



Install Crosswork Data Gateway on VMware vCenter

This chapter contains the following topics:

- [Crosswork Data Gateway Workflows](#), on page 1
- [Log in and Log out of the Data Gateway VM](#), on page 29
- [Crosswork Data Gateway Authentication and Enrollment](#), on page 31
- [Crosswork Data Gateway Post-installation Tasks](#), on page 32
- [Troubleshoot Crosswork Data Gateway Installation and Enrollment](#), on page 33

Crosswork Data Gateway Workflows

Crosswork Data Gateway is installed as a base VM that contains only enough software to register itself with Cisco Crosswork.

Installation workflow

Follow these steps to install a Data Gateway VM for use with Crosswork Network Controller:

1. Choose the deployment profile for the Crosswork Data Gateway VM. See [Crosswork Data Gateway VM requirements](#).
2. Review the installation parameters at [Crosswork Data Gateway Parameters and Deployment Scenarios](#) and make sure that you have all the required information to install Data Gateway using the preferred deployment scenario.
3. Install Data Gateway using a preferred method:

Table 1: Crosswork Data Gateway installation options

VMware	Install Crosswork Data Gateway using vCenter vSphere Client , on page 16
	Install Crosswork Data Gateway via the OVF Tool , on page 27



Note If you plan to install multiple Crosswork Data Gateway VMs due to load or scale requirements or you wish to leverage Crosswork Data Gateway High Availability, we recommend that you install all the Data Gateway VMs first and then proceed with adding them to a Data Gateway pool.

4. Complete the post-installation tasks mentioned in the section [Crosswork Data Gateway Post-installation Tasks, on page 32](#).
5. Verify that the Data Gateway VM has enrolled successfully with Crosswork Network Controller. For information on how to verify the enrollment process, see [Crosswork Data Gateway Authentication and Enrollment, on page 31](#).

After the Data Gateway VM has enrolled successfully with Cisco Crosswork, set up the data collection by creating a Data Gateway pool. For more information, see the *Create a Crosswork Data Gateway Pool* section in the *Cisco Crosswork Network Controller 7.1 Administration Guide*.

Upgrade workflow

The upgrade procedure is required only for the Data Gateway Base VM upgrade. Upgrade of other components, such as collectors, is performed by Cisco Crosswork.

Follow these steps to upgrade a Data Gateway VM for use with Crosswork Network Controller:

1. Shut down and delete the existing Data Gateway VMs. For detailed instructions, see [Delete Crosswork Data Gateway VM from Cisco Crosswork](#).
2. Install new Data Gateway VMs with the same number of VMs as the old configuration. Also, configure the new VMs with identical settings, including the Management interface. For detailed installation instructions, see [Installation workflow, on page 1](#).
3. Verify that the newly installed Data Gateway VMs are enrolled with Cisco Crosswork.

On the **Data Gateway Management** page, confirm that Data Gateway status has the status as:

- **Admin State** is in the **Up** state.
- **Operational State** is in the **Not Ready** state.

For information on how to verify the enrollment process, see [Crosswork Data Gateway Authentication and Enrollment, on page 31](#).

4. Complete all required post-installation tasks, such as configuring network settings. For more information, see [Crosswork Data Gateway Post-installation Tasks, on page 32](#).
5. Verify that devices are attached to the data gateways in the Cisco Crosswork UI.

For detailed information on upgrading the Data Gateway VM, see [Upgrade Cisco Crosswork Network Controller](#).

Crosswork Data Gateway Parameters and Deployment Scenarios

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

During installation, Crosswork Data Gateway creates the following user accounts:

- Crosswork Data Gateway administrator, with the username, `dg-admin`, and the password set during installation. The administrator uses this user ID to log in and troubleshoot the Data Gateway. If the password is forgotten, the Data Gateway must be reinstalled to restore access, as it cannot be recovered or reset.
- Crosswork Data Gateway operator, with the username, `dg-oper` and the password set during installation. The `dg-oper` user has permissions to perform all ‘read’ operations and limited ‘action’ commands.

To know what operations an admin and operator can perform, see the *Supported User Roles* topic in the [Cisco Crosswork Network Controller 7.1 Administration Guide](#).

- Crosswork Data Gateway technical assistance center, with the username, `dg-tac`. The password for this user is set when one of the other users of the Data Gateways enables this account.

The **dg-admin**, **dg-oper**, and **dg-tac** user accounts are reserved usernames and cannot be changed. You can change the passwords for the **dg-admin** and **dg-oper** accounts through the Crosswork Data Gateway user interface. The **dg-tac** account is inactive by default. It can be temporarily activated by an authorized user who enables the account and sets a password.



Note Activating the **dg-tac** account requires a token that only Cisco can provide. If CLI access to the Data Gateway system is required for troubleshooting, Cisco Customer Experience (CX) will assist you in enabling the **dg-tac** account.

For more information, see the *Change Passphrase* section in the [Cisco Crosswork Network Controller 7.1 Administration Guide](#). In case of lost or forgotten passwords, destroy the current VM, you have to create a new VM, and re-enroll the new VM with Cisco Crosswork.

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

In the following table:

* Denotes the mandatory parameters. Parameters without this mark are optional. You can choose them based on your deployment scenario. Deployment scenarios are explained (wherever applicable) in the **Additional Information** column.

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



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

Table 2: Crosswork Data Gateway Deployment Parameters and Scenarios

Label	Key	Description	Additional information
DeploymentOption	DeploymentOption	Parameter conveys the VM resource profile. For an on-premise installation, choose either: <ul style="list-style-type: none"> • onpremise-standard • onpremise-extended 	This parameter is applicable only for the OVF tool.
Host Information			
Hostname*	Hostname	Name of the Data Gateway VM specified as a fully qualified domain name (FQDN). In larger systems, you are likely to have more than one Data Gateway VM. The hostname must, therefore, be unique and created in a way that makes identifying a specific VM easy.	
Description*	Description	A detailed description of the Data Gateway.	
Crosswork Data Gateway Label	Label	Label used by Cisco Crosswork to categorize and group multiple Data Gateway VMs.	
Allow Usable RFC 8190 Addresses*	AllowRFC8190	Choose how to validate interface addresses that fall in a usable RFC 8190 range. Options are: <code>Yes</code> , <code>No</code> , or <code>Ask</code> , where the initial configuration script prompts for confirmation. The default value is <code>Yes</code> .	The default value is <code>Yes</code> to automatically allow interface addresses in an RFC 8190 range.

Label	Key	Description	Additional information
Crosswork Data Gateway Private Key URI	DGCertKey	SCP URI to private key file for session key signing. You can retrieve this using SCP (user@host:path/to/file).	<p>Cisco Crosswork uses self-signed certificates for handshake with Crosswork Data Gateway. These certificates are generated at installation.</p> <p>However, if you want to use third party or your own certificate files, then enter these parameters.</p> <p>Certificate chains override any preset or generated certificates in the Data Gateway VM and are given as an SCP URI (user:host/path/to/file).</p> <p>The host with the URI files must be reachable on the network (from the vNIC0 interface via SCP) and the files must be present at the time of install.</p>
Crosswork Data Gateway Certificate File and Key Passphrase	DGCertChainPwd	Passphrase of the SCP user to retrieve the Crosswork Data Gateway PEM formatted certificate file and private key.	
Data Disk Size	DGAppdataDisk	<p>Indicates the size in GB of a second data disk. The default value of this parameter in each profile is:</p> <ul style="list-style-type: none"> • 20 GB for Standard. • 520 GB for Extended. <p>Do not change the default value without consulting a Cisco representative.</p>	

Label	Key	Description	Additional information
High Availability Network Mode *	HANetworkMode	Indicates the mode for the high-availability network. Options are: <ul style="list-style-type: none"> • L2 • L3 The default value is L2.	When deploying on VMware, set the network to L2.
Passphrase			
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			
<p>In a 3-NIC deployment, you must provide an IP address for Management Traffic (vNIC0) and Control or Data Traffic (vNIC1). The IP address for Device Access Traffic (vNIC2) is assigned during Data Gateway pool creation as explained in the <i>Create a Crosswork Data Gateway Pool</i> section in the Cisco Crosswork Network Controller 7.1 Administration Guide.</p> <p>Note</p> <ul style="list-style-type: none"> • Selecting None in both the IPv4 Method and the IPv6 Method fields of the vNIC results in a nonfunctional deployment. • Although the IP address is assigned when the Data Gateway is added to a pool, you must configure network connectivity for the third interface in VMware either during installation or before adding the Data Gateway to the pool. 			
vNIC Role Assignment			
<p>Role assignment allows you to control the traffic that an interface must handle. If your use case is not supported by the preassigned roles, you can manually assign roles to the interfaces.</p> <p>Each parameter has a predefined role. The parameter accepts the interface value as eth0, eth1, or eth2, which refer to vNIC0, vNIC1, or vNIC2 respectively.</p>			

Label	Key	Description	Additional information
Default Gateway *	NicDefaultGateway	The interface used as the Default Gateway for processing the DNS and NTP traffic. Options are <code>eth0</code> , <code>eth1</code> , or <code>eth2</code> . The default value is <code>eth0</code> .	For information on the type of roles that you must assign to the vNICs, see Table 3 .
Administration *	NicAdministration	The interface used to access the VM through the SSH access. Options are <code>eth0</code> , <code>eth1</code> , or <code>eth2</code> . The default value is <code>eth0</code> .	
External Logging *	NicExternalLogging	The interface used to send logs to an external logging server. Options are <code>eth0</code> , <code>eth1</code> , or <code>eth2</code> . The default value is <code>eth0</code> .	
Management *	NicManagement	The interface used to send the enrollment and other management traffic. Options are <code>eth0</code> , <code>eth1</code> , or <code>eth2</code> . The default value is <code>eth0</code> .	
Control *	NicControl	The interface used to send the destination, device, and collection configuration. Options are <code>eth0</code> , <code>eth1</code> , or <code>eth2</code> . The default value is <code>eth1</code> .	
Northbound System Data *	NicNBSystemData	The interface used to send collection data to the system destination. As the system destinations share the same IP as the interface that allows connection to the collection service, the northbound data for system destinations uses the Control role's interface. Options are <code>eth0</code> , <code>eth1</code> , <code>eth2</code> or <code>eth3</code> .	
Northbound External Data *	NicNBExternalData	The interface used to send the collection data to the external destinations configured by the user. Options are <code>eth0</code> , <code>eth1</code> , or <code>eth2</code> . The default value is <code>eth1</code> .	
Southbound Data *	NicSBData		

Label	Key	Description	Additional information
		<p>The interface used to collect data from the devices.</p> <p>If the interface only has the NicSBData role, it doesn't need an IP during the deployment.</p> <p>Options are <code>eth0</code>, <code>eth1</code>, or <code>eth2</code>. The default value is <code>eth2</code>.</p>	
<p>vNIC IPv4 Address (vNIC0, vNIC1, and vNIC2 based on the number of interfaces you choose to use)</p> <p>Important When using two or three NICs both vNIC0 and vNIC1 must be assigned static IPv4 or IPv6 addresses. All unused vNICs (IPv4 or IPv6) should be left set to Method "None" with the other fields left at the default.</p>			
vNIC IPv4 Method*	Vnic0IPv4Method Vnic1IPv4Method Vnic2IPv4Method	<p>Method in which the interface is assigned an IPv4 address - <code>None</code> or <code>Static</code>.</p> <p>The default value is <code>None</code>.</p>	<ul style="list-style-type: none"> • If you're using IPv4, change the value from none to static, then configure these fields: <ul style="list-style-type: none"> • vNIC IPv4 Address • vNIC IPv4 Netmask • vNIC IPv4 Skip Gateway • vNIC IPv4 Gateway • If you are using IPv6, leave the value set to none and retain the default IPv4 settings.
vNIC IPv4 Address	Vnic0IPv4Address Vnic1IPv4Address Vnic2IPv4Address	IPv4 address of the interface.	
vNIC IPv4 Netmask	Vnic0IPv4Netmask Vnic1IPv4Netmask Vnic2IPv4Netmask	IPv4 netmask of the interface in dotted quad format.	
vNIC IPv4 Skip Gateway	Vnic0IPv4SkipGateway Vnic1IPv4SkipGateway Vnic2IPv4SkipGateway	<p>The default value is <code>False</code>.</p> <p>Setting this to <code>True</code> skips configuring a gateway.</p>	
vNIC IPv4 Gateway	Vnic0IPv4Gateway Vnic1IPv4Gateway Vnic2IPv4Gateway	IPv4 address of the vNIC gateway.	
<p>vNIC IPv6 Address (vNIC0, vNIC1, and vNIC2 based on the number of interfaces you choose to use)</p>			

Label	Key	Description	Additional information
vNIC IPv6 Method*	Vnic0IPv6Method Vnic1IPv6Method Vnic2IPv6Method	Method in which the vNIC interface is assigned an IPv6 address - <i>None</i> , <i>Static</i> , or <i>SLAAC</i> . The default value is <i>None</i> .	<p>If you're using IPv6, change the value from none to static, then configure these fields:</p> <ul style="list-style-type: none"> vNIC IPv6 Address vNIC IPv6 Netmask vNIC IPv6 Skip Gateway vNIC IPv6 Gateway
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 <i>True</i> or <i>False</i> . Selecting <i>True</i> skips configuring a gateway.	
vNIC IPv6 Gateway	Vnic0IPv6Gateway Vnic1IPv6Gateway Vnic2IPv6Gateway	IPv6 address of the vNIC gateway.	
DNS Servers			
DNS Address*	DNS	Space delimited list of IPv4 or IPv6 addresses of the DNS servers accessible from the management interface.	
DNS Search Domain*	Domain	DNS search domain. The default value is <i>localdomain</i> .	
DNS Security Extensions*	DNSSEC	Options are <i>False</i> , <i>True</i> , or <i>Allow-Downgrade</i> . The default value is <i>False</i> . Select <i>True</i> to use DNS security extensions.	
DNS over TLS*	DNSTLS	Options are <i>False</i> , <i>True</i> , and <i>Opportunistic</i> . The default value is <i>False</i> . Select <i>True</i> to use DNS over TLS.	
Multicast DNS*	mDNS	Options are <i>False</i> , <i>True</i> , and <i>Resolve</i> . Select <i>True</i> to use multicast DNS. The default value is <i>False</i> .	If you choose <i>Resolve</i> , only resolution support is enabled. Responding is disabled.

Label	Key	Description	Additional information
Link-Local Multicast Name Resolution *	LLMNR	Options are <code>False</code> , <code>True</code> , <code>Opportunistic</code> , or <code>Resolve</code> . The default value is <code>False</code> .	If you choose <code>Resolve</code> , only resolution support is enabled. Responding is disabled. Select <code>True</code> to use link-local multicast name resolution.
NTPv4 Servers			
NTPv4 Servers *	NTP	Space-delimited list of IPv4, IPv6 addresses, or hostnames of the NTPv4 servers accessible in the management interface.	You must enter value here, such as <code>pool.ntp.org</code> . NTP server is critical for time synchronization between the Data Gateway VM, Crosswork, and devices. Using a nonfunctional or dummy address may cause issues when Cisco Crosswork and Crosswork Data Gateway try to communicate with each other. If you are not using an NTP server, ensure that time gap between Crosswork Data Gateway and Crosswork is not more than 10 minutes. Else, Data Gateway fails to connect.
NTPv4 Authentication	NTPAuth	Select <code>True</code> to use NTPv4 authentication. The default value is <code>False</code> .	

Label	Key	Description	Additional information
NTPv4 Keys	<code>NTPKey</code>	Key IDs to map to the server list. Enter a space-delimited list of Key IDs.	
NTPv4 Key File URI	<code>NTPKeyFile</code>	SCP URI to the chrony key file.	
NTPv4 Key File Passphrase	<code>NTPKeyFilePwd</code>	Password of SCP URI to the chrony key file.	
Remote Syslog Server			

Label	Key	Description	Additional information
Remote Syslog Server*	UseRemoteSyslog	Options are <code>True</code> and <code>False</code> . Select <code>True</code> to send Syslog messages to a remote host. The default value is <code>False</code> .	Configuring an external syslog server sends service events (CLMDSNMP) to the external syslog server. Otherwise, they are logged only to the Crosswork Data Gateway VM. If you want to use an external syslog server, specify the following settings: <ul style="list-style-type: none"> • Use Remote Syslog Server • Syslog Server Address • Syslog Server Port • Syslog Server Protocol
Syslog Server Addresses	SyslogAddress	Hostname, IPv4, or IPv6 address of a syslog server accessible in the management interface.	
Syslog Server Port	SyslogPort	Port number of the syslog server. The default port number is 514.	
Syslog Server Protocol	SyslogProtocol	Options are <code>UDP</code> , <code>REL</code> , or <code>TCP</code> to send the syslog. The default value is <code>UDP</code> .	
Syslog Multiserver Mode	SyslogMultiserverMode	Multiple servers in the failover or simultaneous mode. This parameter is applicable only when the protocol is set to a non-UDP value. UDP must use the simultaneous mode. Options are <code>Simultaneous</code> or <code>Failover</code> . The default value is <code>Simultaneous</code> .	
Syslog over TLS	SyslogTLS	Select <code>True</code> to use TLS to encrypt syslog traffic. The default value is <code>False</code> .	
Syslog TLS Peer Name	SyslogPeerName	Syslog server hostname exactly as entered in the server certificate SubjectAltName or subject common name.	
Syslog Root Certificate File URI	SyslogCertChain	PEM formatted root cert of syslog server retrieved using SCP. The host with the URI files must be reachable on the network (from vNIC0 interface via SCP) and the files must be present at the time of install.	
Syslog Certificate File Passphrase	SyslogCertChainPwd	Password of SCP user to retrieve Syslog certificate chain.	
Remote Auditd Server			

Label	Key	Description	Additional information
Remote auditd Server*	UseRemoteAuditd	Options are <code>True</code> and <code>False</code> . The default value is <code>False</code> . Select <code>True</code> to send auditd messages to a remote host.	If desired, you can configure an external Auditd server. Crosswork Data Gateway sends audit notifications to the Auditd server when configured and present on the network. 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. The default port is 60.	
Controller and Proxy Settings			
Crosswork Controller IP*	ControllerIP	The Virtual IP address or the hostname of the Cisco Crosswork cluster. Note If you are using an IPv6 address, it must be surrounded by square brackets ([1::1]). For <code>ControllerIP</code> in geo redundancy enabled environment, see Table 3: Geo redundancy parameters, on page 15 .	This is required so that the Data Gateway can enroll with the Crosswork server during the installation and initial start up. Excluding this step requires you to manually ingest the certificate. For more information, see Import Controller Signing Certificate File, on page 37 .
Crosswork Controller Port*	ControllerPort	Port of the Cisco Crosswork controller. The default port is 30607.	

Label	Key	Description	Additional information
Controller Signing Certificate File URI*	ControllerSignCertChain	<p>PEM formatted root cert of Cisco Crosswork to validate signing certs retrieved using SCP. Cisco Crosswork generates the PEM file and is available at</p> <pre>cwadmin@Crosswork_VManagement_VIP_address>/usr/cwadmin/controller/gen</pre> <p>The certificate is in the format.</p> <pre>-----BEGIN CERTIFICATE----- MIIC... -----END CERTIFICATE-----</pre> <p>Note If you are using an IPv6 address, it must be surrounded by square brackets ([1::1]).</p> <p>For ControllerSignCertChain in geo redundancy enabled environment, see Table 3: Geo redundancy parameters, on page 15.</p>	<p>Crosswork Data Gateway requires the Controller Signing Certificate File to enroll automatically with Cisco Crosswork.</p> <p>If you specify these parameters during the installation, the certificate file is imported once Data Gateway boots up for the first time.</p> <p>If you do not specify these parameters during installation, then import the certificate file manually by following the procedure Import Controller Signing Certificate File, on page 37.</p>
Controller SSL/TLS Certificate File URI	ControllerTlsCertChain	Cisco Crosswork Controller PEM formatted SSL/TLS certificate file retrieved using SCP.	
Controller Certificate File Passphrase*	ControllerCertChainPwd	Password of SCP user (cw-admin) to retrieve Cisco Crosswork certificate chain.	

Label	Key	Description	Additional information
Proxy Server URL	ProxyURL	URL of the HTTP proxy server.	<p>The proxy parameters apply to the Crosswork Data Gateway cloud deployment.</p> <p>The Data Gateway must connect to the Internet via TLS, and a proxy server may be required if it is not present in your environment.</p> <p>If you want to use a proxy server, specify these parameters.</p>
Proxy Server Bypass List	ProxyBypass	Comma-delimited list of addresses and hostnames that will not use the proxy server.	
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.	

Table 3: Geo redundancy parameters

Label	Key	Description	Additional information
Crosswork Controller IP*	ControllerIP	Use FQDN as the unified endpoint. For more information, see Unified Endpoint Requirements .	

Label	Key	Description	Additional information
Controller Signing Certificate File URI*	ControllerSignCertChain	<p>PEM formatted root certificate of Cisco Crosswork to validate signing certs retrieved using SCP.</p> <p>Cisco Crosswork generates the PEM file and is available at <code>admin@<Crosswork_VM_management_fqdn_address>:/home/cw-admin/controller.pem</code>.</p> <p>The certificate is in the <code>prop:ControllerSignCertChain=cw-admin:\${ControllerIP};/home/cw-admin/controller.pem</code> format.</p>	<p>Crosswork Data Gateway requires the Controller Signing Certificate File to enroll automatically with Cisco Crosswork.</p> <p>If you specify these parameters during the installation, the certificate file is imported once Data Gateway boots up for the first time.</p> <p>If you do not specify these parameters during installation, then import the certificate file manually by following the procedure Import Controller Signing Certificate File, on page 37.</p>

Install Crosswork Data Gateway using vCenter vSphere Client

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

**Note**

- We have included sample images of Crosswork Data Gateway on-premise Standard deployment in the procedure.
- Depending on the vCenter version, the layout and order of fields on the vCenter vSphere screens can vary.
- Leave values blank or use the default unless they are required by the installer (indicated with an asterisk *) or specific to your environment, such as certificates.

Before you begin**Warning**

The default VMware vCenter deployment timeout is 15 minutes. If the time taken to fill the OVF template exceeds 15 minutes, vCenter times out and you have to start over again. To prevent this behavior, it is recommended that you plan for the installation by having the necessary parameters and requirements ready. Refer to the [Table 2: Crosswork Data Gateway Deployment Parameters and Scenarios, on page 4](#) for list of mandatory and optional parameters.

Procedure

-
- Step 1** Download the Crosswork Data Gateway UEFI OVA image file from cisco.com (*.ova). For the 7.1 release, download **cdg-deployment-7.1.0-17.ova**.
- Step 2** Connect to vCenter vSphere Client and select **Actions > Deploy OVF Template**.
- Step 3** The VMware **Deploy OVF Template** wizard appears and highlights the first step, **1 Select template**.
- a) Click **Browse** to navigate to the location where you downloaded the OVA image file and select it.
- Once selected, the filename is displayed in the window.

Figure 1: OVF template selection

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

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

URL

http | https://remoteserver-address/filetodeploy.ovf | .ova

Local file

cdg-deployment-7.1.0-17.ova

CANCEL BACK NEXT

Step 4

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

- Enter a unique name for the VM that you are creating.
- In the **Select a location for the virtual machine** list, choose the data center under which the VM resides.

Figure 2: Name and folder selection

Deploy OVF Template

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

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

Virtual machine name: Crosswork Data Gateway

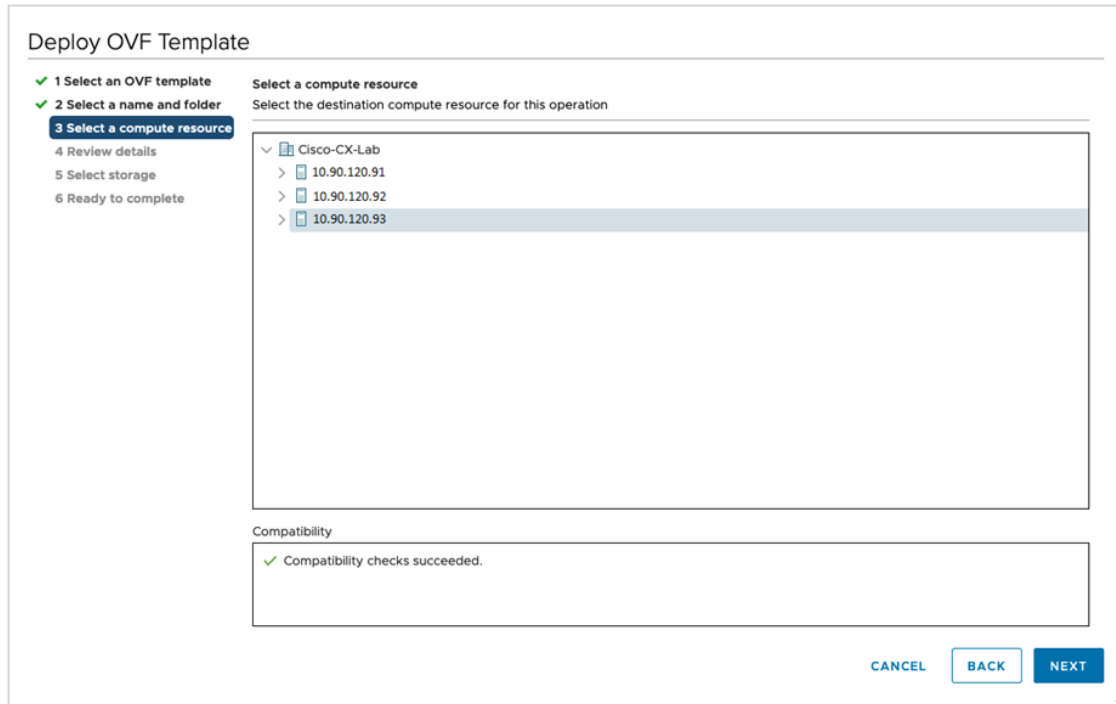
Select a location for the virtual machine.

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

CANCEL BACK NEXT

Step 5 Click **Next** to go to **3 Select a computer resource**. Choose the VM's host or cluster.

Figure 3: Computer resource

**Step 6**

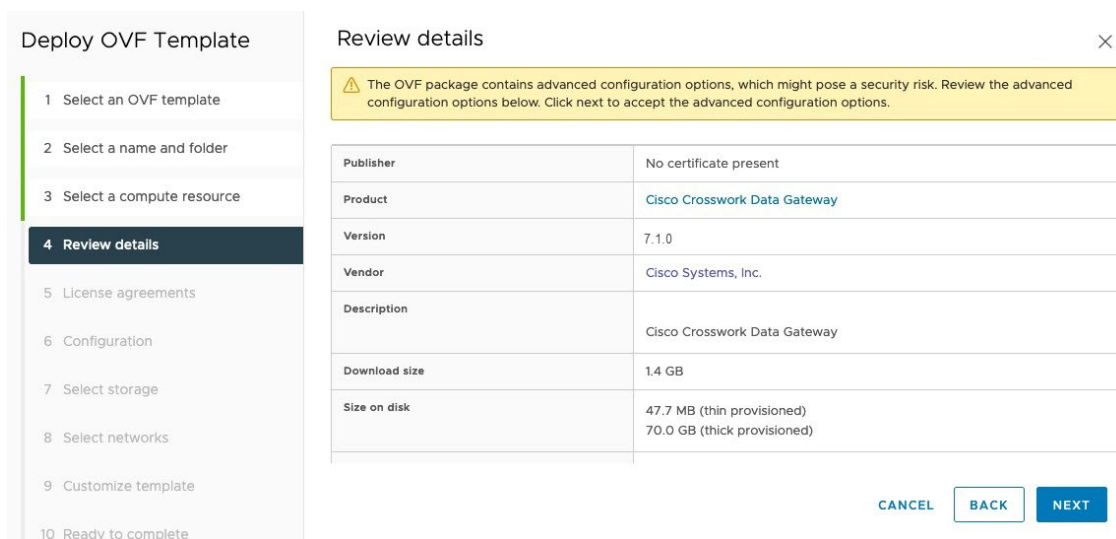
Click **Next**. The VMware vCenter Server validates the OVA. Network speed determines how long validation takes. When the validation is complete, the wizard moves to **4 Review details**.

Take a moment to review the OVF template to make sure it matches the version that you want to install and click **Next**.

Note

This information is gathered from the OVF and cannot be modified.

Figure 4: Review details



Step 7 Click **Next** to go to **5 License agreements**. Review the end-user license agreement, and then click **Accept** if you agree with the conditions. Contact your Cisco representative if you do not agree with the conditions.

Step 8 Click **Next** to go to **6 Configuration**, as shown in the following figure. Select **Crosswork On-Premise Standard** or **Crosswork On-Premise Extended**. See [Crosswork Data Gateway deployment type](#) for more information.

Figure 5: Deployment configuration

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 type="radio"/> Crosswork Cloud	
<input checked="" type="radio"/> Crosswork On-Premise Standard	12 CPU; 48GB RAM; 1-3 NICs; 60GB Disk
<input type="radio"/> Crosswork On-Premise Extended	
<input type="radio"/> Crosswork On-Premise Standard With Extra Resources	

4 Items

CANCEL BACK NEXT

Note

Crosswork Network Controller deployments do not support the Crosswork On-Premise Standard with the extra resources option or any Crosswork Cloud configurations.

Step 9 Click **Next** to go to **7 Select storage**, as shown in the following figure.

- a) Cisco recommends that you select **Thick provision lazy zeroed** from the **Select virtual disk format** drop-down list.
- b) From the **Datastores** table, choose the data store you want to use and review its properties to ensure that there is enough available storage. For Crosswork On-Premise Standard deployment, the storage requirement is 70 GB and for Crosswork On-Premise Extended, it is 570 GB.

Figure 6: Storage selection

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	119 TB	1.46 TB	VM

Compatibility

Compatibility checks succeeded.

CANCEL **BACK** **NEXT**

Step 10

Click **Next** to go to **8 Select networks**, as shown in the following figure. From the drop-down, select the network for each vNIC you plan to use. Leave any unused vNICs configured for the default value. For example,

- 2 NIC: Select the appropriate Destination Network for vNIC0 and vNIC1.
- 3 NIC: Select the appropriate Destination Network for vNIC0, vNIC1, and vNIC2.
- Crosswork does not support the **vNIC3** network.

Note

Leave the vNIC3 set to the default value as it is unused.

Figure 7: Network selection

Deploy OVF Template

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

Select networks
Select a destination network for each source network.

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

4 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL
BACK
NEXT

Step 11

Click **Next** to go to **9 Customize template**, with the **Host information** already expanded. Enter the information for the parameters as explained in [Table 2: Crosswork Data Gateway Deployment Parameters and Scenarios, on page 4](#).

Note

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

Depending on the NIC deployment, note the following:

- For 2 NIC deployments, configure the IP, subnet, and gateway values for vNIC0 and vNIC1. After the Data Gateway pool is created, the VIP address is assigned as a secondary address on vNIC1.
- For the 3 NIC deployments, configure the IP, subnet, and gateway values for vNIC0 and vNIC1. The VIP address will be assigned to vNIC2 once the Data Gateway is added to a pool.

Note

There are three types of configuration settings:

- a. Required settings: Mandatory values like IP addresses and hostnames.
- b. Optional settings: Use case-dependent fields such as certificates or syslog server details.

- c. Reserved settings: Fields that should remain blank unless explicitly instructed by the Customer Experience team. Ensure only required and relevant optional settings are configured. Do not modify reserved fields unless directed. For more information, see [Crosswork Data Gateway Parameters and Deployment Scenarios](#), on page 2.

Figure 8: Host information

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

01. Host Information 10 settings

a. Hostname * Please enter the server's hostname (dg.localdomain)
CDG01

b. Description *
Please enter a short, user friendly description for display in the Crosswork Controller
CDG 01

c. Crosswork Data Gateway Label
An optional freeform label used by the Crosswork Controller to categorize and group multiple DG instances

d. Allow Usable RFC 8190 Addresses
If an address for vNICO, vNIC1, vNIC2, or vNIC3 falls into a usable range identified by RFC 8190 or its predecessors, reject, accept, or request confirmation during initial configuration
Yes

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

f. Crosswork Data Gateway Certificate File ID

CANCEL BACK NEXT

For creating pools in the VMware environment, select L2 and specify IP addresses for creating the HA pool.

Figure 9: High availability network details

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

Please enter the SCP user passphrase to retrieve the Crosswork Data Gateway PEM formatted certificate file and private key

Password _____

Confirm Password _____

h. Data Disk Size Data disk size in GB mounted as /opt/dg/appdata
24

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

j. High Availability Network Mode
Select the network mode to use with external load balancers. This will determine whether all interfaces require an address.
✓ L2
L3

02. Passphrases 2 settings

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

Password _____

Confirm Password _____

- a. Configure the vNIC Role Assignment based on the number of NICs that you have decided to use. Based on the number of NICs, refer to the following to use the customized template configuration:

Note

The default configuration is for 3 NIC deployment.

- See [Deploy OVF Template - Customize Template for 2 vNICs deployment](#).
- See [Deploy OVF Template - Customize Template for 3 vNICs deployment](#).

Figure 10: Customize Template for 2 vNICs deployment

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 <li style="background-color: #0070C0; color: white; padding: 2px;">9 Customize template 10 Ready to complete 	<table border="1"> <tr> <td style="background-color: #D9E1F2;">v 03. vNIC Role Assignment</td> <td style="background-color: #D9E1F2;">7 settings</td> </tr> <tr> <td>a. Default Gateway</td> <td>The interface used as the Default Gateway and for DNS and NTP traffic <input type="text" value="eth0"/></td> </tr> <tr> <td>b. Administration</td> <td>The interface used for SSH access to the VM <input type="text" value="eth0"/></td> </tr> <tr> <td>c. External Logging</td> <td>The interface used to send logs to an external logging server <input type="text" value="eth0"/></td> </tr> <tr> <td>d. Management</td> <td>The interface used for enrolment and other management traffic <input type="text" value="eth0"/></td> </tr> <tr> <td>e. Control</td> <td>The interface used for destination, device, and collection configuration <input type="text" value="eth1"/></td> </tr> <tr> <td>g. Northbound External Data</td> <td>The interface used to send collection data to external destinations <input type="text" value="eth1"/></td> </tr> <tr> <td>h. Southbound Data</td> <td>The interface used collect data from all devices <input type="text" value="eth1"/></td> </tr> </table>	v 03. vNIC Role Assignment	7 settings	a. Default Gateway	The interface used as the Default Gateway and for DNS and NTP traffic <input type="text" value="eth0"/>	b. Administration	The interface used for SSH access to the VM <input type="text" value="eth0"/>	c. External Logging	The interface used to send logs to an external logging server <input type="text" value="eth0"/>	d. Management	The interface used for enrolment and other management traffic <input type="text" value="eth0"/>	e. Control	The interface used for destination, device, and collection configuration <input type="text" value="eth1"/>	g. Northbound External Data	The interface used to send collection data to external destinations <input type="text" value="eth1"/>	h. Southbound Data	The interface used collect data from all devices <input type="text" value="eth1"/>
v 03. vNIC Role Assignment	7 settings																
a. Default Gateway	The interface used as the Default Gateway and for DNS and NTP traffic <input type="text" value="eth0"/>																
b. Administration	The interface used for SSH access to the VM <input type="text" value="eth0"/>																
c. External Logging	The interface used to send logs to an external logging server <input type="text" value="eth0"/>																
d. Management	The interface used for enrolment and other management traffic <input type="text" value="eth0"/>																
e. Control	The interface used for destination, device, and collection configuration <input type="text" value="eth1"/>																
g. Northbound External Data	The interface used to send collection data to external destinations <input type="text" value="eth1"/>																
h. Southbound Data	The interface used collect data from all devices <input type="text" value="eth1"/>																

For 3 vNIC deployments, you can leave the settings with the default values.

Figure 11: Customize template for 3 vNICs deployment

<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 <li style="background-color: #0070C0; color: white; padding: 2px;">9 Customize template 10 Ready to complete 	<table border="1"> <tr> <td style="background-color: #D9E1F2;">v 03. vNIC Role Assignment</td> <td style="background-color: #D9E1F2;">7 settings</td> </tr> <tr> <td>a. Default Gateway</td> <td>The interface used as the Default Gateway and for DNS and NTP traffic <input type="text" value="eth0"/></td> </tr> <tr> <td>b. Administration</td> <td>The interface used for SSH access to the VM <input type="text" value="eth0"/></td> </tr> <tr> <td>c. External Logging</td> <td>The interface used to send logs to an external logging server <input type="text" value="eth0"/></td> </tr> <tr> <td>d. Management</td> <td>The interface used for enrolment and other management traffic <input type="text" value="eth0"/></td> </tr> <tr> <td>e. Control</td> <td>The interface used for destination, device, and collection configuration <input type="text" value="eth1"/></td> </tr> <tr> <td>g. Northbound External Data</td> <td>The interface used to send collection data to external destinations <input type="text" value="eth1"/></td> </tr> <tr> <td>h. Southbound Data</td> <td>The interface used collect data from all devices <input type="text" value="eth2"/></td> </tr> </table>	v 03. vNIC Role Assignment	7 settings	a. Default Gateway	The interface used as the Default Gateway and for DNS and NTP traffic <input type="text" value="eth0"/>	b. Administration	The interface used for SSH access to the VM <input type="text" value="eth0"/>	c. External Logging	The interface used to send logs to an external logging server <input type="text" value="eth0"/>	d. Management	The interface used for enrolment and other management traffic <input type="text" value="eth0"/>	e. Control	The interface used for destination, device, and collection configuration <input type="text" value="eth1"/>	g. Northbound External Data	The interface used to send collection data to external destinations <input type="text" value="eth1"/>	h. Southbound Data	The interface used collect data from all devices <input type="text" value="eth2"/>
v 03. vNIC Role Assignment	7 settings																
a. Default Gateway	The interface used as the Default Gateway and for DNS and NTP traffic <input type="text" value="eth0"/>																
b. Administration	The interface used for SSH access to the VM <input type="text" value="eth0"/>																
c. External Logging	The interface used to send logs to an external logging server <input type="text" value="eth0"/>																
d. Management	The interface used for enrolment and other management traffic <input type="text" value="eth0"/>																
e. Control	The interface used for destination, device, and collection configuration <input type="text" value="eth1"/>																
g. Northbound External Data	The interface used to send collection data to external destinations <input type="text" value="eth1"/>																
h. Southbound Data	The interface used collect data from all devices <input type="text" value="eth2"/>																

Figure 12: Controller settings

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

16. Controller Settings 11 settings

a. Crosswork Controller IP *
Please enter the hostname, IPv4 address, or IPv6 address of the Crosswork Controller accessible from the Default Gateway role

b. Crosswork Controller Port *
Please enter the port number of the Crosswork Controller
30607

c. Controller Signing Certificate File URI
Please enter the optional Crosswork Controller PEM formatted signing certificate file URI retrieved using SCP (user@host:/path/to/file)

d. Controller SSL/TLS Certificate File URI
Please enter the optional Crosswork Controller PEM formatted SSL/TLS certificate file URI retrieved using SCP (user@host:/path/to/file)

e. Controller Certificate File Passphrase
Please enter the SCP user passphrase to retrieve the Crosswork Controller PEM formatted certificate file
Password

CANCEL BACK NEXT

Step 12 Click **Next** to go to **10 Ready to complete**. Review your settings and then click **Finish**.

Figure 13: Review the configuration details

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**

Ready to complete
Click Finish to start creation.

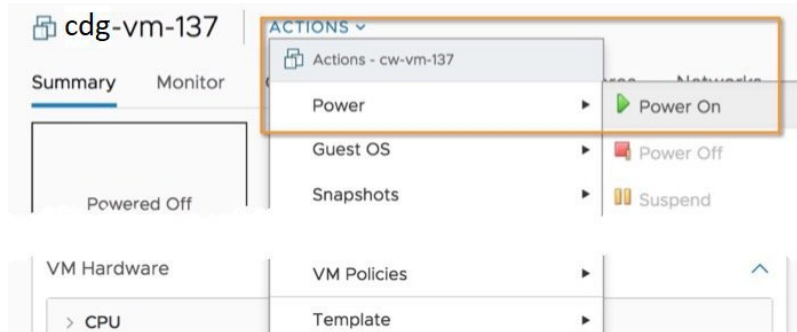
Provisioning type	Deploy from template
Name	CDG02
Template name	dg
Download size	1.4 GB
Size on disk	70.0 GB
Folder	Cisco-CX-Lab
Resource	10.90.147.99
Storage mapping	1
All disks	Datastore: Datastore2; Format: Thick provision lazy zeroed
Network mapping	4
vNIC3	Crosswork-Devices
vNIC2	Crosswork-Devices
vNIC1	Crosswork-Devices
vNIC0	VM Network

CANCEL BACK FINISH

Step 13

Once the deployment status is 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:

Figure 14: Power on VM



Wait for at least 5 minutes for the VM to come up and then log in via 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. The settings have been validated to provide the best network performance. Change these settings at your own risk.

What to do next

- After you log in, the Data Gateway presents you with the welcome screen and options menu indicating that the installation was completed successfully. For information on how to log in, see [Log in and Log out of the Data Gateway VM, on page 29](#).
Log out and proceed with the post-installation tasks that are documented in the *Cisco Crosswork Network Controller 7.1 Administration Guide*.
- Ensure that each Data Gateway is successfully installed and validated before proceeding to the next. Do not begin creating pools until all Data Gateways are confirmed to be built correctly.

Return to the installation workflow: [Install Cisco Crosswork Network Controller on VMware vCenter](#)

Install Crosswork Data Gateway via the OVF Tool

Modify the list of mandatory and optional parameters in the script as per your requirements and run the OVF Tool. Refer to [Table 2: Crosswork Data Gateway Deployment Parameters and Scenarios, on page 4](#) for the list of installation parameters and their default values.



Note The filenames mentioned in this topic are sample names and may differ from the actual filenames on cisco.com.

Follow these steps to log in to the Data Gateway VM from SSH:

Before you begin

- In your vCenter data center, go to **Host > Configure > Networking > Virtual Switches** and select the virtual switch.
- In the virtual switch, select **Edit > Security**, and ensure that the following DVS port group properties are as shown:
 - Set **Promiscuous mode** as Reject
 - Set **MAC address changes** as Reject

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

Procedure

-
- Step 1** On the machine where you have the OVFtool installed, use the following command to confirm that you have OVFtool version 4.4:
- ```
ovftool --version
```
- Step 2** Download the OVA and the sample script files from [cisco.com](http://cisco.com). For these instructions, we use the filename as **cdg-deployment-7.1.0-17.ova**.
- Step 3** Use the following command to extract the files from the tar bundle:
- ```
tar -xvzf cdg-7.1.0-sample-install-scripts.tar.gz
```
- The file bundle is extracted. It includes the **cdg-7.1.0-sample-install-scripts.tar.gz** file and scripts for validating the samples install scripts.
- Step 4** Use the following command to extract the install scripts from the tar bundle:
- ```
tar -xvzf cdg-7.1.0-sample-install-scripts.tar.gz
```
- Step 5** Review the contents of the README file to understand the components that are in the package and how they are validated.
- Step 6** Choose the sample script that corresponds to the deployment you plan to use. Cisco provides sample scripts for 1, 2, and 3 vNIC deployments, which you may optimize to meet your needs.
- Sample scripts for 3 vNIC deployments. Customize the script for the type of deployment that you have planned. For more information, see the sample scripts:
- [Sample Script for Deploying Crosswork Data Gateway with IPv4 Address](#)
  - [Sample Script for Deploying Crosswork Data Gateway with IPv6 Address](#)
  - [Sample Script for Crosswork Data Gateway Dual-Stack Deployment](#)
  - [Sample Script for Crosswork Data Gateway Dual-Stack Deployment with Geo-Redundancy](#)
- Step 7** Use the following command to make the script executable:
- ```
chmod +x {filename}
```
- Step 8** Use the following command to execute the script from the directory where the OVA and script files are stored:
- ```
./{script name} {path and ova file name}
```

For example:

```
./<script name> <Absolute path to cdg-deployment-7.1.0-17.ova>
```

### Step 9

If the values provided in the script are valid, provide the vCenter user's password when you are prompted.

If the script fails due to invalid values, a message like the following is displayed:

```
admin@nso-576-tsdn-410-ai0:~/CDG_Install$./three-nic
/home/admin/CDG_Install/cdg-deployment-7.1.0-17.ova
Opening OVA source: /home/admin/CDG_Install/cdg-deployment-7.1.0-17.ova
The manifest does not validate
Warning:
- Line -1: Unsupported value 'firmware' for attribute 'key' on element 'ExtraConfig'.
- Line -1: Unsupported value 'uefi.secureBoot.enabled' for attribute 'key' on element 'ExtraConfig'.
Enter login information for target vi://rcdn5-spm-vc-01.cisco.com/
Username: johndoe
Password: *****
```

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

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

When the installation is complete, the Data Gateway VM is powered on, is automatically configured based on the settings that you have provided in the script, and registers with the Crosswork cluster.

---

### What to do next

Log in to the VM. For more information, see [Log in and Log out of the Data Gateway VM, on page 29](#). After you log in, the Data Gateway should present you with the welcome screen, and options menu indicating that the installation is complete. Log out and proceed with the postinstallation tasks explained in [Crosswork Data Gateway Post-installation Tasks, on page 32](#).

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

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

- [Access Crosswork Data Gateway VM from SSH, on page 29](#)
- [Access Crosswork Data Gateway through vCenter, on page 30](#)

To log out from the Data Gateway VM, see [Log Out of Crosswork Data Gateway VM, on page 31](#).

## Access Crosswork Data Gateway VM from SSH

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

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

### Procedure

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

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

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

For example,

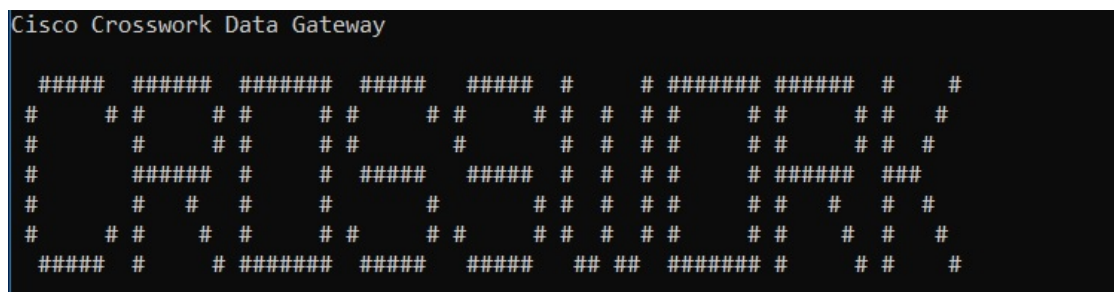
To login as administrator user: `ssh dg-admin@<ManagementNetworkIP>`

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

**Step 2** Provide the corresponding password, which was created during installation process, and press **Enter**.

The Crosswork Data Gateway flash screen opens prompting for password.

*Figure 15: Crosswork screen*



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

## Access Crosswork Data Gateway through vCenter

Follow these steps to log in via vCenter:

### Procedure

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

The Crosswork Data Gateway console comes up.

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

The Crosswork Data Gateway flash screen opens prompting for password.

Figure 16: Crosswork screen

```

Cisco Crosswork Data Gateway

#
#
#
###
#
#
#

```

## Log Out of Crosswork Data Gateway VM

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

## Crosswork Data Gateway Authentication and Enrollment

Once the Crosswork Data Gateway is installed, it identifies itself and enrolls with Cisco Crosswork automatically. Cisco Crosswork then instantiates a new Data Gateway instance in its database and waits for a "first-sign-of-life" from the Data Gateway VM.

After the connectivity is established, the Data Gateway instance confirms the identity of the controller application (Cisco Crosswork) and offers its own proof of identity via signed certificates. Crosswork Data Gateway then downloads the configuration files and functional images (collection profiles) from Cisco Crosswork.

To verify if the Data Gateway VM has enrolled successfully with Cisco Crosswork:

1. Log in to the Cisco Crosswork UI. See [Log into the Cisco Crosswork UI](#).
2. Navigate to **Administration > Data Gateway Management**.
3. Click on the **Data Gateway Instances** tab.

All the Data Gateway VMs that have successfully enrolled with Cisco Crosswork are displayed here.

The initial **Operational State** of Data Gateway VMs is **Unknown**. During the handshake and image download, the status is **Degraded**. After the handshake is complete, the status is **Not Ready**. While it depends on the bandwidth between the Data Gateway VMs and Cisco Crosswork, this operation typically takes between 5 to 10 minutes. If it takes longer than the stipulated duration, contact Cisco Customer Experience team for assistance.

For information about the different operational states of the VMs, see the *Overview of Cisco Crosswork Data Gateway* section in the [Cisco Crosswork Network Controller 7.1 Administration Guide](#).



**Note** The Data Gateway VMs that have the **Role** as **Unassigned** must be assigned to a pool before they can be used. A Data Gateway VM is your physical Data Gateway. You cannot attach or detach devices to it. Devices can be attached only to a Data Gateway pool.

**What to do next:**

Return to the installation workflow: [Install Cisco Crosswork Network Controller on VMware vCenter](#)

## Crosswork Data Gateway Post-installation Tasks

After installing Crosswork Data Gateway, configure the timezone of the Data Gateway VM.

- [Configure the timezone of the Crosswork Data Gateway VM, on page 32](#)

**What to do next:**

Return to the installation workflow: [Install Cisco Crosswork Network Controller on VMware vCenter](#)

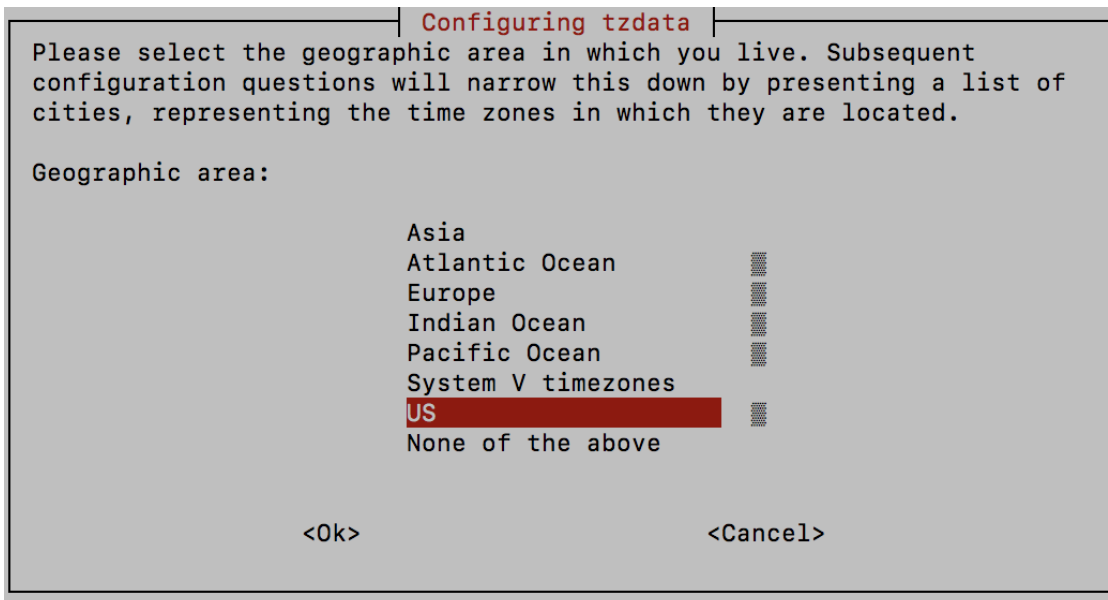
## Configure the timezone of the Crosswork Data Gateway VM

By default, the Crosswork Data Gateway VM launches with the UTC timezone. To ensure that all Data Gateway processes (including Showtech logs) reflect the correct timestamp for your location, update the timezone to match your geographical area.

### Procedure

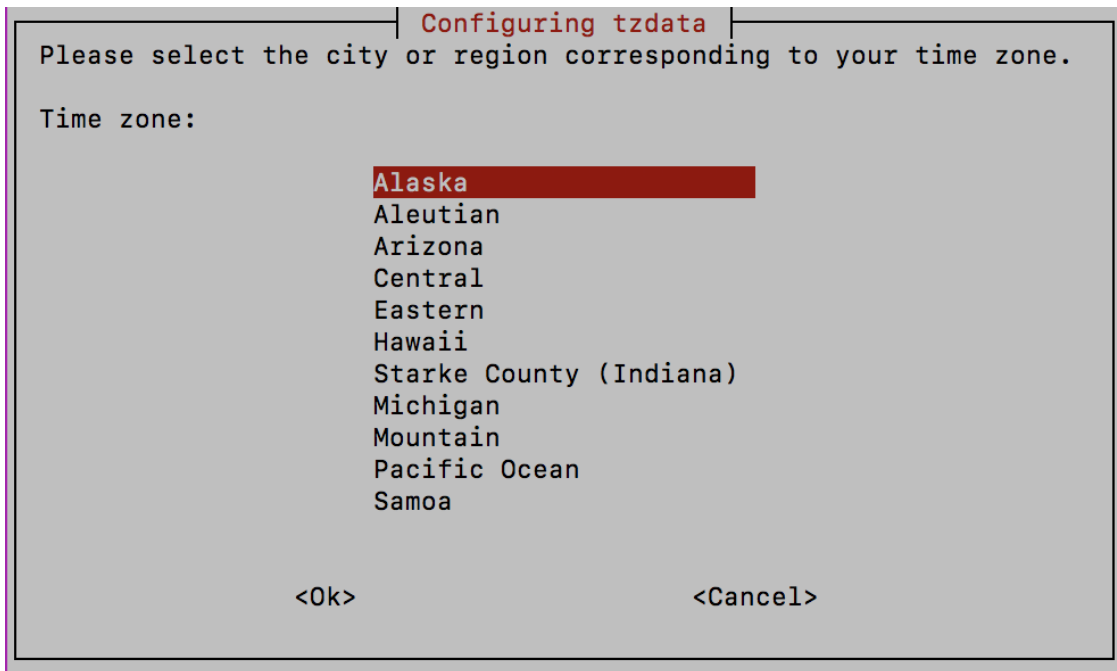
- Step 1** Log in to the Crosswork Data Gateway VM.
- Step 2** In the Crosswork Data Gateway VM interactive menu, select **3 Change Current System Settings**.
- Step 3** From the menu, select **9 Timezone**.
- Step 4** Select the geographical area in which you are located.

*Figure 17: Geographic area selection*



**Step 5** Select the city or region that corresponds to your timezone.

*Figure 18: Region selection*



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

**Step 7** Reboot the Crosswork Data Gateway VM to apply the new timezone to all processes.

**Step 8** Log out of the Crosswork Data Gateway VM.

## Troubleshoot Crosswork Data Gateway Installation and Enrollment

If Crosswork Data Gateway fails to autoenroll with Crosswork Network Controller, you can collect Crosswork Data Gateway show-tech (**Main menu** > **5 Troubleshooting** > **2 Run show-tech**) and check for the reason in `controller-gateway` logs.

For more information on how to collect show-tech logs, see the *Collect show-tech logs from the Interactive Console* section in the *Cisco Crosswork Network Controller 7.1 Administration Guide*. If there are session establishment or certificate-related issues, ensure that the `controller.pem` certificate is uploaded using the Interactive Console.



**Important** When using an IPv6 address, it must be surrounded by square brackets ([1::1]).

The following table lists common problems that might be experienced while installing or enrolling a Data Gateway, and provides approaches to identifying the source of the problem and solving it.

Table 4: Troubleshooting the Installation or Enrollment

| Issue                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Crosswork Data Gateway cannot be enrolled with Crosswork Network Controller due to an NTP issue, that is, there is a clock-drift between the two.</b></p> <p><b>The clock-drift might be with either Crosswork Data Gateway or Crosswork Network Controller.</b></p> <p><b>Also, on the NTP servers for Crosswork Network Controller and Crosswork Data Gateway, the initial time is set to the ESXi server. For this reason, the ESXi server must also have NTP configured.</b></p> <p><b>Sync the clock time on the host and retry.</b></p> | <ol style="list-style-type: none"> <li>1. Log in to the Data Gateway VM.</li> <li>2. From the main menu, select <b>5 Troubleshooting &gt; 2 Run show-tech</b>.<br/>Enter the destination to save the tarball containing logs and vitals and click <b>OK</b>.<br/>The show-tech is now encrypted with a file extension ending with <code>.tar.xz</code>.</li> <li>3. Run the following command to decrypt the show-tech file.<br/><pre>openssl enc -d -AES-256-CBC -pbkdf2 -md sha512 -iter 100000 -in &lt;showtech file&gt; -out &lt;decrypted filename&gt; -pass pass:&lt;encrypt string&gt;</pre><br/>In the show-tech logs (in file <code>session.log</code> at location <code>/opt/dg/log/controller-gateway/session.log</code>), if you see the error <code>UNAUTHENTICATED:invalid certificate. reason: x509: certificate has expired or is not yet valid</code>, then there is a clock-drift between Crosswork Data Gateway and Crosswork Network Controller.</li> </ol> <ol style="list-style-type: none"> <li>3. From the main menu, go to <b>3 Change Current System Settings &gt; 1 Configure NTP</b>.<br/>Configure NTP to sync with the clock time on the Crosswork Network Controller server and try reenrolling Crosswork Data Gateway.</li> </ol> |

| Issue                                                                                                                                                                            | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "Could not collect vitals" due to certificate errors.</b></p>              | <ol style="list-style-type: none"> <li>1. Log in to the Data Gateway VM.</li> <li>2. From the main menu, select <b>5 Troubleshooting &gt; 2 Run show-tech</b>.<br/><br/>Enter the destination to save the tarball containing logs and vitals and click <b>OK</b>.<br/><br/>The show-tech is now encrypted with a file extension ending with .tar.xz.</li> <li>3. Run the following command to decrypt the show-tech file.<br/><br/> <pre>openssl enc -d -AES-256-CBC -pbkdf2 -md sha512 -iter 100000 -in &lt;showtech file&gt; -out &lt;decrypted filename&gt; -pass pass:&lt;encrypt string&gt;</pre> </li> </ol> <p>In the show-tech logs (in file <code>gateway.log</code> at location <code>/opt/dg/log/controller-gateway/gateway.log</code>), if you see certificate errors, then reupload the Controller Signing Certificate, as explained in the following steps:</p> <ol style="list-style-type: none"> <li>1. From the main menu, select <b>3 Change Current System Settings &gt; 7 Import Certificate</b>.</li> <li>2. From the <b>Import Certificates</b> menu, select <b>1 Controller Signing Certificate File</b> and click <b>OK</b>.</li> <li>3. Enter the SCP URI for the certificate file and click <b>OK</b>.</li> </ol> |
| <p><b>Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "gRPC connection cannot be established" due to certificate errors.</b></p> | <ol style="list-style-type: none"> <li>1. Reupload the certificate file using the following steps: <ol style="list-style-type: none"> <li>a. From the main menu, select <b>3 Change Current System Settings &gt; 7 Import Certificate</b>.</li> <li>b. From the <b>Import Certificates</b> menu, select <b>1 Controller Signing Certificate File</b> and click <b>OK</b>.</li> <li>c. Enter the SCP URI for the certificate file and click <b>OK</b>.</li> </ol> </li> <li>2. Reboot the Data Gateway VM: <ol style="list-style-type: none"> <li>a. From the main menu, select <b>5 Troubleshooting</b> and click <b>OK</b>.</li> <li>b. From the Troubleshooting menu, select <b>4 Reboot VM</b> and click <b>OK</b>.</li> <li>c. When the reboot is complete, check if the Data Gateway's operational status is <b>Up</b>.</li> </ol> </li> </ol>                                                                                                                                                                                                                                                                                                                                                                                         |

| Issue                                                                                                                                                                                                                                            | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Crosswork Data Gateway goes into Error state</b>                                                                                                                                                                                              | <ul style="list-style-type: none"> <li>• For vCenter deployment, check the vNIC values in the OVF template and correct them if required.</li> <li>• Before deploying a new Data Gateway instance with the same configuration, delete the existing errored instance. For details on how to delete the instance and its effects on collection jobs, see <a href="#">Delete Crosswork Data Gateway Instance from Crosswork Network Controller</a></li> <li>• If you are redeploying the Data Gateway instance, you must first delete the existing instance that is currently in an error state.<br/>For more information about <ul style="list-style-type: none"> <li>• deleting the instance and its impact on the collection jobs, see <a href="#">Delete Crosswork Data Gateway Instance from Crosswork Network Controller</a></li> <li>• understanding the impact of redeployment on enrollment, see <a href="#">Redeploy a Crosswork Data Gateway Instance</a>.</li> </ul> </li> </ul> |
| <b>Crosswork Data Gateway deploys Standard profile instead of Extended profile</b>                                                                                                                                                               | Check the <code>Deployment</code> parameter in the OVF template in case of vCenter. If <code>Deployment</code> parameter mismatches or does not exist for an Extended profile, then Crosswork Data Gateway deploys the Standard profile by default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>During a Crosswork upgrade, some of the Crosswork Data Gateways may not get upgraded or reenrolled leading to logging multiple error messages in the dg-manager logs.</b>                                                                     | Reenroll or redeploy the Crosswork Data Gateways. For more information, see the <a href="#">Redeploy a Crosswork Data Gateway Instance</a> and <a href="#">Re-enroll Crosswork Data Gateway</a> sections in the <a href="#">Cisco Crosswork Network Controller 7.1 Administration Guide</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>If a Crosswork Data Gateway instance that was previously attached to Crosswork is now reattached to a different Crosswork version 4.x or 5.0, the operational state of the instance may be Degraded with the robot-astack-influxdb error.</b> | <ol style="list-style-type: none"> <li>1. Log in to the Crosswork UI from the SSH.</li> <li>2. Run the Docker executive commands to access the <b>robot-astack-influxdb</b> pod.</li> <li>3. In the pod, navigate to the following directory and delete it:<br/><br/><code>/mnt/dataafs/influxdb</code></li> <li>4. Restart the service using the following command:<br/><br/><code>supervisorctl restart all</code></li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Issue                                                                                                                                                                                                  | Action                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| If a Data Gateway is redeployed without moving the gateway to the Maintenance mode, Crosswork enrollment will be unsuccessful and errors will be logged in the dg-manager and controller-gateway logs. | Move the Data Gateway to the <b>Maintenance</b> mode or manually reenroll the gateway. For more information, see the <a href="#">Re-enroll Crosswork Data Gateway</a> section in the <a href="#">Cisco Crosswork Network Controller 7.1 Administration Guide</a> .                      |
| Crosswork Data Gateway fails to enroll with Cisco Crosswork when the Data Gateway is deployed on a single stack while Crosswork is deployed on dual stack.                                             | Redeploy the Data Gateway on dual stack.<br>For more information, see the <a href="#">Redeploy a Crosswork Data Gateway Instance</a> and <a href="#">Re-enroll Crosswork Data Gateway</a> sections in the <a href="#">Cisco Crosswork Network Controller 7.1 Administration Guide</a> . |

## Import Controller Signing Certificate File

The Controller Certificate file is automatically imported after the VM boots. If there is an import failure, the Data Gateway VM makes several attempts to import the certificate while giving you the option to manually import it.

- You have not specified the **Controller Signing Certificate File URI** under the **Controller Settings** during installation.
- Cisco Crosswork was upgraded or reinstalled and you need to authenticate and enroll Crosswork Data Gateway with Cisco Crosswork.
- Cisco Crosswork configuration is in-progress when Crosswork Data Gateway tries to import the Controller Certificate file.
- The Cisco Crosswork Controller IP address is unreachable or incorrect.
- The Cisco Crosswork username or password is incorrect.

Follow these steps to import the controller signing certificate file:

### Procedure

**Step 1** From the Data Gateway VM's Interactive Menu, select **3 Change Current System Settings**.

The **Change System Settings** menu opens.

**Step 2** Select **7 Import Certificate**.

**Step 3** From the **Import Certificates** menu, select **1 Controller Signing Certificate File**.

**Step 4** Enter the SCP URI for the certificate file.

An example URI is given below:

```
cw-admin@{server ip}:/home/cw-admin/controller.pem
```

**Step 5** Enter the SCP passphrase (the SCP user password).

The certificate file is imported.

**Step 6** Verify that the certificate was installed successfully. See [View the Controller Signing Certificate File, on page 38](#).

---

## View the Controller Signing Certificate File

Follow these steps to view the signing certificate:

### Procedure

---

**Step 1** From the Data Gateway VM's interactive menu, select **2 Show System Settings**.

**Step 2** From the **Show Current System Settings** menu, select **7 Certificates**.

**Step 3** Select **2 Controller Signing Certificate File**.

Crosswork Data Gateway displays the default certificate if no new certificate has been imported. Otherwise, it displays the new certificate if it was successfully imported.

---