Install Crosswork Data Gateway

This section contains the following topics:

Install Cisco Crosswork Data Gateway

This procedure can be used for installing the first Cisco Crosswork Data Gateway or for adding additional Cisco Crosswork Data Gateway VMs.

Note If you are re-deploying Cisco Crosswork Data Gateway with Cisco Crosswork, delete the previous Cisco Crosswork entry for auto-enrollment to work.

Cisco Crosswork Data Gateway Deployment and Set Up Workflow

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

1. Choose the deployment type for Cisco Crosswork Data Gateway i.e., Standard or Extended. See Cisco Crosswork Data Gateway Requirements.
2. Install Cisco Crosswork Data Gateway on your preferred platform:

VMware	Install Cisco Crosswork Data Gateway Using vCenter vSphere Client, on page 10
	Install Cisco Crosswork Data Gateway Via OVF Tool, on page 15
Cisco CSP	Install Cisco Crosswork Data Gateway on Cisco CSP, on page 17

3. Set timezone on Cisco Crosswork Data Gateway VM. See Configure Timezone, on page 27.

4. Verify Cisco Crosswork Data Gateway enrollment with Cisco Crosswork. See Cisco Crosswork Data Gateway Authentication and Enrollment, on page 28.

After verifying that the Cisco Crosswork Data Gateway has successfully enrolled with Cisco Crosswork, create a Cisco Crosswork Data Gateway pool and add the Cisco Crosswork Data Gateway VMs to the pool.

Note If you are going to have multiple Cisco Crosswork Data Gateways due to load or scale and/or you wish to leverage Cisco Data Gateway High Availability, it is recommended that you install all the Cisco Crosswork Data Gateway VMs and then add them to a Data Gateway pool.

Cisco Crosswork Data Gateway Parameters and Deployment Scenarios

Before you begin installing the Cisco Crosswork Data Gateway, read about parameters and possible deployment scenarios mentioned in the next section. You will need to refer this section to supply parameter values when you install Cisco Crosswork Data Gateway using the above methods.

Note Certificate chains override any preset or generated certificates in the VM and are given as an SCP URI (user:host:/path/to/file).

* Denotes the mandatory parameters. Others are optional. You might choose them based on the kind of deployment scenrio you require. Deployment scenarios are explained wherever applicable.

** Denotes parameters that can be entered during install or addressed using additional procedures.

Table 1: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios

Parameter	Description	Deployment Scenario
Host Information		
Hostname*	Hostname of the server specified as a fully qualified domain name (FQDN). **Note** For larger systems it is likely that you will have more than one Cisco Crosswork Data Gateway VMs. The hostname should, therefore, be unique and created in a way that makes identifying a specific VM easy.	
Description*	A detailed description of the Cisco Crosswork Data Gateway instance.	

Parameter	Description	Deployment Scenario
Crosswork Data Gateway Label	Label used by Cisco Crosswork to categorize and group multiple Cisco Crosswork Data Gateway instances.	
Active vNICs	Number of vNICs to use for sending traffic.	You can choose to use either 1, 2, or 3 vNICs as per the following combinations: **Note** If you use one vNIC on your Crosswork cluster , you must use only one interface on the Crosswork Data Gateway. If you use two vNICs on your Crosswork Cluster, then you can use two or three vNICs on the Crosswork Data Gateway. • 1 - sends all traffic through vNIC0. • 2 - sends management traffic through vNIC0 and all data traffic through vNIC1. • 3 - sends management traffic through vNIC0, Northbound data through vNIC1, and Southbound data on vNIC2.
Allow RFC8190	Automatically allow addresses in an RFC 8190 range. If the box is not checked, the initial configuration scripts will prompt for confirmation.	

<table>
<tr><th>Parameter</th><th>Description</th><th>Deployment Scenario</th></tr>
<tr><td>Private Key URI</td><td>SCP URI to private key file for session key signing. You can retrieve this using SCP (user@host:path/to/file).</td><td rowspan="4">Cisco Crosswork uses self-signed certificates for handshake with Cisco Crosswork Data Gateway. These certificates are generated upon installation.

However, if you want to use third-party or your own certificate files, then you must input these three parameters.

Note The host with the URI files must be reachable on the network (from the vNIC0 interface via SCP) and files must be present at the time of install.</td></tr>
<tr><td>Certificate File URI</td><td>SCP URI to PEM formatted signing certificate chain for this VM. You can retrieve this using SCP (user@host:path/to/file).</td></tr>
<tr><td>Certificate File and Key Passphrase</td><td>SCP user passphrase to retrieve the CiscoCrosswork Data Gateway PEM formatted certificate file and private key.</td></tr>
<tr><td>Data Disk Size</td><td>Size in GB of a second data disk. Default size is 5GB for Standard and 500GB for Extended.</td></tr>
<tr><td colspan="3">Passphrases

During installation, Crosswork Data Gateway creates two default user accounts:

1. A Cisco Crosswork Data Gateway administrator, with the username dg-admin and password set during installation. The administrator uses this ID to log in to and troubleshoot Crosswork Data Gateway.

2. A Cisco Crosswork Data Gateway operator, with the username dg-oper and password set during installation. This is a read-only user and has permissions to perform all ‘read’ operations and some limited ‘action’ commands.

To know what operations an admin and operator can perform, see Section Supported User Roles in the Cisco Crosswork Infrastructure 4.0 and Applications Administration Guide.

Note These two pre-defined usernames are reserved and cannot be changed.

Change of password would be allowed from the console for both the accounts.

In case of lost or forgotten passwords, the user would have to create a new VM, destroy the current VM, and re-enroll the new one on the Cisco Crosswork.</td></tr>
<tr><td>dg-admin Passphrase*</td><td>The password you have chosen for the dg-admin user.</td><td></td></tr>
<tr><td>dg-oper Passphrase*</td><td>The password you have chosen for the dg-oper user.</td><td></td></tr>
</table>

Parameter	Description	Deployment Scenario
Note • Cisco Crosswork Data Gateway supports either IPv4 or IPv6 for vNIC0 and vNIC1 interfaces. For the interface(s) and protocol you choose to use, select Method as Static and enter information in Address, Netmask, Skip Gateway, and Gateway fields. The default value is None. • Installation process will only ask for vNIC0 and vNIC1 IP. vNIC2 IP will be assigned during Cisco Crosswork Data Gateway pool creation as explained in the section Create a Cisco Crosswork Data Gateway Pool, on page 29. • Cisco Crosswork does not support dual stack configurations. Therefore, ALL addresses for the environment must be either IPv4 or IPv6.		
[1]vNIC0 IPv4 Address		
vNIC0 IPv4 Method*	How the vNIC0 interface gets its IPv4 address.	
vNIC0 IPv4 Address	IPv4 address of the vNIC0 interface.	
vNIC0 IPv4 Netmask	IPv4 netmask of the vNIC0 interface in dotted quad format.	
vNIC0 IPv4 Skip Gateway	Skip configuring a gateway?	
vNIC0 IPv4 Gateway	IPv4 address of the vNIC0 gateway.	
[1]vNIC0 IPv6 Address		
vNIC0 IPv6 Method*	How the vNIC0 interface gets its IPv6 address.	
vNIC0 IPv6 Address	IPv6 address of the vNIC0 interface.	
vNIC0 IPv6 Netmask	IPv6 prefix of the vNIC0 interface.	
vNIC0 IPv6 Skip Gateway	Skip configuring a gateway?	
vNIC0 IPv6 Gateway	IPv6 address of the vNIC0 gateway.	
[1]vNIC1 IPv4 Address		
vNIC1 IPv4 Method*	How the vNIC1 interface gets its IPv4 address.	
vNIC1 IPv4 Address	IPv4 address of the vNIC1 interface.	

Parameter	Description	Deployment Scenario
vNIC1 IPv4 Netmask	IPv4 netmask of the vNIC1 interface in dotted quad format.	
vNIC1 IPv4 Skip Gateway	Skip configuring a gateway?	
vNIC1 IPv4 Gateway	IPv4 address of the vNIC1 gateway.	
[1]vNIC1 IPv6 Address		
vNIC1 IPv6 Method*	How the vNIC1 interface gets its IPv6 address.	
vNIC1 IPv6 Address	IPv6 address of the vNIC1 interface.	
vNIC1 IPv6 Netmask	IPv6 netmask of the vNIC1 interface in dotted quad format.	
vNIC1 IPv6 Skip Gateway	Skip configuring a gateway?	
vNIC1 IPv6 Gateway	IPv6 address of the vNIC1 gateway.	
DNS Servers		
DNS Address*	Space-delimited list of IPv4/IPv6 addresses of the DNS server accessible from the management interface.	
DNS Search Domain*	DNS search domain	
DNS Security Extensions	Use DNS security extensions?	
DNS over TLS	Use DNS over TLS?	
Multicast DNS	Use multicast DNS?	
Link-Local Multicast Name Resolution	Use link-local multicast name resolution?	
NTPv4 Servers		

Parameter	Description	Deployment Scenario
NTPv4 Servers*	Space-delimited list of IPv4/IPv6 addresses or hostnames of the NTPv4 servers accessible from the management interface.	You must enter a value here, such as pool.ntp.org. NTP server is critical for time synchronization between Crosswork Data Gateway VM, Crosswork, and devices. Using a non-functional 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 will fail to connect.
Use NTPv4 Authentication	Use NTPv4 authentication?	
NTPv4 Keys	Space delimited Key IDs to map to server list.	
NTPv4 Key File URI	SCP URI to the chrony key file.	
NTPv4 Key File Passphrase	Password of SCP URI to the chrony key file.	
Remote Syslog Server		

Parameter	Description	Deployment Scenario
Use Remote Syslog Server?	Send syslog messages to a remote host?	If you want to use an external syslog server, you must specify these seven settings. **Note** If you have configured an external syslog server, the service (CLI/MDT/SNMP/gNMI) events are sent to that external syslog server. Otherwise, they are logged only to the Crosswork Data Gateway VM. To obtain logs, from the main menu, go to 5 Troubleshooting > Run show-tech. **Note** The host with the URI files must be reachable on the network (from vNIC0 interface via SCP) and files must be present at the time of install.
Syslog Server Address	IPv4 or IPv6 address of a syslog server accessible from the management interface. **Note** If you are using an IPv6 addres, it must be surrounded by square brackets ([1::1]).	
Syslog Server Port	Port number of the syslog server.	
Syslog Server Protocol	Use UDP, TCP, or RELP when sending syslog.	
Use Syslog over TLS?	Use TLS to encrypt syslog traffic.	
Syslog TLS Peer Name	Syslog server's hostname exactly as entered in the server certificate SubjectAltName or subject common name.	
Syslog Root Certificate File URI	PEM formatted root cert of syslog server retrieved using SCP.	
Syslog Certificate File Passphrase	Password of SCP user to retrieve Syslog certificate chain.	
Remote Auditd Server		
Use Remote Auditd Server?	Send Auditd message to a remote host?	If you want to use an external Auditd server, you must specify these three settings.
Auditd Server Address	Hostname, IPv4, or IPv6 address of an optional Auditd server	
Auditd Server Port	Port number of an optional Auditd server.	
Controller Settings		
Crosswork Controller IP*	The Virtual IP address of Cisco Crosswork Cluster. **Note** If you are using an IPv6 address, it must be surrounded by square brackets ([1::1]).	

Parameter	Description	Deployment Scenario
Crosswork Controller Port*	Port of the Cisco Crosswork controller.	
Controller Signing Certificate File URI**	PEM formatted root cert of Cisco Crosswork to validate signing certs retrived using SCP. PEM file is generated by Cisco Crosswork and is available at the following location: `cw-admin@<Crosswork_VM_Management_IP_Address>:/home/cw-admin/controller.pem`	The Controller Signing Certificate File is required for the Crosswork Data Gateway to become functional. The certificate file is automatically imported once Crosswork Data Gateway boots up for the first time if you specify these parameters during the installation. If you do not specify these parameters during installation, then you must import the certificate file manually by following the procedure Import Controller Signing Certificate File, on page 34.
Controller SSL/TLS Certificate File URI	Cisco Crosswork Controller PEM formatted SSL/TLS certificate file retrieved using SCP.	
Controller Certificate File Passphrase**	Password of SCP user (cw-admin) to retrieve Cisco Crosswork certificate chain.	This is required if you are providing a controller signing certificate file URI.
Proxy Server URL	URL of management network proxy server.	If you want to use a proxy server, you must specify these parameters.
Proxy Server Bypass List	Space-delimited list of subnets and domains that will not be sent to the proxy server.	
Authenticated Proxy Username	Username for authenticated proxy servers.	
Authenticated Proxy Passphrase	Passphrase for authenticated proxy servers.	
HTTPS Proxy SSL/TLS Certificate File URI	HTTPS proxy PEM formatted SSL/TLS certificate file retrieved using SCP.	
HTTPS Proxy SSL/TLS Certificate File Passphrase	Password of SCP user to retrieve proxy certificate chain.	

[1]Either an IPv4 or IPv6 address must be specified for the interface(s) you choose to use. Selecting None for both will result in a non-functional deployment.

Note If you are not using the default SCP port 22, you can specify the port as a part of the SCP command. For example,

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

where 55 is a custom port.

Install Cisco Crosswork Data Gateway Using vCenter vSphere Client

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

Note The example images shown are only of Cisco Crosswork Data Gateway On-Premise Standard deployment.

Step 1 Download the Cisco Crosswork Data Gateway 2.0 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 will 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 Table 1: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2.

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

Step 3 The VMware Deploy OVF Template wizard appears and highlights the first step, 1 Select template.

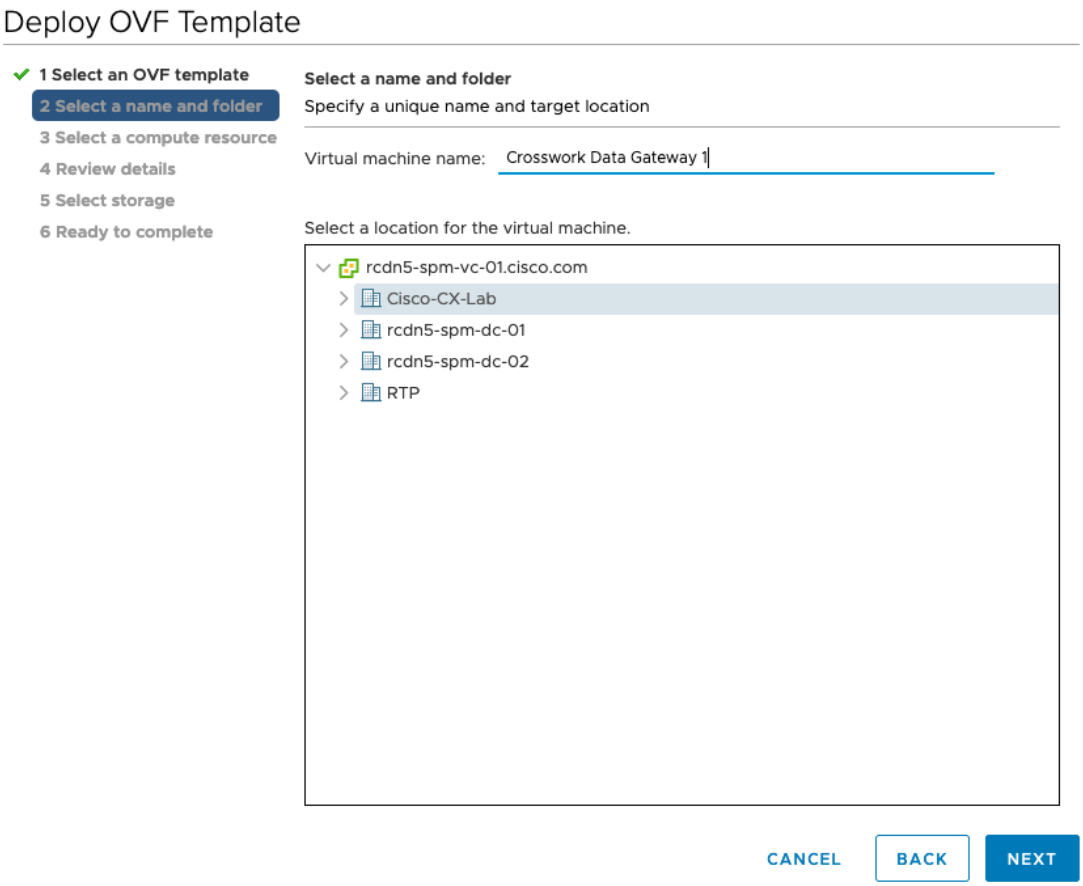
a) Click Browse to navigate to the location where you downloaded the OVA image file and select it.

Once selected, the filename is displayed in the window.

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

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

b) In the Select a location for the virtual machine list, choose the datacenter under which the VM will reside.



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

Step 6 Click Next. The VMware vCenter Server validates the OVA. Network speed will determine how long validation takes. When the validation is complete, the wizard moves to 4 Review details. Review the OVA's information and then click Next.

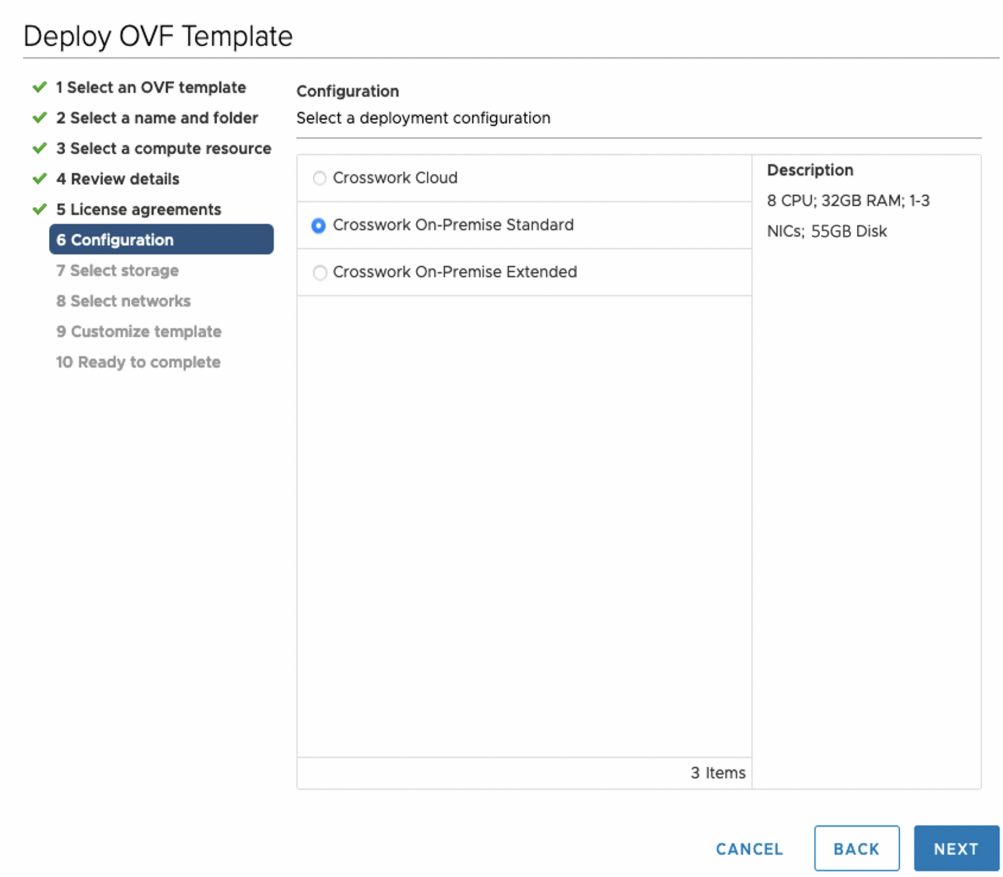
Take a moment to review the OVF template you are deploying.

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

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

Step 8 Click Next to go to 6 Select configuration, as shown in the following figure. Select the type of configuration you want i.e., either Crosswork On-Premise Standard or Crosswork On-Premise Extended.

Note You must choose Crosswork On-Premise Extended if you plan to use Crossowork Data Gateway with Crosswork Health Insights.



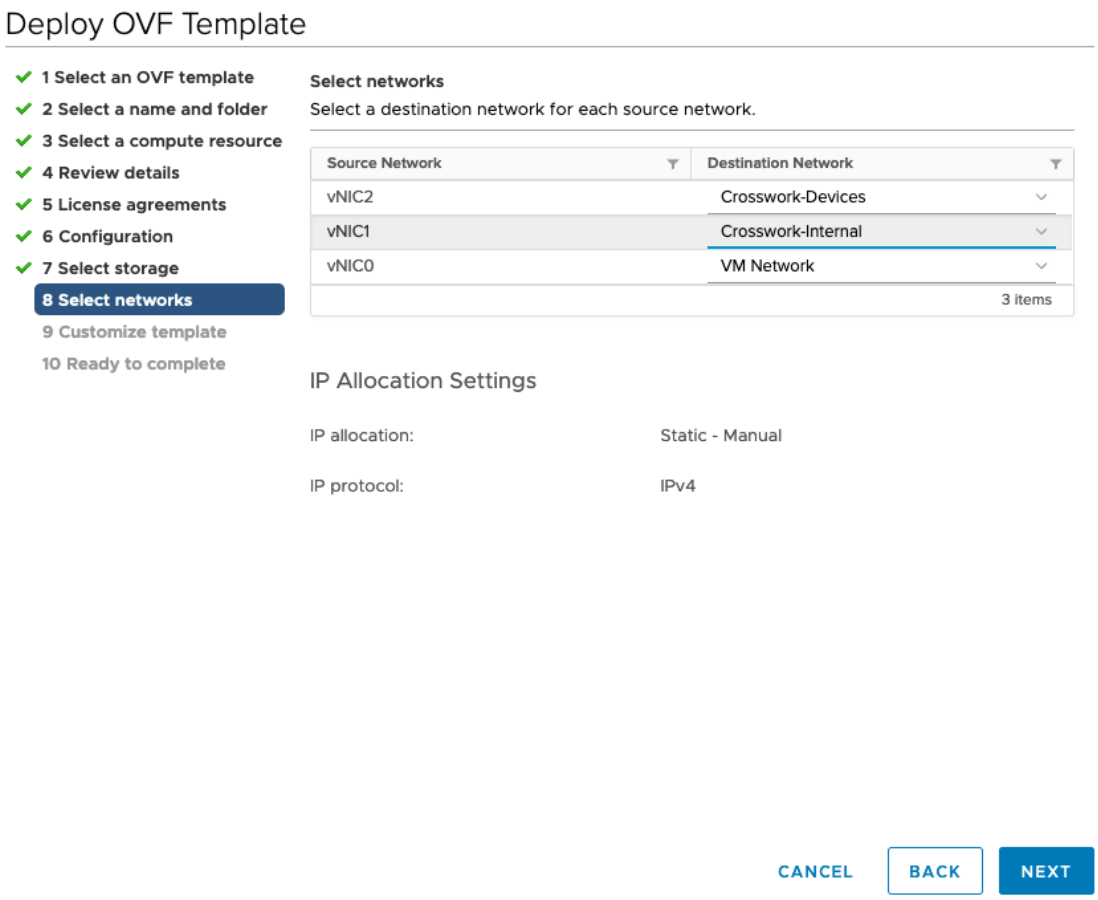
Step 9 Click Next to go to 7 Select storage, as shown in the following figure.

a) Cisco recommends that you select Thick provision lazy zeroed from the Select virtual disk format drop-down list.

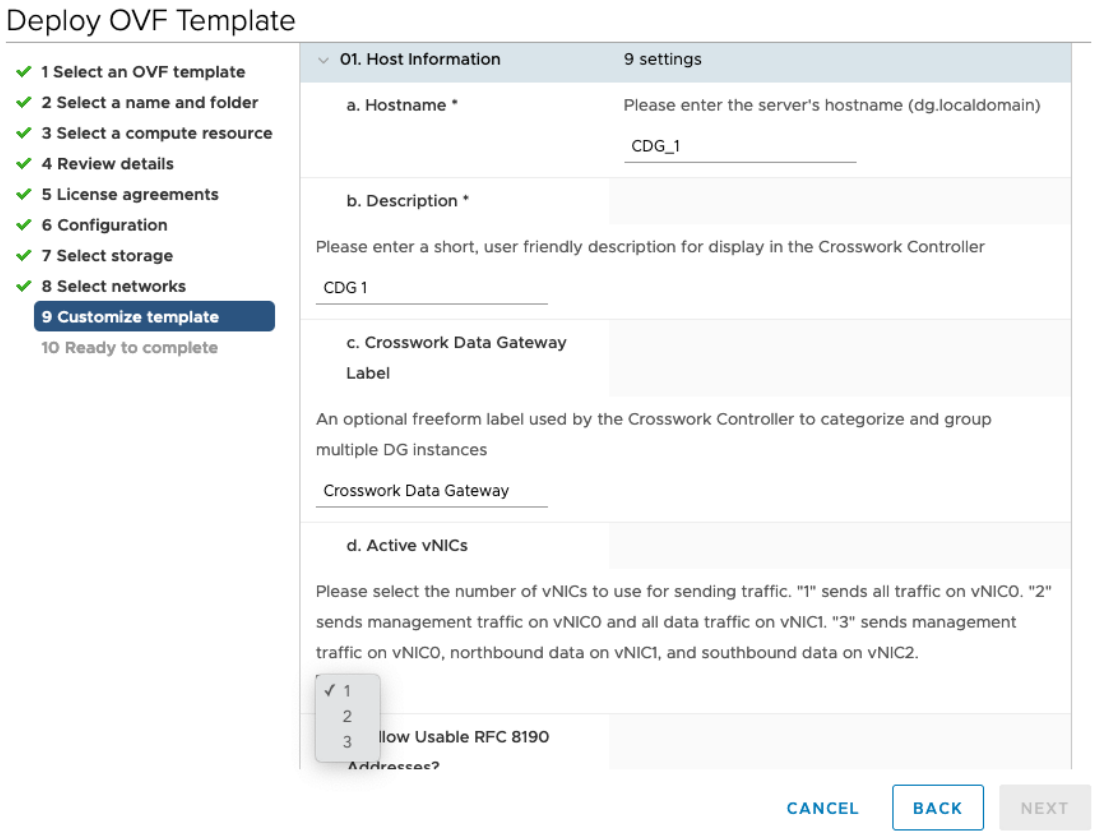
b) From the Datastores table, choose the datastore you want to use and review its properties to ensure there is enough available storage.

Step 10 Click Next to go to 8 Select networks, as shown in the following figure. In the dropdown table at the top of the page, choose the appropriate destination network for each source network, vNIC2, vNIC1, and vNIC0 respectively.

Note Starting with vNIC0, select a destination network for vNICs that will be used and leave unused vNICs set to the default value.



Step 11 Click Next to go to 9 Customize template, with the Host Information Settings already expanded. Enter the information for the parameters as explained in Table Table 1: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2.



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.

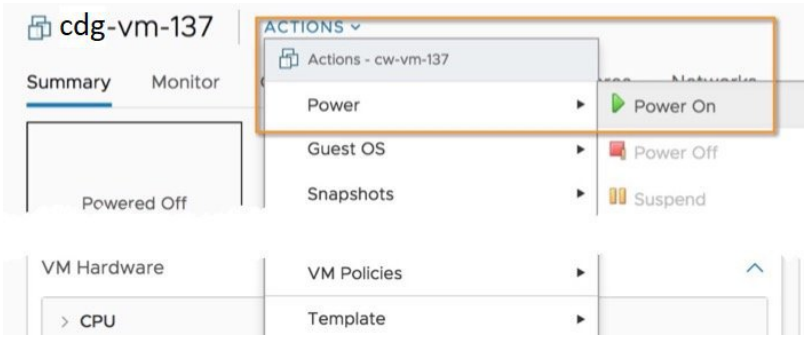
Step 13 Wait for the deployment to finish before continuing. To check the deployment status:

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:



Wait for at least 5 minutes for the VM to come up and then login 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 and any changes are done at your own risk.

What to do next

Login to Cisco Crosswork Data Gateway VM Via vCenter:

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

After you login, the Crossway Data Gateway should present you with the welcome screen and options menu indicating that the installation completed successfully. Log out and proceed with the post-installation tasks explained in the next section.

Install Cisco Crosswork Data Gateway Via OVF Tool

You can modify mandatory/optional parameters in the command/script as per your requirement and run the OVF Tool. Refer Table Table 1: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2.

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

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

# robot.ova path
ROBOT_OVA_PATH="https://engci-maven.cisco.com/artifactory/cdg-group/build/2.0.0_dg200_7_2021-03-31_18-00-00/image/cw-na-dg-2.0.0-7-TESTONLY-20210331.ova"

VM_NAME="dg-32"
DM="thin"
Deployment="onpremise-standard"

ActiveVnics="3"

Hostname="dg-32.cisco.com"
Vnic0IPv4Address="172.23.213.32"
Vnic0IPv4Gateway="172.23.213.1"
Vnic0IPv4Netmask="255.255.255.0"
Vnic0IPv4Method="Static"
Vnic1IPv4Address="32.32.32.32"
Vnic1IPv4Gateway="32.32.32.1"
Vnic1IPv4Netmask="255.255.255.0"
Vnic1IPv4Method="Static"

DNS="171.70.168.183"
NTP="ntp.esl.cisco.com"
Domain="cisco.com"

ControllerIP="172.23.213.10"
ControllerPort="30607"
ControllerSignCertChain="cw-admin@172.23.213.10:/home/cw-admin/controller.pem"
ControllerCertChainPwd="Cwork123!"

Description="Description for Cisco Crosswork Data Gateway for 32"
Label="Label for Cisco Crosswork Data Gateway dg-32"
```

```
dg_adminPassword="cisco123"
dg_operPassword="cisco123"


ProxyUsername="cisco"
ProxyPassphrase="cisco123"


SyslogAddress="127.0.0.1"
SyslogPort=514
SyslogProtocol="UDP"
SyslogTLS=False
SyslogPeerName="combo-46.cisco.com"
SyslogCertChain="root@172.23.213.46:/root/stproxy/proxycert/CA.pem"
SyslogCertChainPwd="cisco123"

# Please replace this information according to your vcenter setup
VCENTER_LOGIN="administrator%40vsphere.local:Vtsisco%40123%21@172.23.213.21"
VCENTER_PATH="DC1/host/172.23.213.8"
DS="datastore1 (5)"

ovftool --acceptAllEulas --X:injectOvfEnv --skipManifestCheck --overwrite --noSSLVerify
--powerOffTarget --powerOn \
--allowExtraConfig --extraConfig:firmware=efi --extraConfig:uefi.secureBoot.enabled=true \
--datastore="$DS" --diskMode="$DM" \
--name=$VM_NAME \
--net:"vNIC0=VM Network" \
--net:"vNIC1=DPortGroupVC-2" \
--net:"vNIC2=DPortGroupVC-1" \
--deploymentOption=$Deployment \
--prop:"ControllerIP=$ControllerIP" \
--prop:"ControllerPort=$ControllerPort" \
--prop:"ControllerSignCertChain=$ControllerSignCertChain" \
--prop:"ControllerCertChainPwd=$ControllerCertChainPwd" \
--prop:"Hostname=$Hostname" \
--prop:"Description=$Description" \
--prop:"Label=$Label" \
--prop:"ActiveVnics=$ActiveVnics" \
--prop:"Vnic0IPv4Address=$Vnic0IPv4Address" \
--prop:"Vnic0IPv4Gateway=$Vnic0IPv4Gateway" \
--prop:"Vnic0IPv4Netmask=$Vnic0IPv4Netmask" \
--prop:"Vnic0IPv4Method=$Vnic0IPv4Method" \
--prop:"Vnic1IPv4Address=$Vnic1IPv4Address" \
--prop:"Vnic1IPv4Gateway=$Vnic1IPv4Gateway" \
--prop:"Vnic1IPv4Netmask=$Vnic1IPv4Netmask" \
--prop:"Vnic1IPv4Method=$Vnic1IPv4Method" \
--prop:"DNS=$DNS" \
--prop:"NTP=$NTP" \
--prop:"dg-adminPassword=$dg_adminPassword" \
--prop:"dg-operPassword=$dg_operPassword" \
--prop:"Domain=$Domain" $ROBOT_OVA_PATH "vi://$VCENTER_LOGIN/$VCENTER_PATH"
```

Step 1 Open a command prompt.

Step 2 Navigate to the location where you installed the OVF Tool.

Step 3 Run the OVF Tool in one of the following ways:

a) Using the command

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

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

For example,

```
ovftool --acceptAllEulas --skipManifestCheck --X:injectOvfEnv -ds="datastore130-2"
 --deploymentOption="onpremise-standard" --diskMode="thin" --prop:"ControllerIP=<controller-ip>"
 --prop:"ControllerPort=30607" --prop:"ControllerSignCertChain=<location of controller.pem file>"

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

b) Using the script

If you want to execute the script thast you have created containing the command and arguments, run the following command:

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

Once the VM powers up, log into the VM. See Login into Crosswork Data Gateway VM. After you login, the Crossway Data Gateway should present you with the welcome screen and options menu indicating that the installation completed successfully. Log out and proceed with the post-installation tasks explained in the next section.

Install Cisco Crosswork Data Gateway on Cisco CSP

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

Step 1 Download the Cisco Crosswork Data Gateway **qcow2** package:

a) Download Cisco Crosswork Data Gateway `qcow2` package from cisco.com to your local machine or a location on your local network that is accessible to your Cisco CSP. For the purpose of these instructions, we will use the package name "cw-na-dg-2.0.0-18-release-qcow2-pkg.tar.gz".

b) Unzip the `qcow2` package with the following command:

```
tar -xvf cw-na-dg-2.0.0-18-release-qcow2-pkg.tar.gz
```

The content of the `qcow2` package is unzipped to a new directory (e.g. `cw-na-dg-2.0.0-18-release-qcow2`).

This new directory will contain the Cisco Crosswork Data Gateway `qcow2` build (e.g. cw-na-dg-2.0.0-18-release-20210409.tar.gz) and other files necessary to validate the build.

Step 2 (optional) Verify the Cisco Crosswork Data Gateway **qcow2** package:

a) Navigate to the directory created in the previous step.

b) Use the following command to verify the signature of the build:

Note The machine where the script is being run needs HTTP access to cisco.com. Please contact Cisco Customer Experience team if access to cisco.com is not possible due to security restrictions, or if you did not get a successful verification message after running the script.

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

Note The cisco_x509_verify_release.py script is only compatible with python 2. Instead of using the provided script, you can also calculate and verify the md5 or SHA512 checksum of the file originally downloaded from Cisco against the checksum posted on Cisco.com.

Step 3 Prepare Cisco Crosswork Data Gateway Service Image for upload to Cisco CSP:

a) The Cisco Crosswork Data Gateway `qcow2` build is a tarball of the `qcow2` and `config.txt` files. Unzip the `.tar.gz` (e.g. cw-na-dg-2.0.0-18-release-20210409.tar.gz) with the following command:

```
tar -xvf ccw-na-dg-2.0.0-18-release-20210409.tar.gz
```

b) Open the `config.txt` file and modify the parameters as per your installation requirements. See Section Table 1: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2.

Following parameters have pre-defined values:

- Deployment
  - Use "Crosswork On-Premise" for Crosswork On-Premise.
- Profile
  - Use "Standard" for standard deployment.
  - Use "Extended" for extended deployment.

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

```
ActiveVnics=
AuditdAddress=
AuditdPort=
ControllerCertChainPwd=
ControllerIP=
ControllerPort=
ControllerSignCertChain=
ControllerTlsCertChain=
Deployment=Crosswork On-Premise
Description=
DGAppdataDisk=
DGCertChain=
DGCertChainPwd=
DGCertKey=
DNS=changeme
DNSSEC=False
DNSTLS=False
Domain=changeme
EnrollmentPassphrase=
EnrollmentURI=
Hostname=changeme
Label=
LLMNR=False
mDNS-False
NTP=changeme
NTPAuth=False
```

```
NTPKey=
NTPKeyFile=
NTPKeyFilePwd=
Profile=Standard
ProxyBypass=
ProxyCertChain=
ProxyCertChainPwd=
ProxyPassphrase=
ProxyURL=
ProxyUsername=
SyslogAddress=
SyslogCertChain=
SyslogCertChainPwd=
SyslogPeerName=
SyslogPort=514
SyslogProtocol=UDP
SyslogTLS=False
UseRemoteAuditd=False
UseRemoteSyslog=False
Vnic0IPv4Address=0.0.0.0
Vnic0IPv4Gateway=0.0.0.1
Vnic0IPv4Method=None
Vnic0IPv4Netmask=0.0.0.0
Vnic0IPv6Address=::0
Vnic0IPv6Gateway=::1
Vnic0IPv6Method=None
Vnic0IPv6Netmask=64
Vnic1IPv4Address=0.0.0.0
Vnic1IPv4Gateway=0.0.0.1
Vnic1IPv4Method=None
Vnic1IPv4Netmask=0.0.0.0
Vnic1IPv6Address=::0
Vnic1IPv6Gateway=::1
Vnic1IPv6Method=None
Vnic1IPv6Netmask=64
Vnic2IPv4Address=0.0.0.0
Vnic2IPv4Gateway=0.0.0.1
Vnic2IPv4Method=None
Vnic2IPv4Netmask=0.0.0.0
Vnic2IPv6Address=::0
Vnic2IPv6Gateway=::1
Vnic2IPv6Method=None
Vnic2IPv6Netmask=64
dg-adminPassword=changeme
dg-operPassword=changeme
```

Step 4 Upload Cisco Crosswork Data Gateway Service Image to Cisco CSP:

a) Log in to the Cisco CSP.

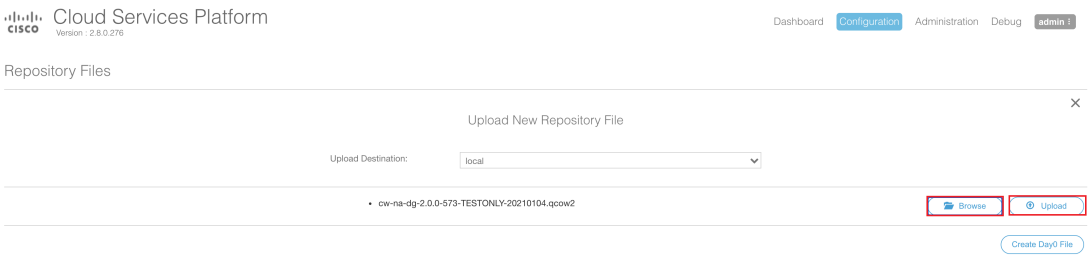
b) Go to Configuration > Repository.

c) On the Repository Files page, Click ⊞ button.

d) Select an Upload Destination.

e) Click Browse, navigate to the `qcow2` file, click Open and then Upload.

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



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

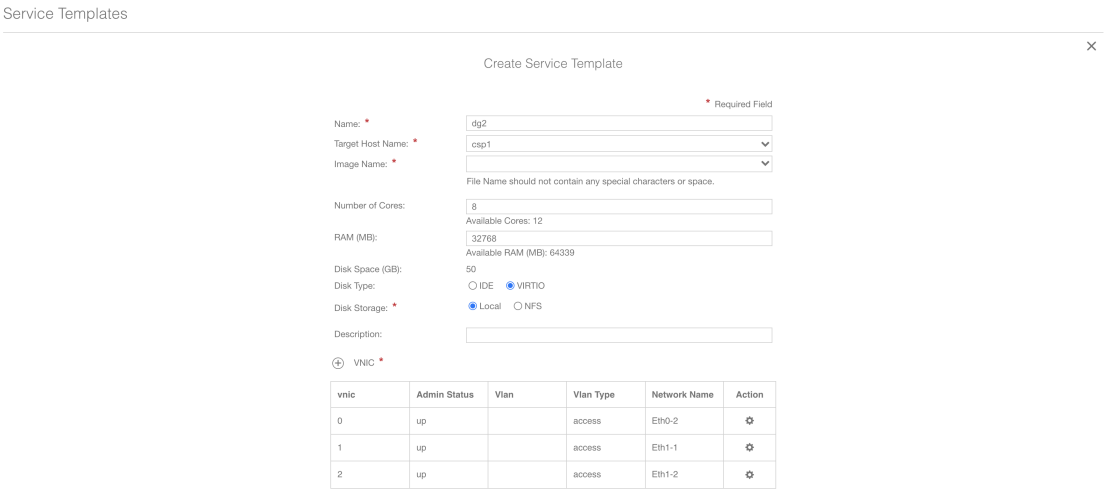
Step 5 Create Crosswork Data Gateway VM:

a) Go to Configuration > Services.

b) On the Service page, click ⊞ button.

c) Check Create Service option.

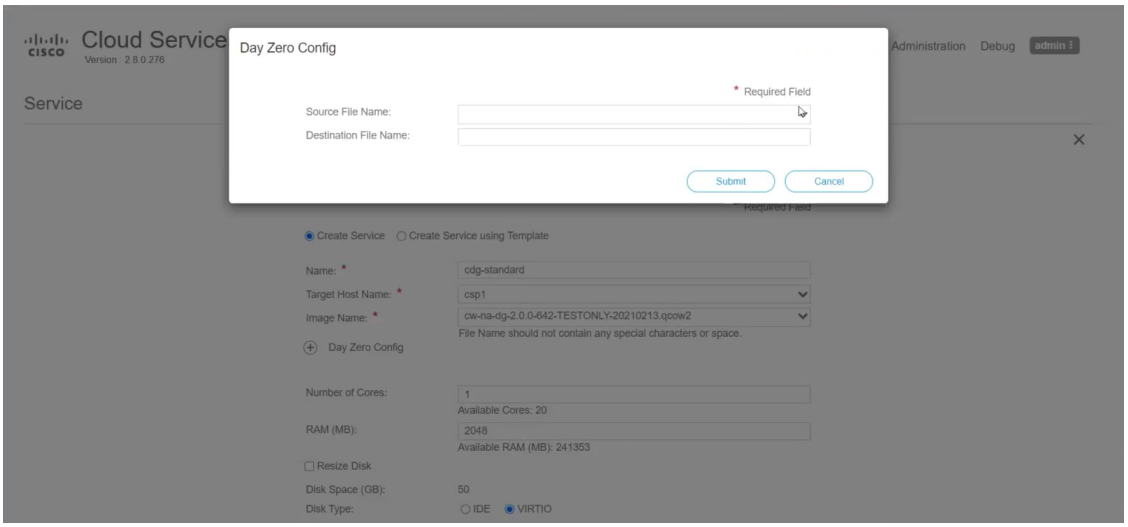
The Create Service Template page is displayed.



d) Enter the values for the following fields:

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

e) Click Day Zero Config.



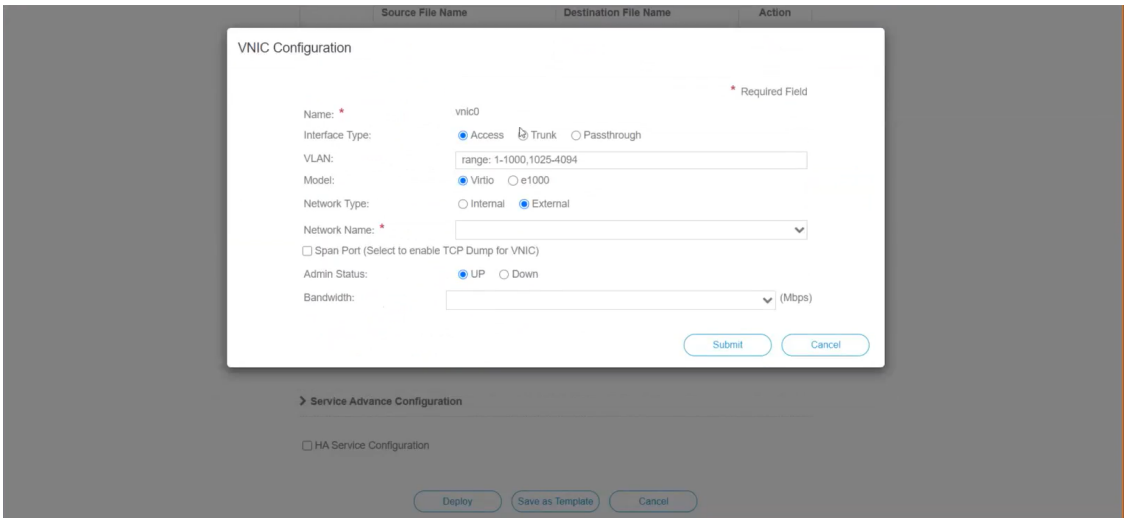
In the Day Zero Config dialog box, do the following:

1. From the Source File Name drop-down list, select a day0 configuration file i.e., the `config.txt` file that you modifed and uploaded earlier.
2. In the Destination File Name field, specify the name of the day0 destination text file. This must always be "config.txt".
3. Click Submit.

f) Enter the values for the following fields:

Field	Description
Number of Cores	Standard: 8 Extended: 16
RAM (MB)	Standard: 32768 Extended: 98304

g) Click VNIC.



In the VNIC Configuration dialog box, do the following:

Note The VNIC Name is set by default.

1. Select the Interface Type as Access.
2. Select the Model as Virtio.
3. Select the Network Type as External.
4. Select Network Name:

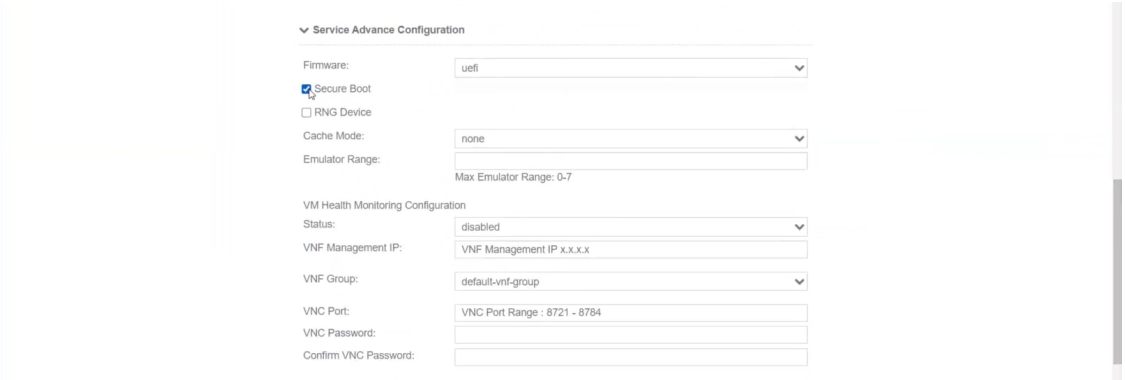
For VNIC...	Select...
vnic0	Eth0-1
vnic1	Eth1-1
vnic2	Eth1-2

5. Select Admin Status as UP.
6. Click Submit.
7. Repeat Steps i to vi for vNIC1 and vNIC2.

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

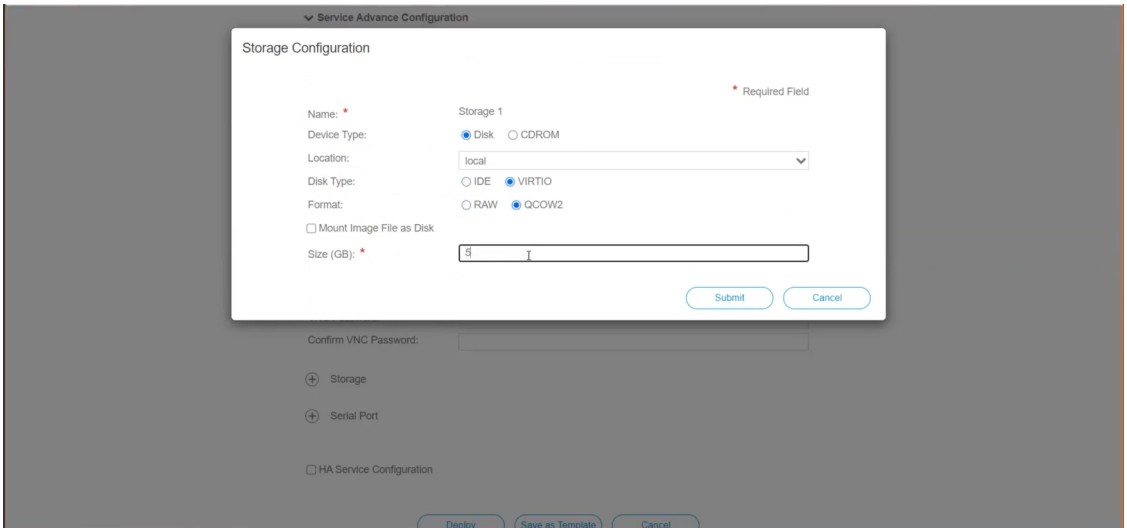
h) Expand the Service Advance Configuration and for Firmware, select uefi from the drop-down.

Check the Secure Boot checkbox.



i) Click Storage.

In the Storage Configuration dialog box, do the following:

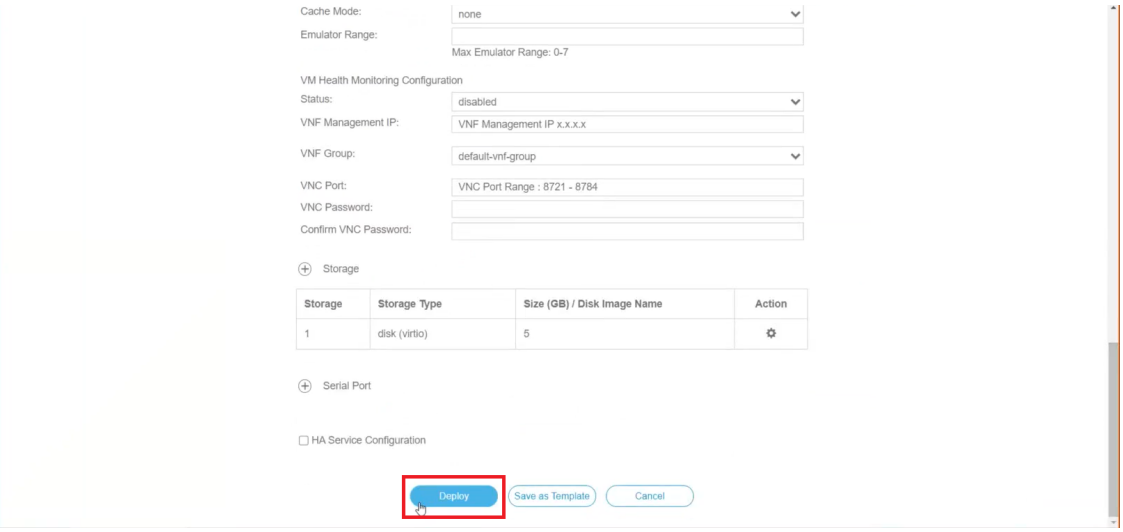


Field	Description
Name	Name of the storage. This is specified by default.

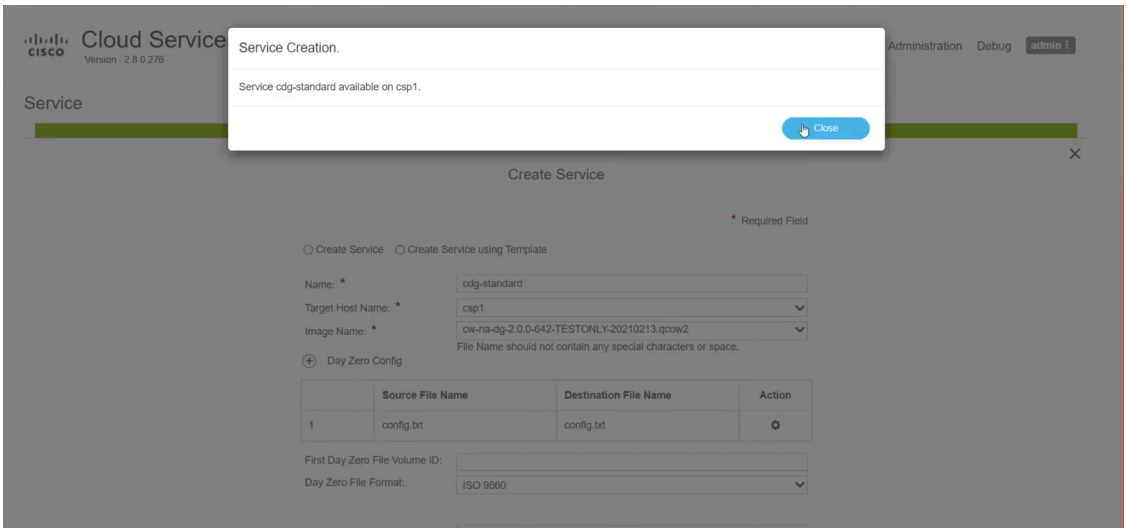
Field	Description
Device Type	Select Disk.
Location	Select local.
Disk Type	Select VIRTIO.
Format	Select QCOW2.
Mount image file as disk?	Leave this unchecked.
Size (GB)	Enter the disk size (5 for Standard and 500 for Extended.)

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

j) Click Deploy.



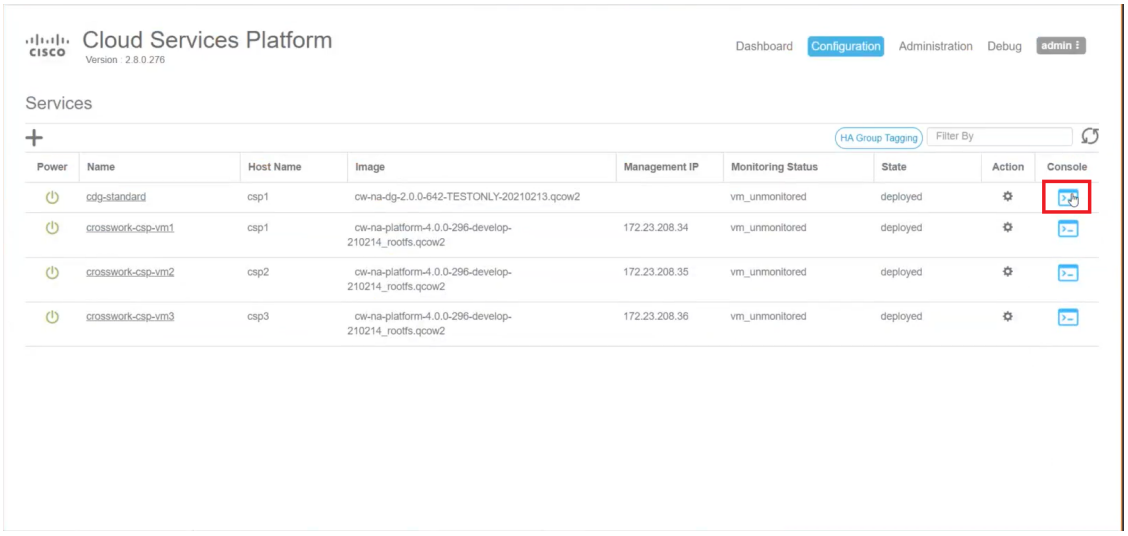
You will see a similar message once the service has successfully deployed. Click Close.



Step 6 Deploy Cisco Crosswork Data Gateway service:

a) Go to Configuration > Services.

b) In the Services table, click the console icon under Console column for the Cisco Crosswork Data Gateway service you created above.



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

d) Once the Cisco Crosswork Data Gateway service connects, enter username and password.

The Cisco Crosswork Data Gateway console is available.

After you login, the Crossway Data Gateway should present you with the welcome screen and options menu indicating that the installation completed successfully. Log out and proceed with the post-installation tasks explained in the next section.

Post-installation Tasks

After installing Cisco Crosswork Data Gateway, complete the following tasks:

- Access Crosswork Data Gateway Via SSH, on page 26
- Configure Timezone, on page 27
- Log Out, on page 28

Access Crosswork Data Gateway Via SSH

Verify that you can access the Cisco Crosswork Data Gateway VM from SSH.

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

Follow these steps to login via SSH.

Step 1 Run the following command:

ssh <username>@<ManagementNetworkIP>

where ManagementNetworkIP is the management network IP address.

For example,

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

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

The Crosswork Data Gateway flash screen opens prompting for password.

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

Note If you are unable to log in via SSH, contact Cisco Customer Experience team for assistance.

Configure Timezone

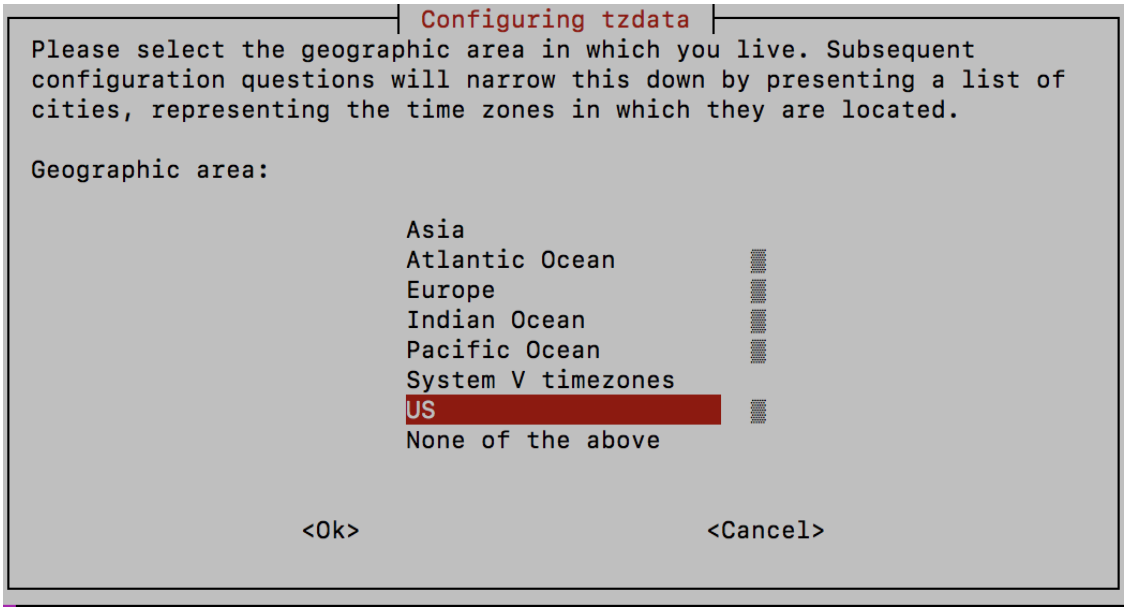
The Crosswork Data Gateway first launches with default timezone as UTC.

Follow the steps to configure timezone:

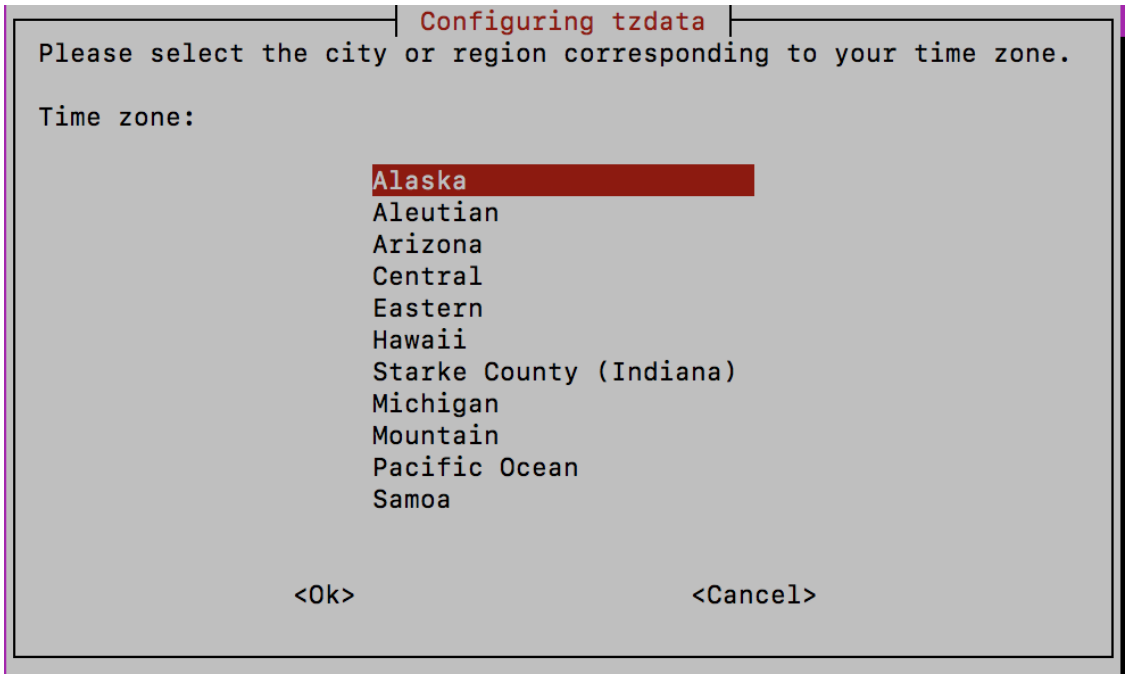
Step 1 In Crosswork Data Gateway VM interactive menu, select Change Current System Settings.

Step 2 Select 9 Configure Timezone.

Step 3 Select the geographic area in which you live.



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



Step 5 Select OK to save the settings.

Step 6 Reboot the Crosswork Data Gateway VM so that all processes pick up the new timezone.

Log Out

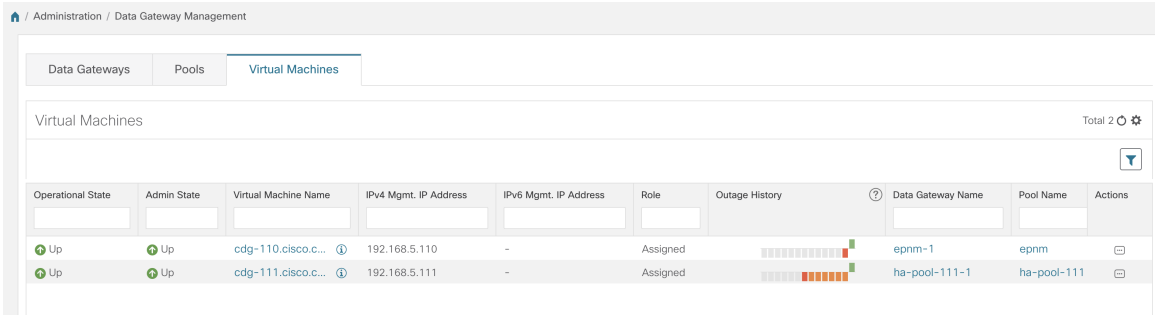
To log out, select option l Logout from the Main Menu and press Enter or click OK.

Cisco Crosswork Data Gateway Authentication and Enrollment

Once the Crosswork Data Gateway is deployed, it identifies itself to the Cisco Crosswork and enrolls itself with it. 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.

Once the connectivity is established, the Crosswork Data Gateway instance confirms the identity of the controller and offers its own proof of identity via signed certificates during this initial connection.

To verify if Crosswork Data Gateway VM was enrolled with Cisco Crosswork, in Cisco Crosswork UI, go to Administration > Data Gateway Management. Click on Virtual Machines tab. All of the Cisco Crosswork Data Gateway VMs that have enrolled with Cisco Crosswork are displayed here.



Newly installed Crosswork Data Gateway VMs will have the Operational Status as "Degraded" until they enroll successfully with Cisco Crosswork.

Note Previously onboarded Cisco Crosswork Data Gateway VMs that have the Operational Status as "Degraded" will need to be investigated to determine what is wrong.

While it depends on the bandwidth between the Crosswork Data Gateway VMs and Cisco Crosswork, this operation typically takes less than 5 minutes. Click the icon in the Virtual Machines pane to refresh the pane to reflect the latest operational status of the Crosswork Data Gateway VMs. If the Crosswork Data Gateway VMs fail to enroll, contact Cisco Customer Experience team for assistance.

Crosswork Data Gateway VMs that have the Role as "Unassigned" need to be assigned to a pool before they can used.

Note 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.

Create a Cisco Crosswork Data Gateway Pool

A pool ensures that your devices are managed and collections occur with minimal to no disruption. A pool can consist of one or more Cisco Crosswork Data Gateway VMs with an option to enable high availability. If a Crosswork Data Gateway VM goes down, Cisco Crosswork automatically replaces that VM with a spare VM in the pool. Devices and existing collection jobs are automatically moved from the failed VM to the spare Crosswork Data Gateway VM. Once the VM that went down becomes active again, it becomes the new spare VM in the pool.

You can create multiple pools. But, you must create at least one pool and assign Crosswork Data Gateway VM to it.

Note We recommend creating pools with Cisco Crosswork Data Gateways of similar profiles i.e., either all standard Crosswork Data Gateways or all extended Crosswork Data Gateways in a pool. Heterogenous pools i.e., pools with different types of Crosswork Data Gateways must only be created for device or job migration.

Follow the steps to create a Cisco Crosswork Data Gateway pool:

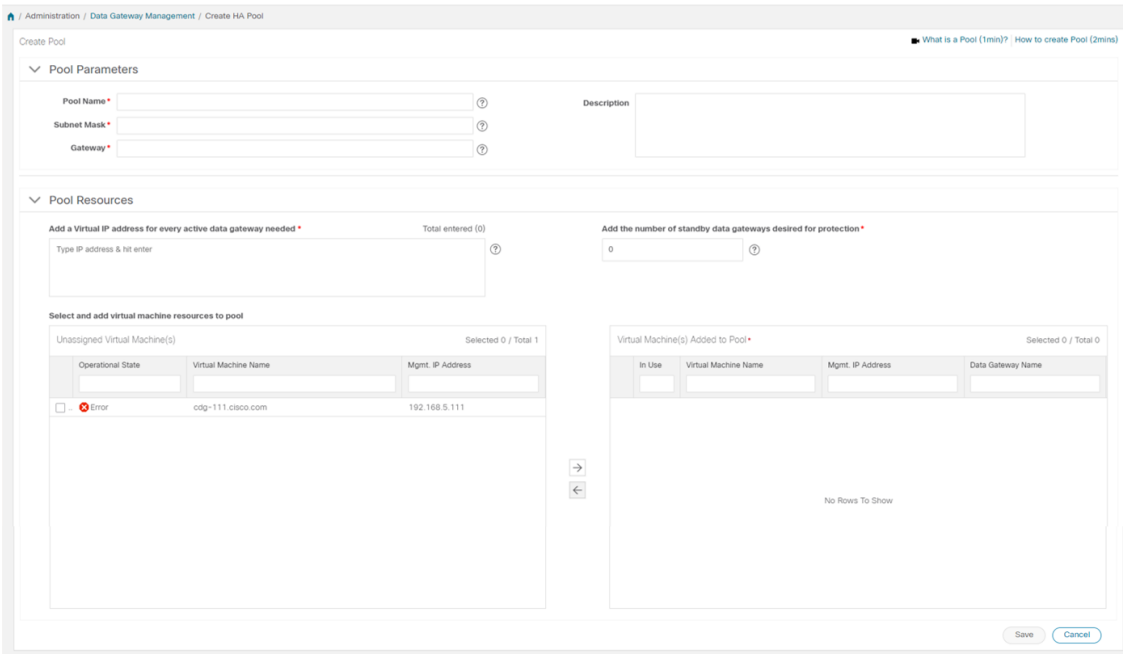
Before you begin

Before you create a Cisco Crosswork Data Gateway pool, ensure that:

- You have installed all Cisco Crosswork Data Gateway VMs that you wish to add to the pool.
- Have network information such as Subnet mask and Gateway information ready.
- Decide if you wish to enable high availability for the pool.

Step 1 From the main menu, choose Administration > Data Gateway Management and click Pools tab.

Step 2 In the Pools tab, click ⊞ button. The Create Pool page opens.



Step 3 In the Pool Parameters pane, enter the values for the following parameters:

Field	Description
Pool Name	Name of the pool that suitably describes the network.
Subnet Mask	Subnet mask for each Cisco Crosswork Data Gateway to communicate with the devices.
Gateway	Gateway address for each Cisco Crosswork Data Gateway to communicate with the devices. **Note** This field is not applicable if a Cisco Crosswork Data Gateway VM has fewer than 3 vNICs.
Description	A description of the pool.

Step 4 In the Pool Resources pane, add the following details:

- A virtual IP address for every active Crosswork Data Gateway VM.

  Note Enter either IPv4 or IPv6 addresses that is not in use on the network. Combination is not allowed.

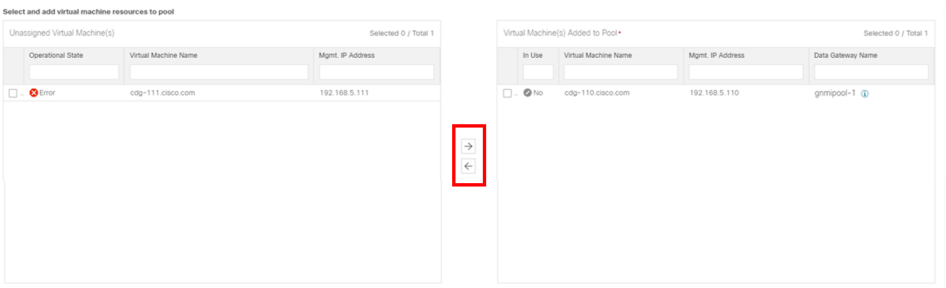
- Number of standby Cisco Crosswork Data Gateways desired for protection. Entering a value greater than 0 in this field enables high availability for the pool.

The number of Crosswork Data Gateway VMs you add to the pool should be equal to the total number of virtual IPs and standby Crosswork Data Gateway VMs. For example, if you have entered 3 virtual IPs and wish to have 2 standy VMs, you should add 5 Cisco Crosswork Data Gateway VMs to the pool.

Step 5 Add Cisco Crosswork Data Gateway VM to the pool.

- To add a Cisco Crosswork Data Gateway VM to the pool, select VMs from the Unassigned Virtual Machine(s) on the left and click right arrow to move the VMs to the Virtual Machine(s) Added to Pool.
- To remove a Cisco Crosswork Data Gateway VM from the pool, select VMs from the Virtual Machine(s) Added to Pool on the right and click left arrow to move these to the Unassigned Virtual Machine(s).

  Note A Cisco Crosswork Data Gateway VM can be taken out of the pool only if all devices have been unmapped from it. Once a Crosswork Data Gateway VM is removed from the pool, a standy Crosswork Data Gateway VM in the same pool becomes its replacement automatically.



Step 6 Click Save.

Once you add a Cisco Crosswork Data Gateway VM to a pool, a virtual Crosswork Data Gateway gets created automatically and is visible under Data Gateways tab. You can then attach or detach devices to the virtual Crosswork Data Gateway and run collection jobs.

Note You can attach or detach devices only to a virtual Crosswork Data Gateway.

Troubleshoot Crosswork Data Gateway Installation and Enrollment

If Crosswork Data Gateway fails to auto-enroll with Cisco Crosswork, you can collect Crosswork Data Gateway showtech (Main menu > 5 Troubleshooting > Run show-tech) and check for the reason in

`controller-gateway` logs. If there are session establishment/certificate related issues, ensure that the `controller.pem` certificate is uploaded using the interactive menu.

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 2: Troubleshooting the Installation/Enrollment

Issue	Action
1. Cannot enroll Crosswork Data Gateway with Cisco Crosswork	
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 into the Crosswork Data Gateway VM. 2. From the main menu, go to 5 Troubleshooting > Run show-tech. Enter the destination to save the tarball containing logs and vitals and click OK. In the show-tech logs (in file `session.log` at location `/cdg/logs/components/controller-gateway/session.log`), if you see the error `UNAUTHENTICATED:invalid certificate. reason: x509: certificate has expired or is not yet valid`, then there is a clock-drift between Crosswork Data Gateway and Cisco Crosswork. 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 re-enrolling Crosswork Data Gateway.
2. Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "Could not collect vitals"	

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 into the Crosswork Data Gateway VM. 2. From the main menu, select 5 Troubleshooting > Run show-tech. Enter the destination to save the tarball containing logs and vitals and click OK. In the show-tech logs (in file `gateway.log` at location `/cdg/logs/components/controller-gateway/gateway.log`), if you see certificate errors, then re-upload the Controller Signing Certificate, as explained in the steps below: 1. From the main menu, select 3 Change Current System Settings > 7 Import Certification. 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.
3. Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "gRPC connection cannot be established"	
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. Re-upload the certificate file as explained in the troubleshooting scenario 2. above. 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 7 Reboot VM and click OK. c. Once the reboot is complete, check if the Crosswork Data Gateway's operational status is Up.
Crosswork Data Gateway goes into Error state	Check the vNIC values in the OVF template in case of vCenter and config.txt in case of Cisco CSP.
Crosswork Data Gateway enrollment with 1 NIC Cisco Crosswork fails	Check the vNIC values in the OVF template in case of vCenter and config.txt in case of Cisco CSP. 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.

Issue	Action
Crosswork Data Gateway deploys standard profile instead of extended	Check the deploymentoption property in the OVF template in case of vCenter and config.txt in case of Cisco CSP. If "deploymentoption" property mismatches or does not exist for extended profile template, then Crosswork Data Gateway deploys standard profile.

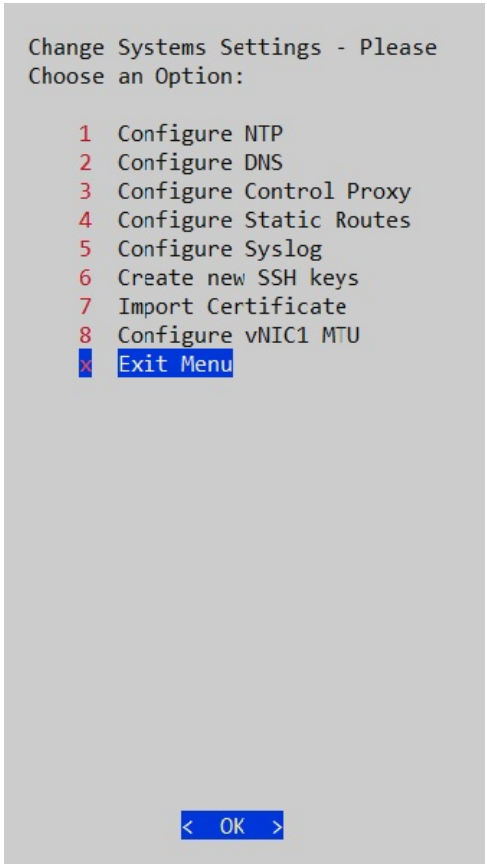
Import Controller Signing Certificate File

Follow these steps to import controller signing certificate file.

Note This is needed only if you have not specified Controller Signing Certificate File URI under the Controller Settings in the OVF template. Otherwise, the file will be automatically imported after the VM boots.

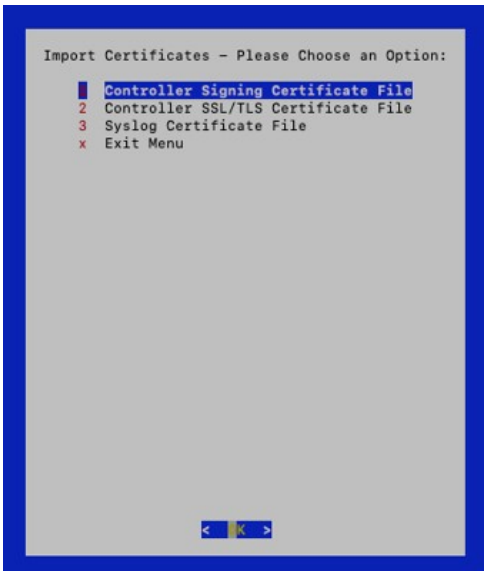
Step 1 From the Cisco Crosswork Data Gateway VM's interactive menu, select 3 Change Current System Settings.

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 pasword).

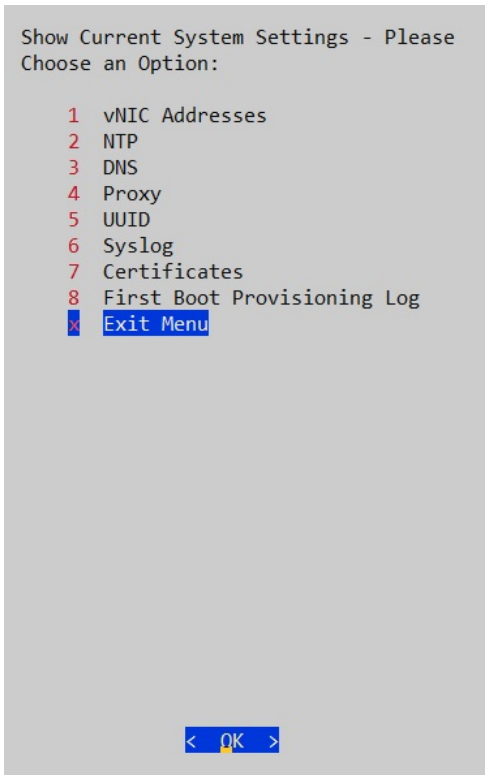
The certificate file is imported.

Step 6 Follow the next procedure to check if the certificate is installed.

View the Controller Signing Certificate File

Follow the 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.