Cisco Crosswork Data Gateway 6.0.1 Installation and Configuration Guide for Cloud Applications

First Published: 2024-02-06

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

CHAPTER 1

Overview

This section contains the following topics:

- Audience, on page 1
- Overview of Cisco Crosswork Data Gateway, on page 1

Audience

This guide is for experienced network administrators who want to deploy Cisco Crosswork Data Gateway for Crosswork Cloud in their network. Users of this guide should have a valid login for the Cisco Crosswork Cloud environment. This guide assumes that you are familiar with the following topics:

- Understanding of the datacenter where you want to install Cisco Crosswork Data Gateway. With this knowledge, you must be able to deploy applications using one of the supported virtualization platforms:
  - VMware vCenter: Deploy OVF templates using VMware vCenter CLI or OVF Tool.
  - OpenStack: Deploy Cisco Crosswork Data Gateway on the OpenStack using the CLI or UI.
  - Amazon EC2: Deploy the CloudFormation template in Amazon Elastic Compute Cloud (EC2).
- Monitoring and troubleshooting of network components.
- Different operating systems used on devices that form your network, such as Cisco IOS-XR, IOS-XE, and NX-OS.
- Proxy settings necessary to connect from your company's internal network to Crosswork Cloud.

Overview of Cisco Crosswork Data Gateway

Cisco Crosswork Data Gateway enables collection of data from the monitored devices and forwards the collected data to the Cisco Crosswork Cloud applications. These applications can use the data for further analysis and if required, alert an administrator for further action.

Attention This guide explains how to install and configure Crosswork Data Gateway for use with Crosswork applications hosted in the cloud and managed by Cisco.

For details on deploying the Crosswork Data Gateway with Crosswork applications deployed in your data center or in a cloud environment that you manage, refer to *Cisco Crosswork Network Controller 6.0 Installation Guide*.

Crosswork Data Gateway has been validated for use with the following Crosswork Cloud SaaS applications:

- Cisco Crosswork Trust Insights is a SaaS solution that reports on the integrity of devices and provides forensics for assured inventory.
- Cisco Crosswork Cloud Traffic Analysis provides rich analysis, visualization, and optimization recommendations for network traffic flows.

CHAPTER 2

Installation Requirements

This chapter provides information about the general guidelines and minimum requirements for installing Crosswork Data Gateway on the following platforms:

- VMware
- OpenStack
- Amazon EC2

Crosswork Data Gateway Preinstallation Checklist

The preinstallation checklist helps you:

- Gather the information required to complete the installation.
- Verify that all system requirements are met and all the required ports are enabled.

Before installing Crosswork Data Gateway, complete the preinstallation checklist.

1. Ensure that the host server meets the resource requirements. See Resource and Configuration Requirements, on page 4
2. Enable ports that are required for Crosswork Data Gateway to operate. See Ports Used, on page 6.
3. Understand if a proxy server may be required in your environment. See Proxy Server Requirements, on page 7.
4. Determine the data center where you plan on deploying Crosswork Data Gateway, and gather the IP address(s) you want to use for deploying Crosswork Data Gateway. For information on the required settings, and details about your environment that must be provided during the Crosswork Data Gateway installation, see Resource and Configuration Requirements, on page 4.
5. Determine whether you want to enroll Crosswork Data Gateway with Crosswork Cloud during the Day 0 installation or after the installation of Crosswork Data Gateway. Cisco recommends the preference for the former enrollment approach through the auto enrollment procedure. See Add Enrollment Token to Configuration File, on page 96 for more information.

Resource and Configuration Requirements

The table shows software requirements for the supported virtualization platforms along with the physical and network resource requirements needed to support the Crosswork Data Gateway.

Note The resource requirements to install Crosswork Data Gateway are the same for all the data centers.

Table 1: VM Requirements for Cloud Applications

Requirement	Description
Data Center	**VMware** • VMware vCenter server 6.7, ESXi 6.5 • VMware vCenter Server 7.0, ESXi 6.5 and 6.7 **OpenStack** • OpenStack OSP16 **Amazon** • Amazon Elastic Cloud Compute
Memory	32 GB
Total Disk space (Boot disk + Data disk)	74 GB (50 GB + 24 GB) **Note** Data disk space is an optional requirement.
vCPU	8

Table 2: Supported Interfaces

<table>
<tr><th>Interfaces</th><th>Description</th></tr>
<tr><td>Interfaces</td><td>
Minimum: 1
Maximum: 3
Crosswork Data Gateway can be deployed with either 1, 2, or 3 interfaces as per the following combinations:
<table>
<tr><th>No. of NICs</th><th>vNIC0</th><th>vNIC1</th><th>vNIC2</th></tr>
<tr><td>1</td><td>• Management traffic
• Control/Northbound External Data traffic
• Southbound Data traffic</td><td>—</td><td>—</td></tr>
<tr><td>2</td><td>• Management traffic</td><td>• Control/Northbound External Data traffic
• Southbound traffic</td><td>—</td></tr>
<tr><td>3</td><td>• Management traffic</td><td>• Control/Northbound External Data traffic</td><td>• Southbound Data traffic</td></tr>
</table>
• Management traffic: for accessing the Interactive Console and troubleshooting the Crosswork Data Gateway VM.
• Control/Northbound External Data traffic: to receive configuration of collection jobs from the Crosswork Cloud and to forward collected data to the Crosswork Cloud.
Important Crosswork Data Gateway can connect to the Cloud only when the Control or Data interface has access to the Internet.
• Southbound Data traffic: for device management and telemetry data.
For deployment using multiple vNICs, you can assign traffic types across different vNICs based on the network design. For example, in a 2 vNIC deployment, you can select either vNIC0 or vNIC1 for processing the following traffic:
• Management traffic
• Control/Northbound External Data traffic
• Southbound Data traffic
</td></tr>
</table>

Table 3: Configuration Options

Interfaces	Description
IP Addresses	One, two, three, or four IPv4 or IPv6 addresses based on the number of interfaces you choose to use. **Note** Crosswork does not support dual stack configurations. Therefore, ALL addresses for the environment must be either IPv4 or IPv6.
NTP Servers	The IPv4 or IPv6 addresses or host names of the NTP servers you plan to use. If you want to enter multiple NTP servers, separate them with spaces. These should be the same NTP servers you use to synchronize devices, clients, and servers across your network. **Note** Confirm that the NTP IP address or host name is reachable on the network or installation fails. The Crosswork Data Gateway host and virtual machine must be synchronized to an NTP server or the enrollment with Crosswork Cloud may not go through.
DNS Servers	The IPv4 or IPv6 addresses of the DNS servers you plan to use. If you want to enter multiple DNS servers, separate them with spaces. These should be the same DNS servers you use to resolve host names across your network.
DNS Search Domain	The search domain you want to use with the DNS servers (for example, cisco.com). You can only have one search domain.
(Optional) Proxy Server	URL of an optional management network proxy server. If your environment requires an HTTP or HTTPS proxy in order to access URLs on the public Internet, you must configure a proxy server for the Cisco Crosswork Data Gateway to connect to Crosswork Cloud.
(Optional) Syslog Server	Hostname, IPv4, or IPv6 address of an optional Syslog server.
(Optional) Auditd Server	Hostname, IPv4, or IPv6 address of an optional Auditd server.

Ports Used

The following table shows the minimum set of ports needed for Crosswork Data Gateway to operate correctly.

Note This is only to enable the base Crosswork Data Gateway functionality. Additional ports may be enabled depending on the application that is running the Crosswork Data Gateway.

Table 4: Ports to be opened for Management Traffic

Port	Protocol	Used for...	Direction
22	TCP	SSH server	Inbound
22 **Note** The SCP port can be configured.	TCP	SCP client	Outbound
123	UDP	NTP Client	Outbound
53	UDP	DNS Client	Outbound
443	TCP	Crosswork Cloud Controller	Outbound

Table 5: Ports to be opened for Control/Northbound External Data Traffic

Port	Protocol	Used for...	Direction
179	TCP	BGP	Outbound
179	TCP	BGP	Inbound
161	UDP	SNMP	Outbound
2055	UDP	Netflow	Inbound

Proxy Server Requirements

Many production environments do not allow direct connectivity to public Internet sites. If your environment requires an HTTP or HTTPS proxy to access URLs on the public Internet, enable Cisco Crosswork Data Gateway to use the configured proxy server. Cisco Crosswork Data Gateway connects to the Crosswork Cloud service through this proxy server. Consult with your network administrator to understand if a proxy server may be required.

If a proxy server is required, the details of the proxy server on the Crosswork Data Gateway are configured in one of the following ways:

- (Recommended) By entering the proxy server credentials during installation. See **Controller and Proxy Settings** in Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 12.
- From the Interactive Console of the Crosswork Data Gateway after installation. See Configure Control Proxy, on page 113

Amazon EC2 Settings

This section describes the settings that must be configured to install Crosswork Data Gateway on Amazon EC2.

Attention Most of the requirements discussed in this section are Amazon EC2 concepts and not imposed exclusively by Crosswork Cloud.

Table 6: Amazon EC2 Prerequisites

Requirement	Description
VPC & Subnets	Virtual Private Cloud (VPC) is created and configured with dedicated subnets for Crosswork interfaces (Management and Data) and Crosswork Data Gateway (Management, Data, and Device) interfaces. Ensure that you do not use any addresses mentioned in the section.
Endpoints	An endpoint is created in your VPC with the following parameters: • **Service name:** EC2 service for the region (availability zone) where you are deploying. • **Private DNS names:** Enabled • **Endpoint type:** Interface • Under **Subnets**, specify the management subnet that you intend to use for the installation. If you are using different management subnets for the Crosswork VM and the Crosswork Data Gateway VM, ensure that you specify both the management subnets to ensure that the endpoint has access to the subnets.
IAM role	A role is created in Identity and Access Management (IAM) with relevant permission policies. An IAM role is an identity that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust. **Note** • The minimum permissions required for a Crosswork role are **ec2:AssignPrivateIpAddresses** and **ec2:UnassignPrivateIpAddresses**. • The trust policy for your role must have the **"Action": "sts:AssumeRole"** condition.
Key pairs	Key pairs (private keys used to log into the VMs) are created and configured.

Requirement	Description
IP addresses	**Crosswork Data Gateway**: IP addresses for Management Traffic and Data Traffic only: • The IP addresses must be able to reach the gateway address for the network where Cisco Crosswork Data Gateway will be installed, or the installation fails. • Now, your IP allocation is permanent and cannot be changed without redeployment. For more information, contact the Cisco Customer Experience team.
Security group	A security group must be created and configured to specify which ports or traffic are allowed.
Instance type	The **m5.2xlarge** instance type is supported for Crosswork Data Gateway (production and lab deployments) deployments.
CloudFormation (CF) template	The CF template (.yaml) files for Crosswork Data Gateway VMs that must be uploaded during the installation using CloudFormation templates procedure. For more information, see Install Crosswork Data Gateway using CloudFormation (CF) Template, on page 78.
User data	The VM-specific parameters script that must be specified during the manual installation procedure. For more information, see: • Install Crosswork Data Gateway using CloudFormation (CF) Template, on page 78 • Install Crosswork Data Gateway on Amazon EC2 Manually, on page 85

CHAPTER 3

Installation Tasks

This section contains the following topics:

Install Cisco Crosswork Data Gateway

Cisco Crosswork Data Gateway is initially deployed as a VM called Base VM 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	Install Crosswork Data Gateway using vCenter vSphere Client, on page 25 Install Crosswork Data Gateway via OVF Tool, on page 34

OpenStack	Install Crosswork Data Gateway on OpenStack from OpenStack CLI, on page 39 Install Crosswork Data Gateway on OpenStack from the OpenStack UI, on page 54
Amazon EC2	Install Crosswork Data Gateway using CloudFormation (CF) Template, on page 78 Install Crosswork Data Gateway on Amazon EC2 Manually, on page 85

2. Plan your installation. See Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 12 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 88. This feature is supported only on OpenStack and Amazon EC2 platforms.

3. 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 96. 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 97.

4. Register Cisco Crosswork Data Gateway with Crosswork Cloud. See Register Crosswork Data Gateway with Crosswork Cloud Applications, on page 101.

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, on page 131). 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, on page 105.

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, on page 108. 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 7: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios

Label	Key	Description	Additional Information
Host Information			
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 `No`, `Yes`, or `Ask`, where the initial configuration script prompts for confirmation. The default value is `Yes`.	
Private Key URI	`DGCertKey`	URI to private key file for session key signing. You can retrieve this using SCP (`user@host:path/to/file`).	Crosswork Cloud uses self-signed certificates for handshake with Cisco Crosswork Data Gateway. These certificates are generated at installation. However, if you want to use third party or your own certificate files enter these 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.
Certificate File and Key Passphrase	`DGCertChainPwd`	SCP user passphrase to retrieve the Cisco Crosswork Data Gateway PEM formatted certificate file and private key.	

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.
Passphrases			
dg-admin Passphrase*	`dg-adminPassword`	The password you have chosen for the dg-admin user. Password must be 8–64 characters.	
dg-oper Passphrase*	`dg-operPassword`	The password you have chosen for the dg-oper user. Password must be 8-64 characters.	
Interfaces **Note** 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 **None**.			
vNIC Role Assignment			

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 `eth0`, `eth1`, `eth2`, or `eth3`. The default value is `eth0`.	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 eth0 and eth1 interfaces. • The NicControl, NicNBExternalData, and NicSBData roles map to eth1. • The NicControl, NicNBExternalData, NicSBData roles map to `eth1`. • The NicSBData role maps to `eth2`. • The NicControl, and NicNBExternalData roles map to `eth1`.
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 `eth0`, `eth1`, `eth2`, or `eth3`. The default value is `eth0`.	
NicExternalLogging*	`NicExternalLogging`	Interface used to send logs to Crosswork Cloud. Options are `eth0`, `eth1`, `eth2`, or `eth3`. The default value is `eth0`.	
NicManagement*	`NicManagement`	Interface used to send the enrollment and other management traffic. Options are `eth0`, `eth1`, `eth2`, or `eth3`. The default value is `eth0`.	
NicControl*	`NicControl`	Interface used for sending the destination, device, and collection configuration. Options are `eth0`, `eth1`, `eth2`, or `eth3`. The default value is `eth0`.	
NicNBSystemData*	`NicNBSystemData`	Interface used to send the collected data to the system destination. Options are `eth0`, `eth1`, `eth2`, or `eth3`. The default value is `eth0`.	

Label	Key	Description	Additional Information
NicNBExternalData*	`NicNBExternalData`	Interface used to send collection data to Crosswork Cloud. Options are `eth0`, `eth1`, `eth2`, or `eth3`. The default value is `eth0`.	
NicSBData*	`NicSBData`	Interface used to collect data from all devices. Options are `eth0`, `eth1`, `eth2`, or `eth3`. The default value is `eth0`.	
vNIC IPv4 Address (vNIC0, vNIC1, and vNIC2 based on the number of interfaces you choose to use)			

Label	Key	Description	Additional Information

vNIC IPv4 Method*	`Vnic0IPv4Method`
	`Vnic1IPv4Method`
	`Vnic2IPv4Method`
		Options are `None`, `Static`, or `DHCP`.
		Note DHCP support is enabled only for deployments performed using the QCOW2 images.
		To use IPv4 address, select Method as `Static` or `DHCP`, and select the vNICxIPv6 Method as `None`.
		The default value for Method is `None`.
			If you have selected **Method** as:
			• **None**: Skip the rest of the fields for IPv4 address. Enter information in the vNIC IPv6 Address parameters.
			• **Static**: Enter information in **Address**, **Netmask**, **Skip Gateway**, and **Gateway** fields
			• **DHCP**: Values for the vNIC IPv4 Address parameters are assigned automatically.
			Do not change the default values.

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 `True` or `False`.
		Selecting `True` skips configuring a gateway.
		The default value is `False`.	

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

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

Label	Key	Description	Additional Information

vNIC IPv6 Method*	`Vnic0IPv6Method`
	`Vnic1IPv6Method`
	`Vnic2IPv6Method`
		Options are `None`, `Static`, `DHCP` or `SLAAC (QCOW2 only)`.
		The default value for **Method** is `None`.
		Note DHCP support is enabled only for deployments performed using the QCOW2 images.
			If you have selected **Method** as:
			- **None**: Skip the rest of the fields for IPv6 address. Enter information in the **vNIC*x* IPv4 Address** parameters.
			- **Static**: Enter information in **Address**, **Netmask**, **Skip Gateway**, and **Gateway** fields
			- **DHCP**: Values for the vNIC IPv6 Address parameters are assigned automatically.
			Do not change the VnicxIPv6Address default values.

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

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

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

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

DNS Servers			
DNS Address*	`DNS`	Space-delimited list of IPv4 or IPv6 addresses of the DNS server accessible in the management interface.	
DNS Search Domain	`Domain`	DNS search domain. The default value is `localdomain`.	

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

Label	Key	Description	Additional Information
Use NTPv4 Authentication	`NTPAuth`	Select `True` to use NTPv4 authentication. The default value is `False`.	The `NTPKey`, `NTPKeyFile`, and `NTPKeyFilePwd` can be configured only when the `NTPAuth` is set to `True`.
NTPv4 Keys	`NTPKey`	Key IDs to map to the server list. Enter space-delimited list of Key IDs.	
NTPv4 Key File URI	`NTPKeyFile`	SCP URI to the chrony key file.	
NTPv4 Key File Passphrase	`NTPKeyFilePwd`	Password of SCP URI to the chrony key file.	
Remote Syslog Server			

Label	Key	Description	Additional Information
Use Remote Syslog Server*	`UseRemoteSyslog`	Select `True` to send syslog messages to a remote host. The default value is `False`.	Configuring an external syslog server sends service events to the external syslog server. Otherwise, they are logged only to the Cisco Crosswork Data Gateway VM. If you want to use an external syslog server, you must specify these seven settings. **Note** The host with the URI files must be reachable on the network (from vNIC0 interface via SCP) and files must be present at the time of install.
Syslog Server Address	`SyslogAddress`	IPv4 or IPv6 address of a syslog server accessible in the management interface. **Note** If you are using an IPv6 address, surround it with square brackets ([1::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 `UDP`, `TCP`, or `RELP` to send the syslog. The default value is `UDP`.	
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 Simultaneous). Options are `Simultaneous` or `Failover`. The default value is `Simultaneous`.	
Use Syslog over TLS	`SyslogTLS`	Select `True` to use TLS to encrypt syslog traffic. The default value is `False`.	
Syslog TLS Peer Name	`SyslogPeerName`	The syslog server hostname exactly as entered in the server certificate SubjectAltName or subject common name.	
Syslog Root Certificate File URI	`SyslogCertChain`		

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.	
Remote Auditd Server			
Use Remote Auditd Server*	`UseRemoteAuditd`	Select `True` to send Auditd message to a remote host. The default value is `False`.	Configure the Crosswork Data Gateway VM to send auditd messages to a remote server. Specify these three settings to forward auditd messages to an external Auditd server.
Auditd Server Address	`AuditdAddress`	Hostname, IPv4, or IPv6 address of an optional Auditd server.	
Auditd Server Port	`AuditdPort`	Port number of an optional Auditd server. The default port number is `60`.	
Controller and Proxy Settings			
Proxy Server URL	`ProxyURL`	URL of an optional HTTP proxy server.	In Cloud deployment, Cisco Crosswork Data Gateway must connect to the Internet via TLS. If you use a proxy server, specify these parameters.
Proxy Server Bypass List	`ProxyBypass`	Comma-separated list of addresses and hostnames that will not use the proxy.	
Authenticated Proxy Username	`ProxyUsername`	Username for authenticated proxy servers.	
Authenticated Proxy Passphrase	`ProxyPassphrase`	Passphrase for authenticated proxy servers.	
HTTPS Proxy SSL/TLS Certificate File URI	`ProxyCertChain`	HTTPS proxy PEM formatted SSL/TLS certificate file retrieved using SCP.	
HTTPS Proxy SSL/TLS Certificate File Passphrase	`ProxyCertChainPwd`	Password of SCP user to retrieve proxy certificate chain.	
Enrollment Package Transfer			

Label	Key	Description	Additional Information
Autoenrollment token	`CloudEnrollmentToken`	The unique enrollment token retrieved from Crosswork Cloud. Crosswork Data Gateway uses this token to automatically enroll with Crosswork Cloud. Configure the number of permitted number of autoenrollment requests and the expiry date of the token. The default values are: • Number of uses: 5 • Expiry: 30 days The maximum accepted values: • Number of uses: 50 • Expiry: 366 days	
Enrollment Destination Host and Path**	`EnrollmentURI`	SCP host and path to transfer the enrollment package using SCP (`user@host:/path/to/file`).	Cisco Crosswork Data Gateway requires the Enrollment package to enroll with Crosswork Cloud. If you specify these parameters during the installation, the enrollment package is automatically transferred to the local host once Cisco Crosswork Data Gateway boots up for the first time. If you do not specify these parameters during installation, then export enrollment package manually by following the procedure Obtain the Enrollment Package, on page 98.
Enrollment Passphrase**	`EnrollmentPassphrase`	SCP user passphrase to transfer enrollment package.	

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

Install Crosswork Data Gateway on VMware

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

- Install Crosswork Data Gateway using vCenter vSphere Client, on page 25
- Install Crosswork Data Gateway via OVF Tool, on page 34

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 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.

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**.

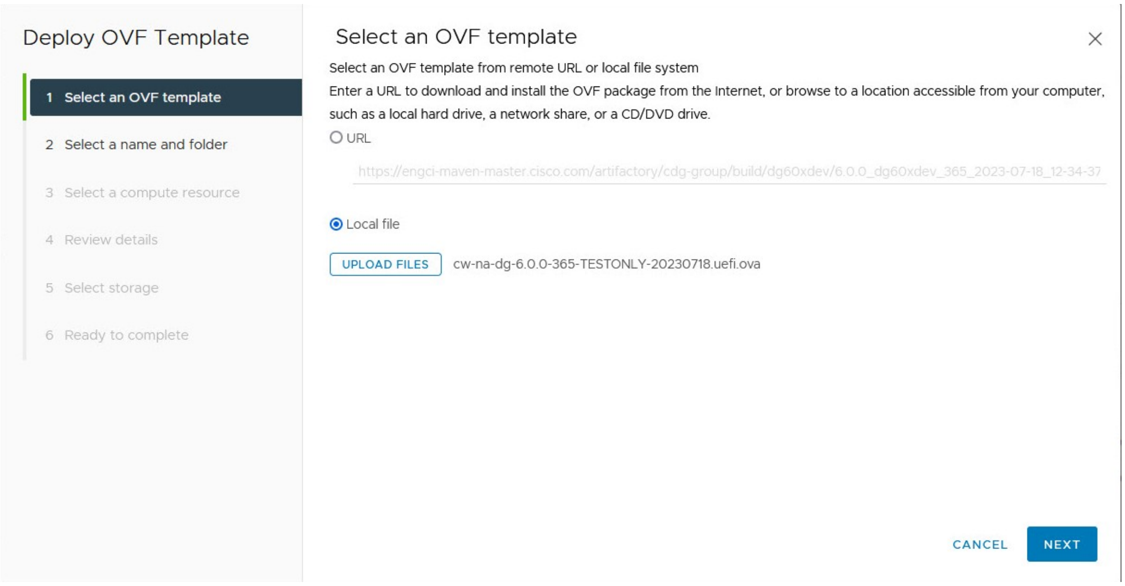
Warning The default VMware vCenter deployment timeout is 15 minutes. If the time taken to fill the OVF template exceeds 15 minutes, vCenter times out and you have to start over again. To prevent this, it is recommended that you plan for the installation by having the necessary parameters and requirements ready. See Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 12 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



Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

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

○ URL

https://engci-maven-master.cisco.com/artifactory/cdg-group/build/dg60xdev/6.0.0_dg60xdev_365_2023-07-18_12-34-37

● Local file

UPLOAD FILES cw-na-dg-6.0.0-365-TESTONLY-20230718.uefi.ova

CANCEL NEXT

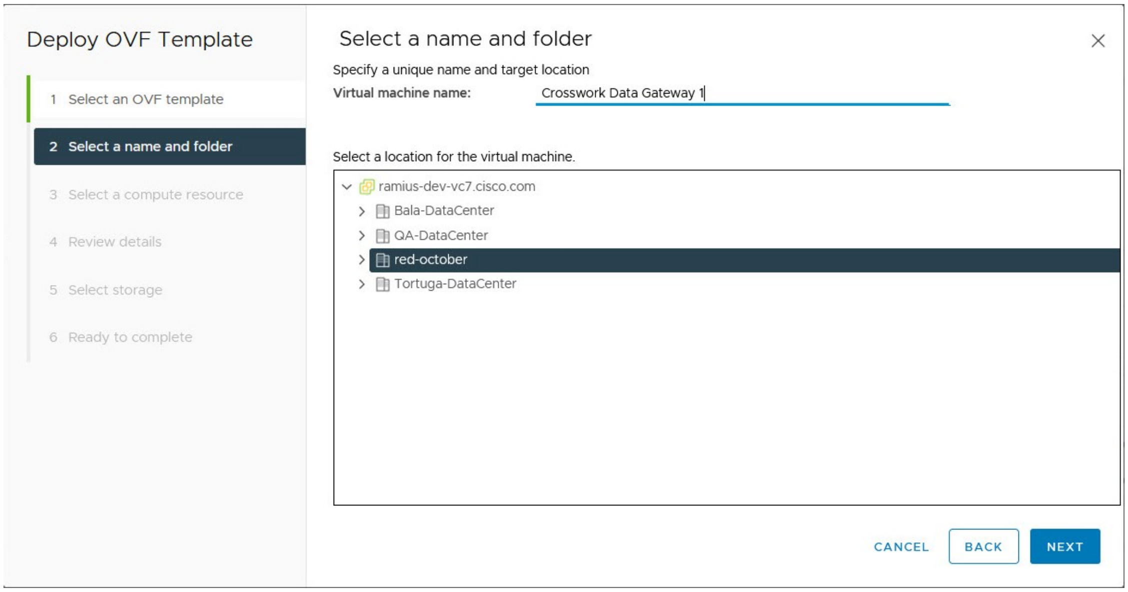
Step 6 Click **Next** to go to **2 Select name and folder**, as shown in the following figure.

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



Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name: Crosswork Data Gateway 1

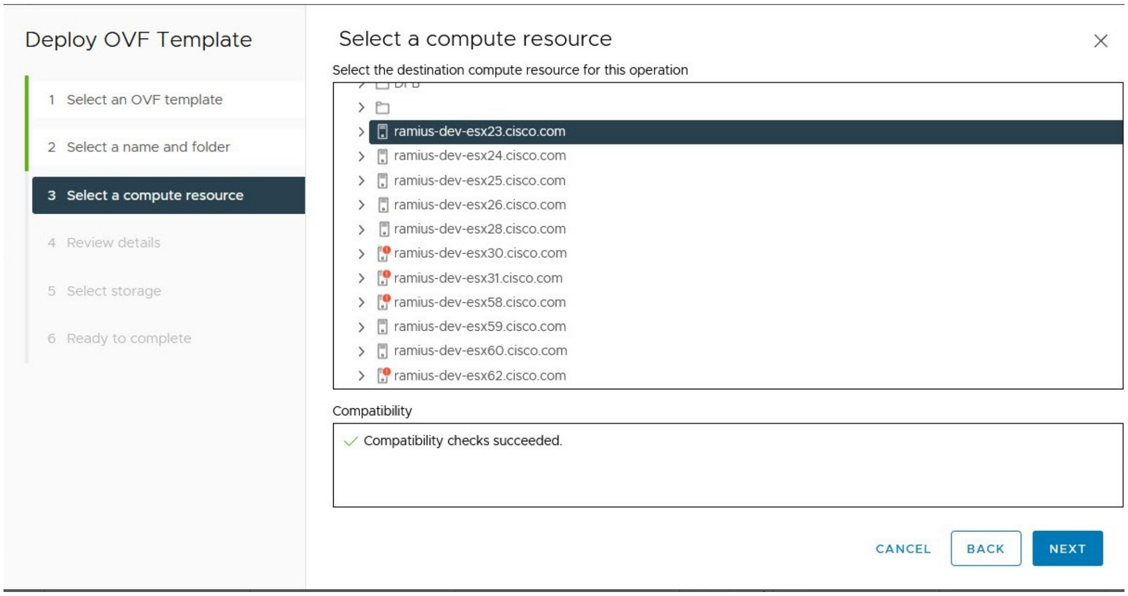
Select a location for the virtual machine.

- ramius-dev-vc7.cisco.com
  - Bala-DataCenter
  - QA-DataCenter
  - red-october
  - Tortuga-DataCenter

CANCEL BACK NEXT

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



Select a compute resource

Select the destination compute resource for this operation

- ramius-dev-esx23.cisco.com
- ramius-dev-esx24.cisco.com
- ramius-dev-esx25.cisco.com
- ramius-dev-esx26.cisco.com
- ramius-dev-esx28.cisco.com
- ramius-dev-esx30.cisco.com
- ramius-dev-esx31.cisco.com
- ramius-dev-esx58.cisco.com
- ramius-dev-esx59.cisco.com
- ramius-dev-esx60.cisco.com
- ramius-dev-esx62.cisco.com

Compatibility

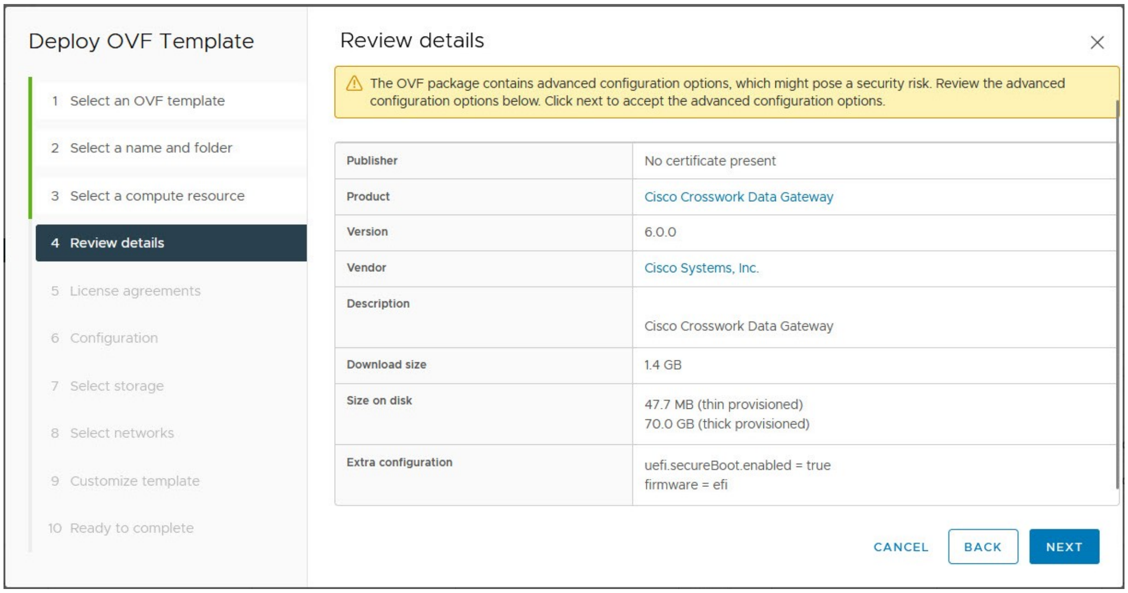
✓ Compatibility checks succeeded.

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



Review details

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

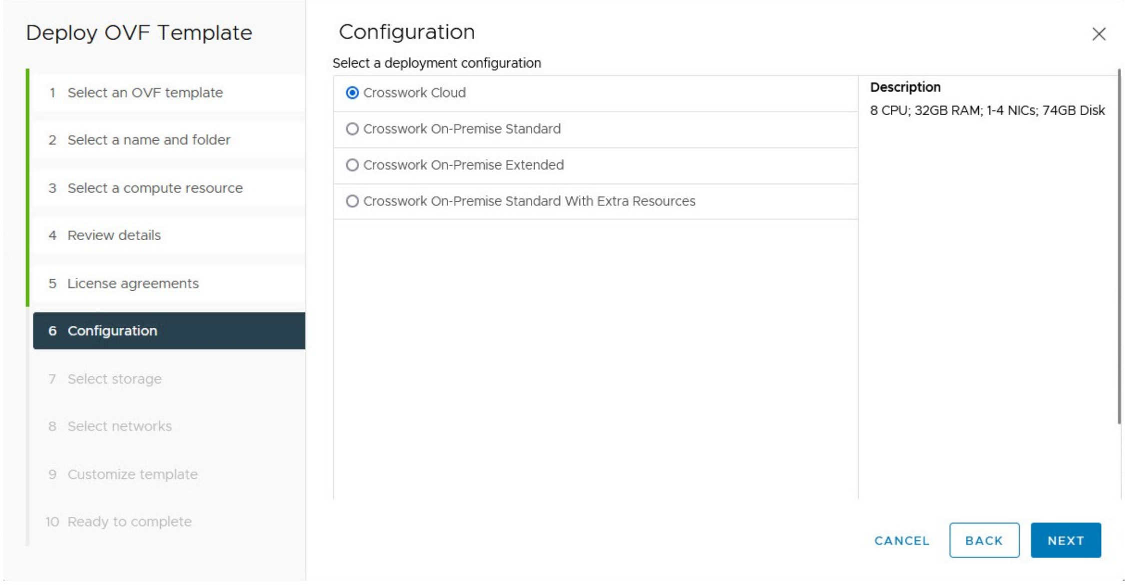
Publisher	No certificate present
Product	Cisco Crosswork Data Gateway
Version	6.0.0
Vendor	Cisco Systems, Inc.
Description	Cisco Crosswork Data Gateway
Download size	1.4 GB
Size on disk	47.7 MB (thin provisioned) 70.0 GB (thick provisioned)

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

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



Deploy OVF Template

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

Configuration

Select a deployment configuration

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

Description

8 CPU; 32GB RAM; 1-4 NICs; 74GB Disk

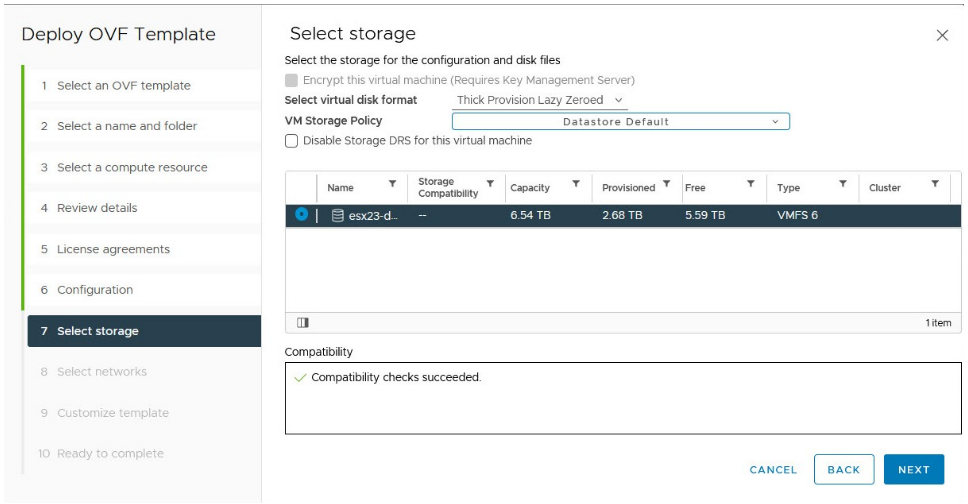
Step 11 Click **Next** to go to **7 Select storage**, as shown in the following figure.

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

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

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

Figure 6: Deploy OVF Template - Select storage Window



Deploy OVF Template

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

Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thick Provision Lazy Zeroed

VM Storage Policy: Datastore Default

□ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	Type	Cluster
●	esx23-d...	--	6.54 TB	2.68 TB	5.59 TB	VMFS 6	

1 item

Compatibility

✓ Compatibility checks succeeded.

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.

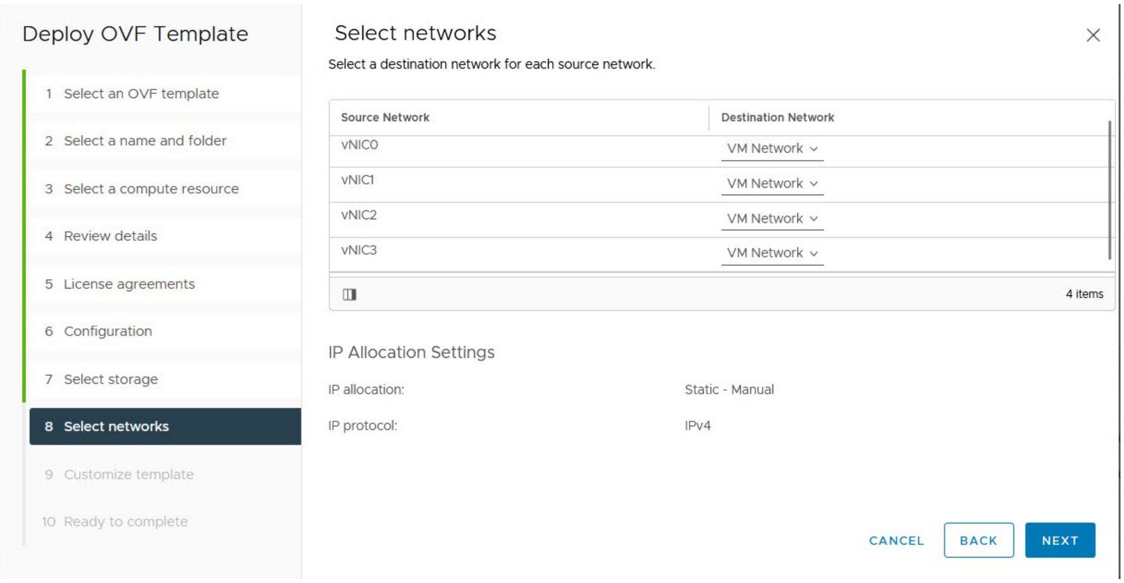
The names used for your network varies based on how the environment was originally configured. You can modify the names in Step 13 based on the settings you configure when reviewing the installation parameters.

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



Select networks

Select a destination network for each source network.

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

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

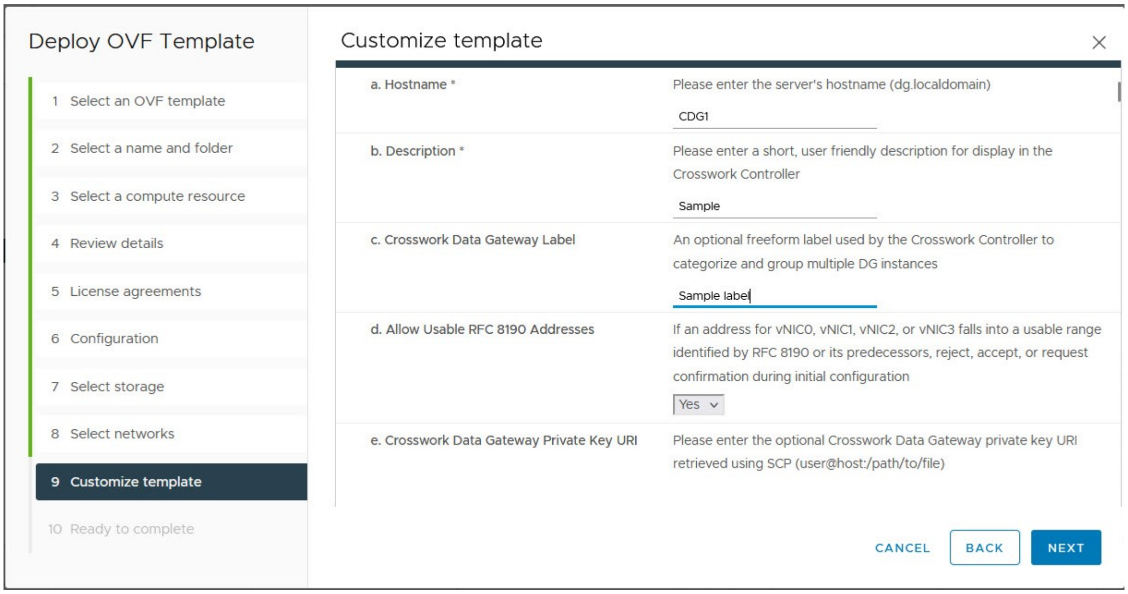
Step 13 Click **Next** to go to **9 Customize template**, with the **Host Information Settings** already expanded. Enter the information for the parameters as described in Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 12.

Values that are not explicitly mentioned in Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 12 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 > Host information Window



Customize template

a. Hostname * — Please enter the server's hostname (dg.localdomain)
CDG1

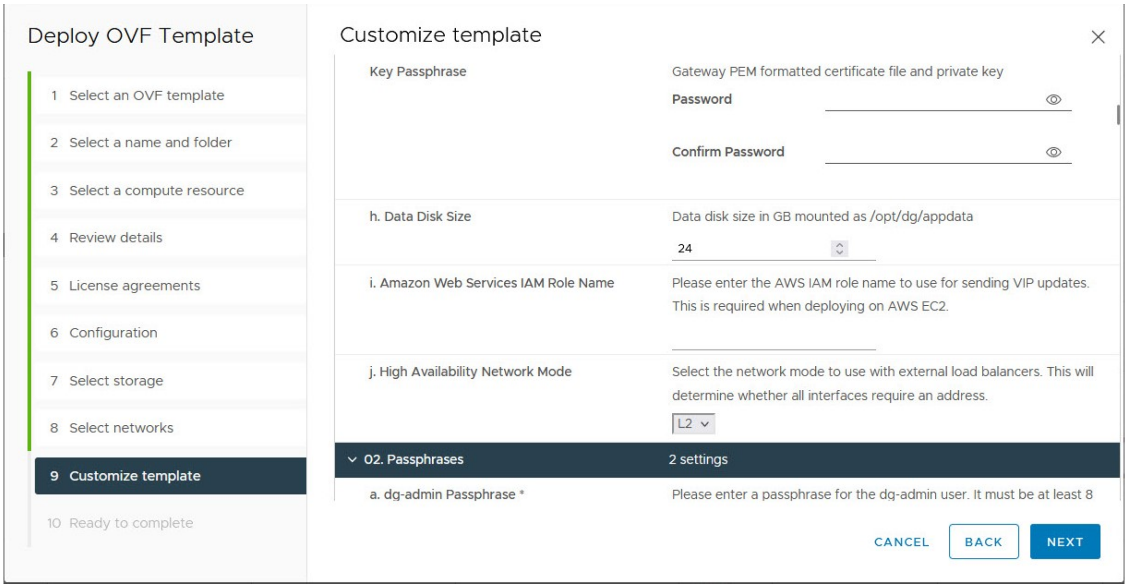
b. Description * — Please enter a short, user friendly description for display in the Crosswork Controller
Sample

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 > Host information Window > High Availability Network Mode



Customize template

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

02. Passphrases — 2 settings

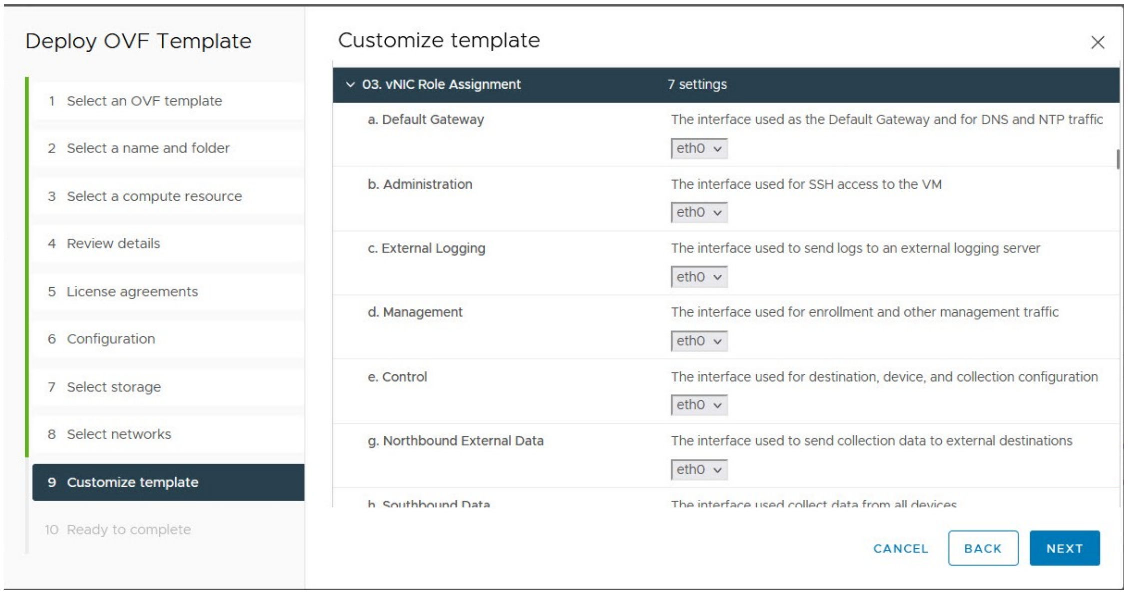
a. dg-admin Passphrase * — Please enter a passphrase for the dg-admin user. It must be at least 8

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

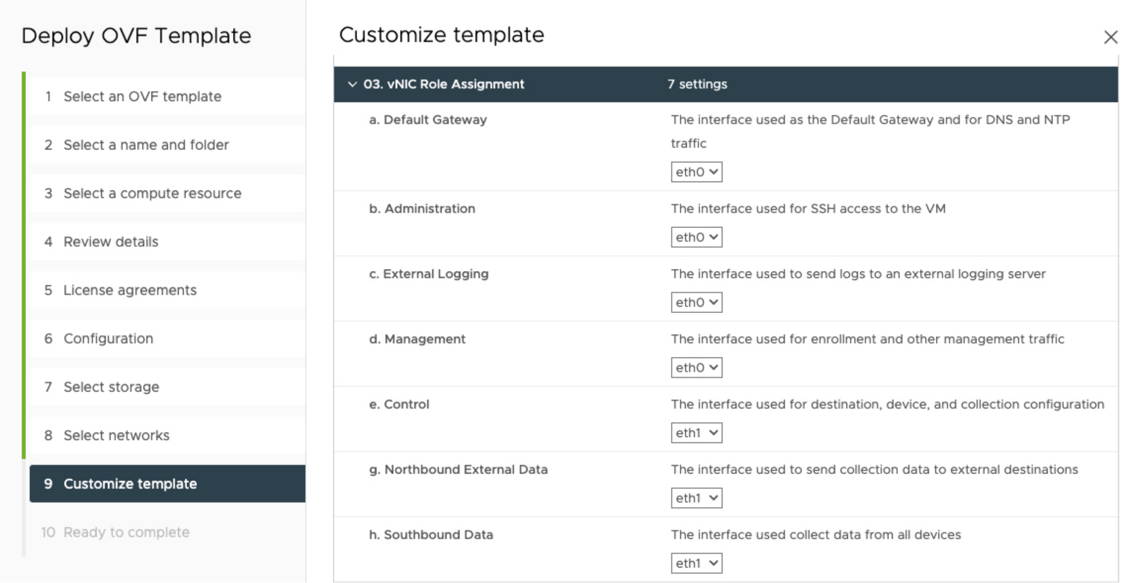
1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Configuration
7 Select storage
8 Select networks
9 Customize template
10 Ready to complete

Customize template

03. vNIC Role Assignment — 7 settings

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

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



Deploy OVF Template

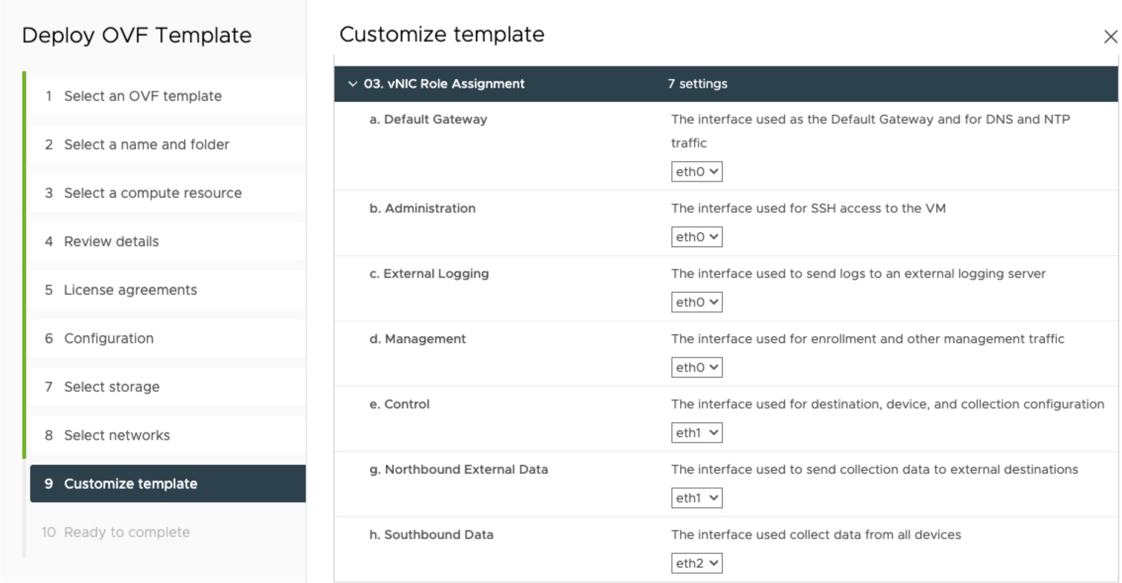
1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Configuration
7 Select storage
8 Select networks
9 Customize template
10 Ready to complete

Customize template

03. vNIC Role Assignment — 7 settings

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

b. Administration — The interface used for SSH access to the VM — eth0

c. External Logging — The interface used to send logs to an external logging server — eth0

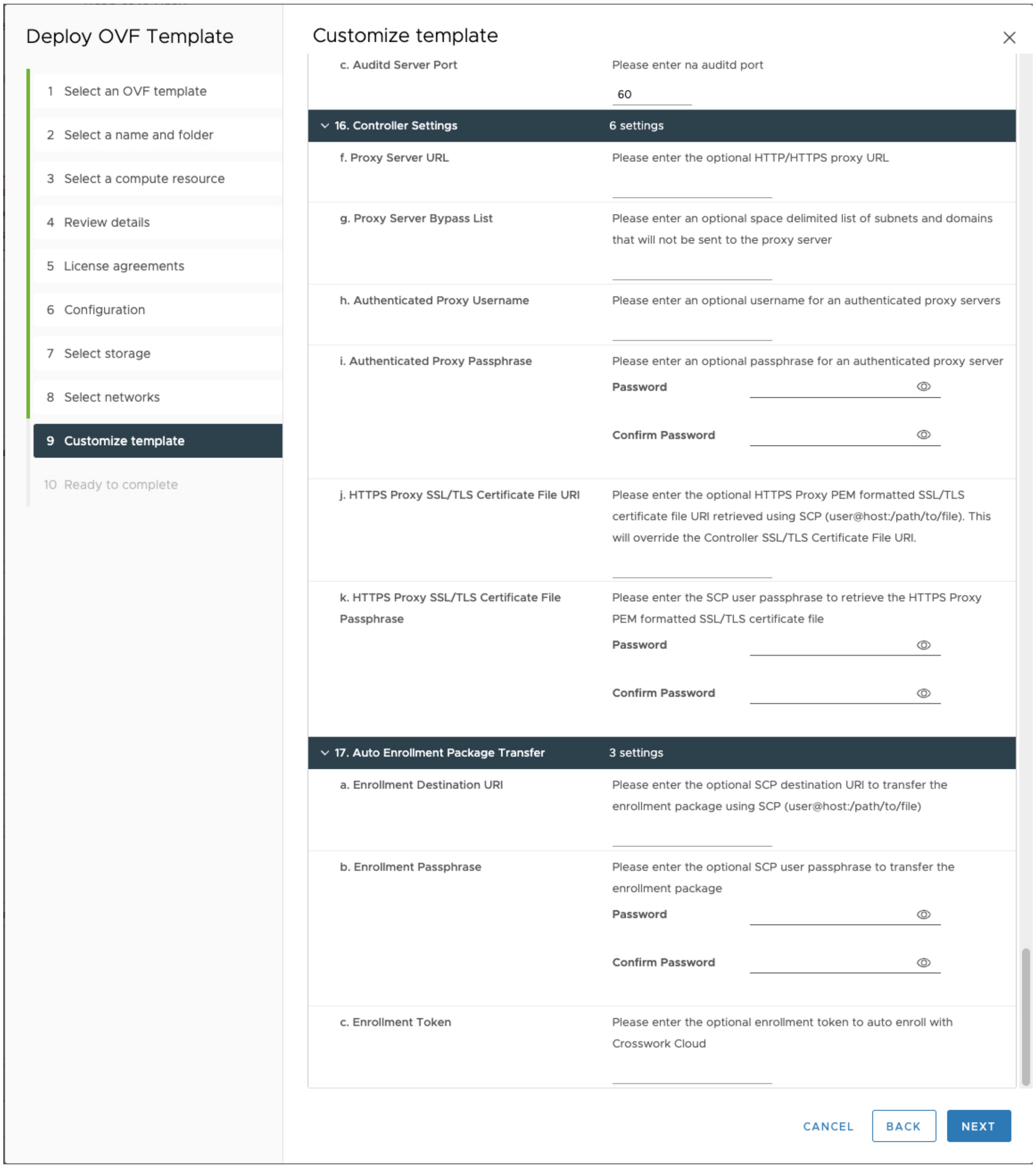
d. Management — The interface used for enrollment and other management traffic — eth0

e. Control — The interface used for destination, device, and collection configuration — eth1

g. Northbound External Data — The interface used to send collection data to external destinations — eth1

h. Southbound Data — The interface used collect data from all devices — eth2

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



c. Auditd Server Port — Please enter na auditd port: 60

16. Controller Settings — 6 settings

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
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
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
Password
Confirm Password

c. Enrollment Token — Please enter the optional enrollment token to auto enroll with Crosswork Cloud

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:

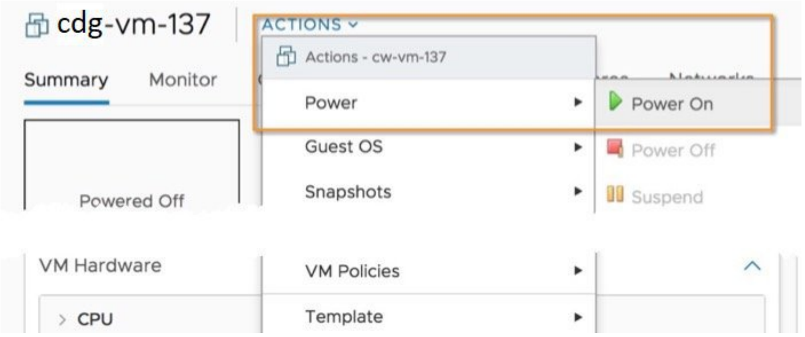
a) Open the vCenter vSphere client.

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

Wait for the deployment status to become 100%. 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 38.

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 98.

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 12 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:

```
ovftTool --version
```

Step 2 Download the OVA and the sample script files from 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 36.

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 7: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 13 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-aio:~/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:
```

```
- 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 38. 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 39.

Proceed to enrolling the Crosswork Data Gateway with Crosswork Cloud. See Obtain the Enrollment Package, on page 98.

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 38
- Access Crosswork Data Gateway VM from SSH, on page 39

To log out of the Crosswork Data Gateway VM, see Log Out of Crosswork Data Gateway VM, on page 39.

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 **l 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 39
- Install Crosswork Data Gateway on OpenStack from the OpenStack UI, on page 54

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 12.
- 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 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. Contact Cisco Customer Experience team if access to cisco.com is not possible due to security restrictions, or if you did not get a successful verification message after running the script.

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

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

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

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

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 12 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 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.text`. You will need to specifiy the same IP addresses when creating the ports for the VM in Step 9.

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

f) Proceed to **Step 5**.

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

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

b) Open the `config.txt` file and modify the parameters as per your installation requirements. Refer to the section Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 12 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 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) 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-vol1
```

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

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

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

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

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

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

Sample commands to create ports for CDG VMs with 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-cdg1.txt --block-device-mapping
vdb=cdg1:::true cdg1-nodhcp
```

OR

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

Commands to install Crosswork Data Gateway VM with 1 NIC with DHCP

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

For example:

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

OR

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

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

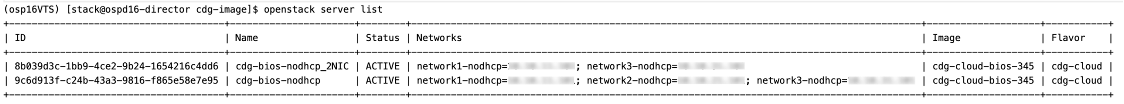
For example, the command to install a VM with 2 NICs is:

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

Verify that the Crosswork Data Gateway VMs were installed successfully.

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

```
openstack server list
```



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

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

From OpenStack CLI

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

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

For example:

```
openstack console url show cdg-dhcp
```

2. Log in as the dg-admin or dg-oper user (as per the role assigned to you) and the corresponding password you had entered in the `config.txt` file of the VM. The Crosswork Data Gateway Interactive console is displayed after you 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 98.

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 12.
- 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 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. Please contact Cisco Customer Experience team if access to cisco.com is not possible due to security restrictions, or if you did not get a successful verification message after running the script.

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

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

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

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

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.**

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 12 for more information.

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

This is a sample `config.txt` file for a 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 12 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 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) Repeat **Step 4 (b)** and **Step 4 (c)** to update and save a unique `config.txt` file for each VM using static addressing.

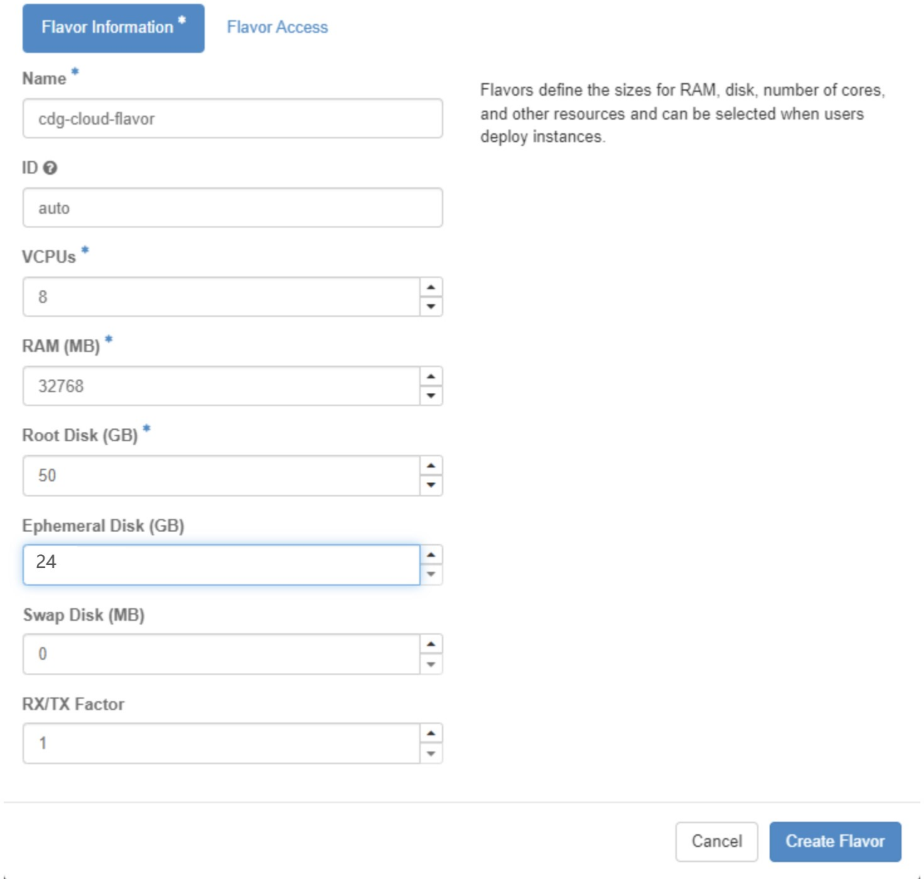
e) Proceed to **Step 5**.

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



Name * cdg-cloud-flavor

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

ID auto

VCPUs * 8

RAM (MB) * 32768

Root Disk (GB) * 50

Ephemeral Disk (GB) 24

Swap Disk (MB) 0

RX/TX Factor 1

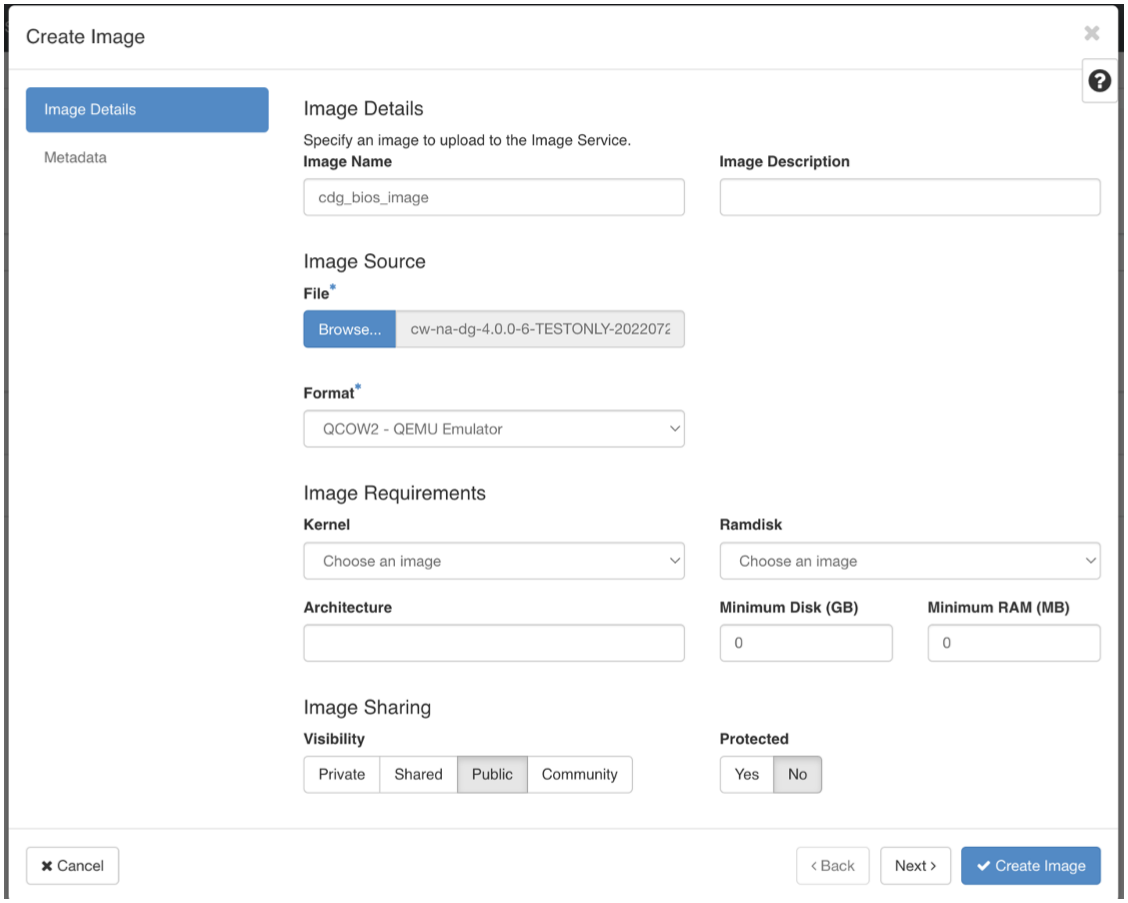
Step 7 **Create an image for OpenStack install.**

a) Enter details in the following fields:

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

b) Click **Create Image**.

Figure 16: Create Image Window



Create Image

Image Details

Specify an image to upload to the Image Service.

Image Name: cdg_bios_image

Image Description:

Image Source

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

Format*: QCOW2 - QEMU Emulator

Image Requirements

Kernel: Choose an image

Ramdisk: Choose an image

Architecture:

Minimum Disk (GB): 0

Minimum RAM (MB): 0

Image Sharing

Visibility: Private Shared [✓ Public] Community

Protected: Yes [✓ No]

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

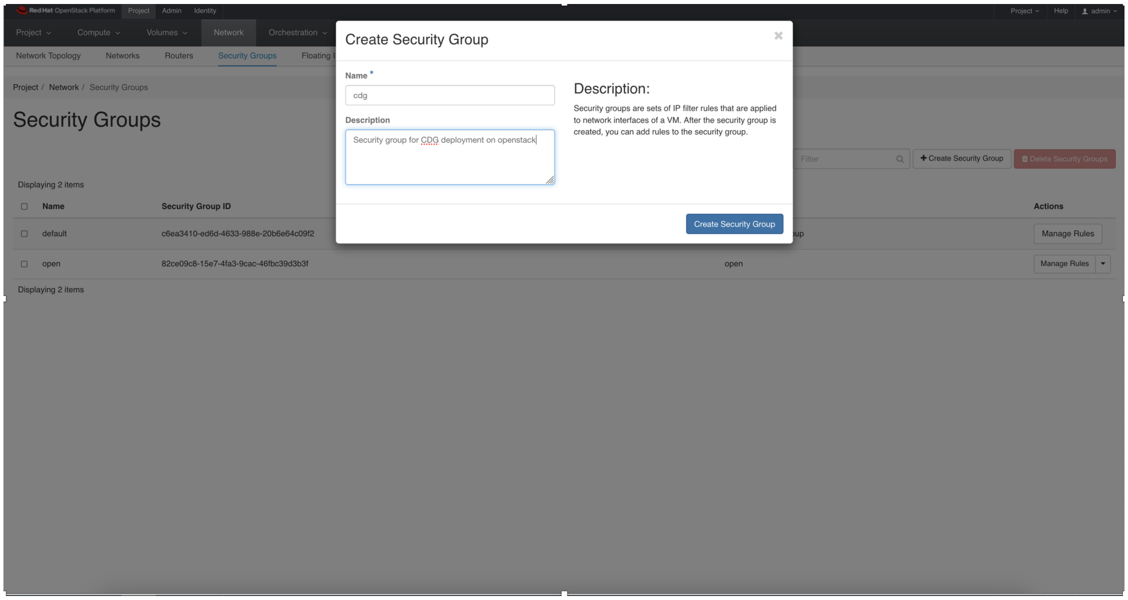
OpenStack does not allow incoming TCP/UDP/ICMP connections by default. Create a security policy to allow incoming connections from TCP/UDP/ICMP protocols.

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

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

b) Click **+ Create Security Group**.

Figure 17: Create Security Group Window



Create Security Group

Name *

cdg

Description

Security group for CDG deployment on openstack

Description:

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

Displaying 2 items

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

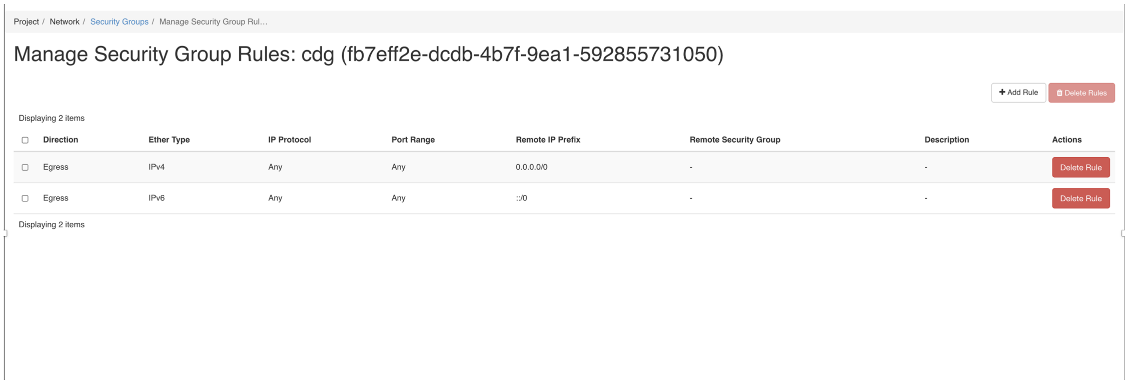
Displaying 2 items

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


Project / Network / Security Groups / Manage Security Group Rul…
+ Add Rule
Delete Rules

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

Displaying 2 items

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

Displaying 2 items

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

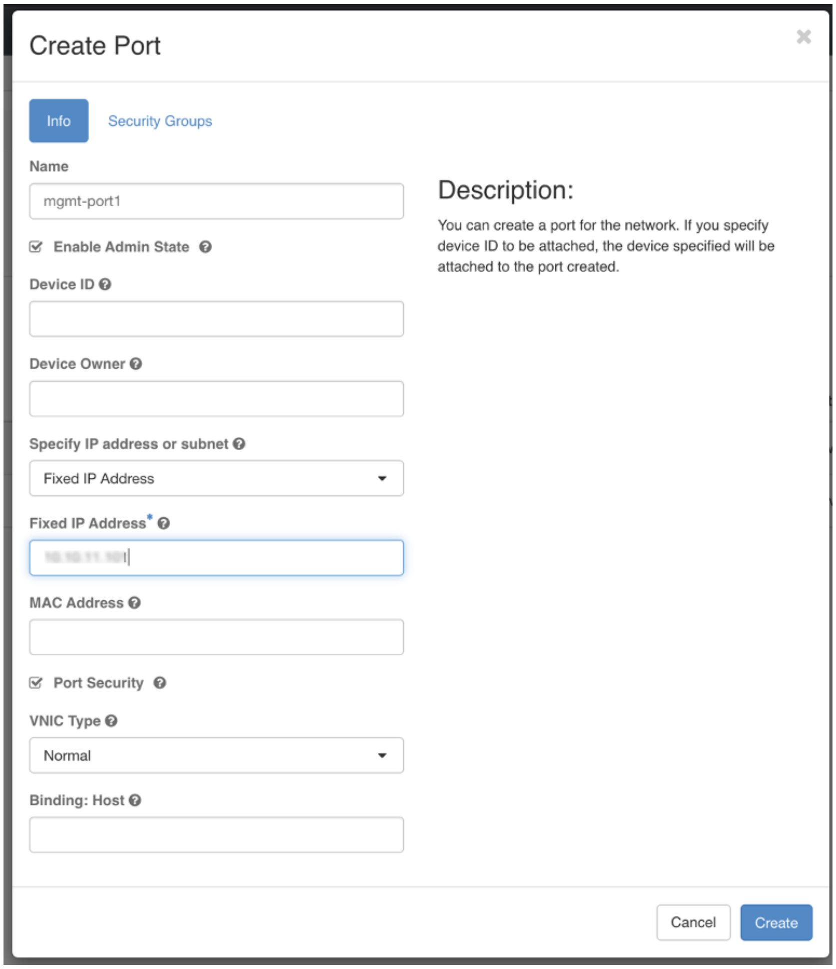
Important This step is required only if you are using Static addressing. If you are using DHCP addressing, the IP addresses for the ports are automatically assigned from the IP addresses allocation pool for the subnet.

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

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

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

Figure 19: Create Port Window



Create Port

Info | Security Groups

Name: mgmt-port1

☑ Enable Admin State

Device ID:

Device Owner:

Specify IP address or subnet: Fixed IP Address

Fixed IP Address*: [redacted]

MAC Address:

☑ Port Security

VNIC Type: Normal

Binding: Host:

Description:

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

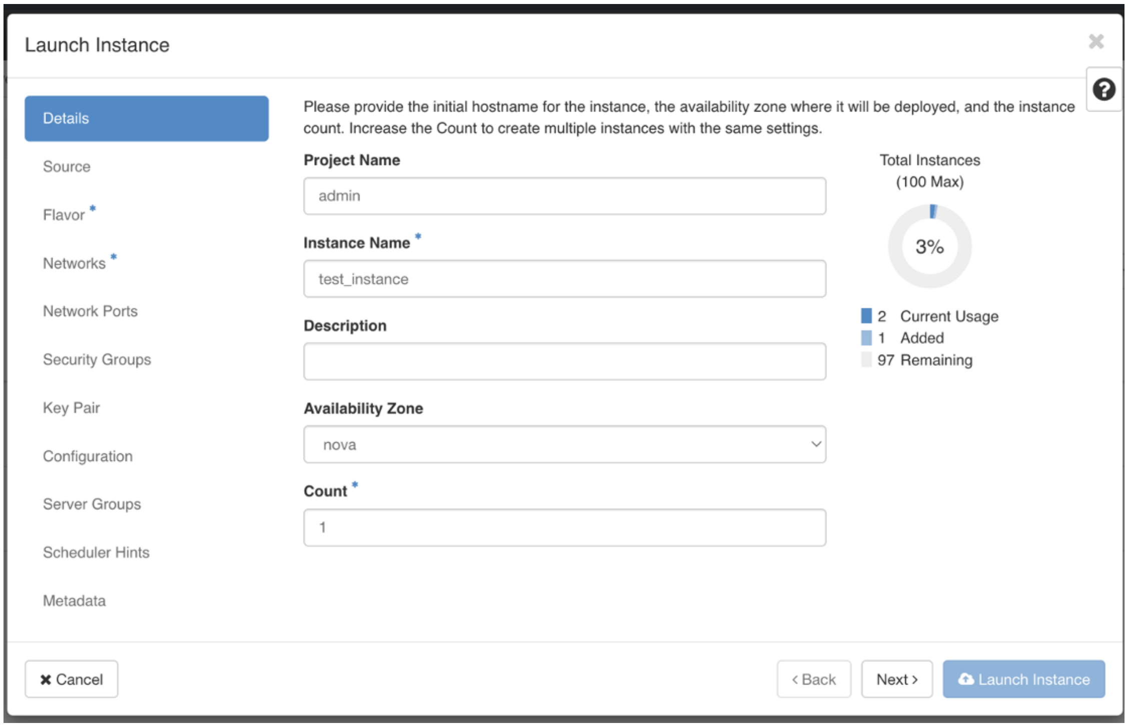
Step 10 Navigate to **Compute** > **Instances**. Click **Launch Instance** in this page.

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

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

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

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

Step 12 In the **Source** tab:

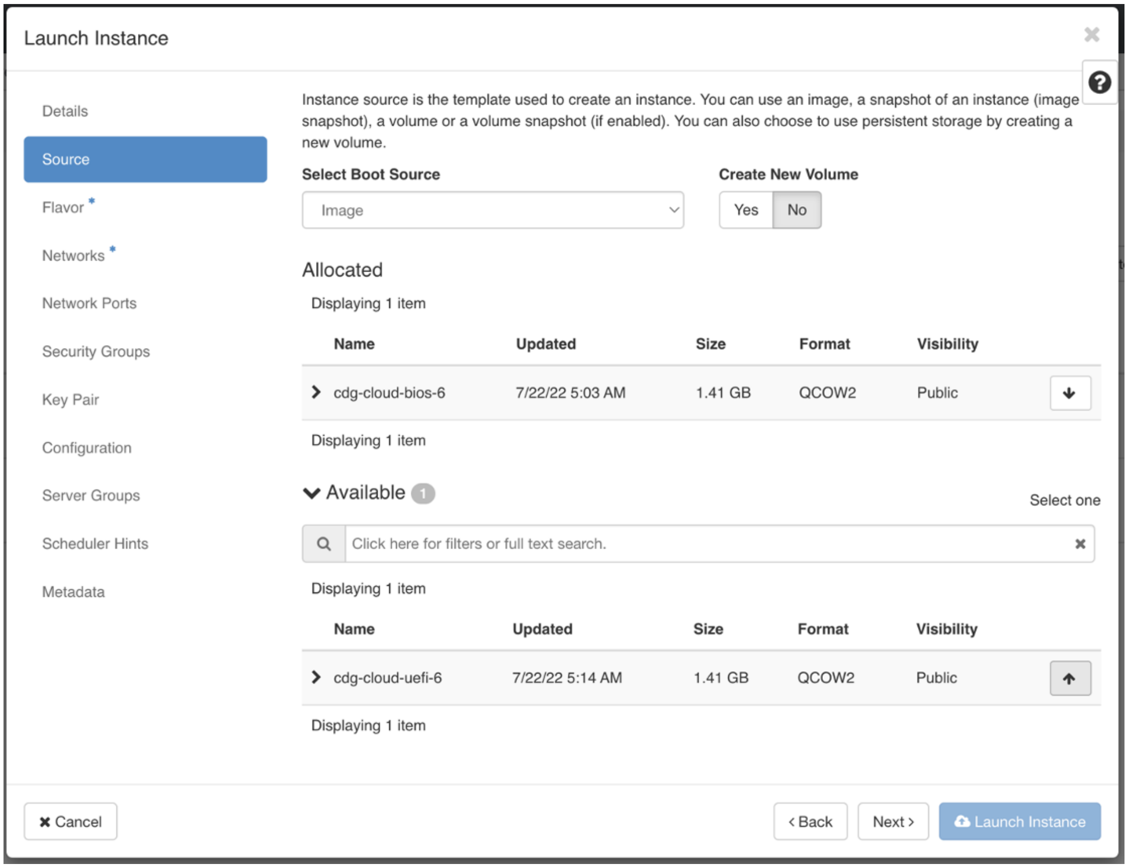
a. **Select Boot Source** - Select **Image** from the drop-down list.

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



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

Select Boot Source: Image

Create New Volume: Yes [✓ No]

Allocated

Displaying 1 item

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

Displaying 1 item

Available 1 — Select one

Click here for filters or full text search.

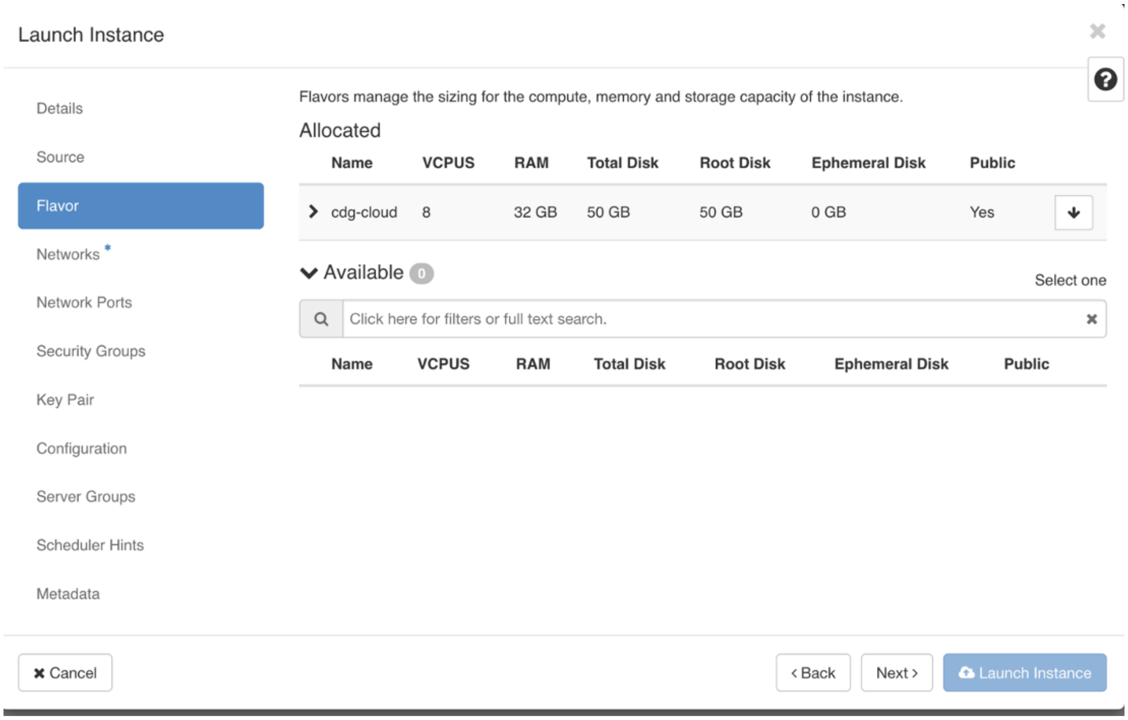
Displaying 1 item

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

Displaying 1 item

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

Figure 22: Launch Instance Window - Flavor Tab



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

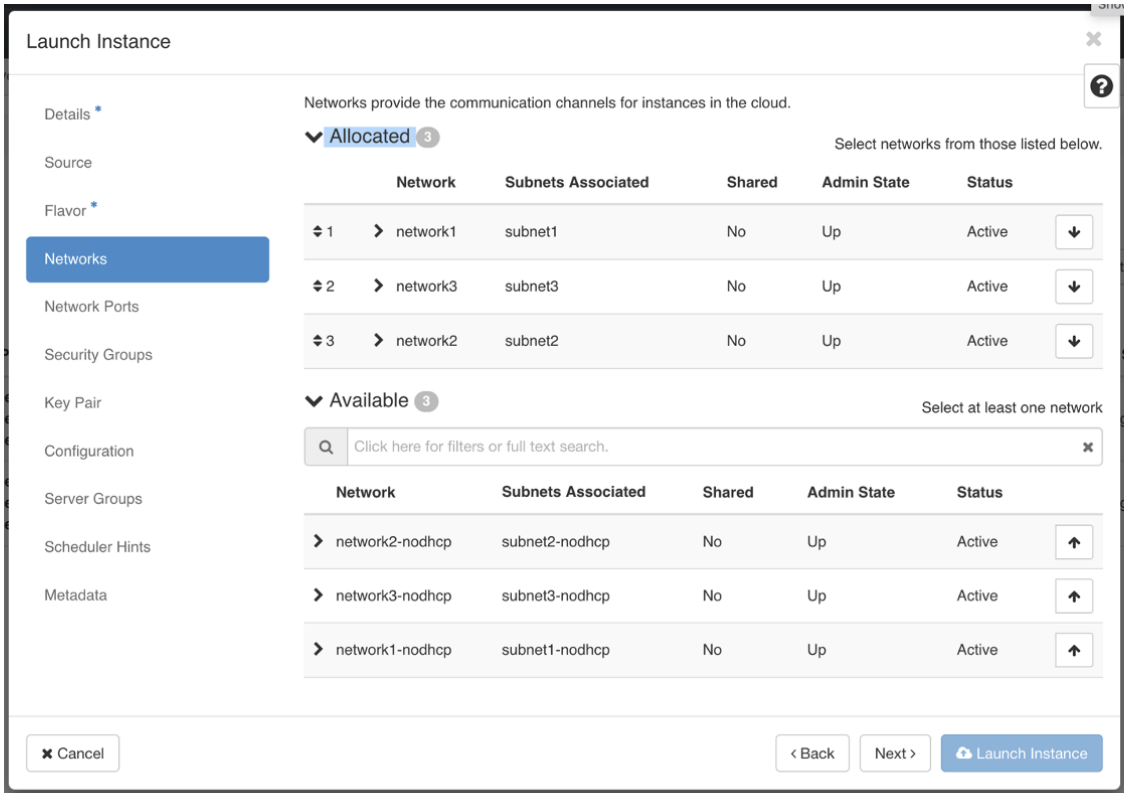
Click here for filters or full text search.

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public

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



Networks provide the communication channels for instances in the cloud.

Allocated 3

Select networks from those listed below.

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

Available 3

Select at least one network

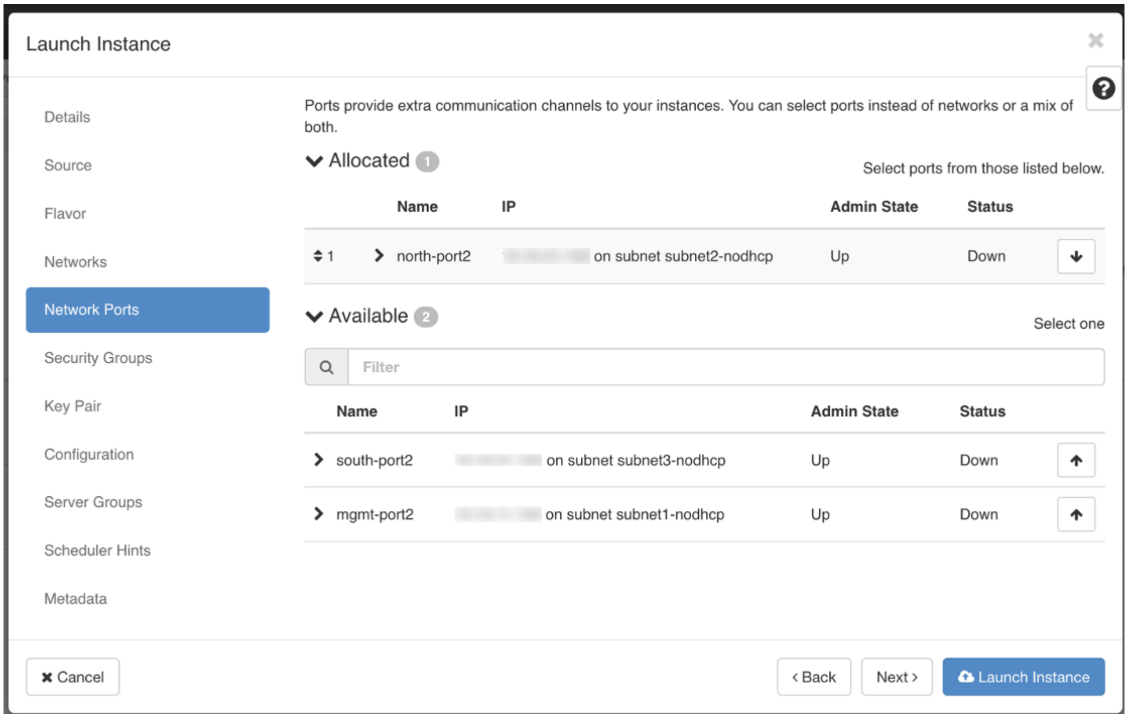
Click here for filters or full text search.

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

Step 15 Assign ports to the VM.

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

Figure 24: Launch Instance Window - Network Ports Tab



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

Allocated 1

Select ports from those listed below.

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

Available 2

Select one

Filter

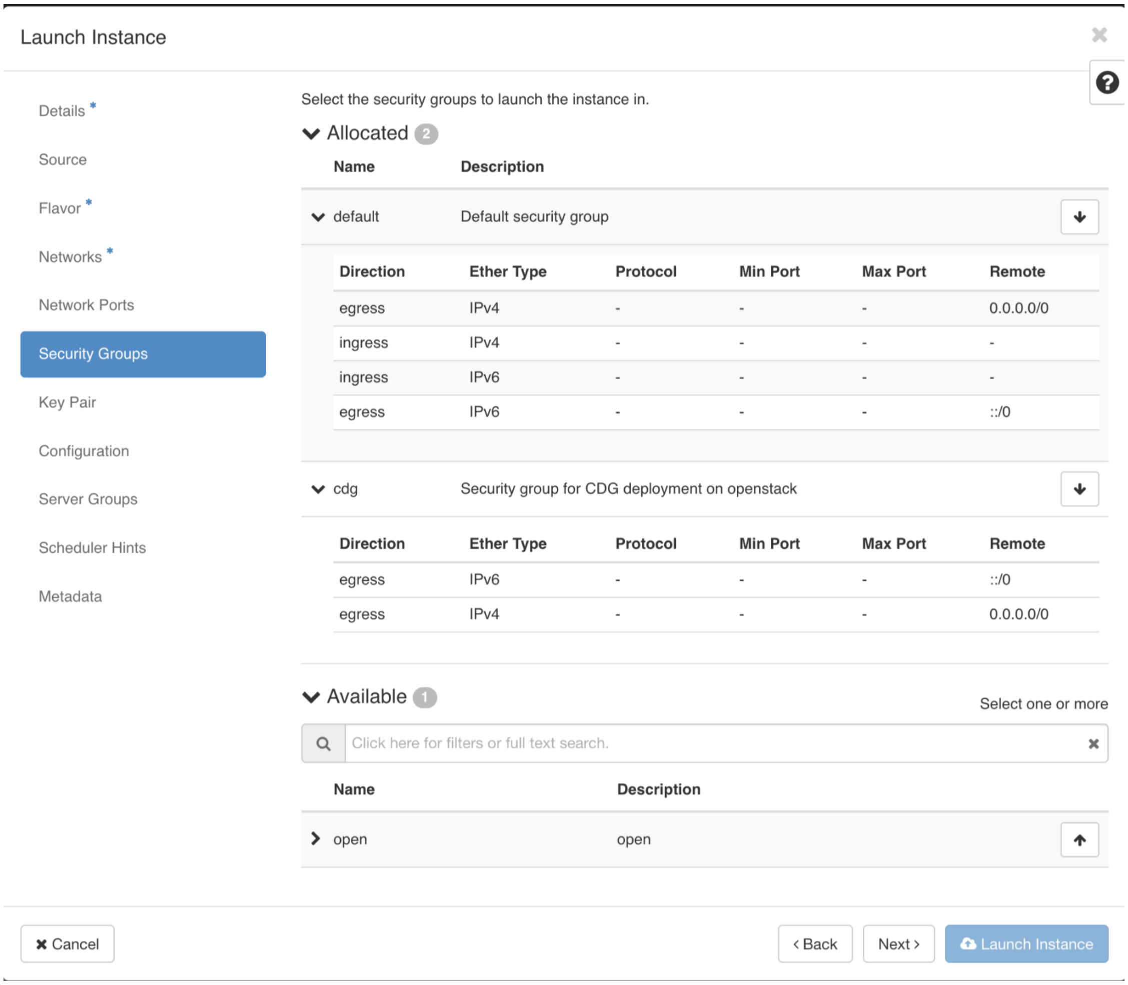
Name	IP	Admin State	Status	
south-port2	[redacted] on subnet subnet3-nodhcp	Up	Down	↑
mgmt-port2	[redacted] on subnet subnet1-nodhcp	Up	Down	↑

Click **Next**.

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

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

Figure 25: Launch Instance Window - Security Groups Tab



Select the security groups to launch the instance in.

Allocated 2

Name	Description
default	Default security group

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

Name	Description
cdg	Security group for CDG deployment on openstack

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

Available 1

Select one or more

Click here for filters or full text search.

Name	Description
open	open

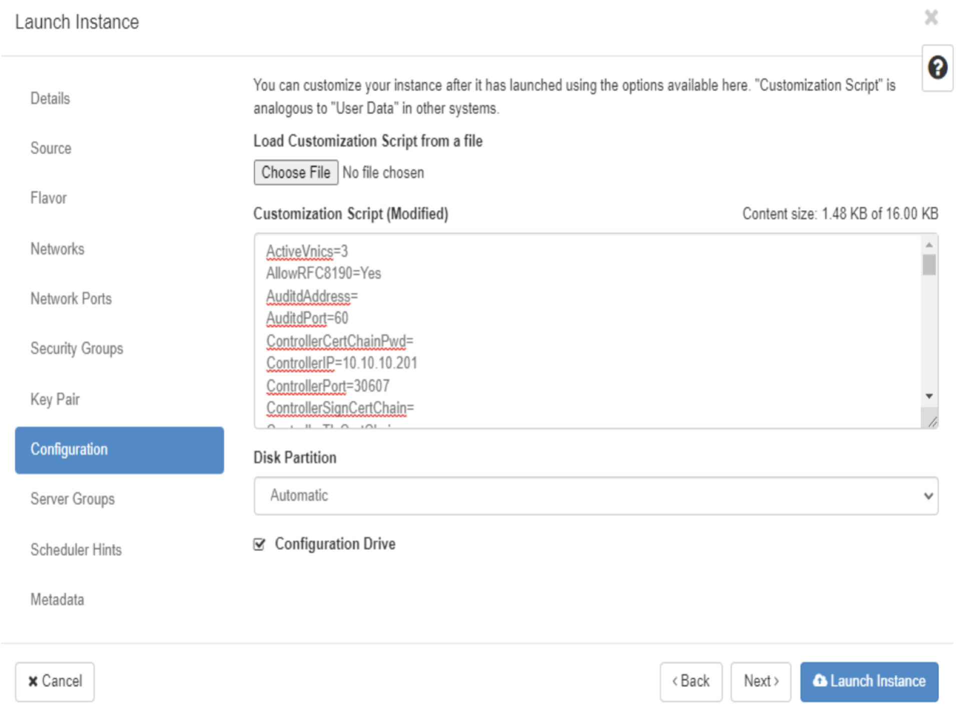
Click **Next**.

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

Step 18 In the **Configuration** tab:

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

Figure 26: Launch Instance Window - Configuration Tab



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

Load Customization Script from a file

Choose File No file chosen

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

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

Disk Partition: Automatic

☑ Configuration Drive

Step 19 Click **Launch Instance**.

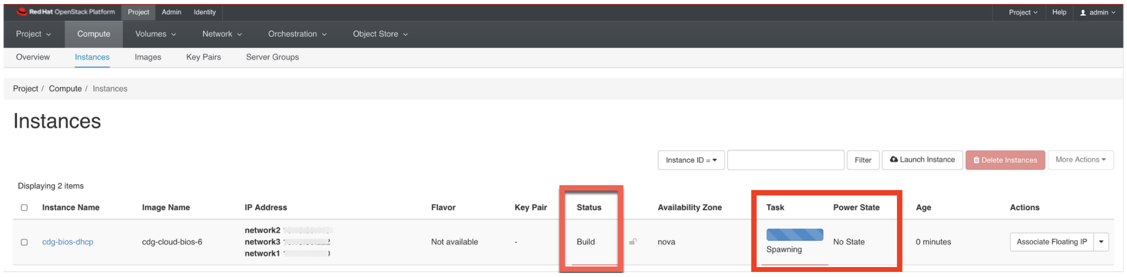
OpenStack begins installation of the VM.

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

Verify that the Crosswork Data Gateway VMs were installed successfully.

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

   Figure 27: Instances Window - Status of CDG VM Installation

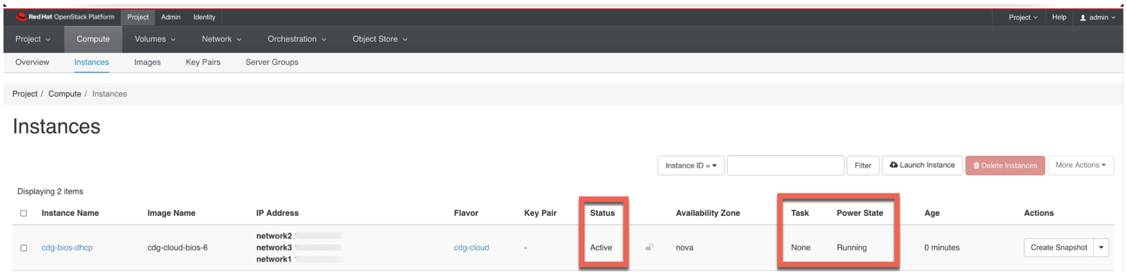
   Displaying 2 items

□	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 [redacted] network3 [redacted] network1 [redacted]	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



Displaying 2 items

□	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 [redacted] network3 [redacted] network1 [redacted]	cdg-cloud	-	Active		nova	None	Running	0 minutes	Create Snapshot ▾

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

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

5. Log in as the dg-admin or dg-oper user (as per the role assigned to you) and the corresponding password you had entered in the `config.txt` file of the VM. The Interactive console of the Crosswork Data Gateway is displayed after you 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 99.

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 78
- Install Crosswork Data Gateway on Amazon EC2 Manually, on page 85

Install Crosswork Data Gateway using CloudFormation (CF) Template

- Extract CF Template Image, on page 78
- Roles and Policy Permissions , on page 79
- CF Template Parameters for Installing Crosswork Data Gateway, on page 80
- Manage CF Template Deployment, on page 83

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 8: 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 9: 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. Default value is `m5.2xlarge`. This is a mandatory parameter.
CNCControllerIP	Host address of the Crosswork Data Gateway controller. 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. The options are: • `1`: to deploy all the interfaces. • `2`: to deploy the Management and Data interfaces. • `3`: to deploy the Management, Data, and Control interfaces.
`CDGInterface0IPAddress`	A free IP address on the subnet. If set to 0.0.0.0, the IP address is automatically allocated. 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. 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. This is a mandatory parameter.
`CDGInterface1SubnetId`	The seconnd interface subnet for the Crosswork Data Gateway. The subnet must be in the same availability zone as the `CDGInterface0SubnetId`.
`CDGInterface1Gateway`	The second interface default gateway on the selected subnet. Typically, the first address on the subnet. 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. 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. 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 `CDGInterface0SubnetId`.

Parameter	Description
`CDGInterface2Gateway`	The third interface default gateway on the selected subnet. Typically, the first address on the subnet. This is a mandatory parameter.
`CDGInterface2SubnetNetmask`	The thrid 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. This is a mandatory parameter.
`CNCControllerIP`	Host address of the Crosswork Crosswork Data Gateway controller.
`HANetworkMode`	The Crosswork Data Gateway HA mode. The pool mode options are: • `L2`: Use this option when you specify IP addresses for creating the HA pool. • `L3`: Use this option when you specify FQDN for creating the HA pool and for multisubnet deployment.
`DataDiskSize`	Size of the Crosswork data disk. The minimum size is 20. Default size is 50. This is a mandatory parameter.
`CDGProfile`	The deployment profile of Crosswork Data Gateway. • `Standard` • `Extended` 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. Configure the number of permitted number of autoenrollment requests and the expiry date of the token. The default values are: • Number of uses: 5 • Expiry: 30 days The maximum accepted values: • Number of uses: 50 • Expiry: 366 days

Table 10: Crosswork Data Gateway and Network Load Balancer (NLB) Stack Parameters

Parameter	Description
`VpcId`	The VPC ID of the worker instances. This is a mandatory parameter.
`SubnetId1`	The management ID of subnet 1. This is a mandatory parameter.
`SubnetId2`	The management ID of subnet 2. This is a mandatory parameter.
`DomainName`	The domain name. This is a mandatory parameter.
`HostedZoneId`	The hosted zone ID. This is a mandatory parameter.
`CdgPoolHostname`	Name of the Route53 record. 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. This is a mandatory parameter.
`LBIPaddress2`	The second LB IP address on subnet. 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 83
- Monitor the Installation, on page 84

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, on page 8 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:

a. Under **Prerequisite - Prepare template**, select **Template is ready**.

b. 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 84 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, on page 8.
- 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.**

a) Prepare the user data for Crosswork Data Gateway VMs. See Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 12 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, on page 110.

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 12.

Table 11: Cisco Crosswork Data Gateway Mandatory Deployment Parameters

Name	Parameter	Default Value
AllowRFC8190	`AllowRFC8190`	The default value is `Yes`.
Auditd Server Port	`AuditdPort`	The default port is `60`.
Deployment	`Deployment`	The default value is `Crosswork Cloud`.
Crosswork Controller Port	`ControllerPort`	The default port is `443`.
Description	Description	The default value is `CDG auto configure`.
dg-admin Passphrase	`dg-adminPassword`	The default password is `changeme`. Reset the default value with the password that you have chosen for the dg-admin user. Password must be 8-64 characters.
dg-oper Passphrase	`dg-operPassword`	The default password is `changeme`. Reset the default value with the password you have chosen for the dg-oper user. 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
		`208.67.222.222`
		`208.67.220.220`

DNS Security Extensions	`DNSSEC`	The default value of this parameter is `False`.
DNS over TLS	`DNSTLS`	The default value of this parameter is `False`.

Name	Parameter	Default Value
DNS Search Domain	`Domain`	The default value of this parameter is `localdomain`.
Crosswork Data Gateway HA mode	`HANetworkMode`	The default value of this parameter is `L2`.
Hostname	`Hostname`	The default value of this parameter is `dg-<eth0 address>`. Where `<eth0-address>` is the address of vNIC0.
Link-Local Multicast Name Resolution	`LLMNR`	The default value of this parameter is `False`.
Multicast DNS	`mDNS`	The default value of this parameter is `False`.
NicAdministration	`NicAdministration`	The default value of this parameter is `eth0`.
NicControl	`NicControl`	The default value of this parameter is `eth1`.
NicDefaultGateway	`NicDefaultGateway`	The default value of this parameter is `eth0`.
NicExternalLogging	`NicExternalLogging`	The default value of this parameter is `eth0`.
NicManagement	`NicManagement`	The default value of this parameter is `eth0`.
NicNBExternalData	`NicNBExternalData`	The default value of this parameter is `eth1`.
NicNBSystemData	`NicNBSystemData`	The default value of this parameter is `eth1`.
NicSBData	`NicSBData`	The default value of this parameter is the last active interface such as eth0 if 1-NIC deployment, eth1 if 2-NIC.

NTPv4 Servers	`NTP`	The default values of this parameter are
		`162.159.200.1`
		`65.100.46.164`
		`40.76.132.147`
		`104.131.139.195`

Use NTPv4 Authentication	`NTPAuth`	The default value of this parameter is `False`.
Profile	`Profile`	The default value of this parameter is `Crosswork-Cloud`.
Syslog Multiserver Mode	`SyslogMultiserverMode`	The default value of this parameter is `Simultaneous`.
Syslog Server Port	`SyslogPort`	The default value of this parameter is `514`.
Syslog Server Protocol	`SyslogProtocol`	The default value of this parameter is `UDP`.
Use Syslog over TLS	`SyslogTLS`	The default value of this parameter is `False`.

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

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 92 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 97 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 92
- Add Enrollment Token to Configuration File, on page 96

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.

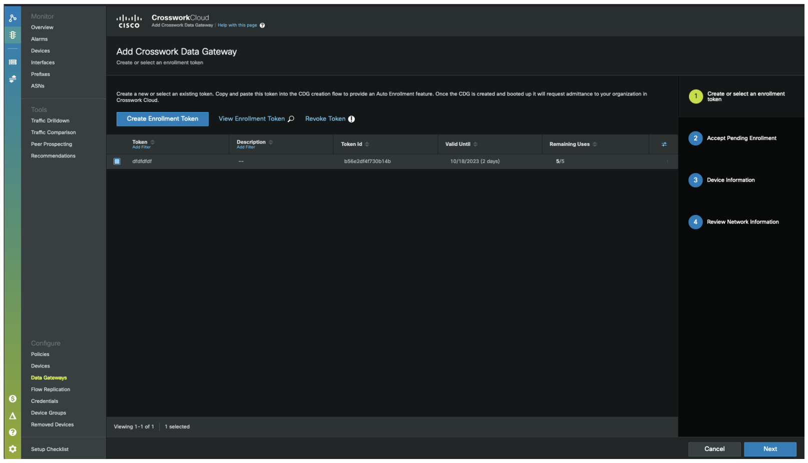
Step 3 Click **Add Crosswork Data Gateway**

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:**

  a. In the **Add Crosswork Data Gateway** page, click **Create Enrollment Token**.

  Figure 29: Crosswork Cloud UI



Add Crosswork Data Gateway

Create or select an enrollment token

Create a new or select an existing token. Copy and paste this token into the CDG creation flow to provide an Auto Enrollment feature. Once the CDG is created and booted up it will request admittance to your organization in Crosswork Cloud.

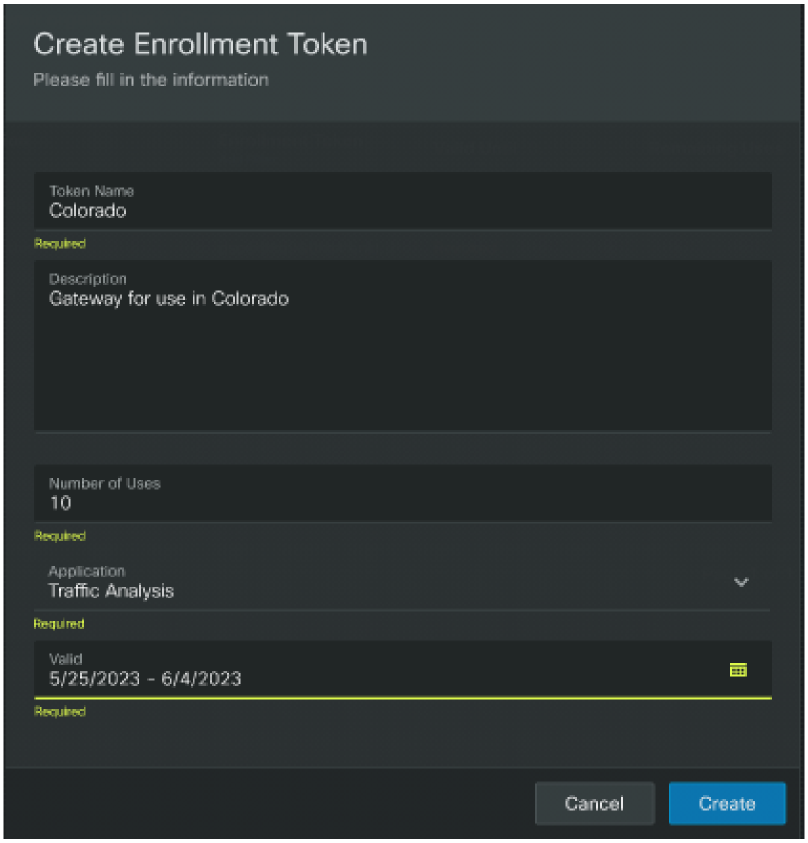
	Token	Description	Token Id	Valid Until	Remaining Uses
☐	dfdfdfdf	--	b56e2df4f730b14b	10/18/2023 (2 days)	5/5

  b. In the **Create Enrollment Token** window, enter the following:

  1. **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

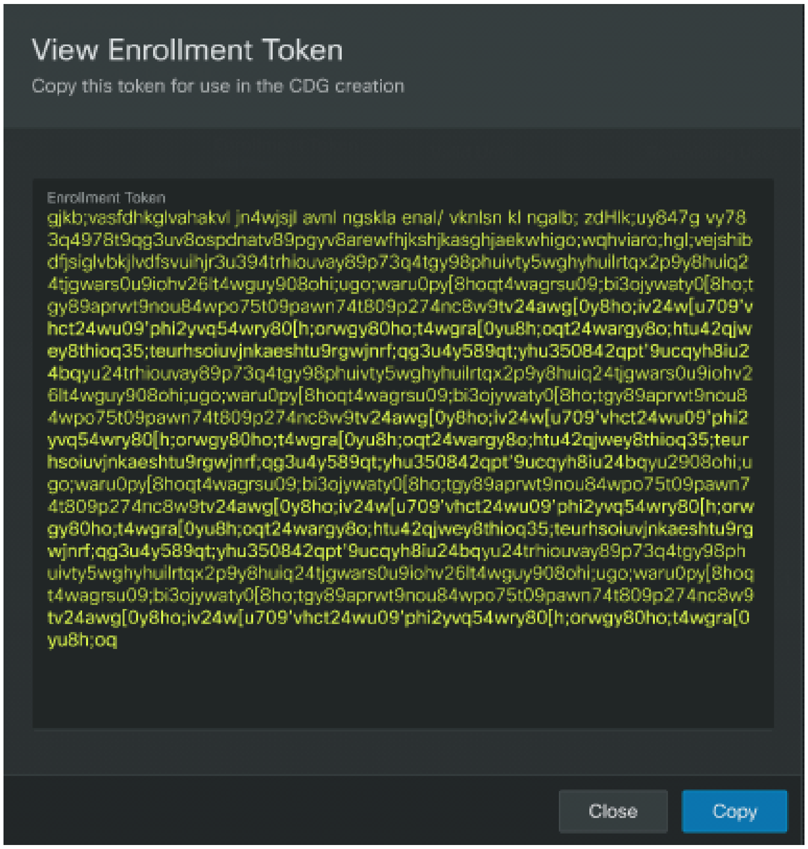
Valid: 5/25/2023 - 6/4/2023

Required

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



View Enrollment Token

Copy this token for use in the CDG creation

Enrollment Token

```
gjkb;vasfdhkglvahakvl jn4wjsjl avnl ngskla enal/ vknlsn kl ngalb; zdHlk;uy847g vy78
3q4978t9qg3uv8ospdnatv89pgyv8arewfhjkshjkasghjaekwhigo;wqhviaro;hgl;vejshib
dfjsiglvbkjlvdfsvuihjr3u394trhiouvay89p73q4tgy98phuivty5wghyhuilrtqx2p9y8huiq2
4tjgwars0u9iohv26lt4wguy908ohi;ugo;waru0py[8hoqt4wagrsu09;bi3ojywaty0[8ho;t
gy89aprwt9nou84wpo75t09pawn74t809p274nc8w9tv24awg[0y8ho;iv24w[u709'v
hct24wu09'phi2yvq54wry80[h;orwgy80ho;t4wgra[0yu8h;oqt24wargy8o;htu42qjw
ey8thioq35;teurhsoiuvjnkaeshtu9rgwjnrf;qg3u4y589qt;yhu350842qpt'9ucqyh8iu2
4bqyu24trhiouvay89p73q4tgy98phuivty5wghyhuilrtqx2p9y8huiq24tjgwars0u9iohv2
6lt4wguy908ohi;ugo;waru0py[8hoqt4wagrsu09;bi3ojywaty0[8ho;tgy89aprwt9nou8
4wpo75t09pawn74t809p274nc8w9tv24awg[0y8ho;iv24w[u709'vhct24wu09'phi2
yvq54wry80[h;orwgy80ho;t4wgra[0yu8h;oqt24wargy8o;htu42qjwey8thioq35;teur
hsoiuvjnkaeshtu9rgwjnrf;qg3u4y589qt;yhu350842qpt'9ucqyh8iu24bqyu2908ohi;u
go;waru0py[8hoqt4wagrsu09;bi3ojywaty0[8ho;tgy89aprwt9nou84wpo75t09pawn7
4t809p274nc8w9tv24awg[0y8ho;iv24w[u709'vhct24wu09'phi2yvq54wry80[h;orw
gy80ho;t4wgra[0yu8h;oqt24wargy8o;htu42qjwey8thioq35;teurhsoiuvjnkaeshtu9rg
wjnrf;qg3u4y589qt;yhu350842qpt'9ucqyh8iu24bqyu24trhiouvay89p73q4tgy98ph
uivty5wghyhuilrtqx2p9y8huiq24tjgwars0u9iohv26lt4wguy908ohi;ugo;waru0py[8hoq
t4wagrsu09;bi3ojywaty0[8ho;tgy89aprwt9nou84wpo75t09pawn74t809p274nc8w9
tv24awg[0y8ho;iv24w[u709'vhct24wu09'phi2yvq54wry80[h;orwgy80ho;t4wgra[0
yu8h;oq
```

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

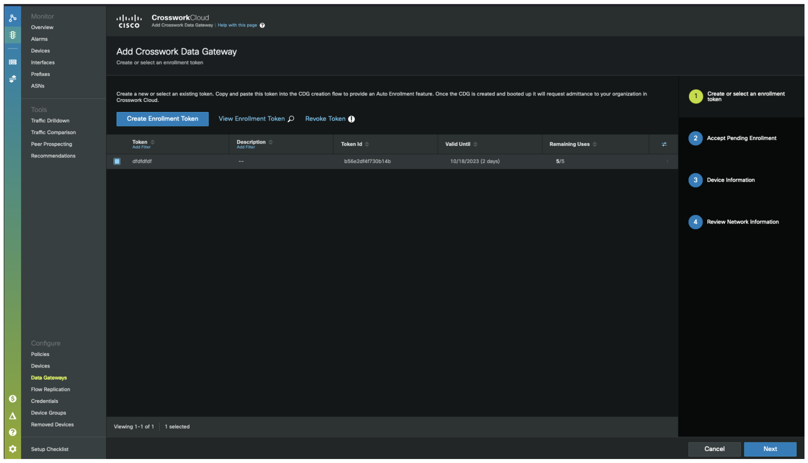
- **Use an existing token**

  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



Add Crosswork Data Gateway

Create or select an enrollment token

Create a new or select an existing token. Copy and paste this token into the CDG creation flow to provide an Auto Enrollment feature. Once the CDG is created and booted up it will request admittance to your organization in Crosswork Cloud.

	Token Add Filter	Description Add Filter	Token Id	Valid Until	Remaining Uses
☑	dfdfdfdf	--	b56e2df4f730b14b	10/18/2023 (2 days)	5/5

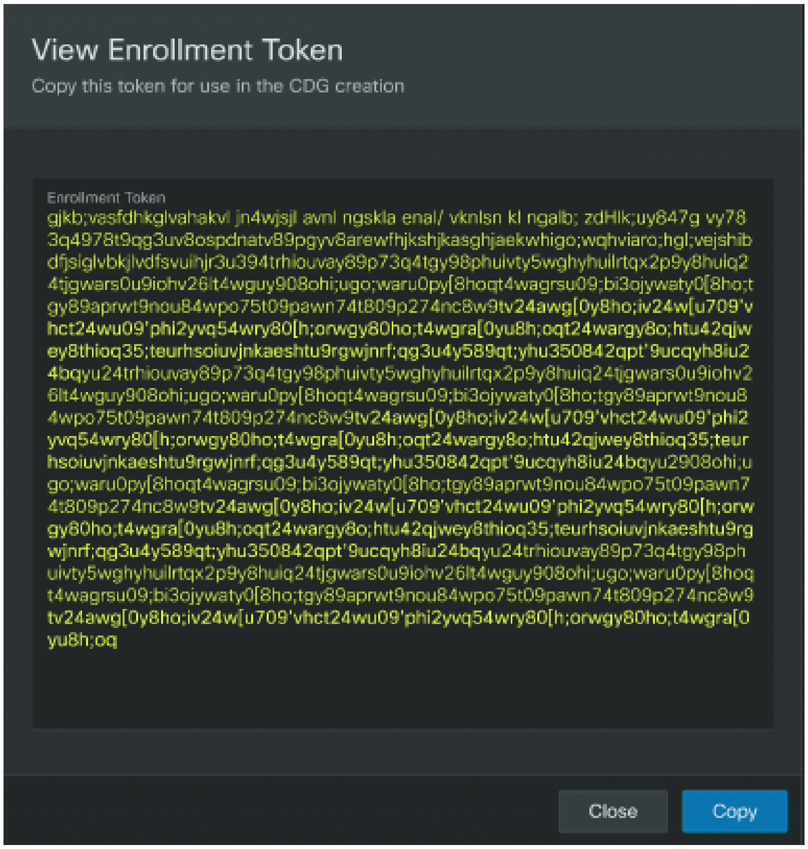
Viewing 1-1 of 1 | 1 selected

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



View Enrollment Token

Copy this token for use in the CDG creation

Enrollment Token

```
gjkb;vasfdhkglvahakvl jn4wjsjl avnl ngskla enal/ vknlsn kl ngalb; zdHlk;uy847g vy78
3q4978t9qg3uv8ospdnatv89pgyv8arewfhjkshjkasghjaekwhigo;wqhviaro;hgl;vejshib
dfjsiglvbkjlvdfsvulhjr3u394trhiouvay89p73q4tgy98phuivty5wghyhuilrtqx2p9y8huiq2
4tjgwars0u9iohv26lt4wguy908ohi;ugo;waru0py[8hoqt4wagrsu09;bi3ojywaty0[8ho;t
gy89aprwt9nou84wpo75t09pawn74t809p274nc8w9tv24awg[0y8ho;iv24w[u709'v
hct24wu09'phi2yvq54wry80[h;orwgy80ho;t4wgra[0yu8h;oqt24wargy8o;htu42qjw
ey8thioq35;teurhsoiuvjnkaeshtu9rgwjnrf;qg3u4y589qt;yhu350842qpt'9ucqyh8iu2
4bqyu24trhiouvay89p73q4tgy98phuivty5wghyhuilrtqx2p9y8huiq24tjgwars0u9iohv2
6lt4wguy908ohi;ugo;waru0py[8hoqt4wagrsu09;bi3ojywaty0[8ho;tgy89aprwt9nou8
4wpo75t09pawn74t809p274nc8w9tv24awg[0y8ho;iv24w[u709'vhct24wu09'phi2
yvq54wry80[h;orwgy80ho;t4wgra[0yu8h;oqt24wargy8o;htu42qjwey8thioq35;teur
hsoiuvjnkaeshtu9rgwjnrf;qg3u4y589qt;yhu350842qpt'9ucqyh8iu24bqyu2908ohi;u
go;waru0py[8hoqt4wagrsu09;bi3ojywaty0[8ho;tgy89aprwt9nou84wpo75t09pawn7
4t809p274nc8w9tv24awg[0y8ho;iv24w[u709'vhct24wu09'phi2yvq54wry80[h;orw
gy80ho;t4wgra[0yu8h;oqt24wargy8o;htu42qjwey8thioq35;teurhsoiuvjnkaeshtu9rg
wjnrf;qg3u4y589qt;yhu350842qpt'9ucqyh8iu24bqyu24trhiouvay89p73q4tgy98ph
uivty5wghyhuilrtqx2p9y8huiq24tjgwars0u9iohv26lt4wguy908ohi;ugo;waru0py[8hoq
t4wagrsu09;bi3ojywaty0[8ho;tgy89aprwt9nou84wpo75t09pawn74t809p274nc8w9
tv24awg[0y8ho;iv24w[u709'vhct24wu09'phi2yvq54wry80[h;orwgy80ho;t4wgra[0
yu8h;oq
```

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 96 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 92 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 102.

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 99).
- By using the **Display base64 Encoded Enrollment Package** option from the Interactive Console (see Create an Encoded Enrollment Package, on page 100)

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 98.

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,
    "memory": 31,
    "nics": 1,
    "base_vm": "true"
  },
  "interfaces": [
    {
      "name": "eth0",
      "mac": "xx:xx:xx:xx:xx:xx",
      "ipv4Address": "x.x.x.x/24",
      "roles":
"ADMINISTRATION,CONTROL,DEFAULT_GATEWAY,EXTERNAL_LOGGING,MANAGEMENT,NB_EXTERNAL_DATA,NB_SYSTEM_DATA,SB_DATA"

    }
  ],
  "certChain": [

"MIIJcjCCBVqgAwIBAgIUVBf8hVppCcDBA+yZG6tzIEvq/mEwDQYJKoZIhvcNAQENBQAwLDELMAkGA1UECgwCRExHTAbBgNVBAMMFG1hbmFzLWNkZzQ1MC
10ZXN0MDExMB4XDTIzMDIwMTE3MTQ0OVoXDTQzMDIwMjE3MTQ0OVowLDELMAkGA1UECgwCRExHTAbBgNVBAMMFG1hbmFzLWNkZzQ1MC10ZXN0MDExMIIEIjANB
gkqhkiG9w0BAQEFAAOCBA8AMIIECgKCBAEAuvgTWyIDi6FOlecovhbUoGagARPQ32QBkz3s07QgpkatyJalHUYTeseGi0rAPKfzDXoeTZioK5JphDKLRnSze6XJBM
kNpaNyhRTEXWcR/Dds5lRzMQ9qwY3NpWuYlJLKgmbxypabttakLGs0FjXNuqBm4RL3XrhMMboRDkwf7YF5WSMQnszfTGRfDtEVMPMC3xeIul9FLkULSl8FaPgt2cJN
ylK9Z0l9KeRxpQHP0M5G+d3Nt0ytEFkCdTyjKlwhJRmdpXUcoqaXJLHygl29XbuKMJA58ByurbWhR/0th7VAzFFSM5/mncVrvoG0NH8pxpXl6ZMPKDyLeHRkyX6EOBb
kwPD3ysEmT/Hw+XsVbOpt8alLQeaQK8MaOsbManZ0ksR8DZk/g8QUXwFWoRsNnq8+GfpvBdzVkoyT1irp43QFrsXxdpTX8pATlwNxoZOkD21jDK7sYTQoNHxK1A1KRu
YTMHDQZt30C5oHRvZfA9V95MWxt+oRaUhdq7JXG8UYyDc/FhVmoqlbEE8ossdBiGwncz/xQ4jaEmAu3UAWFWRISFZuSLdoPD/PsgfblPpYFhnuq/5Um49HB2PYXZuI
yJaKbhX6FAzD49dE6Zm5VuaZPrfPm8v4mu/2l+PPhTfY17nYyXRwBMCX7ZwXtfyZ+bH3xSgi7rG3Vqkte4XqNL/lVkHod2SXKWQ4M/l/cV0FDNX9ifVwPtlmUQgRlen
KvzXWSxCqXCK3o1qjz1TELPUPvvkKoZk3x6AqD5IZoriWX5CGHv1ikqHQCD1V9DatnbmIHPVtVQyM30TycVw8uOHJLDqU130LqDCl26kORCT26muJRi35DN4NpIszh2
oBAaYH6hy7rZaIMIC/Uw6BZ4AJ4k4Bpobv1yrDxf0xeg5Nvf47/GP+LLsn9JeaRhUOdFF8xcNINHjXvH8IfJ72H1IlH1srRB73+V4w3rCC92lsDK8sxN8YAssQm+IRa
Ze6Pw4lvddlfu1VYs7PqYwI9LSbeCePzPbKZ4zgl7/A2Ijh8XsV52HZ7shOPgUyaNbjvBi/+/0pI3wILFTbawVAmlEOTOekYm+N1pWWcwH9sB6SEXjG7mLl1jGWFHqV
nduZtjABjWhPE2ZHluZW1A2aLU25Lhd4do+DeDwtsMiMOgvIkSm5c5YS2xjDvZmJF2pf85AY0brVUjRep0z46p3D+zFtuW9DPYn65M+Bypf+OZIms7TfhUXxZlwKCLEM
xvcUc0gc6eOeMhF21DC26cLBbE2eY5Y99mu8RtQPOLeCC9tcaYifhOB2f9pEGFOuX3DnSc0oXFzhBo9IZhCNUyPjvp1H/bERuFAiENGo0QPy3+vf+IMQK3JKX0BLpMF2Hc
0KhwIDAQABo4GLMIGIMB0GA1UdDgQWBBRBbcosvgUjVkqagHBuZ2UHslsiTzAfBgNVHSMEGDAWgBRBbcosvgUjVkqagHBuZ2UHslsiTzAPBgNVHRMBAf8EBTADAQH/MDUG
A1UdEQQuMCyCFG1hbmFzLWNkZzQ1MC10ZXN0MDExghRtYW5hcy1jZGc0NTAtdGVzdDAxMTANBgkqhkiG9w0BAQ0FAAOCBAEAoLczUuKA4Z8RC5QMVTyx9xeFMslPx7XEF2z
DOhesdTs1SVUDoolp1KaQa5hyYtyD5fwzipSgY4H1ylTkyrB+LMbVrGAE6K5A1//rMaft7KWbhJqx57O6FY0JghefGpVyAZ/gW/HI9uxPbDaWHG/SNXPH3zRb/mEIX2vksG
1rpYFlUDap2rDoGNahMC7ueNeDcPYMJ9F5hTQeI/goqg31BE6uUI6mY9gfdMZ94EFcs/R1kI1XR/YwzoCibRWtiJqiZRIuZHX3rYa2vYX8QWIV9BXcVx561r342dTy5/1w9F
ZZHL0SQiWjXozOHFEHBwdMCLo4SbQRuWj8qFg4+dGGuBZvpZkGiaB7bwgbBx/JzOpEC0Kv5IZ9YGVnDeX7O9idNkAIRZsbE88U+VZu6D1XstrrRlPmbC/cgPbo3iXTHJZkXa9
4734TSBYI1si1uJzAzJXfAYLYR0yoYYoxx7xS4/up0U0amess/HaQcuEl0BiYS+/cEnF5r4QT9rQQTIK43G2Gi40vIX6kFYjmKD9Tk7A++ToEWt+BfNIlYjoNHbR8vyrMCFI
J4AlzLYu5/229Vog62LTdpupXJxC7s8sBzfU6TrdCJx0A2FhiHQFS3E1rZAnBpYPkzAGLQBeArlslwOH5dMAgxyOG2wFgca5Ce8PEJRFeB3M+oi3AOv8nJoseXfaPHyuhemDQ
o9XkBEg4w/PSq5rnM8vfWm6P1ajo2PbDJq8y8zP0yNjyEP8Dc6TL2bvHn4Jmzz/OQZ4m5a003UrmbDK+sQwUmNVfd7MMcqmVFvJmhOXc41Ui3srhwoPf5gK82m8S0/QhsWSoz
wGgKxPGT6NR46rRXBxXcuzYyAxSwrsPntMONYRepOUmTFW4a7Ra9srSM06QcREmX7F1S3h4HetxB/4M/Kmx4XmNRQ+T4HnR9HXJnZ+KXaBkHIy8Lt55JrdlvNmGXcFU/uV9di
F08uwiO+ChhaZC8yfFG855f/dKdHanVBqp5fS47B3IYTC9AxF37q/6Hv1udZDzSkFbWqUWbANCgxOn4poCfePcAXKQ7iDcPr1JYu3XTJBpxzADKBqRa28G3Y1lriD0k7pb7HII
11YCdG10C53OmboLrhmnM6BFHYUGI0sMWWmsiiDrCpblyn63khdBzzzA++9tnJtp0eFBOHo5GoJbSqfY+XnpZ5zr2Nt9mE61e8Cv8G4LFXkpCgkKJr5v/VshrFcFLlPCudU8Cy
PhpqQNBGD0+YHOxhFGDdUCyM3rE7gGAAch4rJD1wkq2WacVSF7fwmMdzGlAsb+IbBiDmaelQ6y17LeiWqA3xeSZLXQ7xyXHjYa3hWbjwbAM17vI/9RvnHZSGYEjyNrEmWZuew=="

  ],
  "version": "6.0.0 (branch dg45x - build number 19)",
  "duuid": "a3bf6411-1ad0-418c-9957-eb199e9395e0",
  "profileType": "VM_PROFILE_STANDARD"
}
```

Obtain the Enrollment Package

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

Step 1 Log in to Cisco Crosswork Data Gateway.

Step 2 From the Main Menu, select **Get Enrollment Package**.

Step 3 Select **Export Enrollment Package** or **Display base64 Encoded Enrollment Package**.

Step 4 Click **OK**.

What to do next

Depending on the option that you have selected, obtain the enrollment package referring to Export Enrollment Package, on page 99 or Create an Encoded Enrollment Package, on page 100

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 101 if you had already specified the **Auto Enrollment Package Transfer** settings during installation.

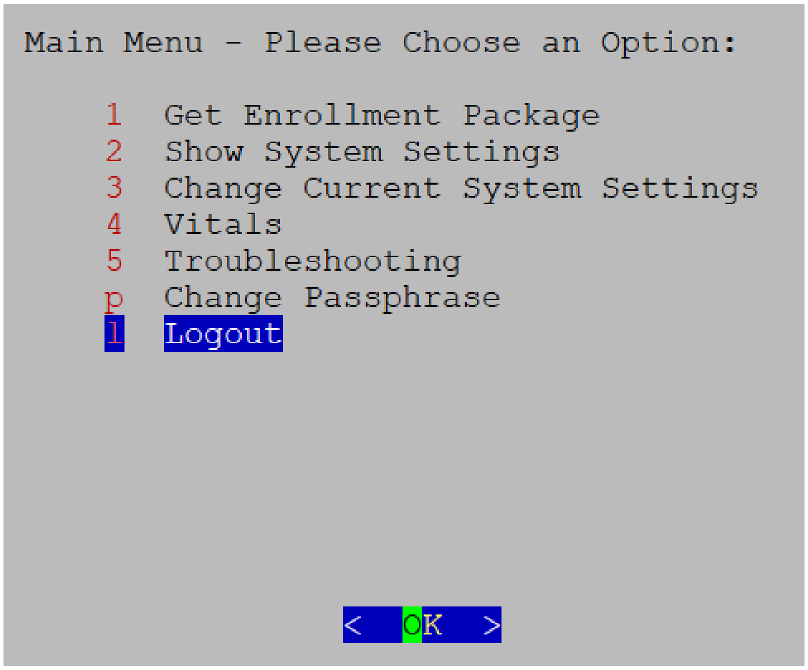
Step 1 Log in to the Cisco Crosswork Data Gateway.

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 101.

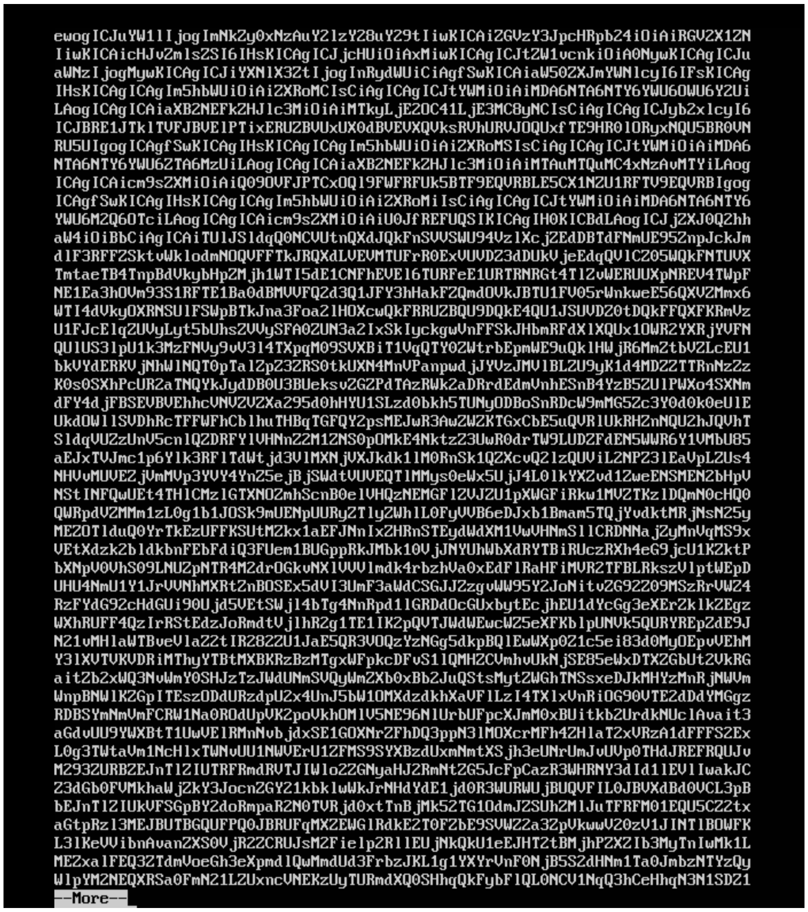
Create an Encoded Enrollment Package

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.

Figure 35: Enrollment Package Content



```
ewogICJuYW1lIjogImNkZy0xNzAuY2lzY28uY29tIiwKICAiZGVzY3JpcHRpb24iOiAiRGV2X1ZN
IiwKICAicHJvZmlsZSI6IHsKICAgICJjcHUiOiAxMiwKICAgICJtZW1vcnkiOiA0NywKICAgICJu
aWNzIjogMywKICAgICJiYXNlX3ZtIjogInRydWUiCiAgfSwKICAiaW50ZXJmYWNlcyI6IFsKICAg
IHsKICAgICAgIm5hbWUiOiAiZXRoMCIsCiAgICAgICJtYWMiOiAiMDA6NTA6NTY6YWU6OWU6Y2Ui
LAogICAgICAiaXB2NEFkZHJlc3MiOiAiMTkyLjE2OC41LjE3MC8yNCIsCiAgICAgICJyb2xlcyI6
ICJBRE1JTklTVFJBVElPTixERUZBVUxUX0dBVEVXQVksRVhURVJOQUxfTE9HR0lORyxNQU5BR0VN
RU5UIgogICAgfSwKICAgIHsKICAgICAgIm5hbWUiOiAiZXRoMSIsCiAgICAgICJtYWMiOiAiMDA6
NTA6NTY6YWU6ZTA6MzUiLAogICAgICAiaXB2NEFkZHJlc3MiOiAiMTAuMTQuMC4xNzAvMTYiLAog
ICAgICAicm9sZXMiOiAiQ09OVFJPTCxOQl9FWFRFUk5BTF9EQVRBLE5CX1NZU1RFTV9EQVRBIgog
ICAgfSwKICAgIHsKICAgICAgIm5hbWUiOiAiZXRoMiIsCiAgICAgICJtYWMiOiAiMDA6NTA6NTY6
YWU6M2Q6OTciLAogICAgICAicm9sZXMiOiAiU0JfREFUQSIKICAgIH0KICBdLAogICJjZXJ0Q2hh
aW4iOiBbCiAgICAiTUlJSldqQ0NCVUtnQXdJQkFnSVVSWU94VzlXcjZEdDBTdFNmUE95ZnpJckJm
dlF3RFFZSktvWklodmNOQVFFTkJRQXdLVEVMTUFrR0ExVUVDZ3dDUkVjeEdqQVlCZ05WQkFNTUVX
TmtaeTB4TnpBdVkybHpZMjh1WTI5dE1CNFhEVE16TURFeE1URTRNRGt4TlZvWERUUXpNREV4TWpF
NE1Ea3hOVm93S1RFTE1Ba0dBMVVFQ2d3Q1JFY3hHakFZQmdOVkJBTU1FV05rWnkweE56QXVZMmx6
WTI4dVkyOXRNSUlFSWpBTkJna3Foa2lHOXcwQkFRRUZBQU9DQkE4QU1JSUVDZ0tDQkFFQXFKRmVz
U1FJcElqZUVyLyt5bUhsZVVySFA0ZUN3a2IxSkIyckgwVnFFSkJHbmRFdXlXQUx1OWR2YXRjYVFN
QUlUS3lpU1k3MzFNVy9vV3l4TXpqM09SVXBiT1VqQTY0ZWtrbEpmWE9uQklHWjR6Mm5tbVZLcEU1
bkVYdERKVjNhWlNQT0pTalZpZ3ZRS0tkUXN4MnVPanpwdjJYVzJMVlBLZU9yK1d4MDZZTTRnNzZz
K0s0SXhPcUR2aTNQYkJydDB0U3BUeksvZGZPdTAzRWk2aDRrdEdmVnhESnB4YzB5ZU1PWXo4SXNm
dFY4djFBSEVBVEhhcVNVZVZXa295d0hHYU1SLzd0bkh5TUNyODBoSnRDcW9mMG5Zc3Y0d0k0eUlE
UkdOWllSVDhRcTFFWFhCblhuTHBqTGFQY2psMEJwR3AwZWZKTGxCbE5uQVRlUkRHZnNQU2hJQVhT
S1dqVUZzUnV5cnlQZDRFYlVHNnZ2M1ZNS0pOMkE4NktzZ3UwR0drTW9LUDZFdEN5WWR6Y1VMbU85
aEJxTVJmc1p6Ylk3RFlTdWtjd3VlMXNjVXJkdk1lM0RnSk1QZXcvQ2lzQUViL2NPZ3lEaVpLZUs4
NHVvMUVEZjVmMVp3YVY4YnZ5ejBjSWdtVUVEQTlMMys0eWx5UjJ4L0lkYXZvd1ZweENSMEN2bHpV
NStINFQwUEt4THlCMzlGTXNOZmhScnB0elVHQzNEMGFlZVJZU1pXWGFiRkw1MVZTKzlDQmN0cHQ0
QWRpdVZMMm1zL0g1b1JOSk9mUENpUURyZTlyZWhlL0FyVVB6eDJxb1Bmam5TQjYvdktMRjNsN25y
MEZOTlduQ0YrTkEzUFFKSUtMZkx1aEFJNnIxZHRnSTEydWdXM1VwVHNmS1lCRDNNajZyMnVqMS9x
VEtXdzk2bldkbnFEbFdiQ3FUem1BUGppRkJMbk10VjJNYUhWbXdRYTBiRUczRXh4eG9jcU1KZktP
bXNpV0VhS09LNUZpNTR4M2drOGkvNXlVVVlmdk4rbzhVa0xEdFlRaHFiMVR2TFBLRkszVlptWEpD
UHU4NmU1Y1JrVVNhMXRtZnBOSEx5dVI3UmF3aWdCSGJJZzgvWW95Y2JoNitvZG92Z09MSzRrVWZ4
RzFYdG92cHdGUi90Ujd5VEtSWjl4bTg4NnRpd1lGRDdOcGUxbytEcjhEU1dYcGg3eXErZklkZEgz
WXhRUFF4QzIrRStEdzJoRmdtVjlhR2g1TE1IK2pQVTJWdWEwcWZ5eXFKblpUNVk5QURYREpZdE9J
N21vMHlaWTBveVlaZ2tIR282ZU1JaE5QR3VOQzYzNGg5dkpBQlEwWXp0Z1c5ei83d0MyOEpvVEhM
Y3lXVTVKVDRiMThyYTBtMXBKRzBzMTgxWFpkcDFvS1lQMHZCVmhvUkNjSE85eWxDTXZGbUt2VkRG
aitZb2xWQ3NvWmY0SHJzTzJWdUNmSVQyWmZXb0xBb2JuQStsMytZWGhTNSsxeDJkMHYzMnRjNWVm
WnpBNWlKZGpITEszODdURzdpU2x4UnJ5bW1OMXdzdkhXaVFlLzI4TXlxVnRiOG90VTE2dDdYMGgz
RDBSYmNmVmFCRW1Na0ROdUpVK2poVkhOMlV5NE96NlUrbUFpcXJmM0xBUitkb2UrdkNUclAvait3
aGdvUU9YWXBtT1UwVElRMnNvbjdxSE1GOXNrZFhDQ3ppN3lMOXcrMFh4ZHlaT2xVRzA1dFFFS2Ex
L0g3TWtaVm1NcHlxTWNvUU1NWVErU1ZFMS9SYXBzdUxmNmtXSjh3eUNrUmJvUVp0THdJREFRQUJv
M293ZURBZEJnTlZIUTRFRmdRVTJIWlo2ZGNyaHJ2RmNtZG5JcFpCazR3WHRNY3dId1lEVlIwakJC
Z3dGb0FVMkhhWjZkY3JocnZGY21kbklwWkJrNHdYdE1jd0R3WURWUjBUQVFIL0JBVXdBd0VCL3pB
bEJnTlZIUkVFSGpBY2doRmpaR2N0TVRjd0xtTnBjMk52TG1OdmJZSUhZM1JuTFRFM01EQU5CZ2tx
aGtpRzl3MEJBUTBGQUFPQ0JBRUFqMXZEWGlRdkE2T0FZbE9SVWZ2a3ZpVkwwV20zV1JJNTlBOWFK
L3lKeVVibnAvanZXS0VjR2ZCRUJsM2Fielp2RllEUjNkQkU1eEJHT2tBMjhPZXZIb3MyTnIwMk1L
MEZxalFEQ3ZTdmVoeGh3eXpmdlQwMmdUd3FrbzJKL1g1YXYrVnF0NjB5S2dHNm1Ta0JmbzNTYzQy
WlpYM2NEQXRSa0FmN21LZUxncVNEKzUyTURmdXQ0SHhqQkFybFlQL0NCV1NqQ3hCeHhqN3N1SDZ1
--More--
```

Step 3 Copy the package contents and paste it to a .json file. Save this file.

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 101.

Register Crosswork Data Gateway with Crosswork Cloud Applications

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

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

Step 1 Log in to Crosswork Cloud.

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

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

Step 4 Enter a name for the Crosswork Data Gateway.

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

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

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

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

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

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

What to do next

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

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

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

If the Crosswork Data Gateway has not successfully connected to the Crosswork Cloud service, refer to the Troubleshoot the Crosswork Data Gateway Connectivity, on page 102 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 12: Troubleshooting Crosswork Data Gateway Connectivity

Issue	Action
Crosswork Data Gateway cannot be enrolled with Cisco Crosswork Cloud due to an NTP issue, i.e., there is a clock-drift between the two.	1. Log into the Crosswork Data Gateway VM. 2. From the main menu, go to **5 Troubleshooting** > **Run show-tech**. Enter the destination to save the tarball containing logs and vitals and click **OK**. In the show-tech logs (in file `session.log` at location `/cdg/logs/components/controller-gateway/session.log`), if you see the error `UNAUTHENTICATED:invalid certificate. reason: x509: certificate has expired or is not yet valid` , then there is a clock-drift between Crosswork Data Gateway and Cisco Crosswork Cloud. 3. From the main menu, go to **3 Change Current System Settings** > **1 Configure NTP**. Configure NTP to sync with the clock time on the Cisco Crosswork Cloud server and try enrolling the Crosswork Data Gateway with Crosswork Cloud again.
Crosswork Data Gateway does not have direct connectivity to external web services.	**1.** Configure a proxy server if a proxy server is missing in your environment. **2.** If a proxy server is already present in your enviroment, check if the proxy URL is correct. **3.** Check if the credentials of the proxy (certificate, proxy name etc) are correct. To update the proxy server details on the Crosswork Data Gateway, see Configure Control Proxy, on page 113.

CHAPTER 4

Configure Crosswork Data Gateway Instance

A Cisco Crosswork Data Gateway instance is created as a standalone instance and can be geographically separate from the controller application (Crosswork Cloud). This instance is capable of connecting to the controller application which will enable data collection from the network.

This chapter contains the following topics:

Manage Crosswork Data Gateway Users

This section contains the following topics:

Supported User Roles

Cisco Crosswork Data Gateway supports only two users with the following user roles:

- **Administrator**: One default **dg-admin** user with administrator role is created when Cisco Crosswork Data Gateway is brought up for the first time. This user cannot be deleted and has both read and write privileges such as starting and shutting down the Cisco Crosswork Data Gateway VM, registering an application, applying authentication certificates, configuring server settings, and performing a kernel upgrade.
- **Operator**: The **dg-oper** user is also created by default during the initial VM bring up. This user can review the health of the Cisco Crosswork Data Gateway, retrieve error logs, receive error notifications and run connectivity tests between Cisco Crosswork Data Gateway instance and the output destination.

Note

- User credentials are configured for both the user accounts during Cisco Crosswork Data Gateway installation.
- Users are locally authenticated.

The following table shows the permissions available to each role:

Table 13: Permissions Per Role

Permissions	Administrator	Operator
Get Enrollment Package	✓	✓
Show system settings		
vNIC Addresses NTP DNS Proxy UUID Syslog Certificates First Boot Provisioning Log Timezone Enrollment Token	✓	✓
Change Current System Settings		

Permissions	Administrator	Operator
Configure NTP Configure DNS Configure Control Proxy Configure Static Routes Configure Syslog Create new SSH keys Import Certificate Configure vNIC MTU Configure Timezone Configure Password Requirements Configure Simultaneous Login Limits Configure Idle Timeout Configure Login Check Frequency Configure Interface Address Configure Enrollment Token	✓	✕
Vitals		
Docker Containers Docker Images Controller Reachability NTP Reachability Route Table ARP Table Network Connections Disk Space Usage Linux services NTP Status System Uptime	✓	✓
Troubleshooting		

Permissions	Administrator	Operator
Run Diagnostic Commands	✓	✓
Run show-tech	✓	✓
Export auditd logs	✓	✓
Re-enroll Data Gateway	✓	✓
Enable TAC Shell Access	✓	×
Change Passphrase	✓	✓

Change Passphrase

Both administrator and operator users can change their own passphrases but not each others'.

Follow these steps to change your passphrase:

Step 1 From the Main Menu, select **Change Passphrase** and click **OK**.

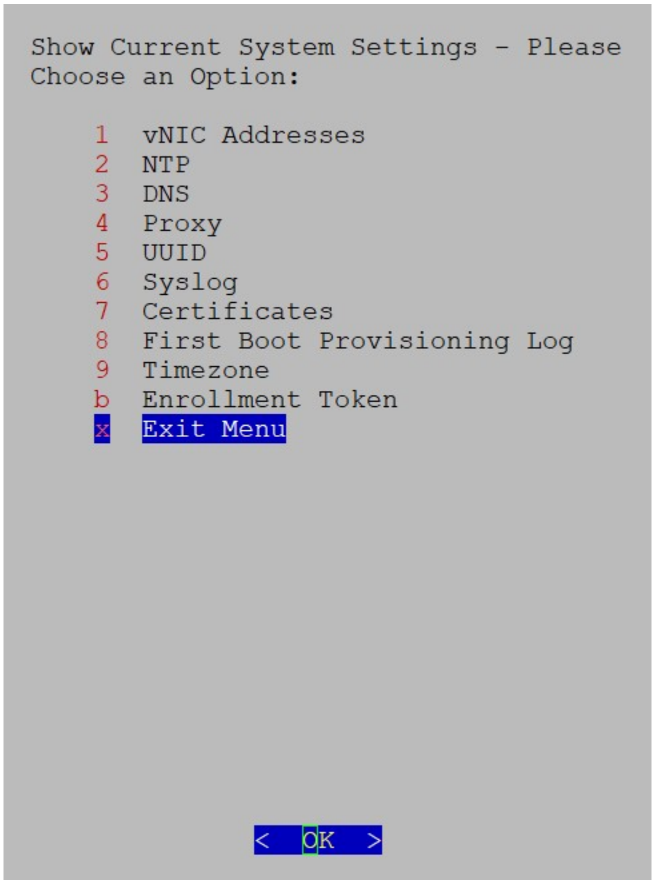
Step 2 Enter your current password and press **Enter**.

Step 3 Enter new password and press **Enter**. Re-type the new password and press **Enter**.

View Current System Settings

Crosswork Data Gateway allows you to view the following settings:

Figure 36: Show Current System Settings Menu



```
Show Current System Settings - Please
Choose an Option:

    1  vNIC Addresses
    2  NTP
    3  DNS
    4  Proxy
    5  UUID
    6  Syslog
    7  Certificates
    8  First Boot Provisioning Log
    9  Timezone
    b  Enrollment Token
    x  Exit Menu
```

Follow these steps to view the current system settings:

Step 1 From the Main Menu, select **Show System Settings**.

Step 2 In the prompt, click **OK** to open the **Show Current System Settings** menu.

Step 3 Select the setting you want to view.

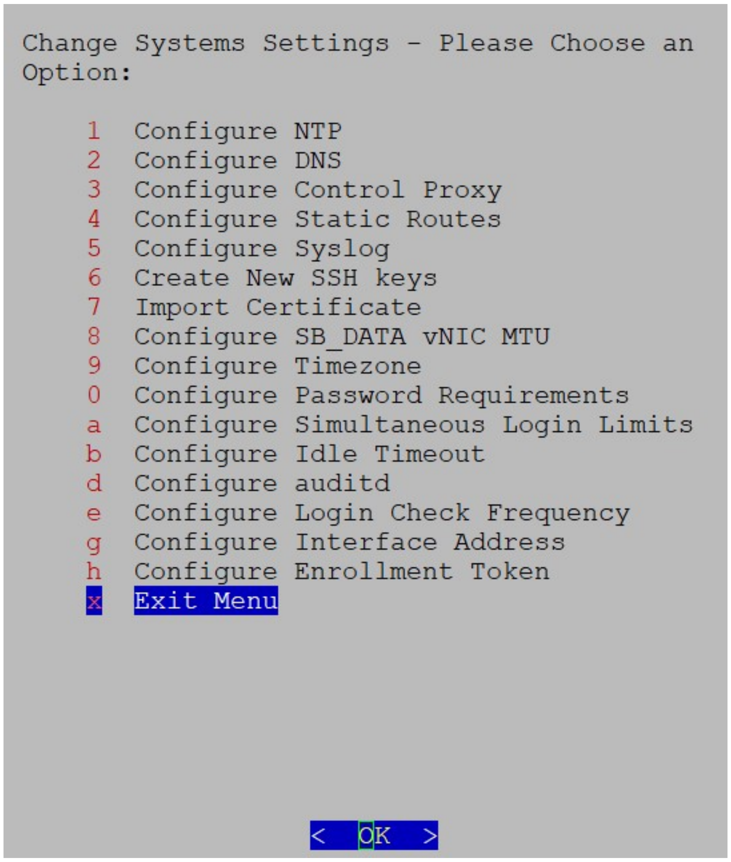
Setting Option	Description
1 vNIC Addresses	Displays the vNIC configuration, including address information.
2 NTP	Displays currently configured NTP server details.
3 DNS	Displays DNS server details.
4 Proxy	Displays proxy server details (if any configured).
5 UUID	Displays the system UUID.

Setting Option	Description
6 Syslog	Displays the Syslog forwarding configuration. If no Syslog forwarding is configured, this will display only "# Forwarding configuration follows" on screen.
7 Certificates	Provides options to view the following certificate files: • Crosswork Data Gateway signing certificate file • Controller signing certificate file • Controller SSL/TLS certificate file • Syslog certificate file • Collector certificate file
8 First Boot Provisioning Log	Displays the content of the first boot log file.
9 Timezone	Displays the current timezone setting.
b Enrollment Token	Displays the token that Crosswork Data Gateway used to enroll with Crosswork Cloud.

Change Current System Settings

Crosswork Data Gateway allows you to configure the following settings:

Figure 37: Change System Settings Menu



```
Change Systems Settings - Please Choose an
Option:

    1  Configure NTP
    2  Configure DNS
    3  Configure Control Proxy
    4  Configure Static Routes
    5  Configure Syslog
    6  Create New SSH keys
    7  Import Certificate
    8  Configure SB_DATA vNIC MTU
    9  Configure Timezone
    0  Configure Password Requirements
    a  Configure Simultaneous Login Limits
    b  Configure Idle Timeout
    d  Configure auditd
    e  Configure Login Check Frequency
    g  Configure Interface Address
    h  Configure Enrollment Token
    x  Exit Menu

                 <  OK  >
```

Follow these steps to modify the current system settings:

Step 1 From the Main Menu, select **3 Change Current System Settings**.

Step 2 Select the setting that you want to modify.

- NTP
- DNS
- Control proxy
- Static routes
- Syslog
- SSH keys
- Certificate
- vNIC MTU
- Timezone
- Password requirements

- Simultaneous login limits
- Idle timeout
- Auditd
- Login check frequency
- Interface address
- Enrollment token

Note

- Crosswork Data Gateway system settings can only be configured by the administrator.
- When using an IPv6 address, it must be surrounded by square brackets ([1::1]).
- In the Settings options where you require to use SCP, if you are not using the default SCP port 22, you can specify the port as a part of the SCP command. For example,

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

  Where 55 is a custom port.

Configure NTP

It is important that NTP time be synchronized with the controller application and its Crosswork Data Gateway instances. If not, then session handshake doesn't happen and functional images are not downloaded. In such cases, error message clock time not matched and sync failed is logged in controller-gateway.log. To access log files, see Run show-tech, on page 130. You can use Controller Reachability and NTP Reachability options from **Main Menu** > **Vitals** to check NTP reachability for the controller application as well as the Crosswork Data Gateway. See View Crosswork Data Gateway Vitals, on page 122. If NTP has been set incorrectly,you will see error Session not established.

When configuring Crosswork Data Gateway to use authentication via a keys file, the chrony.keys file must be formatted in a specific way as documented at https://chrony.tuxfamily.org/doc/3.5/chrony.conf.html#keyfile. For sites that use ntpd and are configured to use a ntp.keys file, it is possible to convert from ntp.keys to chrony.keys using the tool https://github.com/mlichvar/ntp2chrony/blob/master/ntp2chrony/ntp2chrony.py. The tool converts ntpd configuration into a chrony compatible format, but only the keys file is required to be imported into Crosswork Data Gateway.

Follow the steps to configure NTP settings:

Step 1 From the **Change Current System Settings** Menu, select **Configure NTP**.

Step 2 Enter the following details for the new NTP server:

- Server list, space delimited
- Use NTP authentication?
- Key list, space delimited and must match in number with server list
- Key file URI to SCP to the VM

- Key file passphrase to SCP to the VM

Step 3 Click **OK** to save the settings.

Configure DNS

Step 1 From the **Change Current System Settings** menu, select **Configure DNS** and click **OK**.

Step 2 Enter the new DNS server address(es) and domain.

Step 3 Click **OK** to save the settings.

Configure Control Proxy

If you have not configured a proxy server during installation, avail this option to set up a proxy sever:

Step 1 From the **Change Current System Settings** menu, select **Configure Control Proxy** and click **OK**.

Step 2 Click **Yes** for the following dialog if you wish to proceed. Click **cancel** otherwise.

Step 3 Enter the new Proxy server details:

- Server URL
- Bypass addresses
- Proxy username
- Proxy passphrase

Step 4 Click **OK** to save the settings.

Configure Static Routes

The static routes are configured when Crosswork Data Gateway receives add/delete requests from the collectors. The **Configure Static Routes** option from the main menu can be used for troubleshooting purpose.

⚠ **Caution** Static routes configured using this option are lost when the Crosswork Data Gateway reboots.

Add Static Routes

Follow the steps to add static routes:

Step 1 From the **Change Current System Settings** menu, select **4 Configure Static Routes**.

Step 2 To add a static route, select **a Add**.

Step 3 Select the interface for which you want to add a static route.

Step 4 Select the IP version.

Step 5 Enter IPv4 or IPv6 subnet in CIDR format when prompted.

Step 6 Click **OK** to save the settings.

Delete Static Routes

Follow the steps to delete a static route:

Step 1 From the **Change Current System Settings** Menu, select **4 Configure Static Routes**.

Step 2 To delete a static route, select **d Delete**.

Step 3 Select the interface for which you want to delete a static route.

Step 4 Select the IP version.

Step 5 Enter IPv4 or IPv6 subnet in CIDR format.

Step 6 Click **OK** to save the settings.

Configure Syslog

You can configure the remote servers during the Day0 installation through the configuration file. If you want to modify the Syslog server list, port number, protocol, and certificate file in Day1 installation or later use the Interactive Console.

Note For any Syslog server configuration with IPv4 or IPv6 support for different Linux distributions, please refer to your system administrator and configuration guides.

Follow the steps to configure Syslog:

Before you begin

Crosswork Data Gateway lets you configure multiple servers through the following modes:

- Simultaneous: Crosswork Data Gateway sends messages to all the configured Syslog server addresses. When one of the servers is unresponsive, the message is queued to the disk until the servers are response.
- Failover: Crosswork Data Gateway sends message to the first Syslog server address. If the server is not available, the message is sent to the subsequent configured address. When all the servers in the list are unresponsive, the message is queued to the disk until the servers are response.

Step 1 From the **Change Current System Settings** menu, select **5 Configure Syslog**.

Step 2 In the **Use Syslog** window, select **True** to continue configuring the Syslog server.

Step 3 In the **Select Syslog Multiserver Mode** window, select **Simultaneous** or **Failover**.

Step 4 Enter the values for the following Syslog attributes:

- Server address or hostname: Space-delmited list of IPv4 or IPv6 address of Syslog server accessible from the management interface.
- Port: Port number of the Syslog server
- Protocol: Use UDP, TCP, or RELP when sending system logs.
- Use Syslog over TLS?: Use TLS to encrypt Syslog traffic.
- TLS Peer Name: Syslog server's hostname exactly as entered in the server certificate SubjectAltName or subject common name.
- Syslog Root Certificate File URI: PEM formatted root cert of Syslog server retrieved using SCP.
- Syslog Certificate File Passphrase: Password of SCP user to retrieve Syslog certificate chain.

Step 5 Click **OK** to save the settings.

Create New SSH Keys

Creating new SSH keys will remove the current keys.

Follow the steps to create new SSH keys:

Step 1 From the **Change Current System Settings** Menu, select **6 Create new SSH keys**.

Step 2 Click **OK**. Crosswork Data Gateway launches an auto-configuration process that generates new SSH keys.

Import Certificate

Updating any certificate other than Controller Signing Certificate causes a collector restart.

Crosswork Data Gateway allows you to import the following certificates:

- Controller signing certificate file
- Controller SSL/TLS certificate file
- Syslog certificate file
- Proxy certificate file

Step 1 From the **Change Current System Settings** Menu, select **Import Certificate**.

Step 2 Select the certificate you want to import.

Step 3 Enter SCP URI for the selected certificate file.

Step 4 Enter passphrase for the SCP URI and click **OK**.

Configure vNIC2 MTU

You can change vNIC2 MTU only if you are using 3 NICs.

If your interface supports jumbo frames, the MTU value lies in the range of 60-9000, inclusive. For interfaces that do not support jumbo frames, the valid range is 60-1500, inclusive. Setting an invalid MTU causes Crosswork Data Gateway to revert the change back to the currently configured value. Please verify with your hardware documentation to confirm what the valid range is. An error will be logged into kern.log for MTU change errors which can be viewed after running showtech.

Step 1 From the **Change Current System Settings** menu, select **Configure vNIC1 MTU**.

Step 2 Enter the vNIC2 MTU value.

Step 3 Click **OK** to save the settings.

Configure Timezone of the Crosswork Data Gateway VM

The Crosswork Data Gateway VM first launches with default timezone as UTC. Update the timezone with your geographical area so that all Crosswork Data Gateway processes (including the showtech logs) reflect the timestamp corresponding to the location you have chosen.

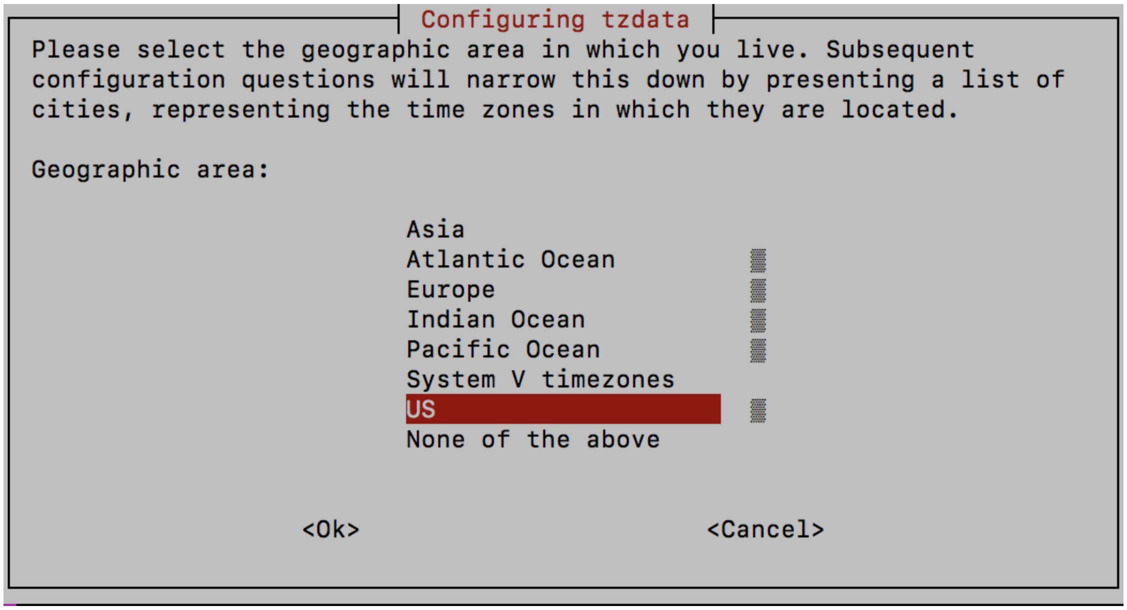
Step 1 Log in to the Crosswork Data Gateway VM.

Step 2 In the Crosswork Data Gateway VM interactive menu, select **3 Change Current System Settings**.

Step 3 From the menu, select **9 Timezone**.

Step 4 Select the geographic area in which you live.

Figure 38: Timezone Settings - Geographic Area Selection

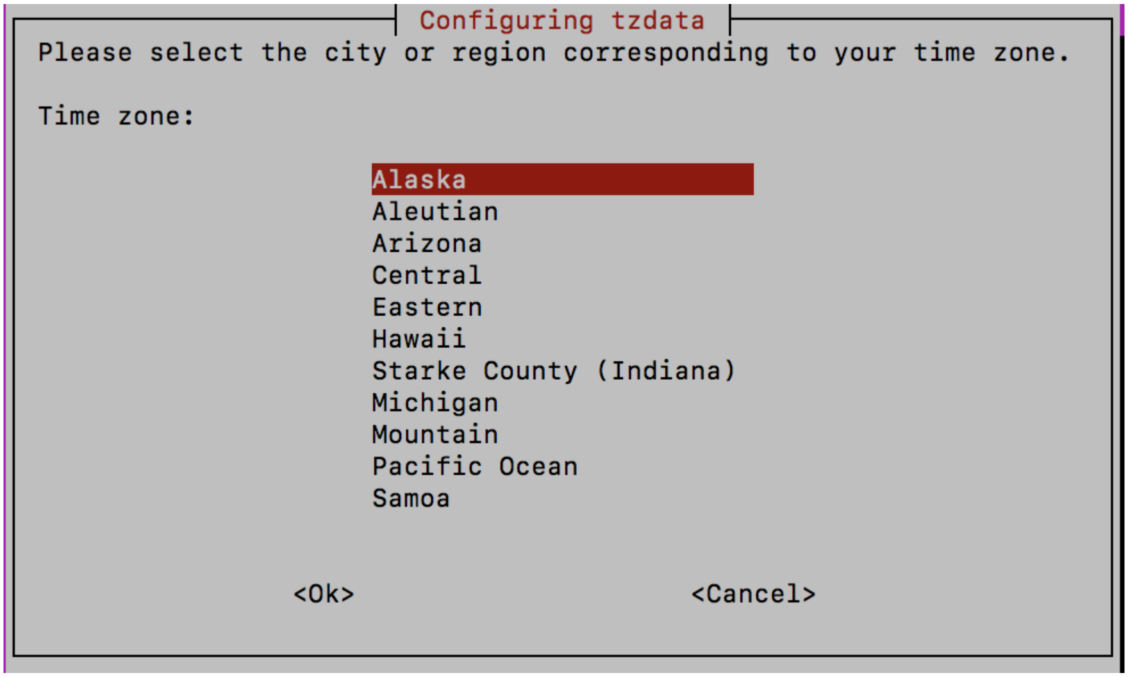


```
Configuring tzdata
Please select the geographic area in which you live. Subsequent
configuration questions will narrow this down by presenting a list of
cities, representing the time zones in which they are located.

Geographic area:
```

Step 5 Select the city or region corresponding to your timezone.

Figure 39: Timezone Settings - Region Selection



```
                    Configuring tzdata
Please select the city or region corresponding to your time zone.

Time zone:

                    Alaska
                    Aleutian
                    Arizona
                    Central
                    Eastern
                    Hawaii
                    Starke County (Indiana)
                    Michigan
                    Mountain
                    Pacific Ocean
                    Samoa


             <Ok>                       <Cancel>
```

Step 6 Select **OK** to save the settings.

Step 7 Reboot the Crosswork Data Gateway VM so that all processes pick up the new timezone. See *Reboot Crosswork Data Gateway VM* section in *Cisco Crosswork Network Controller 6.0 Administration Guide*.

Step 8 Log out of the Crosswork Data Gateway VM.

Configure Password Requirements

You can configure the following password requirements:

- Password Strength
- Password History
- Password expiration
- Login Failures

Step 1 From **Change Current System Settings** menu, select **Configure Password Requirements**.

Step 2 Select the password requirement you want to change.

Set the options you want to change:

- **Password Strength**
  - Min Number of Classes

    - Min Length
    - Min Changed Characters
    - Max Digit Credit
    - Max Upper Case Letter Credit
    - Max Lower Case Letter Credit
    - Max Other Character Credit
    - Max Monotonic Sequence
    - Max Same Consecutive Characters
    - Max Same Class Consecutive Characters

- **Password History**
    - Change Retries
    - History Depth
- **Password expiration**
    - Min Days
    - Max Days
    - Warn Days
- **Login Failures**
    - Login Failures
    - Initial Block Time (sec)
    - Address Cache Time (sec)

Step 3 Click **OK** to save the settings.

Configure Simultaneous Login Limits

By default, Crosswork Data Gateway supports 10 simultaneous sessions for the **dg-admin** and **dg-oper** user on each VM. To change this:

Step 1 From the **Change Current System Settings** menu, select **a Configure Simultaneous Login Limits**.

Step 2 In the window that appears, enter the number of simultaneous sessions for the **dg-admin** and **dg-oper** user.

Step 3 Select **Ok** to save your changes.

Configure Idle Timeout

Step 1 From the **Change Current System Settings** menu, select **b Configure Idle Timeout**.

Step 2 Enter the new value of idle timeout in the window that appears.

Step 3 Enter **Ok** to save your changes.

Configure Remote Auditd Server

Use this procedure to configure the auditd daemon export to a remote server.

Step 1 From the **Change Current System Settings** menu, select **c Configure auditd**.

Step 2 Enter the following details:

- Remote auditd server address.
- Remote auditd server port.

Step 3 Select **OK** to save your changes.

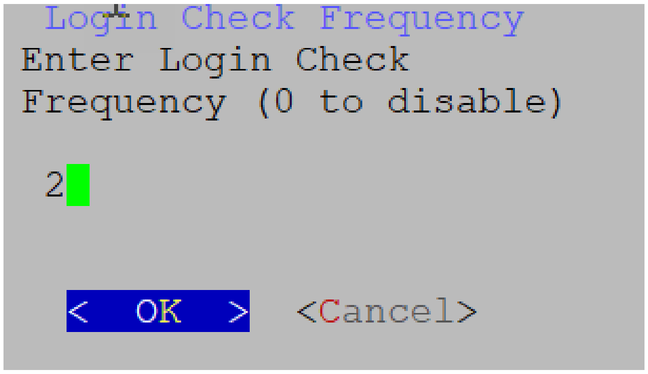
Configure Login Frequency

You can configure the number of permissible log in attempts the user can make after a log in failure.

Step 1 From the **Change Current System Settings** menu, select **Configure Login Check Frequency** and click **OK**.

Step 2 In the **Login Check Frequency** window, enter the number of log in attempts you want to monitor. To disable the feature, enter 0.

Figure 40: Login Check Frequency Window

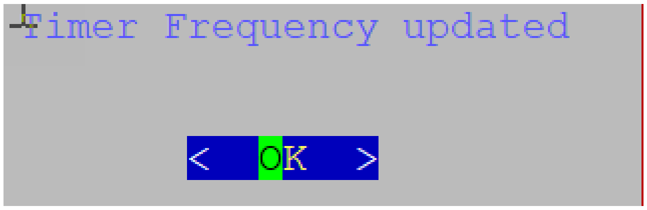


```
Enter Login Check
Frequency (0 to disable)

 2
```

After the timer is updated, a confirmation window appears.

Figure 41: Timer Frequency Updated Window



```
Timer Frequency updated
```

Configure Interface Address

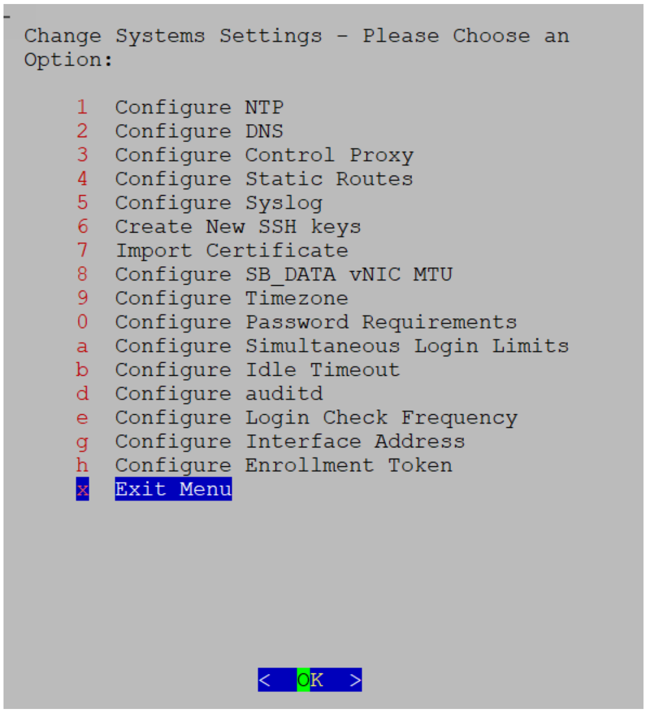
After you have deployed a Crosswork Data Gateway instance, you can reconfigure the interfaces that are already associated with an instance. When you reconfigure an interface, you can change its name, associate IP address, or access the security group that is associated with an interface.

Before you begin

- All the devices must be detached from the Crosswork Data Gateway instance for which you want to reconfigure the interface address.
- The Crosswork Data Gateway instance must be in the maintenance mode.

Step 1 From the **Change System Settings** menu, select **Configure Interface Address**.

Figure 42: Change System Settings Menu

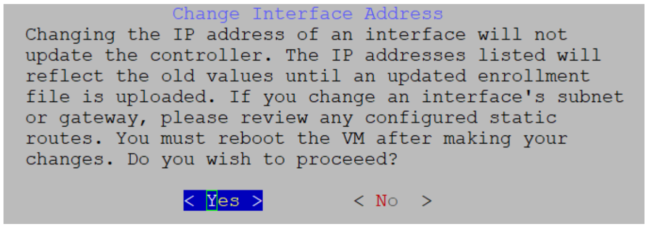


```
Change Systems Settings - Please Choose an
Option:

    1  Configure NTP
    2  Configure DNS
    3  Configure Control Proxy
    4  Configure Static Routes
    5  Configure Syslog
    6  Create New SSH keys
    7  Import Certificate
    8  Configure SB_DATA vNIC MTU
    9  Configure Timezone
    0  Configure Password Requirements
    a  Configure Simultaneous Login Limits
    b  Configure Idle Timeout
    d  Configure auditd
    e  Configure Login Check Frequency
    g  Configure Interface Address
    h  Configure Enrollment Token
    x  Exit Menu
```

Step 2 In the **Change Interface Address** confirmation box, click **Yes**.

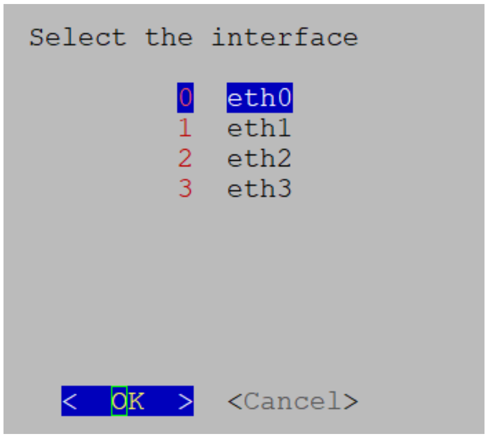
Figure 43: Change Interface Address Confirmation Message



```
Change Interface Address
Changing the IP address of an interface will not
update the controller. The IP addresses listed will
reflect the old values until an updated enrollment
file is uploaded. If you change an interface's subnet
or gateway, please review any configured static
routes. You must reboot the VM after making your
changes. Do you wish to proceeed?
```

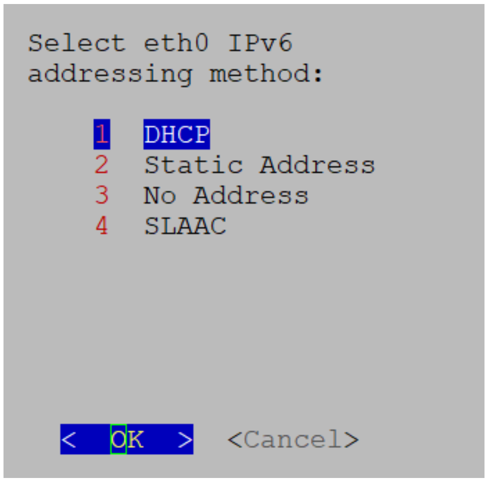
Step 3 Select the interface that you want to reconfigure and click **OK**. The options are `eth0`, `eth1`, `eth2`, or `eth3`.

Figure 44: Interface Selection Menu



Step 4 Select the <interface> IPv4 addressing method. The options are `DHCP`, `Static Address`, or `No address`. Cisco recommends that you select the option that you had specified during the Day0 installation.

Figure 45: IPv6 Address Selection



Step 5 Enter the IPv4 address and click **OK**.

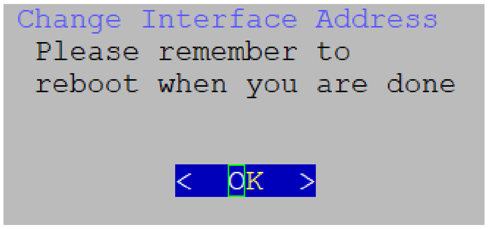
Step 6 Enter the IPv4 Netmask address and click **OK**.

Step 7 In the **Skip <interface> IPv4 gateway configuration confirmation** box, select `True` or `False` and click **OK**.

Step 8 If you have selected `True` in the previous step, specify the IPv4 gateway address.

Step 9 In the **Change Interface Address** confirmation box, click **OK**.

Figure 46: Confirmation Message



```
Change Interface Address
 Please remember to
 reboot when you are done
```

After the interface is configured, make sure to reboot the VM.

Enroll Crosswork Data Gateway with the Crosswork cloud, See Register Crosswork Data Gateway with Crosswork Cloud Applications, on page 101 for procedure on how to enroll Cisco Crosswork Data Gateway with Crosswork Cloud applications.

Configure Enrollment Token

Before you begin

Ensure that you have downloaded and copied the enrollment token from Crosswork Cloud.

Step 1 From the **Change Current System Settings** menu, select **h Configure Enrollment Token** and click **OK**.

The **Configure Enrollment Token** is displayed indicating that you must re-enroll Crosswork Data Gateway with Crosswork Cloud after the enrollment token is updated.

Step 2 In the **Configure Enrollment Token** window, click **OK**.

Step 3 In the **Enter Enrollment Token** window, enter the new enrollment token.

Step 4 Click **OK** to save the token.

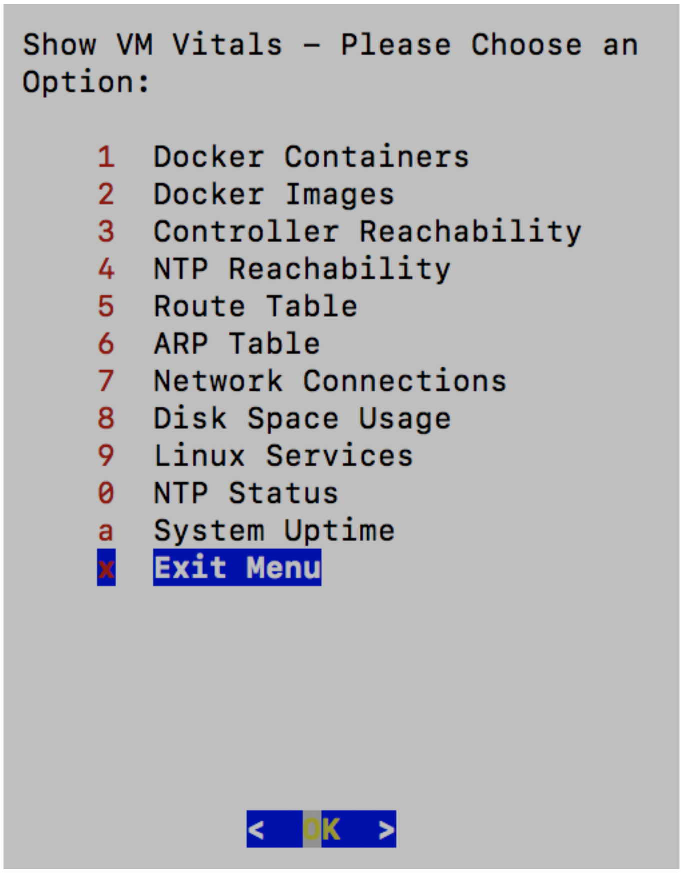
View Crosswork Data Gateway Vitals

Follow these steps to view Cisco Crosswork Data Gateway vitals:

Step 1 From the Main Menu, select **Vitals**.

Step 2 From the **Show VM Vitals** menu, select the vital you want to view.

Figure 47: Show VM Vitals Menu



```
Show VM Vitals - Please Choose an
Option:

    1  Docker Containers
    2  Docker Images
    3  Controller Reachability
    4  NTP Reachability
    5  Route Table
    6  ARP Table
    7  Network Connections
    8  Disk Space Usage
    9  Linux Services
    0  NTP Status
    a  System Uptime
    x  Exit Menu


                <  OK  >
```

Vital	Description
Docker Containers	Displays the following vitals for the Docker containers currently instantiated in the system: • Container ID • Image • Name • Command • Created Time • Status • Port

Vital	Description
Docker Images	Displays the following details for the Docker images currently saved in the system: • Repository • Image ID • Created Time • Size • Tag
Controller Reachability	Displays the results of controller reachability test run: • Default IPv4 gateway • Default IPv6 gateway • DNS server • Controller • Controller session status
NTP Reachability	Displays the result of NTP reachability tests: • NTP server resolution • Ping • NTP Status • Current system time
Route Table	Displays IPv4 and IPv6 routing tables.
ARP Table	Displays ARP tables.
Network Connections	Displays the current network connections and listening ports.
Disk Space Usage	Displays the current disk space usage for all partitions.
Linux Services	Displays the status of the following Linux services: • NTP • SSH • Syslog • Docker • Cisco Crosswork Data Gateway Infrastructure containers.
Check NTP Status	Displays the NTP server status.

Vital	Description
Check System Uptime	Displays the system uptime.

Troubleshooting Crosswork Data Gateway VM

To access **Troubleshooting** menu, select **5 Troubleshooting** from the Main Menu.

Note The image shows the Troubleshooting menu corresponding to **dg-admin** user. Few of these options are not available to **dg-oper** user. See Table Table 13: Permissions Per Role, on page 106.

The **Troubleshooting** menu that provides the following options:

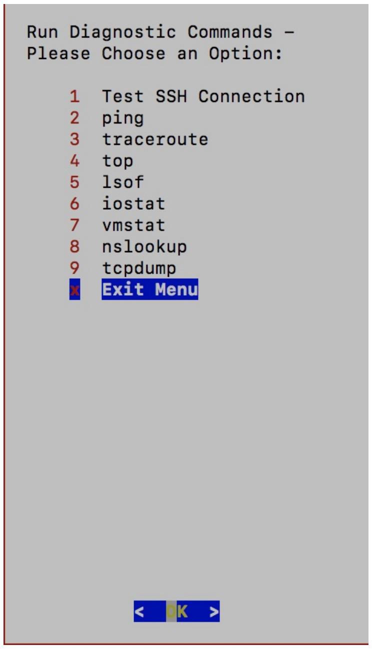
Note Crosswork Cloud does not support the **Troubleshooting** > **Remove All Non-Infra Containers and Reboot** option.

- Run Diagnostic Commands, on page 125
- Run show-tech, on page 130
- Shutdown the Crosswork Data Gateway VM, on page 130
- Export auditd Logs, on page 130
- Enable TAC Shell Access, on page 131

Run Diagnostic Commands

The **Run Diagnostics** menu provides you the following options in the console:

Figure 48: Run Diagnostics Menu



```
Run Diagnostic Commands -
Please Choose an Option:

    1  Test SSH Connection
    2  ping
    3  traceroute
    4  top
    5  lsof
    6  iostat
    7  vmstat
    8  nslookup
    9  tcpdump
    x  Exit Menu
```

Ping a Host

Crosswork Data Gateway provides you ping utility that can be used to check reachability to any IP address.

Step 1 From Main Menu, navigate to **Troubleshooting** > **Run Diagnostics** > **ping**.

Step 2 Enter the following information:

- Number of pings
- Destination hostname or IP
- Source port (UDP, TCP, TCP Connect)
- Destination port (UDP, TCP, TCP Connect)

Step 3 Click **OK**.

Traceroute to a Host

Crosswork Data Gateway provides the traceroute option to help troubleshoot latency issues. Using this option provides you a rough time estimate for the Crosswork Data Gateway to reach the destination.

Step 1 From Main Menu, navigate to **Troubleshooting** > **Run Diagnostics** > **traceroute**.

Step 2 Enter the traceroute destination.

Step 3 Click **OK**.

Command Options to Troubleshoot

Crosswork Data Gateway provides several commands for troubleshooting.

Step 1 From Main Menu, navigate to **Troubleshooting** > **Run Diagnostics**.

Step 2 Select the command and other option or filters for each of the commands:

- **4 top**
- **5 lsof**
- **6 iostat**
- **7 vmstat**
- **8 nsolookup**

Step 3 Click **Ok**.

Once you have selected all the options, Crosswork Data Gateway clears the screen and runs the command with the specified options.

Download tcpdump

Crosswork Data Gateway provides the tcpdump option that allows you to capture and analyze network traffic.

Note This task can only be performed by a **dg-admin** user.

Step 1 From Main Menu, navigate to **Troubleshooting** > **Run Diagnostics** > **tcpdump**.

Step 2 Select an interface to run the tcpdump utility. To run the utility for all the interfaces, select the **All** option.

Step 3 Select the appropriate check box to view the packet information on the screen or save the captured packets to a file.

Step 4 Enter the following details and click **OK**.

- Packet count limit
- Collection time limit
- File size limit
- Filter expression

Depending on the option you choose, Crosswork Data Gateway displays the packet capture information on the screen or saves it to a file. After the tcpdump utility reaches the specified limit, Crosswork Data Gateway compresses the file, and prompts for the SCP credentials to transfer the file to a remote host. The compressed file is deleted once the transfer is complete or if you've decided to cancel the file transfer before completion.

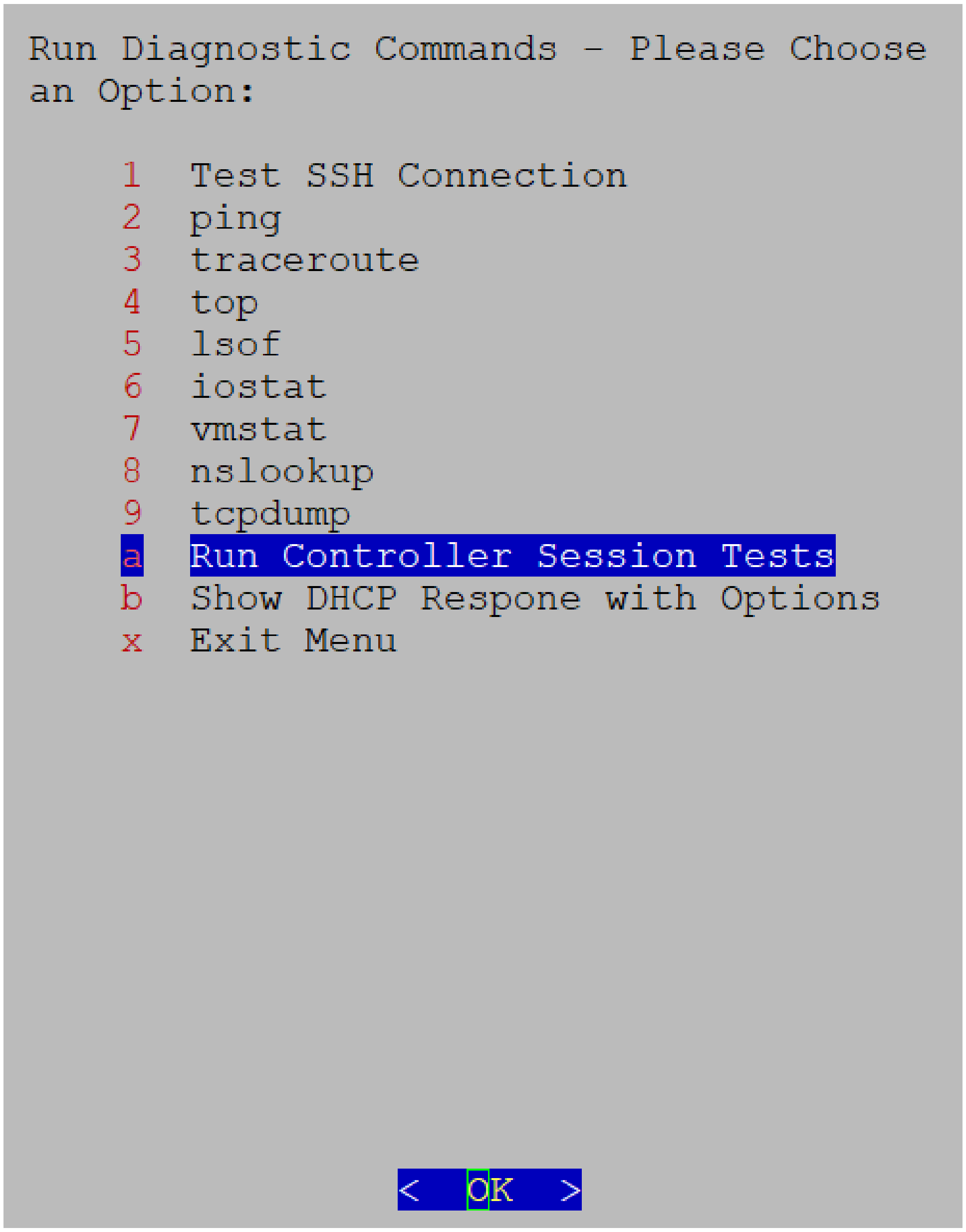
Run a Controller Session Test

After Crosswork Data Gateway is installed, you can validate if the instance is able to establish a connection with Crosswork Cloud by using the controller session test option. In addition to the connection tests, the utility validates and analyzes the discrepancies between the resources (CPU and memory) assigned to the VM and the resources prescribed by the deployment profile.

From Main Menu, navigate to **Troubleshooting** > **Run Diagnostics** > **Run Controller Session Tests**. If the connection is completed, the console displays a message indicating that the instance was able to establish a connection. When the connection fails, additional validation tests are performed, and the following information is displayed:

- DNS server IP address
- DNS domain
- NTP server address
- NTP status
- Proxy URL
- Proxy reachability status
- Controller URL
- Controller reachability status
- The date when the tests were last performed.

Figure 49: Run Controller Session Tests Menu

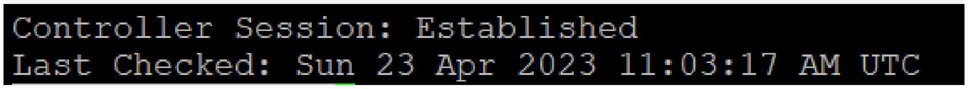


```
Run Diagnostic Commands - Please Choose
an Option:

    1  Test SSH Connection
    2  ping
    3  traceroute
    4  top
    5  lsof
    6  iostat
    7  vmstat
    8  nslookup
    9  tcpdump
    a  Run Controller Session Tests
    b  Show DHCP Respone with Options
    x  Exit Menu

                 <  OK  >
```

Figure 50: Result of the Run Controller Session Tests Menu



```
Controller Session: Established
Last Checked: Sun 23 Apr 2023 11:03:17 AM UTC
```

What to do next

If the controller session was not established, review the information displayed on the console to determine the probable cause of the failure and perform the corrective actions proposed on the console.

Run show-tech

Crosswork Data Gateway provides the show_tech option to export its log files to a user-defined SCP destination.

The collected data includes the following:

- Logs of all the Data Gateway components running on Docker containers
- VM Vitals

It creates a tarball in the directory where it is executed. The output is a tarball named `DG-<CDG version>-<CDG host name>-year-month-day--hour-minute-second.tar.xz.enc`.

The execution of this command may take several minutes depending on the state of Crosswork Data Gateway.

Step 1 From **Troubleshooting** menu, select **Show-tech** and click **OK**.

Step 2 Enter the destination to save the tarball containing logs and vitals.

Step 3 Enter your SCP passphrase and click **OK**.

The showtech file downloads in an encrypted format.

Note Depending on how long the system was in use, it may take several minutes to download the showtech file.

Step 4 After the download is complete run the following command to decrypt it:

Note In order to decrypt the file, you must use OpenSSL version 1.1.1i. Use the command `openssl version` to check the openssl version on your system.

To decrypt the file on a MAC, you must install OpenSSL 1.1.1+. This is because LibreSSL's `openssl` command does not support all the switches supported by OpenSSL's `openssl` command.

```
openssl enc -d -AES-256-CBC -pbkdf2 -md sha512 -iter 100000 -in <showtech file> -out <decrypted
filename> -pass pass:<password>
```

Shutdown the Crosswork Data Gateway VM

From the **Troubleshooting** Menu, select **5 Shutdown VM** to power off the Crosswork Data Gateway VM.

Export auditd Logs

Follow the steps to export auditd logs:

Step 1 From **Troubleshooting**, select **Export audit Logs**.

Step 2 Enter a passphrase for auditd log tarball encryption.

Step 3 Click **OK**.

Re-enroll Crosswork Data Gateway

Follow the steps to re-enroll Crosswork Data Gateway:

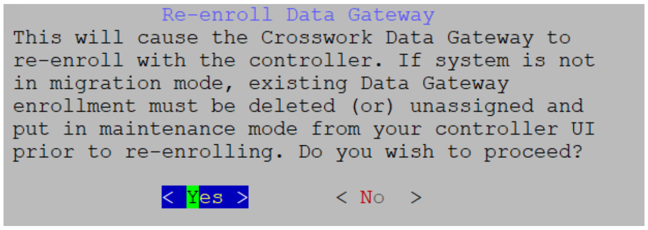
Before you begin

The existing Crosswork Data Gateway enrollment must be deleted from the controller prior to re-enrolling.

Step 1 From **Troubleshooting** menu, select **Re-enroll Data Gateway**.

Step 2 Review the information inn the confirmation window and click **Yes**.

Figure 51: Re-enroll Data Gateway Confirmation Window



```
            Re-enroll Data Gateway
This will cause the Crosswork Data Gateway to
re-enroll with the controller. If system is not
in migration mode, existing Data Gateway
enrollment must be deleted (or) unassigned and
put in maintenance mode from your controller UI
prior to re-enrolling. Do you wish to proceed?
```

Remove Rotated Log Files

Follow the steps to removes all rotated log files (*.gz or *.xz) in the `/var/log` and `/opt/dg/log` folders.

Step 1 From **Troubleshooting** menu, select **Remove Rotated Log files**.

Step 2 Select **Yes** in the dialog that appears to save your changes.

Enable TAC Shell Access

The TAC Shell Access function allows a Cisco engineer to directly log in to the Ubuntu shell via multifactor authentication, using a reserved user named **dg-tac**.

Initially, the **dg-tac** user account is locked and password is expired to prevent the user from getting a shell prompt. Once enabled, the dg-tac user is active until the next calendar day, 12:00 a.m UTC (midnight UTC), which is less than 24 hours.

The steps to enable the **dg-tac** user are as follows:

Note Enabling this access requires you to communicate actively with the Cisco engineer.

Before you begin

Ensure that the Cisco engineer who is working with you has access to the SWIMS Aberto tool.

Step 1 Log in to the Data Gateway VM as the **dg-admin** user.

Step 2 From the main menu, select **Troubleshooting**.

Step 3 From the **Troubleshooting** menu, select **t Enable TAC Shell Access**.

A dialog appears, warning that the **dg-tac** user login requires a password that you set and a response to a challenge token from TAC. At this point, you may answer **No** to stop the enable process or **Yes** to continue.

Step 4 If you continue, the system prompts for a new password to use and shows the day when the account disables itself.

Step 5 Enter a password to unlock the account in the console menu.

Step 6 Log out of the Crosswork Data Gateway.

Step 7 Follow these steps if the Crosswork Data Gateway VM can be accessed by the Cisco engineer directly. Move to **Step 8** otherwise.

a) Share the password that you had set in Step 5 for the **dg-tac** user with the Cisco engineer who is working with you.

b) The Cisco engineer logs in as the **dg-tac** user Via SSH with the password you had set.

After entering the password, the system presents the challenge token. The Cisco engineer signs the challenge token using the SWIMS Aberto tool and pastes the signed response to the challenge token back at the Crosswork Data Gateway VM.

c) The Cisco engineer logs in successfully as the **dg-tac** user and completes the troubleshooting.

There is a 15-minute idle timeout period for the **dg-tac** user. If logged out, the Cisco engineer needs to sign a new challenge to log in again.

d) After troubleshooting is complete, the Cisco engineer logs out of the TAC shell.

Step 8 If Crosswork Data Gateway VM cannot be accessed directly by the Cisco engineer, start a meeting with the Cisco engineer with desktop sharing enabled.

a) Log in as the **dg-tac** user Via SSH using the following command:

```
ssh dg-tac@<DG hostname or IP>
```

b) Enter the password that you set for the **dg-tac** user.

After entering the password, the system presents the challenge token. Share this token with the Cisco engineer who will then sign the token using the SWIMS Aberto tool and share the response with you.

c) Paste the signed response to the challenge token back to the Crosswork Data Gateway VM and press enter to get the shell prompt.

d) Share your desktop or follow the Cisco engineer's instructions for troubleshooting.

There is a 15-minute idle timeout period for the **dg-tac** user. If logged out, the Cisco engineer needs to sign a new challenge to log in again.

e) Log out of the TAC shell after troubleshooting is complete.

Audit TAC Shell Events

Timestamp information of the following list of TAC shell events is logged to the **tac_shell.log** file. The Tac shell events are also sent to the Crosswork Cloud controller.

- TAC shell enabled
- TAC shell disabled
- dg-tac login
- dg-tac log out

If the Data Gateway is unable to connect to the Crosswork Cloud controller, the TAC shell events are logged in the `/opt/dg/data/controller-gateway/audit/pending` folder. Once the Crosswork Cloud controller is reachable, these events are sent within 5 minutes.

The **tac_shell.log** file is available in the showtech bundle of the Crosswork Data Gateway VM.

CHAPTER 5

Delete the Virtual Machine

This section contains the following topics:

Delete VM using vSphere UI

This section explains the procedure to delete a Crosswork Data Gateway VM from vCenter.

Note Be aware that this procedure deletes all your Crosswork Data Gateway data.

Before you begin

Ensure you have deleted the Crosswork Data Gateway from Crosswork Cloud as described in the *Section: Delete Crosswork Data Gateways* of the respective Crosswork Cloud application user guide.

Step 1 Log in to the VMware vSphere Web Client.

Step 2 In the **Navigator** pane, right-click the app VM that you want to remove and choose **Power** > **Power Off**.

Step 3 Once the VM is powered off, right-click the VM again and choose **Delete from Disk**.

The VM is deleted.

Delete VM from OpenStack

Follow the steps to delete the Crosswork Data Gateway Service from OpenStack using the OpenStack UI:

Note This procedure deletes the Crosswork Data Gateway VM data. The Crosswork Data Gateway VM cannot be recovered once it has been deleted.

Before you begin

Ensure that you have deleted the Crosswork Data Gateway from Crosswork Cloud as described in the Section: *Delete Crosswork Data Gateways* in the *Cisco Crosswork Cloud User Guide*.

Step 1 **From the OpenStack UI:**

a) Log in to the OpenStack UI.

b) Navigate to **Compute** > **Instances**.

c) From the list of VM displayed in this page, select the VM you want to delete.

d) Click **Delete Instances**.

e) Click **Delete Instances** in the confirmation window that appears to delete the VM.

OR

Step 2 **From the OpenStack CLI:**

a) Log in to the OpenStack VM from CLI.

b) Run the following command:

```
openstack server delete CDG_VM_name
```

For example,

```
openstack server delete cdg-ospd1
```

c) (Optional) Confirm that the VM has been deleted by viewing the list of all VMs.

```
openstack server list
```