



Cisco Crosswork Data Gateway 4.0.1 Installation and Configuration Guide for Cloud Applications

First Published: 2022-12-16

Last Modified: 2022-12-16

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.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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 NON-INFRINGEMENT 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.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Overview 1

Audience 1

Overview of Cisco Crosswork Data Gateway 1

CHAPTER 2

Installation Requirements 3

VM Requirements 3

Ports Used 6

Proxy Server Requirements 7

CHAPTER 3

Installation Tasks 9

Install Cisco Crosswork Data Gateway 9

Cisco Crosswork Data Gateway Deployment Parameters and Scenarios 10

Install Crosswork Data Gateway Using vCenter vSphere Client 19

Install Crosswork Data Gateway Via OVF Tool 25

Install Crosswork Data Gateway on OpenStack from OpenStack CLI 27

Install Crosswork Data Gateway on OpenStack from the OpenStack UI 34

Generate Enrollment Package 51

Export Enrollment Package 52

Register Crosswork Data Gateway with Crosswork Cloud Applications 53

Troubleshoot the Crosswork Data Gateway Connectivity 54

CHAPTER 4

Configure Crosswork Data Gateway VM 57

Use the Interactive Console 57

Manage Crosswork Data Gateway Users 58

Supported User Roles 59

Change Password 61

View Current System Settings	61
Change Current System Settings	62
Configure NTP	63
Configure DNS	64
Configure Control Proxy	64
Configure Static Routes	64
Add Static Routes	64
Delete Static Routes	65
Configure Syslog	65
Create New SSH Keys	66
Import Certificate	66
Configure vNIC2 MTU	66
Configure Timezone of the Crosswork Data Gateway VM	67
Configure Password Requirements	68
Configure Simultaneous Login Limits	69
Configure Idle Timeout	70
Configure Remote Auditd Server	70
View Crosswork Data Gateway Vitals	70
Troubleshooting Crosswork Data Gateway VM	73
Run Diagnostic Commands	73
Ping a Host	74
Traceroute to a Host	74
Command Options to Troubleshoot	75
Download tcpdump	75
Run show-tech	76
Shutdown the Crosswork Data Gateway VM	76
Export auditd Logs	76
Remove Rotated Log Files	77
Enable TAC Shell Access	77
Audit TAC Shell Events	78
 CHAPTER 5	
Delete the Virtual Machine	79
Delete VM using vSphere UI	79
Delete Crosswork Data Gateway Service from Cisco CSP	79

Delete VM from OpenStack	80
--------------------------	----



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 Cloud environment. This guide assumes that you are familiar with the following topics:

- Deploying OVF templates using VMware vCenter or OVF Tool.
- Deploying QCOW2 images on Cisco Cloud Services Platform (CSP).
- OpenStack platform.
- Network monitoring and troubleshooting.
- 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 the Cisco 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 Cisco Crosswork Data Gateway for Cloud applications. For details on deploying Crosswork Data Gateway with on-premise applications, refer to the *Cisco Crosswork Infrastructure 4.3 and Applications Installation Guide*.

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

- Cisco Crosswork Trust Insights is a cloud-based SaaS solution that reports on the integrity of devices and provides forensics for assured inventory.
- Cisco Crosswork Cloud Traffic Analysis service is a hosted application that 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.
- Cisco Cloud Services Platform (Cisco CSP).
- OpenStack Platform.

Crosswork Data Gateway Pre-installation Checklist

The pre-installation checklist helps you:

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

Before installing Crosswork Data Gateway, complete the pre-installation checklist.

1. Ensure that the host server meets the resource requirements. See [VM Requirements, on page 3](#)
2. Enable ports that are required for the 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](#).
 - [VM Requirements, on page 3](#)
 - [Ports Used, on page 6](#)
 - [Proxy Server Requirements, on page 7](#)

VM 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.

The resource requirements to install Crosswork Data Gateway are the same for all the data centers, unless stated otherwise.

Table 1: Cisco Crosswork Data Gateway VM Requirements

Requirement	Description
Data Center	<p>VMware</p> <ul style="list-style-type: none"> • VMWare vCenter 7.0, ESXi 7.0 installed on the hosts • VMWare vCenter Server 6.7 (Update 3g or later), ESXi 6.7 Update 1 installed on hosts <p>Cisco CSP</p> <ul style="list-style-type: none"> • Cisco CSP 2.8.0.276 or later <p>Allowed_hardware_list = ['CSP-2100', 'CSP-2100-UCSD', 'CSP-2100-X1', 'CSP-2100-X2', 'CSP-5200', 'CSP-5216', 'CSP-5228', 'CSP-5400', 'CSP-5436', 'CSP-5444', 'CSP-5456']</p> <p>OpenStack</p> <ul style="list-style-type: none"> • OpenStack OSP16
Memory	32 GB
Disk space	74 GB
vCPU	8

Requirement	Description			
Interfaces	Minimum: 1			
	Maximum: 3			
	Crosswork Data Gateway can be deployed with either one, two or three interfaces as per the combinations below:			
	No. of NICs	vNIC0	vNIC1	vNIC2
	1	<ul style="list-style-type: none">• Management Traffic• Control/Data Traffic• Device Access Traffic	—	—
	2	<ul style="list-style-type: none">• Management Traffic	<ul style="list-style-type: none">• Control/Data Traffic• Device Access Traffic	—
3	<ul style="list-style-type: none">• Management Traffic	<ul style="list-style-type: none">• Control/Data Traffic	<ul style="list-style-type: none">• Device Access Traffic	
<ul style="list-style-type: none">• Management traffic: for accessing the Interactive Console and troubleshooting the Crosswork Data Gateway VM.• Control/Data traffic: to receive configuration of collection jobs from the Crosswork Cloud and to forward collected data to the Crosswork Cloud.• Device access traffic: for device management and telemetry data.				
IP Addresses	One, two or three 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 will fail.		
	The Cisco Crosswork Data Gateway host and virtual machine must be synchronized to an NTP server or the enrollment with Crosswork Cloud may not go through.			

Requirement	Description
NTPv4 Authentication	The NTPv4 authentication process that you want to use for a strong cryptographic authentication.
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.
Syslog Server Address	The IPv4 or IPv6 address of a syslog server accessible from the management interface. For more information on how to configure the Syslog Server, see Table 4: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 11 .
Auditd Server Address	The Hostname, IPv4, or IPv6 address of an optional Auditd server. For more information on how to configure the Auditd Server Address, see Table 4: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 11 .

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 2: Ports to be opened for Management Traffic

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

Table 3: Ports to be opened for Control/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 in order to access URLs on the public Internet, you must configure a proxy server in order for the Cisco Crosswork Data Gateway to successfully connect to the Crosswork Cloud service. 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 10.
- From the Interactive Console of the Crosswork Data Gateway after installation. See [Configure Control Proxy](#), on page 64



CHAPTER 3

Installation Tasks

This section contains the following topics:

- [Install Cisco Crosswork Data Gateway, on page 9](#)
- [Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 10](#)
- [Install Crosswork Data Gateway Using vCenter vSphere Client, on page 19](#)
- [Install Crosswork Data Gateway Via OVF Tool, on page 25](#)
- [Install Crosswork Data Gateway on OpenStack from OpenStack CLI, on page 27](#)
- [Install Crosswork Data Gateway on OpenStack from the OpenStack UI, on page 34](#)
- [Generate Enrollment Package, on page 51](#)
- [Export Enrollment Package, on page 52](#)
- [Register Crosswork Data Gateway with Crosswork Cloud Applications, on page 53](#)
- [Troubleshoot the Crosswork Data Gateway Connectivity, on page 54](#)

Install Cisco Crosswork Data Gateway

Cisco Crosswork Data Gateway is initially deployed as a VM called Base VM (containing only enough software to enroll itself with Crosswork Cloud). Once the Crosswork Data Gateway is registered with Crosswork Cloud, Crosswork Cloud pushes the collection job configuration down to the Crosswork Data Gateway, enabling it to gather the data it needs from the network devices.

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

Cisco Crosswork Data Gateway Deployment and Set Up Workflow

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

1. Plan your installation. Refer to the topic [Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 10](#) for information on deployment parameters and possible deployment scenarios.
2. Install Cisco Crosswork Data Gateway on your preferred platform:

VMware	Install Crosswork Data Gateway Using vCenter vSphere Client, on page 19
	Install Crosswork Data Gateway Via OVF Tool, on page 25

OpenStack	Install Crosswork Data Gateway on OpenStack from OpenStack CLI, on page 27 Install Crosswork Data Gateway on OpenStack from the OpenStack UI, on page 34
-----------	---

3. Generate and export Enrollment package.
 - [Generate Enrollment Package, on page 51](#)
 - [Export Enrollment Package, on page 52](#)
4. Enroll Cisco Crosswork Data Gateway with Crosswork Cloud applications. See [Register Crosswork Data Gateway with Crosswork Cloud Applications, on page 53](#).

Cisco Crosswork Data Gateway Deployment Parameters and Scenarios

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

Interface addresses

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

User Accounts

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

- Cisco Crosswork Data Gateway administrator, with the username, **dg-admin** and the password set during installation. The administrator uses this ID to log in and troubleshoot Cisco Crosswork Data Gateway.
- Cisco Crosswork Data Gateway operator, with the username, **dg-oper** and the password set during installation. This is a read-only user and has permissions to perform all 'read' operations and limited 'action' commands.
- A **dg-tac** user account that is used to enable Cisco to assist you in troubleshooting issues with the Crosswork Data Gateway. ([Enable TAC Shell Access, on page 77](#)). 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 59](#).

The **dg-admin** and **dg-oper** user accounts are reserved usernames and cannot be changed. You can change the password from the console for both the accounts. See [Change Password, on page 61](#). In case of lost or forgotten passwords, you have to create a new VM, destroy the current VM, and re-enroll the new VM on Crosswork Cloud.

Installation Parameters and Scenarios

In the following table:

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

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

Table 4: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios

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

Name	Parameter	Description	Additional Information
Active vNICs [*]	ActiveVnics	Number of vNICs to use for sending traffic.	<p>You can choose to use either 1, 2 or 3 interfaces as per your network requirements.</p> <p>For information on how you can route traffic, see <i>Interfaces</i> in the VM Requirements, on page 3 table.</p>
AllowRFC8190 [*]	AllowRFC8190	Automatically allow addresses in an RFC 8190 range. Options are <i>yes</i> , <i>no</i> or <i>ask</i> , where the initial configuration script prompts for confirmation. The default value is <i>yes</i> .	
Private Key URI	DGCertKey	URI to private key file for session key signing. You can retrieve this using SCP (user@host:path/to/file).	<p>Crosswork Cloud uses self-signed certificates for handshake with Cisco Crosswork Data Gateway. These certificates are generated at installation.</p> <p>However, if you want to use third-party or your own certificate files enter these three parameters.</p> <p>Certificate chains override any preset or generated certificates in the Cisco Crosswork Data Gateway VM and are given as an SCP URI (user:host:/path/to/file).</p> <p>Note The host with the URI files must be reachable on the network (from the vNIC0 interface via SCP) and files must be present at the time of install.</p>
Certificate File URI	DGCertChain	URI to PEM formatted signing certificate chain for this VM. You can retrieve this using SCP (user@host:path/to/file).	
Certificate File and Key Passphrase	DGCertChainPwd	SCP user passphrase to retrieve the Cisco Crosswork Data Gateway PEM formatted certificate file and private key.	

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

Name	Parameter	Description	Additional Information
vNIC IPv4 Method*	Vnic0IPv4Method Vnic1IPv4Method Vnic2IPv4Method	None or Static or DHCP. The default value for Method is None .	<p>If you have selected Method as:</p> <ul style="list-style-type: none">• None: Skip the rest of the fields for IPv4 address. Enter information in the vNIC IPv6 Address parameters.• Static: Enter information in Address, Netmask, Skip Gateway, and Gateway fields• DHCP: Leave all the Vnic IPv4 Address parameters to their default values. These values are assigned automatically.
vNIC IPv4 Address	Vnic0IPv4Address Vnic0IPv4Address Vnic0IPv4Address	IPv4 address of the interface.	
vNIC IPv4 Netmask	Vnic0IPv4Netmask Vnic0IPv4Netmask Vnic0IPv4Netmask	IPv4 netmask of the interface in dotted quad format.	
vNIC IPv4 Skip Gateway	Vnic0IPv4SkipGateway Vnic1IPv4SkipGateway Vnic2IPv4SkipGateway	Options are True or False . The default value is False . Selecting True skips configuring a gateway for the interface.	
vNIC IPv4 Gateway	Vnic0IPv4Gateway Vnic1IPv4Gateway Vnic2IPv4Gateway	IPv4 address of the interface gateway.	
vNIC IPv6 Address (vNIC0, vNIC1, and vNIC2 based on the number of interfaces you choose to use)			

Name	Parameter	Description	Additional Information
vNIC IPv6 Method [*]	Vnic0IPv6Method Vnic1IPv6Method Vnic2IPv6Method	None or Static or DHCP . The default value for Method is None .	<p>If you have selected Method as:</p> <ul style="list-style-type: none">• None: Skip the rest of the fields for IPv6 address. Enter information in the vNIC IPv4 Address parameters.• Static: Enter information in Address, Netmask, Skip Gateway, and Gateway fields• DHCP: Leave all the Vnicx IPv6 Address parameters as is to their default values. These value are assigned automatically.
vNIC IPv6 Address	Vnic0IPv6Address Vnic1IPv6Address Vnic2IPv6Address	IPv6 address of the interface.	
vNIC IPv6 Netmask	Vnic0IPv6Netmask Vnic1IPv6Netmask Vnic2IPv6Netmask	IPv6 prefix of the interface.	
vNIC IPv6 Skip Gateway	Vnic0IPv6SkipGateway Vnic1IPv6SkipGateway Vnic2IPv6SkipGateway	Options are <code>True</code> or <code>False</code> . The default value is <code>False</code> . Selecting <code>True</code> skips configuring a gateway for the interface.	
vNIC IPv6 Gateway	Vnic0IPv6Gateway Vnic1IPv6Gateway Vnic2IPv6Gateway	IPv6 address of the interface gateway.	
DNS Servers			
DNS Address [*]	DNS	Space-delimited list of IPv4 or IPv6 addresses of the DNS server accessible from the management interface.	
DNS Search Domain [*]	Domain	DNS search domain	
DNS Security Extensions [*]	DNSSEC	Options are <code>False</code> , <code>True</code> , <code>Allow-Downgrade</code> . Select <code>True</code> to use DNS security extensions. By default, this parameter is <code>False</code> .	
DNS over TLS [*]	DNSTLS	Options are <code>False</code> , <code>True</code> , and <code>Opportunistic</code> . Select <code>True</code> to use DNS over TLS. By default, this parameter is <code>False</code> .	

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

Name	Parameter	Description	Additional Information
Use Remote Syslog Server [*]	UseRemoteSyslog	Select Yes to send syslog messages to a remote host. The default value is No.	<p>Configuring an external syslog server sends service events to the external syslog server. Otherwise, they are logged only to the Cisco Crosswork Data Gateway VM.</p> <p>If you want to use an external syslog server, you must specify the following settings:</p> <ul style="list-style-type: none">• Use Remote Syslog Server• Syslog Server Address• Syslog Server Port• Syslog Server Protocol <p>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.</p>
Syslog Server Address	SyslogAddress	IPv4 or IPv6 address of a syslog server accessible from the management interface. Note If you are using an IPv6 address, surround it with square brackets ([1::1]).	
Syslog Server Port	SyslogPort	Port number of the optional syslog server. The port value can range between 1 and 65535. By default, this value is set to 514.	
Syslog Server Protocol	SyslogProtocol	Use UDP or TCP when sending syslog. Default value is UDP.	
Use Syslog over TLS?	SyslogTLS	Select Yes to use TLS to encrypt syslog traffic. By default, this parameter is set to No.	
Syslog TLS Peer Name	SyslogPeerName	The syslog server hostname exactly as entered in the server certificate SubjectAltName or subject common name.	
Syslog Root Certificate File URI	SyslogCertChain	URI to the PEM formatted root cert of syslog server retrieved using SCP.	
Syslog Certificate File Passphrase	SyslogCertChainPwd	Password of SCP user to retrieve Syslog certificate chain.	
Remote Auditd Server			

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

Name	Parameter	Description	Additional Information
Enrollment Destination Host and Path**	EnrollmentURI	SCP host and path to transfer the enrollment package using SCP (user@host:/path/to/file).	Cisco Crosswork Data Gateway requires the Enrollment package to enroll with Crosswork Cloud. If you specify these parameters during the installation, the enrollment package is automatically transferred to the local host once Cisco Crosswork Data Gateway boots up for the first time. If you do not specify these parameters during installation, then export enrollment package manually by following the procedure Export Enrollment Package , on page 52.
Enrollment Passphrase**	EnrollmentPassphrase	SCP user passphrase to transfer enrollment package.	

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

Install Crosswork Data Gateway Using vCenter vSphere Client

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

- Step 1** Refer to the *Crosswork Data Gateway 4.0.1 Release notes* and download the Crosswork Data Gateway image (*.ova) file.
- Note** When using the latest Mozilla Firefox version to download the .ova image, if the downloaded file has the extension as .dms, change the extension back to .ova before installation.
- Step 2** Connect to vCenter and login with your credentials.
- Step 3** Select the data center where you want to deploy the Crosswork Data Gateway VM.
- Step 4** Connect to vCenter vSphere Client. Then select **Actions > Deploy OVF Template**.
- Warning** The default VMware vCenter deployment timeout is 15 minutes. If the time taken to complete the OVF template deployment exceeds 15 minutes, vCenter times out and you will have to start over again. To prevent this, we recommend that you plan what you will enter by reviewing the template before you start the deployment.
- Connect to vCenter and login with your credentials
- Step 5** The VMware **Deploy OVF Template** wizard appears and highlights the first step, **1 Select template**.

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

The filename is displayed in the window.

Step 6

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

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

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

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

Deploy OVF Template

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

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

Virtual machine name:

Select a location for the virtual machine.

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

CANCEL
BACK
NEXT

Step 7

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

Step 8

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

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

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

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

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

Deploy OVF Template

<ul style="list-style-type: none"> ✓ 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 	<p>Configuration Select a deployment configuration</p> <table border="1"> <thead> <tr> <th></th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="radio"/> Crosswork Cloud</td> <td>8 CPU; 32GB RAM; 1-3 NICs; 74GB Disk</td> </tr> <tr> <td><input type="radio"/> Crosswork On-Premise Standard</td> <td></td> </tr> <tr> <td><input type="radio"/> Crosswork On-Premise Extended</td> <td></td> </tr> <tr> <td><input type="radio"/> Crosswork On-Premise Standard With Extra Resources</td> <td></td> </tr> </tbody> </table> <p style="text-align: right;">4 Items</p>		Description	<input checked="" type="radio"/> Crosswork Cloud	8 CPU; 32GB RAM; 1-3 NICs; 74GB Disk	<input type="radio"/> Crosswork On-Premise Standard		<input type="radio"/> Crosswork On-Premise Extended		<input type="radio"/> Crosswork On-Premise Standard With Extra Resources	
	Description										
<input checked="" type="radio"/> Crosswork Cloud	8 CPU; 32GB RAM; 1-3 NICs; 74GB Disk										
<input type="radio"/> Crosswork On-Premise Standard											
<input type="radio"/> Crosswork On-Premise Extended											
<input type="radio"/> Crosswork On-Premise Standard With Extra Resources											

[CANCEL](#)
[BACK](#)
[NEXT](#)

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

- a) In the **Select virtual disk format** field,
 - For production environment, choose **Thick Provision Lazy Zeroed**.
 - For development environment, choose **Thin Provision**.
- b) From the **Datastores** table, choose the datastore you want to use.

Deploy OVF Template

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

Select storage
Select the storage for the configuration and disk files

☐ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thick Provision Lazy Zeroed ▾

VM Storage Policy: Datastore Default ▾

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

Compatibility

✓ Compatibility checks succeeded.

CANCEL
BACK
NEXT

Step 12

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

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

Note In the following image,

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

Deploy OVF Template

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

Select networks

Select a destination network for each source network.

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

3 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL

BACK

NEXT

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

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

Enter the information for the parameters as described in [Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 10](#).

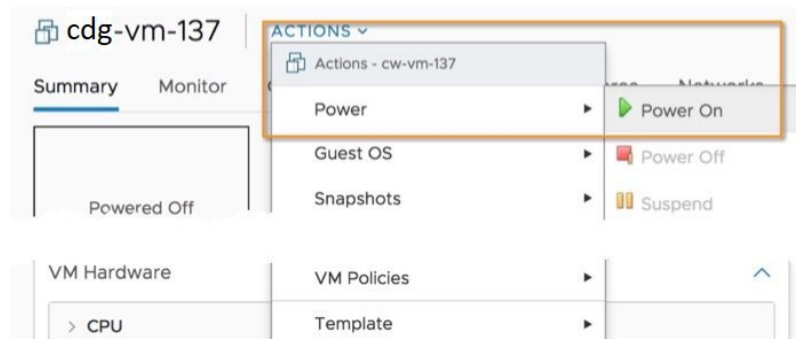
Note When this menu is first displayed, there will be an error "7 properties have invalid values". This is normal and will clear as you enter appropriate values.

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

Step 15 Check deployment status.

- a) Open the vCenter vSphere client.
- b) In the **Recent Tasks** tab for the host VM, view the status for the **Deploy OVF template** and **Import OVF package** jobs.

Step 16 After the deployment status becomes 100%, power on the VM to complete the deployment process. Expand the host's entry so you can click the VM and then choose **Actions > Power > Power On**, as shown in the following figure:



Wait for at least five minutes for the VM to come up and then login through vCenter or SSH.

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

Verify that the installation was successful.

1. Login to Crosswork Data Gateway VM Via vCenter:

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

2. Access Crosswork Data Gateway VM Via SSH:

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

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

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

For example,

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

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



Note The SSH process is protected from brute force attacks by blocking the client IP after a number of login failures. Failures such as incorrect username or password, connection disconnect, or algorithm mismatch are counted against the IP. Up to 4 failures within a 20 minute window will cause the client IP to be blocked for at least 7 minutes. Continuing to accumulate failures will cause the blocked time to be increased. Each client IP is tracked separately.

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

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

What to do next

Proceed to enrolling the Crosswork Data Gateway with Crosswork Cloud by generating and exporting the enrollment package. See [Export Enrollment Package, on page 52](#).

Install Crosswork Data Gateway Via OVF Tool

You can modify mandatory/optional parameters in the command/script as per your requirement and run the OVF Tool. See [Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 10](#).

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

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

# robot.ova path

DG_OVA_PATH="<mention the orchestrator path>"

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

ActiveVnics="2"

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

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

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

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

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

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

SyslogAddress="<syslog_server_address>"
SyslogPort=<syslog_server_port>
SyslogProtocol="<syslog_server_protocol>"
SyslogTLS=False
```

```

SyslogPeerName="<syslog_server_peer_name>"
SyslogCertChain="<syslog_server_root_certificate>"
SyslogCertChainPwd="<password>"

# Please replace this information according to your vcenter setup
VCENTER_LOGIN="<vCenter login details>"
VCENTER_PATH="<vCenter path>"
DS="<DS details>"

ovftool --acceptAllEulas --X:injectOvfEnv --skipManifestCheck --overwrite --noSSLVerify
--powerOffTarget --powerOn \
--datastore="$DS" --diskMode="$DM" \
--name=$VM_NAME \
--net:"vNIC0=VM Network" \
--net:"vNIC1=DPortGroupVC-1" \
--deploymentOption=$Deployment \
--prop:"EnrollmentURI=$EnrollmentURI" \
--prop:"EnrollmentPassphrase=$EnrollmentPassphrase" \
--prop:"Hostname=$Hostname" \
--prop:"Description=$Description" \
--prop:"Label=$Label" \
--prop:"ActiveVnics=$ActiveVnics" \
--prop:"Vnic0IPv4Address=$Vnic0IPv4Address" \
--prop:"Vnic0IPv4Gateway=$Vnic0IPv4Gateway" \
--prop:"Vnic0IPv4Netmask=$Vnic0IPv4Netmask" \
--prop:"Vnic0IPv4Method=$Vnic0IPv4Method" \
--prop:"Vnic1IPv4Address=$Vnic1IPv4Address" \
--prop:"Vnic1IPv4Gateway=$Vnic1IPv4Gateway" \
--prop:"Vnic1IPv4Netmask=$Vnic1IPv4Netmask" \
--prop:"Vnic1IPv4Method=$Vnic1IPv4Method" \
--prop:"DNS=$DNS" \
--prop:"NTP=$NTP" \
--prop:"dg-adminPassword=$dg_adminPassword" \
--prop:"dg-operPassword=$dg_operPassword" \
--prop:"Domain=$Domain" $DG_OVA_PATH "vi://$VCENTER_LOGIN/$VCENTER_PATH"

```

-
- Step 1** Open a command prompt on the machine you will running the install from.
- Step 2** Open the template file and edit it to match the settings you chose for the Cisco Crosswork Data Gateway.
- Step 3** Navigate to the location where you installed the OVF Tool.
- Step 4** Run the OVF Tool using the script.

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

For example,

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

Verify that the installation was successful.

1. Login to Crosswork Data Gateway VM Via vCenter:

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

2. Access Crosswork Data Gateway VM Via SSH:

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

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

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

For example,

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

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

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



Note The SSH process is protected from brute force attacks by blocking the client IP after a number of login failures. Failures such as incorrect username or password, connection disconnect, or algorithm mismatch are counted against the IP. Up to 4 failures within a 20 minute window will cause the client IP to be blocked for at least 7 minutes. Continuing to accumulate failures will cause the blocked time to be increased. Each client IP is tracked separately.

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

What to do next

Proceed to enrolling the Crosswork Data Gateway with Crosswork Cloud. See [Export Enrollment Package, on page 52](#).

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 10](#).

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

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

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

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

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

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

- 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
```

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

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

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

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

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

- Navigate to the directory where you have downloaded the Crosswork Data Gateway release image.
- Open the `config.txt` file and modify the parameters as per your installation requirements. Refer to the section [Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 10](#) for more information.

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

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

```

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

```

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

- c) Save the `config.txt` file with the hostname of the VM or a name that makes it easy for you to identify the VM for which you have updated it.
- d) **(Important)** Make a note of the IP address that you enter here for the vNIC IP addresses in the `config.txt`. You will need to specify the same IP addresses when creating the ports for the VM in Step 9.
- e) Repeat **Step 3 (b)** and **Step 3 (d)** to update and save a unique `config.txt` file for each VM using static addressing.
- f) Proceed to **Step 5**.

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

- a) Navigate to the directory where you have downloaded the Crosswork Data Gateway release image.
- b) Open the `config.txt` file and modify the parameters as per your installation requirements. Refer to the section [Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 10](#) for more information.

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

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

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

```

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

```

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

- d) Repeat **Step 4 (b)** and **Step 4 (c)** to update and save a unique config.txt file for each VM using DHCP addressing.
- e) Proceed to **Step 5**.

Step 5 Log in to the OpenStack VM from CLI.

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

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

Step 7 Create image for OpenStack install.

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

For example:

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

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

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

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

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

Sample commands:

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

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

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

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

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

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

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

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

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

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

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

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

For example,

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

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

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

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

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

For example:

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

OR

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

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

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

For example:

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

OR

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

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

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

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

Verify that the Crosswork Data Gateway VMs were installed successfully.

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

```
openstack server list
```

```
(osp16VTS) [stack@spid16-director cdg-image]$ openstack server list
```

ID	Name	Status	Networks	Image	Flavor
8b039d3c-1bb9-4ce2-9b24-1654216c4dd6	cdg-bios-nodhcp_2NIC	ACTIVE	network1-nodhcp=10.0.0.1; network3-nodhcp=10.0.0.1	cdg-cloud-bios-345	cdg-cloud
9cd913f-c24b-43a3-9816-f865e58e7e95	cdg-bios-nodhcp	ACTIVE	network1-nodhcp=10.0.0.1; network2-nodhcp=10.0.0.1; network3-nodhcp=10.0.0.1	cdg-cloud-bios-345	cdg-cloud

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

From OpenStack CLI

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

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

For example:

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

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

From OpenStack UI

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

What to do next

Proceed to adding the Crosswork Data Gateway with Crosswork Cloud. See [Export Enrollment Package, on page 52](#).

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 10](#).
- Decide the addressing method that you will use (DHCP or Static) for the VM(s).
- Have network information such as IP addresses, subnets and ports ready for each VM if you are using Static addressing.
- Understand security group rules and security policies before you create security groups to apply to the VM.

Step 1

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

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

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

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

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

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

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

- 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
```

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

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

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

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

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

- Navigate to the directory where you have downloaded the Crosswork Data Gateway release image.
- Open the `config.txt` file and modify the parameters as per your installation requirements. Refer to the section [Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 10](#) for more information.

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

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

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

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

```

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

```

- c) Save the `config.txt` file with the hostname of the VM or a name that makes it easy for you to identify the VM for which you have updated it.
- d) **(Important)** Make a note of the IP address that you enter here for the vNIC IP addresses in the `config.txt`. You will need to specify the same IP addresses when creating the ports for the VM in Step 9.
- e) Repeat **Step 3 (b)** and **Step 3 (d)** to update and save a unique `config.txt` file for each VM using static addressing.
- f) Proceed to **Step 5**.

Step 4

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

- a) Navigate to the directory where you have downloaded the Crosswork Data Gateway release image.
- b) Open the `config.txt` file and modify the parameters as per your installation requirements. Refer to the section [Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 10](#) for more information.

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

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

```

ActiveVnics=3
AllowRFC8190=Yes
AuditdAddress=
AuditdPort=60
ControllerCertChainPwd=

```

```

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

```

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

- c) Save the `config.txt` file with the hostname of the VM or a name that makes it easy for you to identify the VM for which you have updated it.
- d) Repeat **Step 4 (b)** and **Step 4 (c)** to update and save a unique `config.txt` file for each VM using static addressing.
- e) Proceed to **Step 5**.

Step 5

Log in to the OpenStack VM from the OpenStack UI.

Step 6

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

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

Flavor Information **Flavor Access**

Name ^{*}
cdg-cloud-flavor

ID [?]
auto

VCPUs ^{*}
8

RAM (MB) ^{*}
32768

Root Disk (GB) ^{*}
50

Ephemeral Disk (GB)
10

Swap Disk (MB)
0

RX/TX Factor
1

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

Cancel Create Flavor

Step 7

Create an image for OpenStack install.

- a) Enter details in the following fields:
 1. **Image Name** - Specify a name for the image you are creating.

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

b) Click **Create Image**.

Create Image

Image Details
Specify an image to upload to the Image Service.

Image Name
cdg_bios_image

Image Description

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

Format*
QCOW2 - QEMU Emulator

Image Requirements

Kernel
Choose an image

Ramdisk
Choose an image

Architecture

Minimum Disk (GB)
0

Minimum RAM (MB)
0

Image Sharing

Visibility
Private Shared **Public** Community

Protected
Yes No

✕ Cancel < Back Next > ✓ Create Image

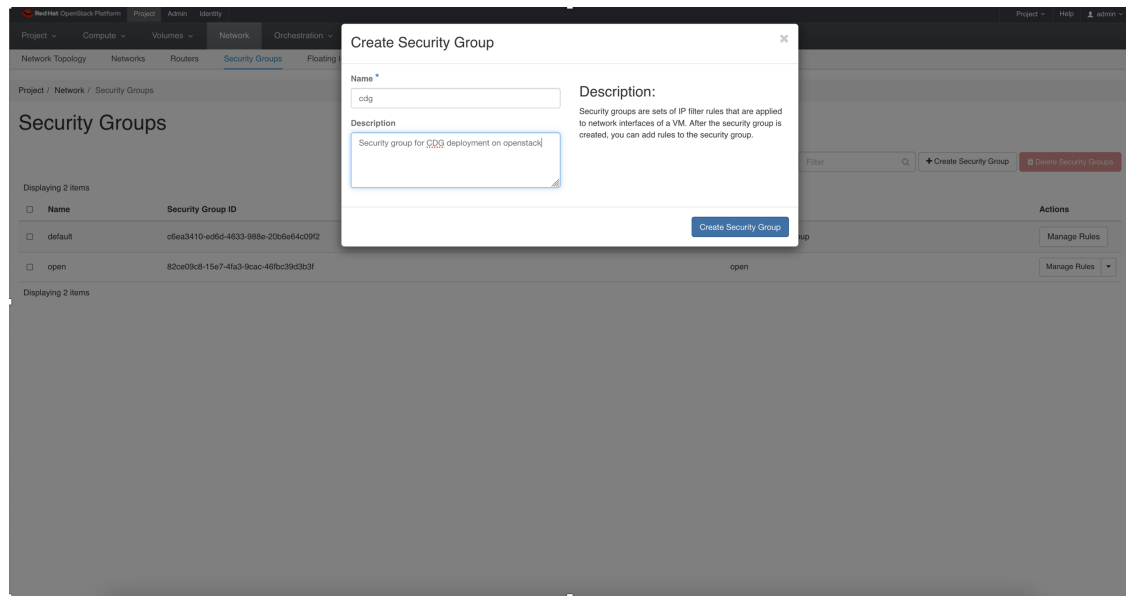
Step 8

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

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

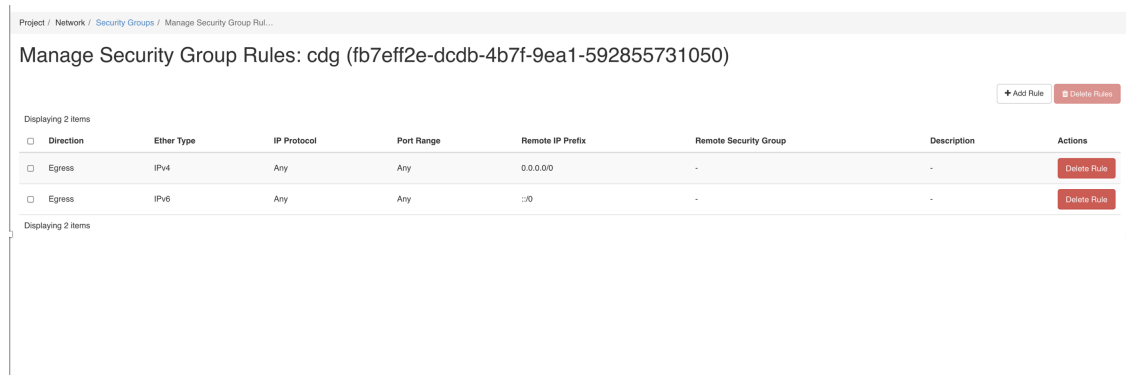
Note You can create security groups and apply them to the VM even after the Crosswork Data Gateway is deployed.

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



- c) Specify the **Name** and **Description** of the security group. Click **Create Security Group**.
- d) In the new window that appears to create security rules, click **Add Rule** to create a security policy for each protocol by specifying the direction, port range and the IP addresses range.

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



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

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

- a) In the OpenStack UI, navigate to **Network > Networks**.
- b) Depending on the number of NICs in your deployment, (starting with the management network), select a network and click **+ Create Ports**.
- c) Enter details in the **Name** and **Fixed IP Address** fields. Select the **Enable Admin State** and **Port Security** check box.

Create Port

Info Security Groups

Name

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

☒ **Enable Admin State** ⓘ

Device ID ⓘ

Device Owner ⓘ

Specify IP address or subnet ⓘ

Fixed IP Address* ⓘ

MAC Address ⓘ

☒ **Port Security** ⓘ

VNIC Type ⓘ

Binding: Host ⓘ

Cancel **Create**

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

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

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

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

Launch Instance

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

Project Name
admin

Instance Name
test_instance

Description

Availability Zone
nova

Count
1


Total Instances (100 Max)
3%

2 Current Usage
1 Added
97 Remaining

Launch Instance

Step 12

In the **Source** tab:

- Select Boot Source** - Select **Image** from the drop down list.
- Create New Volume** - Select **No**.
- 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.
- Click **Next**.

Launch Instance

Details

Source

Flavor

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

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

Select Boot Source

Image

Create New Volume

Yes

No

Allocated

Displaying 1 item

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

Available 1

Select one

Q

Click here for filters or full text search.

×

Displaying 1 item

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

Displaying 1 item


✕ Cancel

< Back

Next >

Launch Instance

Step 13

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

Launch Instance ✕ ?

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

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

Allocated

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

Available 0 Select one


Click here for filters or full text search.
✕

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

✕ Cancel
< Back
Next >
Launch Instance

Step 14

Assign networks to the VM. Depending on the number of vNICs in your deployment, select up to 3 networks for the

VM by clicking  for each network from the list of networks in the **Available** pane. Doing this will move the selected networks to the **Allocated** pane. Click **Next**.

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

Launch Instance

Details •

Source

Flavor •

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Networks provide the communication channels for instances in the cloud.

Allocated 3 Select networks from those listed below.

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


Available 3 Select at least one network

Click here for filters or full text search.

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

Cancel < Back Next > Launch Instance

Step 15 Assign ports to the VM.

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

Launch Instance

Details

Source

Flavor

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

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

▼ Allocated 1

Select ports from those listed below.

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

▼ Available 2

Select one

Q

Filter

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

✕ Cancel

< Back

Next >

Launch Instance

Click **Next**.

Step 16

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

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

Launch Instance

Details

Source

Flavor

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Select the security groups to launch the instance in.

Allocated 2

Name	Description
default	Default security group
cdg	Security group for CDG deployment on openstack

Available 1

Select one or more

Click here for filters or full text search.

Name	Description
open	open

Cancel

Back

Next

Launch Instance

Click **Next**.

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

Step 18 In the **Configuration** tab:

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

Launch Instance ✕

?

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

Source Load Customization Script from a file
 No file chosen

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

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Disk Partition
 Automatic

☒ Configuration Drive

Step 19 Click **Launch Instance**.

OpenStack begins installation of the VM.

Step 20 Repeat **Step 9** to **Step 20** of the procedure to install all Crosswork Data Gateway VMs.**Verify that the Crosswork Data Gateway VMs were installed successfully.**

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

Project / Compute / Instances

Instances

Displaying 2 items

<input type="checkbox"/>	Instance Name	Image Name	IP Address	Flavor
<input type="checkbox"/>	cdg-bios-dhcp	cdg-cloud-bios-6	network2 network3 network1	Not available

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

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

Project / Compute / Instances

Instances

Displaying 2 items

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

- After the Status changes to **Active**, wait for about 10 minutes.
Click the Crosswork Data Gateway VM name. The link to the VM console opens.

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

What to do next

Proceed to enrolling the Crosswork Data Gateway with Crosswork Cloud by generating and exporting the enrollment package. See [Export Enrollment Package, on page 52](#).

Generate Enrollment Package

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

- By supplying **Auto Enrollment Package** parameters during installation process (see Auto Enrollment Package under [Table 4: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios](#)).
- By using the **Export Enrollment Package** option from the Interactive Console (see [Export Enrollment Package, on page 52](#))

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

If you opted not to export the enrollment package during install, then you must export it before you can enroll the Crosswork Data Gateway with Crosswork Cloud. The steps to do so are described in [Export Enrollment Package, on page 52](#).



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

A sample enrollment package JSON is shown below:

```
{
  "name": "dg116.cisco.com",
  "description": "CDG Base VM for Automation",
  "profile": {
    "cpu": 8,
    "memory": 31,
    "nics": 3
  },
  "interfaces": [
    {
      "name": "eth0",
      "mac": "00:50:56:9e:09:7a",
      "ipv4Address": "<ip_address>/24"
    },
    {
      "name": "eth1",
      "mac": "00:50:56:9e:67:c3",
      "ipv4Address": "<ip_address>/16"
    }
  ]
}
```

```

        "name": "eth2",
        "mac": "00:50:56:9e:83:83",
        "ipv4Address": "<ip_address>/16"
    },
    ],
    "certChain": [
        "<cert_chain>"
    ],
    ],
    "version": "1.1.0 (branch dgl10dev - build number 152)",
    "duid": "d58fe482-fdca-468b-a7ad-dfbfa916e58b"
}

```

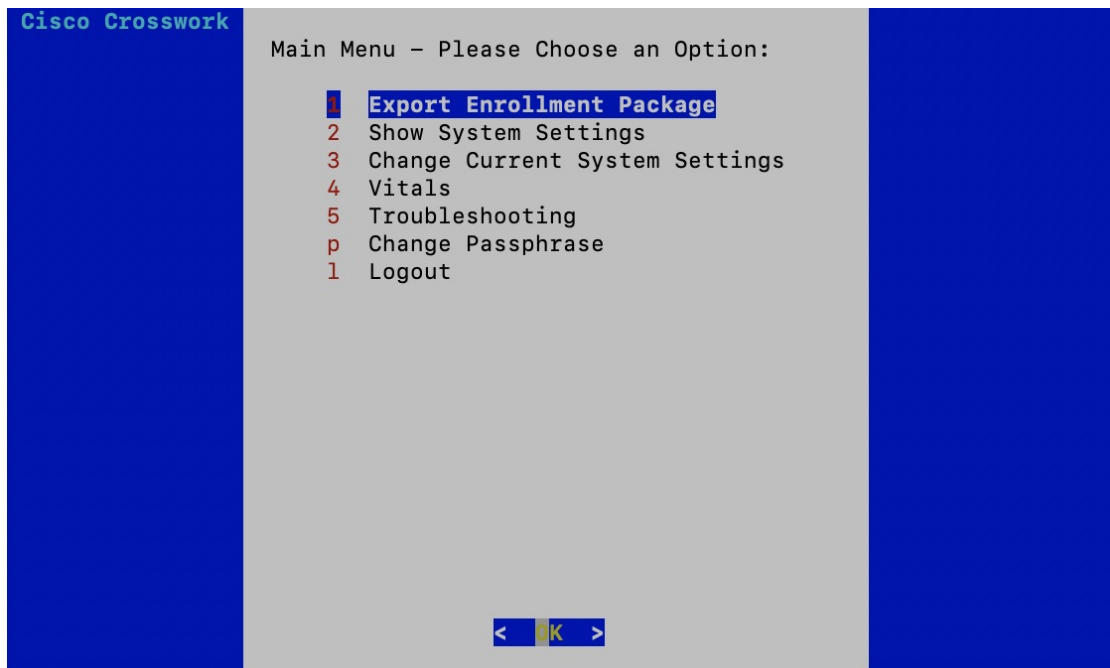
Export Enrollment Package

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



Note This is needed only if you have not specified **Auto Enrollment Package Transfer** settings during installation. Otherwise, the file will be copied to the SCP URI destination you selected after the VM boots. Proceed to [Register Crosswork Data Gateway with Crosswork Cloud Applications, on page 53](#) if you had already specified the **Auto Enrollment Package Transfer** settings during installation.

- Step 1** Log in to the Cisco Crosswork Data Gateway.
- Step 2** From the Main Menu, select **1 Export Enrollment Package** and click **OK**.



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

Note

- The host must run an SCP server. Ideally, you should export the enrollment package to the local computer you will use to access the Crosswork server.
- If you are not using the default port 22, you can specify the port as a part of the SCP command. For example, to export the enrollment package as an admin user, placing the file in that user's home directory with port 4000, you can give the following command:

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

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

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

Step 5 If you could not copy the enrollment package directly to your local computer, manually copy the enrollment package from the SCP server to your local computer.

What to do next

Proceed with enrolling the Cisco Crosswork Data Gateway with Crosswork Cloud as explained in [Register Crosswork Data Gateway with Crosswork Cloud Applications, on page 53](#).

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 54](#) 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 5: 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.	<ol style="list-style-type: none"> 1. Log into the Crosswork Data Gateway VM. 2. From the main menu, go to 5 Troubleshooting > Run show-tech. Enter the destination to save the tarball containing logs and vitals and click OK. In the show-tech logs (in file <code>session.log</code> at location <code>/cdg/logs/components/controller-gateway/session.log</code>), if you see the error <pre>UNAUTHENTICATED:invalid certificate. reason: x509: certificate has expired or is not yet valid</pre> , then there is a clock-drift between Crosswork Data Gateway and Cisco Crosswork Cloud. 3. From the main menu, go to 3 Change Current System Settings > 1 Configure NTP. Configure NTP to sync with the clock time on the Cisco Crosswork Cloud server and try enrolling the Crosswork Data Gateway with Crosswork Cloud again.

Issue	Action
Crosswork Data Gateway does not have direct connectivity to external web services.	<ol style="list-style-type: none"><li data-bbox="958 289 1521 357">1. Configure a proxy server if a proxy server is missing in your environment.<li data-bbox="958 367 1521 434">2. If a proxy server is already present in your environment, check if the proxy URL is correct.<li data-bbox="958 445 1521 512">3. Check if the credentials of the proxy (certificate, proxy name etc) are correct. <p data-bbox="958 543 1521 646">To update the proxy server details on the Crosswork Data Gateway, see Configure Control Proxy, on page 64.</p>



CHAPTER 4

Configure Crosswork Data Gateway VM

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

This chapter contains the following topics:

- [Use the Interactive Console, on page 57](#)
- [Manage Crosswork Data Gateway Users, on page 58](#)
- [View Current System Settings, on page 61](#)
- [Change Current System Settings, on page 62](#)
- [View Crosswork Data Gateway Vitals, on page 70](#)
- [Troubleshooting Crosswork Data Gateway VM, on page 73](#)

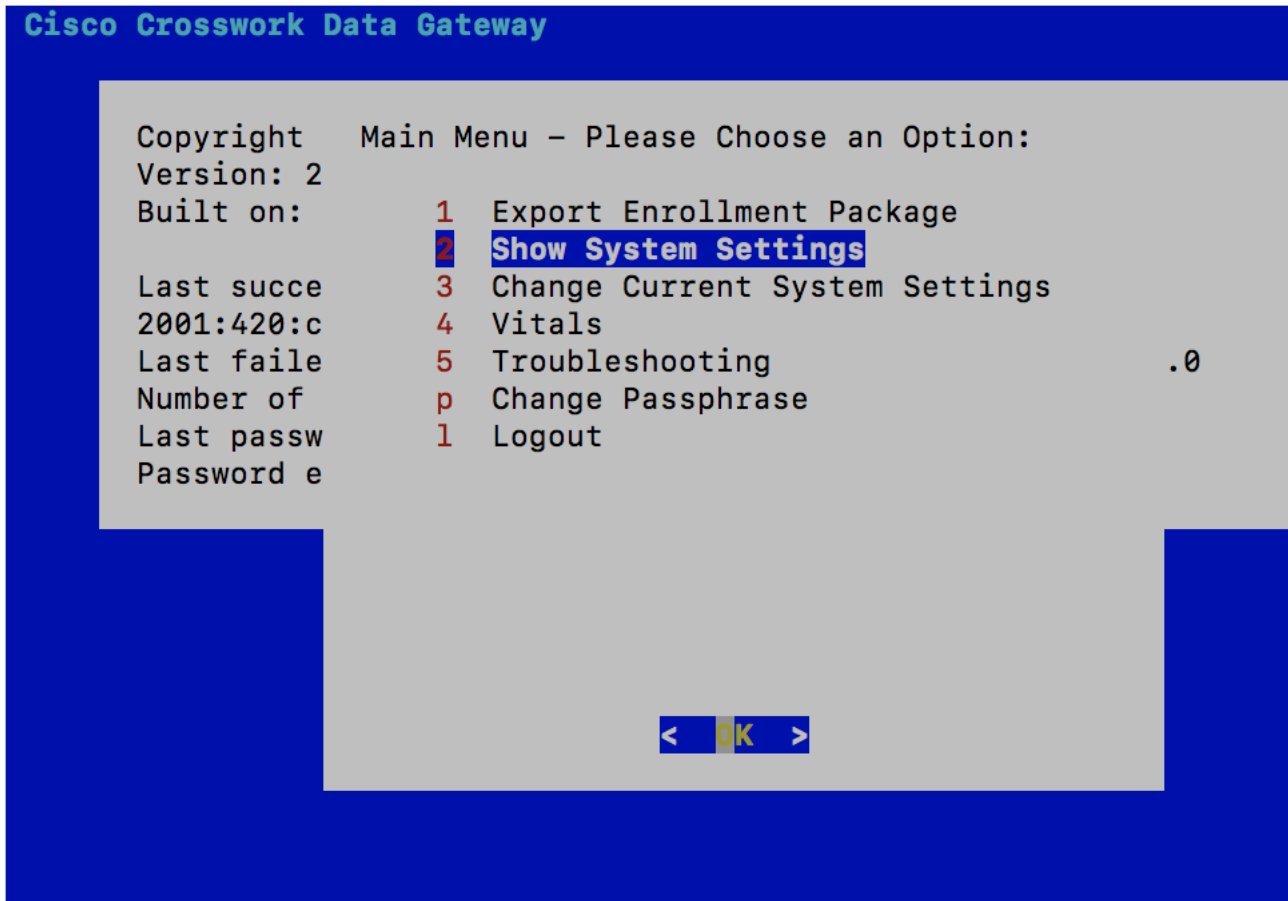
Use the Interactive Console

Cisco Crosswork Data Gateway launches an interactive console upon successful login. The interactive console displays the **Main Menu** as shown in the following figure:



Note

The Main Menu shown here corresponds to **dg-admin** user. It is different for **dg-oper** user as the operator does not have same privileges as the administrator. See Table [Table 6: Permissions Per Role, on page 59](#).



The Main Menu presents the following options:

1. Export Enrollment Package
2. Show System Settings
3. Change Current System Settings
4. Vitals
5. Troubleshooting
- p. Change Passphrase
- l. Logout

Manage Crosswork Data Gateway Users

This section contains the following topics:

- [Supported User Roles](#), on page 59
- [Change Password](#), on page 61

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 6: Permissions Per Role

Permissions	Administrator	Operator
Export Enrollment Package	✓	✓
Show system settings		
vNIC Addresses	✓	✓
NTP		
DNS		
Proxy		
UUID		
Syslog		
Certificates		
First Boot Provisioning Log		
Timezone		
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 vNIC2 MTU Configure Timezone Configure Password Requirements Configure Simultaneous Login Limits Configure Idle Timeout	✓	×
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		
Run Diagnostic Commands	✓	✓
Run show-tech	✓	✓
Export auditd logs	✓	✓
Enable TAC Shell Access	✓	×
Change Passphrase	✓	✓

Change Password

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 **p Change Passphrase** and click **OK**.
 - Step 2** Input 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:

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
-  Exit Menu

< OK >

Follow these steps to view the current system settings:

-
- Step 1** From the Main Menu, select **2 Show System Settings**, as shown in the following figure:
 - Step 2** Click **OK**. The **Show Current System Settings** menu opens.

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.
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: <ul style="list-style-type: none"> • 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.

Change Current System Settings

Crosswork Data Gateway allows you to configure the following settings:

- NTP.
- DNS.
- Control proxy.
- Static routes.
- Syslog.
- SSH keys.
- Certificate.
- vNIC2 MTU.

- Timezone.
- Password requirements.
- Simlutaneous login limits.
- Idle timeout.
- Configure auditd.

**Note**

- Crosswork Data Gateway system settings can only be configured by the administrator.
- In 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 76](#). 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 70](#). 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 **1 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 **2 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 **3 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.



Note 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



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

Follow the steps to configure Syslog:

- Step 1** From the **Change Current System Settings** Menu, select **5 Configure Syslog**.
- Step 2** Enter the new values for the following syslog attributes:
- Server address: IPv4 or IPv6 address of a syslog server accessible from the management interface. If you are using an IPv6 address, it must be surrounded by square brackets ([1::1]).
 - Port: Port number of the syslog server
 - Protocol: Use UDP, TCP, or RELP when sending syslog.
 - Use Syslog over TLS?: Use TLS to encrypt syslog traffic.
 - TLS Peer Name: Syslog server's hostname exactly as entered in the server certificate SubjectAltName or subject common name.
 - Syslog Root Certificate File URI: PEM formatted root cert of syslog server retrieved using SCP.
 - Syslog Certificate File Passphrase: Password of SCP user to retrieve Syslog certificate chain.
- Step 3** 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 **7 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 **8 Configure vNIC1 MTU**.
- Step 2** Enter vNIC2 MTU value.
- Step 3** Click **OK** to save the settings.
-

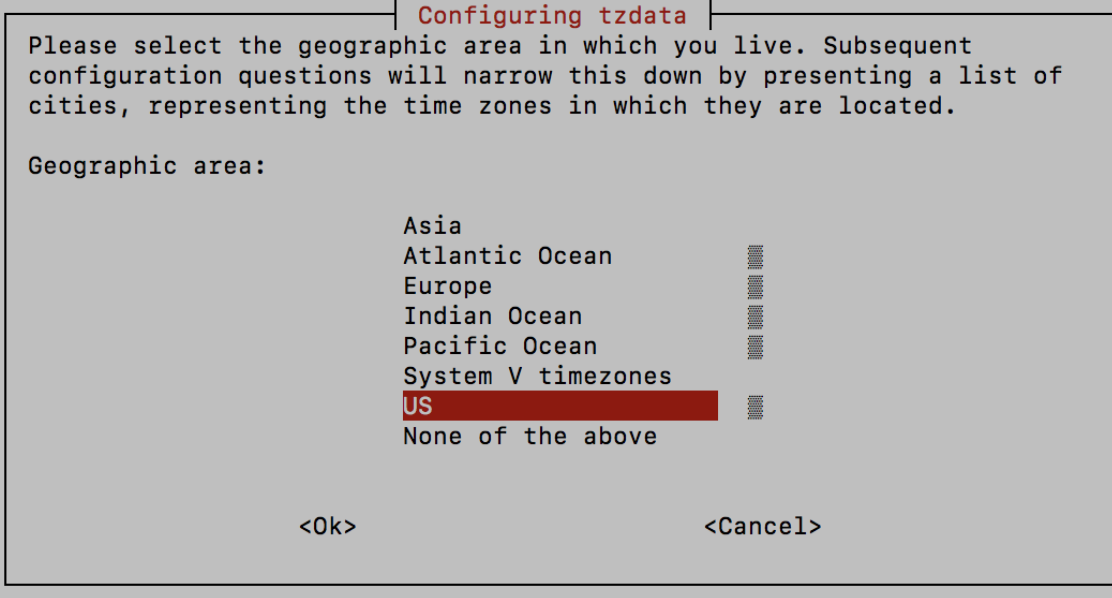
Configure Timezone of the Crosswork Data Gateway VM

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 In Crosswork Data Gateway VM interactive menu, select **Change Current System Settings**.

Step 2 Select **9 Timezone**.

Step 3 Select the geographic area in which you live.



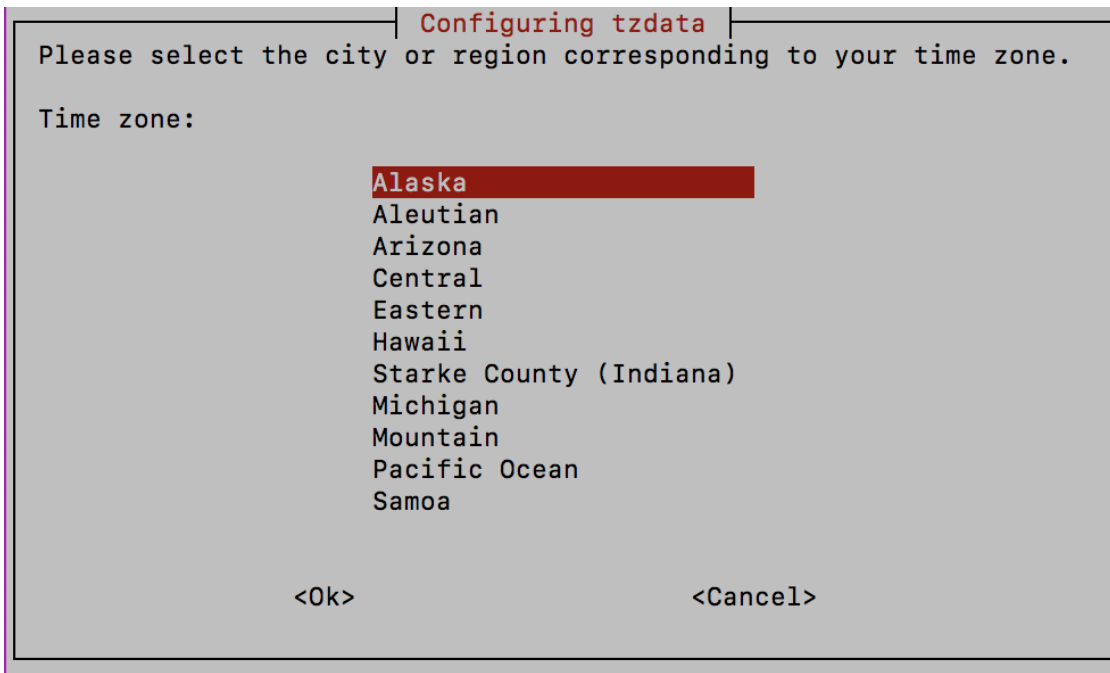
```
Configuring tzdata
Please select the geographic area in which you live. Subsequent
configuration questions will narrow this down by presenting a list of
cities, representing the time zones in which they are located.

Geographic area:

      Asia
      Atlantic Ocean
      Europe
      Indian Ocean
      Pacific Ocean
      System V timezones
      US
      None of the above

      <Ok>                <Cancel>
```

Step 4 Select the city or region corresponding to your timezone.



- Step 5** Select **OK** to save the settings.
- Step 6** Reboot the Crosswork Data Gateway VM so that all processes pick up the new timezone.
- Step 7** 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 **0 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.
-

View Crosswork Data Gateway Vitals

Follow these steps to view Cisco Crosswork Data Gateway vitals:

-
- Step 1** From the Main Menu, select **4 Vitals**.
- Step 2** From the **Show VM Vitals** menu, select the vital you want to view.

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	<p>Displays the following vitals for the Docker containers currently instantiated in the system:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Repository • Image ID • Created Time • Size • Tag
Controller Reachability	Displays the results of controller reachability test run: <ul style="list-style-type: none"> • Default IPv4 gateway • Default IPv6 gateway • DNS server • Controller • Controller session status
NTP Reachability	Displays the result of NTP reachability tests: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 6: Permissions Per Role, on page 59](#).

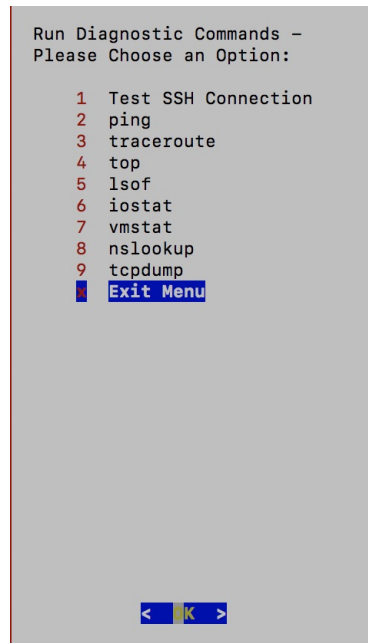
The **Troubleshooting** menu that provides you the following options:

- [Run Diagnostic Commands, on page 73](#)
- [Run show-tech, on page 76](#)
- [Shutdown the Crosswork Data Gateway VM, on page 76](#)
- [Export auditd Logs, on page 76](#)
- [Enable TAC Shell Access, on page 77](#)

Run Diagnostic Commands

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

Figure 1: Run Diagnostics 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 **Run Diagnostics** menu, select **2 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 **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 **Run Diagnostics** menu, select **3 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 Navigate to **5 Troubleshooting > 1 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 nslookup**

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 Go to **5 Troubleshooting > Run Diagnostics > 9 tcpdump**.

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

Step 3 Select the appropriate checkbox 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. Once 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 show-tech

Crosswork Data Gateway provides the option **show_tech** 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 **5 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 **9 Export audit Logs**.

Step 2 Enter a passphrase for auditd log tarball encryption.

Step 3 Click **OK**.

Remove Rotated Log Files

Use this procedure to remove all rotated log files (*.gz or *.xz) in the /var/log and /opt/dg/log folders.

Step 1 From **Troubleshooting** menu, select **8 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 **5 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, on page 79](#)
- [Delete Crosswork Data Gateway Service from Cisco CSP, on page 79](#)
- [Delete VM from OpenStack, on page 80](#)

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 Crosswork Data Gateway Service from Cisco CSP

Follow the steps to delete the Crosswork Data Gateway Service from Cisco CSP:

Before you begin

Ensure that 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 into your Cisco CSP.
- Step 2** Go to **Configuration > Services**.
The **Service** table shows the current status of the services.
- Step 3** Find your service instance in the **Service Name** column and click **Delete** under the **Action** column.
-

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:**
- Log in to the OpenStack UI.
 - Navigate to **Compute > Instances**.
 - From the list of VM displayed in this page, select the VM you want to delete.
 - Click **Delete Instances**.
 - Click **Delete Instances** in the confirmation window that appears to delete the VM.

OR

- Step 2 From the OpenStack CLI:**
- Log in to the OpenStack VM from CLI.
 - Run the following command:

```
openstack server delete CDG_VM_name
```


For example,

```
openstack server delete cdg-ospdl
```
 - (Optional) Confirm that the VM has been deleted by viewing the list of all VMs.

```
openstack server list
```
