



Installation Tasks

This section contains the following topics:

- [Install Cisco Crosswork Data Gateway, on page 1](#)
- [Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2](#)
- [Install Crosswork Data Gateway on VMware, on page 15](#)
- [Install Crosswork Data Gateway on OpenStack Platform, on page 23](#)
- [Install Crosswork Data Gateway on Amazon EC2, on page 62](#)
- [Generate Enrollment Package, on page 70](#)
- [Obtain the Enrollment Package, on page 72](#)
- [Register Crosswork Data Gateway with Crosswork Cloud Applications, on page 74](#)
- [Troubleshoot the Crosswork Data Gateway Connectivity, on page 75](#)

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. Ensure that you have the software image required to deploy Cisco Crosswork Data Gateway on your preferred platform:

VMware	Install Crosswork Data Gateway Using vCenter vSphere Client, on page 15
	Install Crosswork Data Gateway Via OVF Tool, on page 21

OpenStack	Install Crosswork Data Gateway on OpenStack from OpenStack CLI, on page 24 Install Crosswork Data Gateway on OpenStack from the OpenStack UI, on page 38
Amazon EC2	Install Crosswork Data Gateway on Amazon EC2 using CloudFormation Template, on page 62 Install Crosswork Data Gateway on Amazon EC2 Manually, on page 63

3. Generate and export Enrollment package.
 - [Generate Enrollment Package, on page 70](#)
 - [Obtain the Enrollment Package, on page 72](#)
4. Enroll Cisco Crosswork Data Gateway with Crosswork Cloud applications. See [Register Crosswork Data Gateway with Crosswork Cloud Applications, on page 74](#).

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. It 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 in 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 reenroll 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.



Note When entering the parameters for deployment, ensure that you add the correct parameters. If the parameter values are incorrect, you have to destroy the current Crosswork Data Gateway VM, create a new VM, and reenroll the new VM with Cisco Crosswork.

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.	

Name	Parameter	Description	Additional Information
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 <code>Crosswork Cloud</code> for Cloud deployment.	You must specify this parameter for VMware or OVF tool installation.
AllowRFC8190	AllowRFC8190	Automatically allow addresses in an RFC 8190 range. Options are <code>True</code> , <code>False</code> , or <code>Ask</code> , where the initial configuration script prompts for confirmation. The default value is <code>True</code> .	

Name	Parameter	Description	Additional Information
Private Key URI	DGCertKey	URI to private key file for session key signing. You can retrieve this using SCP (user@host:path/to/file).	<p>Crosswork Cloud uses self-signed certificates for handshake with Cisco Crosswork Data Gateway. These certificates are generated at installation.</p> <p>However, if you want to use third party or your own certificate files enter these parameters.</p> <p>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).</p> <p>Note The host with the URI files must be reachable on the network (in the vNIC0 interface via SCP) and files must be present at the time of install.</p>
Certificate File and Key Passphrase	DGCertChainPwd	SCP user passphrase to retrieve the Cisco Crosswork Data Gateway PEM formatted certificate file and private key.	
Data Disk Size	DGAppdataDisk	<p>Size in GB of a second data disk. The minimum size is 20GB.</p> <p>The default size is 24GB.</p>	

Name	Parameter	Description	Additional Information
AwsIamRole	AwsIamRole	AWS IAM role name for EC2 installation.	A role created in Identity and Access Management (IAM) in the AWS environment with relevant permissions.
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 both IPv4 Method and IPv6 Method fields results in a nonfunctional deployment.			
vNIC Role Assignment			
Role assignment allows you to control the traffic that an interface must handle. If the preassigned roles don't meet the specific needs of your organization, you can explicitly assign roles to interfaces.			
Each parameter has a predefined role. The parameter accepts the interface value as eth0, eth1, or eth2. The fourth interface, eth3, allows you to separate SSH, management, control (Crosswork Cloud service), and north data, and south data traffic.			

Name	Parameter	Description	Additional Information
NicDefaultGateway	NicDefaultGateway	Interface used as the Default Gateway for processing the DNS and NTP traffic. Traffic that is not assigned to any other interface is defaulted to this interface. Options are <code>eth0</code> , <code>eth1</code> , <code>eth2</code> , or <code>eth3</code> . The default value is <code>eth0</code> .	<p>You can configure the number of interfaces based on the vNIC model that you chose to deploy Crosswork Data Gateway. For example, if you deployed Crosswork Data Gateway on 2 active vNICs, the roles must be configured to use the <code>eth0</code> and <code>eth1</code> interfaces.</p> <ul style="list-style-type: none"> • The <code>NicControl</code>, <code>NicNBExternalData</code>, and <code>NicSBData</code> roles map to <code>eth1</code>. • The <code>NicControl</code>, <code>NicNBExternalData</code>, <code>NicSBData</code> roles map to <code>eth1</code>. • The <code>NicSBData</code> role maps to <code>eth2</code>. • The <code>NicControl</code>, and <code>NicNBExternalData</code> roles map to <code>eth1</code>.
NicAdministration	NicAdministration	Interface used to route the traffic associated with the administration of the Crosswork Data Gateway. The interface uses SSH protocol through the configured port. Options are <code>eth0</code> , <code>eth1</code> , <code>eth2</code> , or <code>eth3</code> . The default value is <code>eth0</code> .	
NicExternalLogging	NicExternalLogging	Interface used to send logs to Crosswork Cloud. Options are <code>eth0</code> , <code>eth1</code> , <code>eth2</code> , or <code>eth3</code> . The default value is <code>eth0</code> .	
NicManagement	NicManagement	Interface used to send the enrollment and other management traffic. Options are <code>eth0</code> , <code>eth1</code> , <code>eth2</code> , or <code>eth3</code> . The default value is <code>eth0</code> .	
NicControl	NicControl	Interface used for sending the destination, device, and collection configuration. Options are <code>eth0</code> , <code>eth1</code> , <code>eth2</code> , or <code>eth3</code> . The default value is <code>eth0</code> .	
NicNBExternalData	NicNBExternalData	Interface used to send collection data to Crosswork Cloud. Options are <code>eth0</code> , <code>eth1</code> , <code>eth2</code> , or <code>eth3</code> . The default value is <code>eth0</code> .	

Name	Parameter	Description	Additional Information
NicSBData	NicSBData	Interface used to collect data from all devices. Options are <code>eth0</code> , <code>eth1</code> , <code>eth2</code> , or <code>eth3</code> . The default value is <code>eth0</code> .	
vNIC IPv4 Address (vNIC0, vNIC1, vNIC2, and vNIC3 based on the number of interfaces you choose to use)			

Name	Parameter	Description	Additional Information
vNIC IPv4 Method*	Vnic0IPv4Method Vnic1IPv4Method Vnic2IPv4Method Vnic3IPv4Method	Options are <code>None</code> , <code>Static</code> , or <code>DHCP</code> . Note DHCP support is enabled only for deployments performed using the QCOW2 images. To use IPv4 address, select Method as <code>Static</code> or <code>DHCP</code> , and select the vNICxIPv6 Method as <code>None</code> . The default value for Method is <code>None</code> .	If you have selected Method as: <ul style="list-style-type: none"> • 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: Values for the vNIC IPv4 Address parameters are assigned automatically. Do not change the default values.
vNIC IPv4 Address*	Vnic0IPv4Address Vnic1IPv4Address Vnic2IPv4Address Vnic3IPv4Address	IPv4 address of the interface.	
vNIC IPv4 Netmask*	Vnic0IPv4Netmask Vnic1IPv4Netmask Vnic2IPv4Netmask Vnic3IPv4Netmask	IPv4 netmask of the interface in dotted quad format.	
vNIC IPv4 Skip Gateway*	Vnic0IPv4SkipGateway Vnic1IPv4SkipGateway Vnic2IPv4SkipGateway Vnic3IPv4SkipGateway	Options are <code>True</code> or <code>False</code> . Selecting <code>True</code> skips configuring a gateway. The default value is <code>False</code> .	
vNIC IPv4 Gateway*	Vnic0IPv4Gateway Vnic1IPv4Gateway Vnic2IPv4Gateway Vnic3IPv4Gateway	IPv4 address of the vNIC gateway.	
vNIC IPv6 Address (vNIC0, vNIC1, vNIC2, and vNIC3 based on the number of interfaces you choose to use)			

Name	Parameter	Description	Additional Information
vNIC IPv6 Method*	Vnic0IPv6Method Vnic1IPv6Method Vnic2IPv6Method Vnic3IPv6Method	Options are <code>None</code> , <code>Static</code> , <code>DHCP</code> or <code>SLAAC</code> (QCOW2 only). The default value for Method is <code>None</code> . Note DHCP support is enabled only for deployments performed using the QCOW2 images.	<p>If you have selected Method as:</p> <ul style="list-style-type: none"> • None: Skip the rest of the fields for IPv6 address. Enter information in the vNICx IPv4 Address parameters. • Static: Enter information in Address, Netmask, Skip Gateway, and Gateway fields • DHCP: Values for the vNIC IPv6 Address parameters are assigned automatically. <p>Do not change the VnicIPv6Address default values.</p>
vNIC IPv6 Address*	Vnic0IPv6Address Vnic1IPv6Address Vnic2IPv6Address Vnic3IPv6Address	IPv6 address of the interface.	
vNIC IPv6 Netmask*	Vnic0IPv6Netmask Vnic1IPv6Netmask Vnic2IPv6Netmask Vnic3IPv6Netmask	IPv6 prefix of the interface.	
vNIC IPv6 Skip Gateway*	Vnic0IPv6SkipGateway Vnic1IPv6SkipGateway Vnic2IPv6SkipGateway Vnic3IPv6SkipGateway	Options are <code>True</code> or <code>False</code> . Selecting <code>True</code> skips configuring a gateway. The default value is <code>False</code> .	
vNIC IPv6 Gateway*	Vnic0IPv6Gateway Vnic1IPv6Gateway Vnic2IPv6Gateway Vnic3IPv6Gateway	IPv6 address of the vNIC gateway.	
DNS Servers			
DNS Address*	DNS	Space-delimited list of IPv4 or IPv6 addresses of the DNS server accessible in the management interface.	

Name	Parameter	Description	Additional Information
DNS Search Domain	Domain	DNS search domain. The default value is localdomain.	
DNS Security Extensions	DNSSEC	Options are False, True, or Allow-Downgrade. Select True to use DNS security extensions. The default value is False.	
DNS over TLS	DNSTLS	Options are False, True, or Opportunistic. Select True to use DNS over TLS. The default value is False.	
Multicast DNS	mDNS	Options are False, True, or Resolve. Select True to use multicast DNS. The default value is False.	
Link-Local Multicast Name Resolution	LLMNR	Options are False, True, Opportunistic, or Resolve. Select True to use link-local multicast name resolution. The default value is False.	
NTP Servers			
NTPv4 Servers*	NTP	NTPv4 server list. Enter space-delimited list of IPv4, IPv6 addresses, or hostnames of the NTPv4 servers accessible in the management interface.	You must enter a value here, such as <sample>.ntp.org. NTP server is critical for time synchronization between Cisco Crosswork Data Gateway, Crosswork Cloud, and devices. Using a nonfunctional or dummy address may cause issues when Crosswork Cloud and Cisco Crosswork Data Gateway try to communicate with each other.

Name	Parameter	Description	Additional Information
Use NTPv4 Authentication	NTPAuth	Select <code>True</code> to use NTPv4 authentication. The default value is <code>False</code> .	The <code>NTPKey</code> , <code>NTPKeyFile</code> , and <code>NTPKeyFilePwd</code> can be configured only when the <code>NTPAuth</code> is set to <code>True</code> .
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 <code>True</code> to send syslog messages to a remote host. The default value is <code>False</code> .	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 these seven settings. 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 in the management interface. Note If you are using an IPv6 address, surround it with square brackets ([::1]).	
Syslog Server Port	SyslogPort	Port number of the optional syslog server. The port value can range 1–65535. By default, this value is set to 514.	
Syslog Server Protocol	SyslogProtocol	Options are <code>UDP</code> , <code>TCP</code> , or <code>RELP</code> to send the syslog. The default value is <code>UDP</code> .	
Use Syslog over TLS	SyslogTLS	Select <code>True</code> to use TLS to encrypt syslog traffic. By default, this parameter is set to <code>False</code> .	
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 <code>True</code> to send Auditd message to a remote host. The default value is <code>False</code> .	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. The default port number is 60.	
Controller and Proxy Settings			
Proxy Server URL	ProxyURL	URL of an optional HTTP 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 Obtain the Enrollment Package , on page 72.
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 on VMware

You can install the Crosswork Data Gateway on VMware in one of the following ways:

- [Install Crosswork Data Gateway Using vCenter vSphere Client, on page 15](#)
- [Install Crosswork Data Gateway Via OVF Tool, on page 21](#)

Install Crosswork Data Gateway Using vCenter vSphere Client

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

Step 1 Refer to [Cisco Crosswork Data Gateway 4.5 Release Notes for Cloud Application](#) 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 have to start over again. To prevent this, we recommend that you plan what you 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

✓ 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

Select a name and folder
Specify a unique name and target location

Virtual machine name:

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

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

	Description
<input checked="" type="radio"/> Crosswork Cloud	8 CPU; 32GB RAM; 1-3 NICs; 74GB Disk
<input type="radio"/> Crosswork On-Premise Standard	
<input type="radio"/> Crosswork On-Premise Extended	
<input type="radio"/> Crosswork On-Premise Standard With Extra Resources	

4 Items

CANCEL
BACK
NEXT

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


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

Select 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.

CANCEL BACK NEXT

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

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

Select networks
Select a destination network for each source network.

Source Network	Destination Network
vNIC3	VM Network
vNIC2	VM Network
vNIC1	VM Network
vNIC0	VM Network

4 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL
BACK
NEXT

Step 13

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

Note

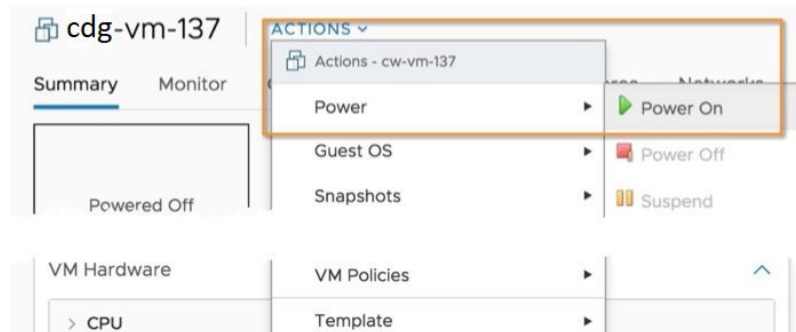
- The VMware vCenter Server 6.7, 6.5, ESXi version 5.5 or 6.0 has issue with expanding the correct parameters. To override this issue, ensure that in the **Customize template > 03. vNIC Role Assignment** section, the following parameters are set as:
 - All the roles are set to eth0.
 - **16. Controller Setting > a. Crosswork Controller IP:** crosswork.cisco.com
 - **16. Controller Setting > b. Crosswork Controller Port:** 443
- 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 is an error "7 properties have invalid values". This is normal and 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.
- Open the vCenter vSphere client.
 - 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 log in 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 reenroll the new one on the Crosswork Cloud.

Verify that the installation was successful.

1. Log in to Crosswork Data Gateway VM Via vCenter:

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

- 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 several 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 causes the client IP to be blocked for at least 7 minutes. Continuing to accumulate failures 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 reinstall 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 [Obtain the Enrollment Package, on page 72](#).

Install Crosswork Data Gateway Via OVF Tool

You can modify mandatory or optional parameters in the command or script as per your requirement and run the OVF Tool (ovftool). See [Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2](#).



Note Ensure that you specify all the mandatory and optional parameters with the desired values when you build the script. Parameters that are not included in the script are considered with their default values for deployment.

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="Crosswork-Cloud"

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 Gateway : "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 where you want to install Crosswork Data Gateway.

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

Note The sample shell script includes only the mandatory options. If you want to customize the optional parameters in the OVF Tool command, see the [Table 1: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 3](#) for information about these parameters.

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

Step 4 Run the OVF Tool using the script.

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

For example,

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

Verify that the installation was successful.

1. Log in 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`) 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 workstation 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>`

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 causes the client IP to be blocked for at least 7 minutes. Continuing to accumulate failures 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 reinstall with the correct network settings.

What to do next

Proceed to enrolling the Crosswork Data Gateway with Crosswork Cloud. See [Obtain the Enrollment Package, on page 72](#).

Install Crosswork Data Gateway on OpenStack Platform

You can install the Crosswork Data Gateway on OpenStack Platform in one of the following ways:

- [Install Crosswork Data Gateway on OpenStack from OpenStack CLI, on page 24](#)
- [Install Crosswork Data Gateway on OpenStack from the OpenStack UI, on page 38](#)

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 one or more VMs.
- 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](https://www.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 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](https://www.cisco.com). Please contact Cisco Customer Experience team if access to [cisco.com](https://www.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.**

- Navigate to the directory where you have downloaded the Crosswork Data Gateway release image.
- 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 1 NIC deployment with the host name as `cdg1-nodhcp` when using static addressing. Mandatory parameters in this list have been highlighted.

```
#### Required Parameters

### Deployment Settings

## Resource Profile
# How much memory and disk should be allocated?
# Default value: Crosswork-Cloud
Profile=Crosswork-Cloud

### Host Information

## Hostname
# Please enter the server's hostname (dg.localdomain)
Hostname=changeme

## Description
# Please enter a short, user friendly description for display in the Crosswork Controller
Description=changeme

### Passphrases

## dg-admin Passphrase
# Please enter a passphrase for the dg-admin user. It must be at least 8 characters.
dg-adminPassword=changeme

## dg-oper Passphrase
# Please enter a passphrase for the dg-oper user. It must be at least 8 characters.
dg-operPassword=changeme

### vNIC0 IPv4 Address

## vNIC0 IPv4 Method
# Skip or statically assign the vNIC0 IPv4 address
```

```

# Default value: DHCP
Vnic0IPv4Method=None

## vNIC0 IPv4 Address
# Please enter the server's IPv4 vNIC0 address if statically assigned
Vnic0IPv4Address=0.0.0.0

## vNIC0 IPv4 Netmask
# Please enter the server's IPv4 vNIC0 netmask if statically assigned
Vnic0IPv4Netmask=0.0.0.0

## vNIC0 IPv4 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv4SkipGateway=False

## vNIC0 IPv4 Gateway
# Please enter the server's IPv4 vNIC0 gateway if statically assigned
Vnic0IPv4Gateway=0.0.0.1

### vNIC0 IPv6 Address

## vNIC0 IPv6 Method
# Skip or statically assign the vNIC0 IPv6 address
# Default value: None
Vnic0IPv6Method=None

## vNIC0 IPv6 Address
# Please enter the server's IPv6 vNIC0 address if statically assigned
Vnic0IPv6Address=::0

## vNIC0 IPv6 Netmask
# Please enter the server's IPv6 vNIC0 netmask if statically assigned
Vnic0IPv6Netmask=64

## vNIC0 IPv6 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv6SkipGateway=False

## vNIC0 IPv6 Gateway
# Please enter the server's IPv6 vNIC0 gateway if statically assigned
Vnic0IPv6Gateway=::1

### DNS Servers

## DNS Address
# Please enter a space delimited list of DNS server addresses accessible from the Default Gateway
  role
DNS=changeme

## DNS Search Domain
# Please enter the DNS search domain
Domain=changeme

### NTPv4 Servers

## NTPv4 Servers
# Please enter a space delimited list of NTPv4 server hostnames or addresses accessible from the
  Default Gateway role
NTP=changeme

#### Optional Parameters

```

```
### Host Information

## Label
# An optional freeform label used by the Crosswork Controller to categorize and group multiple DG
  instances
Label=

## Allow Usable RFC 8190 Addresses
# If an address for vNIC0, vNIC1, vNIC2, or vNIC3 falls into a usable range identified by RFC 8190
  or its predecessors, reject, accept, or request confirmation during initial configuration
# Default value: Yes
AllowRFC8190=Yes

## Crosswork Data Gateway Private Key URI
# Please enter the optional Crosswork Data Gateway private key URI retrieved using SCP
  (user@host:/path/to/file)
DGCertKey=

## Crosswork Data Gateway Certificate File URI
# Please enter the optional Crosswork Data Gateway PEM formatted certificate file URI retrieved
  using SCP (user@host:/path/to/file)
DGCertChain=

## Crosswork Data Gateway Certificate File and Key Passphrase
# Please enter the SCP user passphrase to retrieve the Crosswork Data Gateway PEM formatted
  certificate file and private key
DGCertChainPwd=

### DNS Servers

## DNS Security Extensions
# Use DNS security extensions
# Default value: False
DNSSEC=False

## DNS over TLS
# Use DNS over TLS
# Default value: False
DNSTLS=False

## Multicast DNS
# Use multicast DNS
# Default value: False
mDNS=False

## Link-Local Multicast Name Resolution
# Use link-local multicast name resolution
# Default value: False
LLMNR=False

### NTPv4 Servers

## NTPv4 Authentication
# Use authentication for all NTPv4 servers
# Default value: False
NTPAuth=False

## NTPv4 Keys
# Please enter a space delimited list of IDs present in the key file. The number of IDs in the
  list must match the number of servers, even if some or all are the same ID.
NTPKey=

## NTPv4 Key File URI
# Please enter the optional Chrony key file retrieved using SCP (user@host:/path/to/file)
```

```
NTPKeyFile=

## NTPv4 Key File Passphrase
# Please enter the SCP user passphrase to retrieve the Chrony key file
NTPKeyFilePwd=

### Remote Syslog Servers

## Remote Syslog Server
# Send Syslog messages to a remote host
# Default value: False
UseRemoteSyslog=False

## Syslog Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the Syslog server accessible from the
  Default Gateway role
SyslogAddress=

## Syslog Server Port
# Please enter a Syslog port
# Default value: 514
SyslogPort=514

## Syslog Server Protocol
# Please enter the Syslog protocol
# Default value: UDP
SyslogProtocol=UDP

## Syslog over TLS
# Use Syslog over TLS (must use TCP or RELP as the protocol)
# Default value: False
SyslogTLS=False

## Syslog TLS Peer Name
# Please enter the Syslog server's hostname exactly as entered in the server certificate
  subjectAltName or subject common name
SyslogPeerName=

## Syslog Root Certificate File URI
# Please enter the optional Syslog root PEM formatted certificate file retrieved using SCP
  (user@host:/path/to/file)
SyslogCertChain=

## Syslog Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the Syslog PEM formatted certificate file
SyslogCertChainPwd=

### Remote Auditd Servers

## Remote auditd Server
# Send auditd messages to a remote host
# Default value: False
UseRemoteAuditd=False

## Auditd Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the auditd server accessible from the
  Default Gateway role
AuditdAddress=

## Auditd Server Port
# Please enter na auditd port
# Default value: 60
AuditdPort=60
```

```
### Controller Settings

## Proxy Server URL
# Please enter the optional HTTP/HTTPS proxy URL
ProxyURL=

## Proxy Server Bypass List
# Please enter an optional space delimited list of subnets and domains that will not be sent to
the proxy server
ProxyBypass=

## Authenticated Proxy Username
# Please enter an optional username for an authenticated proxy servers
ProxyUsername=

## Authenticated Proxy Passphrase
# Please enter an optional passphrase for an authenticated proxy server
ProxyPassphrase=

## HTTPS Proxy SSL/TLS Certificate File URI
# Please enter the optional HTTPS Proxy PEM formatted SSL/TLS certificate file URI retrieved using
SCP (user@host:/path/to/file). This will override the Controller SSL/TLS Certificate File URI.
ProxyCertChain=

## HTTPS Proxy SSL/TLS Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the HTTPS Proxy PEM formatted SSL/TLS certificate
file
ProxyCertChainPwd=

### Auto Enrollment Package Transfer

## Enrollment Destination Host and Path
# Please enter the optional SCP destination host and path to transfer the enrollment package using
SCP (user@host:/path/to/file)
EnrollmentURI=

## Enrollment Passphrase
# Please enter the optional SCP user passphrase to transfer the enrollment package
EnrollmentPassphrase=

#### Static Parameters - Do not change this section

### Deployment Settings

## Deployment Type
# What type of deployment is this?
# Default value: Crosswork Cloud
Deployment=Crosswork Cloud

### Host Information

## Data Disk Size
# Data disk size in GB mounted as /opt/dg/appdata
DGAppdataDisk=24

### vNIC Role Assignment

## Default Gateway
# The interface used as the Default Gateway and for DNS and NTP traffic
# Default value: eth0
NicDefaultGateway=eth0

## Administration
# The interface used for SSH access to the VM
```

```

# Default value: eth0
NicAdministration=eth0

## External Logging
# The interface used to send logs to an external logging server
# Default value: eth0
NicExternalLogging=eth0

## Management
# The interface used for enrollment and other management traffic
# Default value: eth0
NicManagement=eth0

## Control
# The interface used for destination, device, and collection configuration
# Default value: eth0
NicControl=eth0

## Northbound System Data
# The interface used to send collection data to the system destination
# Default value: eth0
NicNBSystemData=eth0

## Northbound External Data
# The interface used to send collection data to external destinations
# Default value: eth0
NicNBExternalData=eth0

## Southbound Data
# The interface used collect data from all devices
# Default value: eth0
NicSBData=eth0

```

- 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 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 1 NIC deployment with the host name as `cdg1-nodhcp` when using DHCP. Mandatory parameters in this list have been highlighted.

```

#### Required Parameters

### Deployment Settings

## Resource Profile
# How much memory and disk should be allocated?
# Default value: Crosswork-Cloud
Profile=Crosswork-Cloud

### Host Information

## Hostname
# Please enter the server's hostname (dg.localdomain)
Hostname=changeme

```

```
## Description
# Please enter a short, user friendly description for display in the Crosswork Controller
Description=changeme

### Passphrases

## dg-admin Passphrase
# Please enter a passphrase for the dg-admin user. It must be at least 8 characters.
dg-adminPassword=changeme

## dg-oper Passphrase
# Please enter a passphrase for the dg-oper user. It must be at least 8 characters.
dg-operPassword=changeme

### vNIC0 IPv4 Address

## vNIC0 IPv4 Method
# Skip or statically assign the vNIC0 IPv4 address
# Default value: DHCP
Vnic0IPv4Method=None

## vNIC0 IPv4 Address
# Please enter the server's IPv4 vNIC0 address if statically assigned
Vnic0IPv4Address=0.0.0.0

## vNIC0 IPv4 Netmask
# Please enter the server's IPv4 vNIC0 netmask if statically assigned
Vnic0IPv4Netmask=0.0.0.0

## vNIC0 IPv4 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv4SkipGateway=False

## vNIC0 IPv4 Gateway
# Please enter the server's IPv4 vNIC0 gateway if statically assigned
Vnic0IPv4Gateway=0.0.0.1

### vNIC0 IPv6 Address

## vNIC0 IPv6 Method
# Skip or statically assign the vNIC0 IPv6 address
# Default value: None
Vnic0IPv6Method=None

## vNIC0 IPv6 Address
# Please enter the server's IPv6 vNIC0 address if statically assigned
Vnic0IPv6Address>:::0

## vNIC0 IPv6 Netmask
# Please enter the server's IPv6 vNIC0 netmask if statically assigned
Vnic0IPv6Netmask=64

## vNIC0 IPv6 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv6SkipGateway=False

## vNIC0 IPv6 Gateway
# Please enter the server's IPv6 vNIC0 gateway if statically assigned
Vnic0IPv6Gateway>:::1

### DNS Servers
```

```

## DNS Address
# Please enter a space delimited list of DNS server addresses accessible from the Default Gateway
  role
DNS=changeme

## DNS Search Domain
# Please enter the DNS search domain
Domain=changeme

### NTPv4 Servers

## NTPv4 Servers
# Please enter a space delimited list of NTPv4 server hostnames or addresses accessible from the
  Default Gateway role
NTP=changeme

#### Optional Parameters

### Host Information

## Label
# An optional freeform label used by the Crosswork Controller to categorize and group multiple DG
  instances
Label=

## Allow Usable RFC 8190 Addresses
# If an address for vNIC0, vNIC1, vNIC2, or vNIC3 falls into a usable range identified by RFC 8190
  or its predecessors, reject, accept, or request confirmation during initial configuration
# Default value: Yes
AllowRFC8190=Yes

## Crosswork Data Gateway Private Key URI
# Please enter the optional Crosswork Data Gateway private key URI retrieved using SCP
  (user@host:/path/to/file)
DGCertKey=

## Crosswork Data Gateway Certificate File URI
# Please enter the optional Crosswork Data Gateway PEM formatted certificate file URI retrieved
  using SCP (user@host:/path/to/file)
DGCertChain=

## Crosswork Data Gateway Certificate File and Key Passphrase
# Please enter the SCP user passphrase to retrieve the Crosswork Data Gateway PEM formatted
  certificate file and private key
DGCertChainPwd=

### DNS Servers

## DNS Security Extensions
# Use DNS security extensions
# Default value: False
DNSSEC=False

## DNS over TLS
# Use DNS over TLS
# Default value: False
DNSTLS=False

## Multicast DNS
# Use multicast DNS
# Default value: False
mDNS=False

```



```
## Link-Local Multicast Name Resolution
# Use link-local multicast name resolution
# Default value: False
LLMNR=False

### NTPv4 Servers

## NTPv4 Authentication
# Use authentication for all NTPv4 servers
# Default value: False
NTPAuth=False

## NTPv4 Keys
# Please enter a space delimited list of IDs present in the key file. The number of IDs in the
list must match the number of servers, even if some or all are the same ID.
NTPKey=

## NTPv4 Key File URI
# Please enter the optional Chrony key file retrieved using SCP (user@host:/path/to/file)
NTPKeyFile=

## NTPv4 Key File Passphrase
# Please enter the SCP user passphrase to retrieve the Chrony key file
NTPKeyFilePwd=

### Remote Syslog Servers

## Remote Syslog Server
# Send Syslog messages to a remote host
# Default value: False
UseRemoteSyslog=False

## Syslog Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the Syslog server accessible from the
Default Gateway role
SyslogAddress=

## Syslog Server Port
# Please enter a Syslog port
# Default value: 514
SyslogPort=514

## Syslog Server Protocol
# Please enter the Syslog protocol
# Default value: UDP
SyslogProtocol=UDP

## Syslog over TLS
# Use Syslog over TLS (must use TCP or RELP as the protocol)
# Default value: False
SyslogTLS=False

## Syslog TLS Peer Name
# Please enter the Syslog server's hostname exactly as entered in the server certificate
subjectAltName or subject common name
SyslogPeerName=

## Syslog Root Certificate File URI
# Please enter the optional Syslog root PEM formatted certificate file retrieved using SCP
(user@host:/path/to/file)
SyslogCertChain=

## Syslog Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the Syslog PEM formatted certificate file
```

```
SyslogCertChainPwd=

### Remote Auditd Servers

## Remote auditd Server
# Send auditd messages to a remote host
# Default value: False
UseRemoteAuditd=False

## Auditd Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the auditd server accessible from the
  Default Gateway role
AuditdAddress=

## Auditd Server Port
# Please enter na auditd port
# Default value: 60
AuditdPort=60

### Controller Settings

## Proxy Server URL
# Please enter the optional HTTP/HTTPS proxy URL
ProxyURL=

## Proxy Server Bypass List
# Please enter an optional space delimited list of subnets and domains that will not be sent to
the proxy server
ProxyBypass=

## Authenticated Proxy Username
# Please enter an optional username for an authenticated proxy servers
ProxyUsername=

## Authenticated Proxy Passphrase
# Please enter an optional passphrase for an authenticated proxy server
ProxyPassphrase=

## HTTPS Proxy SSL/TLS Certificate File URI
# Please enter the optional HTTPS Proxy PEM formatted SSL/TLS certificate file URI retrieved using
  SCP (user@host:/path/to/file). This will override the Controller SSL/TLS Certificate File URI.
ProxyCertChain=

## HTTPS Proxy SSL/TLS Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the HTTPS Proxy PEM formatted SSL/TLS certificate
  file
ProxyCertChainPwd=

### Auto Enrollment Package Transfer

## Enrollment Destination Host and Path
# Please enter the optional SCP destination host and path to transfer the enrollment package using
  SCP (user@host:/path/to/file)
EnrollmentURI=

## Enrollment Passphrase
# Please enter the optional SCP user passphrase to transfer the enrollment package
EnrollmentPassphrase=

#### Static Parameters - Do not change this section

### Deployment Settings

## Deployment Type
```

```

# What type of deployment is this?
# Default value: Crosswork Cloud
Deployment=Crosswork Cloud

### Host Information

## Data Disk Size
# Data disk size in GB mounted as /opt/dg/appdata
DGAppdataDisk=24

### vNIC Role Assignment

## Default Gateway
# The interface used as the Default Gateway and for DNS and NTP traffic
# Default value: eth0
NicDefaultGateway=eth0

## Administration
# The interface used for SSH access to the VM
# Default value: eth0
NicAdministration=eth0

## External Logging
# The interface used to send logs to an external logging server
# Default value: eth0
NicExternalLogging=eth0

## Management
# The interface used for enrollment and other management traffic
# Default value: eth0
NicManagement=eth0

## Control
# The interface used for destination, device, and collection configuration
# Default value: eth0
NicControl=eth0

## Northbound System Data
# The interface used to send collection data to the system destination
# Default value: eth0
NicNBSystemData=eth0

## Northbound External Data
# The interface used to send collection data to external destinations
# Default value: eth0
NicNBExternalData=eth0

## Southbound Data
# The interface used collect data from all devices
# Default value: eth0
NicSBData=eth0

```

- 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 24 GB second data disk.

```
openstack volume create --size
```

Sample commands:

```
openstack volume create --size 24 cdg-voll
```

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 1 NICs using static addressing:

```
openstack port create --network network1 --fixed-ip subnet=subnet1,ip-address=10.10.11.101
mgmt-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
```

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 1 NIC that uses static addressing

```
openstack server create --flavor <flavor_name> --image <image_name> --port <mgmt-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
--config-drive True --user-data config-nodhcp-cdgl.txt --block-device-mapping
vdb=cdgl:::true cdgl-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 1 NIC 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 <flavor_name> --image <image_name> --network <network1>
--config-drive True --user-data <config.txt> --host <boot_drive>
--block-device-mapping vdb=<volume_name>:::true <CDG_hostname>
```

OR

```
openstack server create --config-drive true --flavor cdg --image --key-name default --network
--security-group --user-data
```

Note The number of networks in the command to install the VMs depends 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= ; network3-nodhcp=	cdg-cloud-bios-345	cdg-cloud
9c6d913f-c24b-43a3-9816-f865e58e7e95	cdg-bios-nodhcp	ACTIVE	network1-nodhcp= ; network2-nodhcp= ; network3-nodhcp=	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 log in 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 [Obtain the Enrollment Package, on page 72](#).

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 one or more VMs.
- 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](https://www.cisco.com) to your local machine or a location on your local network that is accessible to your OpenStack. In these instructions, we 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.**

- Navigate to the directory where you have downloaded the Crosswork Data Gateway release image.
- 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.txt` file for each of the VMs.

This is a sample `config.txt` file for a 1 NIC deployment with the host name as `cdg1-nodhcp` when using static addressing. Mandatory parameters in this list have been highlighted.

```
#### Required Parameters

### Deployment Settings

## Resource Profile
# How much memory and disk should be allocated?
# Default value: Crosswork-Cloud
Profile=Crosswork-Cloud
```

```
### Host Information

## Hostname
# Please enter the server's hostname (dg.localdomain)
Hostname=changeme

## Description
# Please enter a short, user friendly description for display in the Crosswork Controller
Description=changeme

### Passphrases

## dg-admin Passphrase
# Please enter a passphrase for the dg-admin user. It must be at least 8 characters.
dg-adminPassword=changeme

## dg-oper Passphrase
# Please enter a passphrase for the dg-oper user. It must be at least 8 characters.
dg-operPassword=changeme

### vNIC0 IPv4 Address

## vNIC0 IPv4 Method
# Skip or statically assign the vNIC0 IPv4 address
# Default value: DHCP
Vnic0IPv4Method=None

## vNIC0 IPv4 Address
# Please enter the server's IPv4 vNIC0 address if statically assigned
Vnic0IPv4Address=0.0.0.0

## vNIC0 IPv4 Netmask
# Please enter the server's IPv4 vNIC0 netmask if statically assigned
Vnic0IPv4Netmask=0.0.0.0

## vNIC0 IPv4 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv4SkipGateway=False

## vNIC0 IPv4 Gateway
# Please enter the server's IPv4 vNIC0 gateway if statically assigned
Vnic0IPv4Gateway=0.0.0.1

### vNIC0 IPv6 Address

## vNIC0 IPv6 Method
# Skip or statically assign the vNIC0 IPv6 address
# Default value: None
Vnic0IPv6Method=None

## vNIC0 IPv6 Address
# Please enter the server's IPv6 vNIC0 address if statically assigned
Vnic0IPv6Address>:::0

## vNIC0 IPv6 Netmask
# Please enter the server's IPv6 vNIC0 netmask if statically assigned
Vnic0IPv6Netmask=64

## vNIC0 IPv6 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv6SkipGateway=False
```



```
## vNIC0 IPv6 Gateway
# Please enter the server's IPv6 vNIC0 gateway if statically assigned
Vnic0IPv6Gateway=::1

### DNS Servers

## DNS Address
# Please enter a space delimited list of DNS server addresses accessible from the Default Gateway
role
DNS=changeme

## DNS Search Domain
# Please enter the DNS search domain
Domain=changeme

### NTPv4 Servers

## NTPv4 Servers
# Please enter a space delimited list of NTPv4 server hostnames or addresses accessible from
the Default Gateway role
NTP=changeme

#### Optional Parameters

### Host Information

## Label
# An optional freeform label used by the Crosswork Controller to categorize and group multiple
DG instances
Label=

## Allow Usable RFC 8190 Addresses
# If an address for vNIC0, vNIC1, vNIC2, or vNIC3 falls into a usable range identified by RFC
8190 or its predecessors, reject, accept, or request confirmation during initial configuration
# Default value: Yes
AllowRFC8190=Yes

## Crosswork Data Gateway Private Key URI
# Please enter the optional Crosswork Data Gateway private key URI retrieved using SCP
(user@host:/path/to/file)
DGCertKey=

## Crosswork Data Gateway Certificate File URI
# Please enter the optional Crosswork Data Gateway PEM formatted certificate file URI retrieved
using SCP (user@host:/path/to/file)
DGCertChain=

## Crosswork Data Gateway Certificate File and Key Passphrase
# Please enter the SCP user passphrase to retrieve the Crosswork Data Gateway PEM formatted
certificate file and private key
DGCertChainPwd=

### DNS Servers

## DNS Security Extensions
# Use DNS security extensions
# Default value: False
DNSSEC=False

## DNS over TLS
# Use DNS over TLS
# Default value: False
DNSTLS=False
```

```
## Multicast DNS
# Use multicast DNS
# Default value: False
mDNS=False

## Link-Local Multicast Name Resolution
# Use link-local multicast name resolution
# Default value: False
LLMNR=False

### NTPv4 Servers

## NTPv4 Authentication
# Use authentication for all NTPv4 servers
# Default value: False
NTPAuth=False

## NTPv4 Keys
# Please enter a space delimited list of IDs present in the key file. The number of IDs in the
# list must match the number of servers, even if some or all are the same ID.
NTPKey=

## NTPv4 Key File URI
# Please enter the optional Chrony key file retrieved using SCP (user@host:/path/to/file)
NTPKeyFile=

## NTPv4 Key File Passphrase
# Please enter the SCP user passphrase to retrieve the Chrony key file
NTPKeyFilePwd=

### Remote Syslog Servers

## Remote Syslog Server
# Send Syslog messages to a remote host
# Default value: False
UseRemoteSyslog=False

## Syslog Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the Syslog server accessible from
# the Default Gateway role
SyslogAddress=

## Syslog Server Port
# Please enter a Syslog port
# Default value: 514
SyslogPort=514

## Syslog Server Protocol
# Please enter the Syslog protocol
# Default value: UDP
SyslogProtocol=UDP

## Syslog over TLS
# Use Syslog over TLS (must use TCP or RELP as the protocol)
# Default value: False
SyslogTLS=False

## Syslog TLS Peer Name
# Please enter the Syslog server's hostname exactly as entered in the server certificate
# subjectAltName or subject common name
SyslogPeerName=

## Syslog Root Certificate File URI
```

```
# Please enter the optional Syslog root PEM formatted certificate file retrieved using SCP
(user@host:/path/to/file)
SyslogCertChain=

## Syslog Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the Syslog PEM formatted cetificate file
SyslogCertChainPwd=

### Remote Auditd Servers

## Remote auditd Server
# Send auditd messages to a remote host
# Default value: False
UseRemoteAuditd=False

## Auditd Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the auditd server accessible from
the Default Gateway role
AuditdAddress=

## Auditd Server Port
# Please enter na auditd port
# Default value: 60
AuditdPort=60

### Controller Settings

## Proxy Server URL
# Please enter the optional HTTP/HTTPS proxy URL
ProxyURL=

## Proxy Server Bypass List
# Please enter an optional space delimited list of subnets and domains that will not be sent to
the proxy server
ProxyBypass=

## Authenticated Proxy Username
# Please enter an optional username for an authenticated proxy servers
ProxyUsername=

## Authenticated Proxy Passphrase
# Please enter an optional passphrase for an authenticated proxy server
ProxyPassphrase=

## HTTPS Proxy SSL/TLS Certificate File URI
# Please enter the optional HTTPS Proxy PEM formatted SSL/TLS certificate file URI retrieved
using SCP (user@host:/path/to/file). This will override the Controller SSL/TLS Certificate File
URI.
ProxyCertChain=

## HTTPS Proxy SSL/TLS Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the HTTPS Proxy PEM formatted SSL/TLS
certificate file
ProxyCertChainPwd=

### Auto Enrollment Package Transfer

## Enrollment Destination Host and Path
# Please enter the optional SCP destination host and path to transfer the enrollment package
using SCP (user@host:/path/to/file)
EnrollmentURI=

## Enrollment Passphrase
# Please enter the optional SCP user passphrase to transfer the enrollment package
```

```

EnrollmentPassphrase=

#### Static Parameters - Do not change this section

### Deployment Settings

## Deployment Type
# What type of deployment is this?
# Default value: Crosswork Cloud
Deployment=Crosswork Cloud

### Host Information

## Data Disk Size
# Data disk size in GB mounted as /opt/dg/appdata
DGAppdataDisk=24

### vNIC Role Assignment

## Default Gateway
# The interface used as the Default Gateway and for DNS and NTP traffic
# Default value: eth0
NicDefaultGateway=eth0

## Administration
# The interface used for SSH access to the VM
# Default value: eth0
NicAdministration=eth0

## External Logging
# The interface used to send logs to an external logging server
# Default value: eth0
NicExternalLogging=eth0

## Management
# The interface used for enrollment and other management traffic
# Default value: eth0
NicManagement=eth0

## Control
# The interface used for destination, device, and collection configuration
# Default value: eth0
NicControl=eth0

## Northbound System Data
# The interface used to send collection data to the system destination
# Default value: eth0
NicNBSystemData=eth0

## Northbound External Data
# The interface used to send collection data to external destinations
# Default value: eth0
NicNBExternalData=eth0

## Southbound Data
# The interface used collect data from all devices
# Default value: eth0
NicSBData=eth0

```

- 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 1 NIC deployment with the host name as `cdg1-nodhcp` when using static addressing. Mandatory parameters in this list have been highlighted.

```
#### Required Parameters

### Deployment Settings

## Resource Profile
# How much memory and disk should be allocated?
# Default value: Crosswork-Cloud
Profile=Crosswork-Cloud

### Host Information

## Hostname
# Please enter the server's hostname (dg.localdomain)
Hostname=changeme

## Description
# Please enter a short, user friendly description for display in the Crosswork Controller
Description=changeme

### Passphrases

## dg-admin Passphrase
# Please enter a passphrase for the dg-admin user. It must be at least 8 characters.
dg-adminPassword=changeme

## dg-oper Passphrase
# Please enter a passphrase for the dg-oper user. It must be at least 8 characters.
dg-operPassword=changeme

### vNIC0 IPv4 Address

## vNIC0 IPv4 Method
# Skip or statically assign the vNIC0 IPv4 address
# Default value: DHCP
Vnic0IPv4Method=None

## vNIC0 IPv4 Address
# Please enter the server's IPv4 vNIC0 address if statically assigned
Vnic0IPv4Address=0.0.0.0

## vNIC0 IPv4 Netmask
# Please enter the server's IPv4 vNIC0 netmask if statically assigned
Vnic0IPv4Netmask=0.0.0.0

## vNIC0 IPv4 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv4SkipGateway=False

## vNIC0 IPv4 Gateway
# Please enter the server's IPv4 vNIC0 gateway if statically assigned
```

```

Vnic0IPv4Gateway=0.0.0.1

### vNIC0 IPv6 Address

## vNIC0 IPv6 Method
# Skip or statically assign the vNIC0 IPv6 address
# Default value: None
Vnic0IPv6Method=None

## vNIC0 IPv6 Address
# Please enter the server's IPv6 vNIC0 address if statically assigned
Vnic0IPv6Address=::0

## vNIC0 IPv6 Netmask
# Please enter the server's IPv6 vNIC0 netmask if statically assigned
Vnic0IPv6Netmask=64

## vNIC0 IPv6 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv6SkipGateway=False

## vNIC0 IPv6 Gateway
# Please enter the server's IPv6 vNIC0 gateway if statically assigned
Vnic0IPv6Gateway=::1

### DNS Servers

## DNS Address
# Please enter a space delimited list of DNS server addresses accessible from the Default Gateway
  role
DNS=changeme

## DNS Search Domain
# Please enter the DNS search domain
Domain=changeme

### NTPv4 Servers

## NTPv4 Servers
# Please enter a space delimited list of NTPv4 server hostnames or addresses accessible from
the Default Gateway role
NTP=changeme

#### Optional Parameters

### Host Information

## Label
# An optional freeform label used by the Crosswork Controller to categorize and group multiple
  DG instances
Label=

## Allow Usable RFC 8190 Addresses
# If an address for vNIC0, vNIC1, vNIC2, or vNIC3 falls into a usable range identified by RFC
8190 or its predecessors, reject, accept, or request confirmation during initial configuration
# Default value: Yes
AllowRFC8190=Yes

## Crosswork Data Gateway Private Key URI
# Please enter the optional Crosswork Data Gateway private key URI retrieved using SCP
(user@host:/path/to/file)
DGCertKey=

```

```
## Crosswork Data Gateway Certificate File URI
# Please enter the optional Crosswork Data Gateway PEM formatted certificate file URI retrieved
using SCP (user@host:/path/to/file)
DGCertChain=

## Crosswork Data Gateway Certificate File and Key Passphrase
# Please enter the SCP user passphrase to retrieve the Crosswork Data Gateway PEM formatted
certificate file and private key
DGCertChainPwd=

### DNS Servers

## DNS Security Extensions
# Use DNS security extensions
# Default value: False
DNSSEC=False

## DNS over TLS
# Use DNS over TLS
# Default value: False
DNSTLS=False

## Multicast DNS
# Use multicast DNS
# Default value: False
mDNS=False

## Link-Local Multicast Name Resolution
# Use link-local multicast name resolution
# Default value: False
LLMNR=False

### NTPv4 Servers

## NTPv4 Authentication
# Use authentication for all NTPv4 servers
# Default value: False
NTPAuth=False

## NTPv4 Keys
# Please enter a space delimited list of IDs present in the key file. The number of IDs in the
list must match the number of servers, even if some or all are the same ID.
NTPKey=

## NTPv4 Key File URI
# Please enter the optional Chrony key file retrieved using SCP (user@host:/path/to/file)
NTPKeyFile=

## NTPv4 Key File Passphrase
# Please enter the SCP user passphrase to retrieve the Chrony key file
NTPKeyFilePwd=

### Remote Syslog Servers

## Remote Syslog Server
# Send Syslog messages to a remote host
# Default value: False
UseRemoteSyslog=False

## Syslog Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the Syslog server accessible from
the Default Gateway role
SyslogAddress=
```

```
## Syslog Server Port
# Please enter a Syslog port
# Default value: 514
SyslogPort=514

## Syslog Server Protocol
# Please enter the Syslog protocol
# Default value: UDP
SyslogProtocol=UDP

## Syslog over TLS
# Use Syslog over TLS (must use TCP or RELP as the protocol)
# Default value: False
SyslogTLS=False

## Syslog TLS Peer Name
# Please enter the Syslog server's hostname exactly as entered in the server certificate
subjectAltName or subject common name
SyslogPeerName=

## Syslog Root Certificate File URI
# Please enter the optional Syslog root PEM formatted certificate file retrieved using SCP
(user@host:/path/to/file)
SyslogCertChain=

## Syslog Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the Syslog PEM formatted certificate file
SyslogCertChainPwd=

### Remote Auditd Servers

## Remote auditd Server
# Send auditd messages to a remote host
# Default value: False
UseRemoteAuditd=False

## Auditd Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the auditd server accessible from
the Default Gateway role
AuditdAddress=

## Auditd Server Port
# Please enter na auditd port
# Default value: 60
AuditdPort=60

### Controller Settings

## Proxy Server URL
# Please enter the optional HTTP/HTTPS proxy URL
ProxyURL=

## Proxy Server Bypass List
# Please enter an optional space delimited list of subnets and domains that will not be sent to
the proxy server
ProxyBypass=

## Authenticated Proxy Username
# Please enter an optional username for an authenticated proxy servers
ProxyUsername=

## Authenticated Proxy Passphrase
# Please enter an optional passphrase for an authenticated proxy server
ProxyPassphrase=
```



```
## HTTPS Proxy SSL/TLS Certificate File URI
# Please enter the optional HTTPS Proxy PEM formatted SSL/TLS certificate file URI retrieved
using SCP (user@host:/path/to/file). This will override the Controller SSL/TLS Certificate File
URI.
ProxyCertChain=

## HTTPS Proxy SSL/TLS Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the HTTPS Proxy PEM formatted SSL/TLS
certificate file
ProxyCertChainPwd=

### Auto Enrollment Package Transfer

## Enrollment Destination Host and Path
# Please enter the optional SCP destination host and path to transfer the enrollment package
using SCP (user@host:/path/to/file)
EnrollmentURI=

## Enrollment Passphrase
# Please enter the optional SCP user passphrase to transfer the enrollment package
EnrollmentPassphrase=

#### Static Parameters - Do not change this section

### Deployment Settings

## Deployment Type
# What type of deployment is this?
# Default value: Crosswork Cloud
Deployment=Crosswork Cloud

### Host Information

## Data Disk Size
# Data disk size in GB mounted as /opt/dg/appdata
DGAppdataDisk=24

### vNIC Role Assignment

## Default Gateway
# The interface used as the Default Gateway and for DNS and NTP traffic
# Default value: eth0
NicDefaultGateway=eth0

## Administration
# The interface used for SSH access to the VM
# Default value: eth0
NicAdministration=eth0

## External Logging
# The interface used to send logs to an external logging server
# Default value: eth0
NicExternalLogging=eth0

## Management
# The interface used for enrollment and other management traffic
# Default value: eth0
NicManagement=eth0

## Control
# The interface used for destination, device, and collection configuration
# Default value: eth0
NicControl=eth0
```

```
## Northbound System Data
# The interface used to send collection data to the system destination
# Default value: eth0
NicNBSystemData=eth0

## Northbound External Data
# The interface used to send collection data to external destinations
# Default value: eth0
NicNBExternalData=eth0

## Southbound Data
# The interface used collect data from all devices
# Default value: eth0
NicSBData=eth0
```

- 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**.

Flavor Information *
Flavor Access

Name *

ID ⓘ

VCPUs *

RAM (MB) *

Root Disk (GB) *

Ephemeral Disk (GB)

Swap Disk (MB)

RX/TX Factor

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

Cancel
Create Flavor

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.

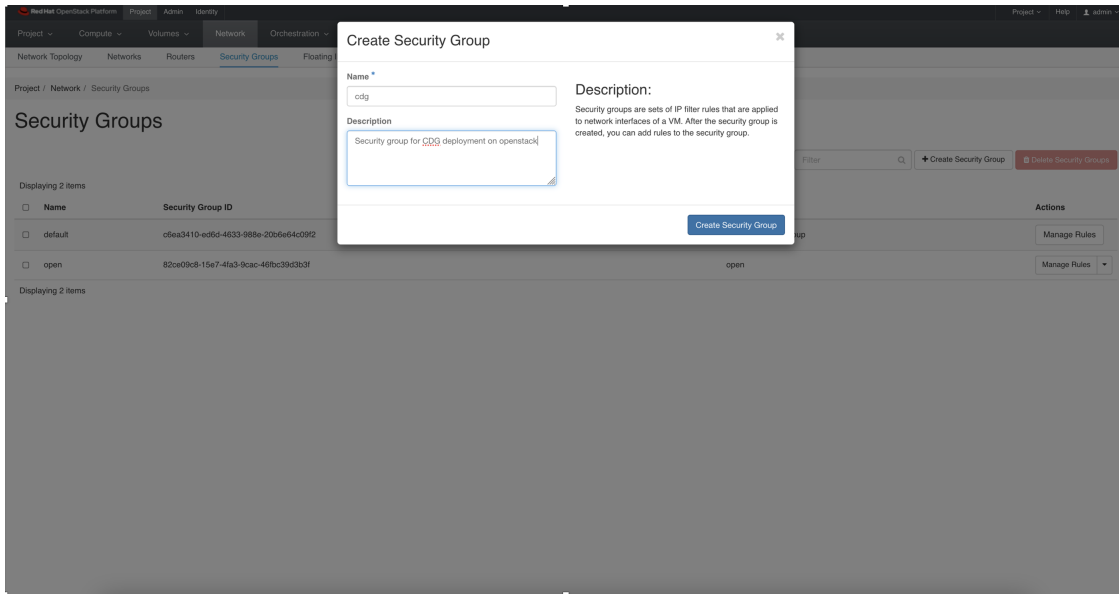
b) Click **Create Image**.

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.

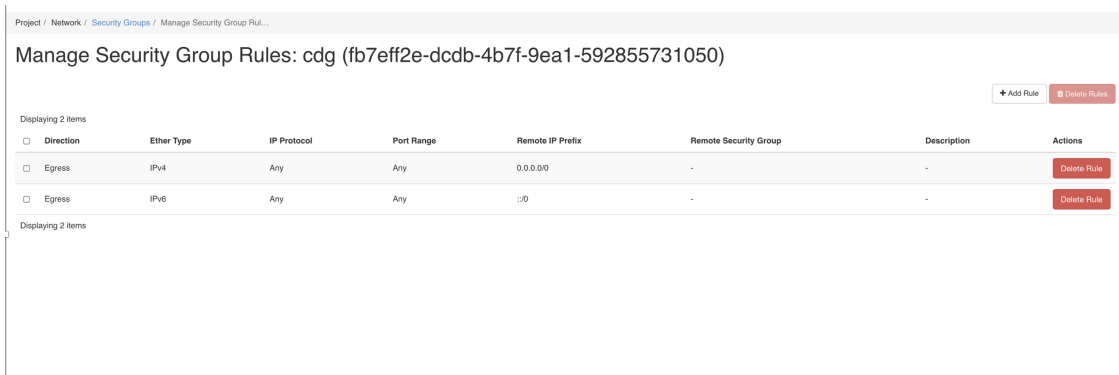
Note You can create security groups and apply them to the VM even after the Crosswork Data Gateway is deployed.

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



- 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.



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

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.

Enable Admin State

Device ID

Device Owner

Specify IP address or subnet
Fixed IP Address

Fixed IP Address*
192.168.1.101

MAC Address

Port Security

VNIC Type
Normal

Binding: Host

Cancel Create

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.

Launch Instance

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)
3%

2 Current Usage
1 Added
97 Remaining

✕ Cancel < Back Next > Launch Instance

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 ✕

Details

Source

Flavor ^{*}

Networks ^{*}

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

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

Q 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

✕ Cancel
< Back
Next >
Launch Instance

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**.

Launch Instance ✕ ?

Details

Source

Flavor

Networks [•]

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

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 Select one

Q Click here for filters or full text search. ✕

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public
------	-------	-----	------------	-----------	----------------	--------

✕ Cancel < Back Next > Launch Instance

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 moves 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

Details ^{*}

Source

Flavor ^{*}

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

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	↑

✕ Cancel < Back Next > Launch Instance

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. .

Launch Instance

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	on subnet subnet2-nodhcp	Up	Down

▼ Available 2 Select one

Q Filter

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

✕ Cancel < Back Next > Launch Instance

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.

Launch Instance
✕

- Details *
- Source
- Flavor *
- Networks *
- Network Ports
- Security Groups
- Key Pair
- Configuration
- Server Groups
- Scheduler Hints
- Metadata

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 ↑

✕ Cancel
< Back
Next >
Launch Instance

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.

Launch Instance ✕

?

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

Source Load Customization Script from a file
 No file chosen

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

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Disk Partition
 Automatic

Configuration Drive

```

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

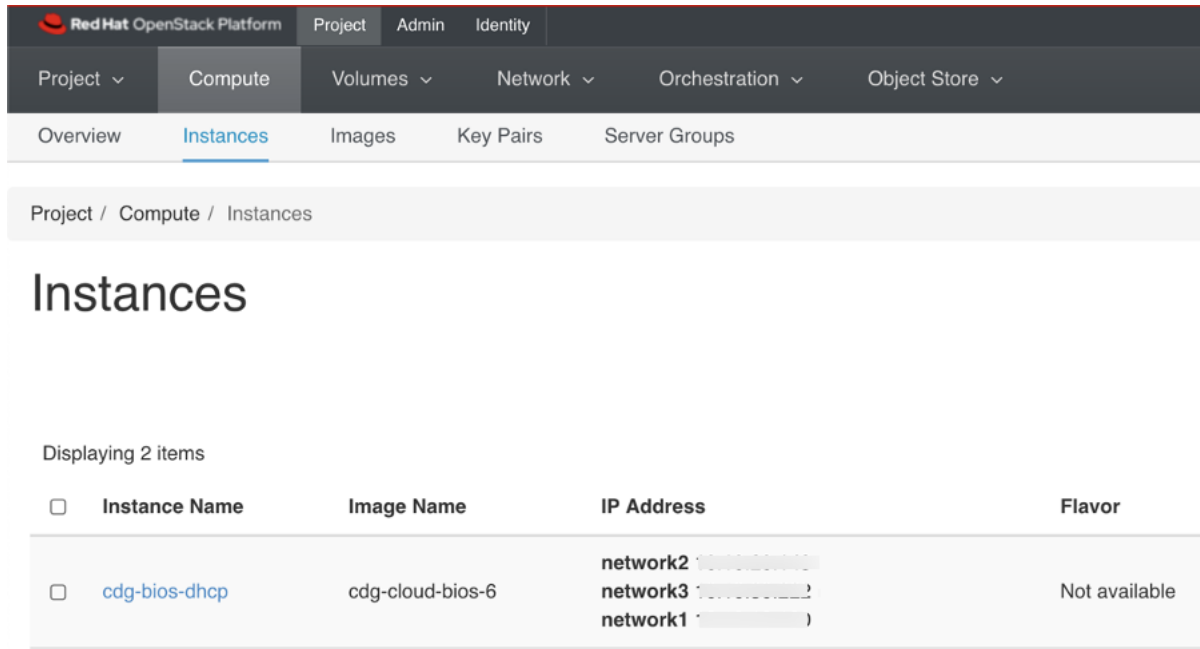
Step 19 Click **Launch Instance**.

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.



Red Hat OpenStack Platform Project Admin Identity

Project Compute Volumes Network Orchestration Object Store

Overview Instances Images Key Pairs Server Groups

Project / Compute / Instances

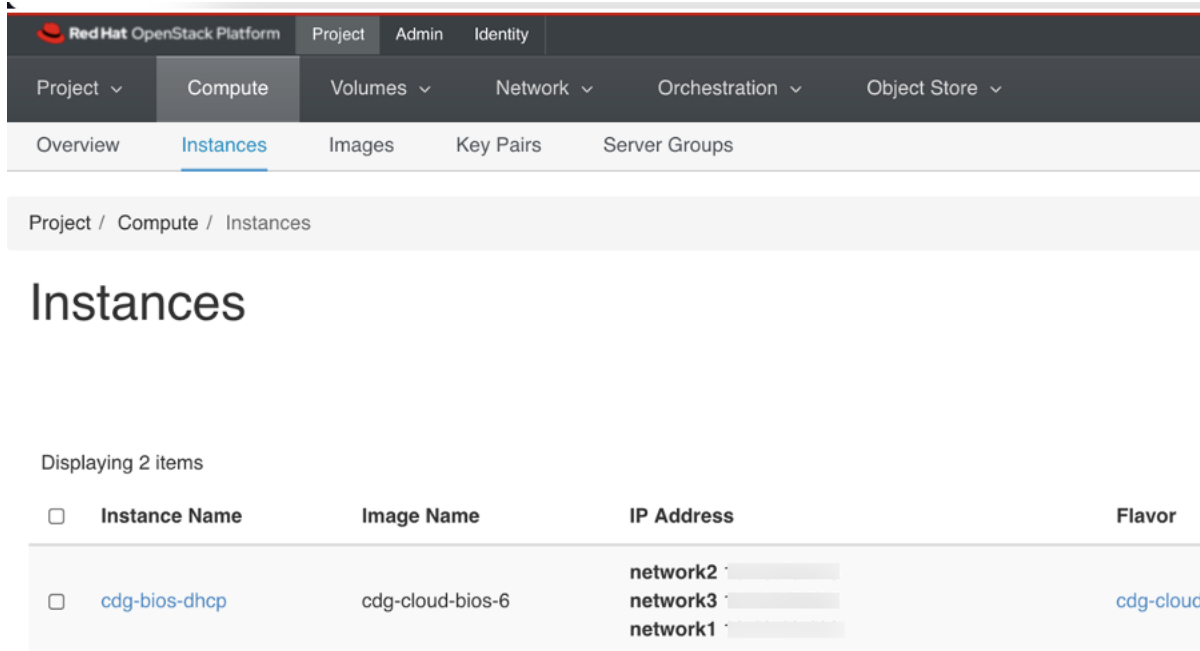
Instances

Displaying 2 items

<input type="checkbox"/>	Instance Name	Image Name	IP Address	Flavor
<input type="checkbox"/>	cdg-bios-dhcp	cdg-cloud-bios-6	network2 network3 network1	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**.

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



Red Hat OpenStack Platform Project Admin Identity

Project Compute Volumes Network Orchestration Object Store

Overview Instances Images Key Pairs Server Groups

Project / Compute / Instances

Instances

Displaying 2 items

<input type="checkbox"/>	Instance Name	Image Name	IP Address	Flavor
<input type="checkbox"/>	cdg-bios-dhcp	cdg-cloud-bios-6	network2 network3 network1	cdg-cloud

- 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 72](#).

Install Crosswork Data Gateway on Amazon EC2

You can install the Crosswork Data Gateway on Amazon EC2 in one of the following ways:

- [Install Crosswork Data Gateway on Amazon EC2 using CloudFormation Template, on page 62](#)
- [Install Crosswork Data Gateway on Amazon EC2 Manually, on page 63](#)

Install Crosswork Data Gateway on Amazon EC2 using CloudFormation Template

Installing Crosswork Data Gateway on EC2 using CloudFormation (CF) templates involves creating a template (YAML formatted text file) which describes the VM resources and their properties. Whenever you create a stack, CloudFormation provisions the resources that are described in your template and installs the VMs.

Before you begin

- Ensure that you have met the requirements specified in the section [Amazon EC2 Settings](#).
- All the Cisco Crosswork VMs have been installed.

Step 1 Log in to AWS and search for the CloudFormation service. The CloudFormation dashboard opens.

Step 2 Click **Stacks** from the side menu.

All existing stacks in the environment are displayed here.

Step 3 In **Step 1 - Specify template**, select the following settings:

- a) Under **Prepare template**, select **Template is ready**.
- b) Under **Template source**, select **Upload a template file**.
- c) Click **Choose file**, and select your CF template (.yaml file).
- d) Click **Next**.

Step 4 In **Step 2 - Specify stack details**, enter relevant values for the stack name and each parameter field, and click **Next**.

Note The parameter field names visible in this window are defined by the parameters in the CF template.

Step 5 In **Step 3 - Configure stack options**, enter the relevant values for the settings based on your production preferences. Click **Next** to continue.

Step 6 In **Step 4 - Review**, review the settings you have configured.

Step 7 Select the acknowledgment checkbox, and click **Create stack** to start the VM installation.

Verify that the VMs were installed successfully

1. In the CloudFormation dashboard, click **Stacks** from the side menu to view the list of stacks.
2. Select the stack you installed. The stack details are displayed on the right. Click on each tab in this window to view details of the stack creation.

The status of the stack in the **Events** tab will be **CREATE_IN_PROGRESS**

3. After the stack has been created:
 - The status of the stack changes to **CREATE_COMPLETE** and the **Logical ID** displays the stack name.
 - The **Resources** tab displays details of the all the resources that the CF template has created, including the physical IDs.
 - The **Output** tab has details of the VM's interface IP addresses.
4. Click the **Physical ID** of the VM instance in your stack.

Doing this will open the Instances window in the EC2 dashboard with details of the selected VM instance.
5. Click **Connect** (top right corner).
6. In the **Connect to instance** window that appears, click the **EC2 Serial Control** tab and click **Connect**.
7. Click on the **EC2 serial console** tab. Click **Connect** to connect to the console of the VM.
8. Log in to the VM as a `dg-admin` or `dg-oper` user using the password you configured.

The Interactive Console of the VM is displayed on successful login.

Install Crosswork Data Gateway on Amazon EC2 Manually

Follow these steps to install Crosswork Data Gateway on EC2.



Note

- The Launch Instance workflow offers a wide range of launch options that you can configure based on your requirements. The following procedure lists the mandatory settings that should be configured to install the Crosswork Data Gateway VM successfully.
 - The steps in this procedure explain the installation of a Crosswork Data Gateway VM with one interface.
-

Before you begin

Ensure that you have the following information ready before deploying the Crosswork Data Gateway VMs:

- Ensure that you have met the requirements specified in [Amazon EC2 Settings](#).
- All the Cisco Crosswork VMs are installed.
- Decide the number of Crosswork Data Gateway VM instances to install.

- Have the Crosswork Data Gateway AMI image saved in a location accessible to your AWS.

Step 1 Prepare the user data for the Crosswork Data Gateway VMs.

- a) Prepare the user data for Crosswork Data Gateway VMs. See [Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2](#) for more information about the parameters. Sample user data for a VM is attached here for your reference. Important parameters have been highlighted.

For Amazon EC2 deployment, this document assumes that a user of this procedure is familiar with AWS and the CloudFormation concepts, and as such, the CF template creation is out of the scope of this document. In the example, `AwsIamRole` is an optional parameter for the Amazon EC2 deployment.

```
##### Required Parameters

### Deployment Settings

## Resource Profile
# How much memory and disk should be allocated?
# Default value: Crosswork-Cloud
Profile=Crosswork-Cloud

### Host Information

## Hostname
# Please enter the server's hostname (dg.localdomain)
Hostname=changeme

## Description
# Please enter a short, user friendly description for display in the Crosswork Controller
Description=changeme

### Passphrases

## dg-admin Passphrase
# Please enter a passphrase for the dg-admin user. It must be at least 8 characters.
dg-adminPassword=changeme

## dg-oper Passphrase
# Please enter a passphrase for the dg-oper user. It must be at least 8 characters.
dg-operPassword=changeme

### vNIC0 IPv4 Address

## vNIC0 IPv4 Method
# Skip or statically assign the vNIC0 IPv4 address
# Default value: DHCP
Vnic0IPv4Method=None

## vNIC0 IPv4 Address
# Please enter the server's IPv4 vNIC0 address if statically assigned
Vnic0IPv4Address=0.0.0.0

## vNIC0 IPv4 Netmask
# Please enter the server's IPv4 vNIC0 netmask if statically assigned
Vnic0IPv4Netmask=0.0.0.0

## vNIC0 IPv4 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv4SkipGateway=False
```



```
## vNIC0 IPv4 Gateway
# Please enter the server's IPv4 vNIC0 gateway if statically assigned
Vnic0IPv4Gateway=0.0.0.1

### vNIC0 IPv6 Address

## vNIC0 IPv6 Method
# Skip or statically assign the vNIC0 IPv6 address
# Default value: None
Vnic0IPv6Method=None

## vNIC0 IPv6 Address
# Please enter the server's IPv6 vNIC0 address if statically assigned
Vnic0IPv6Address>:::0

## vNIC0 IPv6 Netmask
# Please enter the server's IPv6 vNIC0 netmask if statically assigned
Vnic0IPv6Netmask=64

## vNIC0 IPv6 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv6SkipGateway=False

## vNIC0 IPv6 Gateway
# Please enter the server's IPv6 vNIC0 gateway if statically assigned
Vnic0IPv6Gateway>:::1

### DNS Servers

## DNS Address
# Please enter a space delimited list of DNS server addresses accessible from the Default Gateway
  role
DNS=changeme

## DNS Search Domain
# Please enter the DNS search domain
Domain=changeme

### NTPv4 Servers

## NTPv4 Servers
# Please enter a space delimited list of NTPv4 server hostnames or addresses accessible from the
  Default Gateway role
NTP=changeme

#### Optional Parameters

### Host Information

## Label
# An optional freeform label used by the Crosswork Controller to categorize and group multiple DG
  instances
Label=

## Allow Usable RFC 8190 Addresses
# If an address for vNIC0, vNIC1, vNIC2, or vNIC3 falls into a usable range identified by RFC 8190
  or its predecessors, reject, accept, or request confirmation during initial configuration
# Default value: Yes
AllowRFC8190=Yes

## Crosswork Data Gateway Private Key URI
# Please enter the optional Crosswork Data Gateway private key URI retrieved using SCP
  (user@host:/path/to/file)
```

```

DGCertKey=

## Crosswork Data Gateway Certificate File URI
# Please enter the optional Crosswork Data Gateway PEM formatted certificate file URI retrieved
using SCP (user@host:/path/to/file)
DGCertChain=

## Crosswork Data Gateway Certificate File and Key Passphrase
# Please enter the SCP user passphrase to retrieve the Crosswork Data Gateway PEM formatted
certificate file and private key
DGCertChainPwd=

### DNS Servers

## DNS Security Extensions
# Use DNS security extensions
# Default value: False
DNSSEC=False

## DNS over TLS
# Use DNS over TLS
# Default value: False
DNSTLS=False

## Multicast DNS
# Use multicast DNS
# Default value: False
mDNS=False

## Link-Local Multicast Name Resolution
# Use link-local multicast name resolution
# Default value: False
LLMNR=False

### NTPv4 Servers

## NTPv4 Authentication
# Use authentication for all NTPv4 servers
# Default value: False
NTPAuth=False

## NTPv4 Keys
# Please enter a space delimited list of IDs present in the key file. The number of IDs in the
list must match the number of servers, even if some or all are the same ID.
NTPKey=

## NTPv4 Key File URI
# Please enter the optional Chrony key file retrieved using SCP (user@host:/path/to/file)
NTPKeyFile=

## NTPv4 Key File Passphrase
# Please enter the SCP user passphrase to retrieve the Chrony key file
NTPKeyFilePwd=

### Remote Syslog Servers

## Remote Syslog Server
# Send Syslog messages to a remote host
# Default value: False
UseRemoteSyslog=False

## Syslog Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the Syslog server accessible from the
Default Gateway role

```

```
SyslogAddress=

## Syslog Server Port
# Please enter a Syslog port
# Default value: 514
SyslogPort=514

## Syslog Server Protocol
# Please enter the Syslog protocol
# Default value: UDP
SyslogProtocol=UDP

## Syslog over TLS
# Use Syslog over TLS (must use TCP or RELP as the protocol)
# Default value: False
SyslogTLS=False

## Syslog TLS Peer Name
# Please enter the Syslog server's hostname exactly as entered in the server certificate
subjectAltName or subject common name
SyslogPeerName=

## Syslog Root Certificate File URI
# Please enter the optional Syslog root PEM formatted certificate file retrieved using SCP
(user@host:/path/to/file)
SyslogCertChain=

## Syslog Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the Syslog PEM formatted certificate file
SyslogCertChainPwd=

### Remote Auditd Servers

## Remote auditd Server
# Send auditd messages to a remote host
# Default value: False
UseRemoteAuditd=False

## Auditd Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the auditd server accessible from the
Default Gateway role
AuditdAddress=

## Auditd Server Port
# Please enter na auditd port
# Default value: 60
AuditdPort=60

### Controller Settings

## Proxy Server URL
# Please enter the optional HTTP/HTTPS proxy URL
ProxyURL=

## Proxy Server Bypass List
# Please enter an optional space delimited list of subnets and domains that will not be sent to
the proxy server
ProxyBypass=

## Authenticated Proxy Username
# Please enter an optional username for an authenticated proxy servers
ProxyUsername=

## Authenticated Proxy Passphrase
```

```
# Please enter an optional passphrase for an authenticated proxy server
ProxyPassphrase=

## HTTPS Proxy SSL/TLS Certificate File URI
# Please enter the optional HTTPS Proxy PEM formatted SSL/TLS certificate file URI retrieved using
  SCP (user@host:/path/to/file). This will override the Controller SSL/TLS Certificate File URI.
ProxyCertChain=

## HTTPS Proxy SSL/TLS Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the HTTPS Proxy PEM formatted SSL/TLS certificate
  file
ProxyCertChainPwd=

### Auto Enrollment Package Transfer

## Enrollment Destination Host and Path
# Please enter the optional SCP destination host and path to transfer the enrollment package using
  SCP (user@host:/path/to/file)
EnrollmentURI=

## Enrollment Passphrase
# Please enter the optional SCP user passphrase to transfer the enrollment package
EnrollmentPassphrase=

#### Static Parameters - Do not change this section

### Deployment Settings

## Deployment Type
# What type of deployment is this?
# Default value: Crosswork Cloud
Deployment=Crosswork Cloud

### Host Information

## Data Disk Size
# Data disk size in GB mounted as /opt/dg/appdata
DGAppdataDisk=24

### vNIC Role Assignment

## Default Gateway
# The interface used as the Default Gateway and for DNS and NTP traffic
# Default value: eth0
NicDefaultGateway=eth0

## Administration
# The interface used for SSH access to the VM
# Default value: eth0
NicAdministration=eth0

## External Logging
# The interface used to send logs to an external logging server
# Default value: eth0
NicExternalLogging=eth0

## Management
# The interface used for enrollment and other management traffic
# Default value: eth0
NicManagement=eth0

## Control
# The interface used for destination, device, and collection configuration
# Default value: eth0
```

```

NicControl=eth0

## Northbound System Data
# The interface used to send collection data to the system destination
# Default value: eth0
NicNBSystemData=eth0

## Northbound External Data
# The interface used to send collection data to external destinations
# Default value: eth0
NicNBExternalData=eth0

## Southbound Data
# The interface used collect data from all devices
# Default value: eth0
NicSBData=eth0

```

- b) Repeat the previous step to create the user data for each Crosswork Data VM that you plan to install.

Step 2 Install the Crosswork Data Gateway VM.

- a) Log in to AWS and search for the EC2 service. The EC2 dashboard opens.
- b) Navigate to **Launch Instance** pane on the dashboard and click **Launch Instance** > **Launch Instance**.
A **Launch an Instance** window appears.
- c) In the **Name and tags** section, enter the name of the Crosswork Data Gateway VM.
- d) In the **Application and OS Images (Amazon Machine Image)** section, click **My AMIs** > **Owned by me** and select the Crosswork Data Gateway AMI image in the **Amazon Machine Image (AMI)** field.
- e) In the **Instance type** section, select the **t2.2xlarge** instance type (both production and lab environment) for the Crosswork Data VM you are deploying.
- f) In the **Key pair (login)** section, select a **Key pair name** from the drop-down list.

Note Cisco Crosswork does not support key-based authentication. This is an AWS requirement and will not be used by Cisco Crosswork.

- g) In the **Network Settings** section, click **Edit**.
 1. Enter values in the following fields:
 - **VPC**: Select the appropriate VPC for your environment.
 - **Subnet**: Select the subnet that you wish to assign to the management interface.
 - **Auto-assign public IP**: Select **Disabled**.
 - **Firewall (security groups)**: Specify a security group for the VM. You can create a security group or use an existing security group that you have already created.

After you have entered the details above, under **Advanced network configuration**, a **Network Interface1** is automatically created.
 2. Update the **Description**, **Primary IP** (vNIC0 IP address from the user data), **Subnet**, **Security groups**.
- h) In the **Configure Storage** section, click **Advanced** and click **Add new volume** to add an additional partition for your VM. Update the following fields for the newly created volume.
 - **Device name**: /device/sdb
 - **Size (GiB)**: 20 GB or 520 GB. If you do not specify a size, the default size of 50 GB is considered.

When extra disk space is required for processing additional dossier collection, you can add node disk.

- **Volume type:** We recommend using gp2 or gp3.

i) In the **Advanced Settings** section, update the following fields.

- **IAM instance profile:** Select the AWS IAM role that you had specified in the user data or create a new role.
- **Metadata accessible:** Enabled.
- **Metadata version:** V1 and V2 (token optional)
- **Metadata response hop limit:** 2
- **User data:** Copy the user data that you had prepared in Step 1 and paste it within the window here. If you are providing the parameters in a base64 encoded format, select the check box.

Note Ensure that there are no leading white spaces when you paste the user data otherwise the deployment fails.

Step 3 Click **Launch Instance**. AWS EC2 initiates the installation of the VM.

Step 4 Repeat steps 2 to 4 to install the remaining VMs.

Verify that the VMs were installed successfully.

1. In the EC2 dashboard, click **Instances** from the menu on the left to view the VMs that were deployed. You can search for the VMs using the name, attributes, or tags.
Wait for about 20 minutes for the VMs to be deployed.
2. After the VMs are launched successfully, they have the **Instance State** as **Running**.
3. To verify that the VMs were installed successfully, select a VM and click **Connect** (top-right corner).
4. In the **Connect to instance** window that appears, click the **EC2 Serial Control** tab and click **Connect**.
5. Log in to the VM as a `dg-admin` or `dg-oper` user using the password you configured in the user data.
The Interactive Console of the VM is displayed on successful login.

Generate Enrollment Package

Every Crosswork Data Gateway must be identified by 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 72](#)).
- By using the **Display base64 Encoded Enrollment Package** option from the Interactive Console (see [Create an Encoded Enrollment Package, on page 73](#)).


```

],
"version": "4.5.0 (branch dg45x - build number 19)",
"duuid": "a3bf6411-1ad0-418c-9957-eb199e9395e0",
"profileType": "VM_PROFILE_STANDARD"
}

```

Obtain the Enrollment Package

You can obtain the enrollment package by exporting or copying and pasting the encoded contents of the package to create an enrollment file.

-
- Step 1** Log in to Cisco Crosswork Data Gateway.
 - Step 2** From the Main Menu, select **Get Enrollment Package**.
 - Step 3** Select **Export Enrollment Package** or **Display base64 Encoded Enrollment Package**.
 - Step 4** Click **OK**.
-

What to do next

Depending on the option that you have selected, obtain the enrollment package referring to [Export Enrollment Package, on page 72](#) or [Create an Encoded Enrollment Package, on page 73](#)

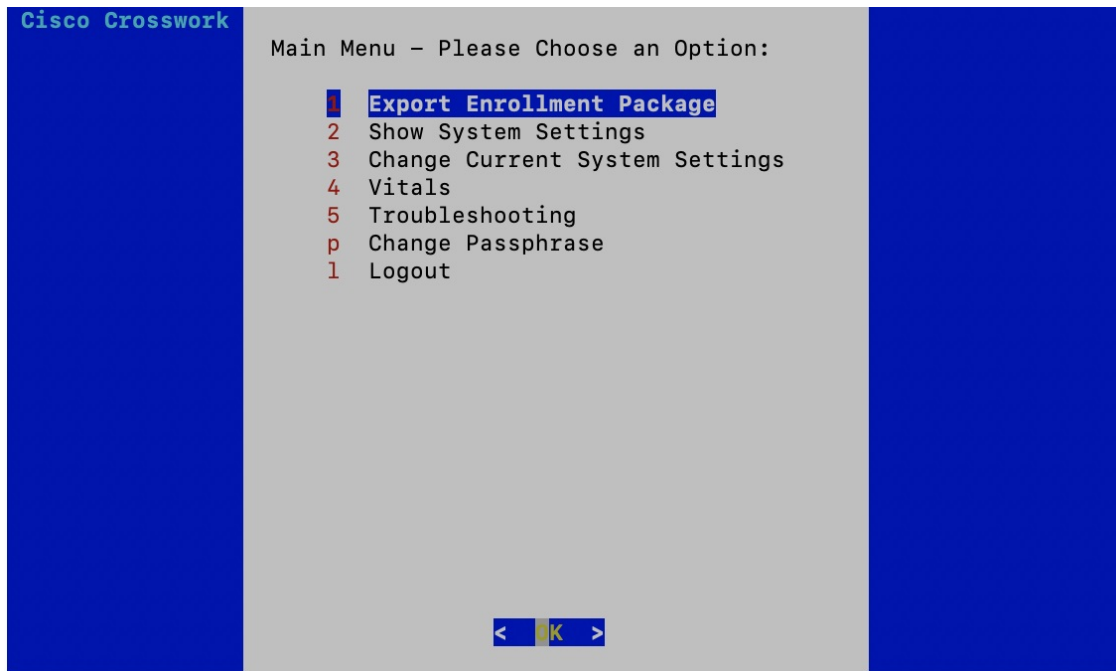
Export Enrollment Package

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 74](#) 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 Get Enrollment Package**.
 - Step 3** Select **Export Enrollment Package**.
 - Step 4** Click **OK**.



Step 5 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'll 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 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 6 Enter the SCP passphrase (the SCP user password) and click **OK**.

Step 7 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 74](#).

Create an Encoded Enrollment Package

You can create an enrollment package file on your local machine by copying and pasting the package contents from the interactive console. The content is secured in the JSON format and encoded using the Base64 schemes.

-
- 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 75](#) 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
<p>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.</p>	<ol style="list-style-type: none"> 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 <code>session.log</code> at location <code>/cdg/logs/components/controller-gateway/session.log</code>), if you see the error <pre>UNAUTHENTICATED:invalid certificate. reason: x509: certificate has expired or is not yet valid</pre>, 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.
<p>Crosswork Data Gateway does not have direct connectivity to external web services.</p>	<ol style="list-style-type: none"> 1. Configure a proxy server if a proxy server is missing in your environment. 2. If a proxy server is already present in your environment, check if the proxy URL is correct. 3. Check if the credentials of the proxy (certificate, proxy name etc) are correct. <p>To update the proxy server details on the Crosswork Data Gateway, see Configure Control Proxy.</p>