatically allow addresses in an RFC 8190 range. Options are `yes`, `no` or `ask`, where the initial configuration script prompts for confirmation. The default value is `yes`.	
Private Key URI	`DGCertKey`	URI to private key file for session key signing. You can retrieve this using SCP (user@host:path/to/file).	Crosswork Cloud uses self-signed certificates for handshake with Cisco Crosswork Data Gateway. These certificates are generated at installation. However, if you want to use third-party or your own certificate files enter these three parameters. Certificate chains override any preset or generated certificates in the Cisco Crosswork Data Gateway VM and are given as an SCP URI (user:host:/path/to/file). **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	`DGCertChain`	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	`DGCertChainPwd`	SCP user passphrase to retrieve the Cisco Crosswork Data Gateway PEM formatted certificate file and private key.	

Name	Parameter	Description	Additional Information
Data Disk Size	`DGAppdataDisk`	Size in GB of a second data disk. The minimum size is 24GB.	
Passphrases			
dg-admin Passphrase*	`dg-adminPassword`	The password you have chosen for the dg-admin user. Password must be 8-64 characters.	
dg-oper Passphrase*	`dg-operPassword`	The password you have chosen for the dg-oper user. Password must be 8-64 characters.	
Interfaces **Note** You must select either an IPv4 or IPv6 address. Selecting **None** in the vNIC IPv4 Method and the vNICx IPv6 Method fields will result in a non-functional deployment.			
vNIC IPv4 Address (vNIC0, vNIC1 and vNIC2 based on the number of interfaces you choose to use)			

Name	Parameter	Description	Additional Information

vNIC IPv4 Method*	`Vnic0IPv4Method`
	`Vnic1IPv4Method`
	`Vnic2IPv4Method`
		None or **Static** or **DHCP**.
		The default value for **Method** is **None**.
			If you have selected **Method** as:
			• **None**: Skip the rest of the fields for IPv4 address. Enter information in the vNIC IPv6 Address parameters.
			• **Static**: Enter information in **Address**, **Netmask**, **Skip Gateway**, and **Gateway** fields
			• **DHCP**: Leave all the Vnic IPv4 Address parameters to their default values. These values are assigned automatically.

vNIC IPv4 Address	`Vnic0IPv4Address` `Vnic0IPv4Address` `Vnic0IPv4Address`	IPv4 address of the interface.	
vNIC IPv4 Netmask	`Vnic0IPv4Netmask` `Vnic0IPv4Netmask` `Vnic0IPv4Netmask`	IPv4 netmask of the interface in dotted quad format.	

vNIC IPv4 Skip Gateway	`Vnic0IPv4SkipGateway`
	`Vnic1IPv4SkipGateway`
	`Vnic2IPv4SkipGateway`
		Options are `True` or `False`.
		The default value is `False`.
		Selecting `True` skips configuring a gateway for the interface.	

vNIC IPv4 Gateway	`Vnic0IPv4Gateway`
	`Vnic1IPv4Gateway`
	`Vnic2IPv4Gateway`
		IPv4 address of the interface gateway.	

vNIC IPv6 Address (vNIC0, vNIC1, and vNIC2 based on the number of interfaces you choose to use)			

Name	Parameter	Description	Additional Information

vNIC IPv6 Method*	`Vnic0IPv6Method`
	`Vnic1IPv6Method`
	`Vnic2IPv6Method`
		None or **Static** or **DHCP**.
		The default value for **Method** is **None**.
			If you have selected **Method** as:
			• **None**: Skip the rest of the fields for IPv6 address. Enter information in the vNIC IPv4 Address parameters.
			• **Static**: Enter information in **Address**, **Netmask**, **Skip Gateway**, and **Gateway** fields
			• **DHCP**: Leave all the Vnicx IPv6 Address parameters as is to their default values. These value are assigned automatically.

vNIC IPv6 Address	`Vnic0IPv6Address`
	`Vnic1IPv6Address`
	`Vnic2IPv6Address`
		IPv6 address of the interface.	

vNIC IPv6 Netmask	`Vnic0IPv6Netmask`
	`Vnic1IPv6Netmask`
	`Vnic2IPv6Netmask`
		IPv6 prefix of the interface.	

vNIC IPv6 Skip Gateway	`Vnic0IPv6SkipGateway`
	`Vnic1IPv6SkipGateway`
	`Vnic2IPv6SkipGateway`
		Options are `True` or `False`.
		The default value is `False`.
		Selecting `True` skips configuring a gateway for the interface.	

vNIC IPv6 Gateway	`Vnic0IPv6Gateway`
	`Vnic1IPv6Gateway`
	`Vnic2IPv6Gateway`
		IPv6 address of the interface gateway.	

DNS Servers			
DNS Address*	`DNS`	Space-delimited list of IPv4 or IPv6 addresses of the DNS server accessible from the management interface.	
DNS Search Domain*	`Domain`	DNS search domain	
DNS Security Extensions *	`DNSSEC`	Options are False, True, Allow-Downgrade. Select True to use DNS security extensions. By default, this parameter is False.	
DNS over TLS*	`DNSTLS`	Options are False, True, and Opportunistic. Select True to use DNS over TLS. By default, this parameter is False.	

Name	Parameter	Description	Additional Information
Multicast DNS*	`mDNS`	Options are False, True and Resolve. Select True to use multicast DNS. By default, this parameter is False.	
Link-Local Multicast Name Resolution*	`LLMNR`	Options are False, True, Opportunistic and Resolve. Select True to use link-local multicast name resolution. By default, this parameter is False.	
NTPv4 Servers			
NTPv4 Servers*	`NTP`	NTPv4 server list. Enter space-delimited list of IPv4 or IPv6 addresses or hostnames of the NTPv4 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, Crosswork Cloud, and devices. Using a non-functional or dummy address may cause issues when Crosswork Cloud and Cisco Crosswork Data Gateway try to communicate with each other.
Use NTPv4 Authentication	`NTPAuth`	Select Yes to use NTPv4 authentication. The default value is No.	
NTPv4 Keys	`NTPKey`	Key IDs to map to the server list. Enter space-delimited list of Key IDs.	
NTPv4 Key File URI	`NTPKeyFile`	SCP URI to the chrony key file.	
NTPv4 Key File Passphrase	`NTPKeyFilePwd`	Password of SCP URI to the chrony key file.	
Remote Syslog Server			

Name	Parameter	Description	Additional Information
Use Remote Syslog Server*	`UseRemoteSyslog`	Select Yes to send syslog messages to a remote host. The default value is No.	Configuring an external syslog server sends service events to the external syslog server. Otherwise, they are logged only to the Cisco Crosswork Data Gateway VM. If you want to use an external syslog server, you must specify the following settings: • Use Remote Syslog Server • Syslog Server Address • Syslog Server Port • Syslog Server Protocol **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 Server Address	`SyslogAddress`	IPv4 or IPv6 address of a syslog server accessible from the management interface. **Note** If you are using an IPv6 address, surround it with square brackets ([1::1]).	
Syslog Server Port	`SyslogPort`	Port number of the optional syslog server. The port value can range between 1 and 65535. By default, this value is set to 514.	
Syslog Server Protocol	`SyslogProtocol`	Use UDP or TCP when sending syslog. Default value is UDP.	
Use Syslog over TLS?	`SyslogTLS`	Select Yes to use TLS to encrypt syslog traffic. By default, this parameter is set to No.	
Syslog TLS Peer Name	`SyslogPeerName`	The syslog server hostname exactly as entered in the server certificate SubjectAltName or subject common name.	
Syslog Root Certificate File URI	`SyslogCertChain`	URI to the PEM formatted root cert of syslog server retrieved using SCP.	
Syslog Certificate File Passphrase	`SyslogCertChainPwd`	Password of SCP user to retrieve Syslog certificate chain.	
Remote Auditd Server			

Name	Parameter	Description	Additional Information
Use Remote Auditd Server*	`UseRemoteAuditd`	Select Yes to send Auditd message to a remote host	Configure the Crosswork Data Gateway VM to send auditd messages to a remote server. Specify these three settings to forward auditd messages to an external Auditd server.
Auditd Server Address	`AuditdAddress`	Hostname, IPv4, or IPv6 address of an optional Auditd server	
Auditd Server Port	`AuditdPort`	Port number of an optional Auditd server.	
Controller and Proxy Settings			
Proxy Server URL	`ProxyURL`	URL of an optional management network proxy server.	In Cloud deployment, Cisco Crosswork Data Gateway must connect to the Internet via TLS. If you use a proxy server, specify these parameters.
Proxy Server Bypass List	`ProxyBypass`	Comma separated list of addresses and hostnames that will not use the proxy	
Authenticated Proxy Username	`ProxyUsername`	Username for authenticated proxy servers.	
Authenticated Proxy Passphrase	`ProxyPassphrase`	Passphrase for authenticated proxy servers.	
HTTPS Proxy SSL/TLS Certificate File URI	`ProxyCertChain`	HTTPS proxy PEM formatted SSL/TLS certificate file retrieved using SCP.	
HTTPS Proxy SSL/TLS Certificate File Passphrase	`ProxyCertChainPwd`	Password of SCP user to retrieve proxy certificate chain.	
Auto Enrollment Package Transfer			

Name	Parameter	Description	Additional Information
Enrollment Destination Host and Path**	`EnrollmentURI`	SCP host and path to transfer the enrollment package using SCP (`user@host:/path/to/file`).	Cisco Crosswork Data Gateway requires the Enrollment package to enroll with Crosswork Cloud. If you specify these parameters during the installation, the enrollment package is automatically transferred to the local host once Cisco Crosswork Data Gateway boots up for the first time. If you do not specify these parameters during installation, then export enrollment package manually by following the procedure Export Enrollment Package, on page 44.
Enrollment Passphrase**	`EnrollmentPassphrase`	SCP user passphrase to transfer enrollment package.	

What do next: Proceed to installing the Cisco Crosswork Data Gateway VM.

Install Crosswork Data Gateway Using vCenter vSphere Client

Follow these steps to install Crosswork Data Gateway using vCenter vSphere Client:

Step 1 Refer to the *Crosswork Data Gateway 4.0.1 Release notes* and download the Crosswork Data Gateway image (*.ova) file.

Note When using the latest Mozilla Firefox version to download the .ova image, if the downloaded file has the extension as .dms, change the extension back to .ova before installation.

Step 2 Connect to vCenter and login with your credentials.

Step 3 Select the data center where you want to deploy the Crosswork Data Gateway VM.

Step 4 Connect to vCenter vSphere Client. Then select **Actions** > **Deploy OVF Template**.

Warning The default VMware vCenter deployment timeout is 15 minutes. If the time taken to complete the OVF template deployment exceeds 15 minutes, vCenter times out and you will have to start over again. To prevent this, we recommend that you plan what you will enter by reviewing the template before you start the deployment.

Connect to vCenter and login with your credentials

Step 5 The VMware **Deploy OVF Template** wizard appears and highlights the first step, **1 Select template**.

a) Select **Local File** and then click **Browse** to navigate to the location where you downloaded the OVA image file and select it.

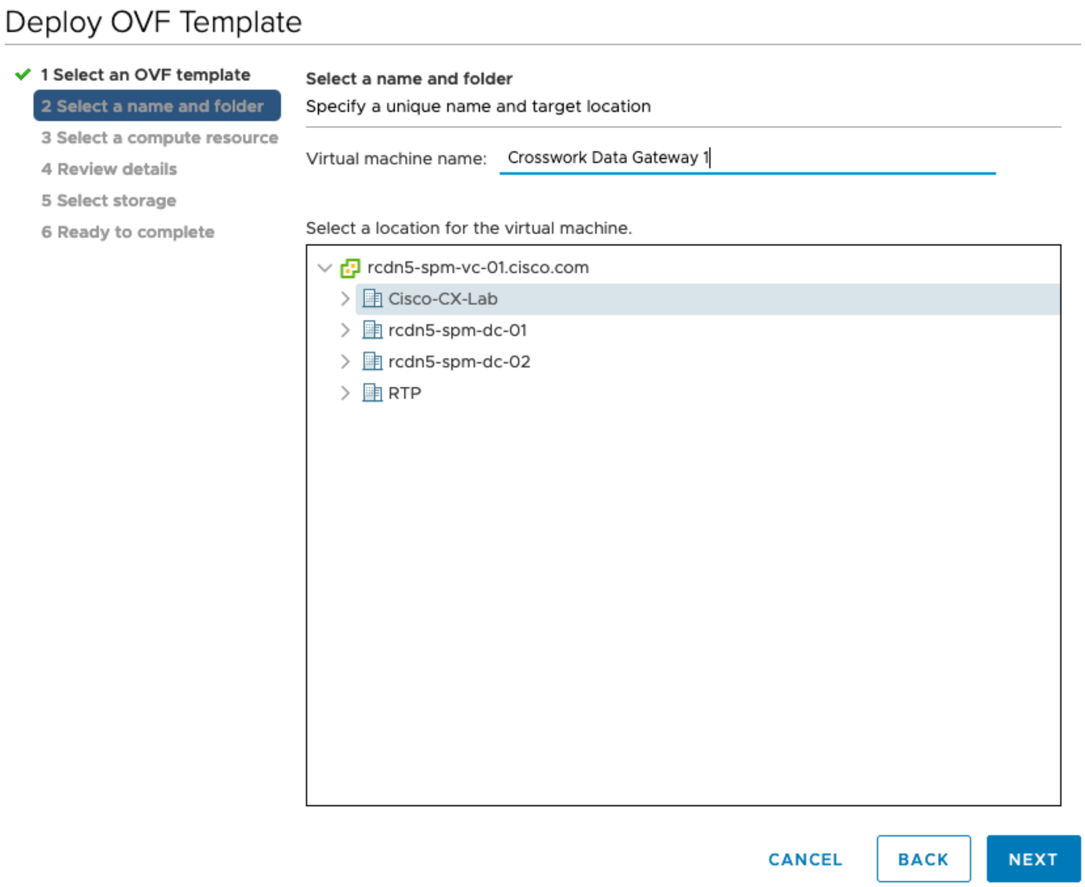
The filename is displayed in the window.

Step 6 Click **Next** to go to **2 Select name and folder**, as shown in the following figure.

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

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

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



Deploy OVF Template

Select a name and folder

Specify a unique name and target location

Virtual machine name: Crosswork Data Gateway 1

Select a location for the virtual machine.

- rcdn5-spm-vc-01.cisco.com
  - Cisco-CX-Lab
  - rcdn5-spm-dc-01
  - rcdn5-spm-dc-02
  - RTP

✓ 1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete
CANCEL
BACK
NEXT

Step 7 Click **Next** to go to **3 Select a compute resource**. Choose the VM's host.

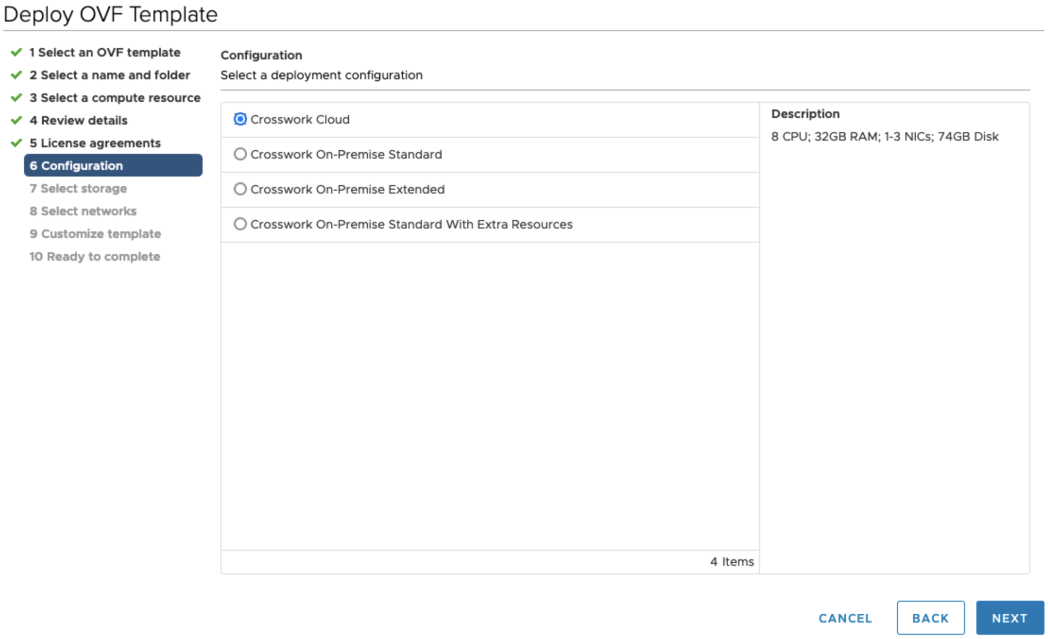
Step 8 Click **Next**. The VMware vCenter Server validates the OVA. The network speed determines how long the validation takes. When the validation is complete, the wizard moves to **4 Review details**. Review the OVA's information and then click **Next**.

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

Note This information is gathered from the OVF and cannot be modified. The template reports disk requirements for an on-premise deployment. This can be ignored as you will select the correct disk configuration in the next step.

Step 9 Click **Next** to go to **5 License agreements**. Review the End User License Agreement and click **Accept**.

Step 10 Click **Next** to go to **6 Configuration**, as shown in the following figure. Select **Crosswork Cloud**.



Deploy OVF Template

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

Configuration
Select a deployment configuration

● Crosswork Cloud
○ Crosswork On-Premise Standard
○ Crosswork On-Premise Extended
○ Crosswork On-Premise Standard With Extra Resources

4 Items

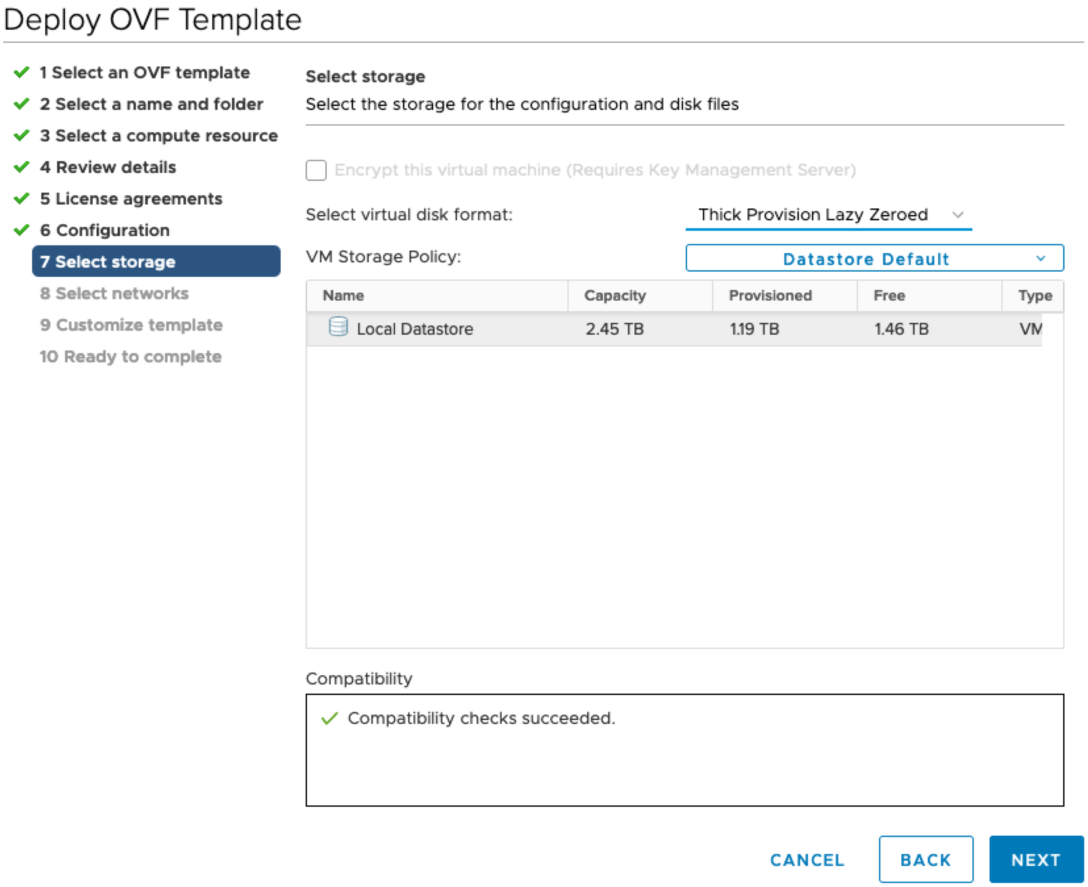
Description
8 CPU; 32GB RAM; 1-3 NICs; 74GB Disk

Step 11 Click **Next** to go to **7 Select storage**, as shown in the following figure.

a) In the **Select virtual disk format** field,

- For production environment, choose **Thick Provision Lazy Zeroed**.
- For development environment, choose **Thin Provision**.

b) From the **Datastores** table, choose the datastore you want to use.



Deploy OVF Template

Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thick Provision Lazy Zeroed

VM Storage Policy: Datastore Default

Name	Capacity	Provisioned	Free	Type
Local Datastore	2.45 TB	1.19 TB	1.46 TB	VM

Compatibility

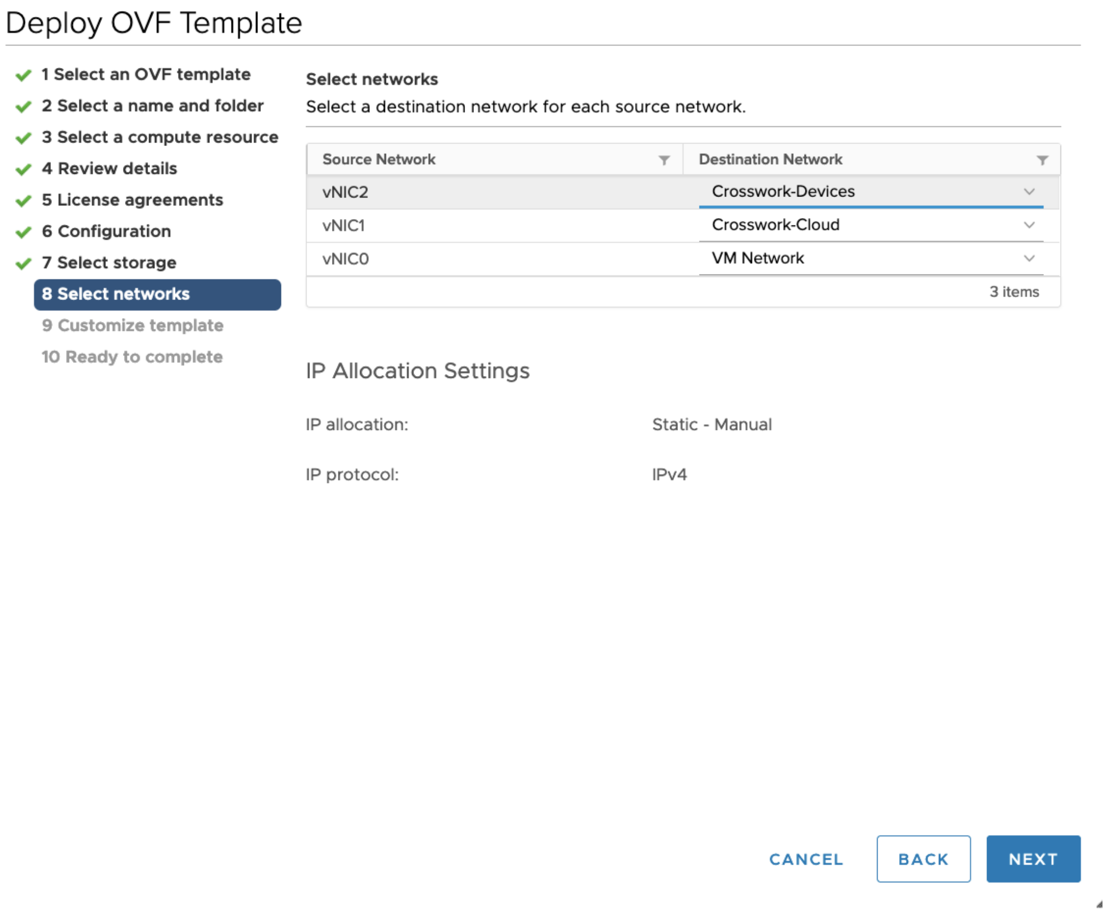
✓ Compatibility checks succeeded.

Step 12 Click **Next** to go to **8 Select networks**, as shown in the following figure. In the drop-down table at the top of the page, choose the appropriate destination network for each source network based on the number of vNICs you plan to use.

Start with **vNIC0** and select a destination network that will be used. Leave unused **vNICs** set to the default value.

Note In the following image,

- **VM Network** is the management network for accessing the Interactive Console and troubleshooting the Crosswork Data Gateway VM.
- **Crosswork-Cloud** is the controller network where the Crosswork Data Gateway connects to Crosswork Cloud.
- **Crosswork-Devices** is the network for device access traffic.



Deploy OVF Template

Select networks

Select a destination network for each source network.

Source Network	Destination Network
vNIC2	Crosswork-Devices
vNIC1	Crosswork-Cloud
vNIC0	VM Network

3 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

Step 13 Click **Next** to go to **9 Customize template**, with the **Host Information Settings** already expanded.

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

Enter the information for the parameters as described in Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2.

Note When this menu is first displayed, there will be an error "7 properties have invalid values". This is normal and will clear as you enter appropriate values.

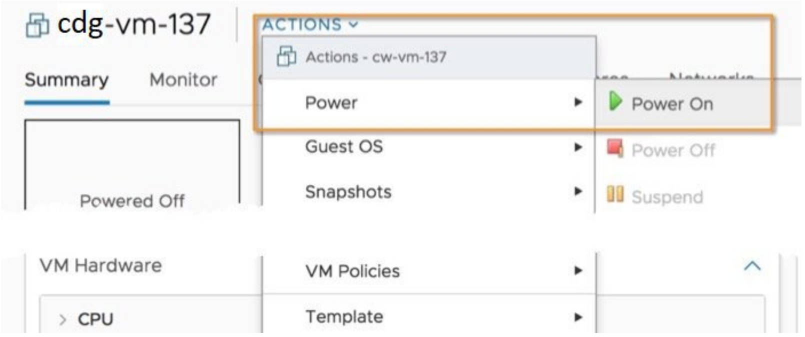
Step 14 Click **Next** to go to **10 Ready to complete**. Review your settings and then click **Finish** if you are ready to begin deployment.

Step 15 Check 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.

Step 16 After the deployment status becomes 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 five minutes for the VM to come up and then login through vCenter or SSH.

Warning Changing the VM's network settings in vCenter may have significant unintended consequences, including but not limited to the loss of static routes and connectivity. Make any changes to these settings at your own risk. If you wish to change the IP address, destroy the current VM, create a new VM, and re-enroll the new one on the Crosswork Cloud.

Verify that the installation was successful.

1. Login to Crosswork Data Gateway VM Via vCenter:

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

2. Access Crosswork Data Gateway VM Via SSH:

1. From your work station with network access to the Cisco Crosswork Data Gateway management IP, run the following command:

   ssh <username>@<ManagementNetworkIP>

   where **ManagementNetworkIP** is the management network IP address in an IPv4 or IPv6 address format.

   For example,

   To log in as an administrator user: **ssh dg-admin@<ManagementNetworkIP>**

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

   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.

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

If you are unable to access the Cisco Crosswork Data Gateway VM, there is an issue with your network configuration settings. From the VMware console, check the network settings. If they are incorrect, it is best to delete the Cisco Crosswork Data Gateway VM and re-install with the correct network settings.

What to do next

Proceed to enrolling the Crosswork Data Gateway with Crosswork Cloud by generating and exporting the enrollment package. See Export Enrollment Package, on page 44.

Install Crosswork Data Gateway Via OVF Tool

You can modify mandatory/optional parameters in the command/script as per your requirement and run the OVF Tool. See Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2 .

Below is a sample script if you are planning to run the OVF tool with a script. The sample that follows creates a Crosswork Data Gateway VM with the hostname of "dg-141" using two network interfaces.

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

# robot.ova path

DG_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 \
--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" $DG_OVA_PATH "vi://$VCENTER_LOGIN/$VCENTER_PATH"
```

Step 1 Open a command prompt on the machine you will running the install from.

Step 2 Open the template file and edit it to match the settings you chose for the Cisco Crosswork Data Gateway.

Step 3 Navigate to the location where you installed the OVF Tool.

Step 4 Run the OVF Tool using the script.

```
root@cxcloudctrl:/opt# ./<script_file>
```

For example,

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

Verify that the installation was successful.

1. Login to Crossworks Data Gateway VM Via vCenter:

1. Locate the VM in vCenter and then right click and select **Open Console**.
2. Enter username (`dg-admin`) and the corresponding password (the one that you created during installation process) and press **Enter**.

2. Access Crosswork Data Gateway VM Via SSH:

1. From your work station with network access to the Cisco Crosswork Data Gateway management IP, run the following command:

   ssh <username>@<ManagementNetworkIP>

   where **ManagementNetworkIP** is the management network IP address in an IPv4 or IPv6 address format.

   For example,

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

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

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

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.

If you are unable to access the Cisco Crosswork Data Gateway VM, there is an issue with your network configuration settings. From the VMware console check the network settings. If they are incorrect, it is best to delete the Cisco Crosswork Data Gateway VM and re-install with the correct network settings.

What to do next

Proceed to enrolling the Crosswork Data Gateway with Crosswork Cloud. See Export Enrollment Package, on page 44.

Install Crosswork Data Gateway on OpenStack from OpenStack CLI

This section provides details of the procedure to install Crosswork Data Gateway on the OpenStack platform.

Note

1. This procedure lists commands to create networks, ports and volumes in the OpenStack environment. Please note that there are multiple ways to do this.
2. All IP addresses mentioned here are sample IP addresses mentioned for the purpose of documentation.

Before you begin

Ensure you have the following information ready:

- Number of Crosswork Data Gateway VM instances to install.
- Plan your installation. Refer to the section Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2.

- Decide the addressing method that you will use (DHCP or Static) for the VM(s).
- Have network information such as IP addresses, subnets, and ports ready for each VM if you are using Static addressing.
- Understand security group rules and policies before you create and use them.

Step 1 **Download and validate the Cisco Crosswork Data Gateway `qcow2` package:**

a) Download the latest available Cisco Crosswork Data Gateway image (*.bios.signed.bin) from cisco.com to your local machine or a location on your local network that is accessible to your OpenStack. For the purpose of these instructions, we will use the package name **"cw-na-dg-4.0.1-65-release-20221130.bios.signed.bin"**.

b) Extract the content of the bin file to the current directory by running the following command.

```
sh cw-na-dg-4.0.1-65-release-20221130.bios.signed.bin
```

This command verifies the authenticity of the product. The directory contains the following files as shown here:

```
CDG-CCO_RELEASE.cer
cisco_x509_verify_release.py3
cw-na-dg-4.0.1-65-release-20221130.bios.tar.gz
README
cisco_x509_verify_release.py
cw-na-dg-4.0.1-65-release-20221130.bios.signed.bin
cw-na-dg-4.0.1-65-release-20221130.bios.tar.gz.signature
```

c) Use the following command to verify the signature of the build:

Note The machine where the script is being run needs HTTP access to cisco.com. Please contact Cisco Customer Experience team if access to cisco.com is not possible due to security restrictions, or if you did not get a successful verification message after running the script.

If you are using python 2.x, use the following command to validate the file:

```
python cisco_x509_verify_release.py -e <.cer file> -i <.tar.gz file> -s <.tar.gz.signature file>
 -v dgst -sha512
```

If you are using python 3.x, use the following command to validate the file:

```
python cisco_x509_verify_release.py3 -e <.cer file> -i <.tar.gz file> -s <.tar.gz.signature file>
 -v dgst -sha512
```

d) Unzip the QCOW2 file (**cw-na-dg-4.0.1-65-release-20221130.bios.tar.gz**) with the following command:

```
tar -xvf cw-na-dg-4.0.1-65-release-20221130.uefi.tar.gz
```

This creates a new directory that contains the `config.txt` file.

Step 2 Complete the steps in Step 3 **OR** Step 4 based on the type of addressing you will be using for the Crosswork Data Gateway VM.

Step 3 **Update the `config.txt` for a Crosswork Data Gateway VM with Static addressing.**

a) Navigate to the directory where you have downloaded the Crosswork Data Gateway release image.

b) Open the `config.txt` file and modify the parameters as per your installation requirements. Refer to the section Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2 for more information.

This is a sample `config.txt` file for a 3-NIC deployment with the host name as `cdg1-nodhcp` when using static addressing. Mandatory parameters in this list have been highlighted.

Note For a single NIC deployment or two NICs deployment, the `config.txt` will have the `ActiveVnics` parameter as 1 or 2 respectively.

```
ActiveVnics=3
AllowRFC8190=Yes
AuditdAddress=
AuditdPort=60
ControllerCertChainPwd=
ControllerIP=crosswork.cisco.com
ControllerPort=443
ControllerSignCertChain=
ControllerTlsCertChain=
Deployment=Cloud
Description=<Description of the VM>
DGAppdataDisk=10
DGCertChain=
DGCertChainPwd=
DGCertKey=
DNS=<DNS server IP address>
DNSSEC=False
DNSTLS=False
Domain=<Domain name>
EnrollmentPassphrase=
EnrollmentURI=
Hostname=<Hostname of VM>
Label=
LLMNR=False
mDNS=False
NTP=<NTP server IP address>
NTPAuth=False
NTPKey=
NTPKeyFile=
NTPKeyFilePwd=
Profile=Standard
ProxyBypass=
ProxyCertChain=
ProxyCertChainPwd=
ProxyPassphrase=
ProxyURL=
ProxyUsername=
SyslogAddress=
SyslogCertChain=
SyslogCertChainPwd=
SyslogPeerName=
SyslogPort=514
SyslogProtocol=UDP
SyslogTLS=False
UseRemoteAuditd=False
UseRemoteSyslog=False
Vnic0IPv4Address=10.10.11.101 //Same IP address needs to be entered when creating ports of the
VM.
Vnic0IPv4Gateway=10.10.11.1
Vnic0IPv4Method=Static
Vnic0IPv4Netmask=255.255.255.0
Vnic0IPv4SkipGateway=False
Vnic0IPv6Address=::0
Vnic0IPv6Gateway=::1
Vnic0IPv6Method=None
Vnic0IPv6Netmask=64
Vnic0IPv6SkipGateway=False
```

```
Vnic1IPv4Address=10.10.21.101 // Same IP address needs to be entered when creating ports of the
VM.
Vnic1IPv4Gateway=10.10.21.1
Vnic1IPv4Method=Static
Vnic1IPv4Netmask=255.255.255.0
Vnic1IPv4SkipGateway=False
Vnic1IPv6Address=::0
Vnic1IPv6Gateway=::1
Vnic1IPv6Method=None
Vnic1IPv6Netmask=64
Vnic1IPv6SkipGateway=False
Vnic2IPv4Address=10.10.31.101 //Same IP address needs to be entered when creating ports of the
VM.
Vnic2IPv4Gateway=10.10.31.1
Vnic2IPv4Method=Static
Vnic2IPv4Netmask=255.255.255.0
Vnic2IPv4SkipGateway=False
Vnic2IPv6Address=::0
Vnic2IPv6Gateway=::1
Vnic2IPv6Method=None
Vnic2IPv6Netmask=64
Vnic2IPv6SkipGateway=False
dg-adminPassword=<Admin user password>
dg-operPassword=<Operator user password>
```

c) Save the `config.txt` file with the hostname of the VM or a name that makes it easy for you to identify the VM for which you have updated it.

d) **(Important)** Make a note of the IP address that you enter here for the vNIC IP addresses in the `config.text`. You will need to specifiy the same IP addresses when creating the ports for the VM in Step 9.

e) Repeat **Step 3 (b)** and **Step 3 (d)** to update and save a unique config.txt file for each VM using static addressing.

f) Proceed to **Step 5**.

Step 4 **Update the `config.txt` for Crosswork Data Gateway VMs using DHCP.**

a) Navigate to the directory where you have downloaded the Crosswork Data Gateway release image.

b) Open the `config.txt` file and modify the parameters as per your installation requirements. Refer to the section Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2 for more information.

This is a sample `config.txt` file for a 3-NIC deployment with the host name as `cdg1-nodhcp` when using DHCP. Mandatory parameters in this list have been highlighted.

Note For a single NIC deployment or two NICs deployment, the `config.txt` will have the `ActiveVnics` parameter as 1 or 2 respectively.

```
ActiveVnics=3
AllowRFC8190=Yes
AuditdAddress=
AuditdPort=60
ControllerCertChainPwd=
ControllerIP=crosswork.cisco.com
ControllerPort=443
ControllerSignCertChain=
ControllerTlsCertChain=
Deployment=Cloud
Description=<Description of the VM>
DGAppdataDisk=10
DGCertChain=
DGCertChainPwd=
DGCertKey=
DNS=<DNS server IP address>
DNSSEC=False
DNSTLS=False
```

```
Domain=<Domain name>
EnrollmentPassphrase=
EnrollmentURI=
Hostname=cdg1-nodhcp
Label=
LLMNR=False
mDNS=False
NTP=<NTP server IP address>
NTPAuth=False
NTPKey=
NTPKeyFile=
NTPKeyFilePwd=
Profile=Standard
ProxyBypass=
ProxyCertChain=
ProxyCertChainPwd=
ProxyPassphrase=
ProxyURL=
ProxyUsername=
SyslogAddress=
SyslogCertChain=
SyslogCertChainPwd=
SyslogPeerName=
SyslogPort=514
SyslogProtocol=UDP
SyslogTLS=False
UseRemoteAuditd=False
UseRemoteSyslog=False
Vnic0IPv4Address=0.0.0.0 //Leave the default value unchanged
Vnic0IPv4Gateway=0.0.0.1
Vnic0IPv4Method=DHCP
Vnic0IPv4Netmask=0.0.0.0
Vnic0IPv4SkipGateway=False
Vnic0IPv6Address=::0
Vnic0IPv6Gateway=::1
Vnic0IPv6Method=None
Vnic0IPv6Netmask=64
Vnic0IPv6SkipGateway=False
Vnic1IPv4Address=0.0.0.0 //Leave the default value unchanged
Vnic1IPv4Gateway=0.0.0.1
Vnic1IPv4Method=DHCP
Vnic1IPv4Netmask=0.0.0.0
Vnic1IPv4SkipGateway=False
Vnic1IPv6Address=::0
Vnic1IPv6Gateway=::1
Vnic1IPv6Method=None
Vnic1IPv6Netmask=64
Vnic1IPv6SkipGateway=False
Vnic2IPv4Address=0.0.0.0 //Leave the default value unchanged
Vnic2IPv4Gateway=0.0.0.1
Vnic2IPv4Method=DHCP
Vnic2IPv4Netmask=0.0.0.0
Vnic2IPv4SkipGateway=False
Vnic2IPv6Address=::0
Vnic2IPv6Gateway=::1
Vnic2IPv6Method=None
Vnic2IPv6Netmask=64
Vnic2IPv6SkipGateway=False
dg-adminPassword=<Administrator user password>
dg-operPassword=<Operator user password>
```

c) Save the `config.txt` file with the hostname of the VM or a name that makes it easy for you to identify the VM for which you have updated it.

d) Repeat **Step 4 (b)** and **Step 4 (c)** to update and save a unique config.txt file for each VM using DHCP addressing.

e) Proceed to **Step 5**.

Step 5 Log in to the OpenStack VM from CLI.

Step 6 **Create the resource profile or flavor for the VMs.**

```
openstack flavor create --public --id auto --vcpus 8 --ram 32768 --disk 74 cdg-cloud
```

Step 7 **Create image for OpenStack install.**

```
openstack image create --public --disk-format qcow2 --container-format bare --file
<bios_release_image_file> <image_name>
```

For example:

```
openstack image create --public --disk-format qcow2 --container-format bare --file
cw-na-dg-4.0.1-65-release-20221130.bios.qcow2 cdg-cloud-bios
```

Step 8 **Create the VM-specific parameters for each Crosswork Data Gateway VM.**

Create the following parameters for each Crosswork Data Gateway VM instance that you want to install.

a) **(Optional) Create a 10 GB second data disk.**

```
openstack  volume create --size <volume_size> <volume_name>
```

Sample commands:

```
openstack volume create --size 10 cdg-vol1
```

b) **Create a security policy to allow incoming TCP/UDP/ICMP connections.**

OpenStack does not allow incoming TCP/UDP/ICMP connections by default. Create a security policy to allow incoming connections from TCP/UDP/ICMP protocols.

```
openstack security group create open
openstack security group rule create open --protocol tcp --dst-port <port_number> --remote-ip
<IP_address>
openstack security group rule create open --protocol udp --dst-port <port_number> --remote-ip
<IP_address>
openstack security group rule create --protocol icmp open
```

c) **Create ports with specified IP address ONLY for Crosswork Data VMs using Static addressing.**

Important This step is required only if you are using Static addressing. If you are using DHCP addressing, the IP addresses for the ports are automatically assigned from the IP addresses allocation pool for the subnet.

```
openstack port create --network network_name --fixed-ip
subnet=subnet_name,ip-address=port_ip_address port_name
```

Sample commands to create ports for CDG VMs with 3 NICs using static addressing:

```
openstack port create --network network1 --fixed-ip subnet=subnet1,ip-address=10.10.11.101
mgmt-port1
openstack port create --network network2 --fixed-ip subnet=subnet2,ip-address=10.10.21.101
north-port1
openstack port create --network network3 --fixed-ip subnet=subnet3,ip-address=10.10.31.101
south-port1
```

In the previous command, `network1` is the management network in your environment, `subnet1` is the subnet on the management network, `mgmt-port1` is the port that we are creating with the IP address as `10.10.11.101` for vNIC0 as specified in the `config.txt` file for the VM.

d) **Apply the security policy to the ports.**

```
openstack port set <port_name> --security-group open
```

For example,

```
openstack port set mgmt-port1 --security-group open
openstack port set north-port1 --security-group open
openstack port set south-port1 --security-group open
```

e) Repeat Step **9** for all the VMs you will be installing.

Step 9 **Install the Crosswork Data Gateway VM(s).**

Commands to install Crosswork Data Gateway VM with 3 NICs that use static addressing

```
openstack server create --flavor <flavor_name> --image <image_name> --port <mgmt-port> --port
<north-port> --port <south-port> --config-drive True --user-data <config.txt> --block-device-mapping
 vdb=<volume_name>:::true <CDG_hostname>
```

For example:

```
openstack server create --flavor  cdg-cloud --image cdg-cloud-bios --port mgmt-port1 --port north-port1
 --port south-port1 --config-drive True --user-data config-nodhcp-cdg1.txt --block-device-mapping
vdb=cdg1:::true cdg1-nodhcp
```

OR

```
openstack server create --config-drive true --flavor cdg --image <image_name> --key-name default
--nic net-id=<network id>,v4-fixed-ip=<CDG static IP> --security-group <security group name> --user-data
 <config.txt> <CDG_hostname>
```

Commands to install Crosswork Data Gateway VM with 3 NICs with DHCP

```
openstack server create --flavor <flavor_name> --image <image_name> --network <network1> --network
<network2> --network <network3> --config-drive True --user-data <config.txt> --host <boot_drive>
--block-device-mapping vdb=<volume_name>:::true <CDG_hostname>
```

For example:

```
openstack server create --flavor cdg-cloud --image cdg-cloud-bios --network network1 --network network2
 --network network3 --config-drive True --user-data config-dhcp-cdg1.txt --block-device-mapping
vdb=cdg1:::true cdg1-dhcp
```

OR

```
openstack server create --config-drive true --flavor cdg --image <image_name> --key-name default
--network <network with dhcp> --security-group <security group name> --user-data <config.txt>
<CDG_name>
```

Note The number of networks in the command to install the VMs will depend on the number of NICs in the deployment.

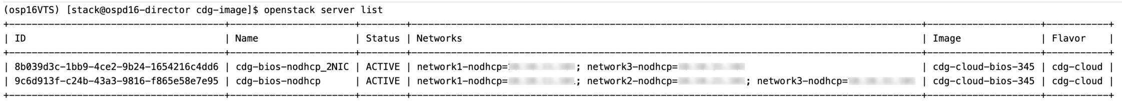
For example, the command to install a VM with 2 NICs is:

```
openstack server create --flavor cdg-cloud --image cdg-cloud-bios --port mgmt-port2 --port
south-port2 --config-drive True --user-data config-nodhcp_2nic.txt --block-device-mapping
vdb=cdg-vol:::true cdg-bios-nodhcp_2NIC
```

Verify that the Crosswork Data Gateway VMs were installed successfully.

Run the following command to view the status of the installation of the VMs.

```
openstack server list
```



```
(osp16VTS) [stack@ospd16-director cdg-image]$ openstack server list
+--------------------------------------+----------------------+--------+---------------------------------------------------------------------------------------------------------------+--------------------+-----------+
| ID                                   | Name                 | Status | Networks                                                                                                      | Image              | Flavor    |
+--------------------------------------+----------------------+--------+---------------------------------------------------------------------------------------------------------------+--------------------+-----------+
| 8b039d3c-1bb9-4ce2-9b24-1654216c4dd6 | cdg-bios-nodhcp_2NIC | ACTIVE | network1-nodhcp=[redacted]; network3-nodhcp=[redacted]                                                        | cdg-cloud-bios-345 | cdg-cloud |
| 9c6d913f-c24b-43a3-9816-f865e58e7e95 | cdg-bios-nodhcp      | ACTIVE | network1-nodhcp=[redacted]; network2-nodhcp=[redacted]; network3-nodhcp=[redacted]                            | cdg-cloud-bios-345 | cdg-cloud |
+--------------------------------------+----------------------+--------+---------------------------------------------------------------------------------------------------------------+--------------------+-----------+
```

After the status of the VMs is displayed as **Active**, wait for about 10 minutes and check if the VM was deployed properly and running as expected either from the CLI or the OpenStack UI.

From OpenStack CLI

1. Run the following command in the OpenStack CLI to fetch the URL of the VM instance.

   ```
   openstack console url show <CDG hostname>
   ```

   For example:

   ```
   openstack console url show cdg-dhcp
   ```
2. Log in as the dg-admin or dg-oper user (as per the role assigned to you) and the corresponding password you had entered in the `config.txt` file of the VM. The Crosswork Data Gateway Interactive console is displayed after you login successfully.

From OpenStack UI

1. Log in to the OpenStack UI.
2. Navigate to **Compute** > **Instances**.
3. Click the Crosswork Data Gateway VM name. The link to the VM console opens in a new tab.
4. Log in as the dg-admin or dg-oper user (as per the role assigned to you) and the corresponding password you had entered in the `config.txt` file of the VM. The Crosswork Data Gateway Interactive console is displayed after you log in successfully.

What to do next

Proceed to adding the Crosswork Data Gateway with Crosswork Cloud. See Export Enrollment Package, on page 44.

Install Crosswork Data Gateway on OpenStack from the OpenStack UI

This section provides details of the procedure to install Crosswork Data Gateway on the OpenStack platform.

Note All IP addresses mentioned here are sample IP addresses mentioned for the purpose of documentation.

Before you begin

Ensure you have the following information ready:

- Number of Crosswork Data Gateway VM instances to install.

- Plan your installation. Refer to the section Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2.
- Decide the addressing method that you will use (DHCP or Static) for the VM(s).
- Have network information such as IP addresses, subnets and ports ready for each VM if you are using Static addressing.
- Understand security group rules and security policies before you create security groups to apply to the VM.

Step 1 **Download and validate the Cisco Crosswork Data Gateway `qcow2` package:**

a) Download the latest available Cisco Crosswork Data Gateway image (*.bios.signed.bin) from cisco.com to your local machine or a location on your local network that is accessible to your OpenStack. For the purpose of these instructions, we will use the package name **"cw-na-dg-4.0.1-65-release-20221130.bios.signed.bin"**.

b) Extract the content of the bin file to the current directory.

```
sh cw-na-dg-4.0.1-65-release-20221130.bios.signed.bin
```

This command verifies the authenticity of the product. The directory contains the following files as shown here:

```
CDG-CCO_RELEASE.cer
cisco_x509_verify_release.py3
cw-na-dg-4.0.1-65-release-20221130.bios.tar.gz
README
cisco_x509_verify_release.py
cw-na-dg-4.0.1-65-release-20221130.bios.signed.bin
cw-na-dg-4.0.1-65-release-20221130.bios.tar.gz.signature
```

If you encounter any network connectivity issues, skip this verification and perform a manual verification as explained in the next step.

```
sh cw-na-dg-4.0.1-65-release-20221130.bios.signed.bin --skip-verification
```

c) Use the following command to verify the signature of the build:

Note The machine where the script is being run needs HTTP access to cisco.com. Please contact Cisco Customer Experience team if access to cisco.com is not possible due to security restrictions, or if you did not get a successful verification message after running the script.

If you are using python 2.x, use the following command to validate the file:

```
python cisco_x509_verify_release.py -e <.cer file> -i <.tar.gz file> -s <.tar.gz.signature file>
 -v dgst -sha512
```

If you are using python 3.x, use the following command to validate the file:

```
python cisco_x509_verify_release.py3 -e <.cer file> -i <.tar.gz file> -s <.tar.gz.signature
file> -v dgst -sha512
```

d) Unzip the QCOW2 file (**cw-na-dg-4.0.1-65-release-20221130.bios.tar.gz**) with the following command:

```
tar -xvf cw-na-dg-4.0.1-65-release-20221130.bios.tar.gz
```

This creates a new directory that contains the `config.txt` file.

Step 2 Complete the steps in Step 3 **OR** Step 4 based on the type of addressing you will be using for the Crosswork Data Gateway VM.

Step 3 **Update the `config.txt` for a Crosswork Data Gateway VM with Static addressing.**

a) Navigate to the directory where you have downloaded the Crosswork Data Gateway release image.

b) Open the `config.txt` file and modify the parameters as per your installation requirements. Refer to the section Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2 for more information.

Important Make a note of the IP address that you are using to create the ports for the VM. You will need to specify the same IP addresses that you enter here for the vNIC IP addresses in the `config.text` file for each of the VMs.

This is a sample `config.txt` file for a 3-NIC deployment with the host name as `cdg1-nodhcp` when using static addressing. Mandatory parameters in this list have been highlighted.

Note For a single NIC deployment or 2 NICs deployment, the `config.txt` will have the `ActiveVnics` parameter as 1 or 2 respectively.

```
ActiveVnics=3
AllowRFC8190=Yes
AuditdAddress=
AuditdPort=60
ControllerCertChainPwd=
ControllerIP=crosswork.cisco.com
ControllerPort=443
ControllerSignCertChain=
ControllerTlsCertChain=
Deployment=Cloud
Description=<Description of the VM>
DGAppdataDisk=10
DGCertChain=
DGCertChainPwd=
DGCertKey=
DNS=<DNS server IP address>
DNSSEC=False
DNSTLS=False
Domain=<Domain name>
EnrollmentPassphrase=
EnrollmentURI=
Hostname=<Hostname of VM>
Label=
LLMNR=False
mDNS=False
NTP=<NTP server IP address>
NTPAuth=False
NTPKey=
NTPKeyFile=
NTPKeyFilePwd=
Profile=Standard
ProxyBypass=
ProxyCertChain=
ProxyCertChainPwd=
ProxyPassphrase=
ProxyURL=
ProxyUsername=
SyslogAddress=
SyslogCertChain=
SyslogCertChainPwd=
SyslogPeerName=
SyslogPort=514
SyslogProtocol=UDP
SyslogTLS=False
```

```
UseRemoteAuditd=False
UseRemoteSyslog=False
Vnic0IPv4Address=10.10.11.101 //Same IP address needs to be entered when creating ports of the
 VM.
Vnic0IPv4Gateway=10.10.11.1
Vnic0IPv4Method=Static
Vnic0IPv4Netmask=255.255.255.0
Vnic0IPv4SkipGateway=False
Vnic0IPv6Address=::0
Vnic0IPv6Gateway=::1
Vnic0IPv6Method=None
Vnic0IPv6Netmask=64
Vnic0IPv6SkipGateway=False
Vnic1IPv4Address=10.10.21.101 // Same IP address needs to be entered when creating ports of the
 VM.
Vnic1IPv4Gateway=10.10.21.1
Vnic1IPv4Method=Static
Vnic1IPv4Netmask=255.255.255.0
Vnic1IPv4SkipGateway=False
Vnic1IPv6Address=::0
Vnic1IPv6Gateway=::1
Vnic1IPv6Method=None
Vnic1IPv6Netmask=64
Vnic1IPv6SkipGateway=False
Vnic2IPv4Address=10.10.31.101 //Same IP address needs to be entered when creating ports of the
 VM.
Vnic2IPv4Gateway=10.10.31.1
Vnic2IPv4Method=Static
Vnic2IPv4Netmask=255.255.255.0
Vnic2IPv4SkipGateway=False
Vnic2IPv6Address=::0
Vnic2IPv6Gateway=::1
Vnic2IPv6Method=None
Vnic2IPv6Netmask=64
Vnic2IPv6SkipGateway=False
dg-adminPassword=<Admin user password>
dg-operPassword=<Operator user password>
```

c) Save the `config.txt` file with the hostname of the VM or a name that makes it easy for you to identify the VM for which you have updated it.

d) **(Important)** Make a note of the IP address that you enter here for the vNIC IP addresses in the `config.txt`. You will need to specify the same IP addresses when creating the ports for the VM in Step 9.

e) Repeat **Step 3 (b)** and **Step 3 (d)** to update and save a unique `config.txt` file for each VM using static addressing.

f) Proceed to **Step 5**.

Step 4 **Update the `config.txt` for a Crosswork Data Gateway VM with DHCP.**

a) Navigate to the directory where you have downloaded the Crosswork Data Gateway release image.

b) Open the `config.txt` file and modify the parameters as per your installation requirements. Refer to the section Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2 for more information.

This is a sample `config.txt` file for a 3-NIC deployment with the host name as `cdg1-nodhcp` when using static addressing. Mandatory parameters in this list have been highlighted.

Note For a single NIC deployment or 2 NICs deployment, the `config.txt` will have the `ActiveVnics` parameter as 1 or 2 respectively.

```
ActiveVnics=3
AllowRFC8190=Yes
AuditdAddress=
AuditdPort=60
ControllerCertChainPwd=
ControllerIP=crosswork.cisco.com
ControllerPort=443
ControllerSignCertChain=
ControllerTlsCertChain=
Deployment=Cloud
Description=<Description of the VM>
DGAppdataDisk=10
DGCertChain=
DGCertChainPwd=
DGCertKey=
DNS=<DNS server IP address>
DNSSEC=False
DNSTLS=False
Domain=<Domain name>
EnrollmentPassphrase=
EnrollmentURI=
Hostname=cdg1-nodhcp
Label=
LLMNR=False
mDNS=False
NTP=<NTP server IP address>
NTPAuth=False
NTPKey=
NTPKeyFile=
NTPKeyFilePwd=
Profile=Standard
ProxyBypass=
ProxyCertChain=
ProxyCertChainPwd=
ProxyPassphrase=
ProxyURL=
ProxyUsername=
SyslogAddress=
SyslogCertChain=
SyslogCertChainPwd=
SyslogPeerName=
SyslogPort=514
SyslogProtocol=UDP
SyslogTLS=False
UseRemoteAuditd=False
UseRemoteSyslog=False
Vnic0IPv4Address=0.0.0.0 //Leave the default value unchanged
Vnic0IPv4Gateway=0.0.0.1
Vnic0IPv4Method=DHCP
Vnic0IPv4Netmask=0.0.0.0
Vnic0IPv4SkipGateway=False
Vnic0IPv6Address=::0
Vnic0IPv6Gateway=::1
Vnic0IPv6Method=None
Vnic0IPv6Netmask=64
Vnic0IPv6SkipGateway=False
Vnic1IPv4Address=0.0.0.0 //Leave the default value unchanged
Vnic1IPv4Gateway=0.0.0.1
Vnic1IPv4Method=DHCP
Vnic1IPv4Netmask=0.0.0.0
Vnic1IPv4SkipGateway=False
Vnic1IPv6Address=::0
Vnic1IPv6Gateway=::1
Vnic1IPv6Method=None
Vnic1IPv6Netmask=64
Vnic1IPv6SkipGateway=False
Vnic2IPv4Address=0.0.0.0 //Leave the default value unchanged
Vnic2IPv4Gateway=0.0.0.1
Vnic2IPv4Method=DHCP
```

```
Vnic2IPv4Netmask=0.0.0.0
Vnic2IPv4SkipGateway=False
Vnic2IPv6Address=::0
Vnic2IPv6Gateway=::1
Vnic2IPv6Method=None
Vnic2IPv6Netmask=64
Vnic2IPv6SkipGateway=False
dg-adminPassword=<Administrator user password>
dg-operPassword=<Operator user password>
```

c) Save the `config.txt` file with the hostname of the VM or a name that makes it easy for you to identify the VM for which you have updated it.

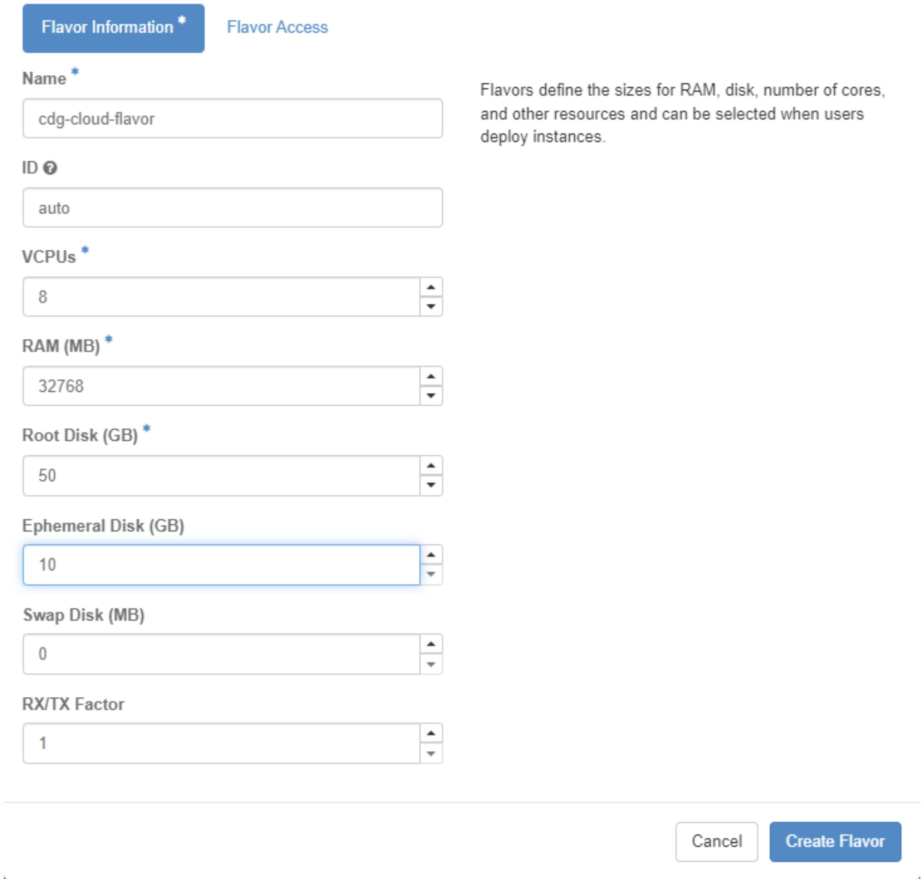
d) Repeat **Step 4 (b)** and **Step 4 (c)** to update and save a unique `config.txt` file for each VM using static addressing.

e) Proceed to **Step 5**.

Step 5 Log in to the OpenStack VM from the OpenStack UI.

Step 6 Navigate to **Compute** > **Flavors** to create the resource profile or flavor.

Enter details in the **Name**, **VCPUs**, **RAM**, **Root Disk** and **Ephemeral Disk** fields as shown in the following image and click **Create Flavor**.



Name *: cdg-cloud-flavor

Flavors define the sizes for RAM, disk, number of cores, and other resources and can be selected when users deploy instances.

ID: auto

VCPUs *: 8

RAM (MB) *: 32768

Root Disk (GB) *: 50

Ephemeral Disk (GB): 10

Swap Disk (MB): 0

RX/TX Factor: 1

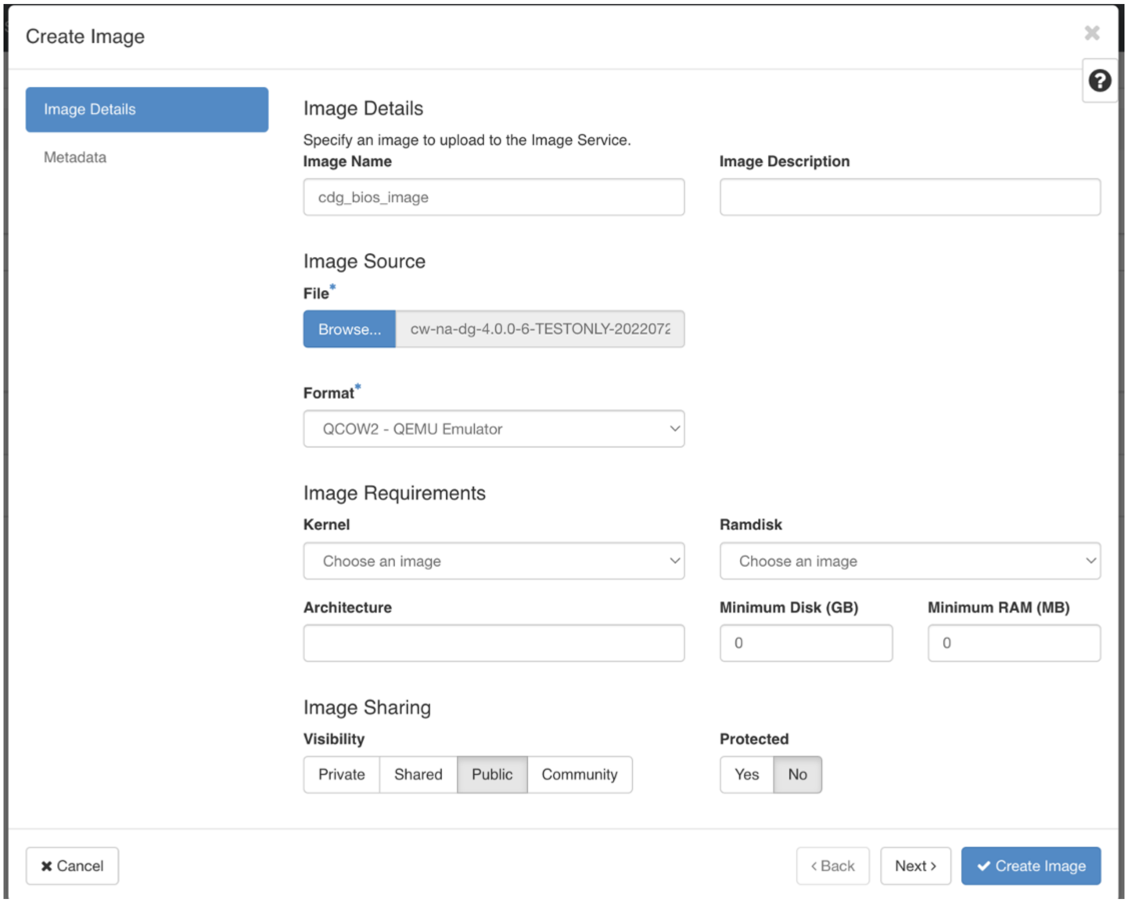
Step 7 **Create an image for OpenStack install.**

a) Enter details in the following fields:

1. **Image Name** - Specify a name for the image you are creating.

2. **File** - Navigate to the directory where you have downloaded the Crosswork Data Gateway release image and select the image.
3. **Format** - Select **QCOW2 - QEMU Emulator** from the drop down list.
4. Leave the other settings to the values as shown in the image.

b) Click **Create Image**.



Create Image

Image Details

Metadata

Image Details

Specify an image to upload to the Image Service.

Image Name: cdg_bios_image

Image Description:

Image Source

File*: Browse... cw-na-dg-4.0.0-6-TESTONLY-2022072

Format*: QCOW2 - QEMU Emulator

Image Requirements

Kernel: Choose an image

Ramdisk: Choose an image

Architecture:

Minimum Disk (GB): 0

Minimum RAM (MB): 0

Image Sharing

Visibility: Private Shared [✓ Public] Community

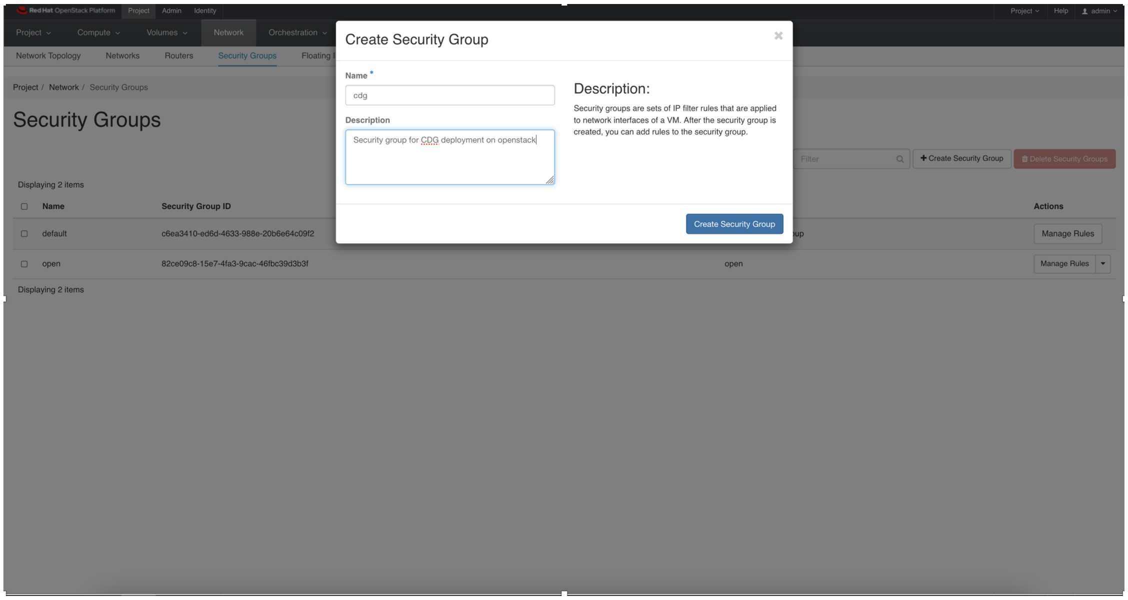
Protected: Yes [✓ No]

Step 8 **Create a security group policy to allow incoming TCP/UDP/ICMP connections.**

OpenStack does not allow incoming TCP/UDP/ICMP connections by default. Create a security policy to allow incoming connections from TCP/UDP/ICMP protocols.

Note You can create security groups and apply them to the VM even after the Crosswork Data Gateway is deployed.

a) In the OpenStack UI, navigate to **Networks** > **Security Groups.**.
b) Click **+ Create Security Group**.



Project / Network / Security Groups

Security Groups

Displaying 2 items

□	Name	Security Group ID		Actions
□	default	c6ea3410-ed6d-4633-988e-20b6e64c09f2	up	Manage Rules
□	open	82ce09c8-15e7-4fa3-9cac-46fbc39d3b3f	open	Manage Rules

Displaying 2 items

Create Security Group

Name *

cdg

Description

Security group for CDG deployment on openstack

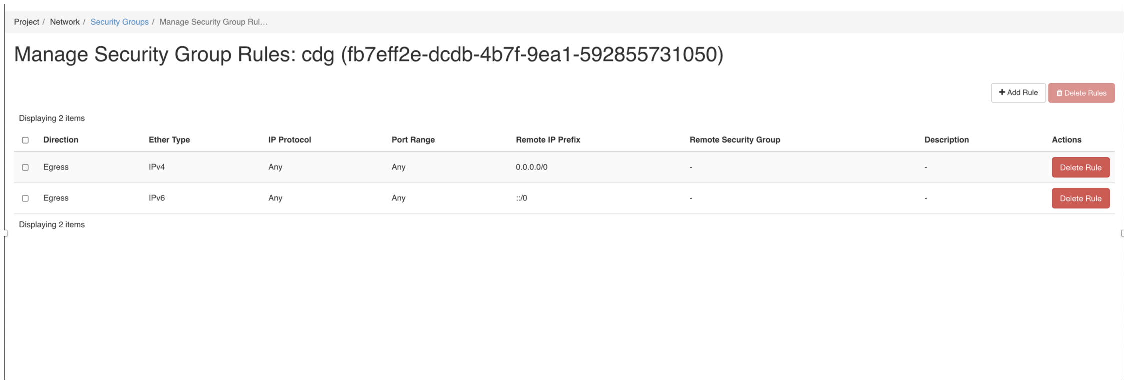
Description:

Security groups are sets of IP filter rules that are applied to network interfaces of a VM. After the security group is created, you can add rules to the security group.

c) Specify the **Name** and **Description** of the security group. Click **Create Security Group**.

d) In the new window that appears to create security rules, click **Add Rule** to create a security policy for each protocol by specifying the direction, port range and the IP addresses range.

The security group contains two rules by default. Use the **Delete Rule** option to delete these rules.



Project / Network / Security Groups / Manage Security Group Rul...

Manage Security Group Rules: cdg (fb7eff2e-dcdb-4b7f-9ea1-592855731050)

Displaying 2 items

□	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Description	Actions
□	Egress	IPv4	Any	Any	0.0.0.0/0	-	-	Delete Rule
□	Egress	IPv6	Any	Any	::/0	-	-	Delete Rule

Displaying 2 items

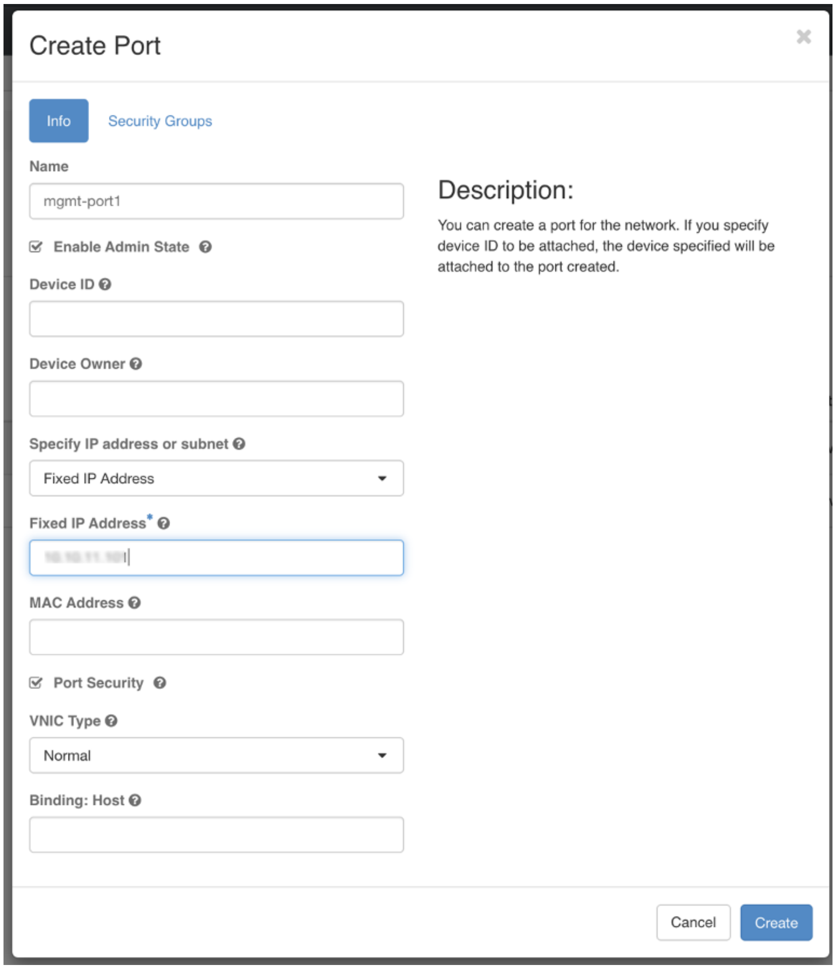
Step 9 **Create ports with specified IP address ONLY if you are using Static addressing.**

Important This step is required only if you are using Static addressing. If you are using DHCP addressing, the IP addresses for the ports are automatically assigned from the IP addresses allocation pool for the subnet.

a) In the OpenStack UI, navigate to **Network** > **Networks**.

b) Depending on the number of NICs in your deployment, (starting with the management network), select a network and click **+ Create Ports**.

c) Enter details in the **Name** and **Fixed IP Address** fields. Select the **Enable Admin State** and **Port Security** check box.



Create Port

Info | Security Groups

Name: mgmt-port1

☑ Enable Admin State

Device ID:

Device Owner:

Specify IP address or subnet: Fixed IP Address

Fixed IP Address*: [redacted]

MAC Address:

☑ Port Security

VNIC Type: Normal

Binding: Host:

Description:

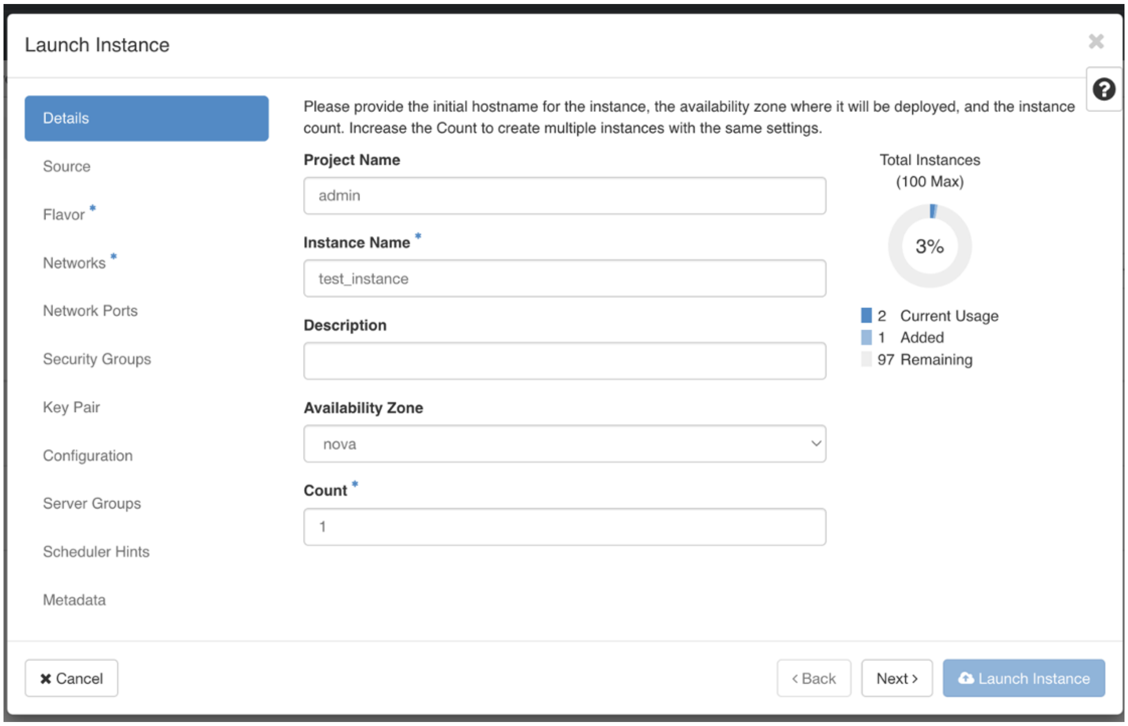
You can create a port for the network. If you specify device ID to be attached, the device specified will be attached to the port created.

Step 10 Navigate to **Compute** > **Instances**. Click **Launch Instance** in this page.

A **Launch Instance** window appears to start the VM installation.

Step 11 In the **Details** tab, specify the VM name in the **Instance Name** field and the **Count** as 1. Click **Next**.

Note For larger systems it is likely that you will have more than one Cisco Crosswork Data Gateway VM. The Cisco Crosswork Data Gateway name should, therefore, be unique and created in a way that makes identifying a specific VM easy. We recommend that you enter the same name you had specified in the `Hostname` parameter in the `config.txt` file for the VM.



Please provide the initial hostname for the instance, the availability zone where it will be deployed, and the instance count. Increase the Count to create multiple instances with the same settings.

Project Name: admin

Instance Name *: test_instance

Description:

Availability Zone: nova

Count *: 1

Total Instances (100 Max)

- 2 Current Usage
- 1 Added
- 97 Remaining

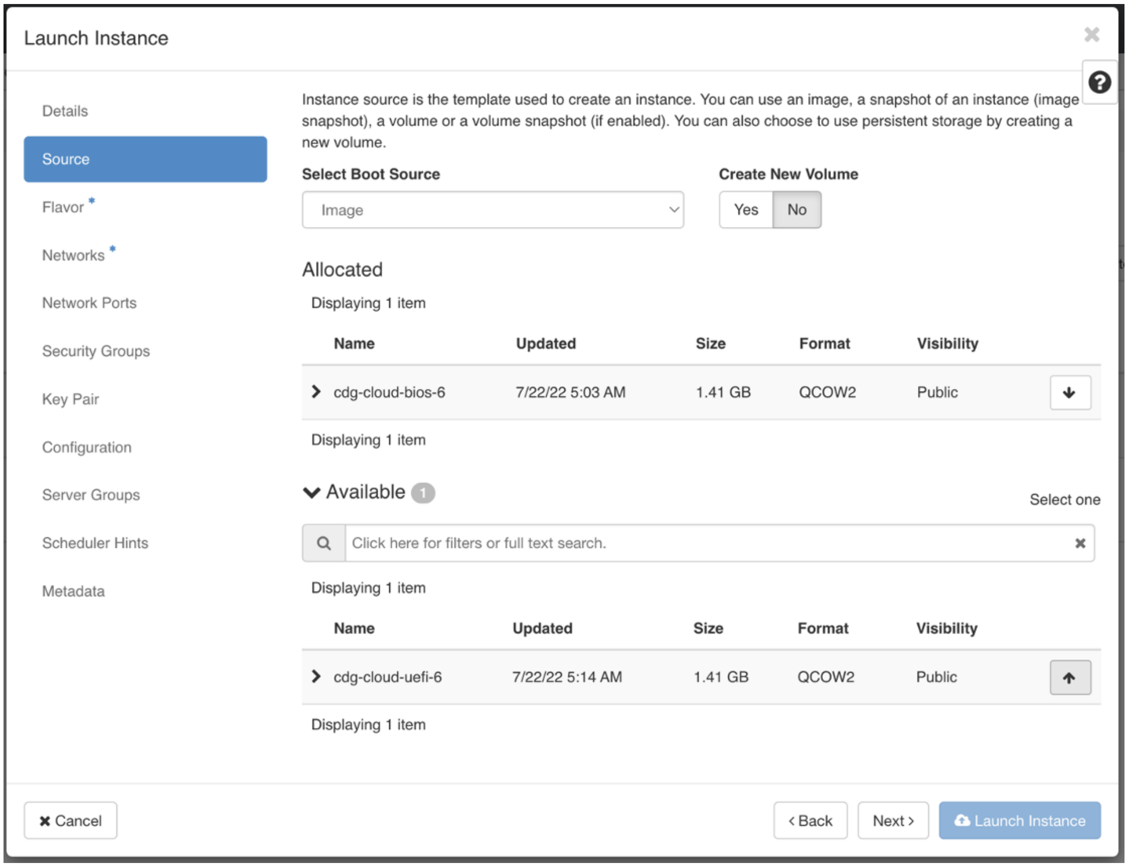
Step 12 In the **Source** tab:

a. **Select Boot Source** - Select **Image** from the drop down list.

b. **Create New Volume** - Select **No**.

c. All images available in the OpenStack environment are listed under the **Available** pane. Click ↑ to select the image. Doing this will now move the image to the **Allocated** pane indicating that you have selected the image.

d. Click **Next**.



Launch Instance

Instance source is the template used to create an instance. You can use an image, a snapshot of an instance (image snapshot), a volume or a volume snapshot (if enabled). You can also choose to use persistent storage by creating a new volume.

Select Boot Source: Image

Create New Volume: Yes [✓ No]

Allocated

Displaying 1 item

	Name	Updated	Size	Format	Visibility	
>	cdg-cloud-bios-6	7/22/22 5:03 AM	1.41 GB	QCOW2	Public	↓

Displaying 1 item

Available 1 — Select one

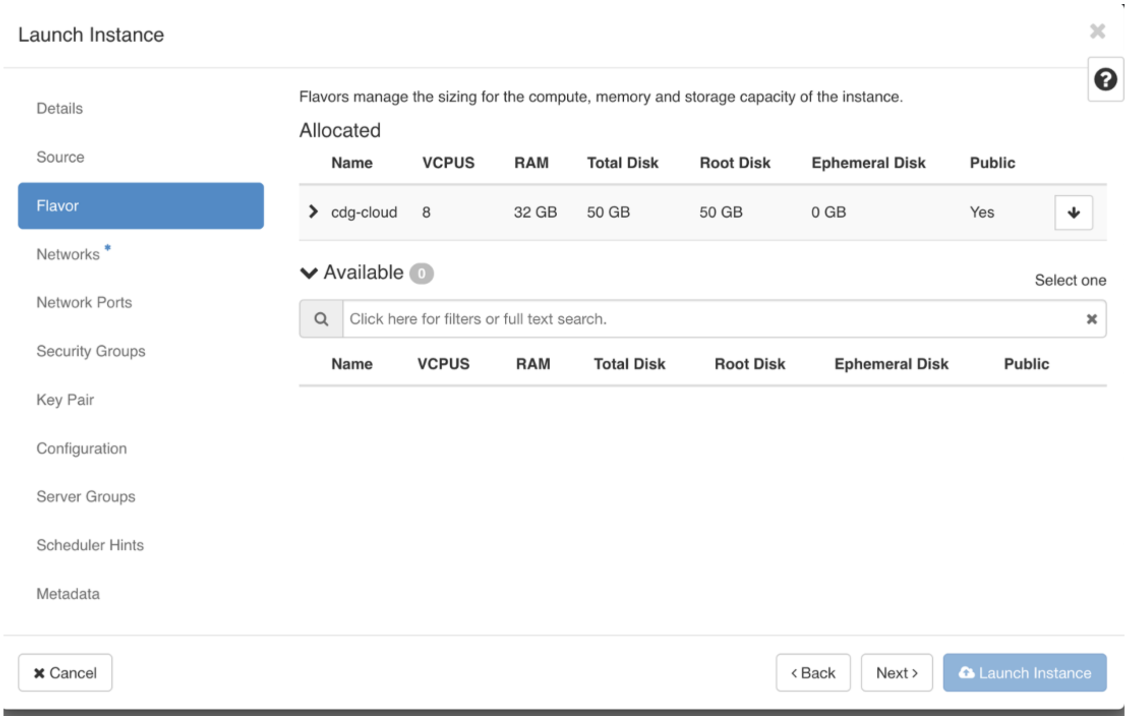
Click here for filters or full text search.

Displaying 1 item

	Name	Updated	Size	Format	Visibility	
>	cdg-cloud-uefi-6	7/22/22 5:14 AM	1.41 GB	QCOW2	Public	↑

Displaying 1 item

Step 13 In the **Flavor** tab, in the **Available** pane, for the flavor you want to select for the VM, click ↑ to move it from the **Available** pane to the **Allocated** pane. Click **Next**.



Flavors manage the sizing for the compute, memory and storage capacity of the instance.

Allocated

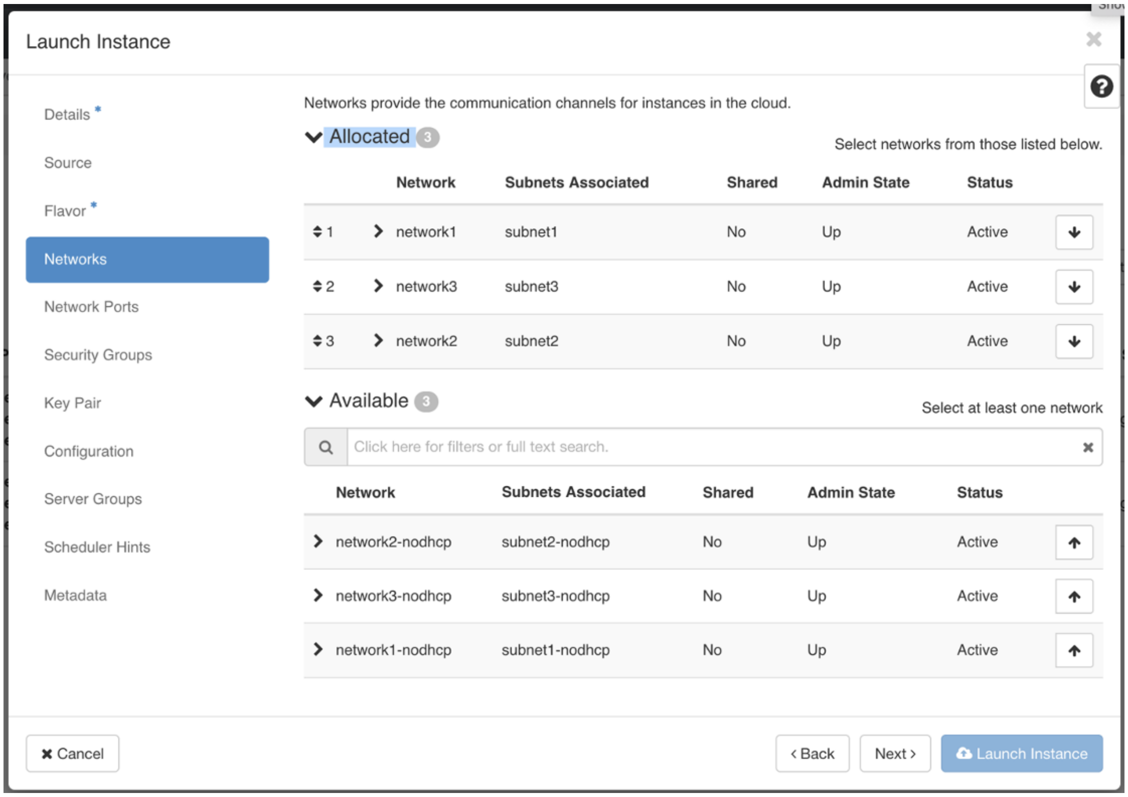
Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public
cdg-cloud	8	32 GB	50 GB	50 GB	0 GB	Yes

Available 0

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public

Step 14 Assign networks to the VM. Depending on the number of vNICs in your deployment, select up to 3 networks for the VM by clicking ↑ for each network from the list of networks in the **Available** pane. Doing this will move the selected networks to the **Allocated** pane. Click **Next**.

Important The order in which you select the networks is important. In a 3-NIC deployment, the first network you select will be assigned to the vNIC0 interface, the second to the vNIC1 interface and the third to the vNIC2 interface.



Launch Instance

Networks provide the communication channels for instances in the cloud.

Allocated 3

Select networks from those listed below.

	Network	Subnets Associated	Shared	Admin State	Status
1	network1	subnet1	No	Up	Active
2	network3	subnet3	No	Up	Active
3	network2	subnet2	No	Up	Active

Available 3

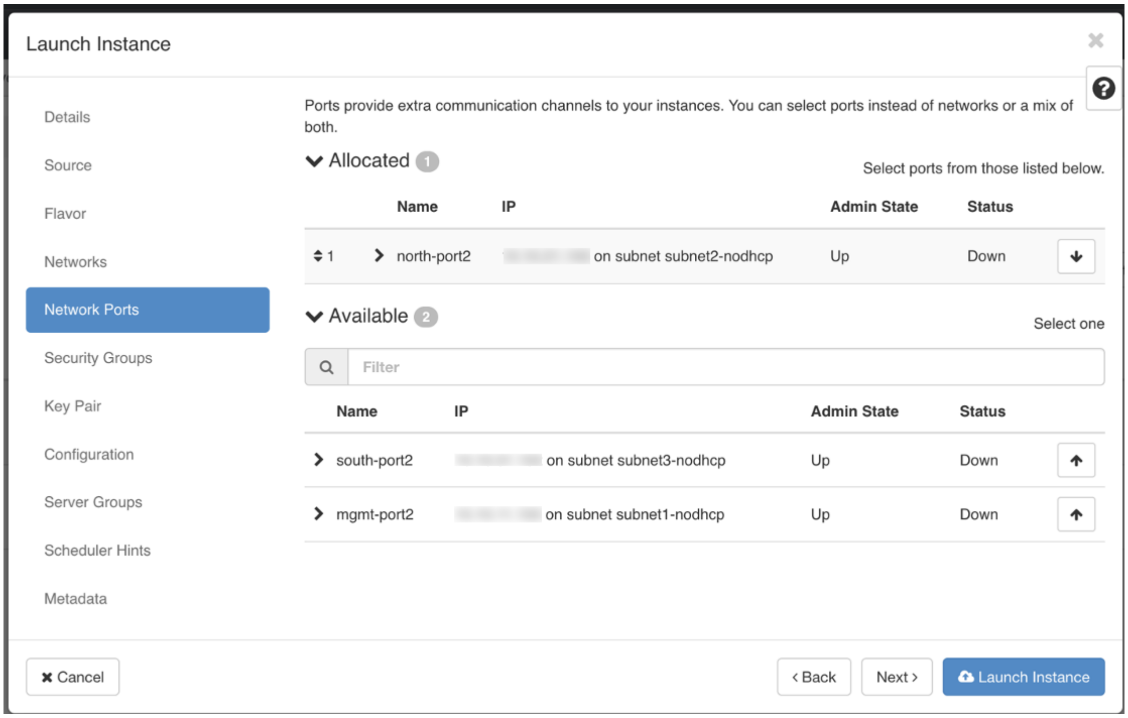
Select at least one network

Click here for filters or full text search.

Network	Subnets Associated	Shared	Admin State	Status
network2-nodhcp	subnet2-nodhcp	No	Up	Active
network3-nodhcp	subnet3-nodhcp	No	Up	Active
network1-nodhcp	subnet1-nodhcp	No	Up	Active

Step 15 Assign ports to the VM.

From the list of ports that are displayed in the **Available** pane, click ↑ to move the port to the **Allocated** pane. .



Ports provide extra communication channels to your instances. You can select ports instead of networks or a mix of both.

Allocated 1

Select ports from those listed below.

	Name	IP	Admin State	Status
1	north-port2	[redacted] on subnet subnet2-nodhcp	Up	Down

Available 2

Select one

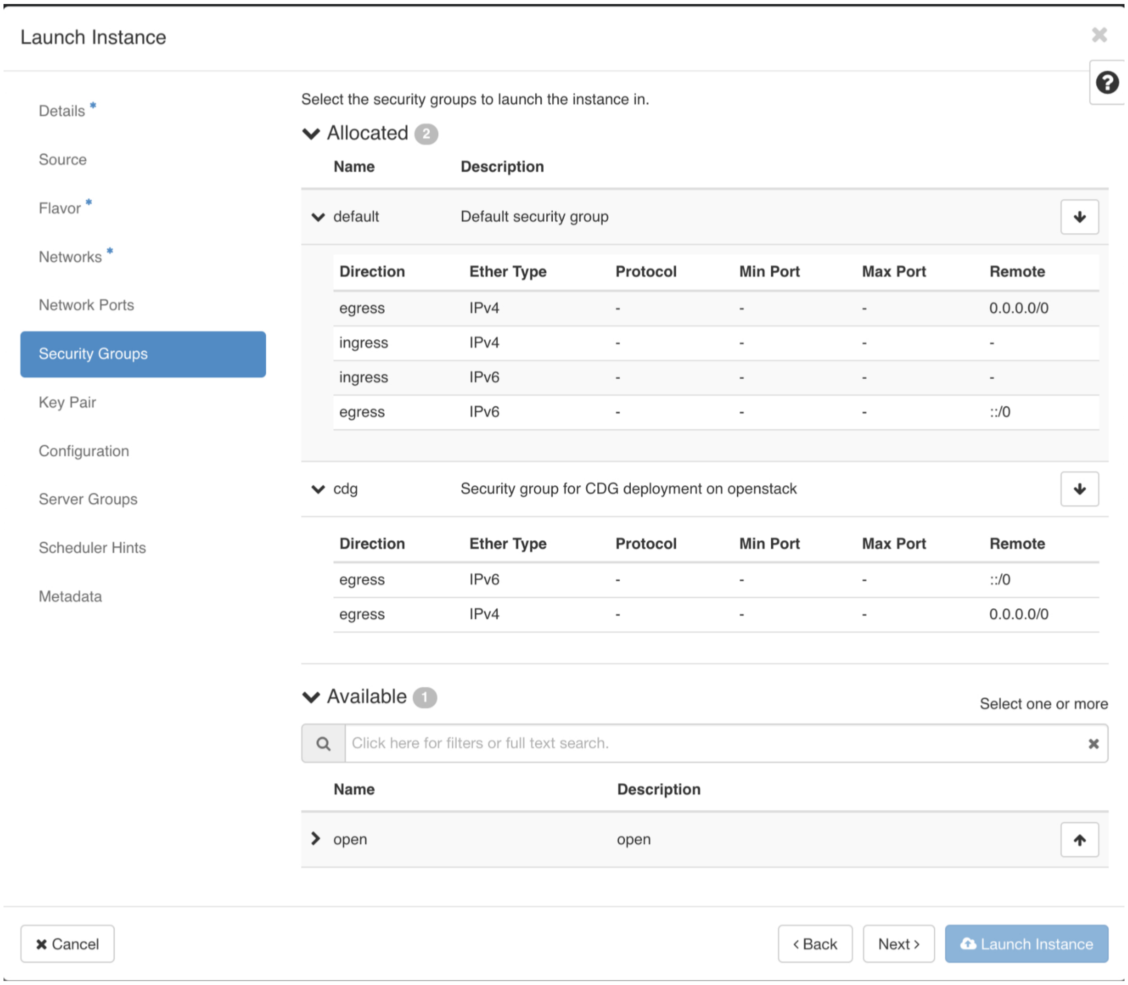
Filter

Name	IP	Admin State	Status
south-port2	[redacted] on subnet subnet3-nodhcp	Up	Down
mgmt-port2	[redacted] on subnet subnet1-nodhcp	Up	Down

Click **Next**.

Step 16 Assign **Security Groups** to the VM by moving the security groups you wish to apply to the VM from the **Available** pane to the **Allocated** pane. .

In the following image, 2 security groups - default and cdg, are applied to the VM.



Select the security groups to launch the instance in.

Allocated 2

Name	Description
default	Default security group

Direction	Ether Type	Protocol	Min Port	Max Port	Remote
egress	IPv4	-	-	-	0.0.0.0/0
ingress	IPv4	-	-	-	-
ingress	IPv6	-	-	-	-
egress	IPv6	-	-	-	::/0

Name	Description
cdg	Security group for CDG deployment on openstack

Direction	Ether Type	Protocol	Min Port	Max Port	Remote
egress	IPv6	-	-	-	::/0
egress	IPv4	-	-	-	0.0.0.0/0

Available 1 — Select one or more

Click here for filters or full text search.

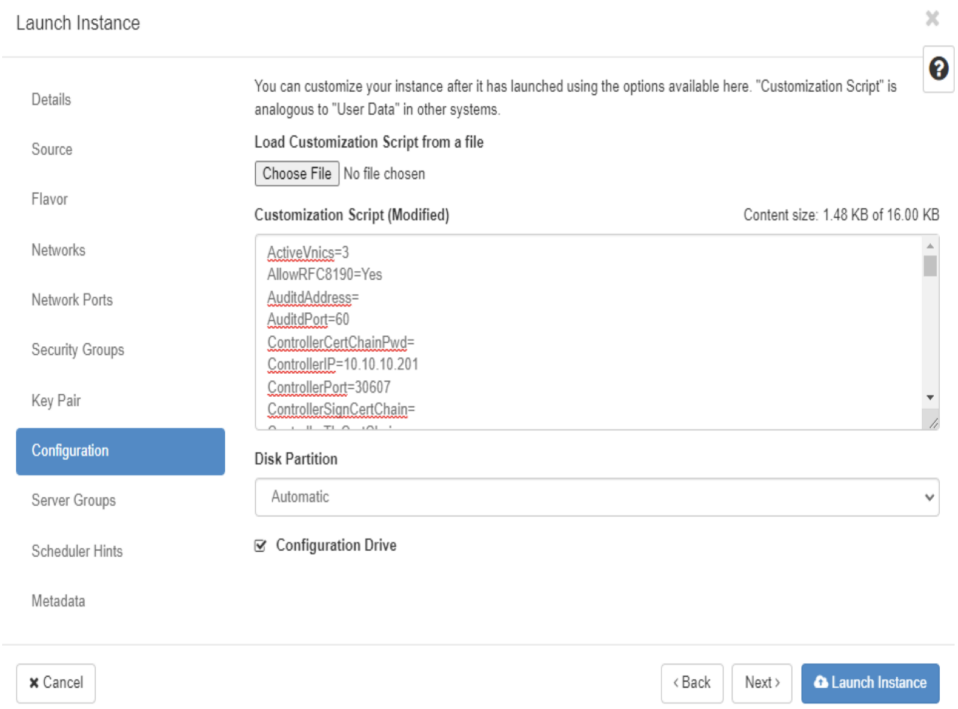
Name	Description
open	open

Click **Next**.

Step 17 In the **Key Pair** tab, click **Next**.

Step 18 In the **Configuration** tab:

- Click **Choose File** to select and upload the `config.txt` file you had modified and saved for the VM.
- Select the **Configuration Drive** check box.



You can customize your instance after it has launched using the options available here. "Customization Script" is analogous to "User Data" in other systems.

Load Customization Script from a file

Choose File No file chosen

Customization Script (Modified) Content size: 1.48 KB of 16.00 KB

```
ActiveVnics=3
AllowRFC8190=Yes
AuditdAddress=
AuditdPort=60
ControllerCertChainPwd=
ControllerIP=10.10.10.201
ControllerPort=30607
ControllerSignCertChain=
```

Disk Partition: Automatic

☑ Configuration Drive

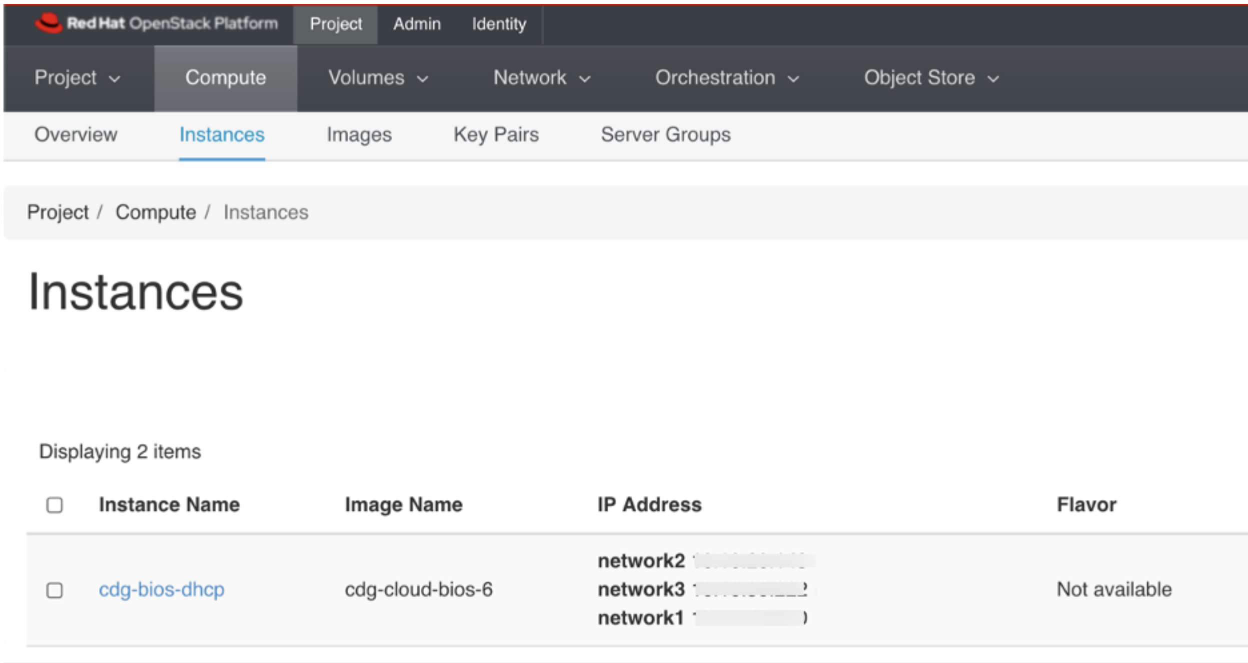
Step 19 Click **Launch Instance**.

OpenStack begins installation of the VM.

Step 20 Repeat **Step 9** to **Step 20** of the procedure to install all Crosswork Data Gateway VMs.

Verify that the Crosswork Data Gateway VMs were installed successfully.

1. In the OpenStack UI, navigate to **Compute** > **Instances**.
2. The list of Crosswork Data Gateway VMs that are installed and being installed is displayed here.



Project / Compute / Instances

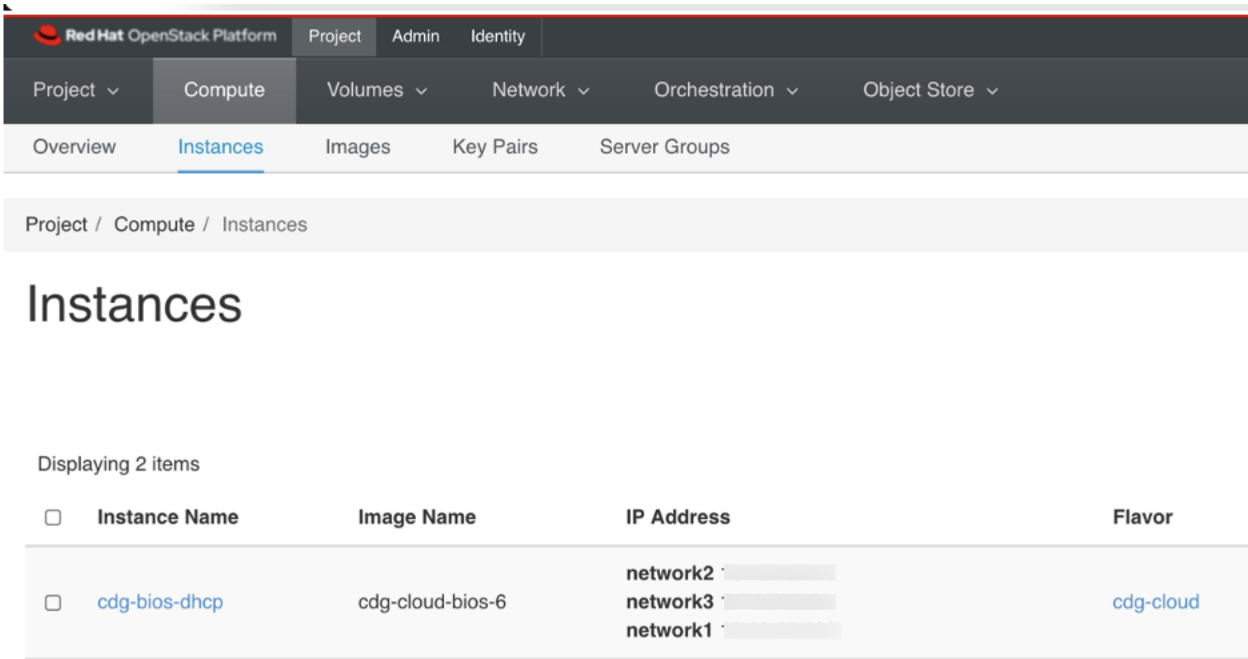
Instances

Displaying 2 items

□	Instance Name	Image Name	IP Address	Flavor
□	cdg-bios-dhcp	cdg-cloud-bios-6	network2 [redacted] network3 [redacted] network1 [redacted]	Not available

A Crosswork Data Gateway VM that is being installed will have the **Status** as **Build**, **Task** as **Spawning** and **Power State** as **No State**.

3. Once the VM is successfully installed, the **Status** changes to **Active**, **Task** is **None** and **Power State** as **Running**.



Project / Compute / Instances

Instances

Displaying 2 items

□	Instance Name	Image Name	IP Address	Flavor
□	cdg-bios-dhcp	cdg-cloud-bios-6	network2 [redacted] network3 [redacted] network1 [redacted]	cdg-cloud

4. After the Status changes to **Active**, wait for about 10 minutes.

   Click the Crosswork Data Gateway VM name. The link to the VM console opens.

5. Log in as the dg-admin or dg-oper user (as per the role assigned to you) and the corresponding password you had entered in the `config.txt` file of the VM. The Interactive console of the Crosswork Data Gateway is displayed after you login successfully.

What to do next

Proceed to enrolling the Crosswork Data Gateway with Crosswork Cloud by generating and exporting the enrollment package. See Export Enrollment Package, on page 44.

Generate Enrollment Package

Every Crosswork Data Gateway must be identified by means of an immutable identifier. This requires generation of an enrollment package. The enrollment package can be generated using any of the following methods:

- By supplying **Auto Enrollment Package** parameters during installation process (see Auto Enrollment Package under Table 1: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios.).
- By using the **Export Enrollment Package** option from the Interactive Console (see Export Enrollment Package, on page 44)

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 Crosswork Data Gateway required for registering, such as Certificate, UUID of the Crosswork Data Gateway, and metadata like Crosswork Data Gateway 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 Crosswork Data Gateway with Crosswork Cloud. The steps to do so are described in Export Enrollment Package, on page 44.

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

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"
  }
```

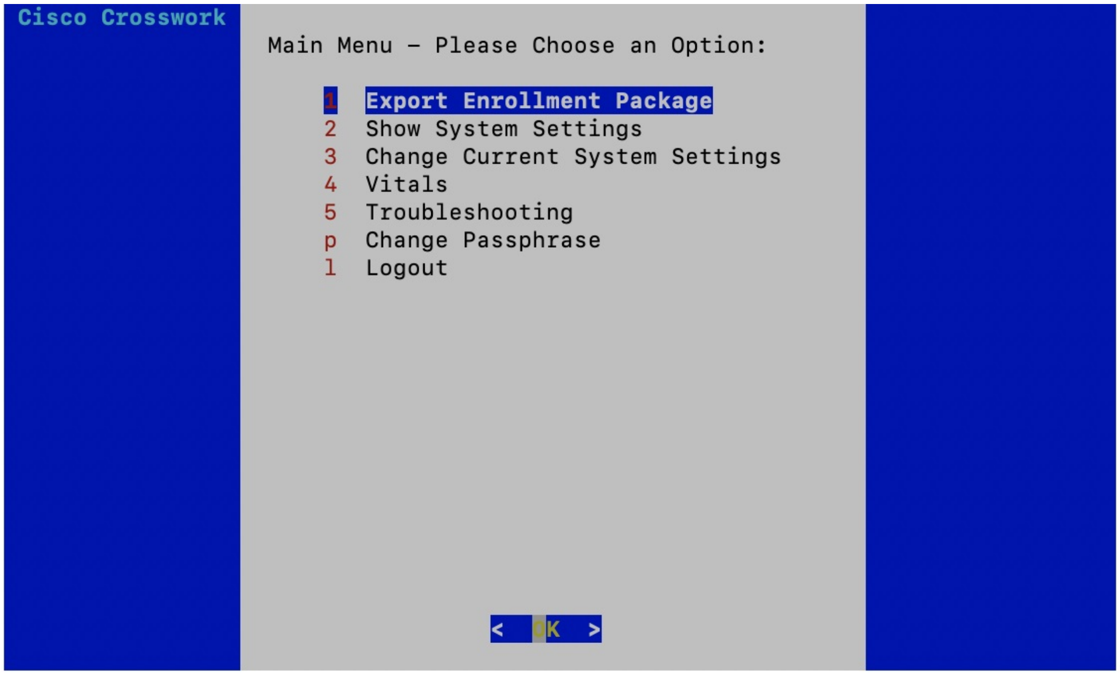
Export Enrollment Package

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 during installation. Otherwise, the file will be copied to the SCP URI destination you selected after the VM boots. Proceed to Register Crosswork Data Gateway with Crosswork Cloud Applications, on page 45 if you had already specified the **Auto Enrollment Package Transfer** settings during installation.

Step 1 Log in to the Cisco Crosswork Data Gateway.

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 you are not using the default port 22, you can specify the port as a part of the SCP command. For example, For example, to export the enrollment package as an admin user, placing the file in that user's home directory with port 4000, you can give the following command:

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

- The enrollment file is created with a unique name. For example: 9208b9bc-b941-4ae9-b1a2-765429766f27.json

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

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.

What to do next

Proceed with enrolling the Cisco Crosswork Data Gateway with Crosswork Cloud as explained in Register Crosswork Data Gateway with Crosswork Cloud Applications, on page 45.

Register Crosswork Data Gateway with Crosswork Cloud Applications

The .json registration file of the Crosswork Data Gateway contains unique digital certificates that are used to enroll Crosswork Data Gateway into Crosswork Cloud. Add that information in Crosswork Cloud as explained below.

Note If you use a firewall on your Crosswork Data Gateway egress traffic, ensure that your firewall configuration allows cdg.crosswork.cisco.com and crosswork.cisco.com.

Step 1 Log in to Crosswork Cloud.

Step 2 From the main window, click **Configure** > **Data Gateways**, then click **Add**.

Step 3 Click **Registration File** to upload the enrollment data file you downloaded from Crosswork Data Gateway, navigate to the location of the .json file, then click **Next**.

Step 4 Enter a name for the Crosswork Data Gateway.

Step 5 In the **Application** field, select the Crosswork Cloud application for which you're using this Crosswork Data Gateway instance. Each Crosswork Data Gateway can be applied to one Crosswork Cloud application only.

Step 6 Complete the rest of the required fields, then click **Next**.

Step 7 (Optional) Enter a tag name, which allows you to group Crosswork Data Gateways with the same tag, then click **Next**.

Step 8 Review the Crosswork Data Gateway information that you entered, then click **Next**.

Step 9 Click **Accept** to accept the security certificate.

A message appears to indicate the Crosswork Data Gateway was successfully added.

What to do next

Repeat this procedure to enroll all the Crosswork Data Gateways in your network with Crosswork Cloud.

To verify that the Crosswork Data Gateway is successfully connected, click **Data Gateways**, click on the name of the Crosswork Data Gateway, and verify the following values for the Crosswork Data Gateway you added:

- **Session Up**: Active
- **Connectivity**: Session Up

If the Crosswork Data Gateway has not successfully connected to the Crosswork Cloud service, refer to the Troubleshoot the Crosswork Data Gateway Connectivity, on page 46 section.

Troubleshoot the Crosswork Data Gateway Connectivity

The following table lists common problems that might be experienced with Crosswork Data Gateway connectivity to the Crosswork Cloud application, and provides approaches to identifying the source of the problem and solving it.

Table 2: Troubleshooting Crosswork Data Gateway Connectivity

Issue	Action
Crosswork Data Gateway cannot be enrolled with Cisco Crosswork Cloud due to an NTP issue, i.e., there is a clock-drift between the two.	1. Log into the 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 `/cdg/logs/components/controller-gateway/session.log`), 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 Crosswork Data Gateway and Cisco Crosswork Cloud. 3. From the main menu, go to **3 Change Current System Settings** > **1 Configure NTP**. Configure NTP to sync with the clock time on the Cisco Crosswork Cloud server and try enrolling the Crosswork Data Gateway with Crosswork Cloud again.

Issue	Action
Crosswork Data Gateway does not have direct connectivity to external web services.	1. Configure a proxy server if a proxy server is missing in your environment. 2. If a proxy server is already present in your enviroment, check if the proxy URL is correct. 3. Check if the credentials of the proxy (certificate, proxy name etc) are correct. To update the proxy server details on the Crosswork Data Gateway, see Configure Control Proxy.