Installation Tasks

This section contains the following topics:

Install Cisco Crosswork Data Gateway

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

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

Cisco Crosswork Data Gateway Deployment and Set Up Workflow

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

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

VMware	Install Crosswork Data Gateway Using vCenter vSphere Client, on page 10
	Install Crosswork Data Gateway Via OVF Tool, on page 16
Cisco CSP	Install Crosswork Data Gateway on Cisco CSP, on page 18

3. Enroll Cisco Crosswork Data Gateway with Crosswork Cloud.

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

- Generate Enrollment Package, on page 26
- Export Enrollment Package, on page 27

Cisco Crosswork Data Gateway Deployment Parameters and Scenarios

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

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

User Accounts

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

- Cisco Crosswork Data Gateway administrator, with the username, **dg-admin** and the password set during installation. The administrator uses this ID to log in and troubleshoot Cisco Crosswork Data Gateway.
- Cisco Crosswork Data Gateway operator, with the username, **dg-oper** and the password set during installation. This is a read-only user and has permissions to perform all ‘read’ operations and limited ‘action’ commands.
- A **dg-tac** user account that is used to enable Cisco to assist you in troubleshooting issues with the Crosswork Data Gateway. (Enable TAC Shell Access). The temporary password for this account is created when you enable troubleshooting access.

To know what operations an admin and operator can perform, see Section Supported User Roles.

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

Installation Parameters and Scenarios

In the following table:

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

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

Table 1: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios

Name	Parameter	Description	Additional Information
Host Information			
Hostname*	`Hostname`	Name of the Cisco Crosswork Data Gateway VM specified as a fully qualified domain name (FQDN). **Note** In larger systems you are likely to have more than one Cisco Crosswork Data Gateway VM. The hostname must, therefore, be unique and created in a way that makes identifying a specific VM easy.	
Description*	`Description`	A detailed description of the Cisco Crosswork Data Gateway.	
Label	`Label`	Label used by Cisco Crosswork Cloud to categorize and group multiple Cisco Crosswork Data Gateways.	
Deployment	`Deployment`	Parameter that conveys the controller type. Specify the value as `cloud` for Cloud deployment.	This paramter is pre-defined for CSP installation. You will need to specify this parameter only in case of VMware or OVF tool installation.

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

Name	Parameter	Description	Additional Information
Data Disk Size	`DGAppdataDisk`	Size in GB of a second data disk. The default size is 20GB.	
Passphrases			
dg-admin Passphrase*	`dg-adminPassword`	The password you have chosen for the dg-admin user. Password must be 8-64 characters.	
dg-oper Passphrase*	`dg-operPassword`	The password you have chosen for the dg-oper user. Password must be 8-64 characters.	
Interfaces **Note** You must select either an IPv4 or IPv6 address. Selecting **None** in both **vNICx IPv4 Method** field and **vNICx IPv6 Method** field will result in a non-functional deployment.			
vNICx IPv4 Address (vNIC0, vNIC1 and vNIC2 based on the number of interfaces you choose to use)			
vNICx IPv4 Method* For example, the parameter name for vNIC0 is vNIC0 IPv4 Method.	`VnicxIPv4Method` For example, the parameter name for vNIC0 is `Vnic0IPv4Method`.	**None** or**Static** The default value for **Method** is **None**. To use IPv4 address, select **Method** as **Static** and select the **vNICx IPv6 Method** as **None**.	If you have selected **Method** as **Static**, enter information in **Address**, **Netmask**, **Skip Gateway**, and **Gateway** fields.
vNICx IPv4 Address	`VnicxIPv4Address`	IPv4 address of the vNICx interface.	
vNICx IPv4 Netmask	`VnicxIPv4Netmask`	IPv4 netmask of the vNICx interface in dotted quad format.	
vNICx IPv4 Skip Gateway	`VnicxIPv4SkipGateway`	Options are `yes` or `no`. Selecting `yes` skips configuring a gateway.	
vNICx IPv4 Gateway	`VnicxIPv4Gateway`	IPv4 address of the vNICx gateway.	
vNICx IPv6 Address (VNIC0, VNIC1, and VNIC2 based on the number of interfaces you choose to use)			

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

Name	Parameter	Description	Additional Information
Link-Local Multicast Name Resolution*	`LLMNR`	Options are False, True, Opportunistic and Resolve. Select True to use link-local multicast name resolution. By default, this parameter is False.	
NTPv4 Servers			
NTPv4 Servers*	`NTP`	NTPv4 server list. Enter space-delimited list of IPv4/IPv6 addresses or hostnames of the NTPv4 servers accessible from the management interface.	You must enter a value here, such as pool.ntp.org. NTP server is critical for time synchronization between Cisco Crosswork Data Gateway, Crosswork Cloud, and devices. Using a non-functional or dummy address may cause issues when Crosswork Cloud and Cisco Crosswork Data Gateway try to communicate with each other. If you are not using an NTP server, ensure that time gap between Cisco Crosswork Data Gateway and Crosswork Cloud is not more than 24 hours. Else, Cisco Crosswork Data Gateway will fail to connect.
Use NTPv4 Authentication	`NTPAuth`	Select Yes to use NTPv4 authentication. The default value is No.	
NTPv4 Keys	`NTPKey`	Key IDs to map to the server list. Enter space-delimited list of Key IDs.	
NTPv4 Key File URI	`NTPKeyFile`	SCP URI to the chrony key file.	
NTPv4 Key File Passphrase	`NTPKeyFilePwd`	Password of SCP URI to the chrony key file.	
Remote Syslog Servers			

Name	Parameter	Description	Additional Information
Use Remote Syslog Server*	`UseRemoteSyslog`	Select Yes to send syslog messages to a remote host. The default value is No.	Configuring an external syslog server sends service events to the external syslog server. Otherwise, they are logged only to the Cisco Crosswork Data Gateway VM. If you want to use an external syslog server, you must specify these seven settings. **Note** The host with the URI files must be reachable on the network (from vNIC0 interface via SCP) and files must be present at the time of install.
Syslog Server Address	`SyslogAddress`	IPv4 or IPv6 address of a syslog server accessible from the management interface. **Note** If you are using an IPv6 address, surround it with square brackets ([1::1]).	
Syslog Server Port	`SyslogPort`	Port number of the optional syslog server. The port value can range between 1 and 65535. By default, this value is set to 514.	
Syslog Server Protocol	`SyslogProtocol`	Use UDP or TCP when sending syslog. Default value is UDP.	
Use Syslog over TLS?	`SyslogTLS`	Select Yes to use TLS to encrypt syslog traffic. By default, this parameter is set to No.	
Syslog TLS Peer Name	`SyslogPeerName`	The syslog server hostname exactly as entered in the server certificate SubjectAltName or subject common name.	
Syslog Root Certificate File URI	`SyslogCertChain`	URI to the PEM formatted root cert of syslog server retrieved using SCP.	
Syslog Certificate File Passphrase	`SyslogCertChainPwd`	Password of SCP user to retrieve Syslog certificate chain.	
Remote Auditd Servers			

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

Name	Parameter	Description	Additional Information
Enrollment Destination Host and Path**	`EnrollmentURI`	SCP host and path to transfer the enrollment package using SCP (`user@host:/path/to/file`).	Cisco Crosswork Data Gateway requires the Enrollment package to enroll with Crosswork Cloud. If you specify these parameters during the installation, the enrollment package is automatically transferred to the local host once Cisco Crosswork Data Gateway boots up for the first time. If you do not specify these parameters during installation, then export enrollment package manually by following the procedure Export Enrollment Package, on page 27.
Enrollment Passphrase**	`EnrollmentPassphrase`	SCP user passphrase to transfer enrollment package.	

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

Install Crosswork Data Gateway Using vCenter vSphere Client

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

Step 1 Refer to the *Crosswork Data Gateway 3.0.x Release notes* and download the recommended Crosswork Data Gateway image file from CCO (*.ova).

Note When using the latest Mozilla Firefox version to download the .ova image, if the downloaded file has the extension as .dms, change the extension back to .ova before installation.

Warning The default VMware vCenter deployment timeout is 15 minutes. If the time taken to complete the OVF template deployment exceeds 15 minutes, vCenter times out and you will have to start over again. To prevent this, we recommend that you plan what you will enter by reviewing the template before you start the deployment.

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

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

Step 4 The VMware **Deploy OVF Template** wizard appears and highlights the first step, **1 Select template**.

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

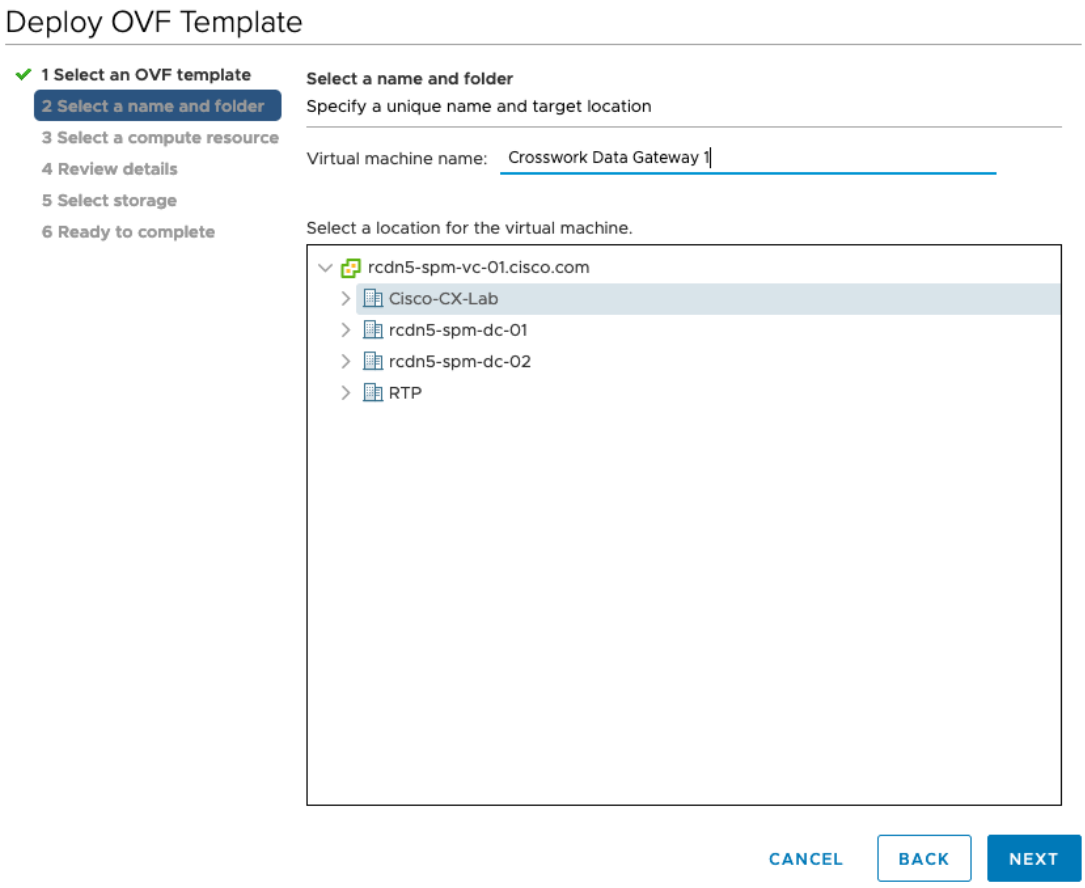
The filename is displayed in the window.

Step 5 Click **Next** to go to **2 Select name and location**, as shown in the following figure.

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

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

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



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

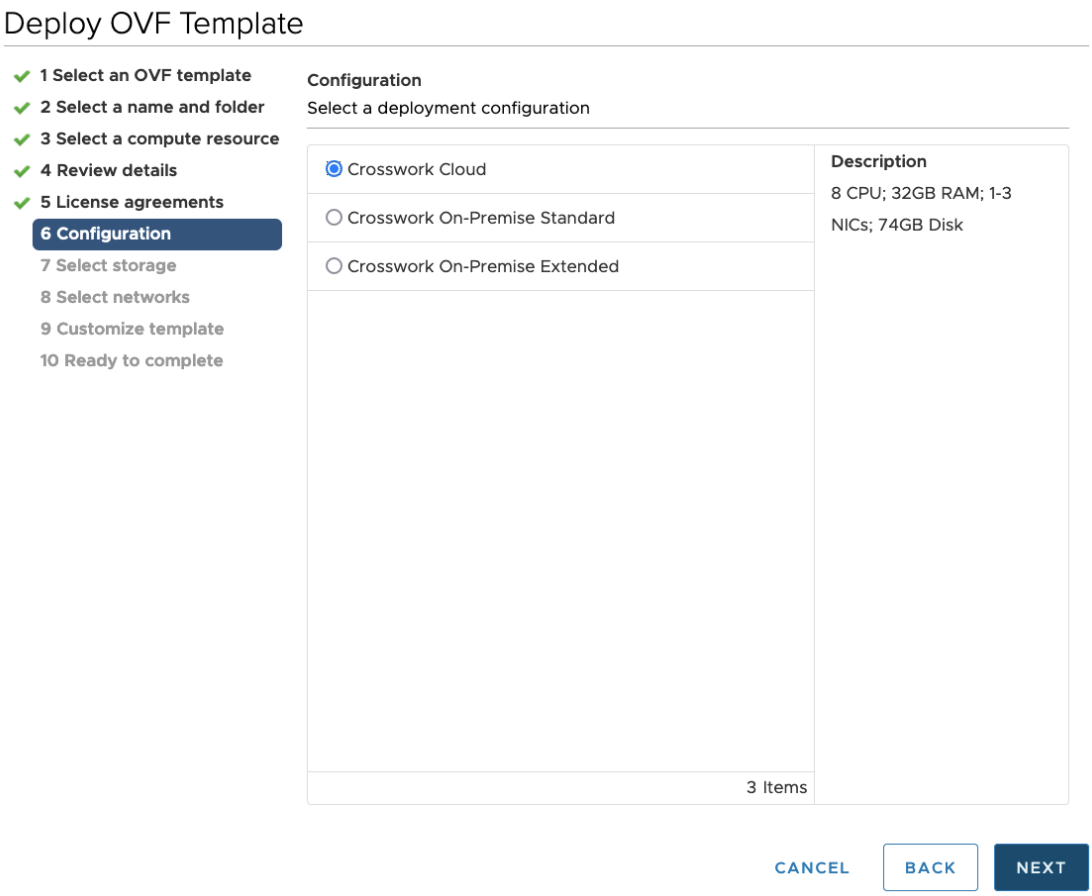
Step 7 Click **Next**. The VMware vCenter Server validates the OVA. The network speed determines how long the validation takes. When the validation is complete, the wizard moves to **4 Review details**. Review the OVA's information and then click **Next**.

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

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

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

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

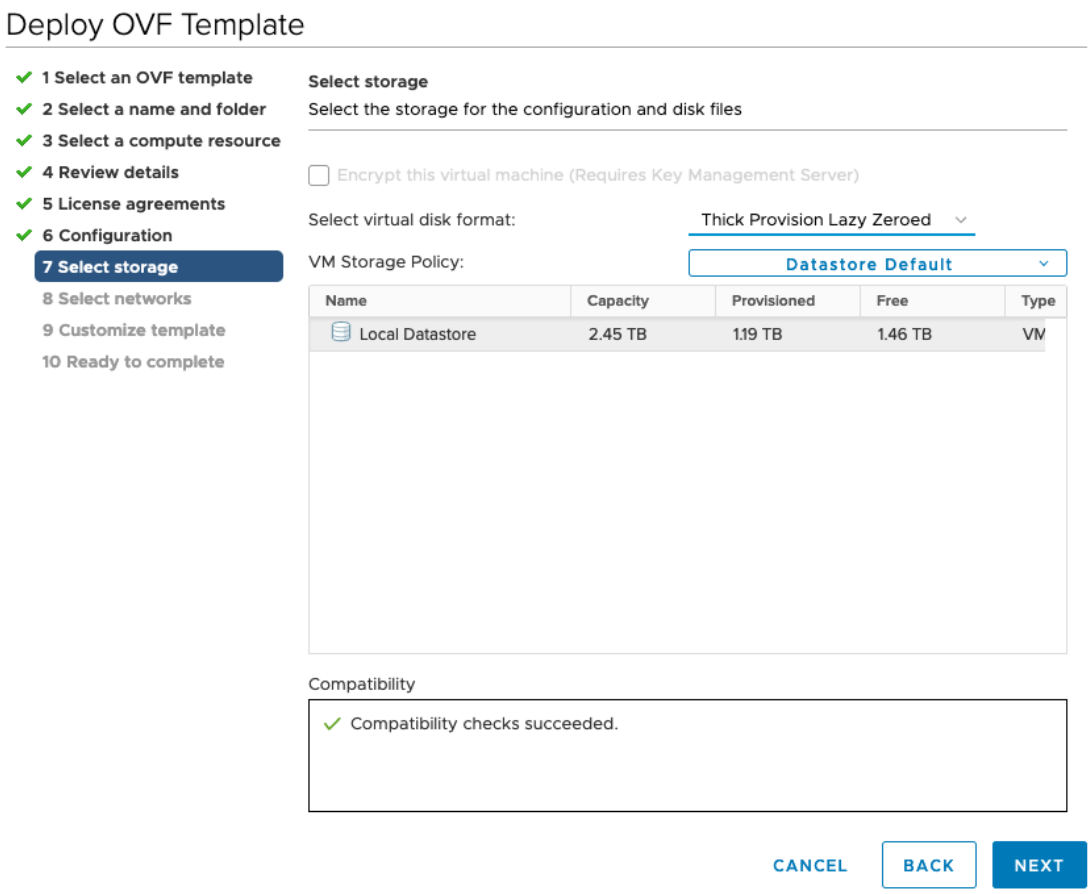


Step 10 Click **Next** to go to **7 Select storage**, as shown in the following figure.

a) In the **Select virtual disk format** field,

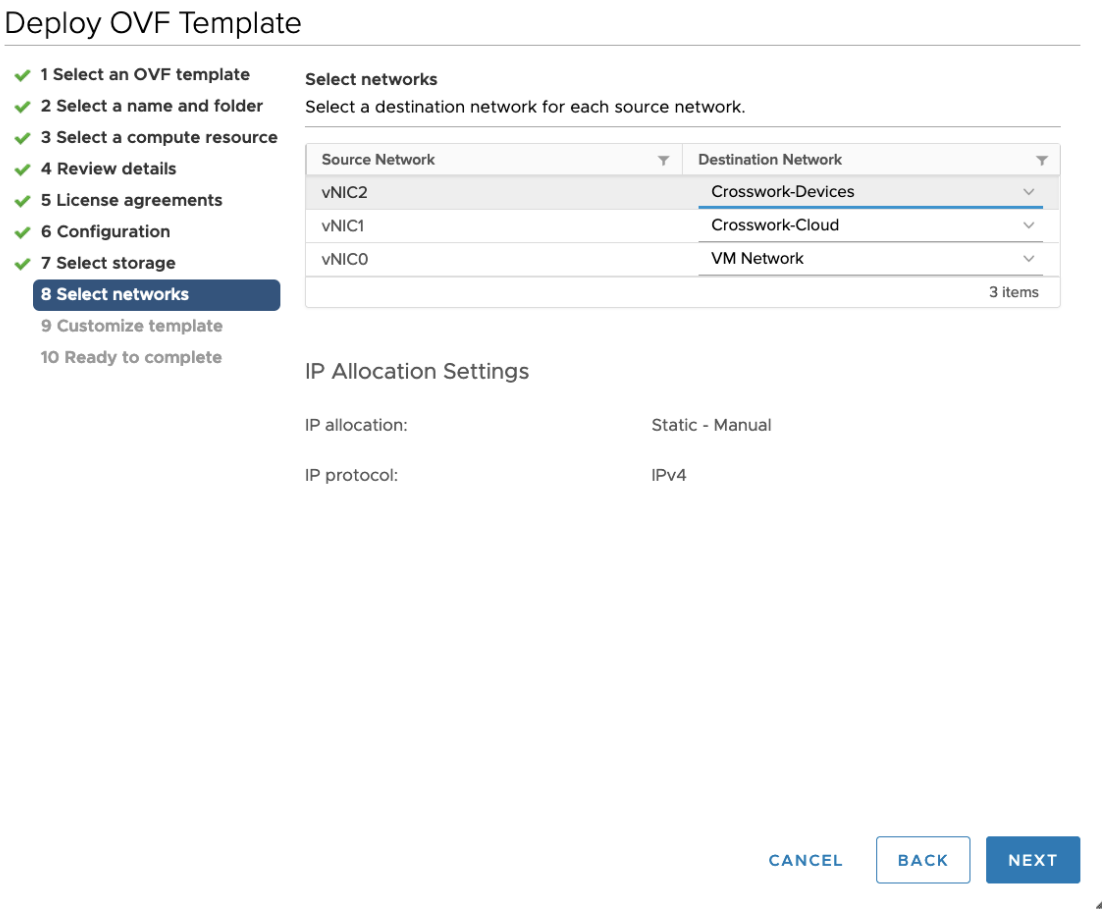
- For production environment, choose **Thick provision lazy zeroed**.
- For development environment, choose **Thin provision**.

b) From the **Datastores** table, choose the datastore you want to use.



Step 11 Click **Next** to go to **8 Select networks**, as shown in the following figure. In the drop-down table at the top of the page, choose the appropriate destination network for each source network based on the number of vNICs you plan to use.

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



Step 12 Click **Next** to go to **9 Customize template**, with the **Host Information Settings** already expanded.

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

Enter the information for the parameters as described in Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2.

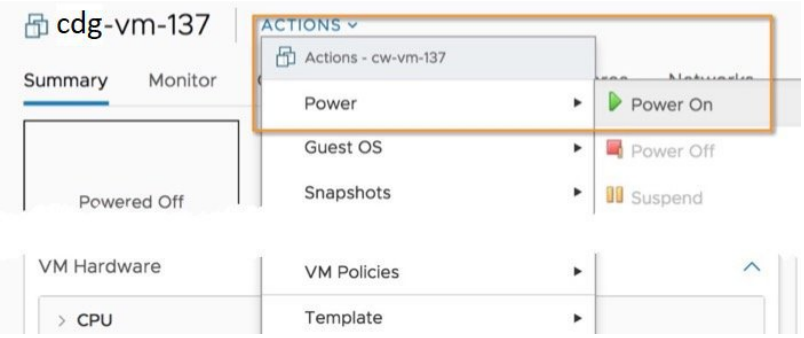
Step 13 Click **Next** to go to **10 Ready to complete**. Review your settings and then click **Finish** if you are ready to begin deployment.

Step 14 Check deployment status.

a) Open the vCenter vSphere client.

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

Step 15 After the deployment status becomes 100%, power on the VM to complete the deployment process. Expand the host's entry so you can click the VM and then choose **Actions** > **Power** > **Power On**, as shown in the following figure:



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

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

What to do next

Login to Crosswork Data Gateway VM Via vCenter:

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

Access Cisco Crosswork Data Gateway VM Via SSH:

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

   ssh <username>@<ManagementNetworkIP>

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

   For example,

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

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

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

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

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

Install Crosswork Data Gateway Via OVF Tool

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

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

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

# robot.ova path

DG_OVA_PATH="<mention the orchestrator path>"

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

ActiveVnics="2"

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

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


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

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

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

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

SyslogAddress="<syslog_server_address>"
SyslogPort=<syslog_server_port>
SyslogProtocol="<syslog_server_protocol>"
SyslogTLS=False
SyslogPeerName="<syslog_server_peer_name>"
SyslogCertChain="<syslog_server_root_certificate>"
SyslogCertChainPwd="<password>"

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

```
DS="<DS details>"

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

Step 1 Open a command prompt.

Step 2 Open the template file and edit it to match the settings you chose for the Cisco Crosswork Data Gateway.

Step 3 Navigate to the location where you installed the OVF Tool.

Step 4 Run the OVF Tool in one of the following ways:

a) **Using the command**

Execute the following command.

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

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

For example,

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

b) **Using the script**

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

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

What to do next

Login to Crosswork Data Gateway VM Via vCenter:

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

Access Cisco Crosswork Data Gateway VM Via SSH:

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

   ssh <username>@<ManagementNetworkIP>

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

   For example,

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

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

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

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

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

Install Crosswork Data Gateway on Cisco CSP

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

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

a) Refer to the *Crosswork Data Gateway 3.0.x Release notes* and download the recommended image file.

b) Extract the Crosswork Data Gateway `qcow2` build from CCO to your local machine or a location on your local network that is accessible to your Cisco CSP.

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

c) Open the `config.txt` file and modify the parameters as per your installation requirements. Refer to the section Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 2.

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

Following parameters have pre-defined values:

- Deployment
  - Use "cloud".

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

```
ActiveVnics=
AuditdAddress=
AuditdPort=
Deployment=cloud
Description=
DGAppdataDisk=
DGCertChain=
DGCertChainPwd=
DGCertKey=
DNS=changeme
DNSSEC=False
DNSTLS=False
Domain=changeme
EnrollmentPassphrase=
EnrollmentURI=
Hostname=changeme
Label=
LLMNR=False
mDNS-False
NTP=changeme
NTPAuth=False
NTPKey=
NTPKeyFile=
NTPKeyFilePwd=
Profile=Standard
ProxyBypass=
ProxyCertChain=
ProxyCertChainPwd=
ProxyPassphrase=
ProxyURL=
ProxyUsername=
SyslogAddress=
SyslogCertChain=
SyslogCertChainPwd=
SyslogPeerName=
SyslogPort=514
SyslogProtocol=UDP
SyslogTLS=False
UseRemoteAuditd=False
UseRemoteSyslog=False
Vnic0IPv4Address=0.0.0.0
Vnic0IPv4Gateway=0.0.0.1
Vnic0IPv4Method=None
Vnic0IPv4Netmask=0.0.0.0
Vnic0IPv6Address=::0
Vnic0IPv6Gateway=::1
Vnic0IPv6Method=None
Vnic0IPv6Netmask=64
Vnic1IPv4Address=0.0.0.0
```

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

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

a) Log in to the Cisco CSP.

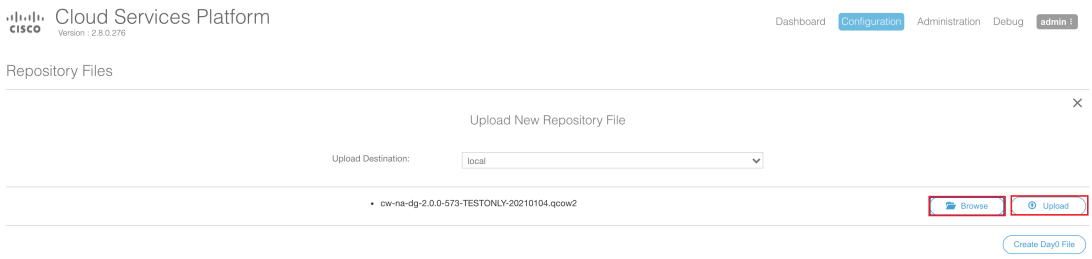
b) Go to **Configuration** > **Repository**.

c) On the **Repository Files** page, Click Crosswork Data Gateway 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 files are uploaded, file name and other relevant information is displayed in the **Repository Files** table.

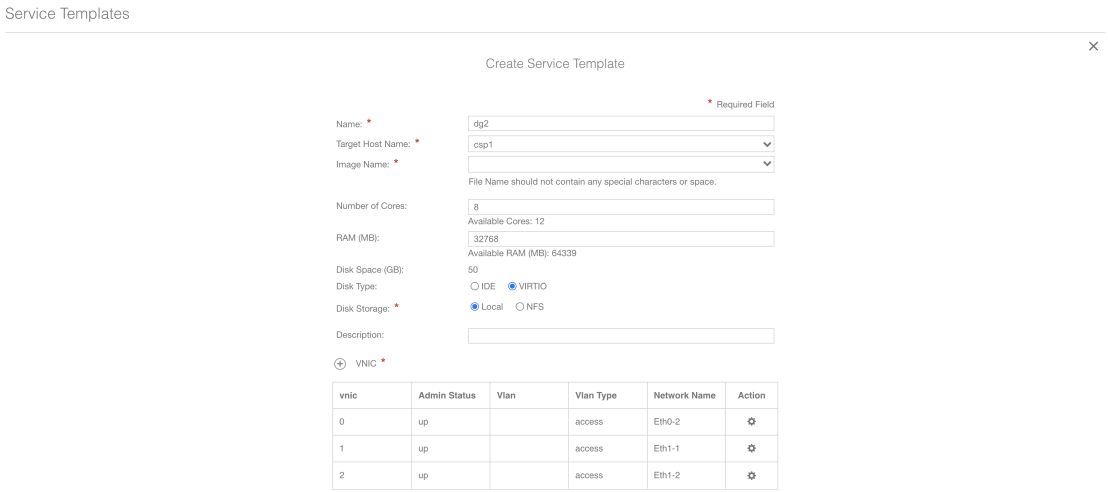
Step 3 **Create Crosswork Data Gateway Service:**

a) Go to **Configuration** > **Services**.

b) On the **Service** page, click ⊞ button.

c) Check **Create Service** option.

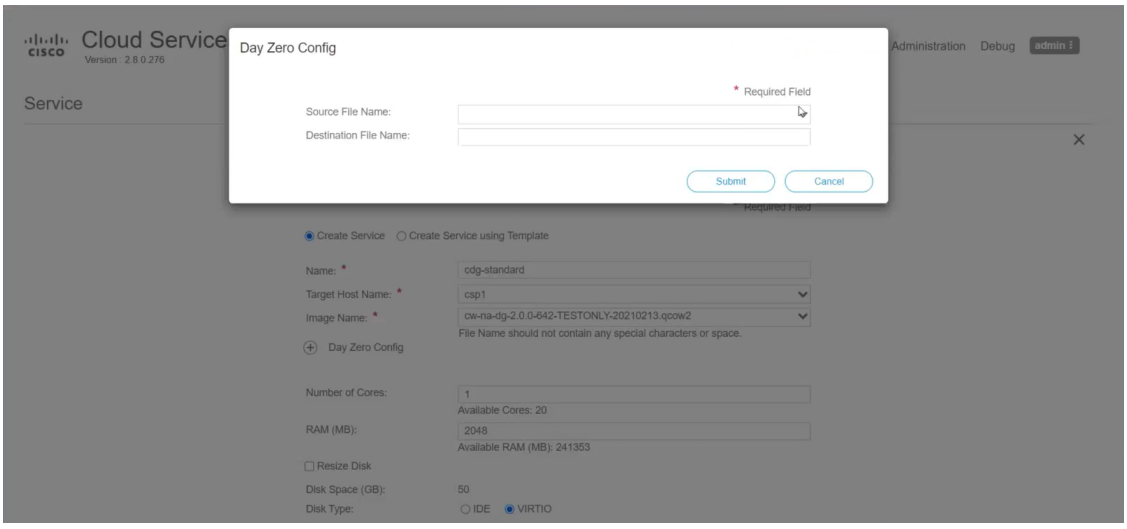
The **Create Service Template** page is displayed.



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**.



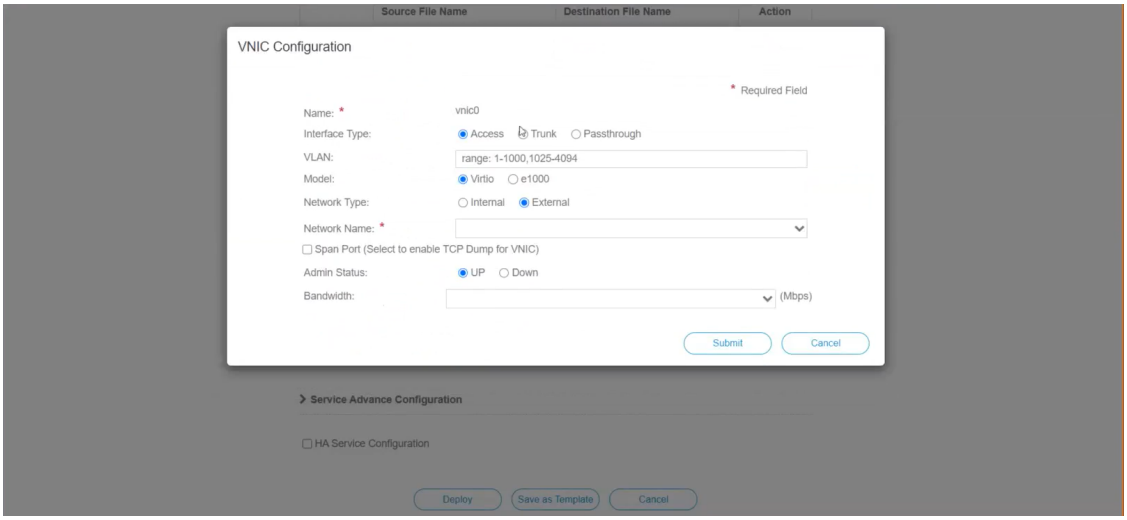
In the **Day Zero Config** dialog box, do the following:

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

f) Enter the values for the following fields:

Field	Description
Number of Cores	8
RAM (MB)	32768

g) Click **VNIC**.



In the **VNIC Configuration** dialog box:

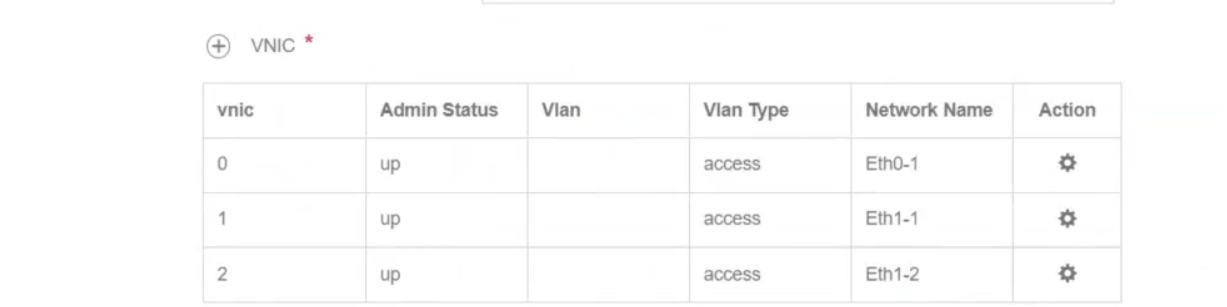
Note The VNIC Name is set by default.

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

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

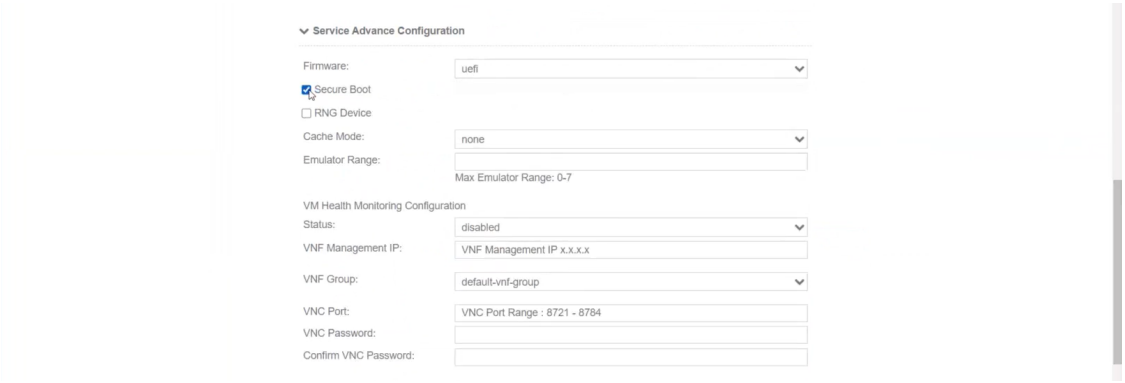
5. Select **Admin Status** as **UP**.
6. Click **Submit**.
7. Repeat Step **g** for VNIC1 and VNIC2 if you plan to have more than one VNIC in your network.

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



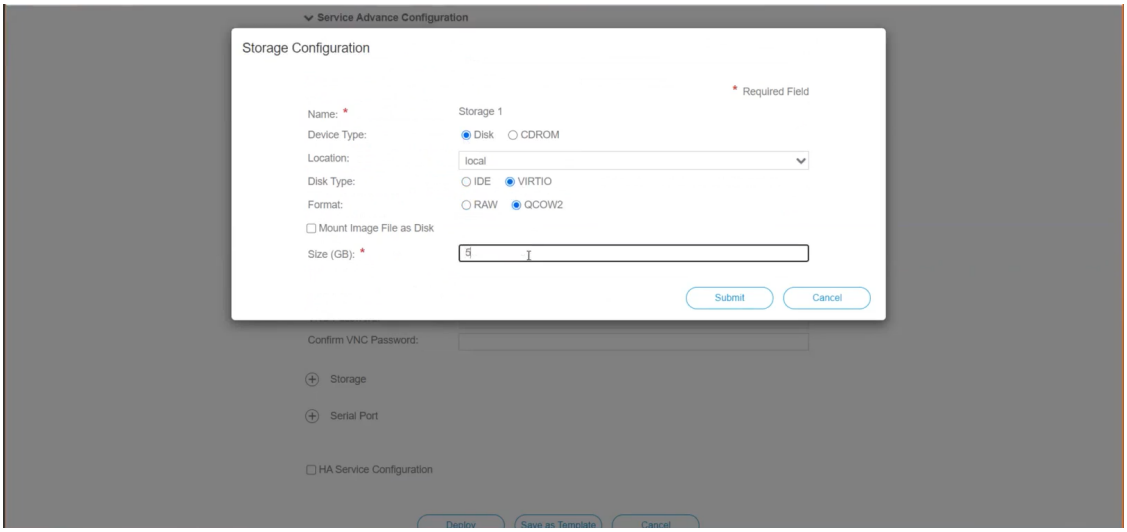
h) Expand the **Service Advance Configuration** and for **Firmware**, select **uefi** from the drop-down.

Check the **Secure Boot** checkbox.



i) Click **Storage**.

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

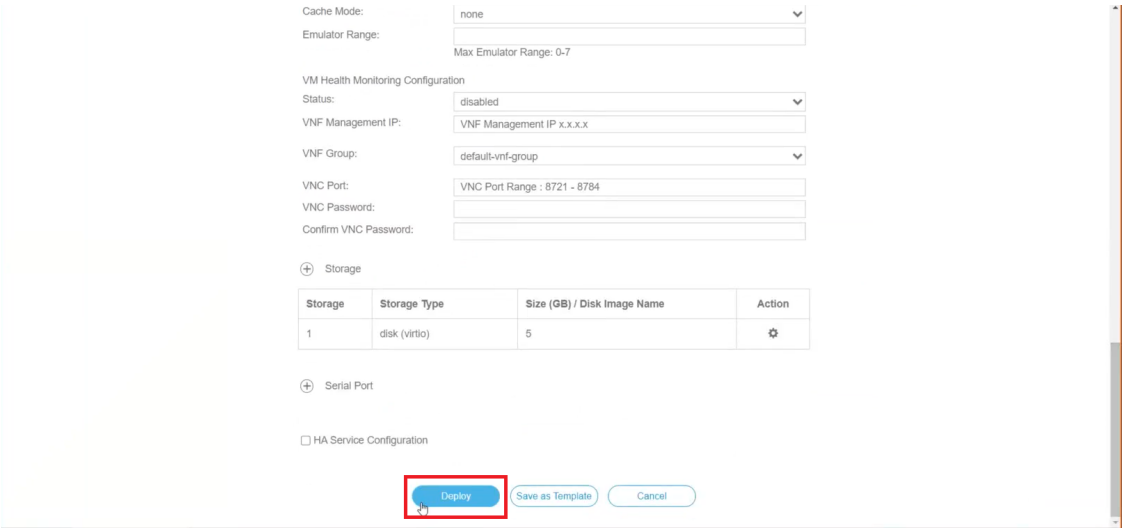


Field	Description
Name	Name of the storage. This is specified by default.

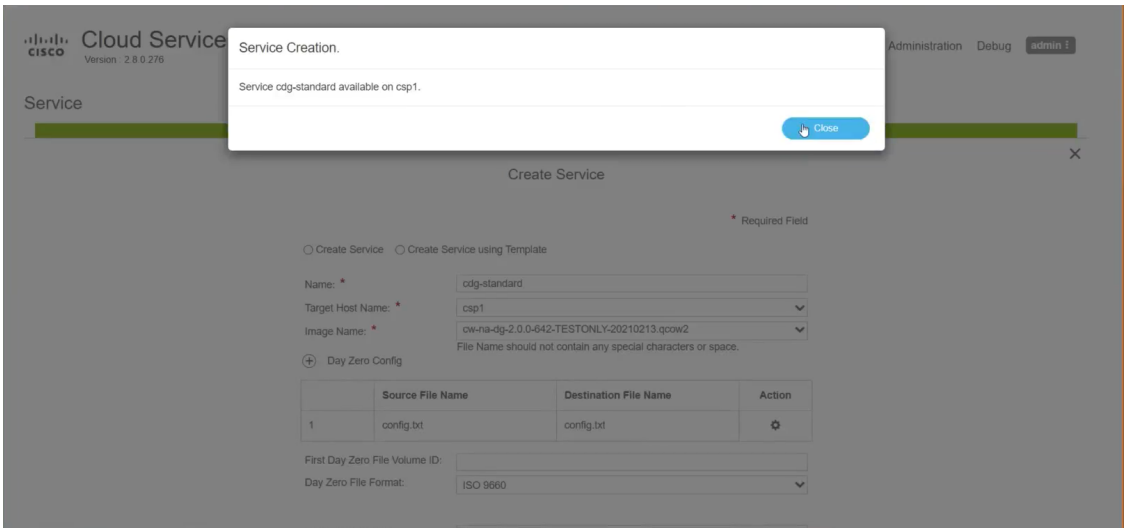
Field	Description
Device Type	Select **Disk**.
Location	Select **local**.
Disk Type	Select **VIRTIO**.
Format	Select **QCOW2**.
Mount image file as disk?	Leave this unchecked.
Size (GB)	Enter the disk size as 70GB.

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

j) Click **Deploy**.



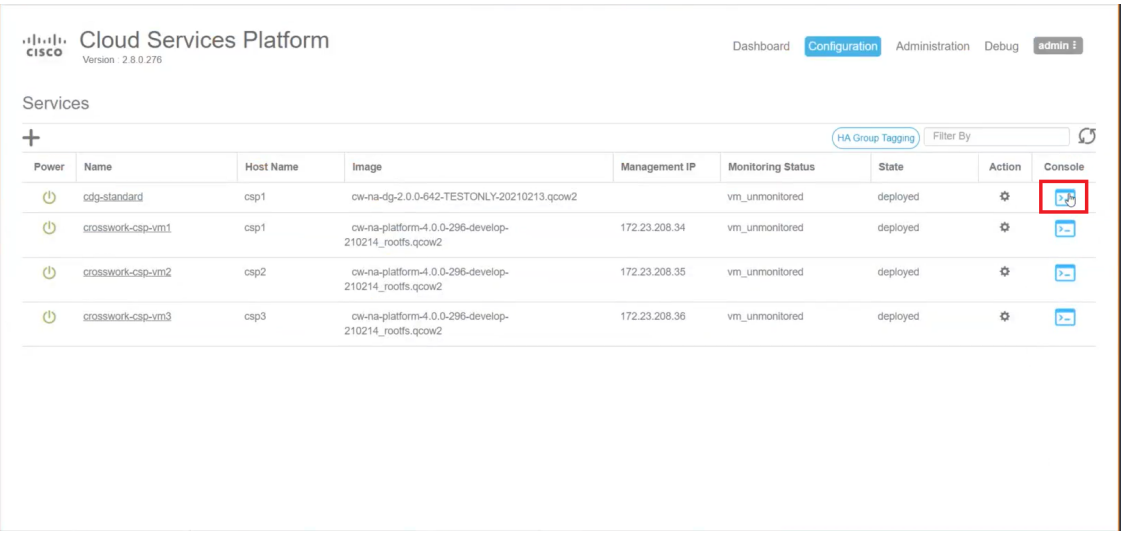
You will see a similar message once the service has successfully deployed. Click **Close**.



Step 4 **Deploy Crosswork Data Gateway service:**

a) Go to **Configuration** > **Services**.

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



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

d) Once the Crosswork Data Gateway service connects, login as the dg-admin or dg-oper user (as per the role assigned to you) and the corresponding password you had entered in the config.txt file.

The Crosswork Data Gateway console is available.

Generate Enrollment Package

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

- By supplying **Auto Enrollment Package** parameters during installation process (see Auto Enrollment Package under Table 1: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios.).
- By using the **Export Enrollment Package** option from the Interactive Console (see Export Enrollment Package, on page 27)

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

If you opted not to export the enrollment package during install, then you must export it before you can enroll the Crosswork Data Gateway with Crosswork Cloud. The steps to do so are described in Export Enrollment Package, on page 27.

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

A sample enrollment package JSON is shown below:

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

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

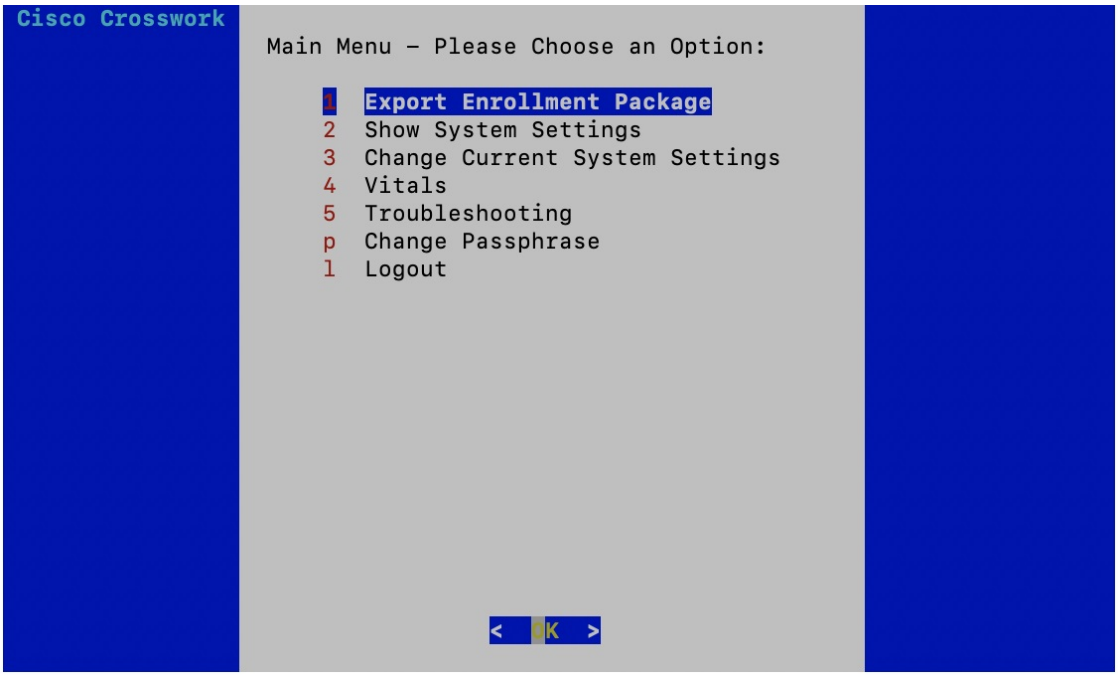

Export Enrollment Package

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

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

Step 1 Log in to the Cisco Crosswork Data Gateway.

Step 2 From the Main Menu, select **1 Export Enrollment Package** and click **OK**.



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

Note

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

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

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

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

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

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

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

- Configure Control Proxy
- Verify the Crosswork Data Gateway Connectivity