



## 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 29](#)
- [Install Crosswork Data Gateway on Amazon EC2, on page 68](#)
- [Auto-Configuration for Deploying Crosswork Data Gateway, on page 78](#)
- [Enroll Crosswork Data Gateway with Crosswork Cloud, on page 81](#)
- [Register Crosswork Data Gateway with Crosswork Cloud Applications, on page 91](#)
- [Troubleshoot the Crosswork Data Gateway Connectivity, on page 92](#)

## Install Cisco Crosswork Data Gateway

Cisco Crosswork Data Gateway is initially deployed as a VM called Base VM that contains 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. Determine the platform where you want to deploy Cisco Crosswork Data Gateway and ensure that you have the required software images:

VMware	<a href="#">Install Crosswork Data Gateway using vCenter vSphere Client, on page 15</a> <a href="#">Install Crosswork Data Gateway via OVF Tool, on page 24</a>
--------	--

OpenStack	<a href="#">Install Crosswork Data Gateway on OpenStack from OpenStack CLI, on page 29</a> <a href="#">Install Crosswork Data Gateway on OpenStack from the OpenStack UI, on page 44</a>
Amazon EC2	<a href="#">Install Crosswork Data Gateway using CloudFormation (CF) Template, on page 68</a> <a href="#">Install Crosswork Data Gateway on Amazon EC2 Manually, on page 75</a>

- Plan your installation. See [Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2](#) for information on deployment parameters and possible deployment scenarios.  
 (Optional) If you are deploying a single NIC, you can utilize the auto-configuration feature to optimize the deployment of data gateways with the bare minimum configuration. See [Auto-Configuration for Deploying Crosswork Data Gateway, on page 78](#). This feature is supported only on OpenStack and Amazon EC2 platforms.
- Identify the preferred procedure for enrolling Crosswork Data Gateway with Crosswork Cloud.
  - If you want to enroll the data gateway during the VM deployment, see [Add Enrollment Token to Configuration File, on page 86](#). This procedure is available from 6.0.1 release onwards.
  - If you want to enroll the data gateway after the VM is deployed, see [Manually Enroll Crosswork Data Gateway with Crosswork Cloud, on page 87](#).
- Register Cisco Crosswork Data Gateway with Crosswork Cloud. See [Register Crosswork Data Gateway with Crosswork Cloud Applications, on page 91](#).

## Cisco Crosswork Data Gateway Deployment Parameters and Scenarios

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

### 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**, **dg-oper**, and **dg-tac** user accounts are reserved usernames and cannot be changed. You can change the password in the console for both the accounts. See [Change Passphrase](#). 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, if required.

### Installation Parameters and Scenarios

The following table provides the label and key values of deployment parameters. Labels represent the parameters that can be configured in the VMware UI and Keys corresponds to field values in the OVF script that match your configuration.

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.



**Caution** When the mandatory parameters are not set, Crosswork Data Gateway is deployed using the default values. However, the default values may not align with your environment requirements.

\*\* 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 Cloud.

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

Label	Key	Description	Additional Information
<b>Host Information</b>			
Hostname*	Hostname	Name of the Cisco Crosswork Data Gateway VM specified as a fully qualified domain name (FQDN).  In larger systems, you are likely to have more than one Cisco Crosswork Data Gateway VM. The hostname must, therefore, be unique and created in a way that makes identifying a specific VM easy.	
Description*	Description	A detailed description of the Cisco Crosswork Data Gateway.	

Label	Key	Description	Additional Information
Label	Label	Label used by Cisco Crosswork Cloud to categorize and group multiple Cisco Crosswork Data Gateways.	
AllowRFC8190*	AllowRFC8190	Automatically allow addresses in an RFC 8190 range. Options are <i>No</i> , <i>Yes</i> , or <i>Ask</i> , where the initial configuration script prompts for confirmation. The default value is <i>Yes</i> .	
Private Key URI	DGCertKey	URI to private key file for session key signing. You can retrieve this using SCP (user@host:path/to/file).	Crosswork Cloud uses self-signed certificates for handshake with Cisco Crosswork Data Gateway. These certificates are generated at installation.
Certificate File and Key Passphrase	DGCertChainPwd	SCP user passphrase to retrieve the Cisco Crosswork Data Gateway PEM formatted certificate file and private key.	However, if you want to use third party or your own certificate files enter these parameters.  Certificate chains override any preset or generated certificates in the Cisco Crosswork Data Gateway VM and are given as an SCP URI (user:host:/path/to/file). 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.

Label	Key	Description	Additional Information
Data Disk Size	DGAppdataDisk	Size in GB of a second data disk.  The default size is 24GB. Do not change the default value without consulting a Cisco representative.	
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.
<b>Passphrases</b>			
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.	
<b>Interfaces</b>			
<b>Note</b>	To install Crosswork Data Gateway properly, either IPv4 or IPv6 addresses must be configured to static or DHCP. The protocol that you do not want to use should be set to <b>None</b> .		
<b>vNIC Role Assignment</b>			

Label	Key	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"> <li>• The <code>NicControl</code>, <code>NicNBExternalData</code>, and <code>NicSBData</code> roles map to <code>eth1</code>.</li> <li>• The <code>NicControl</code>, <code>NicNBExternalData</code>, <code>NicSBData</code> roles map to <code>eth1</code>.</li> <li>• The <code>NicSBData</code> role maps to <code>eth2</code>.</li> <li>• The <code>NicControl</code>, and <code>NicNBExternalData</code> roles map to <code>eth1</code>.</li> </ul>
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> .	
NicNBSystemData*	NicNBSystemData	Interface used to send the collected data to the system destination.  Options are <code>eth0</code> , <code>eth1</code> , <code>eth2</code> , or <code>eth3</code> . The default value is <code>eth0</code> .	

Label	Key	Description	Additional Information
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> .	
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> .	
<b>vNIC IPv4 Address (vNIC0, vNIC1, and vNIC2 based on the number of interfaces you choose to use)</b>			

Label	Key	Description	Additional Information
vNIC IPv4 Method*	Vnic0IPv4Method Vnic1IPv4Method Vnic2IPv4Method	Options are <code>None</code> , <code>Static</code> , or <code>DHCP</code> .  <b>Note</b> 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> .	<p>If you have selected <b>Method</b> as:</p> <ul style="list-style-type: none"> <li>• <b>None</b>: Skip the rest of the fields for IPv4 address. Enter information in the vNIC IPv6 Address parameters.</li> <li>• <b>Static</b>: Enter information in <b>Address</b>, <b>Netmask</b>, <b>Skip Gateway</b>, and <b>Gateway</b> fields</li> <li>• <b>DHCP</b>: Values for the vNIC IPv4 Address parameters are assigned automatically.</li> </ul> <p>Do not change the default values.</p>
vNIC IPv4 Address	Vnic0IPv4Address Vnic1IPv4Address Vnic2IPv4Address	IPv4 address of the interface.	
vNIC IPv4 Netmask	Vnic0IPv4Netmask Vnic1IPv4Netmask Vnic2IPv4Netmask	IPv4 netmask of the interface in dotted quad format.	
vNIC IPv4 Skip Gateway	Vnic0IPv4SkipGateway Vnic1IPv4SkipGateway Vnic2IPv4SkipGateway	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	IPv4 address of the vNIC gateway.	
<b>vNIC IPv6 Address (vNIC0, vNIC1, and vNIC2 based on the number of interfaces you choose to use)</b>			



Label	Key	Description	Additional Information
vNIC IPv6 Method*	Vnic0IPv6Method Vnic1IPv6Method Vnic2IPv6Method	Options are <code>None</code> , <code>Static</code> , <code>DHCP</code> or <code>SLAAC</code> (QCOW2 only).  The default value for <b>Method</b> is <code>None</code> .  <b>Note</b> DHCP support is enabled only for deployments performed using the QCOW2 images.	<p>If you have selected <b>Method</b> as:</p> <ul style="list-style-type: none"> <li>• <b>None</b>: Skip the rest of the fields for IPv6 address. Enter information in the <b>vNICx IPv4 Address</b> parameters.</li> <li>• <b>Static</b>: Enter information in <b>Address</b>, <b>Netmask</b>, <b>Skip Gateway</b>, and <b>Gateway</b> fields</li> <li>• <b>DHCP</b>: Values for the vNIC IPv6 Address parameters are assigned automatically.</li> </ul> <p>Do not change the <code>VnicxIPv6Address</code> default values.</p>
vNIC IPv6 Address	Vnic0IPv6Address Vnic1IPv6Address Vnic2IPv6Address	IPv6 address of the interface.	
vNIC IPv6 Netmask	Vnic0IPv6Netmask Vnic1IPv6Netmask Vnic2IPv6Netmask	IPv6 prefix of the interface.	
vNIC IPv6 Skip Gateway	Vnic0IPv6SkipGateway Vnic1IPv6SkipGateway Vnic2IPv6SkipGateway	Options are <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	IPv6 address of the vNIC gateway.	
<b>DNS Servers</b>			
DNS Address*	DNS	Space-delimited list of IPv4 or IPv6 addresses of the DNS server accessible in the management interface.	
DNS Search Domain	Domain	DNS search domain.  The default value is <code>localdomain</code> .	

Label	Key	Description	Additional Information
DNS Security Extensions	DNSSEC	Options are <code>False</code> , <code>True</code> , or <code>Allow-Downgrade</code> . Select <code>True</code> to use DNS security extensions.  The default value is <code>False</code> .	
DNS over TLS	DNSTLS	Options are <code>False</code> , <code>True</code> , or <code>Opportunistic</code> . Select <code>True</code> to use DNS over TLS.  The default value is <code>False</code> .	
Multicast DNS	mDNS	Options are <code>False</code> , <code>True</code> , or <code>Resolve</code> . Select <code>True</code> to use multicast DNS.  The default value is <code>False</code> .	
Link-Local Multicast Name Resolution	LLMNR	Options are <code>False</code> , <code>True</code> , <code>Opportunistic</code> , or <code>Resolve</code> . Select <code>True</code> to use link-local multicast name resolution.  The default value is <code>False</code> .	
<b>NTP Servers</b>			
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 <code>&lt;sample&gt;.ntp.org</code> . 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.

Label	Key	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.	
<b>Remote Syslog Server</b>			

Label	Key	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> .	<p>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.</p> <p>If you want to use an external syslog server, you must specify these seven settings.</p> <p><b>Note</b> 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.</p>
Syslog Server Address	SyslogAddress	IPv4 or IPv6 address of a syslog server accessible in the management interface.  <b>Note</b> 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> .	
Syslog Multiserver Mode	SyslogMultiserverMode	Multiple servers in the failover or simultaneous mode. This parameter is applicable when the protocol is non-UDP (UDP must use <code>Simultaneous</code> ).  Options are <code>Simultaneous</code> or <code>Failover</code> .  The default value is <code>Simultaneous</code> .	
Use Syslog over TLS	SyslogTLS	Select <code>True</code> to use TLS to encrypt syslog traffic.  The default value is <code>False</code> .	
Syslog TLS Peer Name	SyslogPeerName	The syslog server hostname exactly as entered in the server certificate <code>SubjectAltName</code> or <code>subject common name</code> .	
Syslog Root Certificate File URI	SyslogCertChain		

Label	Key	Description	Additional Information
		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.	
<b>Remote Auditd Server</b>			
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.	
<b>Controller and Proxy Settings</b>			
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.	
<b>Enrollment Package Transfer</b>			

Label	Key	Description	Additional Information
Autoenrollment token	CloudEnrollmentToken	<p>The unique enrollment token retrieved from Crosswork Cloud. Crosswork Data Gateway uses this token to automatically enroll with Crosswork Cloud.</p> <p>Configure the number of permitted number of autoenrollment requests and the expiry date of the token.</p> <p>The default values are:</p> <ul style="list-style-type: none"> <li>• Number of uses: 5</li> <li>• Expiry: 30 days</li> </ul> <p>The maximum accepted values:</p> <ul style="list-style-type: none"> <li>• Number of uses: 50</li> <li>• Expiry: 366 days</li> </ul>	
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.
Enrollment Passphrase**	EnrollmentPassphrase	SCP user passphrase to transfer enrollment package.	
			If you do not specify these parameters during installation, then export enrollment package manually by following the procedure <a href="#">Obtain the Enrollment Package, on page 88</a> .

**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 24](#)

## 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 6.0.1 Release Notes for Cloud Applications* and download the installer bundle (.tar.gz file) and the OVA file from [cisco.com](http://cisco.com) to a directory.

For the purpose of these instructions, we will use the file names as **signed-cw-na-dg-6.0.1-119-release-20231220.uefi.ova** and **cw-na-dg-6.0.1-sample-install-scripts.tar.gz**. The **cw-na-dg-6.0.1-sample-install-scripts.tar.gz** contains the sample scripts for single, two, and three vNIC deployments, which you may optimize to meet your needs.

**Attention** The file names mentioned in this topic are sample names and may differ from the actual file names in [cisco.com](http://cisco.com).

**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 log in with your credentials.

**Step 3** Select the datacenter where you want to deploy the Crosswork Data Gateway VM.

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

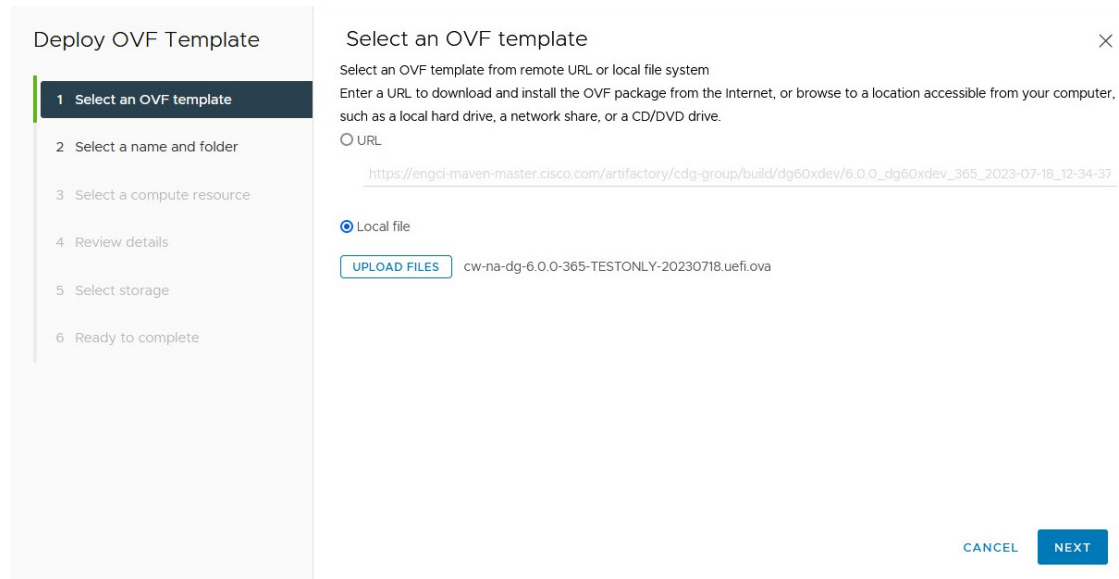
**Warning** The default VMware vCenter deployment timeout is 15 minutes. If the time taken to fill the OVF template exceeds 15 minutes, vCenter times out and you have to start over again. To prevent this, it is recommended that you plan for the installation by having the necessary parameters and requirements ready. See [Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2](#) for list of mandatory and optional parameters.

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

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

Once selected, the file name is displayed in the window.

Figure 1: Deploy OVF Template - Select an OVF Template Window



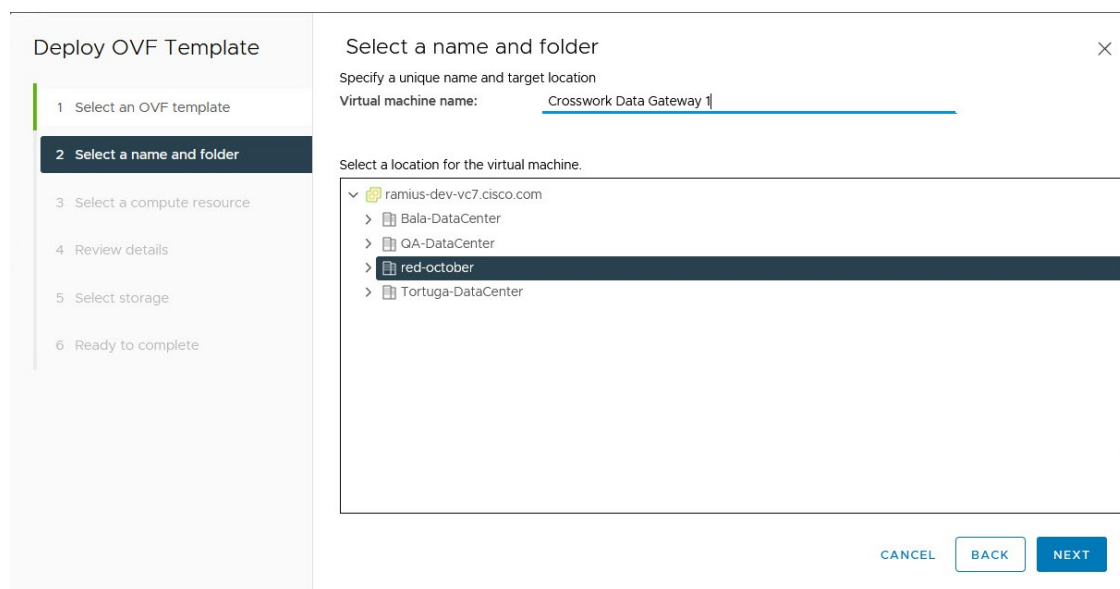
**Step 6** Click **Next** to go to **2 Select name and folder**, as shown in the following figure.

a) Enter a unique name for the VM that you are creating.

For larger systems it is likely that you 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 on which you want to deploy Crosswork Data Gateway.

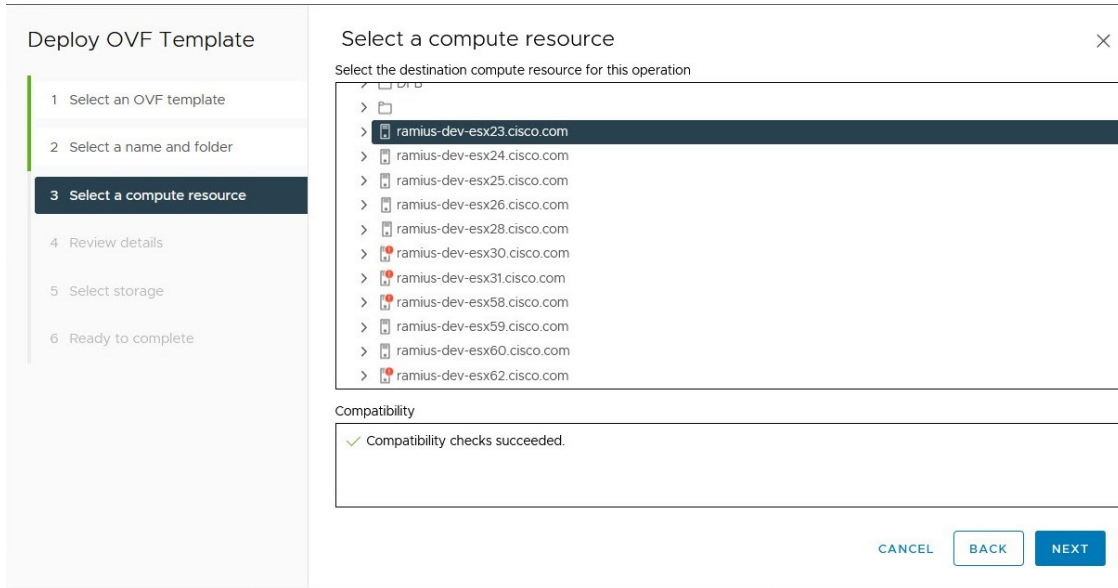
Figure 2: Deploy OVF Template - Name and Folder Selection Window



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



Figure 3: Deploy OVF Template - Select a computer resource Window

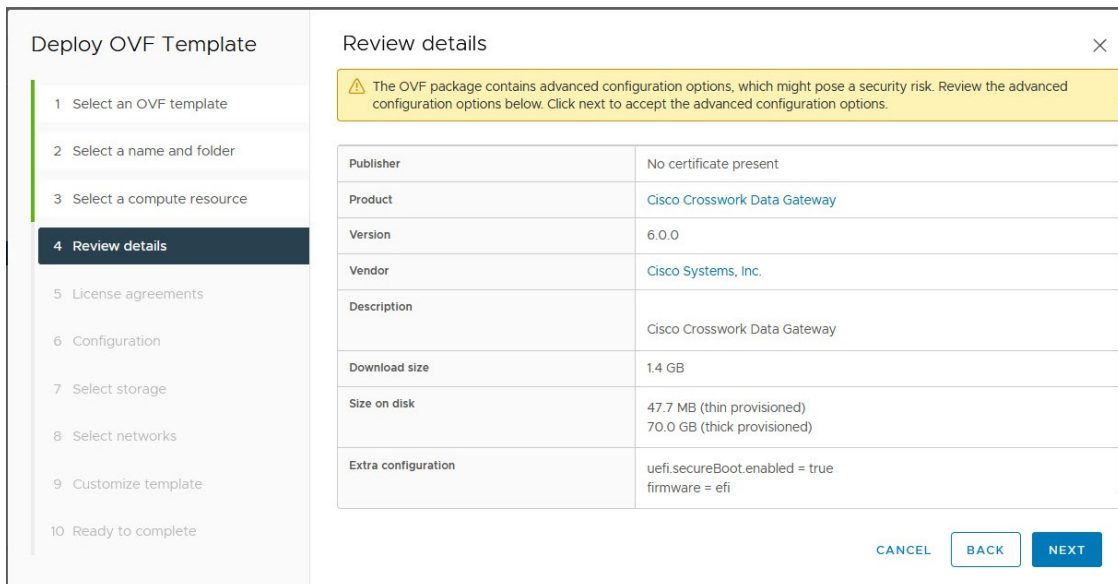
**Step 8**

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 select the correct disk configuration in the [Step 10](#).

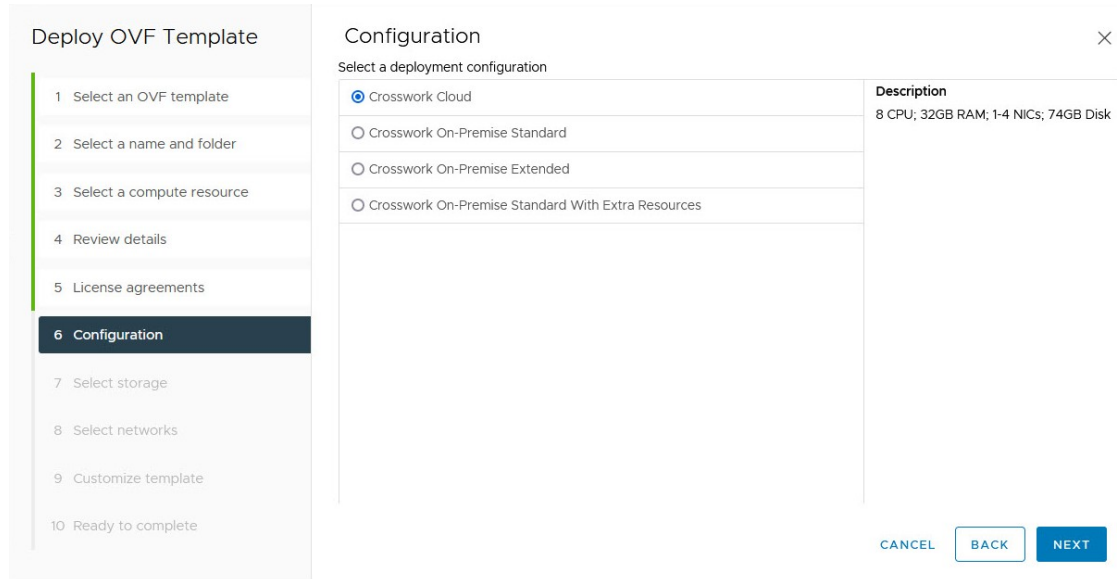
Figure 4: Deploy OVF Template - Review details Window



**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**.

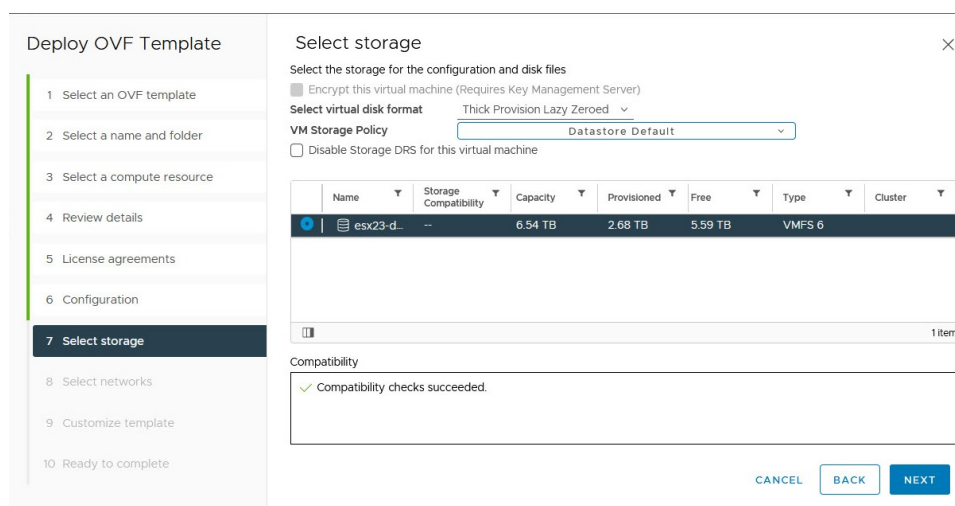
**Figure 5: Deploy OVF Template - Configuration Window**



**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.

**Figure 6: Deploy OVF Template - Select storage Window**



**Step 12**

Click **Next** to go to **8 Select networks**, as shown in the following figure. From the drop-down, at the top of the page, choose the appropriate vNIC role for each interface.

The names used for your network varies based on how the environment was originally configured. You can modify the names in [Step 13](#) based on the settings you configure when reviewing the installation parameters.

Start with vNIC0 and select a destination network that will be used. Leave the 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.

**Figure 7: Deploy OVF Template - Select networks Window**

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

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL BACK NEXT

Crosswork Cloud does not support vNIC3. Cisco advises against modifying the default network settings.

**Step 13**

Click **Next** to go to **9 Customize template**, with the **Host Information Settings** already expanded. Enter the information for the parameters as described in [Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2](#).

Values that are not explicitly mentioned in [Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2](#) but are required to align with your environment should be retained at their default values.

**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.

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

Figure 8: Deploy OVF Template - Customize template &gt; Host information Window

Field	Description
a. Hostname *	Please enter the server's hostname (dg.localdomain) CDG1
b. Description *	Please enter a short, user friendly description for display in the Crosswork Controller Sample
c. Crosswork Data Gateway Label	An optional freeform label used by the Crosswork Controller to categorize and group multiple DG instances Sample label
d. 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 Yes
e. Crosswork Data Gateway Private Key URI	Please enter the optional Crosswork Data Gateway private key URI retrieved using SCP (user@host/path/to/file)

Figure 9: Deploy OVF Template - Customize template &gt; Host information Window &gt; High Availability Network Mode

Key Passphrase	Gateway PEM formatted certificate file and private key Password Confirm Password
h. Data Disk Size	Data disk size in GB mounted as /opt/dg/appdata 24
i. Amazon Web Services IAM Role Name	Please enter the AWS IAM role name to use for sending VIP updates. This is required when deploying on AWS EC2.
j. High Availability Network Mode	Select the network mode to use with external load balancers. This will determine whether all interfaces require an address. L2
<b>02. Passphrases</b> 2 settings	
a. dg-admin Passphrase *	Please enter a passphrase for the dg-admin user. It must be at least 8

**Important** When using 1 or 2 NICs, you only need to configure vNIC0. For the 3 NIC setup, you must configure both vNIC0 and vNIC1.

**Attention** The VMware vCenter Server 6.5 and 6.7 has issue with expanding the correct parameters. To override this issue, when deploying the OVF template, in the **Deploy OVF Template** wizard > **Customize Template** page, configure the following:

- In the **03. vNIC Role Assignment** section, set all the roles to eth0.

**Figure 10: Deploy OVF Template - Customize Template for Single vNIC deployment**

### 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

### Customize template ✕

▼ 03. vNIC Role Assignment 7 settings

a. Default Gateway	The interface used as the Default Gateway and for DNS and NTP traffic <input type="text" value="eth0"/>
b. Administration	The interface used for SSH access to the VM <input type="text" value="eth0"/>
c. External Logging	The interface used to send logs to an external logging server <input type="text" value="eth0"/>
d. Management	The interface used for enrollment and other management traffic <input type="text" value="eth0"/>
e. Control	The interface used for destination, device, and collection configuration <input type="text" value="eth0"/>
g. Northbound External Data	The interface used to send collection data to external destinations <input type="text" value="eth0"/>
h. Southbound Data	The interface used collect data from all devices

CANCEL
BACK
NEXT

**Figure 11: Deploy OVF Template - Customize Template for Two vNIC deployment**

### 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

### Customize template ✕

▼ 03. vNIC Role Assignment 7 settings

a. Default Gateway	The interface used as the Default Gateway and for DNS and NTP traffic <input type="text" value="eth0"/>
b. Administration	The interface used for SSH access to the VM <input type="text" value="eth0"/>
c. External Logging	The interface used to send logs to an external logging server <input type="text" value="eth0"/>
d. Management	The interface used for enrollment and other management traffic <input type="text" value="eth0"/>
e. Control	The interface used for destination, device, and collection configuration <input type="text" value="eth1"/>
g. Northbound External Data	The interface used to send collection data to external destinations <input type="text" value="eth1"/>
h. Southbound Data	The interface used collect data from all devices <input type="text" value="eth1"/>

Figure 12: Deploy OVF Template - Customize Template for 3 vNIC deployment

### 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

### Customize template ✕

03. vNIC Role Assignment 7 settings

a. Default Gateway	The interface used as the Default Gateway and for DNS and NTP traffic <input type="text" value="eth0"/>
b. Administration	The interface used for SSH access to the VM <input type="text" value="eth0"/>
c. External Logging	The interface used to send logs to an external logging server <input type="text" value="eth0"/>
d. Management	The interface used for enrollment and other management traffic <input type="text" value="eth0"/>
e. Control	The interface used for destination, device, and collection configuration <input type="text" value="eth1"/>
g. Northbound External Data	The interface used to send collection data to external destinations <input type="text" value="eth1"/>
h. Southbound Data	The interface used collect data from all devices <input type="text" value="eth2"/>

Figure 13: Deploy OVF Template - Customize Template for Auto Enrollment configuration

The screenshot displays the 'Deploy OVF Template' wizard in the vSphere Client. The left-hand navigation pane lists ten steps, with '9 Customize template' highlighted. The main window is titled 'Customize template' and contains two expandable sections:

- 16. Controller Settings (6 settings):**
  - c. Auditd Server Port: Please enter na auditd port. Value: 60.
  - f. Proxy Server URL: Please enter the optional HTTP/HTTPS proxy URL.
  - g. Proxy Server Bypass List: Please enter an optional space delimited list of subnets and domains that will not be sent to the proxy server.
  - h. Authenticated Proxy Username: Please enter an optional username for an authenticated proxy servers.
  - i. Authenticated Proxy Passphrase: Please enter an optional passphrase for an authenticated proxy server. Fields: Password, Confirm Password.
  - j. 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.
  - k. HTTPS Proxy SSL/TLS Certificate File Passphrase: Please enter the SCP user passphrase to retrieve the HTTPS Proxy PEM formatted SSL/TLS certificate file. Fields: Password, Confirm Password.
- 17. Auto Enrollment Package Transfer (3 settings):**
  - a. Enrollment Destination URI: Please enter the optional SCP destination URI to transfer the enrollment package using SCP (user@host:/path/to/file).
  - b. Enrollment Passphrase: Please enter the optional SCP user passphrase to transfer the enrollment package. Fields: Password, Confirm Password.
  - c. Enrollment Token: Please enter the optional enrollment token to auto enroll with Crosswork Cloud.

At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'.

**Step 14** Click **Next** to go to **10 Ready to complete**. Review your settings and then click **Finish**.

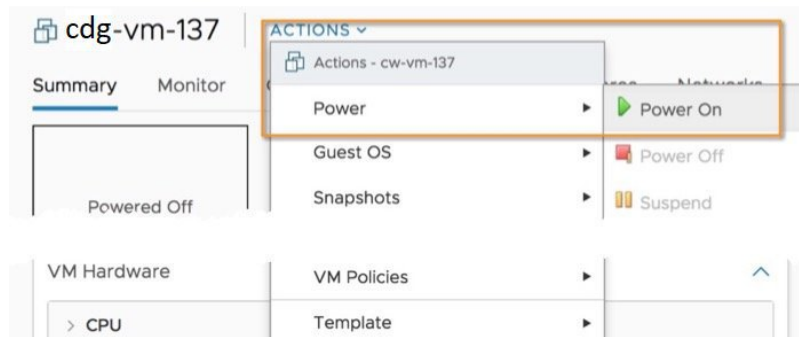
**Step 15** Wait for the deployment to finish before continuing. To check the deployment status:

- 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.

Wait for the deployment status to become 100%. You can now proceed to power on the VM.

**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 right-click and choose **Actions > Power > Power On**, as shown in the following figure:

**Figure 14: Power On Action**



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 re enroll the new one on the Crosswork Cloud.

---

Verify that Crosswork Data Gateway was installed. For more information on how to perform the verification, see [Verify that Crosswork Data Gateway is Installed](#), on page 28.

#### 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 88.

## Install Crosswork Data Gateway via OVF Tool

You must modify the list of mandatory and optional parameters in the script as per your requirements and run the OVF Tool. See [Cisco Crosswork Data Gateway Deployment Parameters and Scenarios](#), on page 2 for the list of installation parameters and their default values.




---

**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.

---

Follow these steps to log in to the Cisco Crosswork Data Gateway VM from SSH.

#### Before you begin

- In your vCenter data center, go to **Host > Configure > Networking > Virtual Switches** and select the virtual switch.



- In the virtual switch, select **Edit > Security**, and ensure that the following DVS port group properties are as shown:
  - Set **Promiscuous mode** as Reject
  - Set **MAC address changes** as Reject

Confirm the settings and repeat the process for each virtual switch used by Crosswork Data Gateway.

- 
- Step 1** On the machine where you have the OVFtool installed, use the following command to confirm that you have OVFtool version 4.4:
- ```
ovftool --version
```
- Step 2** Download the OVA and the sample script files from [cisco.com](https://www.cisco.com). For the purpose of these instructions, we will use the file names as **signed-cw-na-dg-6.0.1-119-release-20231220.uefi.ova** and **cw-na-dg-6.0.1-sample-install-scripts.tar.gz**. The **cw-na-dg-6.0.1-sample-install-scripts.tar.gz** contains the sample scripts for single, two, and three vNIC deployments, which you may optimize to meet your needs.
- Step 3** Use the following command to extract the files from the tar bundle:
- ```
tar -xvzf cw-na-dg-6.0.1-sample-install-scripts.tar.gz
```
- The file bundle is extracted. It includes the **DG-sample-install-scripts.tar** file and scripts for validating the samples install scripts.
- Step 4** Use the following command to extract the install scripts from the tar bundle:
- ```
tar -xvzf DG-sample-install-scripts.tar.gz
```
- Step 5** Review the contents of the README file to understand the components that are in the package and how they are validated.
- Step 6** Choose the sample script that corresponds to the deployment you plan to use. Cisco provides sample scripts for 1, 2, and 3 vNIC deployments, which you may optimize to meet your needs. See [Sample Script for Crosswork Data Gateway IPv4 Deployment, on page 26](#).
- 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 7** Use the following command to make the script executable:
- ```
chmod +x {filename}
```
- Step 8** Use the following command to execute the script from the directory where the OVA and script files are stored:
- ```
./{script name} {path and ova file name}
```
- For example:
- ```
./three-nic /home/admin/CDG_Install/signed-cw-na-dg-6.0.1-119-release-20231220.uefi.ova
```
- Step 9** If the values provided in the script are valid, provide the vCenter user's password when you are prompted.
- If the script fails due to invalid values, a message like the following is displayed:
- ```
admin@nso-576-tsdn-410-ai0:~/CDG_Install$ ./three-nic
/home/admin/CDG_Install/signed-cw-na-dg-6.0.1-119-release-20231220.uefi.ova
Opening OVA source: /home/admin/CDG_Install/signed-cw-na-dg-6.0.1-119-release-20231220.uefi.ova
The manifest does not validate
Warning:
```

## Sample Script for Crosswork Data Gateway IPv4 Deployment

```
- Line -1: Unsupported value 'firmware' for attribute 'key' on element 'ExtraConfig'.
- Line -1: Unsupported value 'uefi.secureBoot.enabled' for attribute 'key' on element 'ExtraConfig'.
Enter login information for target vi://rcdn5-spm-vc-01.cisco.com/
Username: johndoe
Password: *****
```

After entering the password, monitor the screen or the vCenter console to review the installation progress. For example,

```
Opening VI target: vi://johndoe@rcdn5-spm-vc-01.cisco.com:443/Cisco-sample-sample/host/10.10.100.10
Warning:
- Line 146: Unable to parse 'enableMPTSupport' for attribute 'key' on element 'Config'.
- Line 229: Unable to parse 'vmxnet3.noOprom' for attribute 'key' on element 'Config'.
Deploying to VI: vi://johndoe@rcdn5-spm-vc-01.cisco.com:443/Cisco-sample-sample/host/10.10.100.10
Disk progress: 65%
```

When the installation is complete, the Crosswork Data Gateway VM is powered on.

### What to do next

Log in to the VM. For more information, see [Log in and Log out of Crosswork Data Gateway VM, on page 28](#). After you log in, the Crosswork Data Gateway should present you with the welcome screen, and options menu indicating that the installation is complete. Log out and proceed with the post-installation tasks explained in [Log Out of Crosswork Data Gateway VM, on page 29](#).

Proceed to enrolling the Crosswork Data Gateway with Crosswork Cloud. See [Obtain the Enrollment Package, on page 88](#).

## Sample Script for Crosswork Data Gateway IPv4 Deployment

The following example deploys a Crosswork Data Gateway with IPv4 addresses.



**Note** Before running the scripts, ensure that the OVFtool version is 4.4.x.

```
#!/usr/bin/env bash
DM="<thin/thick>"
Disclaimer="<Disclaimer>"
DNSv4="<DNS Server>"
NTP="<NTP Server>"
Domain="<Domain>"
Hostname="<CDG hostname>"

VM_NAME="<VM name on vcenter>"
DeploymentOption="cloud"
DS="<Datastore>"
Host="<ESXi host>"
ManagementNetwork="<vSwitch/dvSwitch>"
DataNetwork="<vSwitch/dvSwitch>"
DeviceNetwork="<vSwitch/dvSwitch>"
ManagementIPv4Address="<CDG managment IP>"
ManagementIPv4Netmask="<CDG managment mask>"
ManagementIPv4Gateway="<CDG managment gateway>"
DataIPv4Address="<CDG Data network IP>"
DataIPv4Netmask="<CDG Data network mask>"
DataIPv4Gateway="<CDG Data network gateway>"
DeviceIPv4Address="<CDG Device network IP>"
DeviceIPv4Netmask="<CDG Device network mask>"
DeviceIPv4Gateway="<CDG Device network gateway>"
```

```

dgadminpwd="<CDG password for dg-admin user>"
dgoperpwd="<CDG password for dg-admin user>"
URI="<user@host:/path/to/file>"
Passphrase="<Passphrase for Enrollment URI server>"

ROBOT_OVA_PATH=$1

VCENTER_LOGIN="Administrator%40vsphere.local@<vCenter-IP>"
VCENTER_PATH="<vCenter-DC-NAME>/host"

ovftool --acceptAllEulas --skipManifestCheck --X:injectOvfEnv -ds=$DS --diskMode=$DM
--overwrite --powerOffTarget --powerOn --noSSLVerify \
--allowExtraConfig \
--name=$VM_NAME \
--deploymentOption=${DeploymentOption} \
--net:"vNIC0=${ManagementNetwork}" \
--prop:"Hostname=${Hostname}" \
--prop:"Description=${Disclaimer}" \
--prop:"DNS=${DNSv4}" \
--prop:"NTP=${NTP}" \
--prop:"Domain=${Domain}" \
--prop:"EnrollmentURI=${URI}" \
--prop:"EnrollmentPassphrase=${Passphrase}" \
--prop:"Vnic0IPv4Method=Static" \
--prop:"Vnic0IPv4Address=${ManagementIPv4Address}" \
--prop:"Vnic0IPv4Gateway=${ManagementIPv4Gateway}" \
--prop:"Vnic0IPv4Netmask=${ManagementIPv4Netmask}" \
--prop:"NicDefaultGateway=eth0" \
--prop:"NicAdministration=eth0" \
--prop:"NicExternalLogging=eth0" \
--prop:"NicManagement=eth0" \
--prop:"NicControl=eth0" \
--prop:"NicNBExternalData=eth0" \
--prop:"NicSBData=eth0" \
--prop:"dg-adminPassword=${dgadminpwd}" \
--prop:"dg-operPassword=${dgoperpwd}" \
$ROBOT_OVA_PATH \
vi://$VCENTER_LOGIN/$VCENTER_PATH/$Host

#####
Append section below for Two NIC deployment
#####
#--net:"vNIC1=${DataNetwork}" \
#--prop:"Vnic1IPv4Method=Static" \
#--prop:"Vnic1IPv4Address=${DataIPv4Address}" \
#--prop:"Vnic1IPv4Gateway=${DataIPv4Gateway}" \
#--prop:"Vnic1IPv4Netmask=${DataIPv4Netmask}" \
#--prop:"NicDefaultGateway=eth0" \
#--prop:"NicAdministration=eth0" \
#--prop:"NicExternalLogging=eth0" \
#--prop:"NicManagement=eth0" \
#--prop:"NicControl=eth1" \
#--prop:"NicNBExternalData=eth1" \
#--prop:"NicSBData=eth1" \

#####
Append section below for three NIC deployment
#####
#--net:"vNIC1=${DataNetwork}" \
#--net:"vNIC2=${DeviceNetwork}" \
#--prop:"Vnic1IPv4Method=Static" \
#--prop:"Vnic2IPv4Method=Static" \
#--prop:"Vnic1IPv4Address=${DataIPv4Address}" \

```

```

#--prop:"Vnic1IPv4Gateway=${DataIPv4Gateway}" \
#--prop:"Vnic1IPv4Netmask=${DataIPv4Netmask}" \
#--prop:"Vnic2IPv4Address=${DeviceIPv4Address}" \
#--prop:"Vnic2IPv4Gateway=${DeviceIPv4Gateway}" \
#--prop:"Vnic2IPv4Netmask=${DeviceIPv4Netmask}" \
#--prop:"NicDefaultGateway=eth0" \
#--prop:"NicAdministration=eth0" \
#--prop:"NicExternalLogging=eth0" \
#--prop:"NicManagement=eth0" \
#--prop:"NicControl=eth1" \
#--prop:"NicNBExternalData=eth1" \
#--prop:"NicSBData=eth2" \

### Auto Enrollment Package Transfer
## Enrollment Token for Crosswork Cloud
# Please enter the optional enrollment token to auto enroll with Crosswork Cloud
#--prop:"CloudEnrollmentToken=TOKEN"

## 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=

```

## Verify that Crosswork Data Gateway is Installed

You can gain assurance that Crosswork Data Gateway is successfully installed through vCenter.

Follow these steps to verify that Crosswork Data Gateway is installed.

- 
- Step 1** Log in to Crosswork Data Gateway VM through vCenter.
  - Step 2** Locate the VM in vCenter and then right-click and select **Open Console**.
  - Step 3** 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**.
- 

## Log in and Log out of Crosswork Data Gateway VM

You can log in to the Crosswork Data Gateway VM in one of the following ways:

- [Access Crosswork Data Gateway through vCenter, on page 28](#)
- [Access Crosswork Data Gateway VM from SSH, on page 29](#)

To log out of the Crosswork Data Gateway VM, see [Log Out of Crosswork Data Gateway VM, on page 29](#).

## Access Crosswork Data Gateway through vCenter

Follow these steps to log in via vCenter:

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

The Crosswork Data Gateway console comes up.

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

---

## Access Crosswork Data Gateway VM from SSH

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.

Follow these steps to log in to the Cisco Crosswork Data Gateway VM from SSH.

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

```
ssh <username>@<ManagementNetworkIP>
```

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

For example,

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

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

- Step 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 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.

## Log Out of Crosswork Data Gateway VM

To log out, select option **1 Logout** from the Main Menu and press Enter or click **OK**.

# 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 29](#)
- [Install Crosswork Data Gateway on OpenStack from the OpenStack UI, on page 44](#)

## Install Crosswork Data Gateway on OpenStack from OpenStack CLI

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



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

### Before you begin

Ensure you have the following information ready:

- Number of Crosswork Data Gateway VM instances to install.
- Plan your installation. Refer to the section [Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2](#).
- Decide the addressing method that you will use (DHCP or Static) for 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://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 **signed-cw-na-dg-6.0.1-119-release-20231220-qcow2.uefi.tar.gz** and **cw-na-dg-6.0.1-sample-install-scripts.tar.gz**.
- b) Use the following command to unzip the installer bundle:

```
tar -xvzf signed-cw-na-dg-6.0.1-119-release-20231220-qcow2.uefi.tar.gz
```

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

```
README
signed-cw-na-dg-6.0.1-119-release-20231220.uefi.tar.gz.signature
signed-cw-na-dg-6.0.1-119-release-20231220.uefi.tar.gz
cisco_x509_verify_release.py3
cisco_x509_verify_release
CDG-CCO_RELEASE
```

- 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://cisco.com). Contact Cisco Customer Experience team if access to [cisco.com](https://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
```

**Step 2** Complete the steps in Step 3 **OR** Step 4 based on the type of addressing you plan to use for the Crosswork Data Gateway VM.

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

- a) Navigate to the directory where you have downloaded the Crosswork Data Gateway release image.
- b) Open the `config.txt` file and modify the parameters as per your installation requirements. Refer to the section [Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2](#) for more information.

This is a sample `config.txt` file for a 1 NIC deployment with the hostname 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=

## Amazon Web Services IAM Role Name
# Please enter the AWS IAM role name to use for sending VIP updates. This is required when deploying
on AWS EC2.
AwsIamRole=

## High Availability Network Mode
# Please enter the mode for the HA Network. This will determine whether all interfaces require an
address.
HANetworkMode=L2

### 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 Multiserver Mode
# Send syslog to all servers (simultaneous) or one at a time (failover)
SyslogMultiserverMode=Simultaneous

## Syslog Server Addresses
# Please enter a space delimited list of hostnames, IPv4 addresses, or IPv6 addresses of the Syslog
  servers 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=

#### 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

### Auto Enrollment Package Transfer

## Enrollment Token for Crosswork Cloud
# Please enter the optional enrollment token to auto enroll with Crosswork Cloud
CloudEnrollmentToken=TOKEN

## 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=

```

- 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 hostname 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 an 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=

#### 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

### Auto Enrollment Package Transfer

## Enrollment Token for Crosswork Cloud
# Please enter the optional enrollment token to auto enroll with Crosswork Cloud
CloudEnrollmentToken=TOKEN

## 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=

```

- 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
signed-cw-na-dg-6.0.1-119-release-20231220.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 one or more Crosswork Data Gateway VMs.****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
```

```
(osp16V75) [stack@osp16-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 88](#).

## 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. For the purpose of these

instructions, we use the package name **signed-cw-na-dg-6.0.1-119-release-20231220.uefi.qcow2.uefi.tar.gz** and **cw-na-dg-6.0.1-sample-install-scripts.tar.gz**.

- b) Use the following command to unzip the installer bundle:

```
tar -xvzf signed-cw-na-dg-6.0.1-119-release-20231220.uefi.qcow2.uefi.tar.gz
```

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

```
README
signed-cw-na-dg-6.0.1-119-release-20231220.uefi.tar.gz.signature
signed-cw-na-dg-6.0.1-119-release-20231220-release.uefi.tar.gz
cisco_x509_verify_release.py3
cisco_x509_verify_release
CDG-CCO_RELEASE
```

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

```
sh signed-cw-na-dg-6.0.1-119-release-20231220.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](http://cisco.com). Please contact Cisco Customer Experience team if access to [cisco.com](http://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
```

**Step 2** Complete the steps in [Step 3](#) OR [Step 4](#) based on the type of addressing you plan on 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 hostname 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=

#### 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

### Auto Enrollment Package Transfer

## Enrollment Token for Crosswork Cloud
# Please enter the optional enrollment token to auto enroll with Crosswork Cloud
CloudEnrollmentToken=TOKEN

## 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=

```

- 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 hostname 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=

#### 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

### Auto Enrollment Package Transfer

## Enrollment Token for Crosswork Cloud
# Please enter the optional enrollment token to auto enroll with Crosswork Cloud
CloudEnrollmentToken=TOKEN

## 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=

```

- 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**.



Figure 15: Flavor Information Window

Flavor Information \* Flavor Access

Name \*  
cdg-cloud-flavor

ID ⓘ  
auto

VCPUs \*  
8

RAM (MB) \*  
32768

Root Disk (GB) \*  
50

Ephemeral Disk (GB)  
24

Swap Disk (MB)  
0

RX/TX Factor  
1

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**.

Figure 16: Create Image Window

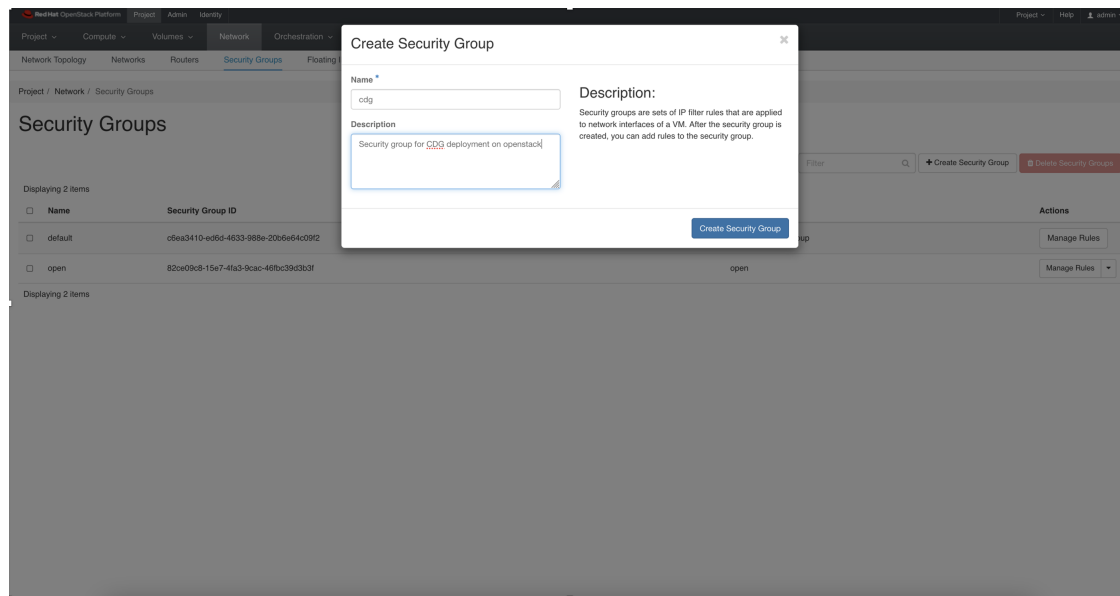
**Step 8 Create a security group policy to allow incoming TCP/UDP/ICMP connections.**

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**.

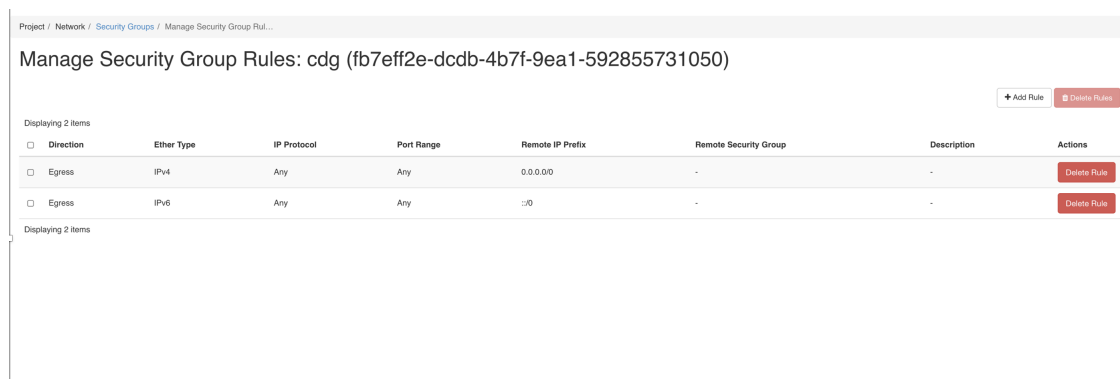
Figure 17: Create Security Group Window



- 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.

Figure 18: Manage Security Group Rules Window



## 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.

Figure 19: Create Port Window

**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: 192.168.11.101

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.

Figure 20: Launch Instance Window

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**.

Figure 21: Launch Instance Window - Source Tab

Launch Instance

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

**Select Boot Source** **Create New Volume**

Image

**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** 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

**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**.

Figure 22: Launch Instance Window - Flavor Tab

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

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.

Figure 23: Launch Instance Window - Networks Tab

Launch Instance

Networks provide the communication channels for instances in the cloud.

▼ **Allocated** 3 Select networks from those listed below.

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

▼ **Available** 3 Select at least one network

🔍 Click here for filters or full text search.

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

✕ 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.



Figure 24: Launch Instance Window - Network Ports Tab

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.

Figure 25: Launch Instance Window - Security Groups Tab

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 |
| <b>Direction</b> | <b>Ether Type</b>      |
| egress           | IPv4                   |
| ingress          | IPv4                   |
| ingress          | IPv6                   |
| egress           | IPv6                   |

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

▼ 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.

Figure 26: Launch Instance Window - Configuration Tab

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  
Choose 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 Automatic

Scheduler Hints  Configuration Drive

Metadata

Cancel < Back Next > Launch Instance

**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.

Figure 27: Instances Window - Status of CDG VM Installation

| Instance Name            | Image Name    | IP Address       | Flavor   | Key Pair      | Status | Availability Zone | Task     | Power State | Age       | Actions               |
|--------------------------|---------------|------------------|----------|---------------|--------|-------------------|----------|-------------|-----------|-----------------------|
| <input type="checkbox"/> | cdg-bios-dhcp | cdg-cloud-bios-6 | network3 | Not available | Build  | nova              | Spawning | No State    | 0 minutes | Associate Floating IP |

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

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

Figure 28: Instances Window - Status of CDG VM Installation

| Instance Name | Image Name       | IP Address                       | Flavor    | Key Pair | Status | Availability Zone | Task | Power State | Age       | Actions         |
|---------------|------------------|----------------------------------|-----------|----------|--------|-------------------|------|-------------|-----------|-----------------|
| cdg-bios-dhcp | cdg-cloud-bios-6 | network2<br>network3<br>network1 | cdg-cloud | -        | Active | us-east-1-nova    | None | Running     | 0 minutes | Create Snapshot |

- 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.
- 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 log in 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 89](#).

## 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 using CloudFormation \(CF\) Template, on page 68](#)
- [Install Crosswork Data Gateway on Amazon EC2 Manually, on page 75](#)

## Install Crosswork Data Gateway using CloudFormation (CF) Template

- [Extract CF Template Image, on page 68](#)
- [Roles and Policy Permissions, on page 69](#)
- [CF Template Parameters for Installing Crosswork Data Gateway, on page 70](#)
- [Manage CF Template Deployment, on page 73](#)

### Extract CF Template Image

This section explains the procedure to extract and validate the Crosswork Data Gateway template image.



#### Attention

The file names mentioned in this topic are sample names and may differ from the actual file names in release version.

**Step 1** Download the template package (**cw-na-platform-cft-6.0.1-signed.tar.gz**).

**Step 2** Use the following command to unzip the package:

```
tar -xzvf cw-na-platform-cft-6.0.0-signed.tar.gz
```

The contents of the package is unzipped to a new directory. This new directory contains the CF template image and files necessary to validate the image.

For example:

```
tar -xzvf cw-na-platform-cft-6.0.1-signed.tar.gz
x CFT-6.0.1_release500_2.tar.gz
x CFT-6.0.1_release500_2.tar.gz.signature
x README
x CW-CCO_RELEASE.cer
x cisco_x509_verify_release.py3
x cisco_x509_verify_release.py
```

**Step 3** Review the contents of the README file in order to understand everything that is in the package and how it will be validated in the following steps.

**Step 4** Navigate to the directory created in the previous step and use the following command to verify the signature of the installer image:

**Note** Use `python --version` to find out the version of Python on your machine.

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
```

For example:

```
python cisco_x509_verify_release.py3 -e CW-CCO_RELEASE.cer -i CFT-6.0.1_release450_2.tar.gz -s
CFT-6.0.1_release450_2.tar.gz.signature -v dgst -sha512
Retrieving CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from CW-CCO_RELEASE.cer.
Successfully verified the signature of CFT-6.0.1_release450_2.tar.gz using CW-CCO_RELEASE.cer
```

The contents of the package is extracted and validated successfully.

**Step 5** In the directory, locate the `install-cnc-templates` file and follow the instructions provided within its **Description** section. Customize the CF templates in the directory to install Cisco Crosswork on AmazonEKS.

## Roles and Policy Permissions

This section describes the roles and the policy permissions that you must have when deploying the CF template on Amazon. For information on how to create and manage the roles, refer to the Amazon documentation.

**Table 2: Amazon EC2 Roles and Actions Assigned to the Roles**

| Role   | Actions                                                                                                                                                                                                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EC2    | DescribeInternetGateways, DescribeNetworkInterfaces, DescribeImages, DeleteLaunchTemplate, DescribeSubnets, DescribeAccountAttributes, DescribeSecurityGroups, RunInstances, DescribeVpcs, DescribeInstances, CreateNetworkInterface, CreateTags, DescribeKeyPairs, CreateLaunchTemplate, DeleteNetworkInterface, TerminateInstances. |
| ELB    | DescribeLoadBalancers, CreateLoadBalancer, ModifyLoadBalancerAttributes, AddTags, DeleteLoadBalancer.                                                                                                                                                                                                                                 |
| ELB v2 | DescribeLoadBalancers, CreateLoadBalancer, AddTags, DeleteLoadBalancer, CreateTargetGroup, CreateListener, DeleteListener, DescribeTargetGroups, ModifyLoadBalancerAttributes, DescribeListeners, RegisterTargets, DeleteTargetGroup, ModifyTargetGroupAttributes, DescribeTargetHealth.                                              |
| IAM    | CreateNodegroup, DescribeNodegroup, DeleteNodegroup                                                                                                                                                                                                                                                                                   |

## CF Template Parameters for Installing Crosswork Data Gateway

This section describes the parameters that are required when creating the Crosswork Data Gateway control plane, node, pool, and other important containers. It also has parameters that are required for creating EC2 Crosswork Data Gateway NLB stack.

**Table 3: Crosswork Data Gateway Deployment Parameters**

| Parameter       | Description                                                                                                                                                                                                    |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VpcId           | The virtual private cloud (VPC) ID of your existing VPC. For example, vpc-0f83aac74690101a3.                                                                                                                   |
| SecGroup        | Precreated security group that must be applied to the stack. For example, sg-096ff4bc355af16a0. The group must allow ingress access to all ports that Crosswork, NSO, Crosswork Data Gateway, and IOS-XR uses. |
| CDGSSHPassword  | The SSH password to be configured on the Crosswork Data Gateway node.                                                                                                                                          |
| CDGOperPassword | The password to be configured on the Crosswork Data Gateway for Dg-Oper user.                                                                                                                                  |
| CDGAmiId        | The Crosswork Data Gateway AMI ID.                                                                                                                                                                             |
| InstanceType    | The EC2 instance type for the node instances.<br>Default value is m5.2xlarge.<br>This is a mandatory parameter.                                                                                                |
| CNCControllerIP | Host address of the Crosswork Data Gateway controller.<br>This is a mandatory parameter.                                                                                                                       |

| Parameter                  | Description                                                                                                                                                                                                                                                                        |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CNCControllerPassword      | The cw-admin user password used to access Crosswork or CNC Controller.                                                                                                                                                                                                             |
| InterfaceDeploymentMode    | Crosswork Data Gateway deployment mode.<br>The options are: <ul style="list-style-type: none"> <li>• 1: to deploy all the interfaces.</li> <li>• 2: to deploy the Management and Data interfaces.</li> <li>• 3: to deploy the Management, Data, and Control interfaces.</li> </ul> |
| CDGInterface0IPAddress     | A free IP address on the subnet. If set to 0.0.0.0, the IP address is automatically allocated.<br>This is a mandatory parameter.                                                                                                                                                   |
| CDGInterface0SubnetId      | The first interface subnet for the Crosswork Data Gateway VM.                                                                                                                                                                                                                      |
| CDGInterface0Gateway       | The default gateway on the selected subnet. Typically, the first address on the subnet.                                                                                                                                                                                            |
| CDGInterface0SubnetNetmask | The first interface subnet netmask in the dotted-decimal form. For example, 255.255.255.0.<br>This is a mandatory parameter.                                                                                                                                                       |
| CDGInterface1IPAddress     | A free IP address on the first subnet. If set to 0.0.0.0, the IP address is automatically allocated.<br>This is a mandatory parameter.                                                                                                                                             |
| CDGInterface1SubnetId      | The second interface subnet for the Crosswork Data Gateway. The subnet must be in the same availability zone as the <code>CDGInterface0SubnetId</code> .                                                                                                                           |
| CDGInterface1Gateway       | The second interface default gateway on the selected subnet. Typically, the first address on the subnet.<br>This is a mandatory parameter.                                                                                                                                         |
| CDGInterface1SubnetNetmask | The second interface subnet netmask in the dotted-decimal form. For example, 255.255.255.0. This parameter is ignored when dual interface mode is not used.<br>This is a mandatory parameter.                                                                                      |
| CDGInterface2IPAddress     | A free IP address on the second subnet. If set to 0.0.0.0, the IP address is automatically allocated.<br>This is a mandatory parameter.                                                                                                                                            |
| CDGInterface2SubnetId      | The third interface subnet for the Crosswork Data Gateway VM. The subnet must be in the same availability zone as the <code>CDGInterface0SubnetId</code> .                                                                                                                         |

| Parameter                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CDGInterface2Gateway       | The third interface default gateway on the selected subnet. Typically, the first address on the subnet.<br><br>This is a mandatory parameter.                                                                                                                                                                                                                                                                                                                                                                                 |
| CDGInterface2SubnetNetmask | The third interface subnet netmask in the dotted-decimal form. For example, 255.255.255.0. This parameter is ignored when triple interface mode is not used.<br><br>This is a mandatory parameter.                                                                                                                                                                                                                                                                                                                            |
| CNCControllerIP            | Host address of the Crosswork Crosswork Data Gateway controller.                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| HANetworkMode              | The Crosswork Data Gateway HA mode.<br><br>The pool mode options are: <ul style="list-style-type: none"> <li>• L2: Use this option when you specify IP addresses for creating the HA pool.</li> <li>• L3: Use this option when you specify FQDN for creating the HA pool and for multisubnet deployment.</li> </ul>                                                                                                                                                                                                           |
| DataDiskSize               | Size of the Crosswork data disk. The minimum size is 20. Default size is 50.<br><br>This is a mandatory parameter.                                                                                                                                                                                                                                                                                                                                                                                                            |
| CDGProfile                 | The deployment profile of Crosswork Data Gateway. <ul style="list-style-type: none"> <li>• Standard</li> <li>• Extended</li> </ul> This is a mandatory parameter.                                                                                                                                                                                                                                                                                                                                                             |
| CdgInstanceHostname        | The Crosswork Data Gateway instance name, for example CDG-01.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| CloudEnrollmentToken       | The unique enrollment token retrieved from Crosswork Cloud. Crosswork Data Gateway uses this token to automatically enroll with Crosswork Cloud.<br><br>Configure the number of permitted number of autoenrollment requests and the expiry date of the token.<br><br>The default values are: <ul style="list-style-type: none"> <li>• Number of uses: 5</li> <li>• Expiry: 30 days</li> </ul> The maximum accepted values: <ul style="list-style-type: none"> <li>• Number of uses: 50</li> <li>• Expiry: 366 days</li> </ul> |



**Table 4: Crosswork Data Gateway and Network Load Balancer (NLB) Stack Parameters**

| Parameter       | Description                                                           |
|-----------------|-----------------------------------------------------------------------|
| VpcId           | The VPC ID of the worker instances.<br>This is a mandatory parameter. |
| SubnetId1       | The management ID of subnet 1.<br>This is a mandatory parameter.      |
| SubnetId2       | The management ID of subnet 2.<br>This is a mandatory parameter.      |
| DomainName      | The domain name.<br>This is a mandatory parameter.                    |
| HostedZoneId    | The hosted zone ID.<br>This is a mandatory parameter.                 |
| CdgPoolHostname | Name of the Route53 record.<br>This is a mandatory parameter.         |
| CdgTargetIP1    | The IP address 1 of the Management node.                              |
| CdgTargetIP2    | The IP address 2 of the Management node.                              |
| LBIPAddress1    | The first LB IP address on subnet.<br>This is a mandatory parameter.  |
| LBIPAddress2    | The second LB IP address on subnet.<br>This is a mandatory parameter. |

## Manage CF Template Deployment

The following sections explain how to deploy a CF template on Amazon EC2 and verify its installation:

- [Deploy a CF Template, on page 73](#)
- [Monitor the Installation, on page 74](#)

### Deploy a CF Template

You can install Crosswork Data Gateway on Amazon EC2 with custom resources. Depending on the configured parameters, the needed components with the capabilities are also installed.

#### Before you begin

- Make sure that you have met the [Amazon EC2 Settings](#) prescribed for installing Crosswork Data Gateway on Amazon EC2.

- Ensure that you have access to the CloudFormation templates that are stored in the S3 bucket or on your local machine. If the template is in Amazon S3, keep the URL of the template file copied.

---

**Step 1** Log in to the AWS account and navigate to the S3 bucket. If the CF template is on your local computer, you can upload the template.

**Step 2** In the AWS CloudFormation console, navigate to the **Stacks** page and choose **Create stack > With new resources (standard)**. The **Create stack** page opens.

**Step 3** Enter the following details:

- Under **Prerequisite - Prepare template**, select **Template is ready**.
- Under **Specify template > Template source**, select one of the following options:
  - If you have the YAML or JSON file URL directing to the S3 bucket where the CF template is located, select **Amazon S3 URL**. In the **Amazon S3 URL** field, enter the URL and click **Next**.
  - If the CF template is saved on your local computer, select **Upload a template file** and click **Choose File** to select the file that you want to upload. After you have selected the template, Amazon uploads the file and displays the S3 URL. Click **Next**.

**Note** (Optional) Click **View in Designer** to view a visual representation of the execution flow in your CF template.

**Step 4** In the **Specify stack details** page, enter the relevant values for the stack name and parameter values. Click **Next**.

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

**Step 5** Review the parameter values that you have configured.

**Step 6** Under the **Capabilities**, select the check boxes next to:

- **I acknowledge that AWS CloudFormation might create IAM resources with custom names.**
- **I acknowledge that AWS CloudFormation might require the following capability: CAPABILITY\_AUTO\_EXPAND.**

**Step 7** Click **Submit**.

---

### What to do next

The time taken to create the cluster can vary based on the size of your deployment profile and the performance characteristics of your hardware. See [Monitor the Installation, on page 74](#) to know how you can check the status of the installation.

## Monitor the Installation

This section describes how to verify if the deployment is complete without errors.

---

**Step 1** In the CloudFormation console, from the left-hand side **Stacks** pane, select the stack that you have deployed.

**Step 2** The stack details are displayed on the right. Click on each tab in this window to view details of the stack. If the stack creation is in progress, the status of the stack in the **Events** tab is `CREATE_IN_PROGRESS`.

**Step 3** After the stack is 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 **Outputs** tab has details of the VM's interface IP addresses.

## 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 must be configured to install the Crosswork Data Gateway VM successfully.
- The steps in this procedure explain the installation of an Extended Crosswork Data Gateway VM with 3 interfaces.

**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 have been 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.

- 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.

```

AwsIamRole=changeme
ActiveVnics=3
AllowRFC8190=Yes
AuditdAddress=
AuditdPort=60
ControllerCertChainPwd=changeme
ControllerIP=
ControllerPort=30607
ControllerSignCertChain=cw-admin@<controller-IP>:/home/cw-admin/controller.pem
ControllerTlsCertChain=
Deployment=Crosswork On-Premise
Description=changeme
DGAppdataDisk=5

```

```

DGCertChain=
DGCertChainPwd=
DGCertKey=
DNS=changeme
DNSSEC=False
DNSTLS=False
Domain=changeme
EnrollmentPassphrase=
EnrollmentURI=
Hostname=changeme
Label=
LLMNR=False
mDNS=False
NTP=changeme
NTPAuth=False
NTPKey=
NTPKeyFile=
NTPKeyFilePwd=
Profile=Extended
ProxyBypass=
ProxyCertChain=
ProxyCertChainPwd=
ProxyPassphrase=
ProxyURL=
ProxyUsername=
SyslogAddress=
SyslogCertChain=
SyslogCertChainPwd=
SyslogPeerName=
SyslogPort=514
SyslogProtocol=UDP
SyslogTLS=False
UseRemoteAuditd=False
UseRemoteSyslog=False
Vnic0IPv4Address=0.0.0.0 //IP address of management interface
Vnic0IPv4Gateway=0.0.0.1
Vnic0IPv4Method=None
Vnic0IPv4Netmask=0.0.0.0
Vnic0IPv4SkipGateway=False
Vnic0IPv6Address=:0
Vnic0IPv6Gateway=:1
Vnic0IPv6Method=None
Vnic0IPv6Netmask=64
Vnic0IPv6SkipGateway=False
Vnic1IPv4Address=0.0.0.0 //IP address of data interface
Vnic1IPv4Gateway=0.0.0.1
Vnic1IPv4Method=None
Vnic1IPv4Netmask=0.0.0.0
Vnic1IPv4SkipGateway=False
Vnic1IPv6Address=:0
Vnic1IPv6Gateway=:1
Vnic1IPv6Method=None
Vnic1IPv6Netmask=64
Vnic1IPv6SkipGateway=False
Vnic2IPv4Address=0.0.0.0 //leave unchanged to default value.
Vnic2IPv4Gateway=0.0.0.1
Vnic2IPv4Method=None
Vnic2IPv4Netmask=0.0.0.0
Vnic2IPv4SkipGateway=False
Vnic2IPv6Address=:0
Vnic2IPv6Gateway=:1
Vnic2IPv6Method=None
Vnic2IPv6Netmask=64
Vnic2IPv6SkipGateway=False

```

```
dg-adminPassword=changeme
dg-operPassword=changeme
```

```
CloudEnrollmentToken=cloudenrollmenttoken //enter the optional enrollment token to auto enroll
with Crosswork Cloud
EnrollmentURI=enrollmenturi //enter the optional SCP destination host and path to transfer the
enrollment package using SCP (user@host:/path/to/file)
EnrollmentPassphrase=enrollmentpassphrase //enter the optional SCP user passphrase to transfer
the enrollment package
```

- 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 following instance types (both production and lab environment) based on the profile of the Crosswork Data VM you are deploying.

- **m5.4xlarge** - for a Standard VM.
- **m5.8xlarge** - for an Extended VM.

- 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**.  
 3. Click **Add network interface** and add details for a second interface (corresponds to vNIC1) and a third interface (vNIC2) of the VM.

**Important** Please note that the user data for the VM does not have an IP address for vNIC2 as this is assigned during pool creation. It is an AWS requirement to assign an IP address each time a network interface is created. You can either enter an IP address in the **Primary IP** field (static IP) of the third interface or leave it blank (AWS assigns an IP automatically).

- 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 (Standard CDG) or 520 GB (Extended CDG)
  - **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 will fail.

**Step 3** Click **Launch Instance**. Amazon 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.

## Auto-Configuration for Deploying Crosswork Data Gateway

The auto-configuration procedure discovers the configuration parameters that are missing, and it automatically defines the mandatory parameters to install Base VM. The configuration parameters are passed using the Dynamic Host Configuration Protocol (DHCP) framework. In the Day 0 configuration, the auto-configuration mechanism defines only the essential parameters with the default values.

A default password is provided during the auto-configuration to comply with the security policies. On the first login, the `dg-admin` and `dg-oper` users must reset the default password. The data gateway instance does not start the collection services until the default password is changed.

Auto-configuration process supports single NIC deployment. In particular, eth0 is configured for the Management network. The eth0 interface is used for the DHCP interaction. The DHCP server contains the default values that the process uses during the auto-configuration. You can configure or modify the default values using the Interactive Console. For information about how to use the console, see [Change Current System Settings](#).



**Important** The auto-configuration ability supports deployment of Crosswork Data Gateway on OpenStack and Amazon EC2.

### Parameters used during Auto-Configuration

The auto-configuration utility configures the following parameters with the default values. For more information about these parameters, see [Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2](#).

**Table 5: Cisco Crosswork Data Gateway Mandatory Deployment Parameters**

| Name                      | Parameter        | Default Value                                                                                                                                                                 |
|---------------------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AllowRFC8190              | AllowRFC8190     | The default value is <code>Yes</code> .                                                                                                                                       |
| Auditd Server Port        | AuditdPort       | The default port is 60.                                                                                                                                                       |
| Deployment                | Deployment       | The default value is <code>Crosswork Cloud</code> .                                                                                                                           |
| Crosswork Controller Port | ControllerPort   | The default port is 443.                                                                                                                                                      |
| Description               | Description      | The default value is <code>CDG auto configure</code> .                                                                                                                        |
| dg-admin Passphrase       | dg-adminPassword | The default password is <code>changeme</code> .<br>Reset the default value with the password that you have chosen for the dg-admin user.<br>Password must be 8-64 characters. |
| dg-oper Passphrase        | dg-operPassword  | The default password is <code>changeme</code> .<br>Reset the default value with the password you have chosen for the dg-oper user.<br>Password must be 8-64 characters.       |
| Data Disk Size            | DGAppdataDisk    | The default value of this parameter is 5.                                                                                                                                     |
| DNS Address               | DNS              | The default values of this parameter are<br><code>208.67.222.222</code><br><code>208.67.220.220</code>                                                                        |
| DNS Security Extensions   | DNSSEC           | The default value of this parameter is <code>False</code> .                                                                                                                   |
| DNS over TLS              | DNSTLS           | The default value of this parameter is <code>False</code> .                                                                                                                   |

| Name                                 | Parameter             | Default Value                                                                                                                                                      |
|--------------------------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DNS Search Domain                    | Domain                | The default value of this parameter is <code>localdomain</code> .                                                                                                  |
| Crosswork Data Gateway HA mode       | HANetworkMode         | The default value of this parameter is <code>L2</code> .                                                                                                           |
| Hostname                             | Hostname              | The default value of this parameter is <code>dg-&lt;eth0 address&gt;</code> .<br>Where <code>&lt;eth0-address&gt;</code> is the address of vNIC0.                  |
| Link-Local Multicast Name Resolution | LLMNR                 | The default value of this parameter is <code>False</code> .                                                                                                        |
| Multicast DNS                        | mDNS                  | The default value of this parameter is <code>False</code> .                                                                                                        |
| NicAdministration                    | NicAdministration     | The default value of this parameter is <code>eth0</code> .                                                                                                         |
| NicControl                           | NicControl            | The default value of this parameter is <code>eth1</code> .                                                                                                         |
| NicDefaultGateway                    | NicDefaultGateway     | The default value of this parameter is <code>eth0</code> .                                                                                                         |
| NicExternalLogging                   | NicExternalLogging    | The default value of this parameter is <code>eth0</code> .                                                                                                         |
| NicManagement                        | NicManagement         | The default value of this parameter is <code>eth0</code> .                                                                                                         |
| NicNBExternalData                    | NicNBExternalData     | The default value of this parameter is <code>eth1</code> .                                                                                                         |
| NicNBSystemData                      | NicNBSystemData       | The default value of this parameter is <code>eth1</code> .                                                                                                         |
| NicSBData                            | NicSBData             | The default value of this parameter is the last active interface such as <code>eth0</code> if 1-NIC deployment, <code>eth1</code> if 2-NIC.                        |
| NTPv4 Servers                        | NTP                   | The default values of this parameter are<br><code>162.159.200.1</code><br><code>65.100.46.164</code><br><code>40.76.132.147</code><br><code>104.131.139.195</code> |
| Use NTPv4 Authentication             | NTPAuth               | The default value of this parameter is <code>False</code> .                                                                                                        |
| Profile                              | Profile               | The default value of this parameter is <code>Crosswork-Cloud</code> .                                                                                              |
| Syslog Multiserver Mode              | SyslogMultiserverMode | The default value of this parameter is <code>Simultaneous</code> .                                                                                                 |
| Syslog Server Port                   | SyslogPort            | The default value of this parameter is <code>514</code> .                                                                                                          |
| Syslog Server Protocol               | SyslogProtocol        | The default value of this parameter is <code>UDP</code> .                                                                                                          |
| Use Syslog over TLS                  | SyslogTLS             | The default value of this parameter is <code>False</code> .                                                                                                        |



| Name                     | Parameter            | Default Value                                               |
|--------------------------|----------------------|-------------------------------------------------------------|
| Use Remote Auditd Server | UseRemoteAuditd      | The default value of this parameter is <code>False</code> . |
| Use Remote Syslog Server | UseRemoteSyslog      | The default value of this parameter is <code>False</code> . |
| vNIC IPv4 Method         | Vnic0IPv4Method      | The default value of this parameter is <code>DHCP</code> .  |
| vNIC IPv4 Skip Gateway   | Vnic0IPv4SkipGateway | The default value of this parameter is <code>False</code> . |
| vNIC IPv6 Method         | Vnic0IPv6Method      | The default value is <code>None</code> .                    |
| vNIC IPv6 Skip Gateway   | Vnic0IPv6SkipGateway | The default value is <code>False</code> .                   |
| vNIC IPv4 Method         | Vnic1IPv4Method      | The default value is <code>None</code> .                    |
| vNIC IPv4 Skip Gateway   | Vnic1IPv4SkipGateway | The default value is <code>False</code> .                   |
| vNIC IPv6 Method         | Vnic1IPv6Method      | The default value is <code>None</code> .                    |
| vNIC IPv6 Skip Gateway   | Vnic1IPv6SkipGateway | The default value is <code>False</code> .                   |
| vNIC IPv4 Method         | Vnic2IPv4Method      | The default value is <code>None</code> .                    |
| vNIC IPv4 Skip Gateway   | Vnic2IPv4SkipGateway | The default value is <code>False</code> .                   |
| vNIC IPv6 Method         | Vnic2IPv6Method      | The default value is <code>None</code> .                    |
| vNIC IPv6 Skip Gateway   | Vnic2IPv6SkipGateway | The default value is <code>False</code> .                   |

## Enroll Crosswork Data Gateway with Crosswork Cloud

Enrolling a data gateway involves authenticating the gateway instance with Crosswork Cloud using a unique token or package. You have the choice to either pre-configure the enrollment parameter to start the enrollment process when the data gateway is deployed or manually enroll the gateway once it has been installed.

Based on your Crosswork Data Gateway version, choose from the following options to start the enrollment:

- From release 6.0.1 onwards, generate or use an existing enrollment token from Crosswork Cloud and add it to the VM configuration file. See [Autoenroll Crosswork Data Gateway with Crosswork Cloud, on page 82](#) for more information.
- For 5.0 and older releases, generate or reuse an enrollment package, export the token, and register the data gateway with Crosswork Cloud. See [Manually Enroll Crosswork Data Gateway with Crosswork Cloud, on page 87](#) for more information.

## Autoenroll Crosswork Data Gateway with Crosswork Cloud

From the 6.0.1 release, you can choose to preconfigure a single or multiple data gateways to enroll automatically with Crosswork Cloud using an enrollment token. You can opt to generate a fresh enrollment token (CloudEnrollmentToken) or make use of a token that is already in existence.

To enable autoenrollment of the data gateway, you must perform the following:

- [Generate Enrollment Token from Crosswork Cloud, on page 82](#)
- [Add Enrollment Token to Configuration File, on page 86](#)

### Generate Enrollment Token from Crosswork Cloud

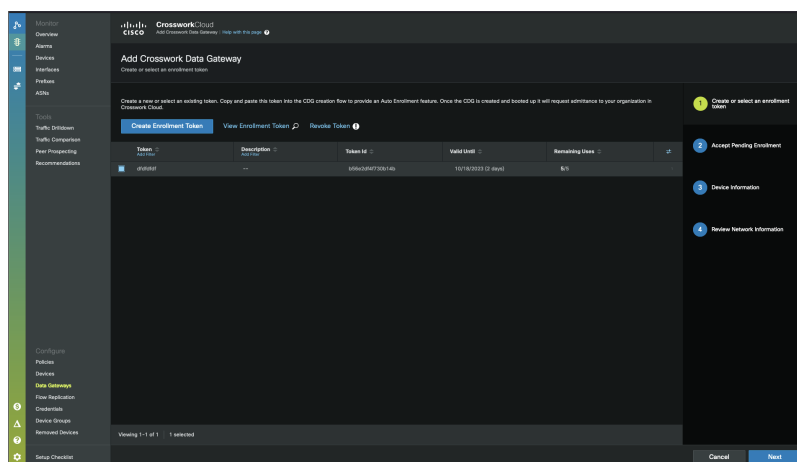
You can create a new or use an existing enrollment token, which can be copied and pasted to the configuration file that you plan on using to install Crosswork Data Gateway.

#### Before you begin

Determine whether you want to create a new enrollment token or utilize an existing token. If there are enough uses left, you can choose to reuse the current token or create a new one. To check the number of uses left for a token, from the Crosswork Cloud UI, window, click **Configure > Data Gateways > Add Crosswork Data Gateway** page. This page lists the available tokens and their state. Review the **Remaining Uses** column.

- Step 1** Log in to Crosswork Cloud.
- Step 2** From the main window, click **Configure > Data Gateways**. The **Data Gateways** page opens.
- Step 3** Click **Add Crosswork Data Gateway**
- Step 4** Depending on your preference to create a new token or use an existing token, follow one of the below procedures:
- **Create a new token:**
    - In the **Add Crosswork Data Gateway** page, click **Create Enrollment Token**.

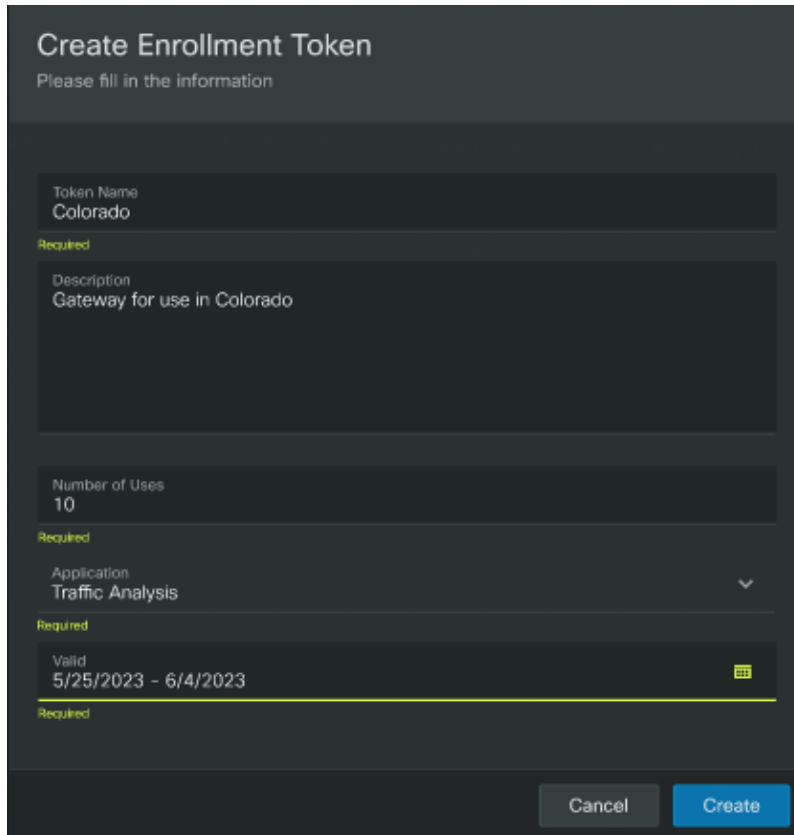
*Figure 29: Crosswork Cloud UI*



- In the **Create Enrollment Token** window, enter the following:
  - Token Name:** Specify a unique name to the token that you are creating.

2. **Description:** Enter a detailed description of the token.
3. **Number of Uses:** Specify the permissible number of token uses. The maximum token usage limit is 50.
4. **Valid Until:** Specify the validity period for the token. The maximum duration is 366 days.

**Figure 30: Create Enrollment Token Window**



**Create Enrollment Token**  
Please fill in the information

Token Name  
Colorado

Required

Description  
Gateway for use in Colorado

Number of Uses  
10

Required

Application  
Traffic Analysis

Required

Valid  
5/25/2023 - 6/4/2023

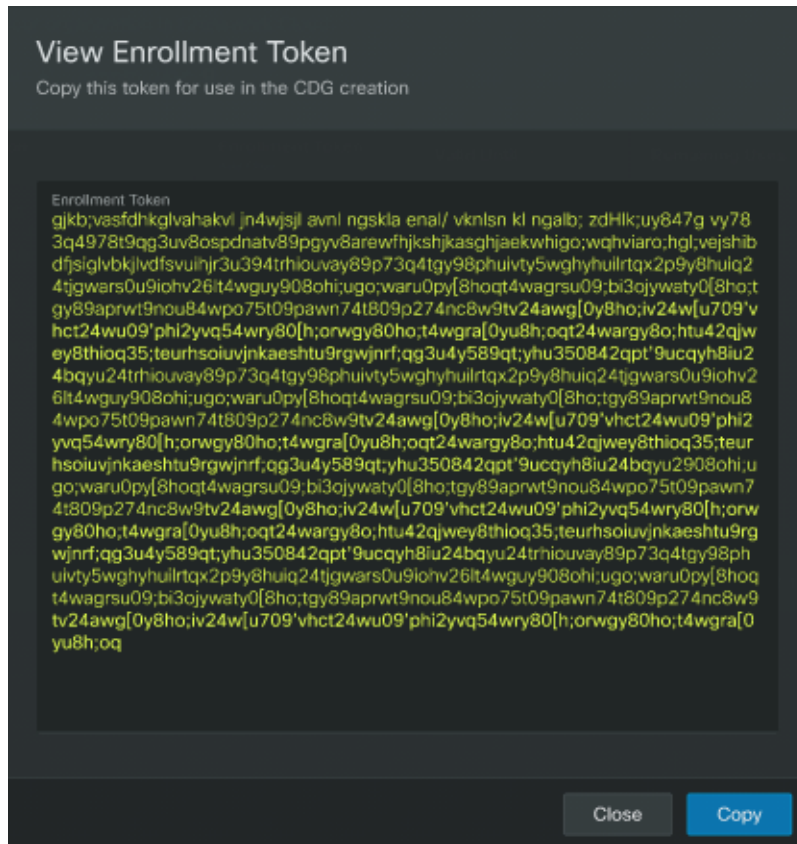
Required

Cancel Create

- c. Click **Create**.

The enrollment token is created and displayed in the **View Enrollment Token** window. The token's content is displayed in a secure JSON format.

Figure 31: View Enrollment Token Window



d. Click **Copy** to copy the token. Paste the copied content in a local file.

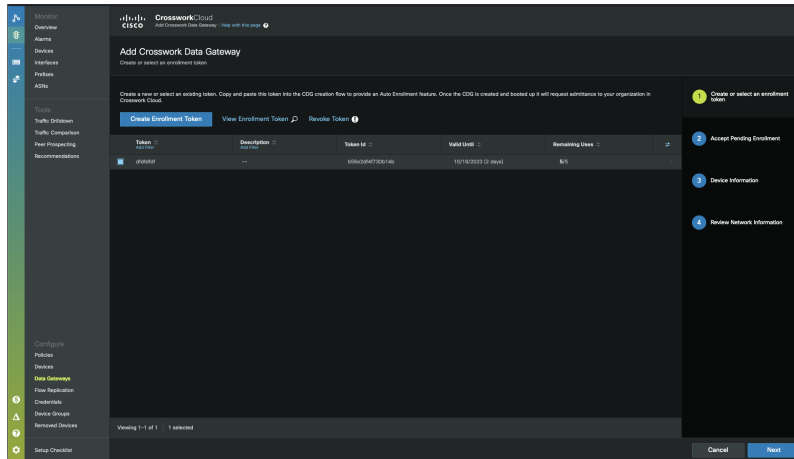
- **Use an existing token**

- a. In the **Add Crosswork Data Gateway** page, select the row corresponding to the token that you intend to use.

When selecting an existing token, consider its expiration date. If the Crosswork Data Gateway will not be installed and registered prior to the expiration date, Cisco recommends you avoid using that token.

You can review the **Valid Until** column on the **Add Crosswork Data Gateway** page to determine the expiration information.

Figure 32: Crosswork Cloud UI

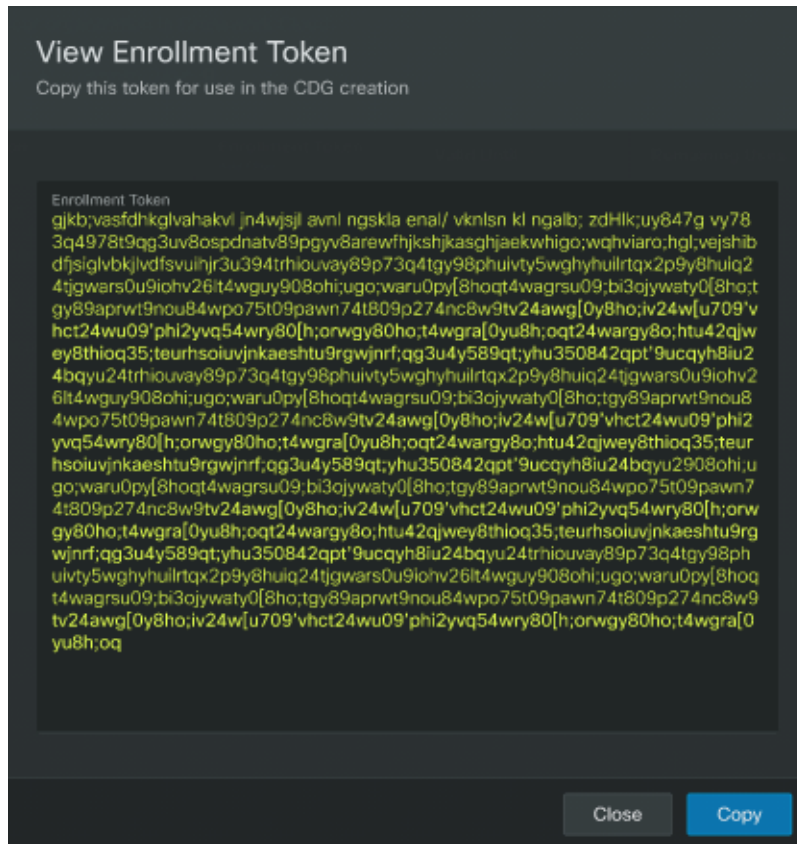


**Note** Clicking on the **Next** button will take you to next stage in the enrollment workflow. For example, upon choosing a row to use a preexisting token and selecting **Next**, Crosswork displays the list of tokens for which the enrollment is pending.

**b.** Click **View Enrollment Token**.

The **View Enrollment Token** window displays the token in a secure JSON format.

Figure 33: View Enrollment Token Window



- c. Click **Copy** to copy the token. Paste the copied content in a local file.

### What to do next

Paste the copied enrollment token into the configuration file you intend to use when installing Crosswork Data Gateway. See [Add Enrollment Token to Configuration File, on page 86](#) for more information.

## Add Enrollment Token to Configuration File

Follow the steps to enable the automatic enrollment of the data gateway with Crosswork Cloud.

### Before you begin

Ensure that you copied the enrollment token from the Crosswork Cloud UI and keep it readily accessible. See [Generate Enrollment Token from Crosswork Cloud, on page 82](#) for more information.

- Step 1** As per your data center, locate the configuration file and paste the enrollment token obtained from the Crosswork Cloud UI. For more information on the configuration files, see the relevant section for your platform:

- [Install Crosswork Data Gateway on VMware](#)

- [Install Crosswork Data Gateway on OpenStack Platform](#)
- [Install Crosswork Data Gateway on Amazon EC2](#)

- Step 2** Connect Crosswork Data Gateway instance with Crosswork Cloud:
- a. Log in to the Crosswork Cloud UI.
  - b. From the main window, click **Configure** > **Data Gateways**. The **Data Gateways** page opens.
  - c. In the table, locate the recently enrolled data gateway and select **Allow** in the **Actions** column. This step allows the gateway to establish communication with the Crosswork Cloud application.

---

### What to do next

Repeat this procedure to enroll the Crosswork Data Gateways in your network with Crosswork Cloud. For more information on Crosswork Cloud, see [Cisco Crosswork Cloud User Guide](#).

If Crosswork Data Gateway has not connected to the Crosswork Cloud service, follow the steps provided in [Troubleshoot the Crosswork Data Gateway Connectivity, on page 92](#).

## Manually Enroll Crosswork Data Gateway with Crosswork Cloud

Every Crosswork Data Gateway must be identified by an immutable identifier. This requires generation of an enrollment package.

You can generate the enrollment package using any of the following methods:

- By using the **Export Enrollment Package** option from the Interactive Console (see [Export Enrollment Package, on page 89](#)).
- By using the **Display base64 Encoded Enrollment Package** option from the Interactive Console (see [Create an Encoded Enrollment Package, on page 90](#)).

The enrollment package is a JSON document created from the information obtained through the OVF template populated by the user during installation. It includes all the necessary information about Crosswork Data Gateway required for registering, such as Certificate, UUID of the Crosswork Data Gateway, and metadata like Crosswork Data Gateway name, creation time, version information, and so on.

If you opted not to export the enrollment package during install, then you must export or copy it before you can enroll the Crosswork Data Gateway with Crosswork Cloud. The steps to do so are described in [Obtain the Enrollment Package, on page 88](#).



---

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

---

Sample enrollment packages in JSON format is shown below:

```
{
  "name": "cdg450-test01",
  "description": "cdg500-test01",
  "profile": {
    "cpu": 8,
```





### What to do next

Depending on the option that you have selected, obtain the enrollment package referring to [Export Enrollment Package, on page 89](#) or [Create an Encoded Enrollment Package, on page 90](#)

### Export Enrollment Package

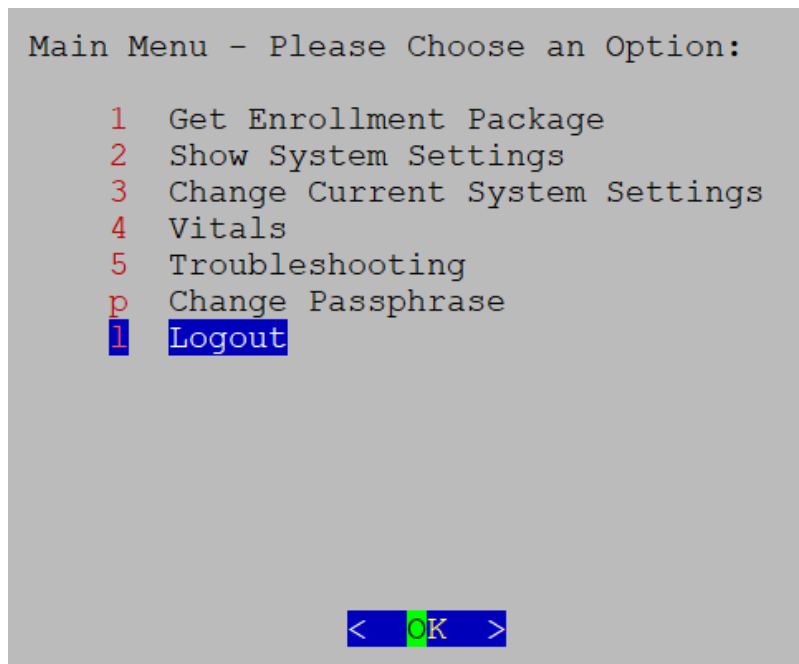
To enroll the Cisco Crosswork Data Gateway with Crosswork Cloud, you must have a copy of the enrollment package on your local computer.



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

*Figure 34: Main Menu*



- 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, 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 91](#).

**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 Cisco Crosswork Data Gateway.

**Step 2** From the Main Menu, select **Get Enrollment Package > Display base64 Encoded Enrollment Package**. The enrollment package content is displayed on the console.





---

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

---

- 
- Step 1** Log in to Crosswork Cloud.
- Step 2** From the main window, click **Configure > Data Gateways**, then click **Add**.
- Step 3** Click **Registration File** to upload the enrollment data file you downloaded from Crosswork Data Gateway, navigate to the location of the .json file, then click **Next**.
- Step 4** Enter a name for the Crosswork Data Gateway.
- Step 5** In the **Application** field, select the Crosswork Cloud application for which you're using this Crosswork Data Gateway instance. Each Crosswork Data Gateway can be applied to one Crosswork Cloud application only.
- Step 6** Complete the rest of the required fields, then click **Next**.
- Step 7** (Optional) Enter a tag name, which allows you to group Crosswork Data Gateways with the same tag, then click **Next**.
- Step 8** Review the Crosswork Data Gateway information that you entered, then click **Next**.
- Step 9** Click **Accept** to accept the security certificate.
- A message appears to indicate the Crosswork Data Gateway was successfully added.
- 

#### What to do next

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

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

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

If the Crosswork Data Gateway has not successfully connected to the Crosswork Cloud service, refer to the [Troubleshoot the Crosswork Data Gateway Connectivity, on page 92](#) 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 6: 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"> <li>1. Log into the Crosswork Data Gateway VM.</li> <li>2. From the main menu, go to <b>5 Troubleshooting &gt; Run show-tech</b>.<br/>Enter the destination to save the tarball containing logs and vitals and click <b>OK</b>.<br/>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<br/> <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.</li> <li>3. From the main menu, go to <b>3 Change Current System Settings &gt; 1 Configure NTP</b>.<br/>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.</li> </ol> |
| <p>Crosswork Data Gateway does not have direct connectivity to external web services.</p>                                                      | <ol style="list-style-type: none"> <li>1. Configure a proxy server if a proxy server is missing in your environment.</li> <li>2. If a proxy server is already present in your environment, check if the proxy URL is correct.</li> <li>3. Check if the credentials of the proxy (certificate, proxy name etc) are correct.</li> </ol> <p>To update the proxy server details on the Crosswork Data Gateway, see <a href="#">Configure Control Proxy</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

