Install Cisco Crosswork Data Gateway on VMware vCenter

This chapter contains the following topics:

- Cisco Crosswork Data Gateway Installation Workflow, on page 1
- Log in and Log out of Crosswork Data Gateway VM, on page 33
- Cisco Crosswork Data Gateway Authentication and Enrollment, on page 35
- Crosswork Data Gateway Post-installation Tasks, on page 36
- Troubleshoot Crosswork Data Gateway Installation and Enrollment, on page 37

Cisco Crosswork Data Gateway Installation Workflow

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

Note If you are redeploying the same Cisco Crosswork Data Gateway with Cisco Crosswork, delete the previous Crosswork Data Gateway entry from the Virtual Machine table under Data Gateway Management. For information on how to delete a Crosswork Data Gateway VM, see Delete Crosswork Data Gateway VM from Cisco Crosswork.

To install Crosswork Data Gateway VM for use with Cisco Crosswork, follow these steps:

1. Choose the deployment profile for the Crosswork Data Gateway VM. See Crosswork Data Gateway VM Requirements.
2. Review the installation parameters at Cisco Crosswork Data Gateway Parameters and Deployment Scenarios and make sure that you have all the required information to install Crosswork Data Gateway using your the preferred deployment scenario.
3. Install Cisco Crosswork Data Gateway using yours preferred method:

Table 1: Crosswork Data Gateway installation options

VMware	Install Cisco Crosswork Data Gateway using vCenter vSphere Client, on page 16
	Install Cisco Crosswork Data Gateway via OVF Tool, on page 28

4. Complete the post-installation tasks mentioned in the section Crosswork Data Gateway Post-installation Tasks, on page 36

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

5. Verify that the Crosswork Data Gateway VM has enrolled successfully with Cisco Crosswork. For information on how to verify the enrollment process, see Cisco Crosswork Data Gateway Authentication and Enrollment, on page 35.

After verifying that the Crosswork Data Gateway VM has enrolled successfully with Cisco Crosswork, set up the Crosswork Data Gateway for collection by creating a Crosswork Data Gateway pool. For more information, see the *Create a Crosswork Data Gateway Pool* section in *Cisco Crosswork Network Controller 5.0 Administration Guide*.

Cisco Crosswork Data Gateway Parameters and Deployment Scenarios

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

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

During installation, Cisco Crosswork Data Gateway creates two 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. 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 5.0 Administration Guide*.

The **dg-admin** and **dg-oper** user accounts are reserved user names and cannot be changed. You can change the password in the console for both the accounts. For more information, see the *Change Passphrase* section in *Cisco Crosswork Network Controller 5.0 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, if required.

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.

Table 2: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios

Label	Key	Description	Additional Information
Host Information			
Hostname*	`Hostname`	Name of the Cisco Crosswork Data Gateway VM specified as a fully qualified domain name (FQDN). In larger systems, you are likely to have more than one Cisco Crosswork Data Gateway VM. The host name must, therefore, be unique and created in a way that makes identifying a specific VM easy.	
Description*	`Description`	A detailed description of the Cisco Crosswork Data Gateway.	
Label	`Label`	Label used by Cisco Crosswork to categorize and group multiple Cisco Crosswork Data Gateway VMs.	
Deployment*	`Deployment`	Parameter that conveys the type of controller application that Crosswork Data Gateway is deployed with. For an on-premise installation, it is Crosswork On-Premise. The default value is `Crosswork On-Premise Standard`. All data gateways in a pool must be of the deployment type.	

Label	Key	Description	Additional Information
Profile*	`Profile`	Parameter conveys the VM resource profile. For an on-premise installation, choose either: • `Standard` • `Extended` The default value is `Standard`.	For VMware vCenter, you cannot configure this parameter. The OVF tool configures this parameter with the default value.
AllowRFC8190*	`AllowRFC8190`	Choose how to validate interface addresses that fall in a usable RFC 8190 range. Options are: `Yes`, `No`, or `Ask`, where the initial configuration scripts prompts for confirmation.	The default value is `Yes` to automatically allow interface addresses in an RFC 8190 range.
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`).	Cisco Crosswork uses self-signed certificates for handshake with Cisco Crosswork Data Gateway. These certificates are generated at installation. However, if you want to use third party or your own certificate files, then enter these parameters. Certificate chains override any preset or generated certificates in the Cisco Crosswork Data Gateway VM and are given as an SCP URI (user:host:/path/to/file). The host with the URI files must be reachable on the network (from the vNIC0 interface via SCP) and files must be present at the time of install.
Certificate File and Key Passphrase	`DGCertChainPwd`	Passphrase of the SCP user to retrieve the Cisco Crosswork Data Gateway PEM formatted certificate file and private key.	

Label	Key	Description	Additional Information
Data Disk Size	`DGAppdataDisk`	Indicates the size in GB of a second data disk. The default value of this parameter in each profile is: • 20 GB for Standard. • 520 GB for Extended.	
HA Network Mode*	`HANetworkMode`	Indicates the mode for the HA network. Options are: • L2 • L3 The default value is `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 In a 3-NIC deployment, you need to provide IP address for Management Traffic (vNIC0) and Control/Data Traffic (vNIC1) only. IP address for Device Access Traffic (vNIC2) is assigned during Crosswork Data Gateway pool creation as explained in the *Create a Crosswork Data Gateway Pool* section in *Cisco Crosswork Network Controller 5.0 Administration Guide*. **Note** Selecting **None** in both IPv4 Method and the IPv6 Method fields of the vNIC results in a nonfunctional deployment.			

Label	Key	Description	Additional Information
NicDefaultGateway*	`NicDefaultGateway`	The interface used as the Default Gateway for processing the DNS and NTP traffic. Options are `eth0`, `eth1`, or `eth2`. The default value is `eth0`.	
NicAdministration*	`NicAdministration`	The interface used to access the VM through the SSH access. Options are `eth0`, `eth1`, or `eth2`. The default value is `eth0`.	
NicExternalLogging*	`NicExternalLogging`	The interface used to send logs to an external logging server. Options are `eth0`, `eth1`, or `eth2`. The default value is `eth0`.	
NicManagement*	`NicManagement`	The interface used to send the enrollment and other management traffic. Options are `eth0`, `eth1`, or `eth2`. The default value is `eth0`.	
NicControl*	`NicControl`	The interface used to send the destination, device, and collection configuration. Options are `eth0`, `eth1`, or `eth2`. The default value is `eth1`.	
NicNBExternalData*	`NicNBExternalData`	The interface used to send the collection data to the external destinations. Options are `eth0`, `eth1`, or `eth2`. The default value is `eth1`.	

Label	Key	Description	Additional Information
NicSBData*	`NicSBData`	The interface used to collect data from the devices. Options are `eth0`, `eth1`, or `eth2`. The default value is `eth2`.	
vNIC IPv4 Address (vNIC0, vNIC1, and vNIC2 based on the number of interfaces you choose to use) **Important** If you plan on using 1 NIC, you must configure Crosswork Data Gateway to get an IPv4 or IPv6 address assigned to vNIC0. When using 2 NICs, specify Method (None or Static) and Type (Ipv4 or IPv6) values for vNIC0 and vNC1. For 3 NICs, specify the Method and Type for vNIC0 and vNIC0. If you're not using a vNIC, choose None as the Method value.			

vNIC IPv4 Method*
For example, the parameter name for vNIC0 is vNIC0 IPv4 Method.
	`Vnic0IPv4Method`
	`Vnic1IPv4Method`
	`Vnic2IPv4Method`
		Method in which the interface is assigned an IPv4 address - `None` or `Static`.
		The default value is `None`.
			If you have selected **Method** as:
			• **None**: Skip the rest of the fields for the vNIC IPv4 parameters. Proceed to enter information in the vNIC IPv6 Address parameters.
			• **Static**: Enter information in **Address**, **Netmask**, **Skip Gateway**, and **Gateway** fields

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`
		The default value is `False`.
		Setting this to `True` skips configuring a gateway.	

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

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

Label	Key	Description	Additional Information

vNIC IPv6 Method*	`Vnic0IPv6Method`
	`Vnic1IPv6Method`
	`Vnic2IPv6Method`
		Method in which the vNIC interface is assigned an IPv6 address - `None`, `Static`, or `SLAAC`.
		The default value is `None`.
			If you have selected **Method** as:
			• **None**: Skip the rest of the fields for the vNIC IPv6 parameters. Enter information in the vNIC IPv4 Address parameters.
			• **Static**: Enter information in **Address**, **Netmask**, **Skip Gateway**, and **Gateway** fields
			Do not change the VnicxIPv6Address default values.

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

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

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

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

vNIC Roles			

Label	Key	Description	Additional Information
Default Gateway	DEFAULT_GATEWAY	The interface that allows all types of traffic to flow. This interface is configured using the route metrics. The DNS and NTP traffic uses the DEFAULT_GATEWAY role. The default value is eth0.	For information on the type of roles that you must assign to the vNICs, see Table 3.
Administration	ADMINISTRATION	The SSH traffic uses the Administration role to access the console menu. The default value is eth0.	
External Logging	EXTERNAL_LOGGING	The interface that allows a connection to an external syslog and auditd servers for sending logs. The default value is eth0.	
Management	MANAGEMENT	The interface that allows a connection to dg-manager for enrollment and other management traffic. The default value is eth0.	
Control	CONTROL	The interface that allows a connection to collection service for destination, device, and collection configuration. The default value is eth1.	
NB System Data	NB_SYSTEM_DATA	As the system destinations share the same IP as interface that allows connection to the collection service, the northbound data for system destinations uses the Control role's interface.	
NB External Data	NB_EXTERNAL_DATA		

Label	Key	Description	Additional Information
		The interface that allows connection to the destinations provided by the user. The default value is `eth1`.	
SB Data	`SB_DATA`	The interface that allows a connection to collect the device data. An interface with only the SB Data role does not need an IP during the deployment. The default value is `eth2`.	
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 `localdomain`.	
DNS Security Extensions *	`DNSSEC`	Options are `False`, `True`, or `Allow-Downgrade`. The default value is `False` Select `True` to use DNS security extensions.	
DNS over TLS*	`DNSTLS`	Options are `False`, `True`, and `Opportunistic`. The default value is `False`. Select `True` to use DNS over TLS.	
Multicast DNS*	`mDNS`	Options are `False`, `True`, and `Resolve`. Select `True` to use multicast DNS. The default value is `False`.	If you choose Resolve, only resolution support is enabled. Responding is disabled.

Label	Key	Description	Additional Information
Link-Local Multicast Name Resolution*	`LLMNR`	Options are `False`, `True`, `Opportunistic`, or `Resolve`. The default value is `False`. Select `True` to use link-local multicast name resolution.	If you choose Resolve, only resolution support is enabled. Responding is disabled.
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 a value here, such as pool.ntp.org. NTP server is critical for time synchronization between Crosswork 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, Crosswork Data Gateway fails to connect.
Use NTPv4 Authentication	`NTPAuth`	Select `True` to use NTPv4 authentication. The default value is `False`.	
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.	

Label	Key	Description	Additional Information
Remote Syslog Server			

Label	Key	Description	Additional Information
Use Remote Syslog Server*	`UseRemoteSyslog`	Options are `True` and `False`. Select `True` to send Syslog messages to a remote host. The default value is `False`.	Configuring an external syslog server sends service events (CLI/MDT/SNMP/gNMI) 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, specify the following settings: • Use Remote Syslog Server • Syslog Server Address • Syslog Server Port • Syslog Server Protocol
Syslog Server Address	`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 `UDP`, `RELP`, or `TCP` to send the syslog. The default value is `UDP`.	
Syslog Multiserver Mode	`SyslogMultiserverMode`	Multiple servers in the failover or simultaneous mode. This parameter is applicable only when the protocol is set to a non-UDP value. UDP must use the simultaneous mode. Options are `Simultaneous` or `Failover`. The default value is `Simultaneous`.	
Use Syslog over TLS?	`SyslogTLS`	Select `True` to use TLS to encrypt syslog traffic. The default value is `False`.	
Syslog TLS Peer Name	`SyslogPeerName`	Syslog server hostname exactly as entered in the server certificate SubjectAltName or subject common name.	
Syslog Root Certificate File URI	`SyslogCertChain`		

Label	Key	Description	Additional Information
		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 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			
Use Remote Auditd Server*	`UseRemoteAuditd`	Options are `True` and `False`. The default value is `False`.Select `True` to send auditd messages to a remote host.	If desired, you can configure an external Auditd server. Cisco 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 host name of Cisco Crosswork Cluster. **Note** If you are using an IPv6 address, it must be surrounded by square brackets ([1::1]).	This is required so that the Crosswork Data Gateway can enroll with the Crosswork server during the installation and initial start up. Excluding this step will require you to manually ingest the certificate. For more information, see Import Controller Signing Certificate File, on page 40.
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`	PEM formatted root cert of Cisco Crosswork to validate signing certs retrieved using SCP. Cisco Crosswork generates the PEM file and is available at the following location: `cw-admin@<Crosswork_VM_Management_VIP_Address>:/home/cw-admin/controller.pem`	Crosswork Data Gateway requires the Controller Signing Certificate File to enroll automatically with Cisco Crosswork. If you specify these parameters during the installation, the certificate file is imported once Crosswork Data Gateway boots up for the first time. 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 40.
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.	The proxy parameters apply to the Crosswork Data Gateway cloud deployment. Crosswork Data Gateway must connect to the Internet via TLS, and a proxy server may be required if it is not present in your environment. If you want to use a proxy server, specify these parameters.
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.	

vNIC Role Assignment

Role assignment allows you to control the traffic that an interface must handle. If the preassigned roles don't meet the specific needs of your organization, you can explicitly assign roles to interfaces. For example, you can assign the role 'ADMINISTRATION' to an interface to route only the SSH traffic.

Each parameter has a predefined role. The parameter accepts the interface value as eth0, eth1, or eth2.

Install Cisco Crosswork Data Gateway using vCenter vSphere Client

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

Note We have included sample images of Cisco Crosswork Data Gateway on-premise Standard deployment in the procedure.

Step 1 Download the Cisco Crosswork Data Gateway 5.0 image file from cisco.com (*.ova).

Warning The default VMware vCenter deployment timeout is 15 minutes. If the time taken to fill the OVF template exceeds 15 minutes, vCenter times out and you have to start over again. To prevent this, it is recommended that you plan for the installation by having the necessary parameters and requirements ready. Refer to the Table 2: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 3 for list of mandatory and optional parameters.

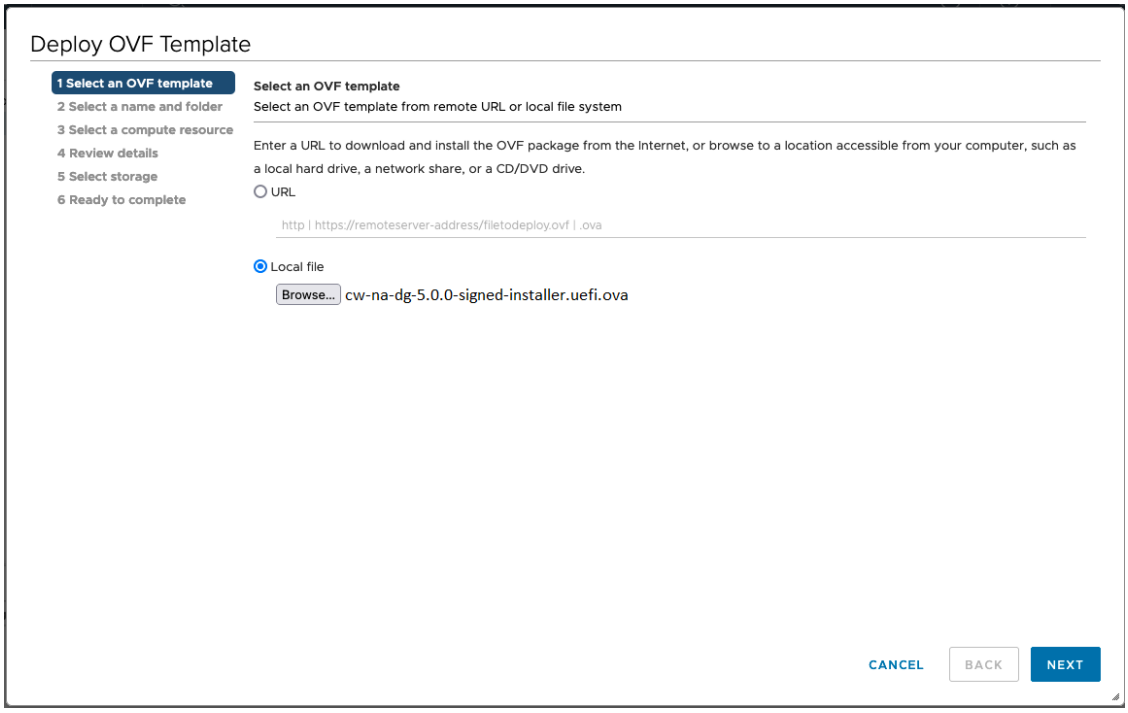
Step 2 Connect to vCenter vSphere Client and select **Actions** > **Deploy OVF Template**.

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 file name is displayed in the window.

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

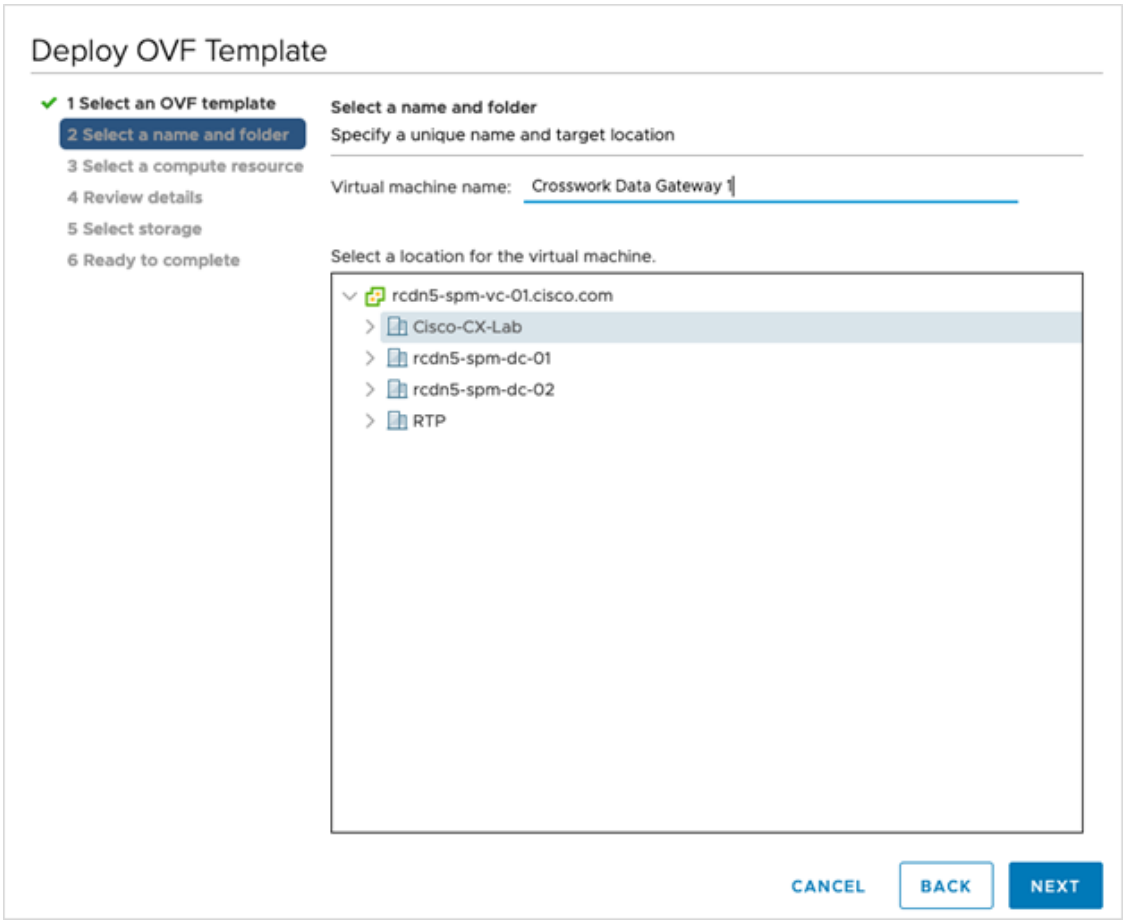


Step 4 Click **Next** to go to **2 Select a name and folder**, as shown in the following figure.

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

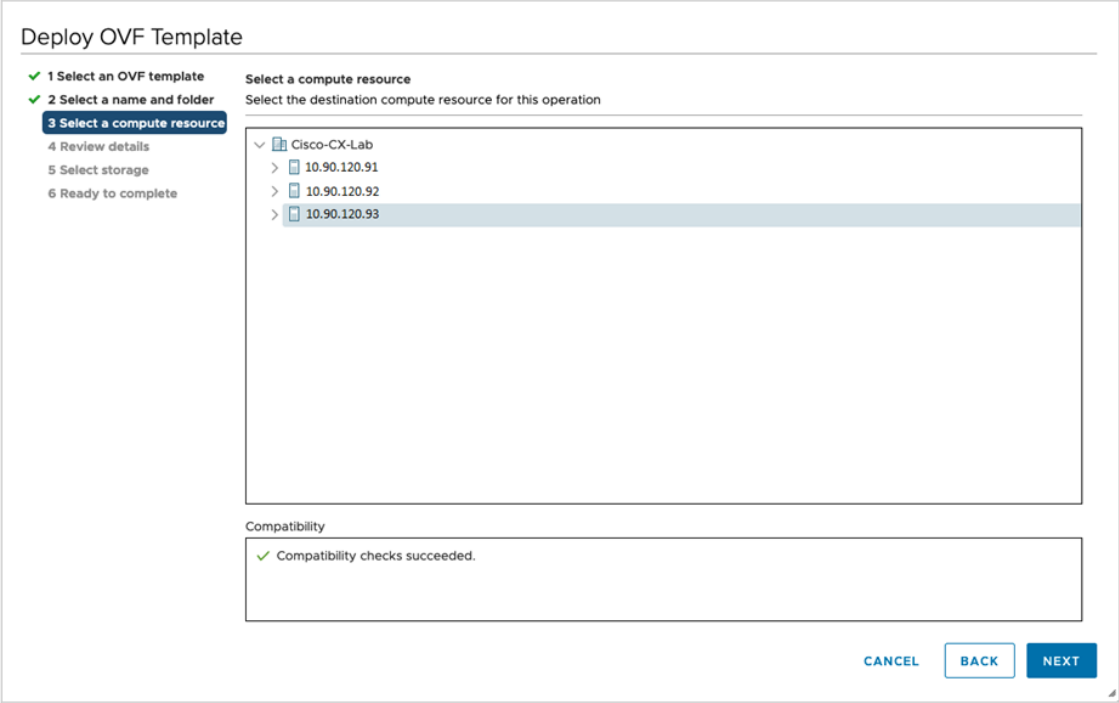
b) In the **Select a location for the virtual machine** list, choose the data center under which the VM resides.

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



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

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

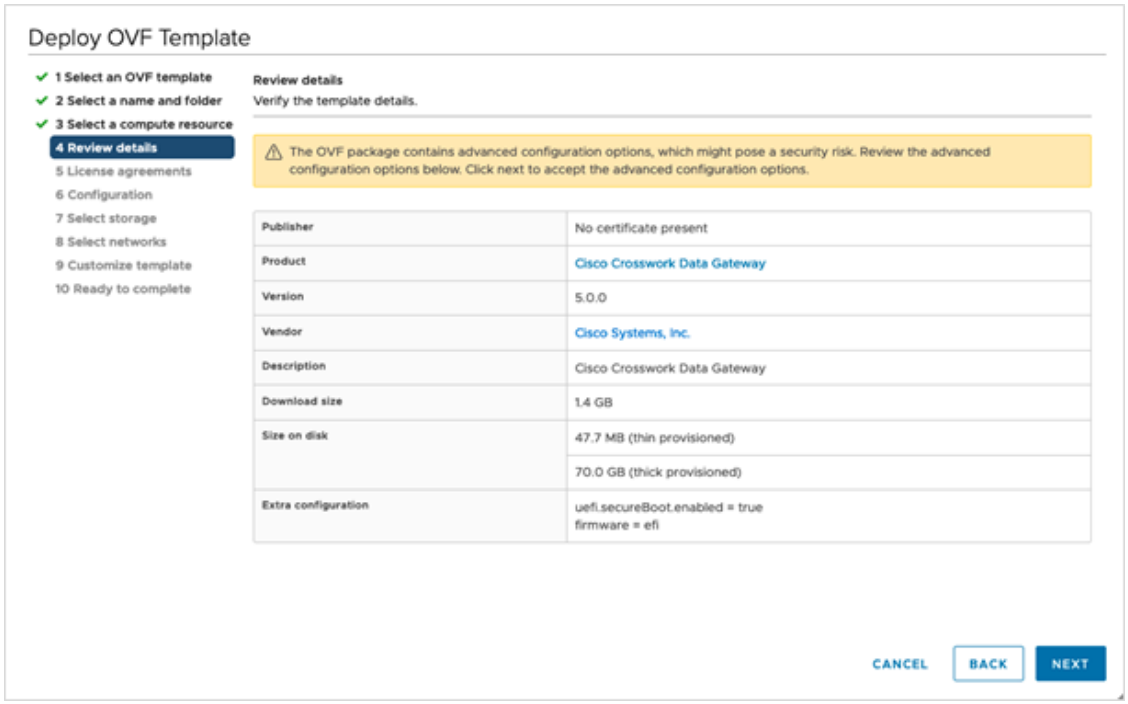


Step 6 Click **Next**. The VMware vCenter Server validates the OVA. Network speed determines how long validation takes. When the validation is complete, the wizard moves to **4 Review details**.

Take a moment to review the OVF template you are deploying and click **Next**.

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

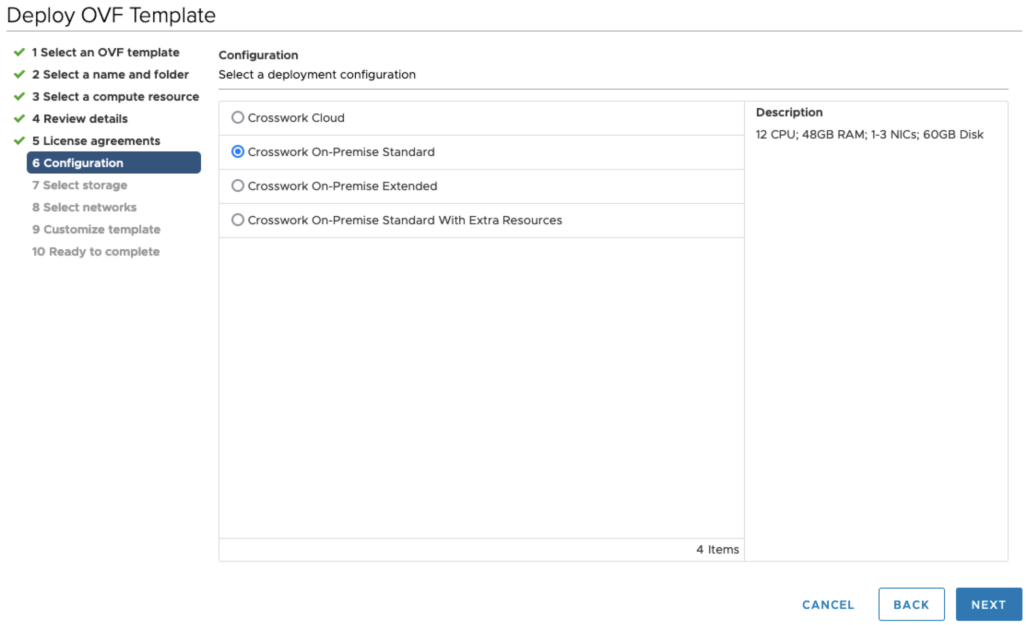
Figure 4: Deploy OVF Template - Review details Window



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 Selecting the Crosswork Data Gateway Deployment Type for more information.

Figure 5: Deploy OVF Template - Configuration Window



Attention Crosswork supports **Crosswork On-Premise Standard** and **Crosswork On-Premise Extended** deployment configuration for on-premises environment.

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 there is enough available storage.

Figure 6: Deploy OVF Template - Select storage Window

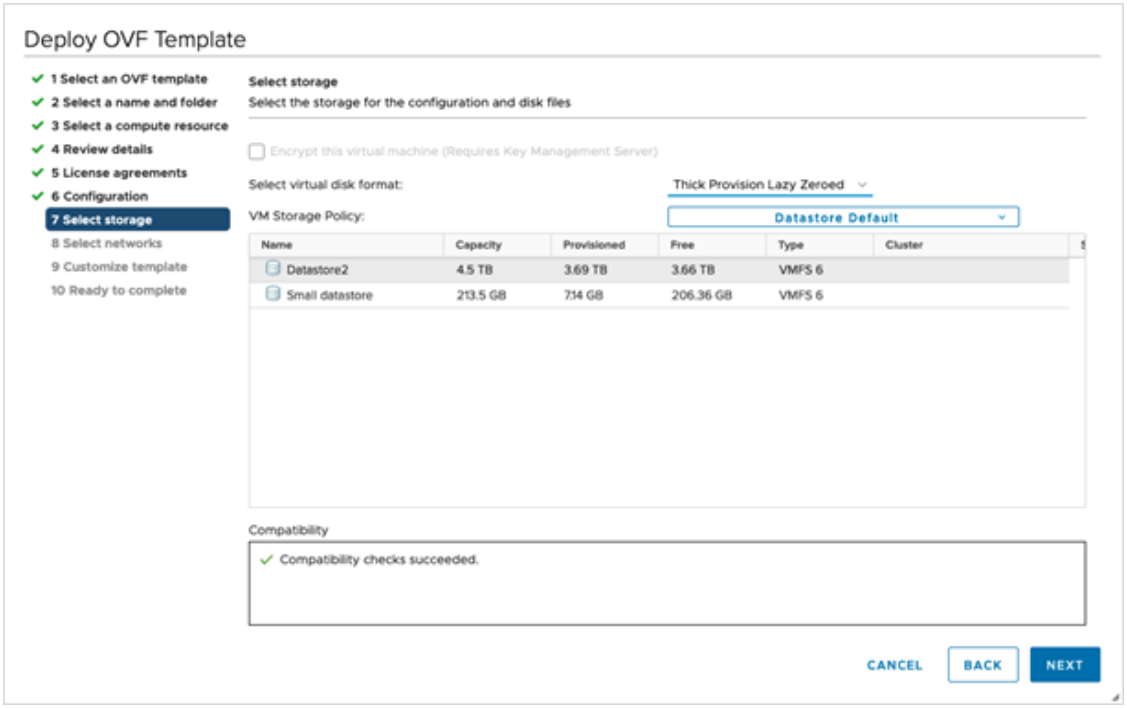
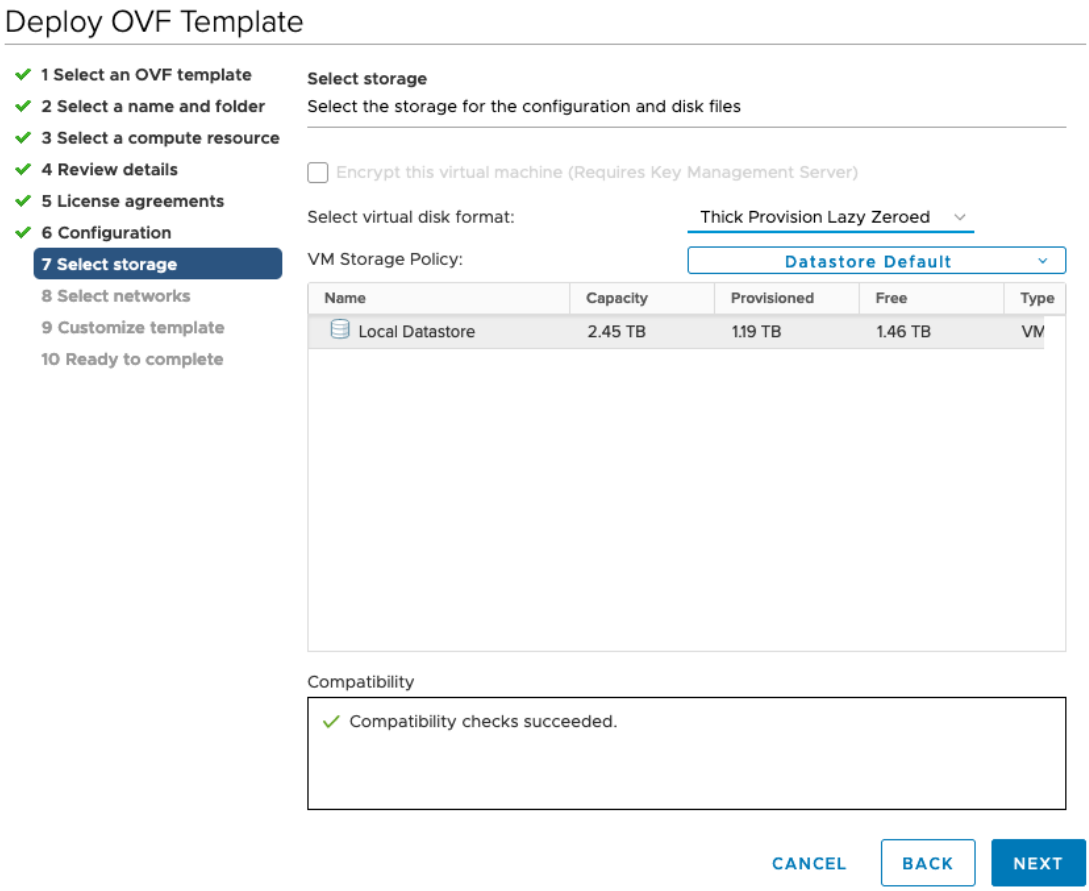
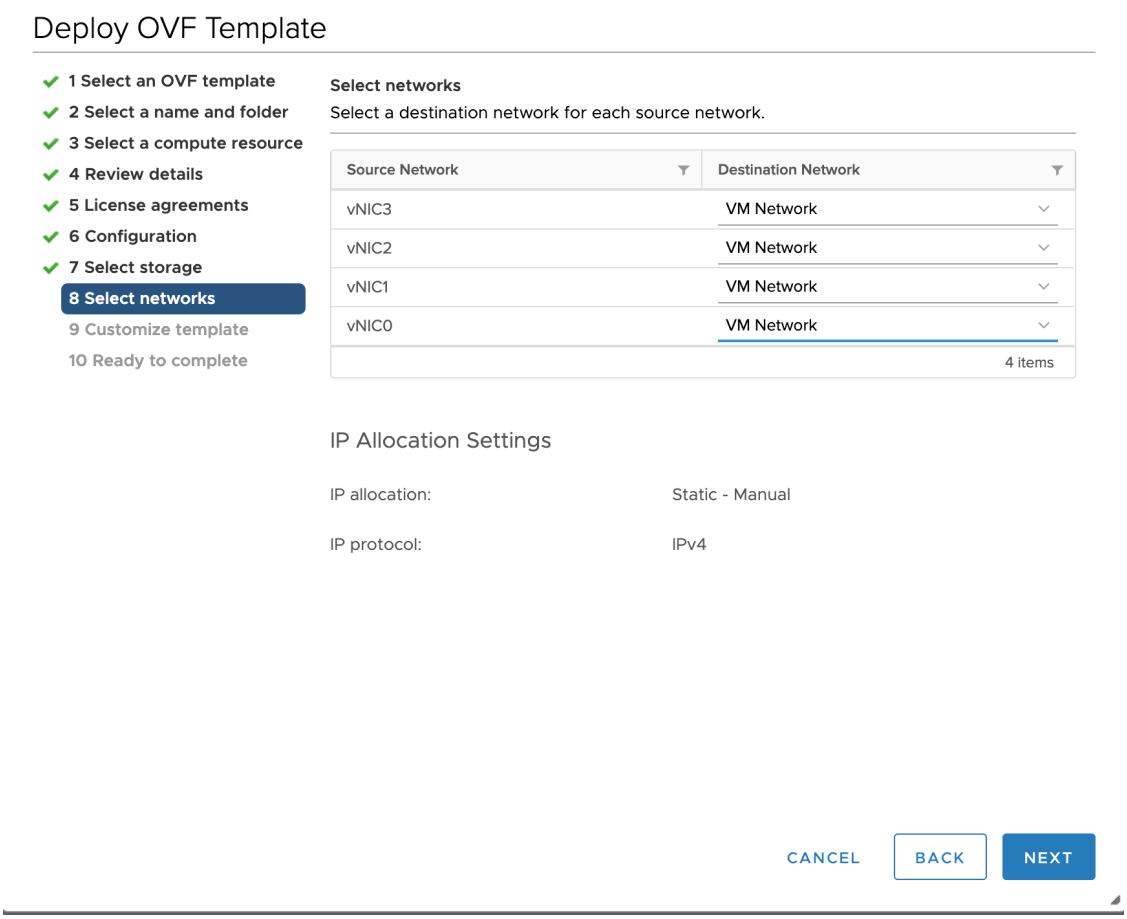


Figure 7: Deploy OVF Template - Select storage Window



Step 10 Click **Next** to go to **8 Select networks**, as shown in the following figure. From the drop-down, at the top of the page, choose the appropriate vNIC role for each interface.

Figure 8: Deploy OVF Template - Select networks Window



Attention Crosswork does not support the **vNIC3** network. Do not configure the IPv4 and IPv6 addresses for **vNIC3**.

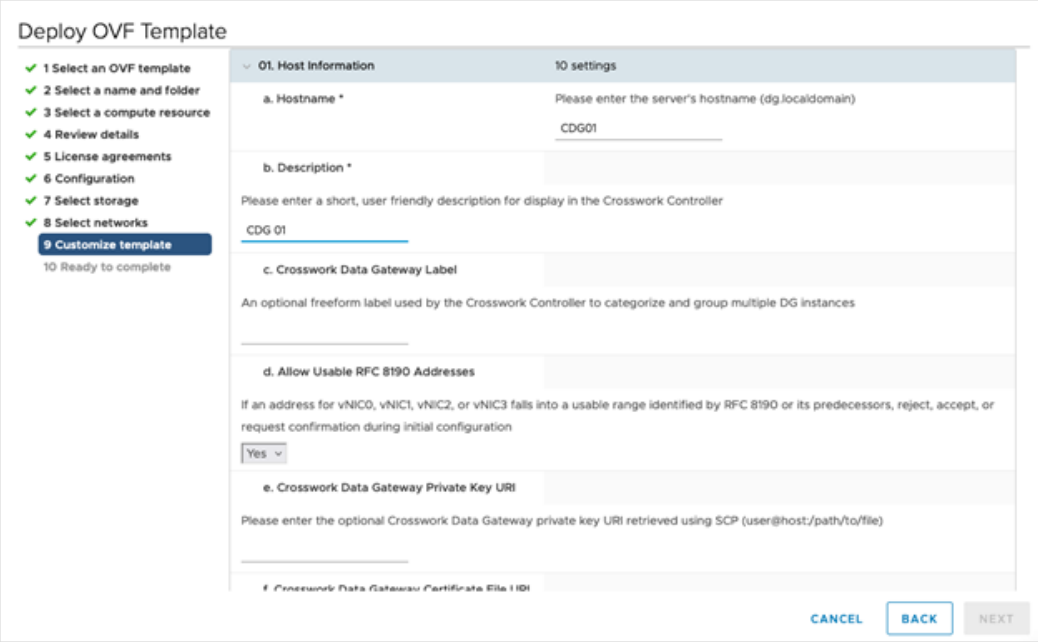
Step 11 Click **Next** to go to **9 Customize template**, with the **Host information** already expanded. Enter the information for the parameters as explained in Table 2: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 3.

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

Important

- For 1 NIC deployment, configure IP, subnet, and gateway values for only vNIC0. After the Crosswork Data Gateway pool is created, VIP address is assigned as a secondary address on vNIC0.
- For 2 and 3 NIC deployments, the IP, subnet, and gateway values are required for vNIC0 and vNIC1. After the Crosswork Data Gateway pool is created, VIP address is assigned as a secondary address on vNIC1.
- In a 3 NIC deployment, the VIP address is assigned to vNIC2 after Crosswork Data Gateway is added to a pool.
- Spare Crosswork Data Gateway in a pool does not have a VIP address.

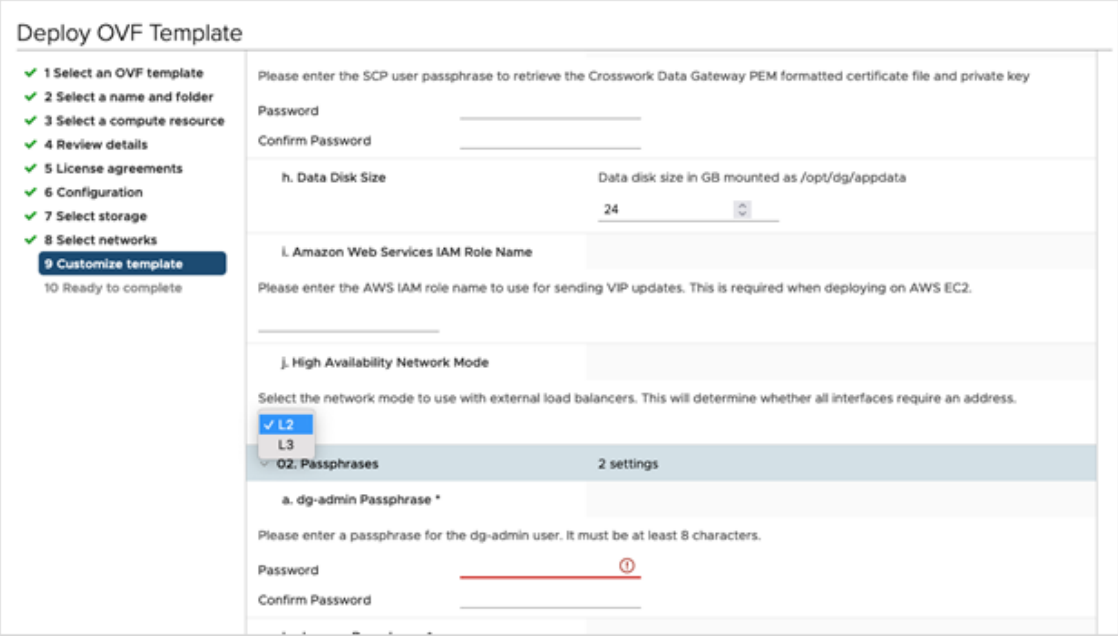
Figure 9: Deploy OVF Template - Customize template > Host information Window



Crosswork Data Gateway supports the following pool mode options:

- L2: When you choose to specify IP addresses for creating the HA pool.
- L3: When you choose to specify FQDN for creating the HA pool and for multisubnet deployment.

Figure 10: Deploy OVF Template - Customize template > Host information Window > High Availability Network Mode



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:

- See Deploy OVF Template - Customize Template for 1 vNIC deployment.
- See Deploy OVF Template - Customize Template for 2 vNICs deployment.
- See Deploy OVF Template - Customize Template for 3 vNICs deployment.

Figure 11: Deploy OVF Template - Customize Template for 1 vNIC deployment

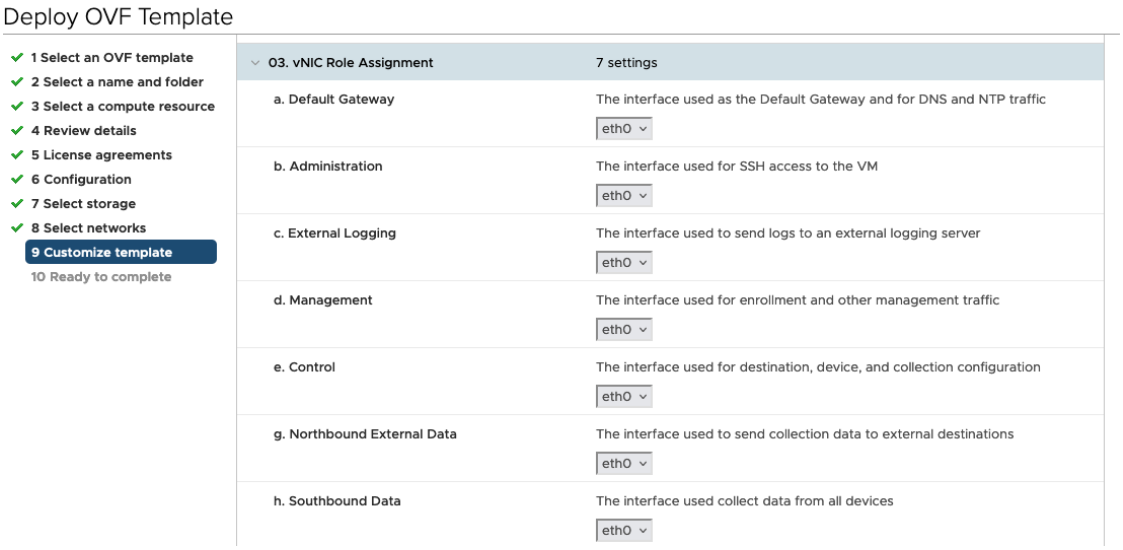
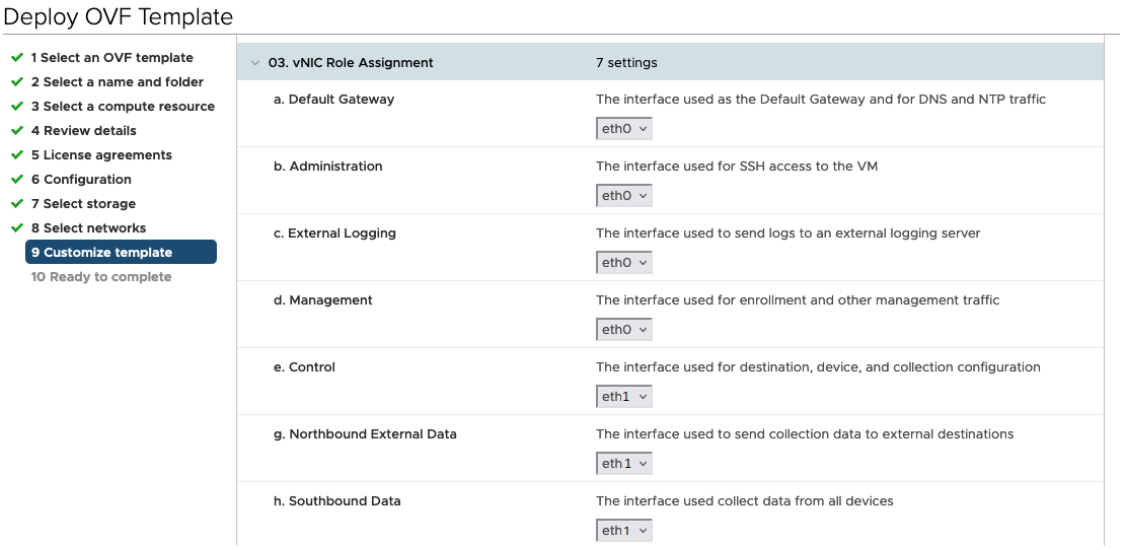
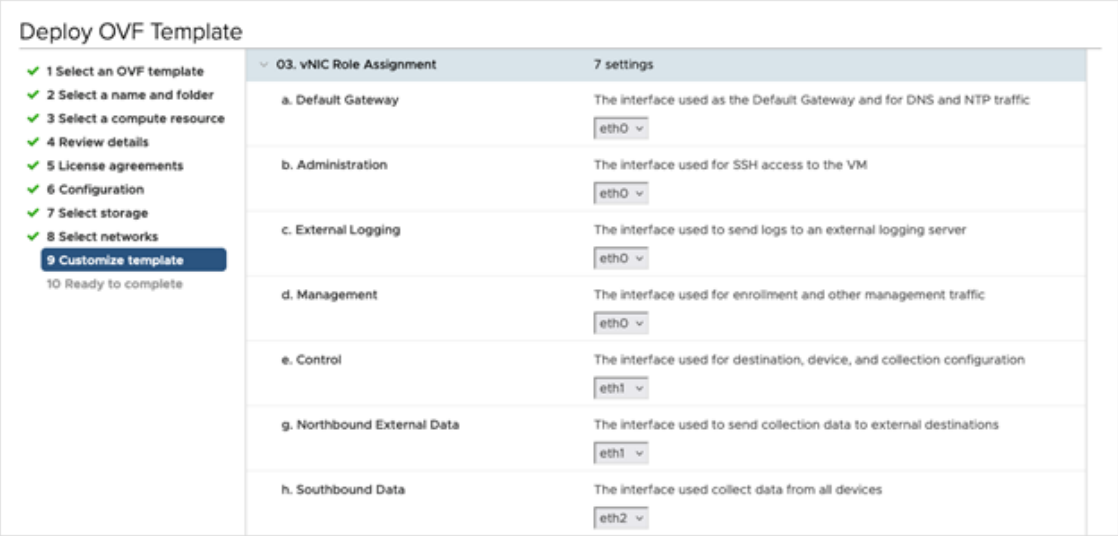


Figure 12: Deploy OVF Template - Customize Template for 2 vNICs deployment



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

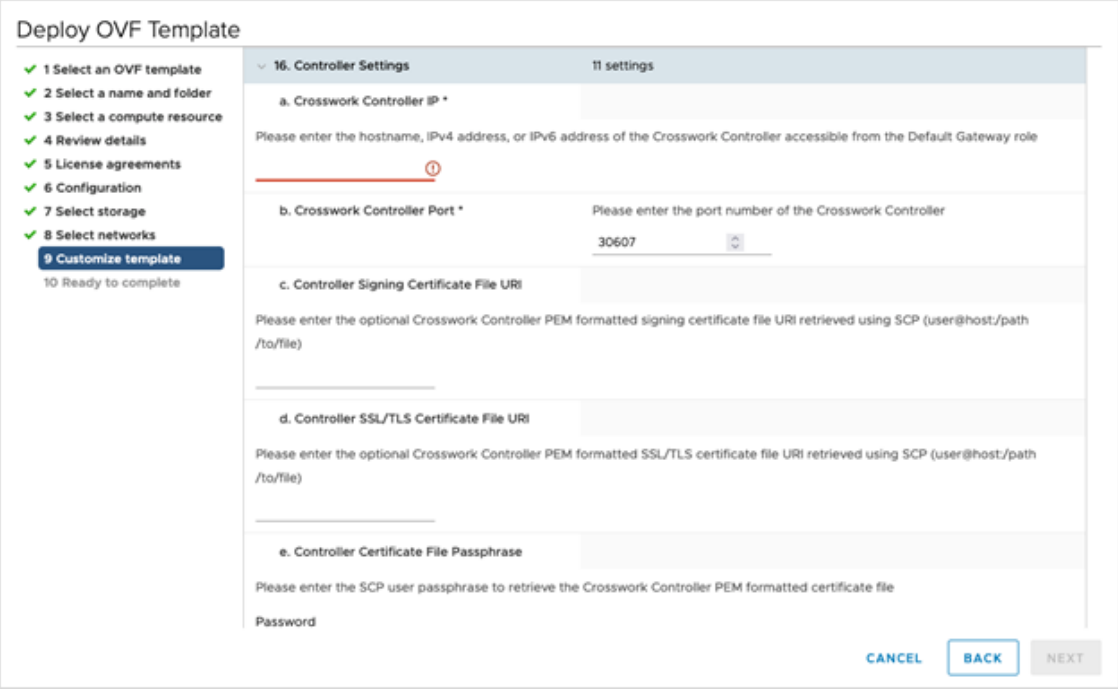
Figure 13: Deploy OVF Template - Customize Template for 3 vNICs deployment



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

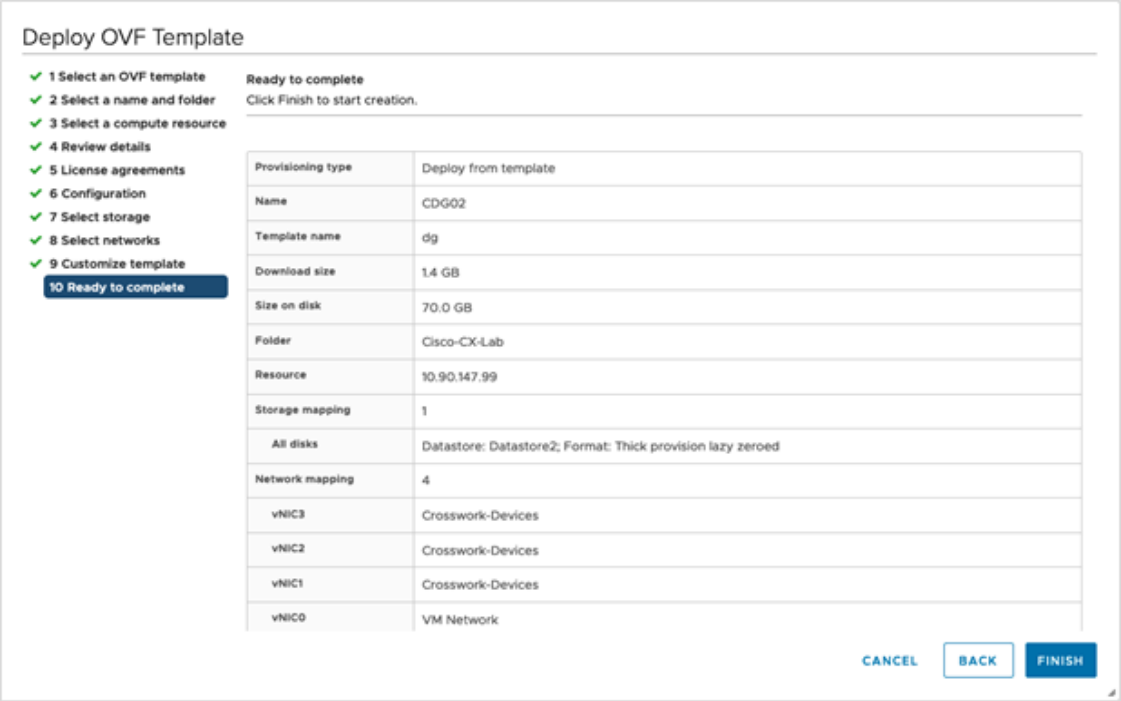
- In the **16. Controller Setting > a. Crosswork Controller IP** section, enter the IP address of the cluster of the DNS host name you assigned to the cluster in your DNS server configuration.
- In the **16. Controller Setting > b. Crosswork Controller Port** section, set the port number to `30607`.

Figure 14: Deploy OVF Template - Customize Template > Controller Settings



Step 12 Click **Next** to go to **10 Ready to complete**. Review your settings and then click **Finish** if you are ready to begin deployment.

Figure 15: Deploy OVF Template - Ready to Complete Window



Step 13 Wait for the deployment to finish before continuing. To check the deployment status:

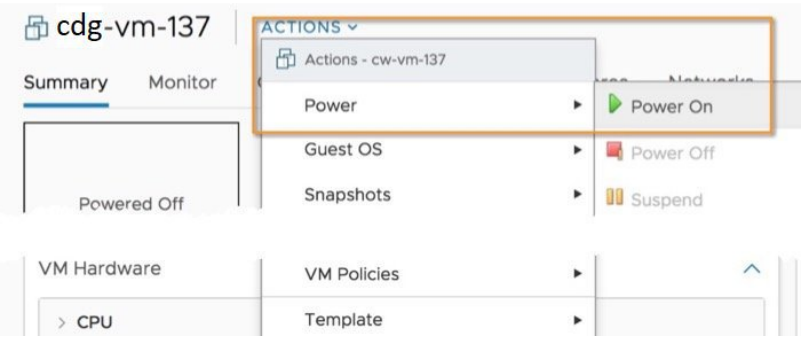
a) Open the vCenter vSphere client.

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

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

Step 14 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 16: Power On Action



Wait for at least 5 minutes for the VM to come up and then log in via vCenter or SSH as explained below.

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. Make changes to these settings at your own risk.

What to do next

After you log in, the Crosswork Data Gateway should present you with the welcome screen and options menu indicating that the installation completed successfully. For information on how to log in, see Log in and Log out of Crosswork Data Gateway VM, on page 33.

Log out and proceed with the postinstallation tasks explained in the next section.

Return to the installation workflow: Install Cisco Crosswork Network Controller on VMware vCenter

Install Cisco Crosswork Data Gateway via OVF Tool

You must modify the list of mandatory and optional parameters in the script as per your requirements and run the OVF Tool. Refer to Table 2: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 3 for the list of installation parameters and their default values.

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

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

Before you begin

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

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

Step 1 On the machine where you have the OVFtool installed, use the following command to confirm that you have OVFtool version 4.4:

```
ovftTool --version
```

Step 2 Download the OVA and the sample script files from cisco.com. For these instructions, we use the file name as **cw-na-dg-5.0.0-45-release-20230418.uefi.ova** and **cw-na-dg-5.0.0-sample-install-scripts.tar.gz** .

Step 3 Use the following command to extract the files from the tar bundle:

```
tar -xvzf cw-na-dg-5.0.0-sample-install-scripts.tar.gz
```

The file bundle is extracted. It includes the **DG-sample-install-scripts.tar** file and scripts for validating the samples install scripts.

Step 4 Use the following command to extract the install scripts from the tar bundle:

```
tar -xvzf DG-sample-install-scripts.tar.gz
```

Step 5 Review the contents of the README file to understand the components that are in the package and how they are validated.

Step 6 Choose the sample script that corresponds to the deployment you plan to use. Cisco provides scripts for 1, 2, and 3 vNIC deployments, which you may optimize to meet your needs.

Sample scripts for 3 vNIC deployment are included in this document. For more information, see Sample Script for Crosswork Data Gateway IPv4 Deployment, on page 30 and Sample Script for Crosswork Data Gateway IPv6 Deployment, on page 31.

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 cw-na-dg-5.0.0-45-release-20230418.uefi.ova>
```

Step 9 If the values provided in the script are valid, provide the vCenter user's password when you are prompted.

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

```
admin@nso-576-tsdn-410-aio:~/CDG_Install$ ./three-nic
/home/admin/CDG_Install/cw-na-dg-5.0.0-45-release-20230418.uefi.ova
Opening OVA source: /home/admin/CDG_Install/cw-na-dg-5.0.0-45-release-20230418.uefi.ova
The manifest does not validate
Warning:
- Line -1: Unsupported value 'firmware' for attribute 'key' on element 'ExtraConfig'.
- Line -1: Unsupported value 'uefi.secureBoot.enabled' for attribute 'key' on element 'ExtraConfig'.
Enter login information for target vi://rcdn5-spm-vc-01.cisco.com/
Username: johndoe
Password: ******
```

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

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

When the installation is complete, the Crosswork Data Gateway VM is powered on, 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 Crosswork Data Gateway VM, on page 33. After you log in, the Crosswork Data Gateway should present you with the welcome screen, and options menu indicating that the installation is complete. Log out and proceed with the postinstallation tasks explained in Crosswork Data Gateway Post-installation Tasks, on page 36.

Sample Script for Crosswork Data Gateway IPv4 Deployment

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

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

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

VM_NAME="<VM name on vcenter>"
DeploymentOption="<onpremise-standard/onpremise-extended>"
DS="<Datastore>"
Host="<ESXi host>"
ManagementNetwork="<vSwitch/dvSwitch>"
DataNetwork="<vSwitch/dvSwitch>"
DeviceNetwork="<vSwitch/dvSwitch>"
ManagementIPv4Address="<CDG managment IP>"
ManagementIPv4Netmask="<CDG managment mask>"
ManagementIPv4Gateway="<CDG managment gateway>"
DataIPv4Address="<CDG Data network IP>"
DataIPv4Netmask="<CDG Data network mask>"
DataIPv4Gateway="<CDG Data network gateway>"
dgadminpwd="<CDG password for dg-admin user>"
dgoperpwd="<CDG password for dg-admin user>"
ControllerIP="<CNC Managment VIP>"
ControllerPassword="<CNC Password>"
ControllerPort="30607"


ROBOT_OVA_PATH=$1

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

ovftool --acceptAllEulas --skipManifestCheck --X:injectOvfEnv -ds=$DS --diskMode=$DM
--overwrite --powerOffTarget --powerOn --noSSLVerify \
--allowExtraConfig \
--name=$VM_NAME \
--deploymentOption=${DeploymentOption} \
--net:"vNIC0=${ManagementNetwork}" \
--prop:"ControllerIP=${ControllerIP}" \
--prop:"ControllerPort=${ControllerPort}" \
--prop:"ControllerSignCertChain=cw-admin@${ControllerIP}:/home/cw-admin/controller.pem" \
--prop:"ControllerCertChainPwd=${ControllerPassword}" \
--prop:"Hostname=${Hostname}" \
--prop:"Description=${Disclaimer}" \
--prop:"DNS=${DNSv4}" \
--prop:"NTP=${NTP}" \
--prop:"Domain=${Domain}" \
--prop:"Vnic0IPv4Method=Static" \
--prop:"Vnic0IPv4Address=${ManagementIPv4Address}" \
--prop:"Vnic0IPv4Gateway=${ManagementIPv4Gateway}" \
--prop:"Vnic0IPv4Netmask=${ManagementIPv4Netmask}" \
--prop:"NicDefaultGateway=eth0" \
--prop:"NicAdministration=eth0" \
--prop:"NicExternalLogging=eth0" \
```

```
--prop:"NicManagement=eth0" \
--prop:"NicControl=eth0" \
--prop:"NicNBExternalData=eth0" \
--prop:"NicSBData=eth0" \
--prop:"dg-adminPassword=${dgadminpwd}" \
--prop:"dg-operPassword=${dgoperpwd}" \
$ROBOT_OVA_PATH \
vi://$VCENTER_LOGIN/$VCENTER_PATH/$Host

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

############################################################
Append section below for three NIC deployment
############################################################
#--net:"vNIC1=${DataNetwork}" \
#--net:"vNIC2=${DeviceNetwork}" \
#--prop:"Vnic1IPv4Method=Static" \
#--prop:"Vnic2IPv4Method=Static" \
#--prop:"Vnic1IPv4Address=${DataIPv4Address}" \
#--prop:"Vnic1IPv4Gateway=${DataIPv4Gateway}" \
#--prop:"Vnic1IPv4Netmask=${DataIPv4Netmask}" \
#--prop:"NicDefaultGateway=eth0" \
#--prop:"NicAdministration=eth0" \
#--prop:"NicExternalLogging=eth0" \
#--prop:"NicManagement=eth0" \
#--prop:"NicControl=eth1" \
#--prop:"NicNBExternalData=eth1" \
#--prop:"NicSBData=eth2" \
```

Sample Script for Crosswork Data Gateway IPv6 Deployment

The following example deploys a Crosswork Data Gateway with IPv6 addresses.

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

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

VM_NAME="<VM name on vcenter>"
DeploymentOption="<onpremise-standard/onpremise-extended>"
DS="<Datastore>"
```

```
Host="<ESXi host>"
ManagementNetwork="<vSwitch/dvSwitch>"
DataNetwork="<vSwitch/dvSwitch>"
DeviceNetwork="<vSwitch/dvSwitch>"
ManagementIPv6Address="<CDG managment IP>"
ManagementIPv6Netmask="<CDG managment mask>"
ManagementIPv6Gateway="<CDG managment gateway>"
DataIPv6Address="<CDG Data network IP>"
DataIPv6Netmask="<CDG Data network mask>"
DataIPv6Gateway="<CDG Data network gateway>"
dgadminpwd="<CDG password for dg-admin user>"
dgoperpwd="<CDG password for dg-admin user>"
ControllerIP="<CNC Managment VIP>"
ControllerPassword="<CNC Password>"
ControllerPort="30607"

ROBOT_OVA_PATH=$1

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

ovftool --acceptAllEulas --skipManifestCheck --X:injectOvfEnv -ds=$DS --diskMode=$DM
--overwrite --powerOffTarget --powerOn --noSSLVerify \
--allowExtraConfig \
--name=$VM_NAME \
--deploymentOption=${DeploymentOption} \
--net:"vNIC0=${ManagementNetwork}" \
--prop:"ControllerIP=${ControllerIP}" \
--prop:"ControllerPort=${ControllerPort}" \
--prop:"ControllerSignCertChain=cw-admin@${ControllerIP}:/home/cw-admin/controller.pem" \
--prop:"ControllerCertChainPwd=${ControllerPassword}" \
--prop:"Hostname=${Hostname}" \
--prop:"Description=${Disclaimer}" \
--prop:"DNS=${DNSv4}" \
--prop:"NTP=${NTP}" \
--prop:"Domain=${Domain}" \
--prop:"Vnic0IPv6Method=Static" \
--prop:"Vnic0IPv6Address=${ManagementIPv6Address}" \
--prop:"Vnic0IPv6Gateway=${ManagementIPv6Gateway}" \
--prop:"Vnic0IPv6Netmask=${ManagementIPv6Netmask}" \
--prop:"NicDefaultGateway=eth0" \
--prop:"NicAdministration=eth0" \
--prop:"NicExternalLogging=eth0" \
--prop:"NicManagement=eth0" \
--prop:"NicControl=eth0" \
--prop:"NicNBExternalData=eth0" \
--prop:"NicSBData=eth0" \
--prop:"dg-adminPassword=${dgadminpwd}" \
--prop:"dg-operPassword=${dgoperpwd}" \
$ROBOT_OVA_PATH \
vi://$VCENTER_LOGIN/$VCENTER_PATH/$Host

############################################################
Append section below for Two NIC deployment
############################################################
#--net:"vNIC1=${DataNetwork}" \
#--prop:"Vnic1IPv6Method=Static" \
#--prop:"Vnic1IPv6Address=${DataIPv6Address}" \
#--prop:"Vnic1IPv6Gateway=${DataIPv6Gateway}" \
#--prop:"Vnic1IPv6Netmask=${DataIPv6Netmask}" \
#--prop:"NicDefaultGateway=eth0" \
#--prop:"NicAdministration=eth0" \
#--prop:"NicExternalLogging=eth0" \
#--prop:"NicManagement=eth0" \
```

```
#--prop:"NicControl=eth1" \
#--prop:"NicNBExternalData=eth1" \
#--prop:"NicSBData=eth1" \

############################################################
Append section below for three NIC deployment
############################################################
#--net:"vNIC1=${DataNetwork}" \
#--net:"vNIC2=${DeviceNetwork}" \
#--prop:"Vnic1IPv6Method=Static" \
#--prop:"Vnic1IPv6Address=${DataIPv6Address}" \
#--prop:"Vnic1IPv6Gateway=${DataIPv6Gateway}" \
#--prop:"Vnic1IPv6Netmask=${DataIPv6Netmask}" \
#--prop:"NicDefaultGateway=eth0" \
#--prop:"NicAdministration=eth0" \
#--prop:"NicExternalLogging=eth0" \
#--prop:"NicManagement=eth0" \
#--prop:"NicControl=eth1" \
#--prop:"NicNBExternalData=eth1" \
#--prop:"NicSBData=eth2" \
```

Log in and Log out of Crosswork Data Gateway VM

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

- Access Crosswork Data Gateway VM from SSH, on page 33
- Access Crosswork Data Gateway through vCenter, on page 34

To log out of the Crosswork Data Gateway VM, see Log Out of Crosswork Data Gateway VM, on page 34.

Access Crosswork Data Gateway VM from SSH

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

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

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

ssh <username>@<ManagementNetworkIP>

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

For example,

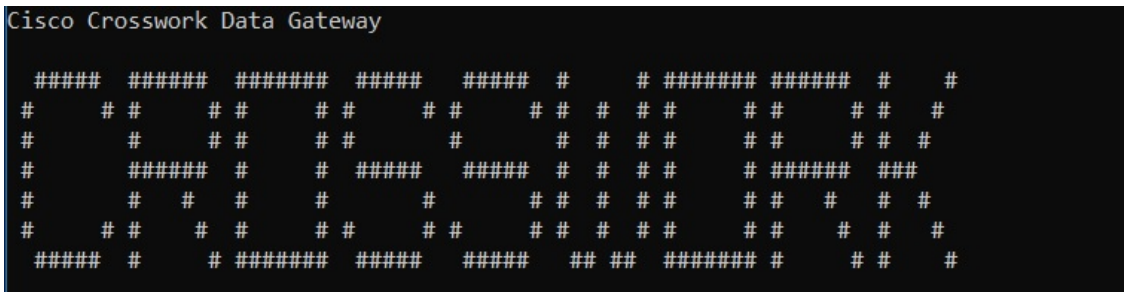
To login as administrator user: **ssh dg-admin@<ManagementNetworkIP>**

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 17: 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:

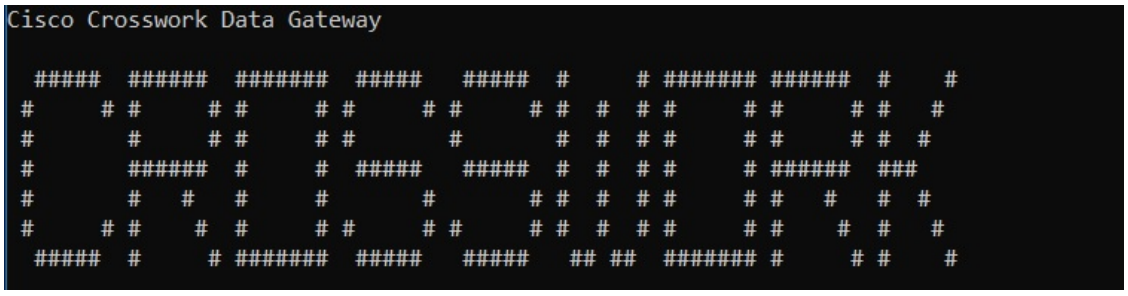
Step 1 Locate the VM in vCenter and then right-click and select **Open Console**.

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 18: Crosswork screen



Log Out of Crosswork Data Gateway VM

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

Cisco 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 Crosswork Data Gateway instance in its database and waits for a "first-sign-of-life" from the Crosswork Data Gateway VM.

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

To verify if the Crosswork 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 Cisco Crosswork Data Gateway VMs that have successfully enrolled with Cisco Crosswork are displayed here.

The initial **Operational State** of Crosswork 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 Crosswork 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 *Cisco Crosswork Network Controller 5.0 Administration Guide*.

Note Cisco Crosswork Data Gateway VMs that were previously onboarded and still have the **Operational State** as **Degraded** need to be investigated. 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 *Cisco Crosswork Network Controller 5.0 Administration Guide*.

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

- Configure Timezone of the Crosswork Data Gateway VM, on page 36

What to do next:

Return to the installation workflow: Install Cisco Crosswork Network Controller on VMware vCenter

Configure Timezone of the Crosswork Data Gateway VM

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

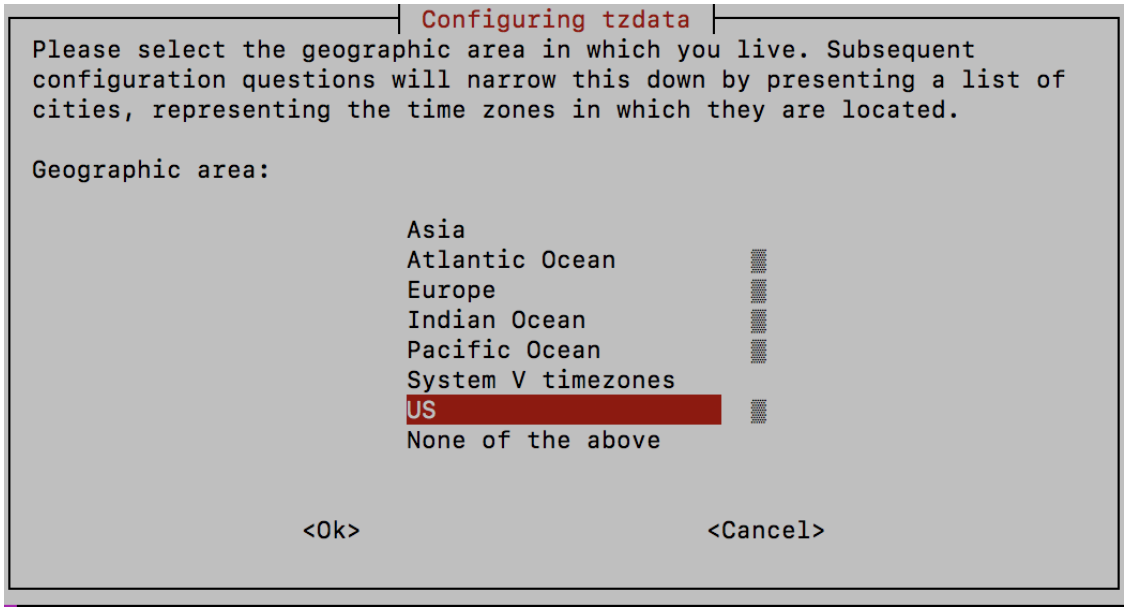
Step 1 Log in to the Crosswork Data Gateway VM.

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

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

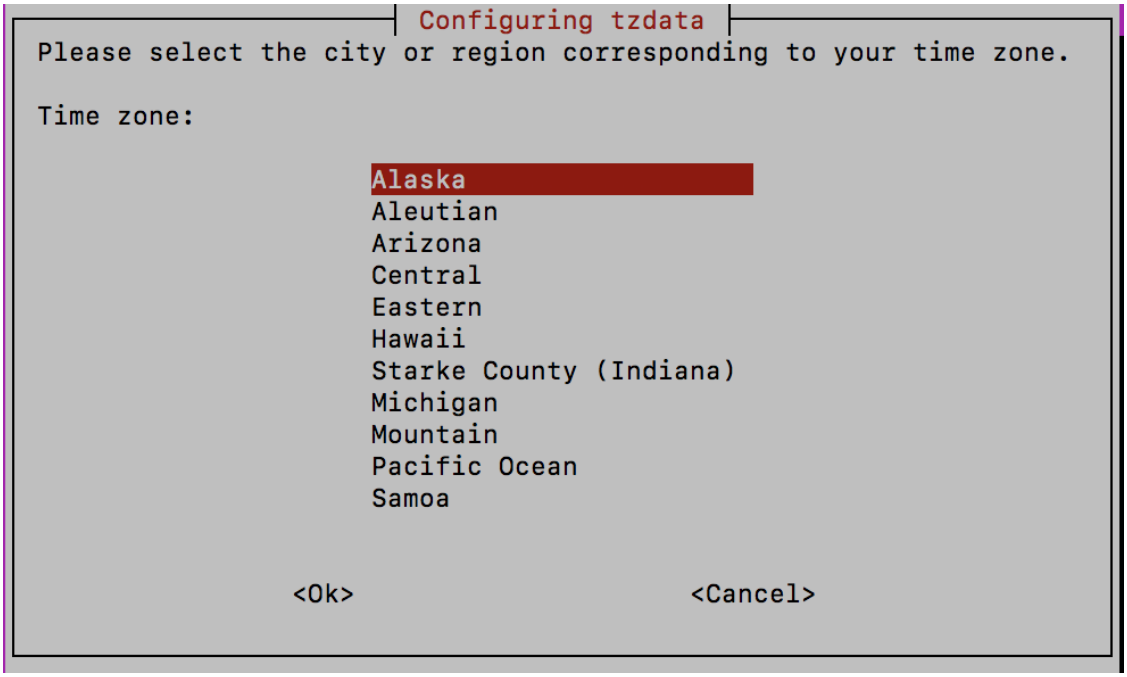
Step 4 Select the geographic area in which you live.

Figure 19: Timezone Settings - Geographic Area Selection



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

Figure 20: Timezone Settings - Region Selection



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

Step 7 Reboot the Crosswork Data Gateway VM so that all processes pick up the new timezone. See *Reboot Crosswork Data Gateway VM* section in *Cisco Crosswork Network Controller 5.0 Administration Guide*.

Step 8 Log out of the Crosswork Data Gateway VM.

Troubleshoot Crosswork Data Gateway Installation and Enrollment

If Crosswork Data Gateway fails to auto-enroll with Cisco Crosswork, 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 *Cisco Crosswork Network Controller 5.0 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 Crosswork Data Gateway, and provides approaches to identifying the source of the problem and solving it.

Table 3: Troubleshooting the Installation/Enrollment

Issue	Action
Crosswork Data Gateway cannot be enrolled with Cisco Crosswork due to an NTP issue, i.e., there is a clock-drift between the two. **The clock-drift might be with either Crosswork Data Gateway or Cisco Crosswork.** **Also, on the NTP servers for Cisco Crosswork and Crosswork Data Gateway, the initial time is set to the ESXi server. For this reason, the ESXi server must also have NTP configured.** **Sync the clock time on the host and retry.**	1. Log in to the Crosswork Data Gateway VM. 2. From the main menu, select **5 Troubleshooting** > **2 Run show-tech**. Enter the destination to save the tarball containing logs and vitals and click **OK**. The show-tech is now encrypted with a file extension ending with .tar.xz. 3. Run the following command to decrypt the show-tech file. `openssl enc -d -AES-256-CBC -pbkdf2 -md sha512 -iter 100000 -in <showtech file> -out <decrypted filename> -pass pass:<encrypt string>` In the show-tech logs (in file `session.log` at location `/opt/dg/log/controller-gateway/session.log`), if you see the error `UNAUTHENTICATED:invalid certificate. reason: x509: certificate has expired or is not yet valid`, then there is a clock-drift between Crosswork Data Gateway and Cisco Crosswork. 3. From the main menu, go to **3 Change Current System Settings** > **1 Configure NTP**. Configure NTP to sync with the clock time on the Cisco Crosswork server and try reenrolling Crosswork Data Gateway.

Issue	Action
Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "Could not collect vitals" due to certificate errors.	1. Log in to the Crosswork Data Gateway VM. 2. From the main menu, select **5 Troubleshooting** > **2 Run show-tech**. Enter the destination to save the tarball containing logs and vitals and click **OK**. The show-tech is now encrypted with a file extension ending with .tar.xz. 3. Run the following command to decrypt the show-tech file. `openssl enc -d -AES-256-CBC -pbkdf2 -md sha512 -iter 100000 -in <showtech file> -out <decrypted filename> -pass pass:<encrypt string>` In the show-tech logs (in file `gateway.log` at location `/opt/dg/log/controller-gateway/gateway.log`), if you see certificate errors, then reupload the Controller Signing Certificate, as explained in the steps below: 1. From the main menu, select **3 Change Current System Settings** > **7 Import Certificate**. 2. From the **Import Certificates** menu, select **1 Controller Signing Certificate File** and click **OK**. 3. Enter the SCP URI for the certificate file and click **OK**.
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.	1. Reupload the certificate file using the following steps: a. From the main menu, select **3 Change Current System Settings** > **7 Import Certificate**. b. From the **Import Certificates** menu, select **1 Controller Signing Certificate File** and click **OK**. c. Enter the SCP URI for the certificate file and click **OK**. 2. Reboot the Crosswork Data Gateway VM following the steps below: a. From the main menu, select **5 Troubleshooting** and click **OK**. b. From the Troubleshooting menu, select **4 Reboot VM** and click **OK**. c. Once the reboot is complete, check if the Crosswork Data Gateway's operational status is **Up**.

Issue	Action
Crosswork Data Gateway goes into Error state	Check the vNIC values in the OVF template in case of vCenter.
Crosswork Data Gateway enrollment with 1 NIC Cisco Crosswork fails	Check the vNIC values in the OVF template in case of vCenter. If ActiveVnics property is missing for 1 NIC and 2 NIC, Crosswork Data Gateway tries to deploy 3 NICs by default. Due to this, Crosswork Data Gateway enrollment with 1 NIC Cisco Crosswork fails post deployment with error in gateway.log that Crosswork Data Gateway expected 1 NIC, but it is not 1 NIC.
Crosswork Data Gateway deploys Standard profile instead of Extended profile	Check the `Deployment` parameter in the OVF template in case of vCenter. If `Deployment` parameter mismatches or does not exist for an Extended profile, then Crosswork Data Gateway deploys the Standard profile by default.
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.	Reenroll or redeploy the Crosswork Data Gateways. For more information, see the *Redeploy a Crosswork Data Gateway Instance* and *Reenroll Crosswork Data Gateway* sections in *Cisco Crosswork Network Controller 5.0 Administration Guide*.

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.	1. Log in to the Crosswork UI from the SSH.
	2. Run the Docker executive commands to access the **robot-astack-influxdb** pod.
	3. In the pod, navigate to the following directory and delete it:
	`/mnt/datafs/influxdb`
	4. Restart the service using the following command:
	`supervisorctl restart all`

If 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 **Maintenance** mode or manually reenroll the gateway. For more information, see the *Reenroll Crosswork Data Gateway* section in *Cisco Crosswork Network Controller 5.0 Administration Guide*.

Import Controller Signing Certificate File

The Controller Certificate file is automatically imported after the VM boots. You will need to perform this step manually for the following reasons:

- You have not specified **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.

Follow these steps to import controller signing certificate file:

Step 1 From the Cisco Crosswork 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 **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. SeeView the Controller Signing Certificate File, on page 41.

View the Controller Signing Certificate File

Follow these steps to view the signing certificate:

Step 1 From the Crosswork 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.