



Cisco Crosswork Data Gateway 3.0.2 Installation and Configuration Guide for Cloud Applications

First Published: 2021-12-21

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)

© 2021 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	5

CHAPTER 3	Installation Tasks	7
	Install Cisco Crosswork Data Gateway	7
	Cisco Crosswork Data Gateway Deployment Parameters and Scenarios	8
	Install Crosswork Data Gateway Using vCenter vSphere Client	16
	Install Crosswork Data Gateway Via OVF Tool	22
	Install Crosswork Data Gateway on Cisco CSP	24
	Generate Enrollment Package	32
	Export Enrollment Package	33

CHAPTER 4	Configure Crosswork Data Gateway VM	35
	Use the Interactive Console	35
	Manage Crosswork Data Gateway Users	36
	Supported User Roles	37
	Change Password	39
	View Current System Settings	39
	Change Current System Settings	40
	Configure NTP	41
	Configure DNS	42

Configure Control Proxy	42
Configure Static Routes	42
Add Static Routes	42
Delete Static Routes	43
Configure Syslog	43
Create New SSH Keys	44
Import Certificate	44
Configure vNIC2 MTU	44
Configure Timezone of the Crosswork Data Gateway VM	45
Configure Password Requirements	46
Configure Simultaneous Login Limits	47
Configure Idle Timeout	48
Configure Remote Auditd Server	48
View Crosswork Data Gateway Vitals	48
Troubleshooting Crosswork Data Gateway VM	51
Run Diagnostic Commands	51
Ping a Host	52
Traceroute to a Host	52
Command Options to Troubleshoot	53
Download tcpdump	53
Run show-tech	54
Shutdown the Crosswork Data Gateway VM	54
Export auditd Logs	54
Remove Rotated Log Files	54
Enable TAC Shell Access	55
Audit TAC Shell Events	56

CHAPTER 5	Delete the Virtual Machine	57
	Delete VM using vSphere UI	57
	Delete Crosswork Data Gateway Service from Cisco CSP	57



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).
- Network monitoring and troubleshooting.
- Familiarity with the different operating systems used on devices that form your network, such as Cisco IOS-XR, IOS-XE, and NX-OS.

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 deployment. For details on Crosswork Data Gateway installation for Crosswork On Premise deployment, refer to the *Cisco Crosswork Infrastructure 4.1 and Applications Installation Guide*.

Crosswork Data Gateway has been validated in conjunction with the following Crosswork Cloud applications:

- Cisco Crosswork Trust Insights
- Cisco Crosswork Traffic Analysis



CHAPTER 2

Installation Requirements

You can deploy Crosswork Data Gateway either on VMware or on Cisco Cloud Services Platform (Cisco CSP) hosts. This section provides information about the general guidelines and minimum requirements for installing Crosswork Data Gateway on either platform.

This section contains the following topics:

- [VM Requirements, on page 3](#)
- [Ports Used, on page 5](#)

VM Requirements

The requirements are same for both VMware and Cisco CSP, unless stated otherwise.

Table 1: Cisco Crosswork Data Gateway VM Requirements

Requirement	Description
Data Center	VMware <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 Cisco CSP <ul style="list-style-type: none">• Cisco CSP 2.8.0.276 or later <code>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']</code>
Memory	32 GB
Disk space	74 GB
vCPU	8

Requirement	Description																
Interfaces	<p>Minimum: 1</p> <p>Maximum: 3</p> <p>Crosswork Data Gateway can be deployed with either one, two or three interfaces as per the combinations below:</p>																
	<table border="1"> <thead> <tr> <th>No. of NICs</th> <th>vNIC0</th> <th>vNIC1</th> <th>vNIC2</th> </tr> </thead> <tbody> <tr> <td>1</td> <td> <ul style="list-style-type: none"> • Management Traffic • Control/Data Traffic • Device Access Traffic </td> <td>—</td> <td>—</td> </tr> <tr> <td>2</td> <td> <ul style="list-style-type: none"> • Management Traffic </td> <td> <ul style="list-style-type: none"> • Control/Data Traffic • Device Access Traffic </td> <td>—</td> </tr> <tr> <td>3</td> <td> <ul style="list-style-type: none"> • Management Traffic </td> <td> <ul style="list-style-type: none"> • Control/Data Traffic </td> <td> <ul style="list-style-type: none"> • Device Access Traffic </td> </tr> </tbody> </table>	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
	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: for data and configuration transfer between Crosswork Data Gateway and Crosswork applications and other external data destinations. • Device access traffic: for device management and telemetry data. 																	
IP Addresses	<p>One, two or three IPv4/IPv6 addresses based on the number of interfaces you choose to use.</p> <p>Note Crosswork does not support dual stack configurations. Therefore, ALL addresses for the environment must be either IPv4 or IPv6.</p>																
NTP Servers	<p>The IPv4/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. Confirm that the NTP IP address or host name is reachable on the network or installation will fail.</p> <p>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.</p>																
DNS Servers	<p>The IPv4/IPv6 addresses of the DNS servers you plan to use. These should be the same DNS servers you use to resolve host names across your network.</p>																

Requirement	Description
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.



Note The Cisco Crosswork Data Gateway application is bundled with Ubuntu Server 20.04.2. Cisco will provide updates as need to address security and other fixes.

In Cloud deployments, Cisco Crosswork Data Gateway must connect to the Internet via TLS, and a proxy server may be required. If there is a proxy server in the network, it needs to be configured either during the installation process or from the Interactive Console of the Crosswork Data Gateway VM after installation. See:

- [Configure Control Proxy, on page 42](#)
- [View Crosswork Data Gateway Vitals](#)

Ports Used

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



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



Note The SCP port can be configured.

Table 2: Ports to be opened for Management Traffic

Port	Protocol	Used for...	Direction
22	TCP	SSH server	Inbound
22	TCP	SCP client	Outbound
123	UDP	NTP Client	Outbound
53	UDP	DNS Client	Outbound
443	TCP	Crosswork Controller	Outbound



CHAPTER 3

Installation Tasks

This section contains the following topics:

- [Install Cisco Crosswork Data Gateway, on page 7](#)
- [Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 8](#)
- [Install Crosswork Data Gateway Using vCenter vSphere Client, on page 16](#)
- [Install Crosswork Data Gateway Via OVF Tool, on page 22](#)
- [Install Crosswork Data Gateway on Cisco CSP, on page 24](#)
- [Generate Enrollment Package, on page 32](#)
- [Export Enrollment Package, on page 33](#)

Install Cisco Crosswork Data Gateway

Cisco Crosswork Data Gateway is initially deployed as a VM called Base VM (containing only enough software to register itself with Crosswork Cloud). Crosswork Cloud orchestrates the collection from the distributed Cisco Crosswork Data Gateway VMs.

Based on the size 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 8](#) 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 16
	Install Crosswork Data Gateway Via OVF Tool, on page 22
Cisco CSP	Install Crosswork Data Gateway on Cisco CSP, on page 24

3. Enroll Cisco Crosswork Data Gateway with Crosswork Cloud.



Note For procedure to enroll Cisco Crosswork Data Gateway with Crosswork Cloud applications, refer to the Section: Add Cisco Crosswork Data Gateway Information in *Cisco Crosswork Cloud User Guide*.

- [Generate Enrollment Package, on page 32](#)
- [Export Enrollment Package, on page 33](#)

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.

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 55](#)). 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 37](#).

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 39](#). 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 3: 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 <code>cloud</code> for Cloud deployment.	This parameter is pre-defined for CSP installation. You will need to specify this parameter only in case of VMware or OVF tool installation.

Name	Parameter	Description	Additional Information
Active vNICs *	ActiveVnics	Number of vNICs to use for sending traffic.	You can choose to use either 1, 2 or 3 interfaces as per your network requirements. For information on how you can route traffic, see <i>Interfaces</i> in the VM Requirements, on page 3 table.
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).	Crosswork Cloud uses self-signed certificates for handshake with Cisco Crosswork Data Gateway. These certificates are generated at installation.
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).	However, if you want to use third-party or your own certificate files enter these three parameters.
Certificate File and Key Passphrase	DGCertChainPwd	SCP user passphrase to retrieve the Cisco Crosswork Data Gateway PEM formatted certificate file and private key.	Certificate chains override any preset or generated certificates in the Cisco Crosswork Data Gateway VM and are given as an SCP URI (user:host:/path/to/file). Note The host with the URI files must be reachable on the network (from the vNIC0 interface via SCP) and files must be present at the time of install.

Name	Parameter	Description	Additional Information
Data Disk Size	DGAppdataDisk	Size in GB of a second data disk. The default size is 20GB.	
Passphrases			
dg-admin Passphrase *	dg-adminPassword	The password you have chosen for the dg-admin user. Password must be 8-64 characters.	
dg-oper Passphrase *	dg-operPassword	The password you have chosen for the dg-oper user. Password must be 8-64 characters.	
Interfaces			
Note You must select either an IPv4 or IPv6 address. Selecting None in both vNICx IPv4 Method field and vNICx IPv6 Method field will result in a non-functional deployment.			
vNICx IPv4 Address (vNIC0, vNIC1 and vNIC2 based on the number of interfaces you choose to use)			
vNICx IPv4 Method* For example, the parameter name for vNIC0 is vNIC0 IPv4 Method.	VnicxIPv4Method For example, the parameter name for vNIC0 is Vnic0IPv4Method.	None or Static The default value for Method is None . To use IPv4 address, select Method as Static and select the vNICx IPv6 Method as None .	If you have selected Method as Static , enter information in Address , Netmask , Skip Gateway , and Gateway fields.
vNICx IPv4 Address	VnicxIPv4Address	IPv4 address of the vNICx interface.	
vNICx IPv4 Netmask	VnicxIPv4Netmask	IPv4 netmask of the vNICx interface in dotted quad format.	
vNICx IPv4 Skip Gateway	VnicxIPv4SkipGateway	Options are <i>yes</i> or <i>no</i> . Selecting <i>yes</i> skips configuring a gateway.	
vNICx IPv4 Gateway	VnicxIPv4Gateway	IPv4 address of the vNICx gateway.	
vNICx IPv6 Address (vNIC0, vNIC1, and vNIC2 based on the number of interfaces you choose to use)			

Name	Parameter	Description	Additional Information
vNICx IPv6 Method* For example, the parameter for vNIC0 is vNIC0 IPv6 Method.	VnicxIPv6Method For example, the parameter for vNIC0 is Vnic0IPv6Method.	None orStatic The default value for Method is None . To use IPv6 address, select Method as Static and select the vNICx IPv4 Method as None .	If you choose to use IPv6 address, enter information in Address , Netmask , Skip Gateway , and Gateway fields.
vNICx IPv6 Address	VnicxIPv6Address	IPv6 address of the vNICx interface.	
vNICx IPv6 Netmask	VnicxIPv6Netmask	IPv6 prefix of the vNICx interface.	
vNICx IPv6 Skip Gateway	VnicxIPv6SkipGateway	Options are <i>yes</i> or <i>no</i> . Selecting <i>yes</i> skips configuring a gateway.	
vNICx IPv6 Gateway	VnicxIPv6Gateway	IPv6 address of the vNICx gateway.	
DNS Servers			
DNS Address*	DNS	Space-delimited list of IPv4/IPv6 addresses of the DNS server accessible from the management interface.	
DNS Search Domain*	Domain	DNS search domain	
DNS Security Extensions*	DNSSEC	Options are <i>False</i> , <i>True</i> , <i>Allow-Downgrade</i> . Select <i>True</i> to use DNS security extensions. By default, this parameter is <i>False</i> .	
DNS over TLS*	DNSTLS	Options are <i>False</i> , <i>True</i> , and <i>Opportunistic</i> . Select <i>True</i> to use DNS over TLS. By default, this parameter is <i>False</i> .	
Multicast DNS*	mDNS	Options are <i>False</i> , <i>True</i> and <i>Resolve</i> . Select <i>True</i> to use multicast DNS. By default, this parameter is <i>False</i> .	

Name	Parameter	Description	Additional Information
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/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. If you are not using an NTP server, ensure that time gap between Cisco Crosswork Data Gateway and Crosswork Cloud is not more than 24 hours. Else, Cisco Crosswork Data Gateway will fail to connect.
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 Servers			

Name	Parameter	Description	Additional Information
Use Remote Syslog Server*	UseRemoteSyslog	Select Yes to send syslog messages to a remote host. The default value is No.	Configuring an external syslog server sends service events to the external syslog server. Otherwise, they are logged only to the Cisco Crosswork Data Gateway VM. If you want to use an external syslog server, you must specify these seven settings. Note The host with the URI files must be reachable on the network (from vNIC0 interface via SCP) and files must be present at the time of install.
Syslog Server Address	SyslogAddress	IPv4 or IPv6 address of a syslog server accessible 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 Servers			

Name	Parameter	Description	Additional Information
Use Remote Auditd Server*	UseRemoteAuditd	Select Yes to send Auditd message to a remote host	Configure Crosswork Data Gateway to send auditd messages to a remote server. Specify these three settings to use 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 33 .
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 3.0.x Release notes* and download the recommended Crosswork Data Gateway image file from CCO (*.ova).

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.

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.

Step 2 Select the data center where you want to deploy the Crosswork Data Gateway VM.

Step 3 Connect to vCenter vSphere Client. Then select **Actions > Deploy OVF Template**.

Step 4 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 5 Click **Next** to go to **2 Select name and location**, 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

Step 6 Click **Next** to go to **3 Select a compute resource**. Choose the VM's host.

Step 7 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 8 Click **Next** to go to **5 accept license agreements**. Review the End User License Agreement and click **Accept**.

Step 9 Click **Next** to go to **6 Select configuration**, as shown in the following figure. Select **Crosswork Cloud**.

Deploy OVF Template

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

Configuration
Select a deployment configuration

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

3 Items

CANCEL BACK NEXT

Step 10 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 11

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.

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 12 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.

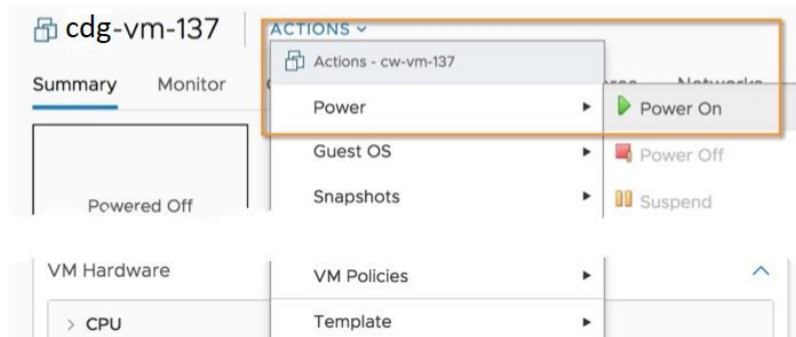
Enter the information for the parameters as described in [Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 8](#).

Step 13 Click **Next** to go to **10 Ready to complete**. Review your settings and then click **Finish** if you are ready to begin deployment.

Step 14 Check deployment status.

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

Step 15 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.

What to do next

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**.

Access Cisco 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 administrator user: `ssh dg-admin@<ManagementNetworkIP>`

To login 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.

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 8](#).

Below is a sample script if you are planning to run the OVF tool with a script:

```
#!/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.
- 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 in one of the following ways:

a) **Using the command**

Execute the following command.

This command contains the location of the source OVF file and location of the vmx file that will be created as a result of executing the command:

```
ovftool <location_of_source_ovf_file> <location_of_vmx_file>
```

For example,

```

ovftool --acceptAllEulas --skipManifestCheck --X:injectOvfEnv -ds="datastore130-2"
--deploymentOption="cloud" --diskMode="thin" --overwrite --powerOffTarget --powerOn
--noSSLVerify --allowExtraConfig --extraConfig:firmware=efi
--extraConfig:uefi.secureBoot.enabled=true --name="cdg147.cisco.com"
--prop:"Hostname=cdg147.cisco.com" --prop:"Description=CDG Base VM for Automation"
--net:"vNIC0=VM Network" --prop:"Vnic0IPv4Method=Static"
--prop:"Vnic0IPv4Address=<vNIC 0 IPv4 address>" --prop:"Vnic0IPv4Netmask=<vNIC0 IPv4 netmask>"
--prop:"Vnic0IPv4Gateway=<vNIC 0 IPv4 gateway>" --net:"vNIC1=DPG991"
--prop:"Vnic1IPv4Method=Static" --prop:"Vnic1IPv4Address=<vNIC1 IPv4 address>"
--prop:"Vnic1IPv4Netmask=<vNIC1 IPv4 netmask>" --prop:"Vnic1IPv4Gateway=<vNIC1 IPv4 gateway>"
--net:"vNIC2=DPG999" --prop:"dg-adminPassword=<password>"
--prop:"dg-operPassword=<password>" --prop:"DNS=<DNS address>"
--prop:"NTP=<NTP>"
--prop:"Domain=cisco.com" <image download URL> <username><password>'@<IP address>/DC/host/<IP
address>

```

b) **Using the script**

If you want to execute the script that you have created containing the command and arguments:

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

What to do next

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**.

Access Cisco 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 administrator user: `ssh dg-admin@<ManagementNetworkIP>`

To login 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.

Install Crosswork Data Gateway on Cisco CSP

Follow the steps to install Crosswork Data Gateway on Cisco CSP:

Step 1 Prepare Crosswork Data Gateway Service Image for upload to Cisco CSP:

- a) Refer to the *Crosswork Data Gateway 3.0.x Release notes* and download the recommended image file.
- b) Extract the Crosswork Data Gateway `qcow2` build from CCO to your local machine or a location on your local network that is accessible to your Cisco CSP.

The build is a tarball of the `qcow2` and `config.txt` files.

- c) 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 8.

Note If you plan to install more than one Data Gateway VM, create a unique `config.txt` file for each Data Gateway VM.

Following parameters have pre-defined values:

- Deployment
 - Use "cloud".

Below is an example of how the `config.txt` file looks like:

```
ActiveVnics=
AuditdAddress=
AuditdPort=
Deployment=cloud
Description=
DGAppdataDisk=
DGCertChain=
DGCertChainPwd=
DGCertKey=
DNS=changeme
DNSSEC=False
DNSTLS=False
Domain=changeme
EnrollmentPassphrase=
EnrollmentURI=
Hostname=changeme
Label=
LLMNR=False
mDNS=False
NTP=changeme
NTPAuth=False
NTPKey=
NTPKeyFile=
NTPKeyFilePwd=
Profile=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
Vnic0IPv4Gateway=0.0.0.1
Vnic0IPv4Method=None
Vnic0IPv4Netmask=0.0.0.0
Vnic0IPv6Address>:::0
Vnic0IPv6Gateway>:::1
Vnic0IPv6Method=None
Vnic0IPv6Netmask=64
Vnic1IPv4Address=0.0.0.0
```

```

Vnic1IPv4Gateway=0.0.0.1
Vnic1IPv4Method=None
Vnic1IPv4Netmask=0.0.0.0
Vnic1IPv6Address>:::0
Vnic1IPv6Gateway>:::1
Vnic1IPv6Method=None
Vnic1IPv6Netmask=64
Vnic2IPv4Address=0.0.0.0
Vnic2IPv4Gateway=0.0.0.1
Vnic2IPv4Method=None
Vnic2IPv4Netmask=0.0.0.0
Vnic2IPv6Address>:::0
Vnic2IPv6Gateway>:::1
Vnic2IPv6Method=None
Vnic2IPv6Netmask=64
dg-adminPassword=changeme
dg-operPassword=changeme

```

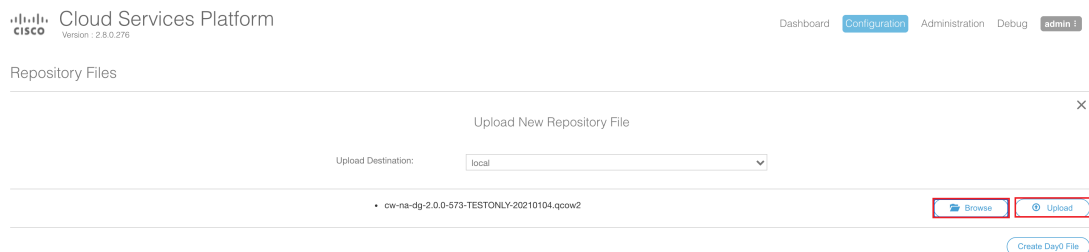
Step 2 Upload Crosswork Data Gateway Service Image to Cisco CSP:

- Log in to the Cisco CSP.
- Go to **Configuration > Repository**.
- On the **Repository Files** page, Click Crosswork Data Gateway button.



- Select an **Upload Destination**.
- Click **Browse**, navigate to the `qcow2` file, click **Open** and then **Upload**.

Repeat this step to upload `config.txt` file.



After the files are uploaded, file name and other relevant information is displayed in the **Repository Files** table.

Step 3 Create Crosswork Data Gateway Service:

- Go to **Configuration > Services**.
- On the **Service** page, click **+** button.
- Check **Create Service** option.

The **Create Service Template** page is displayed.

Service Templates

X

Create Service Template

Name: * * Required Field

Target Host Name: *

Image Name: * * Required Field
File Name should not contain any special characters or space.

Number of Cores:
Available Cores: 12

RAM (MB):
Available RAM (MB): 64339

Disk Space (GB):

Disk Type: IDE VIRTIO

Disk Storage: * Local NFS

Description:

+ VNIC *

vnic	Admin Status	Vlan	Vlan Type	Network Name	Action
0	up		access	Eth0-2	⊗
1	up		access	Eth1-1	⊗
2	up		access	Eth1-2	⊗

d) Enter the values for the following fields:

Field	Description
Name	Name of the VM.
Target Host Name	Choose the target host on which you want to deploy the VM.
Image Name	Select the <code>qcow2</code> image.

e) Click **Day Zero Config**.

Day Zero Config

Source File Name: * Required Field

Destination File Name:

Create Service Create Service using Template

Name: *

Target Host Name: *

Image Name: * * Required Field
File Name should not contain any special characters or space.

+ Day Zero Config

Number of Cores:
Available Cores: 20

RAM (MB):
Available RAM (MB): 241353

Resize Disk

Disk Space (GB):

Disk Type: IDE VIRTIO

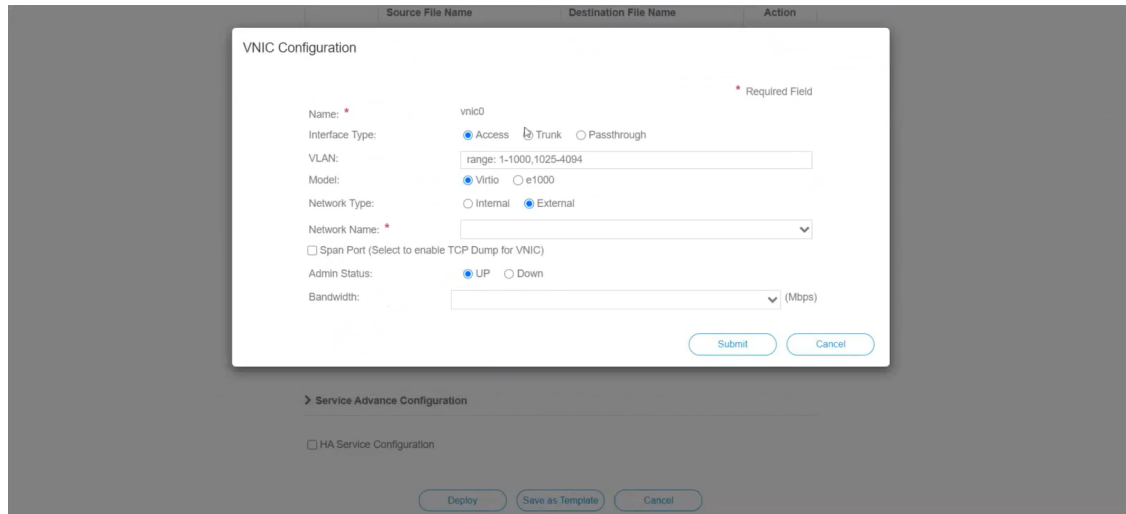
In the **Day Zero Config** dialog box, do the following:

1. From the **Source File Name** drop-down list, select the `config.txt` file that you modified and uploaded earlier.
2. In the **Destination File Name** field, enter "config.txt".
3. Click **Submit**.

f) Enter the values for the following fields:

Field	Description
Number of Cores	8
RAM (MB)	32768

g) Click **VNIC**.



In the **VNIC Configuration** dialog box:

Note The VNIC Name is set by default.

1. Select the **Interface Type** as **Access**.
2. Select the **Model** as **Virtio**.
3. Select the **Network Type** as **External**.
4. Refer to the following table and select the **Network Name**:

For VNIC...	Select...
vnic0	Eth0-1
vnic1	Eth1-1
vnic2	Eth1-2

5. Select **Admin Status** as **UP**.
6. Click **Submit**.
7. Repeat Step **g** for VNIC1 and VNIC2 if you plan to have more than one VNIC in your network.

After you have added all three VNICs, the VNIC table will look like this:

⊕ VNIC *

vnic	Admin Status	Vlan	Vlan Type	Network Name	Action
0	up		access	Eth0-1	⚙️
1	up		access	Eth1-1	⚙️
2	up		access	Eth1-2	⚙️

- h) Expand the **Service Advance Configuration** and for **Firmware**, select **uefi** from the drop-down. Check the **Secure Boot** checkbox.

- i) Click **Storage**.

In the **Storage Configuration** dialog box, do the following:

Field	Description
Name	Name of the storage. This is specified by default.

Field	Description
Device Type	Select Disk .
Location	Select local .
Disk Type	Select VIRTIO .
Format	Select QCOW2 .
Mount image file as disk?	Leave this unchecked.
Size (GB)	Enter the disk size as 70GB.

When you are done with the storage configuration, click **Submit**.

j) Click **Deploy**.

Cache Mode: none

Emulator Range: Max Emulator Range: 0-7

VM Health Monitoring Configuration

Status: disabled

VNF Management IP: VNF Management IP x.x.x.x

VNF Group: default-vnf-group

VNC Port: VNC Port Range : 8721 - 8784

VNC Password:

Confirm VNC Password:

Storage

Storage	Storage Type	Size (GB) / Disk Image Name	Action
1	disk (virtio)	5	⚙️

Serial Port

HA Service Configuration

Deploy Save as Template Cancel

You will see a similar message once the service has successfully deployed. Click **Close**.

Service Creation.

Service cdtg-standard available on csp1.

Close

Administration Debug admin

Service

Create Service

* Required Field

Create Service Create Service using Template

Name: * cdtg-standard

Target Host Name: * csp1

Image Name: * cw-ha-dtg-2.0.0-642-TESTONLY-20210213.qcow2

File Name: should not contain any special characters or space.

Day Zero Config

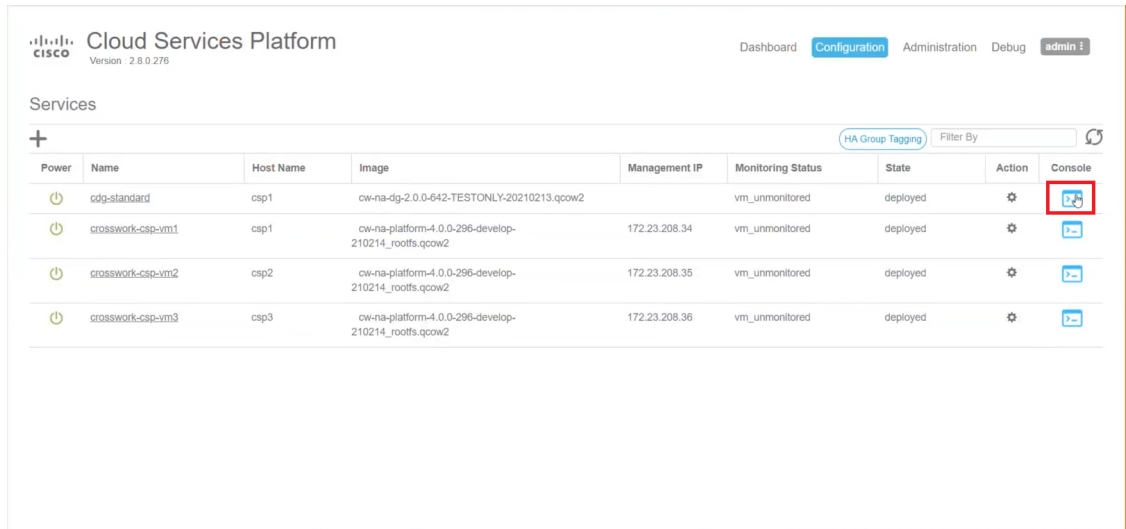
	Source File Name	Destination File Name	Action
1	config.txt	config.txt	⚙️

First Day Zero File Volume ID:

Day Zero File Format: ISO 9660

Step 4 Deploy Crosswork Data Gateway service:

- a) Go to **Configuration > Services**.
- b) In the **Services** table, click the console icon under **Console** column for the Crosswork Data Gateway service you created above.

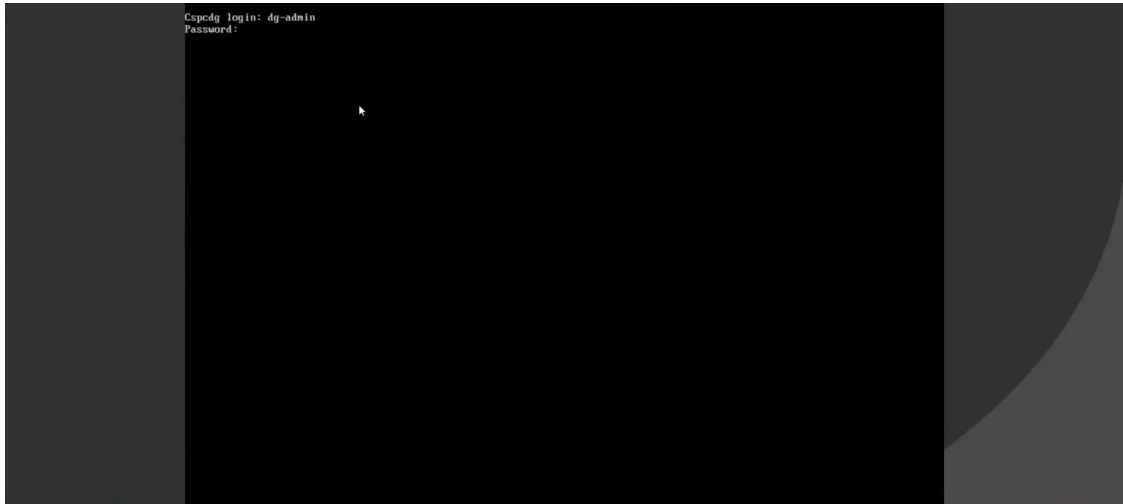


Power	Name	Host Name	Image	Management IP	Monitoring Status	State	Action	Console
	cdg-standard	csp1	cw-na-dg-2.0.0-642-TESTONLY-20210213.qcow2		vm_unmonitored	deployed		
	crosswork-csp-vm1	csp1	cw-na-platform-4.0.0-296-develop-210214_roofts.qcow2	172.23.208.34	vm_unmonitored	deployed		
	crosswork-csp-vm2	csp2	cw-na-platform-4.0.0-296-develop-210214_roofts.qcow2	172.23.208.35	vm_unmonitored	deployed		
	crosswork-csp-vm3	csp3	cw-na-platform-4.0.0-296-develop-210214_roofts.qcow2	172.23.208.36	vm_unmonitored	deployed		

- c) The **noVNC** window opens. Click **Connect** option in the top right corner.



- d) Once the Crosswork Data Gateway service connects, login 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.



The Crosswork Data Gateway console is available.

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 3: 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 33)

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 33.



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

A sample enrollment package JSON is shown below:

```
{
  "name": "dg116.cisco.com",
  "description": "CDG Base VM for Automation",
  "profile": {
    "cpu": 8,
```

```

    "memory": 31,
    "nics": 3
  },
  "interfaces": [
    {
      "name": "eth0",
      "mac": "00:50:56:9e:09:7a",
      "ipv4Address": "<ip_address>/24"
    },
    {
      "name": "eth1",
      "mac": "00:50:56:9e:67:c3",
      "ipv4Address": "<ip_address>/16"
    },
    {
      "name": "eth2",
      "mac": "00:50:56:9e:83:83",
      "ipv4Address": "<ip_address>/16"
    }
  ],
  "certChain": [
    "<cert_chain>"
  ],
  "version": "1.1.0 (branch dg110dev - build number 152)",
  "duuid": "d58fe482-fdca-468b-a7ad-dfbfa916e58b"
}

```

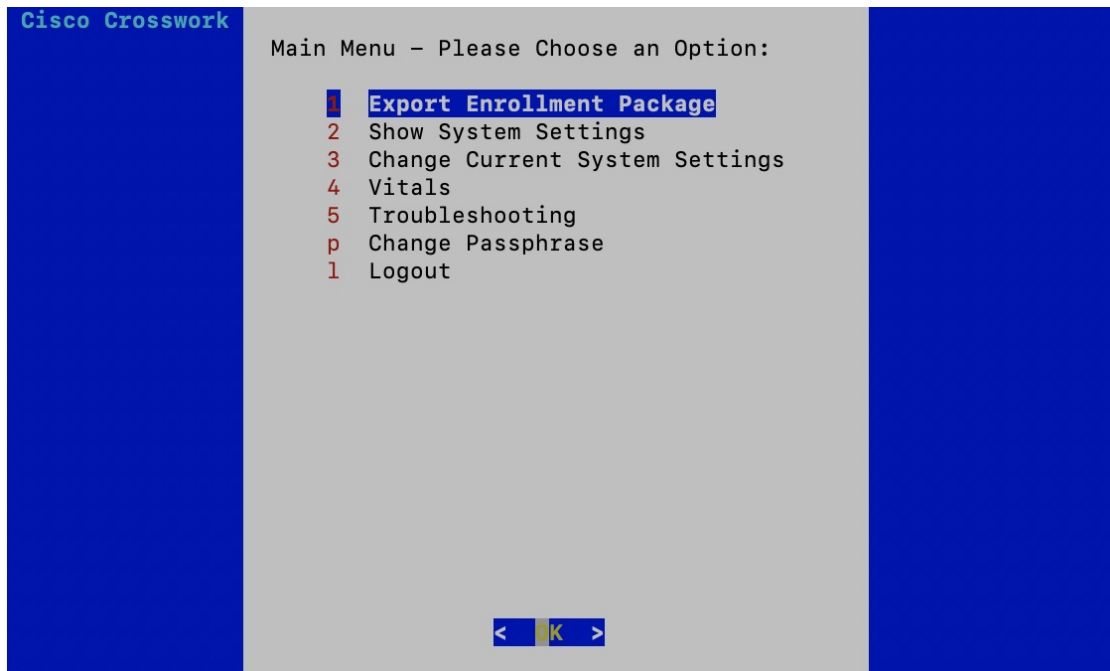
Export Enrollment Package

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



Note This is needed only if you have not specified **Auto Enrollment Package Transfer** settings during installation. Otherwise, the file will be copied to the SCP URI destination you selected after the VM boots.

- 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
```

- Note** 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.

Step 6 Proceed with enrolling the Cisco Crosswork Data Gateway with Crosswork Cloud. For procedure to enroll Cisco Crosswork Data Gateway with Crosswork Cloud applications, refer to the Section: *Add Cisco Crosswork Data Gateway Information* in *Cisco Crosswork Cloud User Guide*.

If you are enrolling Cisco Crosswork Data Gateway with Cisco Crosswork Trust Insights or Cisco Crosswork Traffic Analysis, also perform the following steps. These steps are optional, based on your network environment and required only if you have not specified them during installation.

- [Configure Control Proxy, on page 42](#)
- [View Crosswork Data Gateway Vitals](#)



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:

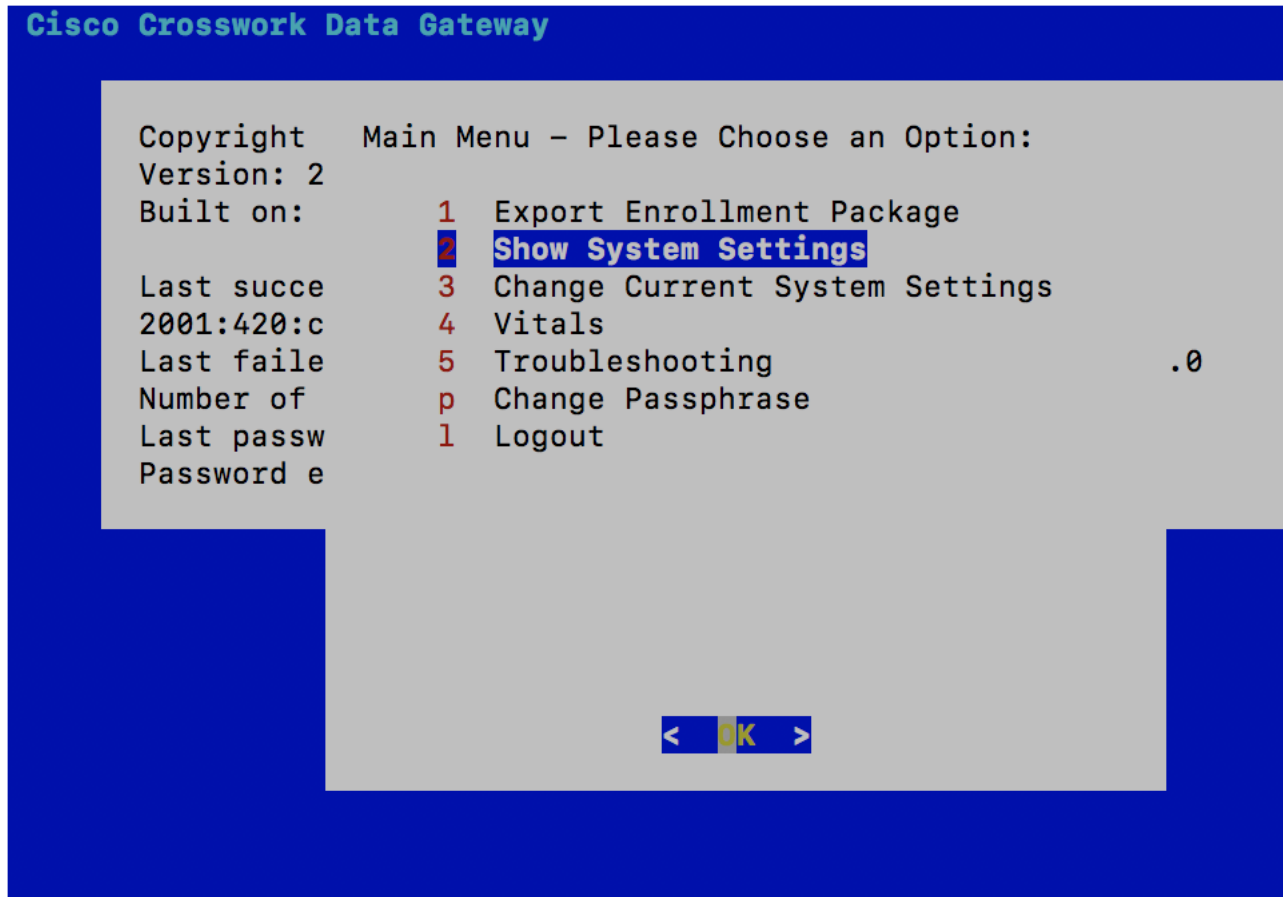
- [Use the Interactive Console, on page 35](#)
- [Manage Crosswork Data Gateway Users, on page 36](#)
- [View Current System Settings, on page 39](#)
- [Change Current System Settings, on page 40](#)
- [View Crosswork Data Gateway Vitals, on page 48](#)
- [Troubleshooting Crosswork Data Gateway VM, on page 51](#)

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 4: Permissions Per Role, on page 37](#).



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 37](#)
- [Change Password, on page 39](#)

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 4: 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	✓	✓
Remove All Collectors and Reboot VM	✓	×
Export auditd logs	✓	✓
Enable TAC Shell Access	✓	×
Change Passphrase	✓	✓

Change Password

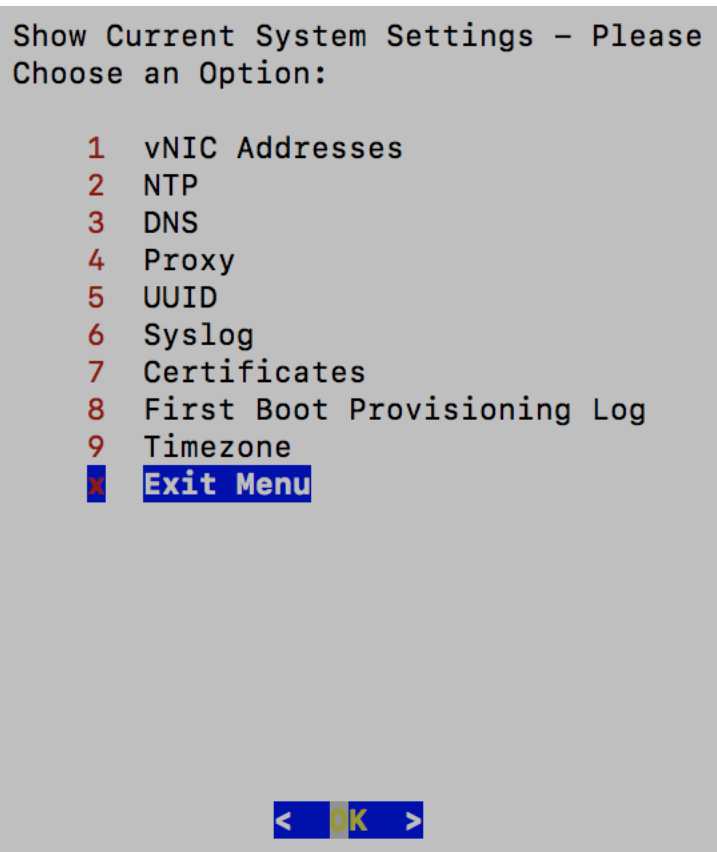
Both administrator and operator users can change their own passphrases but not each others'.

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:



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

**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 54](#). 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 48](#). 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

Many production environments do not allow direct connectivity to public Internet sites. When used to connect to Crosswork Cloud, the Data Gateway **MUST** connect to a public HTTP server. If your environment requires an HTTP/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.

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/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/IPv6 subnet in CIDR format.
- Step 6** Click **OK** to save the settings.
-

Configure Syslog



Note For any Syslog server configuration with IPv4/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]).
 - 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.

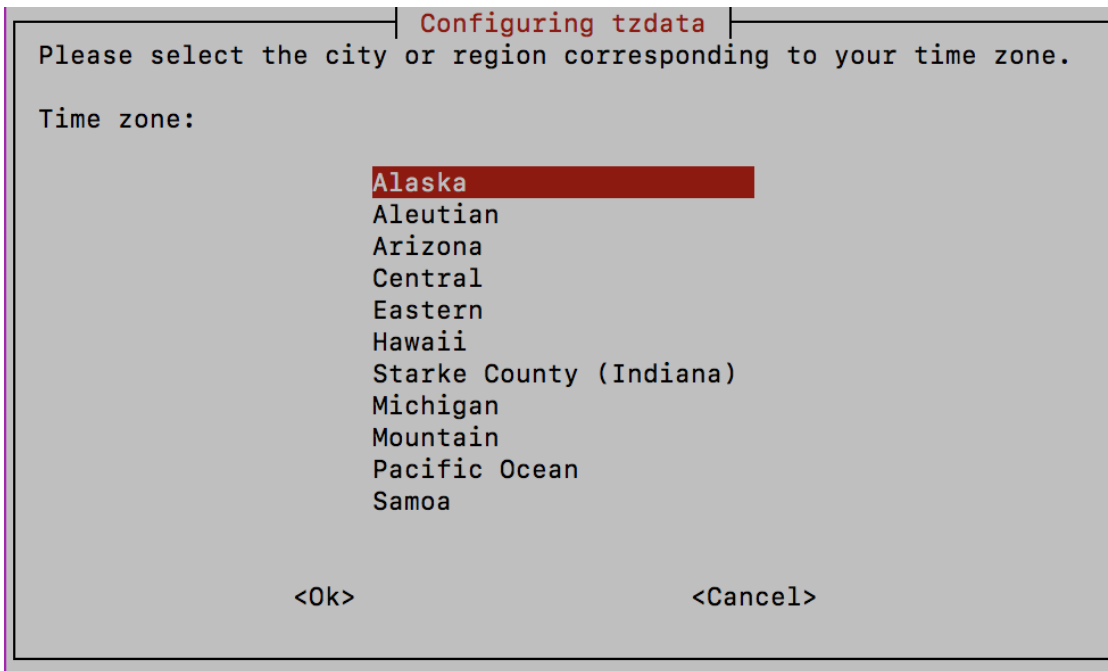
```
Configuring tzdata
Please select the geographic area in which you live. Subsequent
configuration questions will narrow this down by presenting a list of
cities, representing the time zones in which they are located.

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	Displays the following vitals for the docker containers currently instantiated in the system: <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 4: Permissions Per Role, on page 37](#).

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

- [Run Diagnostic Commands, on page 51](#)
- [Run show-tech, on page 54](#)
- [Shutdown the Crosswork Data Gateway VM, on page 54](#)
- [Export auditd Logs, on page 54](#)
- [Enable TAC Shell Access, on page 55](#)

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**.
-

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 removes 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.
- Share the password that you had set in Step 5 for the **dg-tac** user with the Cisco engineer who is working with you.
 - 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.
 - 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.
 - 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.
- Log in as the **dg-tac** user Via SSH using the following command:


```
ssh dg-tac@<DG hostname or IP>
```
 - 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 57](#)
- [Delete Crosswork Data Gateway Service from Cisco CSP, on page 57](#)

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.
-