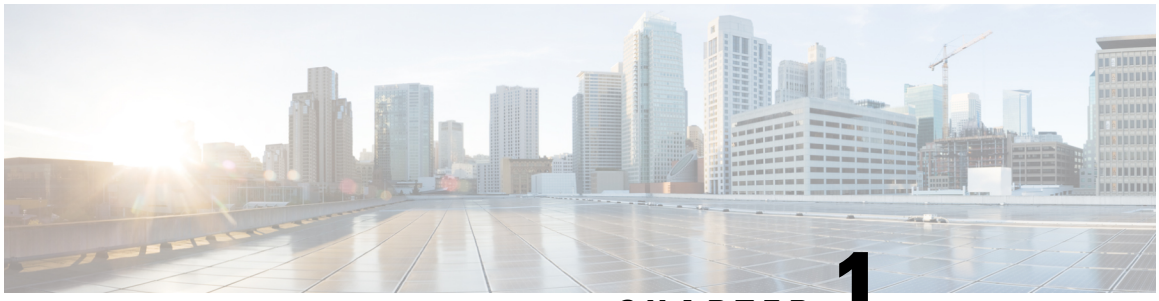
Cisco Crosswork Infrastructure 4.0 and Applications Installation Guide

First Published: 2021-04-19

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Overview

This section contains the following topics:

Audience

This guide is for experienced network users and operators who want to use Cisco Crosswork infrastructure and applications in their network. This guide assumes that you are familiar with the following:

- Deploying OVF templates using VMware vCenter
- Deploying using OVF tool
- Using a Docker container
- Deploying a virtual machine on Cisco Cloud Services Platform (CSP)

Introduction

Cisco Crosswork Infrastructure is a microservices-based platform that brings together streaming telemetry and model-driven application programming interfaces (APIs) to redefine service provider network operations. It retrieves real-time information from the network, analyzes the data, and provides both template-driven and automated tools to apply changes to the network. It employs a cluster architecture to be extensible, scalable, and highly available.

Note Henceforth, Cisco Crosswork Infrastructure is referred to as "Cisco Crosswork" in the guide.

Cisco Crosswork uses Cisco Crosswork Data Gateway, a software package that is separated out into its own Virtual Machine (VM), to gather information from the managed devices and forwards it to the Crosswork applications for analysis and processing. You can then use Crosswork applications to manage the network or respond to changes in the network. Crosswork Data Gateway can also be configured to collect data from network devices and forward that data to non-Crosswork users and applications. The number of Crosswork

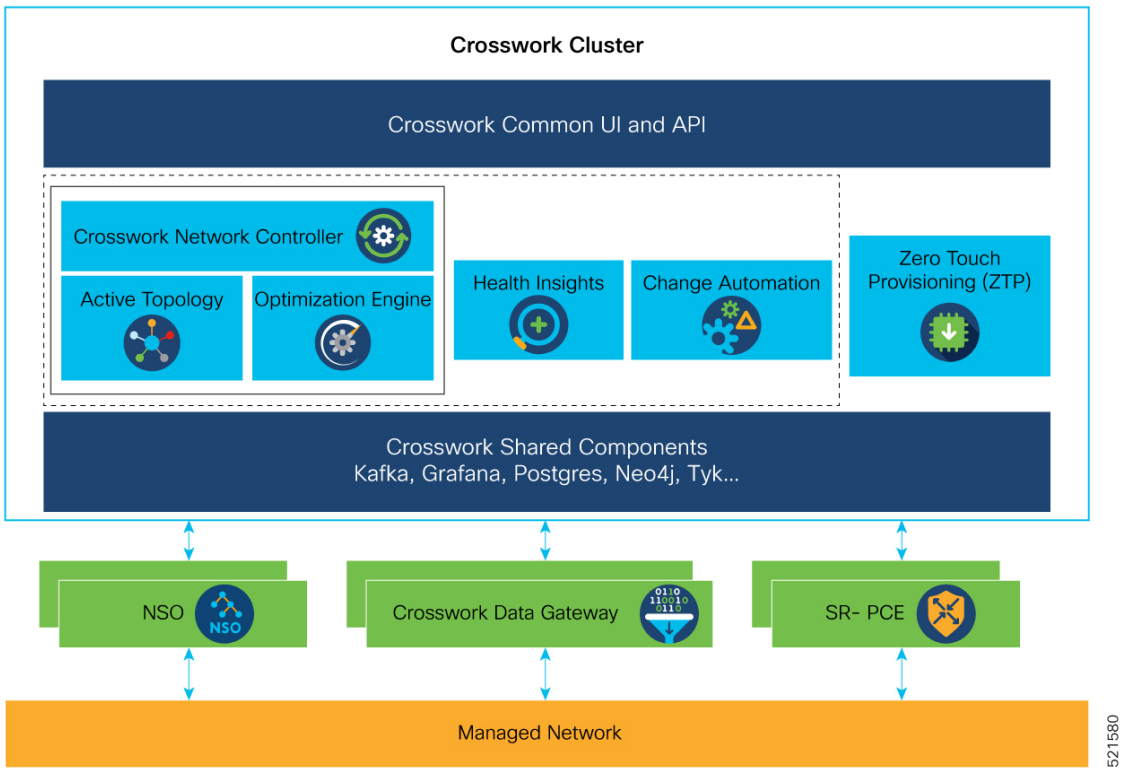
Data Gateways deployed in your network depends on the number of devices, the amount of data being collected, and the overall topology. Work with Cisco Customer Experience team to scale your deployment to best meet your needs.

This guide explains the requirements and installation process to set up the Cisco Crosswork along with the CDG(s). It also explains the requirements of other components that integrate with Cisco Crosswork such as Cisco NSO and the managed devices that make up your network. Details for installation of compatible software on other devices or applications are provided in documentation specific to those devices or applications.

Cisco Network Services Orchestrator (Cisco NSO) functions as the default provider for Crosswork to configure the devices according to their expected functions, including configuring model-driven telemetry (MDT) sensor paths, if any, for data collection. Cisco NSO is vital in supplying device management and configuration-maintenance services.

Cisco WAN Automation Engine (Cisco WAE) providers supply traffic and topology analysis to Cisco Crosswork. The foundation software is Cisco WAE Planning, which provides a cross-sectional view of traffic, topology, and equipment state.

Figure 1: Cisco Crosswork Cluster Architecture



Starting with the 4.0 release, the Cisco Crosswork Platform has adopted a cluster architecture, where the platform services are arranged in a unified cluster. In order to improve resource utilization and provide more resiliency, the design consists of a single cluster instance for all the infrastructure services, such as Kafka, NATS, alerting, topology etc. The Crosswork cluster for 4.0 release consists of at least 3 VMs operating in a hybrid configuration. Additional worker nodes can be added, as needed, to match the requirements of your network. A hybrid node can run infrastructure and application pods, while a worker node can only run the application pods.

Cisco Crosswork Portfolio

Cisco Crosswork supports the following applications:

- Cisco Crosswork Change Automation and Health Insights: Cisco Crosswork Change Automation and Health Insights enables service providers to quickly deploy intent-driven, closed-loop operations. It provides a ready-to-use solution to automate change-impact and remediation, monitor KPIs, notify user of any anomalies, and prepare network changes triggered by KPI changes.
- Cisco Crosswork Optimization Engine: Cisco Crosswork Optimization Engine provides real-time network optimization allowing operators to effectively maximize network capacity utilization, as well as increase service velocity. Leveraging real-time protocols, such as BGP-LS and Path Computation Element Communication Protocol (PCEP), SR-PCE and Cisco Crosswork Optimization Engine enable closed-loop tracking of the network state, reacting quickly to changes in network conditions to support a self-healing network.
- Cisco Crosswork Zero Touch Provisioning: The Cisco Crosswork Zero Touch Provisioning (ZTP) application allows users to quickly and easily bring up devices using a Cisco-certified software image and a day-zero software configuration of the customer's choice. Once provisioned in this way, the new device is onboarded to the Crosswork device inventory (and, if it is configured to Cisco NSO), where it can be monitored and managed like other devices.

Cisco Crosswork supports Cisco Crosswork Network Controller, an integrated solution combining essential components such as Cisco Network Services Orchestrator, Segment Routing Path Computation Element (SR-PCE), Cisco Crosswork Active Topology, and Cisco Crosswork Optimization Engine. The solution enables you to proactively manage your end-to-end networks and provides intent-based and closed-loop automation solutions to ensure faster innovation, good user experience, and operational excellence. Cisco Crosswork Network Controller can also optionally integrate with Cisco Crosswork Change Automation and Health Insights and Cisco Crosswork Zero Touch Provisioning.

- Cisco Crosswork Active Topology (part of Cisco Crosswork Network Controller) enables visualization of topology and services on logical and geographical maps.

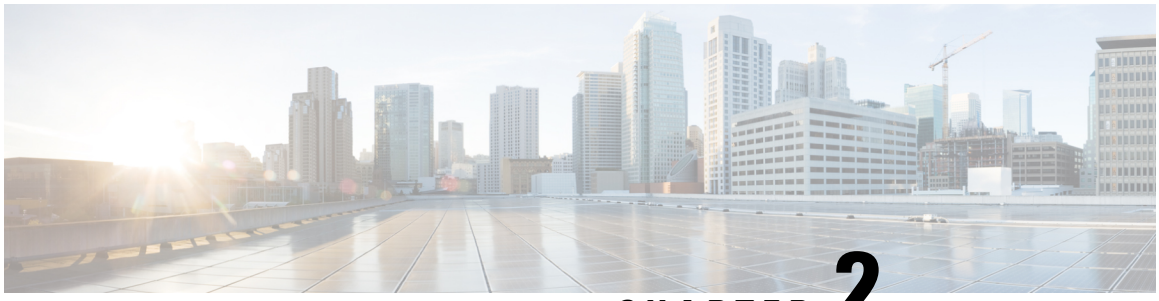
Table 1: Supported Crosswork product versions

Product	Version
Crosswork Data Gateway (CDG)	2.0
Crosswork Network Change Automation (NCA)	4.0
Crosswork Health Insights (HI)	4.0
Crosswork Optimization Engine (COE)	2.0
Crosswork Zero Touch Provisioning (ZTP)	2.0
Crosswork Network Controller (CNC)	2.0

Table 2: Supported Cisco NSO and NED versions

Software/Driver	Version
Cisco Network Services Orchestrator (Cisco NSO)	• 5.4.2
Cisco Network Element Driver (NED)	Cisco IOS XR: • CLI: 7.33, 7.33.1 • NETCONF: 6.6, 6.6.3, 7.3, 7.3.1 Cisco IOS: • CLI: 6.67, 6.67.8

For more information, see Cisco NSO and NED Requirements, on page 16 and Crosswork Portfolio Dependency matrix, on page 17.



CHAPTER 2

Installation Requirements

This section contains the following topics:

Cisco Crosswork Infrastructure Requirements

This section explains the requirements for installing the Cisco Crosswork.

The Crosswork cluster for 4.0 release consists of at least 3 VMs operating in a hybrid configuration. This is the minimum configuration necessary to support the applications in a typical network. Additional worker nodes can be added later to scale your deployment, as needed, to match the requirements of your network or as other applications are introduced.

In addition, at least 1 VM is needed to deploy Crosswork Data Gateway. This configuration can be scaled by adding additional resources if it is determined that your use case requires more resources and to support Crosswork Data Gateway high availability (HA).

The data center resources need to run NSO are addressed in the NSO installation Guide and are not addressed in this document.

Data Center Requirements

Cisco Crosswork can be deployed in either a vCenter managed data center or onto Cisco CSP. To aid in the deployment, Cisco has developed a cluster installation tool. This tool works in both environments. However, there are limitations to the tool which are detailed later in this section.

Note The machine where you run the installer must have network connectivity to the Cisco Crosswork cluster in order to complete the installation. If this mandatory requirement cannot be met, you must manually install the cluster. For more information on manual installation, see Install Cisco Crosswork Manually, on page 34.

- VMware Data Center Requirements, on page 6
- CSP Data Center Requirements, on page 7

VMware Data Center Requirements

This section explains the data center requirements to install Cisco Crosswork on VMware vCenter.

Note The following requirements are mandatory if you are planning to install Cisco Crosswork using the cluster installer. If your vCenter data center does not meet these requirements, then the VMs have to be deployed individually, and connectivity has to be established manually between the VMs.

- VMware vSphere 6.5 or above.
- vCenter Server 6.5 (Update 2d or later) and ESXi 6.5 Update 2 installed on hosts, OR vCenter Server 6.7 (Update 3g or later) and ESXi 6.7 Update 1 installed on hosts.
- All the physical host machines must be organized within the same VMware Data Center, and while it is possible to deploy all the cluster nodes on a single physical host (provided it meets the requirements), it is recommended that the nodes be distributed across multiple physical hosts.
- The networks required for the Crosswork Management and Data networks need to be built and configured within the data center, and must allow L2 communication. A single pair of network names is required for these networks to be used across all the physical host machines hosting the Crosswork VMs.
- To allow use of VRRP, DVS Port group needs to be set to allow Forged Transmits setting as follows:

Property	Value
Promiscuous mode	Reject
MAC address changes	Reject
Forged transmits	Accept

- Ensure the user account you use for accessing vCenter have the following privileges:
  - VM (Provisioning): Clone VM on the VM you are cloning.
  - VM (Provisioning): Customize on the VM or VM folder if you are customizing the guest operating system.
  - VM (Provisioning): Read customization specifications on the root vCenter server if you are customizing the guest operating system.
  - VM (Inventory): Create from the existing VM on the data center or VM folder.

- VM (Configuration): Add new disk on the data center or VM folder.
- Resource: Assign VM to resource pool on the destination host, cluster, or resource pool.
- Datastore: Allocate space on the destination datastore or datastore folder.
- Network: Assign network to which the VM will be assigned.
- Profile-driven storage (Query): This permission setting needs to be allowed at the root of the DC tree level.

- We also recommend you to enable vCenter storage control.

CSP Data Center Requirements

This section explains the data center requirements to install Cisco Crosswork on Cisco Cloud Services Platform (CSP).

- Cisco CSP, Release 2.8.0.276
- Allowed hardware list:

UCSC-C220-M4S, UCSC-C240-M4SX
N1K-1110-X, N1K-1110-S
CSP-2100, CSP-2100-UCSD, CSP-2100-X1, CSP-2100-X2
CSP-5200, CSP-5216, CSP-5228
CSP-5400, CSP-5436, CSP-5444, CSP-5456

- CSP host or cluster is setup and installed with a minimum of 2 physical ethernet interfaces - one ethernet connected to the Management network, and the other to the Data network.

VM Host Requirements

This section explains the VM host requirements.

Table 3: VM Host Requirements

Requirement	Description
CPU/Memory/Storage Profiles (per VM)	The data center host platform has to accommodate 3 VMs of the following minimum configuration (applicable to VMware vCenter and Cisco CSP): VMware vCenter: • Small (for lab deployments only): 8 vCPUs | 48 GB RAM Memory| 1 TB disk space | (Optional) 2 GB RAM disk • Large: 12 vCPUs | 96 GB RAM Memory | 1 TB disk space Cisco CSP: • Small (for lab deployments only): 8 CPU cores | 48 GB RAM Memory| 1 TB disk space | (Optional) 2 GB RAM disk • Large: 12 CPU cores | 96 GB RAM Memory | 1 TB disk space **Note** For assistance in adjusting VM Memory and CPU sizes post installation, contact your Cisco Customer Experience team. Few things to note: • Storage requirements vary based on factors such as the number of devices being supported and the type of deployment selected. However, 1 TB disk space should work for most deployments. • Due to their performance, solid state drives (SSD) are preferred over traditional hard disk drives (HDD). • If you are using HDD, the minimum speed should be over 10,000 RPM. • The VM data store(s) need to have disk access latency of < 10 ms.
Additional Storage	10 GB (approximately) of storage is required for the Crosswork OVA (in vCenter), OR the Crosswork QCOW2 image on each CSP node (in CSP).
Network Connections	For production deployments, we recommend that you use dual interfaces, one for the Management network and one for the Data network. For optimal performance, the Management and Data networks should use links configured at a minimum of 10 Gbps.

Requirement	Description
IP Addresses	2 IP subnets, one for the Management network and one for Data network, with each allowing a minimum of 4 assignable IP addresses (IPv4 or IPv6). A Virtual IP (VIP) address is used to access the cluster, and then 3 IP addresses for each VM in the cluster. If your deployment requires worker nodes, you will need a Management and Data IP address for each worker node. • The IP addresses must be able to reach the gateway address for the network where Cisco Crosswork Data Gateway will be installed, or the installation will fail. • When deploying a IPv6 cluster, the installer needs to run on an IPv6 enabled container/VM. • At this time, your IP allocation is permanent and cannot be changed without re-deployment. For more information, contact your Cisco Customer Experience team.
NTP Servers	The IPv4 or IPv6 addresses or host names of the NTP servers you plan to use. If you want to enter multiple NTP servers, separate them with spaces. These should be the same NTP servers you use to synchronize the Crosswork application VM clock, devices, clients, and servers across your network. • Ensure that the NTP servers are reachable on the network before attempting installation. The installation will fail if the servers cannot be reached. • The ESXi hosts that will run the Crosswork application and Crosswork Data Gateway VM must have NTP configured, or the initial handshake may fail with "certificate not valid" errors.
DNS Servers	The IPv4 or IPv6 addresses of the DNS servers you plan to use. These should be the same DNS servers you use to resolve host names across your network. • Ensure that the DNS servers are reachable on the network before attempting installation. The installation will fail if the servers cannot be reached.
DNS Search Domain	The search domain you want to use with the DNS servers, for example, cisco.com. You can have only one search domain.

Important Notes

- Kubernetes runs within the Crosswork application VM and uses Docker for containerization. The number of containers varies as applications are added or deleted.
- Dual stack configuration is not supported in Crosswork Platform Infrastructure. Therefore, all addresses for the environment must be either IPv4 or IPv6.

Port Requirements

As a general policy, ports that are not needed should be disabled. To view a list of all the open listening ports, log in as a Linux CLI admin user on any Crosswork cluster VM, and run the netstat -aln command.

The following ports are needed by Cisco Crosswork to operate correctly.

Table 4: External Ports

Port	Protocol	Usage
22	TCP	Remote SSH traffic
111	TCP/UDP	GlusterFS (port mapper)
179	TCP	Calico BGP (Kubernetes)
500	UDP	IPSec
2379/2380	TCP	Kubernetes etcd
4500	UDP	IPSec
6443	TCP	kube-apiserver (Kubernetes)
9100	TCP	Kubernetes metamonitoring
10250	TCP	kubelet (Kubernetes)
24007	TCP	GlusterFS
30603	TCP	User interface (NGINX server listens for secure connections on port 443)
30604	TCP	Used for Classic Zero Touch Provisioning (Classic ZTP) on the NGINX server.
30606	TCP	Docker Registry
30607	TCP	Crosswork Data Gateway vitals collection
30608	TCP	Data Gateway gRPC channel with Data Gateway VMs
30617	TCP	Used for Secure Zero Touch Provisioning (Secure ZTP) on the ZTP server.
30649	TCP	To set up and monitor Crosswork Data Gateway collection status.
30650	TCP	astack gRPC channel with astack-client running on Data Gateway VMs
30993, 30994, 30995	TCP	Crosswork Data Gateway sending the collected data to Crosswork Kafka destination.
49152:49170	TCP	GlusterFS

Table 5: Destination Ports

Port	Protocol	Usage
7	TCP/UDP	Discover endpoints using ICMP
22	TCP	Initiate SSH connections with managed devices
53	TCP/UDP	Connect to DNS
123	UDP	Network Time Protocol (NTP)
830	TCP	Initiate NETCONF
2022	TCP	Used for communication between Crosswork and Cisco NSO (for NETCONF).
8080	TCP	REST API to SR-PCE
8888	TCP	Used for communication between Crosswork and Cisco NSO (for HTTPS).
20243	TCP	Used by the DLM Function Pack for communication between DLM and Cisco NSO
20244	TCP	Used to internally manage the DLM Function Pack listener during a Reload Packages scenario on Cisco NSO

Supported Web Browsers

Cisco Crosswork supports the following web browsers:

The recommended display resolution: 1600 x 900 pixels or higher (minimum: 1366 x 768).

Table 6: Supported Web Browsers

Browser	Version
Google Chrome (recommended)	75 or later
Mozilla Firefox	70 or later

In addition to using a supported browser, all client desktops accessing geographical map information in the Crosswork applications must be able to reach the mapbox.com map data URL directly, using the standard HTTPS port 443. Similar guidance may apply if you choose a different map data provider, as explained in "Configure Geographical Map Settings" in the Crosswork application user guides.

Cisco Crosswork Data Gateway Requirements

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

- Crosswork Data Gateway VM Requirements
- Crosswork Data Gateway Ports Requirements

Cisco Crosswork Data Gateway VM Requirements

Cisco Crosswork Data Gateway provides two On-Premise deployment options:

1. Standard: Choose this option to install Crosswork Data Gatewayfor use with all Crosswork applications, except Cisco Crosswork Health Insights.
2. Extended: Choose this option to install Cisco Crosswork Data Gateway for use with Cisco Crosswork Health Insights.

Note The VM resoure requirements for Crosswork Data Gateway differ between Standard and Extended deployments. As a result, Crosswork Data Gateway must be re-installed when moving from standard to extended configuration.

Requirements for both types of deployments are listed below.

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

Table 7: Cisco Crosswork Data Gateway VM Requirements

Requirement	Description
Data Center	VMware • VMware vCenter Server 6.7 (Update 3g or later), ESXi 6.7 Update 1 installed on hosts • VMware vCenter Server 6.5 (Update 2d or later), ESXi 6.5 Update 2 installed on hosts Cisco CSP • Cisco CSP 2.8.0.276 or later Allowed_hardware_list = ['UCSC-C220-M4S', 'UCSC-C240-M4SX', 'N1K-1110-X', 'N1K-1110-S','CSP-2100', 'CSP-2100-UCSD', 'CSP-2100-X1', 'CSP-2100-X2','CSP-5200', 'CSP-5216', 'CSP-5228','CSP-5400', 'CSP-5436', 'CSP-5444', 'CSP-5456'] **Note** CSP host or cluster is setup and installed with a minimum of 2 physical ethernet interfaces. If you plan to install Crosswork Data Gateway on Cisco CSP, plan also for a third ethernet interface.
Memory	• Standard: 32 GB • Extended: 96 GB
Disk space	• Standard: 55 GB (Minimum) • Extended: 550 GB (Minimum)
vCPU	• Standard: 8 • Extended: 16

<table>
<tr><th>Requirement</th><th>Description</th></tr>
<tr><td>Interfaces</td><td>
Minimum: 1
Maximum: 3
Cisco Crosswork Data Gateway can be deployed with either 1, 2, or 3 interfaces as per the combinations below:
Note If you use one interface on your Crosswork cluster, you must use only one interface on the Crosswork Data Gateway. If you use two interfaces on your Crosswork Cluster, then you can use two or three interfaces on the Crosswork Data Gateway as per your network requirements.
<table>
<tr><th>No. of NICs</th><th>vNIC0</th><th>vNIC1</th><th>vNIC2</th></tr>
<tr><td>1</td><td>• Management Traffic
• Control/Data Traffic
• Device Access Traffic</td><td>—</td><td>—</td></tr>
<tr><td>2</td><td>• Management Traffic</td><td>• Control/Data Traffic
• Device Access Traffic</td><td>—</td></tr>
<tr><td>3</td><td>• Management Traffic</td><td>• Control/Data Traffic</td><td>• Device Access Traffic</td></tr>
</table>
• Management traffic: for accessing the UIs and command line and passing Control/Data information between servers (for example, a Crosswork application to Crosswork Data Gateway or NSO).
• Control/Data traffic: for data and configuration transfer between Cisco Crosswork Data Gateway and Crosswork applications and other external data destinations.
• Device access traffic: for device management (NSO or a Crosswork application to the devices as a result of KPI configuration or playbook execution) and telemetry data being forwarded to the Cisco Crosswork Data Gateway.
</td></tr>
<tr><td>IP Addresses</td><td>
1, 2, or 3 IPv4/IPv6 addresses based on the number of interfaces you choose to use.
Note Crosswork does not support dual stack configurations. Therefore, ALL addresses for the environment must be either IPv4 or IPv6.
During installation, you will need to provide IP address for Management Traffic and Control/Data Traffic only. IP address for Device Access Traffic is assigned during Crosswork Data Gateway pool creation as explained in Section: Create a Cisco Crosswork Data Gateway Pool, on page 85.
</td></tr>
</table>

Requirement	Description
NTP Servers	The IPv4/IPv6 addresses or host names of the NTP servers you plan to use. If you want to enter multiple NTP servers, separate them with spaces. These should be the same NTP servers you use to synchronize devices, clients, and servers across your network. Confirm that the NTP IP address or host name is reachable on the network or installation will fail. Also, the ESXi hosts that will run the Crosswork application and Cisco Crosswork Data Gateway VM must have NTP configured, or the initial handshake may fail with "certificate not valid" errors.
DNS Servers	The IPv4 or IPv6 addresses of the DNS servers you plan to use. These should be the same DNS servers you use to resolve host names across your network. Confirm that the DNS servers are reachable on the network before attempting installation. The installation will fail if the servers cannot be reached.
DNS Search Domain	The search domain you want to use with the DNS servers, for example, cisco.com. You can have only one search domain.

Crosswork Data Gateway Ports Requirements

The following tables show the minimum set of ports required for Crosswork Data Gateway to operate correctly.

Note SCP port can be tuned.

Table 8: Ports to be Opened for Management Traffic

Port	Protocol	Used for...	Direction
22	TCP	SSH server	Inbound
22	TCP	SCP client	Outbound
123	UDP	NTP Client	Outbound
53	UDP	DNS Client	Outbound
30607	TCP	Crosswork Controller	Outbound

Table 9: Ports to be Opened for Device Access Traffic

Port	Protocol	Used for...	Direction
161	UDP	SNMP Collector	Outbound
1062	UDP	SNMP Trap Collector	Inbound
9010	TCP	MDT Collector	Outbound
22	TCP	CLI Collector	Outbound

Port	Protocol	Used for...	Direction
6514	TLS	Syslog Collector	Inbound
9898	TCP		
9514	UDP		
Site Specific Default ports differ from XR, XE to vendor. Check platform-specific documentation.	TCP	gNMI Collector	Outbound

Table 10: Ports to be Opened for Control/Data Traffic

Port	Protocol	Used for...	Direction
30649	TCP	Crosswork Controller	Outbound
30993	TCP	Crosswork Kafka	Outbound
Site Specific	Site Specific	Kafka and gRPC Destination	Outbound

Cisco NSO and NED Requirements

The requirements in the following table are applicable if you plan to use Cisco Network Services Orchestrator.

Table 11: Cisco NSO and NED requirements

Software/Driver	Version/Notes
Cisco Network Services Orchestrator (Cisco NSO)	5.4.2 or 5.4.4.1
Cisco Network Element Driver (NED)	Cisco IOS XR: • CLI: 7.33, 7.33.1 • NETCONF: 6.6, 6.6.3, 7.3, 7.3.1 Cisco IOS: • CLI: 6.67, 6.67.8

The following table explains the Function Packs (FP) required for the Cisco Crosswork products:

Table 12: List of required Function Packs

Crosswork Product	Required Function Pack
Cisco Crosswork Network Controller	• Cisco NSO Transport-SDN Function Pack Bundle Installation Guide 2.0 • Cisco NSO Transport-SDN Function Pack Bundle User Guide 2.0 • Cisco NSO DLM Service Pack 1.0 Installation Guide • Cisco Crosswork Telemetry Traffic Collector Function Pack 2.0 Installation Guide
Cisco Crosswork Change Automation and Health Insights	• Cisco Crosswork Telemetry Traffic Collector Function Pack 2.0 Installation Guide • Cisco NSO DLM Service Pack 1.0 Installation Guide • Cisco Crosswork Change Automation Function Pack 1.0 Installation Guide
Cisco Crosswork Optimization Engine	• Cisco Crosswork Telemetry Traffic Collector Function Pack 2.0 Installation Guide • Cisco NSO DLM Service Pack 1.0 Installation Guide

Crosswork Portfolio Dependency matrix

The table below explains the dependencies for each Crosswork product.

Table 13: Dependency matrix

Cisco Crosswork Product	SR-PCE setup	NSO setup	Crosswork Data Gateway Deployment
Cisco Crosswork Network Controller	Mandatory	Mandatory	Standard
Cisco Crossowork Change Automation	Optional	Mandatory	Standard
Cisco Crosswork Health Insights	Optional	Mandatory	Extended
Cisco Crosswork Optimization Engine	Mandatory	Optional	Standard
Cisco Crosswork Zero Touch Provisioning	Optional	Optional	Standard

Network Topology Models

The following figures show the different topology models, and the corresponding network components and connections needed to install and use Cisco Crosswork.

Figure 2: Cisco Crosswork - 1 NIC Network Topology

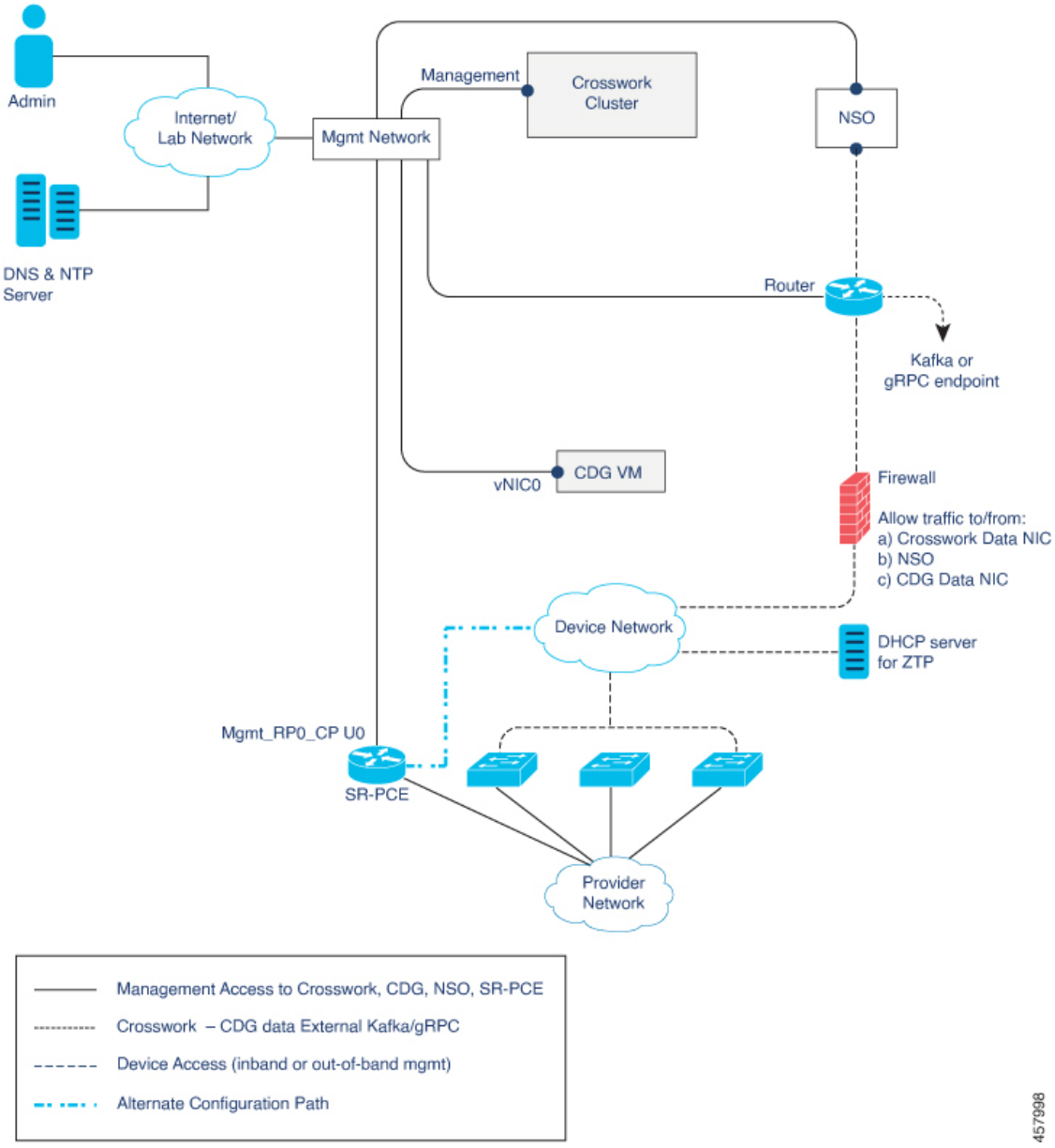


Figure 3: Cisco Crosswork - 2 NIC Network Topology

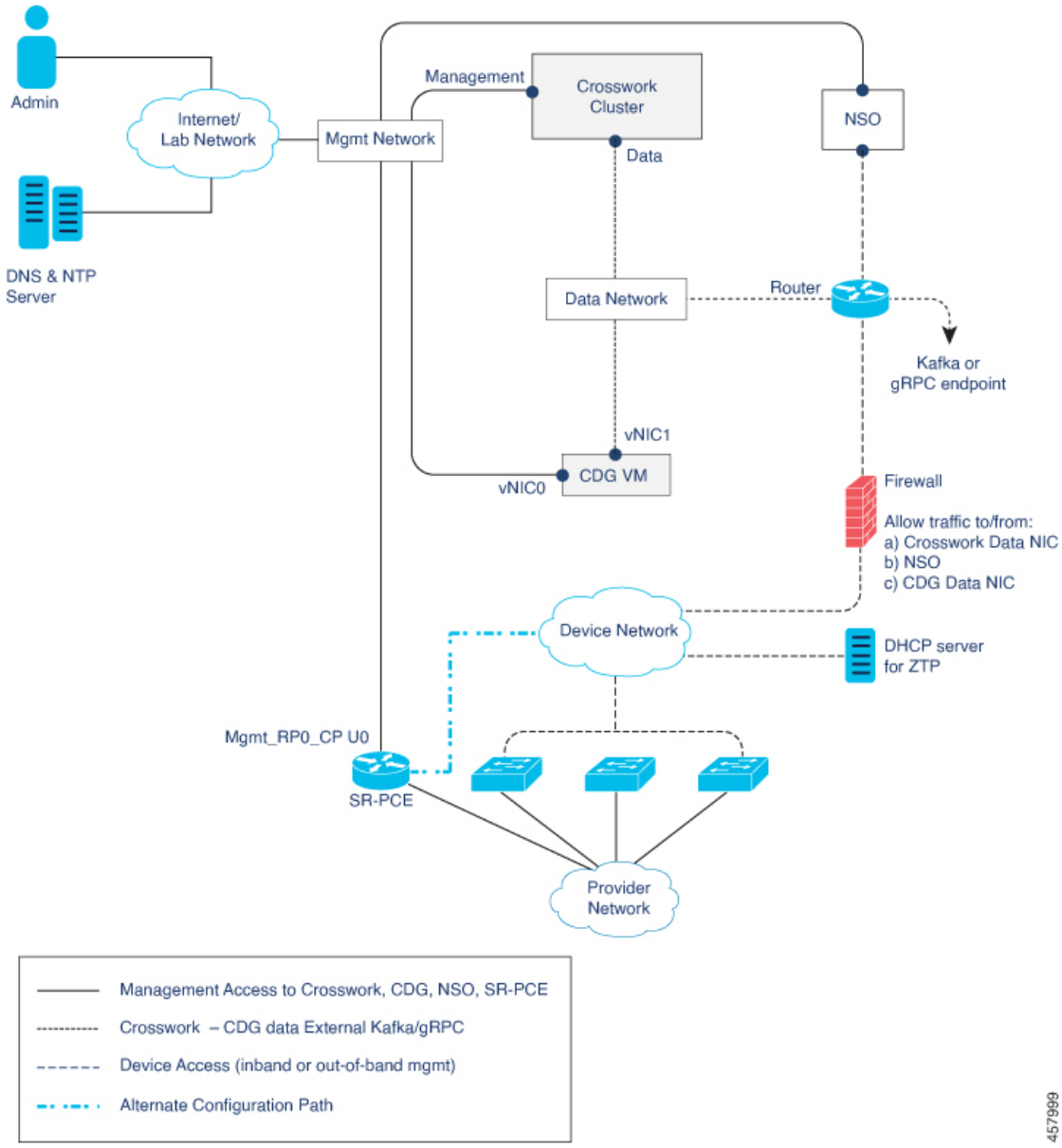
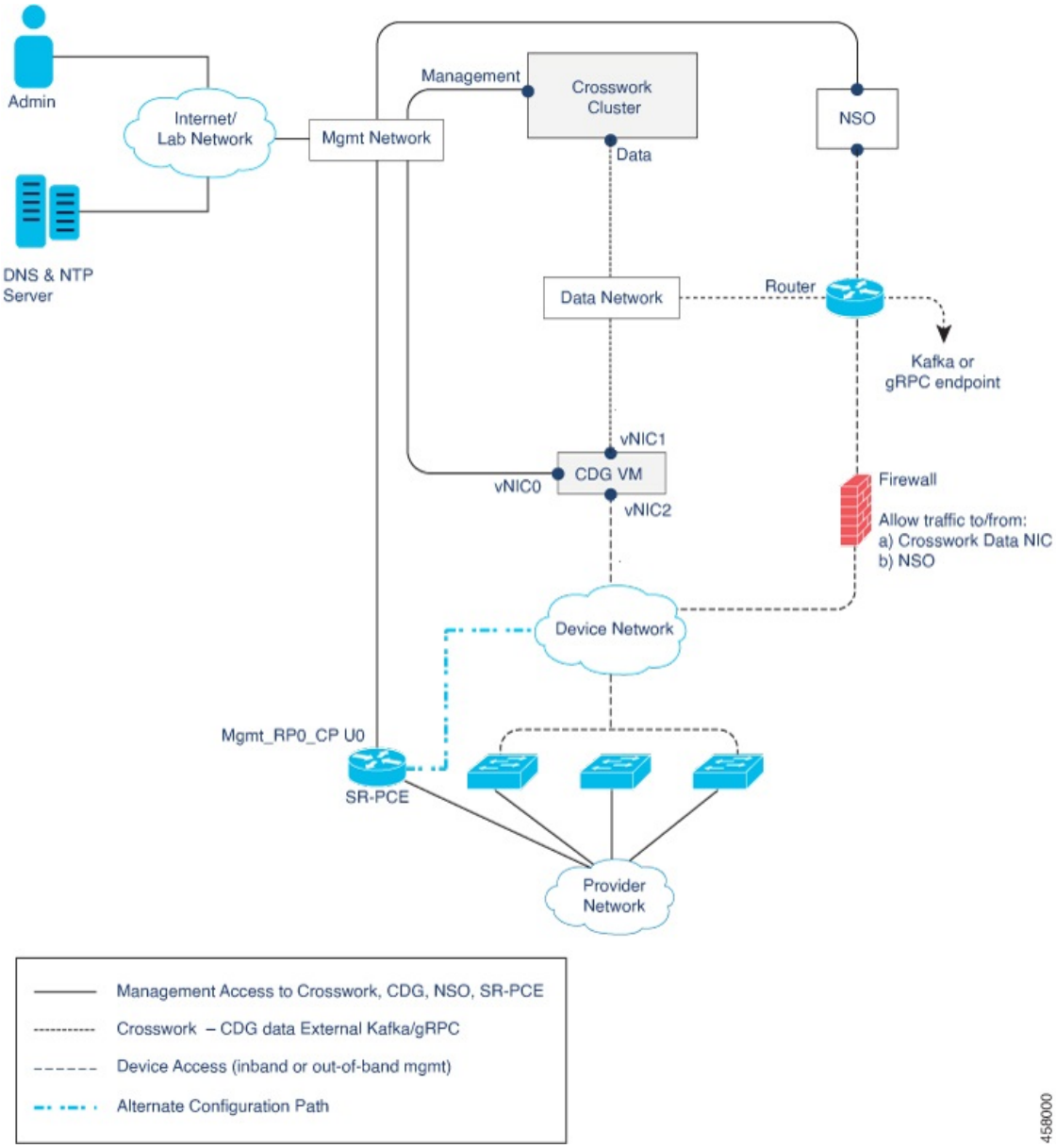


Figure 4: Cisco Crosswork - 3 NIC Network Topology



There are three types of traffic flowing between the network components, as explained below:

Table 14: Types of Network Traffic

Traffic	Description
Management	For accessing the UI and command line, and passing Data information between servers (for example, Cisco Crosswork to Crosswork Data Gateway or NSO)
Data	Data and configuration transfer between Crosswork Data Gateway and Cisco Crosswork, and other data destinations (external Kafka/gRPC).

Traffic	Description
Device Access	Device configuration and management, and telemetry data being forwarded to the Crosswork Data Gateway.

Cisco Crosswork Virtual Machine (VM)

The Cisco Crosswork VM has the following vNIC deployment options:

Table 15: Cisco Crosswork vNIC deployment modes

No. of vNICs	vNIC	Description
1	Management	Management, Data, and Device access passing through a single NIC
2	Management	Management
	Data	Data and Device access

Cisco Crosswork Data Gateway VM

The Cisco Crosswork Data Gateway VM has the following vNIC deployment options:

Table 16: Cisco Crosswork Data Gateway vNIC deployment modes

No. of vNICs	vNIC	Description
1	vNIC0	Management, Data, and Device access passing through a single NIC
2	vNIC0	Management
	vNIC1	Data and Device access
3	vNIC0	Management
	vNIC1	Data
	vNIC2	Device Access

Cisco Network Services Orchestrator (NSO) VM

The NSO VM has the following vNICs:

- Management: Used for Crosswork applications to reach NSO.
- Device Access: Used for NSO to reach devices or NSO Resource Facing Services (RFS).

Note Preference for the number of vNICs can vary from one deployment to another. The number of vNICs can be dependent on the security and traffic isolation needs of the deployment. Crosswork Data Gateway and Crosswork accommodates this variability by introducing a variable number of vNICs.

Routed and Device Networks

Connectivity between the various components should be accomplished via an external routing entity. The figures show various line styles suggesting possible routing domains within the routed network.

- Solid - Management routing domain.
- Dotted - Data/Control routing domain (information transferred between Cisco Crosswork and Cisco Crosswork Data Gateway, and other data destinations (external Kafka or gRPC)).
- Dashes - Device access routing domain (from Cisco Crosswork Data Gateway and NSO).
- Blue dashes - Alternate SR-PCE configuration path

The IP/subnet addressing scheme on each of these domains depends on the type of deployment.

Routing between domains is needed for Crosswork and NSO to reach the devices. However, proper firewall rules need to be in place to allow only select sources (for example, Crosswork and NSO) to reach the devices.

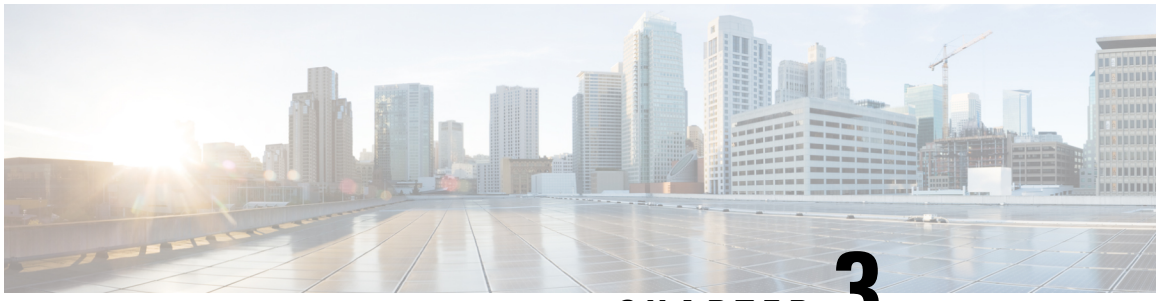
On the device network, devices can be reached in-band or using out-of-band management interfaces, depending on the local security policies of each deployment.

SR-PCE Configuration

A controller supporting Segment Routing Path Computation Element (SR-PCE) is both a device and a Software-Defined Networking (SDN) controller. Some deployments may want to treat an SR-PCE instance as a device, in which case they would need access via the device network. Some deployments may want to treat an SR-PCE instance as an SDN controller and access it on the Management routing domain. Crosswork supports both models. By default, Crosswork will use **`eth0`** (Management) to access SR-PCE as an SDN controller on the Management domain (shown in the figures). To enable Crosswork access to an SR-PCE instance as a device on the device network (shown as alternate path in the figures): When adding an SR-PCE as a provider, add the Property Key and Property Value as **`outgoing-interface`** and **`eth1`** (Data) respectively.

ZTP Requirements

If you plan to use Zero Touch Provisioning, the device network needs to be equipped with a DHCP server.



CHAPTER 3

Install the Crosswork Cluster

This section contains the following topics:

Available Installation Methods

The Cisco Crosswork platform can be installed using the following methods:

Installation using cluster installer tool: The operator uses cluster installer, a one-time day 0 deployment tool, that transfers the inventory data to the running Crosswork cluster and activates the Crosswork cluster management functionality via the GUI. This is the recommended installation method for both vCenter and CSP deployments.

- Install Cisco Crosswork using the Cluster Installer tool, on page 26
  - Install Cisco Crosswork on VMware vCenter , on page 27
  - Install Cisco Crosswork on Cisco CSP, on page 30

Manual installation: This option is available for deployments that cannot use the installer tool, and is recommended only for advanced users.

- Install Cisco Crosswork Manually, on page 34
  - Manual Installation of Cisco Crosswork using vSphere UI, on page 34
  - Manual Installation of Cisco Crosswork on Cisco CSP, on page 42

Installation Parameters

The table below specifies the parameters you need to specify for installing Cisco Crosswork. For more information on the parameters, see Cisco Crosswork Infrastructure Requirements, on page 5.

Parameter Name	Also mentioned as	Description
`ClusterName`		Name of the cluster file
`ClusterIPStack`	`CWIPv4Address`, `CWIPv6Address`	The IP stack protocol: IPv4 or IPv6
`ManagementIPAddress`	`ManagementIPv4Address`, `ManagementIPv6Address`	The Management IP address of the VM (IPv4 or IPv6).
`ManagementIPNetmask`	`ManagementIPv4Netmask`, `ManagementIPv6Netmask`	The Management IP subnet in dotted decimal format (IPv4 or IPv6).
`ManagementIPGateway`	`ManagementIPv4Gateway`, `ManagementIPv6Gateway`	The Gateway IP on the Management Network (IPv4 or IPv6). The address must be reachable, otherwise the installation will fail.
`ManagementVIP`		The Management Virtual IP for the cluster.
`DataIPAddress`	`DataIPv4Address`, `DataIPv6Address`	The Data IP address of the VM (IPv4 or IPv6).
`DataIPNetmask`	`DataIPv4Netmask`, `DataIPv6Netmask`	The Data IP subnet in dotted decimal format (IPv4 or IPv6).
`DataIPGateway`	`DataIPv4Gateway`, `DataIPv6Gateway`	The Gateway IP on the Data Network (IPv4 or IPv6). The address must be reachable, otherwise the installation will fail.
`DataVIP`		The Data Virtual IP for the cluster.
`DNS`	`DNSv4, DNSv6`	The IP address of the DNS server (IPv4 or IPv6). The address must be reachable, otherwise the installation will fail.
`NTP`		NTP server address or name. The address must be reachable, otherwise the installation will fail.
`DomainName`	`Domain`	The domain name used for the cluster
`CWusername`		Username to log into Cisco Crosswork.
`CWPassword`		Password to log into Cisco Crosswork.
`VMSize`		VM size for the cluster (small or large).

Parameter Name	Also mentioned as	Description
`RamDiskSize`	`ramdisk`	Size of the Ram disk. This parameter is only used for lab installations (value must be 2). When a non-zero value is provided for `RamDiskSize`, the `HSDatastore` value is not used.
`VMName`		Name of the VM
`NodeType`	`VMType`	Indicates the type of VM. Choose either "Hybrid" or "Worker".
`IsSeed`		Choose "True" if this is the first VM being built in a new cluster. Choose "False" for all other VMs, or when rebuilding a failed VM.
`InitNodeCount`		Total number of nodes in the cluster including hybrid and worker nodes. The default value is 3.
`InitMasterCount`		Total number of hybrid nodes in the cluster. The default value is 3.
VMware resource data		
`vCenterAddress`		The vCenter IP or host name.
`vCenterUser`		The username needed to log into vCenter.
`vCenterPassword`		The password needed to log into vCenter.
`DCname`		The name of the Data Center resource to use.
`MgmtNetworkName`		The name of the vCenter network to attach to the VM's Management interface.
`DataNetworkName`		The name of the vCenter network to attach to the VM's Data interface.
`Host`		The ESXi host or resource group name.
`Datastore`		The datastore name available to be used by this host or resource group.
`HSDatastore`		The high speed datastore available for this host or resource group.
Cisco CSP resource data		
`name`	`Host`	Host name
`protocol`		Protocol used (e.g. "https")
`server`		Cisco CSP Server IP address

Parameter Name	Also mentioned as	Description
`username`		The username needed to log into Cisco CSP.
`password`		The password needed to log into Cisco CSP.
`insecure`		Default value is "true".
`MgmtNetworkName`		The name of the CSP network to attach to the VM's Management interface.
`DataNetworkName`		The name of the CSP network to attach to the VM's Data interface.

Install Cisco Crosswork using the Cluster Installer tool

Cluster installer tool is the recommended method to install Cisco Crosswork.

The Cisco Crosswork cluster installer is a day 0 installation tool used to deploy the Crosswork cluster with user specified parameters supplied via a template file. The tool is run from a docker container which can be hosted on any docker capable platform including a regular PC/laptop. The docker container contains a set of template files which can be edited to provide the deployment specific data. Separate templates need to be used for vCenter and CSP deployments.

Note Docker version 19 or higher is recommended while using the cluster installer option. For more information on docker, see https://docs.docker.com/get-docker/

Few pointers to know when using the cluster installer tool:

- Make sure that your data center meet all the requirements specified under Cisco Crosswork Infrastructure Requirements, on page 5.
- The install script is safe to run multiple times. Upon error, input parameters can be corrected and re-run. However, it must be noted that running the tool multiple times may result in the deletion and re-creation of VMs.
- The edited template in the `/data` directory will contain sensitive information (VM passwords). The operator needs to manage access to this content. Erase them after use or when you quit the container.
- The `install.log`, `install_tf.log`, and `crosswork-cluster.tfstate` files will be created during the install and stored in the `/data` directory. If you encounter any trouble with the installation, provide these files to the Cisco Customer Experience team when opening a case.
- In case you are using the same installer tool for multiple Crosswork cluster installations, it is important to run the tool from different local directories, allowing for each deployment state files to be independent. The simplest way for doing so is to create on the host machine a local directory for each deployment on the host machine and map each one to the container accordingly.

Note In order to change install parameters or to correct parameters following installation errors, it is important to distinguish whether the installation has managed to deploy the VMs or not. Deployed VMs are evidenced by the output of the installer similar to:

```
vsphere_virtual_machine.crosswork-IPv4-vm["1"]: Creation complete after 2m50s
[id=4214a520-c53f-f29c-80b3-25916e6c297f]
```

In case of deployed VMs, changes to the CW VM settings or the Data Center host for a deployed VM are NOT supported. To change a setting using the installer when the deployed VMs are present, the clean operation needs to be run and the cluster redeployed.

A VM redeployment will delete the VM's data, hence caution is advised. We recommend you to perform VM parameter changes from the CW UI, or alternatively one VM at a time. Installation parameter changes that occur prior to any VM deployment, e.g. an incorrect vCenter parameter, can be performed by applying the change and simply re-running the install operation.

Install Cisco Crosswork on VMware vCenter

This section explains the procedure to install Cisco Crosswork on VMware vCenter using the cluster installer tool.

Before you begin

- Make sure that your environment meets all the vCenter requirements specified under Cisco Crosswork Infrastructure Requirements, on page 5.
- On running, the installer will upload the .ova file into the vCenter if it is not already present, and convert it into a VM template. After the installation is completed successfully, you can delete the template file from the vCenter UI (located under VMs and Templates) if the image is no longer needed.

Step 1 In your docker capable machine, create a directory where you will store everything you will use during the installation.

Step 2 Download the installer bundle (.tar.gz file) and the OVA file from cisco.com to the directory you created previously. For the purpose of these instructions, we will use the file names as "cw-na-platform-4.0.0-37-installer-pkg.tar.gz" and "cw-na-platform-4.0.0-37-release-210410.ova" respectively.

Step 3 Use the following command to unzip the installer bundle:

```
tar -xvf cw-na-platform-4.0.0-37-installer-pkg.tar.gz
```

The contents of the installer bundle is unzipped to a new directory (e.g. `cw-na-platform-4.0.0-37-installer`). This new directory will contain the installer image (e.g. cw-na-platform-installer-4.0.0-37-release-210410.tar.gz) and files necessary to validate the image.

Step 4 Navigate to the directory created in the previous step and use the following command to verify the signature of the installer image:

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

Note If you do not get a successful verification message, please contact the Cisco Customer Experience team.

Step 5 Use the following command to load the installer image file into your Docker environment.

```
docker load -i <.tar.gz file>
```

For example:

```
docker load -i cw-na-platform-installer-4.0.0-37-release-210410.tar.gz
```

The result will be a line similar to the following: (section we will need is underlined for clarity)

```
Loaded image ID: sha256:4a55858a7dd9a5fed7d0d46716e4c9525333525419e5517a4904093f01b3f165
```

Step 6 Launch the Docker container using the following command:

```
docker run --rm -it -v 'pwd':/data 4a55858a7dd9a5fed7d0d46716e4c9525333525419e5517a4904093f01b3f165
```

Note You do not have to enter that full value. In this case, "docker run --rm -it -v 'pwd':/data 4a5" was adequate. You only require enough of the image ID to uniquely identify the image you want to use for the installation.

```
My Machine% docker images
REPOSITORY                                                TAG       IMAGE ID       CREATED         SIZE
cw-na-platform-installer-4.0.0-37-release-210410     <none>    4a55858a7dd9   7 days ago     276MB
```

Step 7 Copy the template file found under `/opt/installer/deployments/4.0.0/vcenter/deployment_template_tfvars` to the `/data` folder using a different name.

For example: `docker cp deployment_template_tfvars /data/deployment.tfvars`

For the rest of this procedure, we will use `deployment.tfvars` in all the examples.

Step 8 Edit the template file in a text editor, adding the necessary parameters:

- Crosswork cluster information such as VM size: Use "Small" for lab deployments, otherwise enter "Large".
- Unique Crosswork VM entries, including names, their IP addresses and node type settings.

  Note Use a strong VM Password (8 character long, including upper & lower case letters, numbers and one special character). The VM setup will fail if a weak password is used.

- vCenter access details and credentials, along with the assignment of the named Crosswork VMs to the Data Center resources.

Note A sample of the template file is posted at the end of this section. The file itself has two parts, the template that you need to fill in with the values for your environment and a set of example data to demonstrate how the information is formatted.

Step 9 From a second terminal window, copy the OVA file to the `/data` directory in your container.

```
docker ps
CONTAINER ID     IMAGE            COMMAND       CREATED         STATUS         PORTS NAMES
1bda806bbd82     4a55858a7dd9     "/bin/sh"     3 hours ago     Up 3 hours     <port-name>
```

Note the container ID.

```
docker cp {image file name} {container id} :/data
```

For example: `docker cp cw-na-platform-4.0.0-37-release-210410.ova 1bda806bbd82:/data`

Step 10 Run the installer.

```
./cw-installer.sh install -p -m /data/<template file name> -o /data/<.ova file>
```

For example:

```
./cw-installer.sh install -p -m /data/deployment.tfvars -o
/data/cw-na-platform-4.0.0-37-release-210410.ova
```

Note If the installation fails, you should try rerunning the installation without the `-p` option. This will deploy the VMs serially rather than in parallel.

Step 11 Enter "yes" when prompted to accept the End User License Agreement (EULA).

Step 12 Enter "yes" when prompted to confirm the operation.

Example

Template example:

The following example might be used for a lab as it deploys the 3 hybrid nodes with two of the VMs on the same host and the third VM on a second host using the small configuration.

Note In case you are using resource pools, please note that individual ESXi host targetting is not allowed and vCenter is responsible for assigning the VM to a host in the resource pool.

If vCenter is not configured with resource pools, then the exact ESXi host path must be passed.

```
*******
vCenter Example
********

//#********* Crosswork Cluster Data *********#

ClusterName = "day0-cluster"
Cw_VM_Image = ""
ManagementVIP = "17.25.87.94"
ManagementIPNetmask = "255.255.255.192"
ManagementIPGateway = "17.25.87.65"
DataVIP = "192.168.123.94"
DataIPNetmask = "255.255.255.0"
DataIPGateway = "0.0.0.0"
DNS = "17.70.168.183"
DomainName = "somedomain.com"
CWPassword = "AStr0ngPa33!"
VMSize = "Small"
NTP = "ntp.com"
ClusterIPStack = "IPv4"
RamDiskSize = 0

#********* Crosswork VM Data Map *********

CwVMs = {
"0" = {
VMName = "vm1",
ManagementIPAddress = "17.25.87.82",
DataIPAddress = "192.168.123.82",
NodeType = "Hybrid"
},
"1" = {
VMName = "vm2",
ManagementIPAddress = "17.25.87.83",
DataIPAddress = "192.168.123.83",
```

```
NodeType = "Hybrid"
},
"2" = {
VMName = "vm3",
ManagementIPAddress = "17.25.87.84",
DataIPAddress = "192.168.123.84",
NodeType = "Hybrid"
}
}


#********* vCenter Resource Data with Cw VM assignment *********

vCenterDC = {
vCenterAddress = "17.25.87.90",
vCenterUser = "administrator@vsphere.local",
vCenterPassword = "vCenterPass",
DCname = "dc-cr",
MgmtNetworkName = "VM Network",
DataNetworkName = "DPortGroup10",
DCfolder = "",
VMs = [{
HostedCwVMs = ["0","1"],
Host = "17.25.87.93",
Datastore = "datastore3",
HSDatastore = "datastore3"
},
{
HostedCwVMs = ["2"],
Host = "17.25.87.92",
Datastore = "datastore2",
HSDatastore = "datastore2"
}
]
}
```

What to do next

The time taken to create the cluster can vary based on the size of your deployment profile and the performance characteristics of your hardware. See Monitor the Installation, on page 48 to know how you can check the status of the installation.

Install Cisco Crosswork on Cisco CSP

This section explains the procedure to install Cisco Crosswork on Cisco CSP using the cluster installer tool.

Before you begin

- Make sure that your environment meets all the CSP requirements specified under Cisco Crosswork Infrastructure Requirements, on page 5.

Step 1 In your docker capable machine, create a directory where you will store everything you will use during the installation.

Step 2 Download the installer bundle (.tar.gz file) and the QCOW2 bundle (.tar.gz file) from cisco.com to the directory you created previously. For the purpose of these instructions, we will use the file names as "cw-na-platform-4.0.0-37-installer-pkg.tar.gz" and "cw-na-platform-4.0.0-37-qcow2-pkg.tar.gz" respectively.

Step 3 Use the following command to unzip the installer bundle:

```
tar -xvf cw-na-platform-4.0.0-37-installer-pkg.tar.gz
```

The contents of the installer bundle is unzipped to a new directory (e.g. `cw-na-platform-4.0.0-37-installer`). This new directory will contain the installer image (e.g. cw-na-platform-installer-4.0.0-37-release-210410.tar.gz) and files necessary to validate the image.

Step 4 Navigate to the directory created in the previous step and use the following command to verify the signature of the installer image:

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

Note If you do not get a successful verification message, please contact the Cisco Customer Experience team.

Step 5 Use the following command to load the installer image file into your Docker environment.

```
docker load -i <.tar.gz file>
```

For example:

```
docker load -i cw-na-platform-installer-4.0.0-37-release-210410.tar.gz
```

The result will be a line similar to the following: (section we will need is underlined for clarity)

```
Loaded image ID: sha256:4a55858a7dd9a5fed7d0d46716e4c9525333525419e5517a4904093f01b3f165
```

Step 6 Launch the Docker container using the following command:

```
docker run --rm -it -v 'pwd':/data 4a55858a7dd9a5fed7d0d46716e4c9525333525419e5517a4904093f01b3f165
```

Note You do not have to enter that full value. In this case, "docker run --rm -it -v 'pwd':/data 4a5" was adequate. You only require enough of the image ID to uniquely identify the image you want to use for the installation.

```
My Machine% docker images
REPOSITORY                                          TAG       IMAGE ID       CREATED         SIZE
cw-na-platform-installer-4.0.0-37-release-210410    <none>    4a55858a7dd9   7 days ago      276MB
```

Step 7 Copy the template file found under `/opt/installer/deployments/4.0.0/csp/deployment_template_tfvars` to the `/data` folder using a different name.

For example: `docker cp deployment_template_tfvars /data/deployment.tfvars`

For the rest of this procedure, we will use `deployment.tfvars` in all the examples.

Step 8 Edit the template file in a text editor, adding the necessary parameters:

- Crosswork cluster information such as VM size: Use "Small" for lab deployments, otherwise enter "Large".
- Unique Crosswork VM entries, including names, their IP addresses and node type settings.

  Note Use a strong VM Password (8 character long, including upper & lower case letters, numbers and one special character). The VM setup will fail if a weak password is used.

- Cisco CSP access details and credentials, along with the assignment of the named Crosswork VMs to the Cisco CSP host resources.

Note A sample of the template file is posted at the end of this section. The file itself has two parts, the template that you need to fill in with the values for your environment and a set of example data to demonstrate how the information is formatted.

Step 9 From a second terminal window, unzip the QCOW2 bundle (.tar.gz file):

```
tar -xvf cw-na-platform-4.0.0-37-qcow2-pkg.tar.gz
```

The contents of the QCOW2 bundle is unzipped to a new directory (e.g. `cw-na-platform-4.0.0-37-qcow2`). This new directory will contain the QCOW2 image (e.g. cw-na-platform-4.0.0-37-release-201410-qcow2.tar.gz) and files necessary to validate the image.

Step 10 Navigate to the directory created in the previous step, and use the following command to verify the signature of the QCOW2 image:

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

Note If you do not get a successful verification message, please contact the Cisco Customer Experience team.

Step 11 Copy the platform release file (qcow2.tar.gz) to the `/data` directory in your container.

```
docker ps
CONTAINER ID     IMAGE            COMMAND       CREATED         STATUS         PORTS NAMES
1bda806bbd82     4a55858a7dd9     "/bin/sh"     3 hours ago     Up 3 hours     <port-name>
```

Note the container ID.

```
docker cp {image file name} {container id} :/data
```

For example: `docker cp cw-na-platform-4.0.0-37-release-201410-qcow2.tar.gz 1bda806bbd82 :/data`

Step 12 Run the installer.

```
./cw-installer.sh install -t csp -m /data/<template file name> -o /data/<qcow2.tar.gz file> -p
```

For example:

```
./cw-installer.sh install -t csp m /data/deployment.tfvars -o
/data/cw-na-platform-4.0.0-37-release-201410-qcow2.tar.gz -p
```

Note If the installation fails, you should try rerunning the installation without the `-p` option. This will deploy the VMs serially rather than in parallel.

Step 13 Enter "yes" when prompted to accept the End User License Agreement (EULA).

Step 14 Enter "yes" when prompted to confirm the operation.

Example

Template example:

The following example might be used for a lab as it deploys the 3 hybrid nodes with two of the VMs on the same host and the third VM on a second host using the small configuration.

```
//*******
//CSP Example
//********

//#********* Crosswork Cluster Data  *********#

  ClusterName = "day0-cluster"
  Cw_VM_Image           = ""
  ManagementVIP     = "17.25.87.94"
  ManagementIPNetmask = "255.255.255.192"
```

```
  ManagementIPGateway = "17.25.87.65"
  DataVIP           = "192.168.123.94"
  DataIPNetmask       = "255.255.255.0"
  DataIPGateway       = "0.0.0.0"
  DNS                 = "17.70.168.183"
  DomainName            = "somedomain.com"
  CWPassword            = "AStr0ngPa33!"
  VMSize                = "Small"
  NTP                   = "ntp.com"
  ClusterIPStack        = "IPv4"
  RamDiskSize = 0

#********* Crosswork VM Data Map *********

CwVMs = {
  "0" = {
    VMName                = "vm1",
    ManagementIPAddress = "17.25.87.82",
    DataIPAddress       = "192.168.123.82",
    NodeType               = "Hybrid"
  },
  "1" = {
    VMName                = "vm2",
    ManagementIPAddress = "17.25.87.83",
    DataIPAddress       = "192.168.123.83",
    NodeType               = "Hybrid"
  },
  "2" = {
    VMName                = "vm3",
    ManagementIPAddress = "17.25.87.84",
    DataIPAddress       = "192.168.123.84",
    NodeType               = "Hybrid"
  }
}


#********* CSP Resource Data with Cw VM assignment *********

CSPCluster = {
  hosts = [{
    name = "host1",
    protocol = "https",
    server = "10.0.0.102",
    username = "admin",
    password = "Spass",
    insecure = true
  },
  {
    name = "host2",
    protocol = "https",
    server = "10.0.0.108",
    username = "admin",
    password = "Spass",
    insecure = true
  }]
  VMs = [{
    HostedCwVMs = ["0","1"],
    Host = "host1",
    MgmtNetworkName = "Eth1-1",
    DataNetworkName = "Eth1-2"
  },
    {
      HostedCwVMs = ["2"],
      Host = "host2",
```

```
      MgmtNetworkName = "Eth0-1",
      DataNetworkName = "Eth9-1"
    }
  ]
}
```

What to do next

The time taken to create the cluster can vary based on the size of your deployment profile and the performance characteristics of your hardware. See Monitor the Installation, on page 48 to know how you can check the status of the installation.

Install Cisco Crosswork Manually

This section describes how Cisco Crosswork can be manually installed in VMware and Cisco CSP.

Manual Installation of Cisco Crosswork using vSphere UI

This section explains the procedure to manually install Cisco Crosswork on VMware vCenter using the vSphere UI. The procedure needs to repeated for each node in the cluster.

Before you begin

- Make sure that your environment meets all the vCenter requirements specified under Cisco Crosswork Infrastructure Requirements, on page 5.

Step 1 Download the latest available Cisco Crosswork image file (*.ova) to your system.

Step 2 With VMware ESXi running, log in to the VMware vSphere Web Client. On the left navigation pane, choose the ESXi host on which you want to deploy the VM.

Step 3 Choose Actions > Deploy OVF Template.

Caution The default VMware vCenter deployment timeout is 15 minutes. The total time needed to deploy the OVA image file may take much longer than 15 minutes, depending on your network speed and other factors. If vCenter times out during deployment, the resulting VM will be unbootable. To prevent this, we recommend that you either set the vCenter deployment timeout to a much longer period (such as one hour), or unTAR the OVA file before continuing, and then deploy using the OVA's four separate Open Virtualization Format and Virtual Machine Disk component files: cw.ovf, cw_rootfs.vmdk, cw_dockerfs.vmdk, and cw_extrafs.vmdk.

Step 4 The VMware Deploy OVF Template window appears, with the first step, 1 - Select an OVF template, highlighted. Click Choose Files 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.

Step 5 Click Next. The Deploy OVF Template window is refreshed, with 2 - Select a name and folder now highlighted. Enter a name and select the respective Datacenter for the Cisco Crosswork VM you are creating.

We recommend that you include the Cisco Crosswork version and build number in the name, for example: Cisco Crosswork 4.0 Build 152.

Step 6 Click Next. The Deploy OVF Template window is refreshed, with 3 - Select a compute resource highlighted. Select the host for your Cisco Crosswork VM.

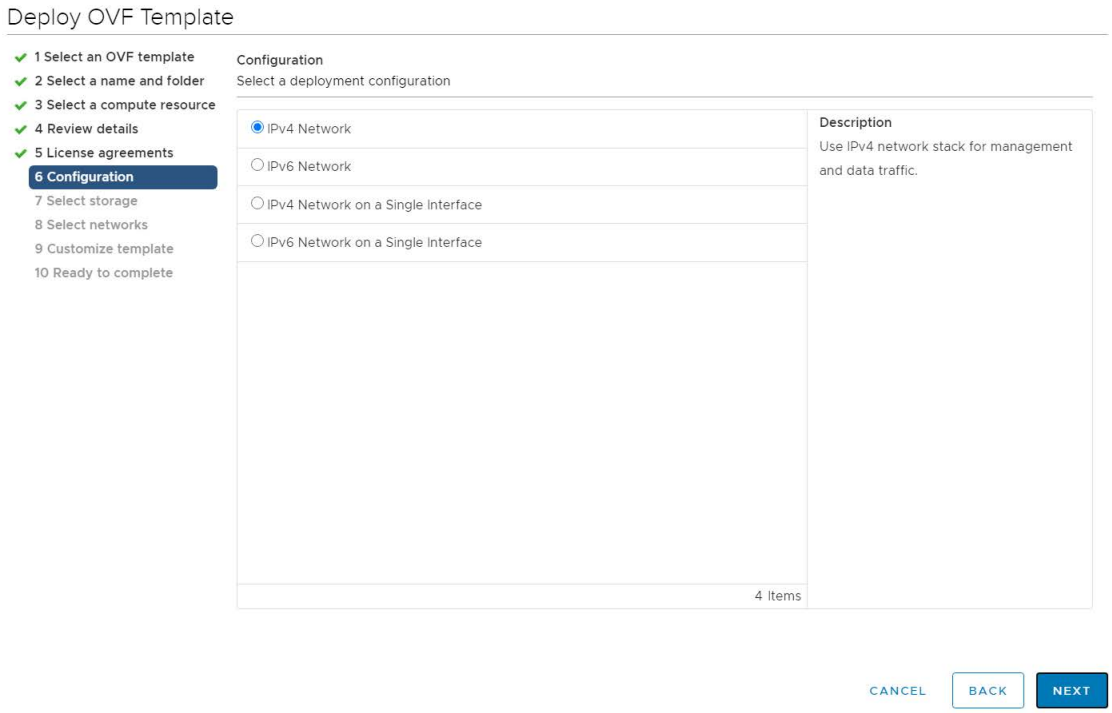
Step 7 Click Next. The VMware vCenter Server validates the OVA. Network speed will determine how long validation takes. After the validation is complete, the Deploy OVF Template window is refreshed, with 4 - Review details highlighted.

Step 8 Review the OVF template that you are deploying. Note that this information is gathered from the OVF, and cannot be modified.

Step 9 Click Next. The Deploy OVF Template window is refreshed, with 5 - License agreements highlighted. Review the End User License Agreement and click the I accept all license agreements checkbox.

Step 10 Click Next The Deploy OVF Template window is refreshed, with 6 - Configuration highlighted. Choose the desired deployment configuration.

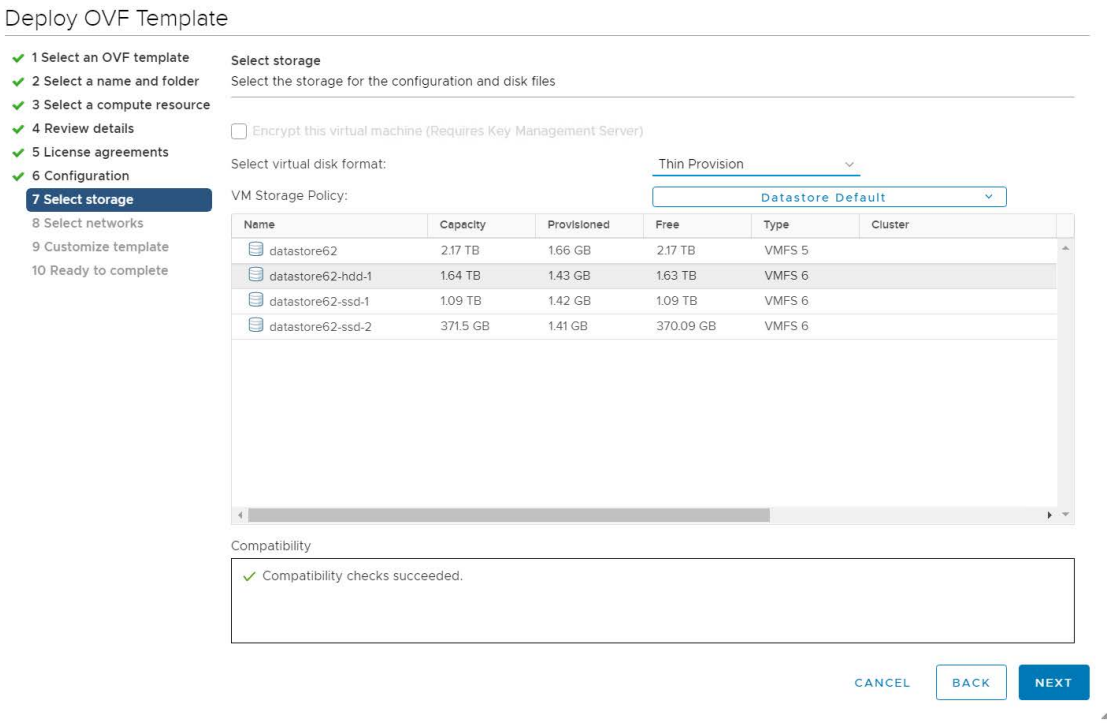
Figure 5: Select a deployment configuration



Note In order for Cisco Crosswork Data Gateway to be deployed using a single interface, Cisco Crosswork must be deployed using a single interface only. Configuring Cisco Crosswork with a single interface should only be done for lab environments.

Step 11 Click Next. The Deploy OVF Template window is refreshed, with 7 - Select Storage highlighted. Choose the relevant option from the Select virtual disk format drop-down list. From the table, choose the datastore you want to use, and review its properties to ensure there is enough available storage.

Figure 6: Select Storage



Note For production deployment, choose the Thick provision eager zeroed option because this will preallocate disk space and provide the best performance. For development purposes, we recommend the Thin provision option because it saves disk space.

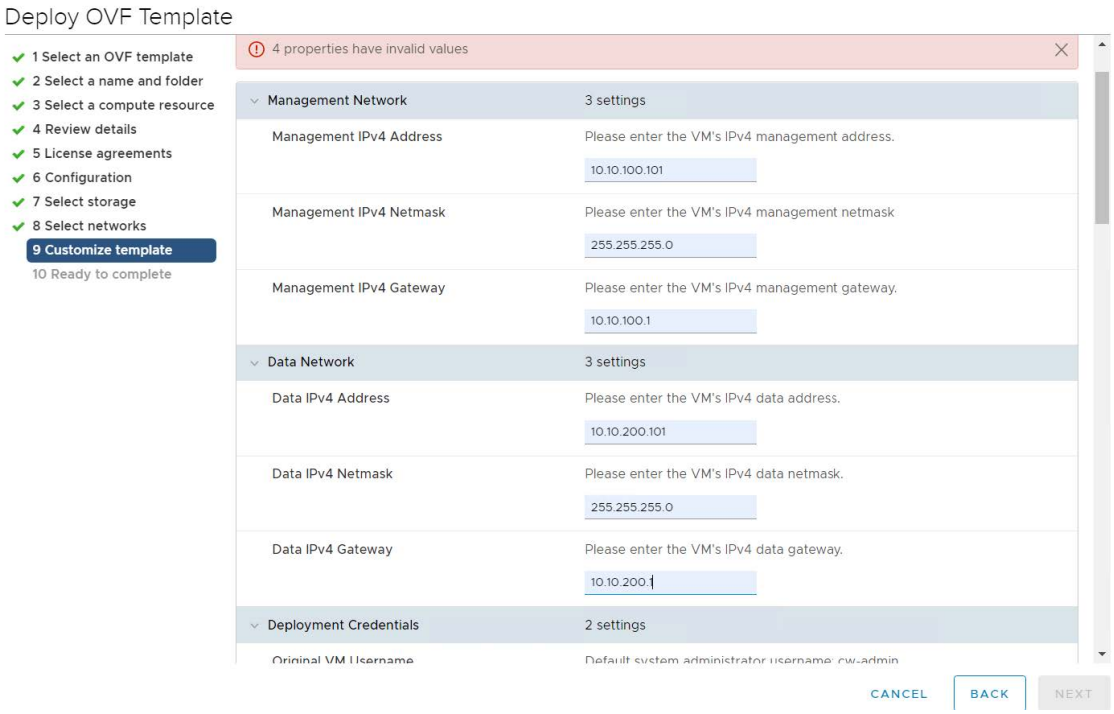
Step 12 Click Next. The Deploy OVF Template window is refreshed, with 8 - Select networks highlighted. From the Data Network and Management Network drop-down lists, choose an appropriate destination network.

Step 13 Click Next. The Deploy OVF Template window is refreshed, with 9 - Customize template highlighted.

a) Expand the Management Network settings. Provide information for the IPv4 or IPv6 deployment (as per your selection).

b) Expand the Data Network settings. Provide information for the IPv4 or IPv6 deployment (as per your selection).

Figure 7: Customize template settings

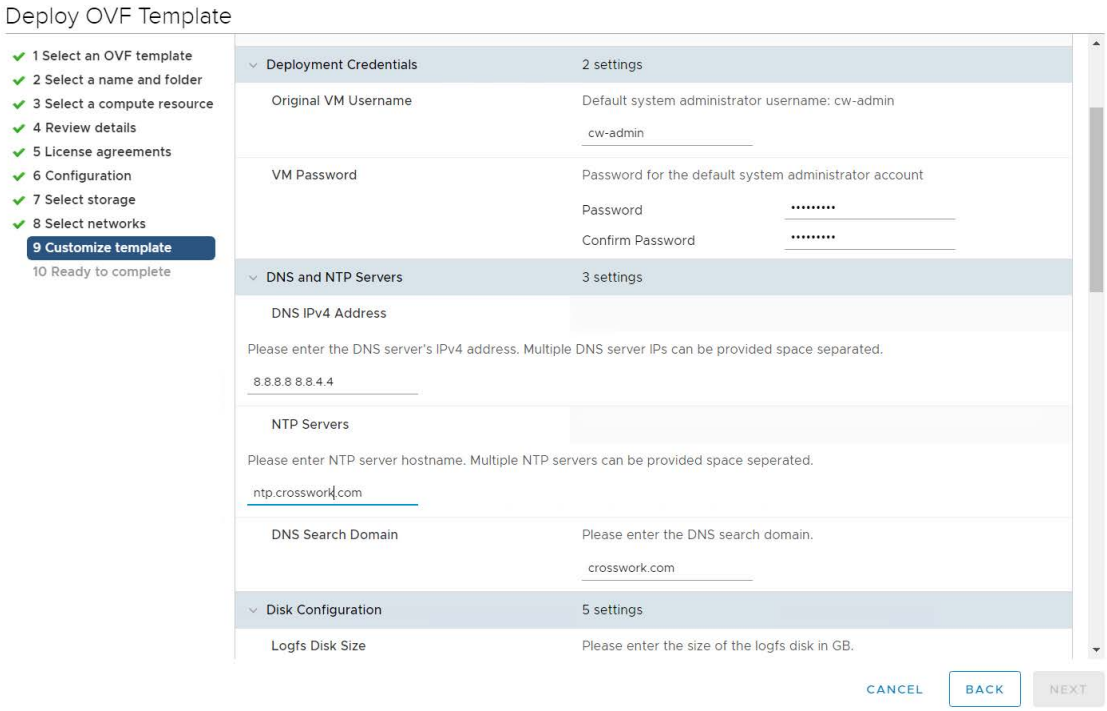


Note Data Network settings are not displayed if you have selected the IPv4 on a Single Interface or IPv6 on a Single Interface configuration.

c) Expand the Deployment Credentials settings. Enter relevant values for the VM Username and Password.

d) Expand the DNS and NTP Servers settings. According to your deployment configuration (IPv4 or IPv6), the fields that are displayed are different. Provide information in the following three fields:

- DNS IP Address: The IP addresses of the DNS servers you want the Cisco Crosswork server to use. Separate multiple IP addresses with spaces.
- DNS Search Domain: The name of the DNS search domain.
- NTP Servers: The IP addresses or host names of the NTP servers you want to use. Separate multiple IPs or host names with spaces.



Note The DNS and NTP servers must be reachable using the network interfaces you have mapped on the host. Otherwise, the configuration of the VM will fail.

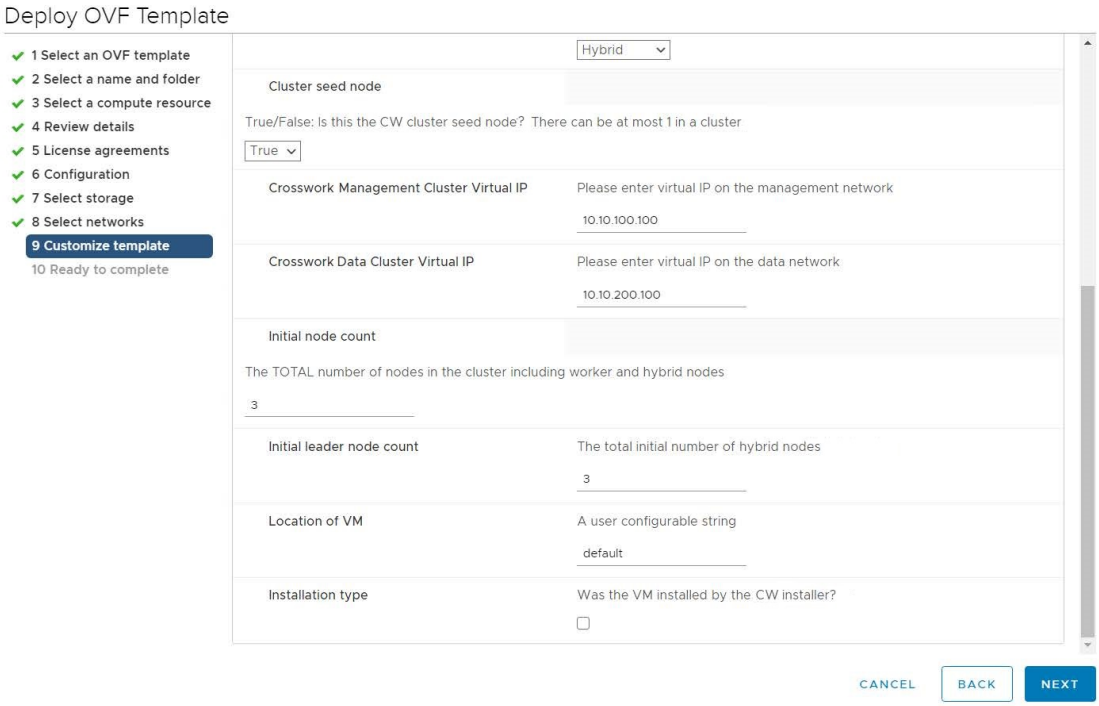
e) Expand Disk Configuration and adjust the amount of storage space available to Cisco Crosswork. The default settings should work for most environments. For assistance in adding additional storage, contact the Cisco Customer Experience team.

f) Expand Crosswork Configuration and enter your legal disclaimer text (users will see this text if they log into the CLI).

g) Expand Crosswork Cluster Configuration. Provide relevant values for the following fields:

- VM Type:
  - Choose Hybrid if this is one of the 3 hybrid nodes.
  - Choose Worker if this is a worker node.
- Cluster Seed node:
  - Choose True if this is the first VM being built in a new cluster.
  - Choose False for all other VMs, or when rebuilding a failed VM.
- Crosswork Management Cluster Virtual IP: Enter the Management Virtual IP address.
- Crosswork Data Cluster Virtual IP: Enter the Data Virtual IP address.
- Initial node count: Default value is 3.
- Initial leader node count: Default value is 3.
- Location of VM: Enter the location of VM.

- Installation type:
  - For new cluster installation: Do not select the checkbox.
  - Replacing a failed VM: Select the checkbox if this VM is being installed to replace a failed VM.



Step 14 Click Next. The Deploy OVF Template window is refreshed, with 10 - Ready to Complete highlighted.

Step 15 Review your settings and then click Finish if you are ready to begin deployment. Wait for the deployment to finish before continuing. To check the deployment status:

a) Open a VMware vCenter client.

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

Step 16 After the first VM deployment is completed, you can create a template to quicken the deployment of the remaining VMs in the cluster. To create a template, select the host and right-click on the newly installed VM and select Template > Convert to Template. A prompt confirming the action is displayed. Click Yes to confirm.

The template is created under the VMs and Templates tab in the vSphere Client UI.

Step 17 To deploy the remaining VMs from the newly created template, right-click on the template and select New VM from This Template.

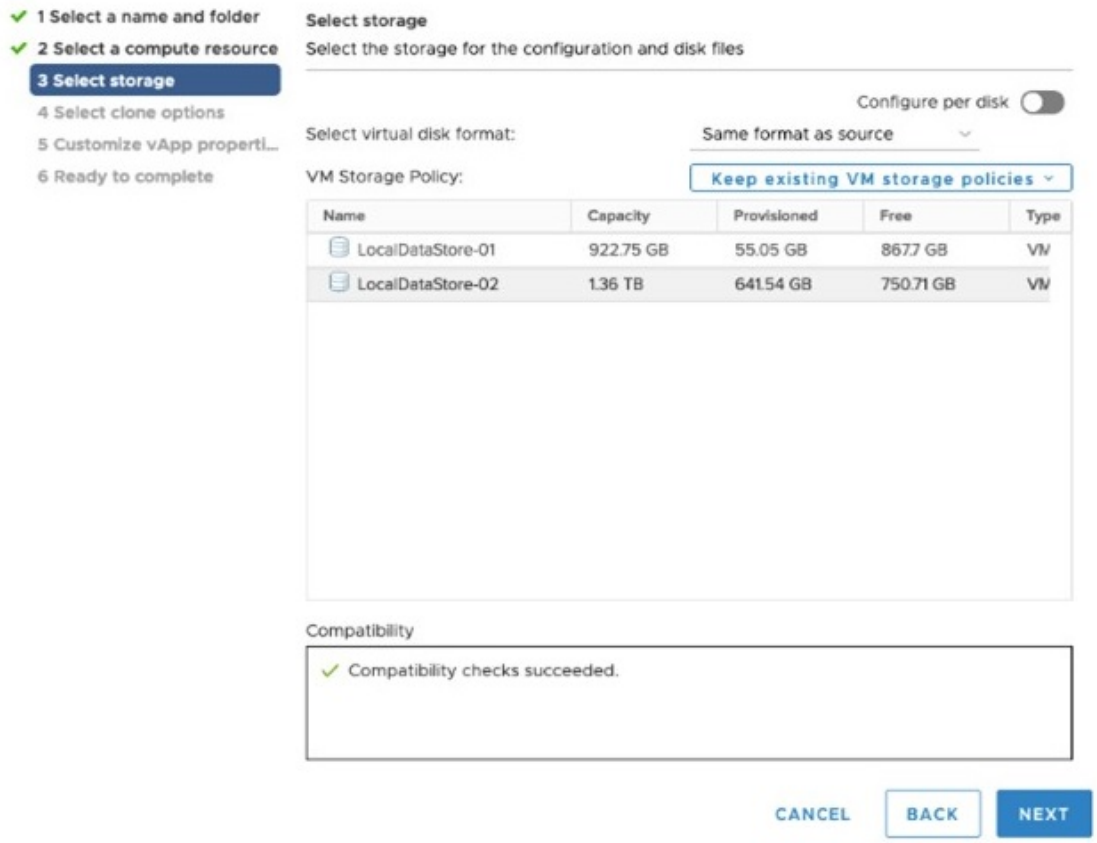
Step 18 The VMware Deploy From Template window appears, with the first step, 1 - Select a name and folder, highlighted. Enter a name and select the respective Datacenter for the VM.

Step 19 Click Next. The Deploy From Template window is refreshed, with 2 - Select a compute resource highlighted. Select the host for your Cisco Crosswork VM.

Step 20 Click Next. The Deploy From Template window is refreshed, with 3 - Select Storage highlighted. Choose Same format as source option as the virtual disk format (recommended).

If you are using a single data store: Select the data store you wish to use, and click Next.

Figure 8: Select Storage - single data store

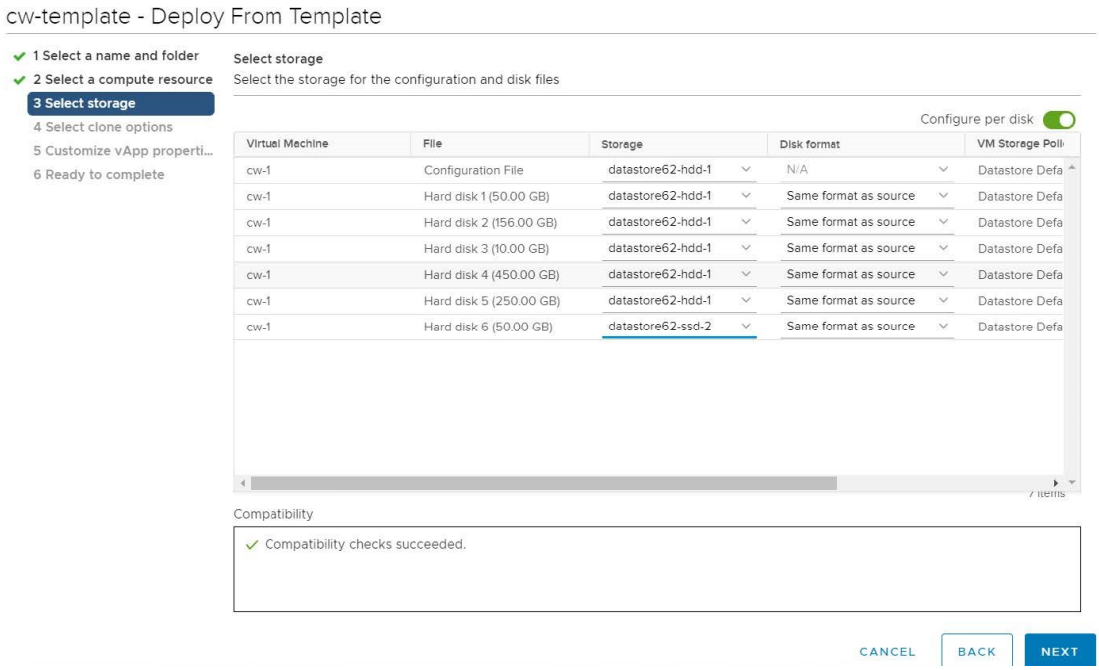


If you are using two data stores (regular and high speed):

- Enable Configure per disk option.
- Select regular data store as the Storage setting for all the disks except disk 6.
- Select high speed (ssd) data store as the Storage setting for disk 6.

  Note This disk must have 50 GB of free storage space.

Figure 9: Select Storage - Configure per disk



- Click Next.

Step 21 The Deploy From Template window is refreshed, with 4 - Select clone options highlighted. You can choose further clone options here.

(Optional) Perform the following steps to configure the disk, memory and Extensive Firmware Interface (EFI) boot settings:

- Choose Customize this virtual machine's hardware and click Next. The Edit Settings dialog box is displayed.
- Under Virtual Hardware tab, enter the relevant values (see VM Host Requirements, on page 7) for CPU and Memory.
- Under VM Options tab, expand Boot Options, select EFI as the Firmware, and check the Secure Boot checkbox.

Step 22 Click Next. The Deploy From Template window is refreshed, with 5 - Customize vApp properties highlighted. The vApp properties from the template is already populated in this window. You need to check the following fields:

- Cluster Seed node:
  - Choose True if this is the first VM being built in a new cluster.
  - Choose False for all other VMs, or when rebuilding a failed VM.
- Management Network settings: Enter correct IP values for each VM in the cluster.
- Data Network settings: Enter correct IP values for each VM in the cluster.
- Crosswork Management Cluster Virtual IP: The Virtual IP will remain same for each cluster node.
- Crosswork Data Cluster Virtual IP: The Virtual IP will remain same for each cluster node.

- Deployment Credentials: Enter same deployment credentials for each VM in the cluster.

Note If this VM is being deployed to replace a failed VM, the IP and other settings must match the machine being replaced.

Step 23 Click Next. The Deploy From Template window is refreshed, with 6 - Ready to complete highlighted. Review your settings and then click Finish if you are ready to begin deployment.

Step 24 Repeat from Step 17 to Step 23 to deploy the remaining VMs in the cluster.

Step 25 You can now power on Cisco Crosswork VMs to complete the deployment process. The VM selected as the cluster seed node must be powered on first, followed by the remaining VMs (after a delay of few minutes). To power on, expand the host's entry, click the Cisco Crosswork VM, and then choose Actions > Power > Power On.

The time taken to create the cluster can vary based on the size of your deployment profile and the performance characteristics of your hardware. See Monitor the Installation, on page 48 to know how you can check the status of the installation.

Note If you are running this procedure to replace a failed VM, then you can check the status from the Cisco Crosswork GUI (go to Administration > Crosswork Manager and click on the cluster tile to check the Crosswork Cluster status.

Manual Installation of Cisco Crosswork on Cisco CSP

Follow the steps to install Cisco Crosswork on Cisco CSP:

Note The below procedure is also used to deploy additional worker nodes in Cisco CSP, by setting the `VMType` value in the `ovf-env.xml` file as Worker.

Step 1 Prepare the Cisco Crosswork service image for upload to Cisco CSP:

a) Download and extract the Cisco Crosswork `qcow2` build from cisco.com 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` file and the template file (.tpl).

Note The procedure requires `ovf-env.xml` file. You must create it using the template file found in the build.

b) Open the `ovf-env.xml` file and modify the parameters as per your installation requirements.

Below is an example of how the `ovf-env.xml` file looks like:

```
<?xml version="1.0" encoding="UTF-8"?>
<Environment>
     xmlns="http://schemas.dmtf.org/ovf/environment/1"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xmlns:oe="http://schemas.dmtf.org/ovf/environment/1"
     xmlns:ve="http://www.cisco.com/schema/ovfenv"
     oe:id=""
   <PlatformSection>
      <Kind>Cisco CSP</Kind>
      <Version>2.8</Version>
```

```
      <Vendor>Cisco</Vendor>
      <Locale>en</Locale>
   </PlatformSection>
   <PropertySection>
         <Property oe:key="CWIPv4Address" oe:value="0.0.0.0"/>
         <Property oe:key="CWIPv6Address" oe:value="::0"/>
         <Property oe:key="CWPassword" oe:value="{{.CWPassword}}"/>
         <Property oe:key="CWUsername" oe:value="{{.CWUsername}}"/>
         <Property oe:key="ClusterName" oe:value="{{.ClusterName}}"/>
         <Property oe:key="CwInstaller" oe:value="True"/>
         <Property oe:key="DNSv4" oe:value="{{.DNSv4}}"/>
         <Property oe:key="DNSv6" oe:value="{{.DNSv6}}"/>
         <Property oe:key="DataIPv4Address" oe:value="{{.DataIPv4Address}}"/>
         <Property oe:key="DataIPv4Gateway" oe:value="{{.DataIPv4Gateway}}"/>
         <Property oe:key="DataIPv4Netmask" oe:value="{{.DataIPv4Netmask}}"/>
         <Property oe:key="DataIPv6Address" oe:value="{{.DataIPv6Address}}"/>
         <Property oe:key="DataIPv6Gateway" oe:value="{{.DataIPv6Gateway}}"/>
         <Property oe:key="DataIPv6Netmask" oe:value="{{.DataIPv6Netmask}}"/>
         <Property oe:key="DataVIP" oe:value="{{.DataVIP}}"/>
         <Property oe:key="Deployment" oe:value="{{.Deployment}}"/>
         <Property oe:key="Disclaimer" oe:value="{{.Disclaimer}}"/>
         <Property oe:key="Domain" oe:value="{{.Domain}}"/>
         <Property oe:key="InitMasterCount" oe:value="{{.InitMasterCount}}"/>
         <Property oe:key="InitNodeCount" oe:value="{{.InitNodeCount}}"/>
         <Property oe:key="IsSeed" oe:value="{{.IsSeed}}"/>
         <Property oe:key="K8Orch" oe:value=""/>
         <Property oe:key="ManagementIPv4Address" oe:value="{{.ManagementIPv4Address}}"/>
         <Property oe:key="ManagementIPv4Gateway" oe:value="{{.ManagementIPv4Gateway}}"/>
         <Property oe:key="ManagementIPv4Netmask" oe:value="{{.ManagementIPv4Netmask}}"/>
         <Property oe:key="ManagementIPv6Address" oe:value="{{.ManagementIPv6Address}}"/>
         <Property oe:key="ManagementIPv6Gateway" oe:value="{{.ManagementIPv6Gateway}}"/>
         <Property oe:key="ManagementIPv6Netmask" oe:value="{{.ManagementIPv6Netmask}}"/>
         <Property oe:key="ManagementVIP" oe:value="{{.ManagementVIP}}"/>
         <Property oe:key="NSOProvider" oe:value="False"/>
         <Property oe:key="NTP" oe:value="{{.NTP}}"/>
         <Property oe:key="VMType" oe:value="{{.VMType}}"/>
         <Property oe:key="corefs" oe:value="20"/>
         <Property oe:key="ddatafs" oe:value="200"/>
         <Property oe:key="logfs" oe:value="10"/>
         <Property oe:key="ramdisk" oe:value="{{.RamDiskSize}}"/>
   </PropertySection>
</Environment>
```

Note Only one node in the cluster must have `IsSeed` set to True.

Step 2 Upload Cisco Crosswork service image to Cisco CSP:

a) Log in to the Cisco CSP.

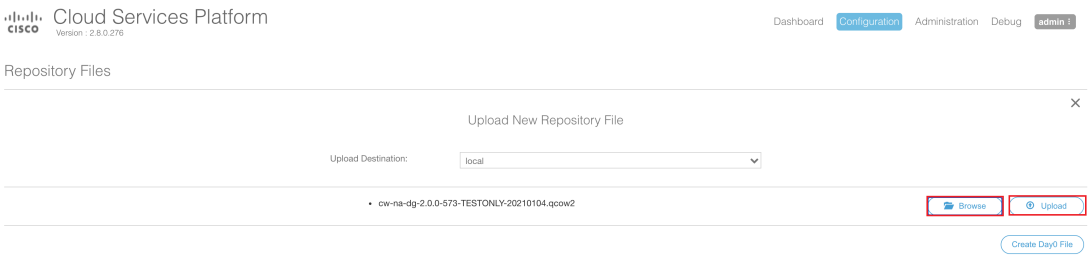
b) Go to Configuration > Repository.

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 `ovf-env.xml` file.



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

Step 3 Create Cisco Crosswork VM:

a) Go to Configuration > Services.

b) On the Service page, click ⊞ button.

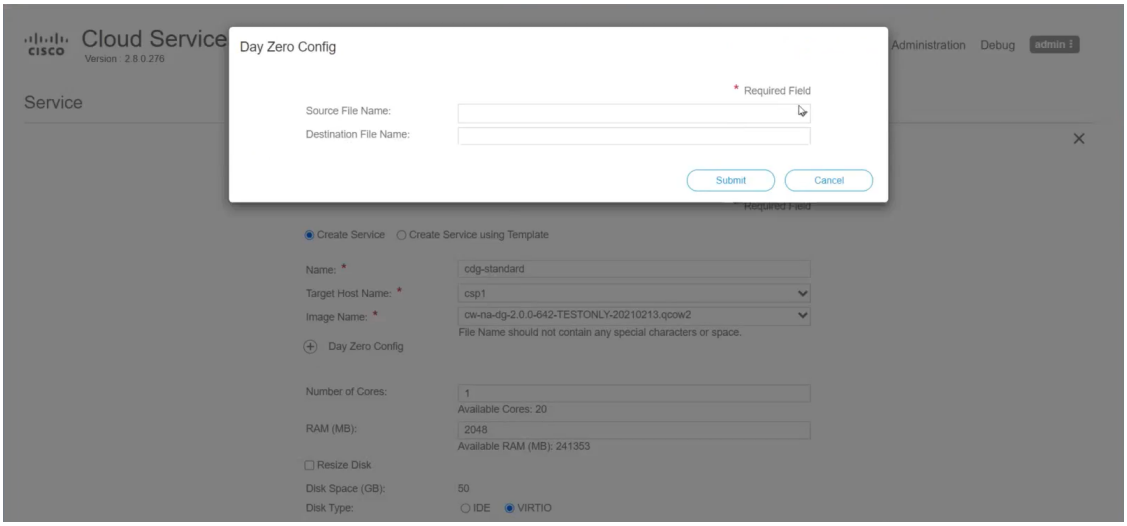
c) Check Create Service option.

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.



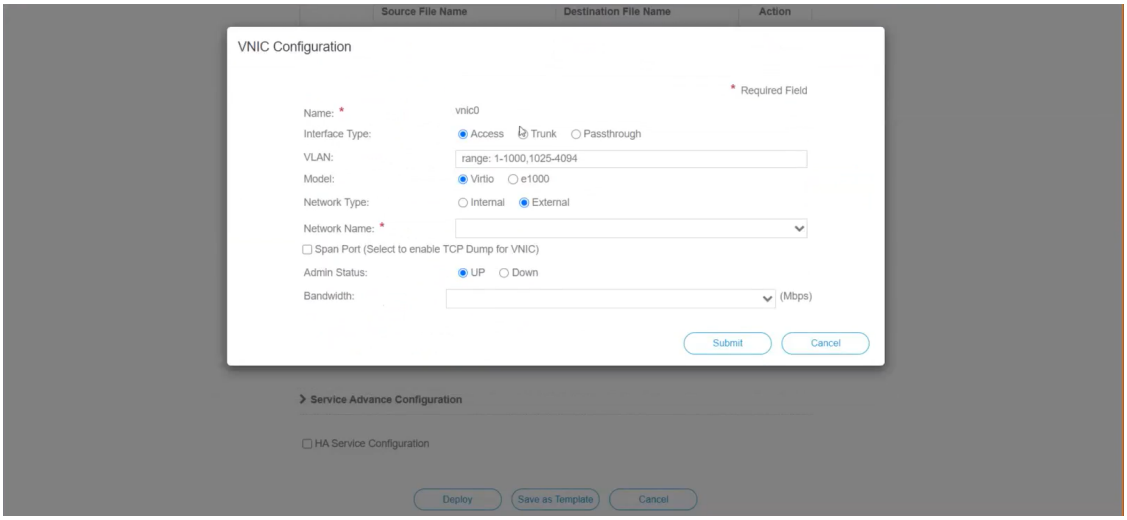
In the Day Zero Config dialog box, do the following:

1. From the Source File Name drop-down list, select a day0 configuration file i.e., the `ovf-env.xml` 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 "ovf-env.xml".
3. Click Submit.

f) Enter the values for the following fields:

Field	Description
Number of CPU Cores	Small: 8 Large: 12
RAM (MB)	Small: 49152 Large: 98304

g) Click VNIC.



In the VNIC Configuration dialog box, perform 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:

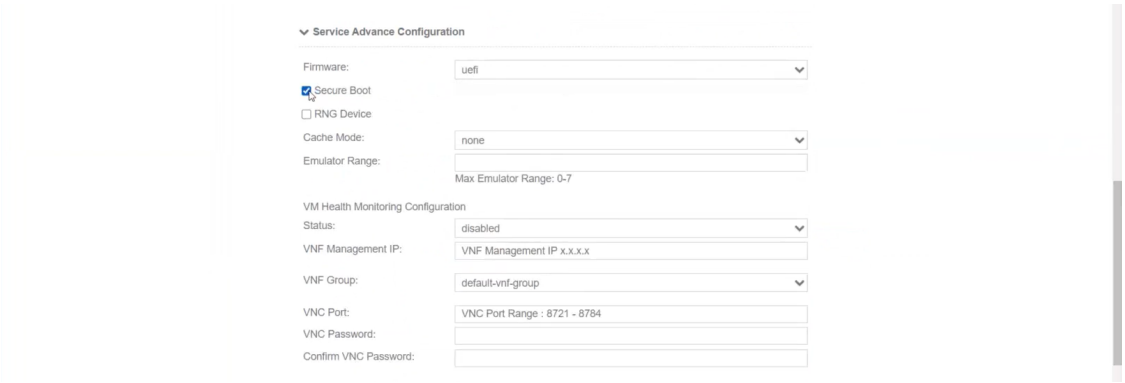
For VNIC...	Select...
vnic0	Eth0-1

For VNIC...	Select...
vnic1	Eth1-1

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:

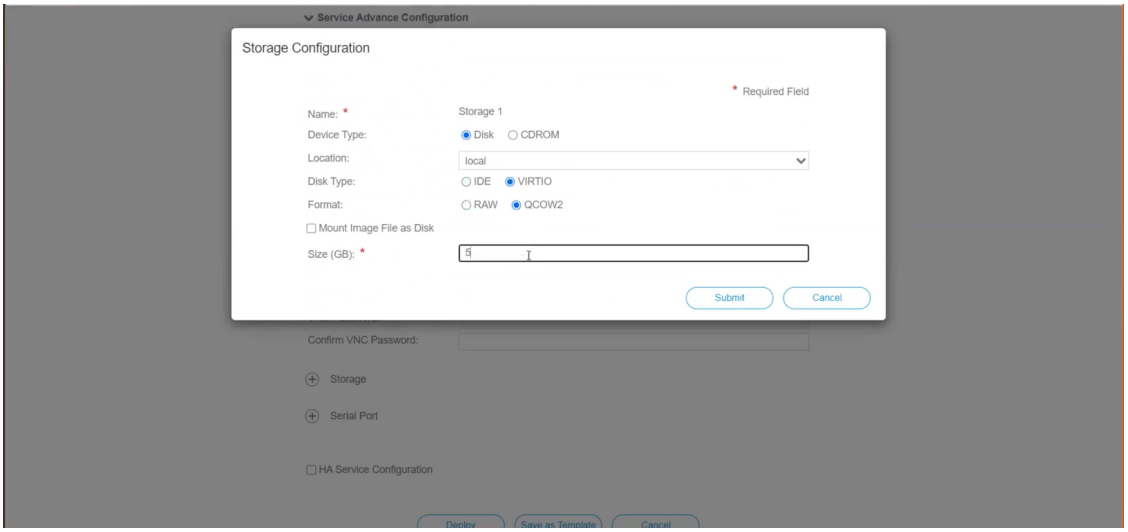
h) Expand the Service Advance Configuration and for Firmware, select uefi from the drop-down.
Check the Secure Boot checkbox.



i) Click Storage. In the Storage Configuration dialog box, fill the following fields:

Field	Description
Name	Name of the storage. This is specified by default.
Device Type	Select Disk.
Location	Select local.
Disk Type	Select VIRTIO.
Format	Select QCOW2.

Field	Description
Mount image file as disk?	Leave this unchecked.
Size (GB)	Enter the disk size (5 for Standard and 500 for Extended.)

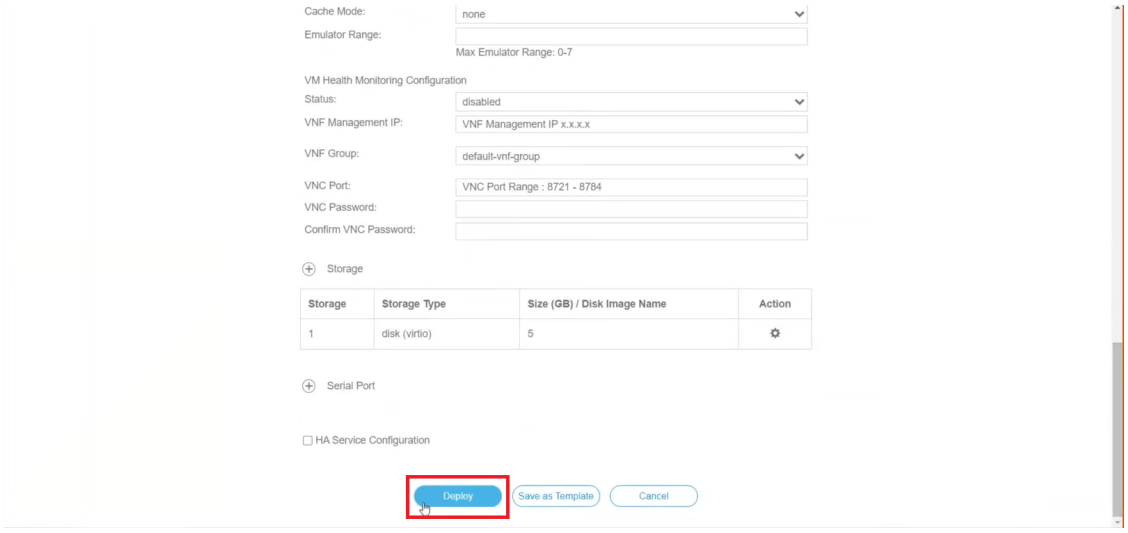


Note You have to configure 3 disks of different sizes:

- Disk 0: 10 GB
- Disk 1: 400 GB
- Disk 2: 50 GB

When you have completed the storage configuration, click Submit.

j) Click Deploy.



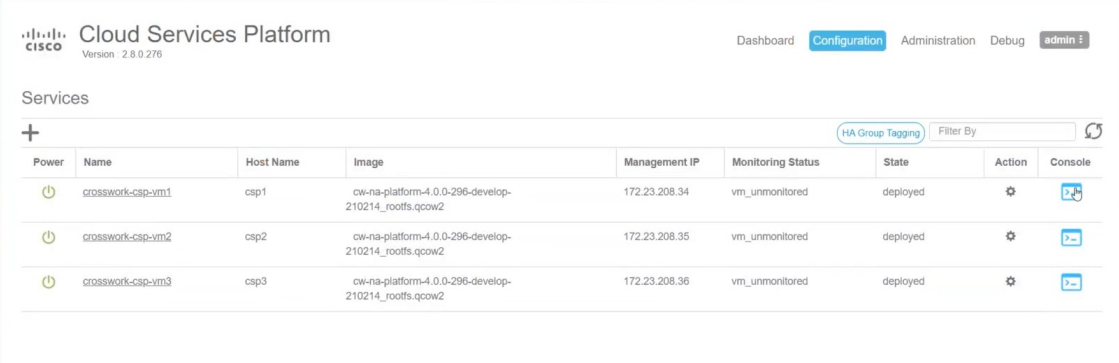
You will see a similar message once the service has successfully deployed. Click Close.

Step 4 Repeat Step 1 to Step 3 for each VM in the cluster.

Step 5 Deploy Cisco Crosswork VM:

a) Go to Configuration > Services.

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



What to do next

The time taken to create the cluster can vary based on the size of your deployment profile and the performance characteristics of your hardware. See Monitor the Installation, on page 48 to know how you can check the status of the installation.

Monitor the Installation

This section explains how to monitor and verify if the installation has completed successfully. As the installer builds and configures the cluster it will report progress. The installer will prompt you to accept the license agreement and then ask if you want to continue the install. After you confirm, the installation will progress and any errors will be logged in either `installer.log` or `installer_tf.log`.

The following is a list of critical steps in the process that you can watch for to be certain that things are progressing as expected:

1. The installer uploads the crosswork image file (OVA file in vCenter & QCOW2 file in CSP) to the data center.
2. The installer creates the VMs, and displays a success message (e.g. "Creation Complete") after each VM is created.

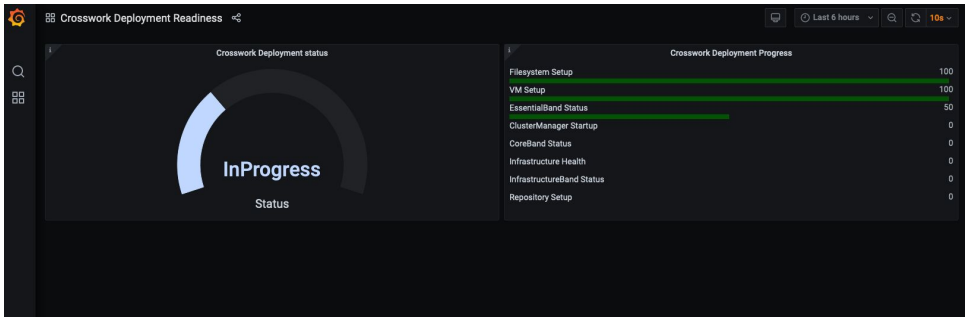
Note For VMware deployments, this activity can also be monitored from the vSphere UI.

3. After the VMs are created successfully, the Crosswork cluster will be created.
4. Once the cluster is created and becomes accessible, a success message (e.g. "CW Installer operation complete") will be displayed on the screen.

The time taken to create the VMs varies based on the size of your deployment profile and the performance characteristics of your hardware. You can wait for the installation to complete, or use any of the following methods to track the progress.

- Using browser accessible dashboard: While the cluster is being created, you can monitor the setup process from a browser accessible dashboard. The URL for this grafana dashboard (in the format `http://{VIP}:30603/grafana.monitoring`) is displayed once the installer completes. Please note that this URL is temporary and will be available only for a limited time (around 30 minutes). At the end of the deployment, the grafana dashboard will report a "Ready" status. If the URL is inaccessible, you can use the other methods described in this section to monitor the installation process.

  Figure 10: Crosswork Deployment Readiness



- Using the console: You can also check the progress from the console of one of the hybrid VMs by using SSH to the Virtual IP address, switching to super user, and running `kubectl get nodes` (to see if the nodes are ready) and `kubectl get pods` (to see the list of active running pods) commands. Repeat the `kubectl get pods` command until you see `robot-ui` in the list of active pods. At this point, you can try to access the Cisco Crosswork UI.

After the Cisco Crosswork UI becomes accessible, you can also monitor the status from the UI. For more information, see Log In to the GUI From a Browser, on page 49.

Failure Scenario

In the event of a failue scenario (listed below), contact the Cisco Customer Experience team and provide the `installer.log` and `installer_tf.log` files (there will be one per VM) for review:

- Installation is incomplete
- Installation is completed, but the VMs are not functional
- Installation is completed, but you are directed to check `firstboot.log` file

Log In to the GUI From a Browser

Once the cluster installer completes the operation, you can check if all the nodes are up and running in the cluster from the Cisco Crosswork UI. Perform the following steps to log in to the Cisco Crosswork GUI and and check the cluster health:

Note During installations on VMware vCenter, if the Cisco Crosswork GUI is not accessible, please access the host's console from the VMware UI to confirm if there was any problem in setting up the VM. When logging in, if you are directed to review the `firstboot.log` file, please check the file to determine the problem. If you are able to identify the error, rectify it and rerun the installer. If you require assistance, please contact the Cisco Customer Experience team.

Step 1 Launch one of the supported browsers (see Supported Web Browsers, on page 11).

Step 2 In the browser's address bar, enter:

`https://<Crosswork Management Network Virtual IP (IPv4)>:30603/`

or

`https://[<Crosswork Management Network Virtual IP (IPv6)>]:30603/`

Note Please note that the IPv6 address in the URL must be enclosed with brackets.

The Log In window opens.

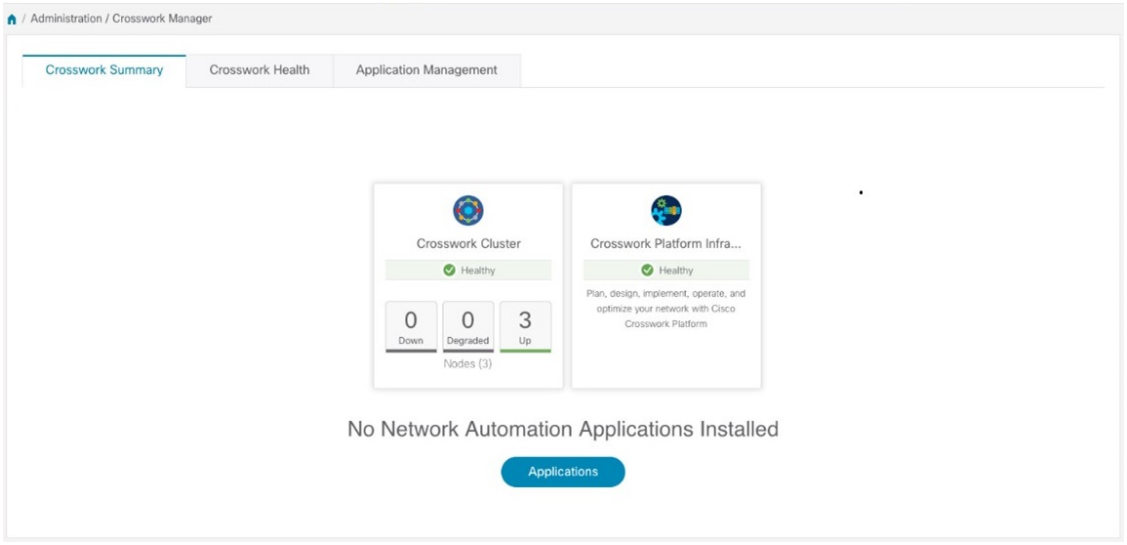
Note When you access the Cisco Crosswork for the first time, some browsers display a warning that the site is untrusted. When this happens, follow the prompts to add a security exception and download the self-signed certificate from the Cisco Crosswork server. After you add a security exception, the browser accepts the server as a trusted site in all future login attempts. If you want to use a CA signed certificate, see the "Manage Certificates" section in the Cisco Crosswork Infrastructure 4.0 and Applications Administrator Guide.

Step 3 Log in to the Cisco Crosswork as follows:

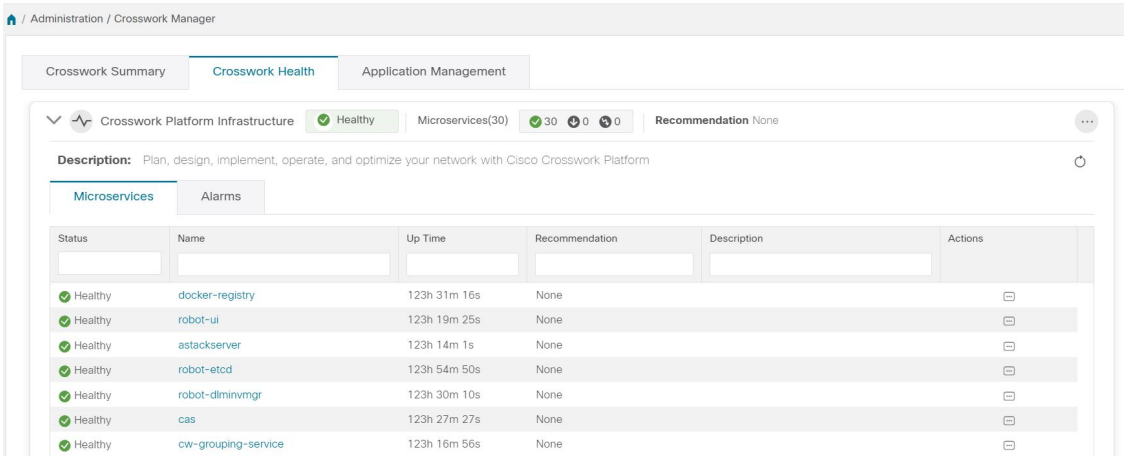
a) Enter the Cisco Crosswork administrator username admin and the default password admin.
b) Click Log In.
c) When prompted to change the administrator's default password, enter the new password in the fields provided and then click OK.

Note Use a strong password (8 character long, including upper & lower case letters, numbers and one special character).

The Crosswork Manager window is displayed.



Step 4 (Optional) Click on the Crosswork Health tab, and click on the Crosswork Infrastructure tile to view the health status of the microservices running on Cisco Crosswork.



Known Limitations

These following scenarios are the caveats for installing the Cisco Crosswork using the cluster installer tool.

- The vCenter host VMs defined must use the same network names (vSwitch) across all hosts in the DC.
- The vCenter storage folders, i.e. datastores organized under a virtual folder structure, are not supported currently. Please ensure that the datastores referenced are not grouped under a folder.
- When deploying a IPv6 cluster, the installer needs to run on an IPv6 enabled container/VM. This requires additionally configuring the docker daemon before running the installer, in either of the following methods:
  1. Linux hosts (ONLY): Run the docker container in host networking mode by adding the "–network host" flag to the docker run command line.

```
docker run --network host <remainder of docker run options>
```

2. Edit the docker daemon configuration (on linux in `/etc/docker/daemon.json`) by adding the following parameters.

Note Your VM's IPv6 address needs to have at least an /80 subnet assigned to it.

```
{

"ipv6": true,
"fixed-cidr-v6": "<the IPv6 subnet routed to your host, at least a /80>"

}
```

Restart the docker.

```
systemctl reload docker
```

- The cluster installer does not configure VMs with VLAN interfaces. As a result, CSP interfaces have to be untrunked with no tagged VLANs used for Management and Data networks. CSP allows non-VLAN tagged interfaces to be shared between multiple VMs, which allows for a more optimal interface assignment when deploying Crosswork and Crosswork Data Gateway VMs on the same CSP.
- Any VMs that are not created by the day 0 installer (for example, manually brought up VMs), cannot be changed either by the day 0 installer or via the Crosswork UI later. Similarly, VMs created via the Crosswork UI cannot be modified using the day 0 installer.
- Crosswork does not support dual stack configurations, and all addresses for the environment must be either IPv4 or IPv6. However, vCenter UI provides a service where a user accessing via IPv4 can upload images to the IPv6 ESXi host. Cluster installer cannot use this service. Follow either of the following workarounds for IPv6 ESXi hosts:
  1. Upload the OVA template image manually, via the GUI and convert it to template.
  2. Run the cluster installer from an IPv6 enabled machine. To do this, configure the docker daemon to map an IPv6 address into the docked container.
- Centos/RHEL hosts, by default, enforce a strict SELinux policy which does not allow the installer container to read from or write to the mounted data volume. On such hosts, run the docker volume command with the Z option as shown below:

```
docker run --rm -it -v `pwd`:/data:Z <remainder of docker options>
```

Troubleshoot the Cluster

By default, the installer will display progress data on the command line. The install log is also copied into the `/data` directory, which is fundamental in identifying the problems.

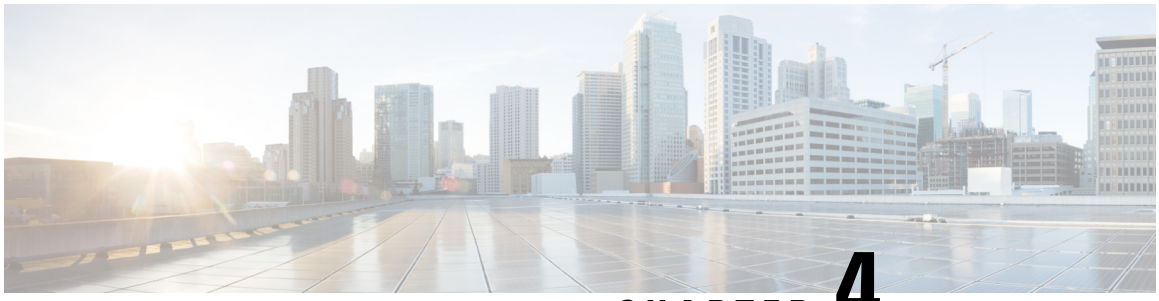
Scenario	Possible Resolution
Missing or invalid parameters	The installer will provide a clue as to the issue, however in case of errors in the manfiest file HCL syntax these can be misguiding. If observing "Type errors", please check the formatting of the configuration manifest. The manifest file can also be passed as a simple JSON file. Use the following converter to validate/convert: https://www.hcl2json.com/
Image upload takes a long time and upload interruption.	The image upload duration depends on the link and datastore performance and can be expected to take around 10 minutes or more. It is best NOT to interrupt the process, which will timeout naturally. However, if an upload is interrupted, the user will need to manually remove the partially uploaded image file from vCenter via the vSphere UI.
vCenter authorization	The vCenter user needs to have authorization to perform the actions as described in the Installation Requirements chapter of this document.
Floating VIP address is not reachable	The VRRP protocol requires unique router_id advertisments to be present on the network segment. By default, Crosswork uses the ID 169 on the management and ID 170 on the data network segments. If a conflict arises, a symptom is that the VIP address is not reachable. Remove the conflicting VRRP router machines or use a different network.
Crosswork VM is not allowing to login	The password specified was not strong enough. Change the configuration manfiest and redeploy.
Error conditions such as: Error: Error locking state: Error acquiring the state lock: resource temporarily unavailable Error: error fetching virtual machine: vm not found Error: Invalid index	These errors are common when re-running the installer after an initial run which was interrupted (Control C, or TCP timeout, etc). Remediation steps are: 1. Run the clean operation (`./cw-installer.sh clean -m <your manifest here>`) OR remove the VM files manually from the vCenter. 2. Remove the state file (`rm /data/crosswork-cluster.tfstate`) and retry.
Deployment fails with: Failed to validate Crosswork cluster initialization.	The clusters' seed VM is either unreachable or one or more of the cluster VMs have failed to get properly configured. 1. Check if the VM is reachable, and collect logs from `/var/log/firstBoot.log` and `/var/log/vm_setup.log` 2. Check status of the other cluster nodes.

Scenario	Possible Resolution

The VMs are deployed but the Crosswork cluster is not being formed.	A successful deployment will allow the operator logging in to the VIP or any cluster IP address to run the following command to get the status of the cluster:
	`sudo kubectl get nodes`
	A healthy output for a 3-node cluster would be:
	`NAME STATUS ROLES AGE VERSION`
	`172-25-87-2-hybrid.cisco.com Ready master 41d v1.16.4`
	`172-25-87-3-hybrid.cisco.com Ready master 41d v1.16.4`
	`172-25-87-4-hybrid.cisco.com Ready master 41d v1.16.4`
	In case of a different output, collect the following logs: `/var/log/firstBoot.log` and `/var/log/vm_setup.log`
	In addition, for any cluster nodes not displaying the Ready state, it is useful to collect:
	`sudo kubectl describe node <name of node>`

The following error is displayed while uploading the image: govc: The provided network mapping between OVF networks and the system network is not supported by any host.	The Dswitch on the vCenter is misconfigured. Please check that it is operational and mapped to the ESXi hosts.
The VMs take a long time to deploy	The disk load on the vCenter plays a major role in cloning VM. To ease loaded systems, it is possible to run the VM install operations in a serialized manner. On higher performance systems, run the deployment in parallel by passing the [-p] flag.
VMs deploy but install fails with Error: timeout waiting for an available IP address	Most likely cause would be an issue in the VM parameters provided or network reachability. Enter the VM host via the vCenter console. and review and collect the following logs: `/var/log/firstBoot.log` and `/var/log/vm_setup.log`
On cluster node failure, the VIP is not transferred to the remaining nodes	Ensure that switch or the vCenter Dswitch connected the VMs allows IP address movement (Allow Forged Transmits in vCenter). For more information, see Data Center Requirements, on page 5.

Scenario	Possible Resolution
When deploying on a vCenter, the following error is displayed towards the end of the VM bringup: Error processing disk changes post-clone: disk.0: ServerFaultCode: NoPermission: RESOURCE (vm-14501:2000), ACTION (queryAssociatedProfile): RESOURCE (vm-14501), ACTION (PolicyIDByVirtualDisk)	Enable Profile-driven storage. Query permissions for the vCenter user at the root level (i.e. for all resources) of the vCenter.
Installer reports plan to add more resources than the current numbr of VMs	Other than the Crosswork cluster VMs, the installer tracks a couple of other meta-resources. Thus when doing an installation of, say a 3-VM cluster, the installer may report a "plan" to add more resources than the number of VMs.
On running or cleaning, installer reports Error: cannot locate virtual machine with UUID "xxxxxxx": virtual machine with UUID "xxxxxxxx" not found	To resolve, remove the `/data/crosswork-cluster.tfstate` file. The installer uses the `tfstate` file stored as `/data/crosswork-cluster.tfstate` to maintain the state of the VMs it has operated upon. If a VM is removed outside of the installer, e.g. via the vCenter UI, this state is out of sync.



CHAPTER 4

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, on page 12.
2. Install Cisco Crosswork Data Gateway on your preferred platform:

VMware	Install Cisco Crosswork Data Gateway Using vCenter vSphere Client, on page 66
	Install Cisco Crosswork Data Gateway Via OVF Tool, on page 71
Cisco CSP	Install Cisco Crosswork Data Gateway on Cisco CSP, on page 73

3. Set timezone on Cisco Crosswork Data Gateway VM. See Configure Timezone, on page 83.

4. Verify Cisco Crosswork Data Gateway enrollment with Cisco Crosswork. See Cisco Crosswork Data Gateway Authentication and Enrollment, on page 84.

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 17: 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 85. • 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 90.
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 17: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 58.

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.

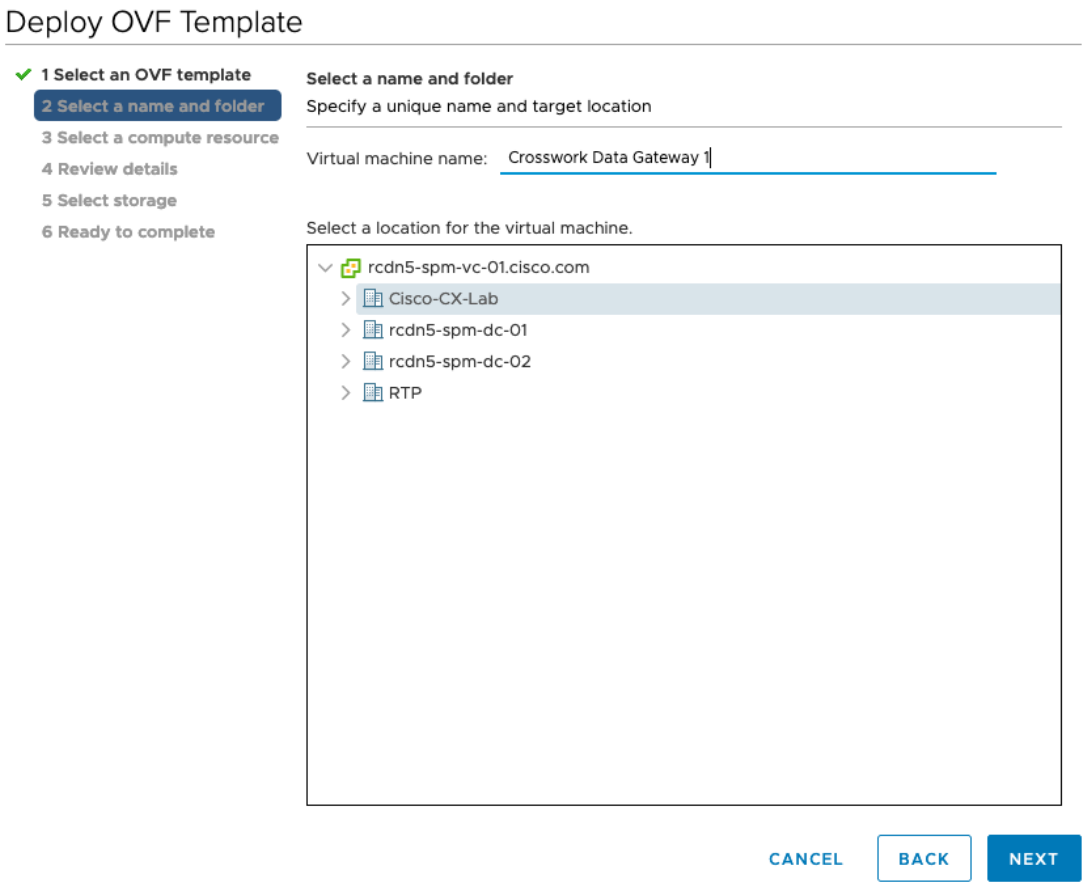
a) Click Browse to navigate to the location where you downloaded the OVA image file and select it.

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.

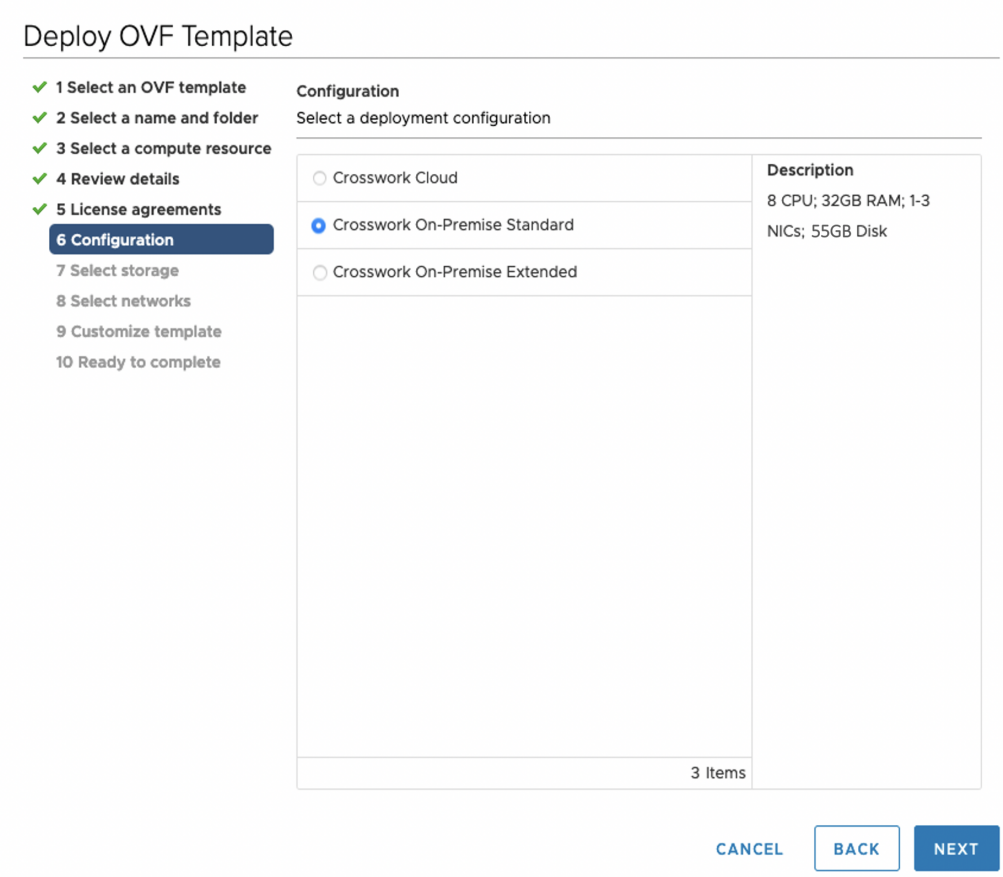
Take a moment to review the OVF template you are deploying.

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.



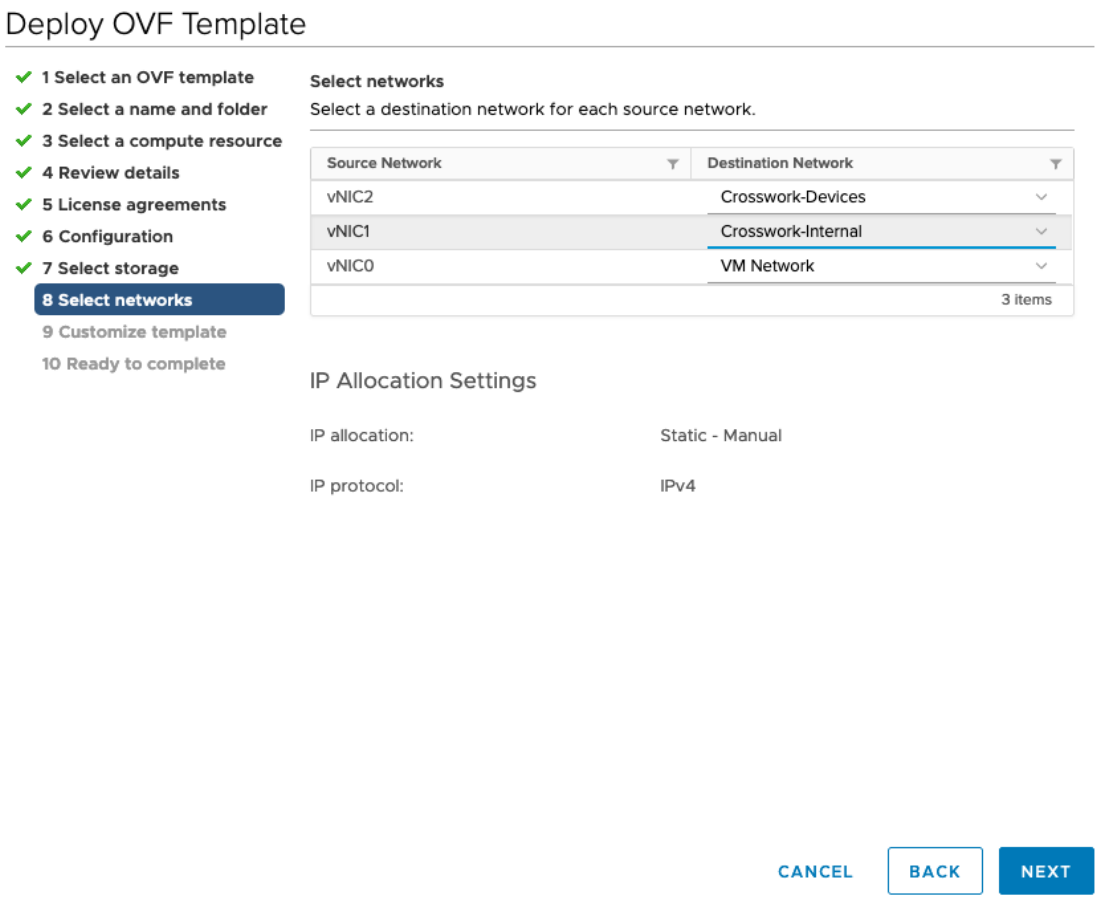
Step 9 Click Next to go to 7 Select storage, as shown in the following figure.

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

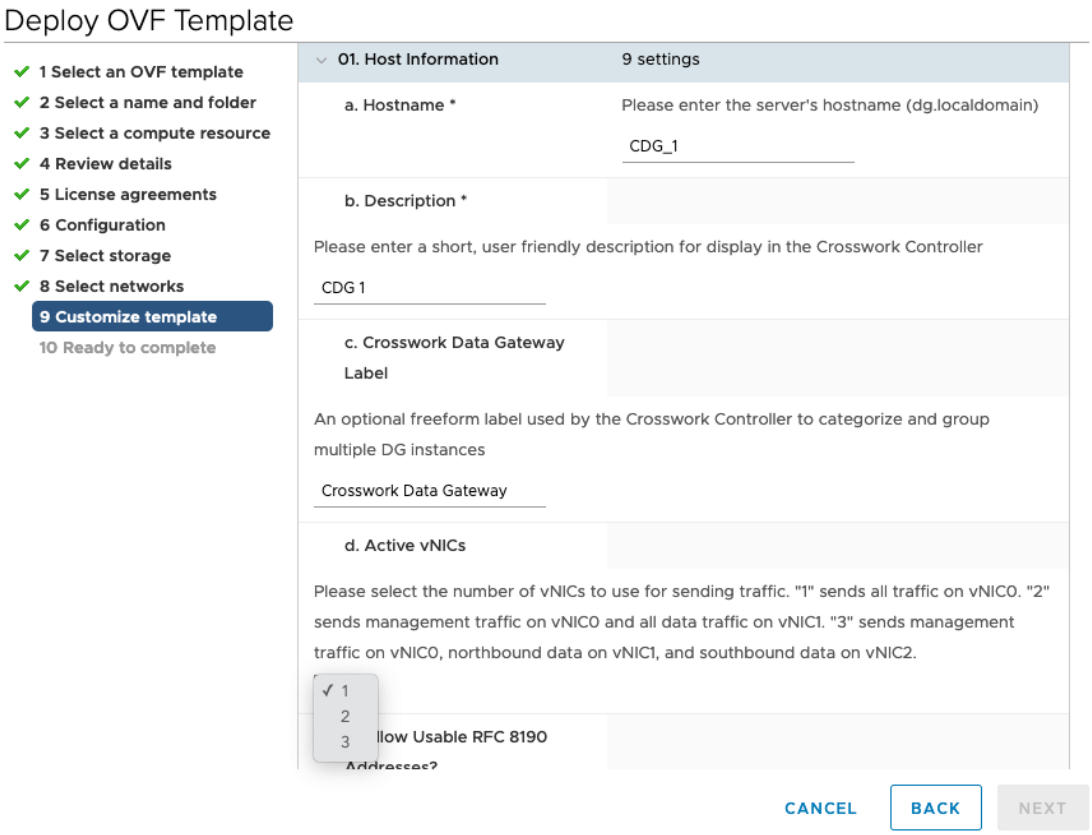
b) From the Datastores table, choose the datastore you want to use and review its properties to ensure there is enough available storage.

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 17: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 58.



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.

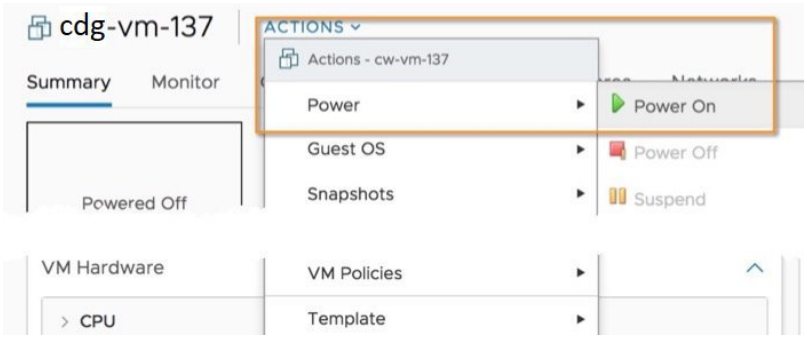
Step 13 Wait for the deployment to finish before continuing. To check the deployment status:

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 17: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 58.

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 17: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 58.

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.

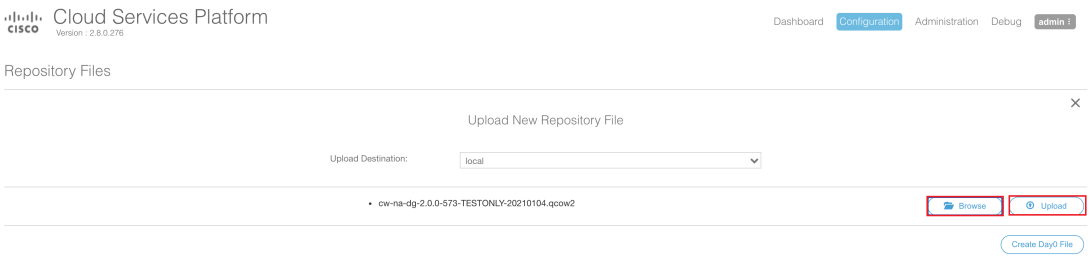
b) Go to Configuration > Repository.

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.

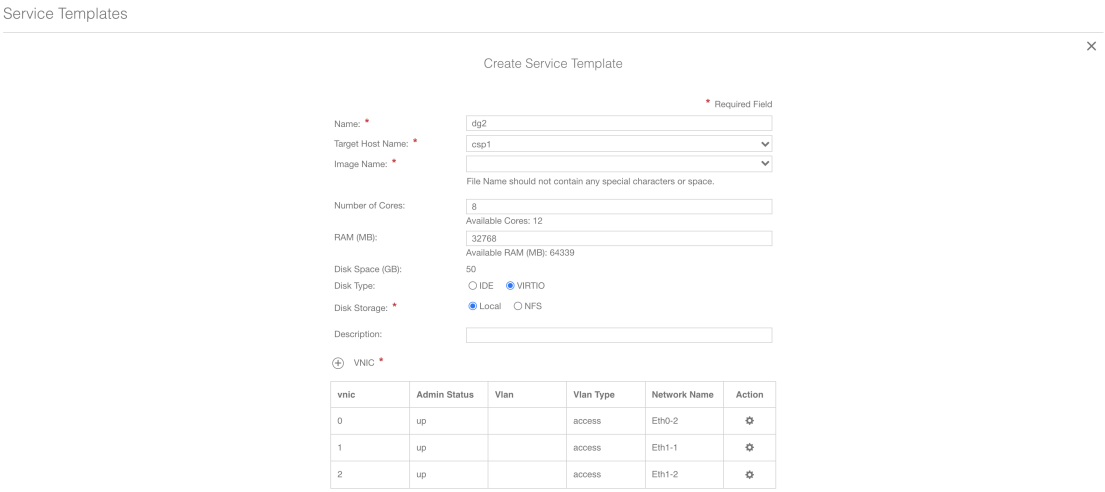
Step 5 Create Crosswork Data Gateway VM:

a) Go to Configuration > Services.

b) On the Service page, click ⊞ button.

c) Check Create Service option.

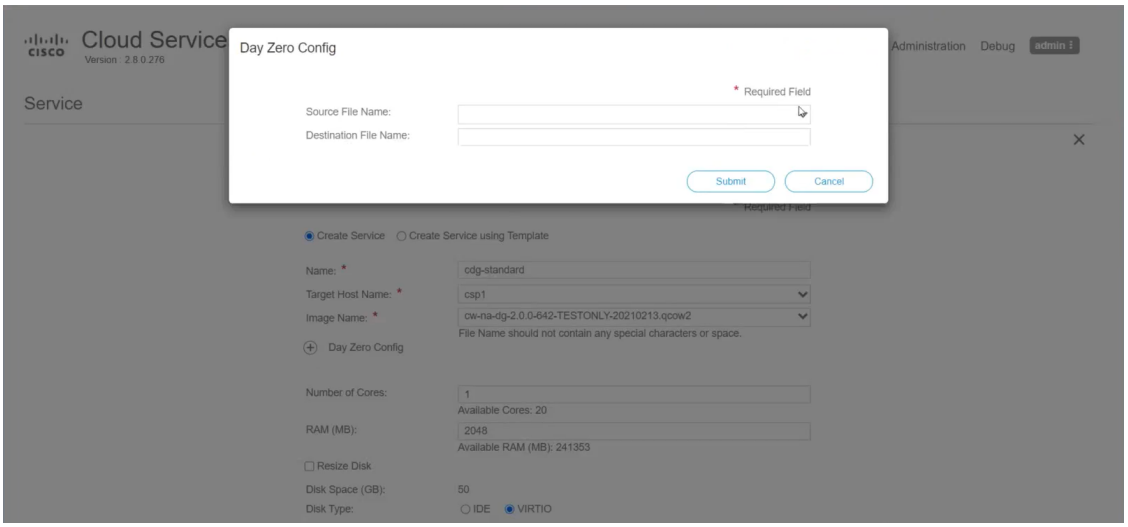
The Create Service Template page is displayed.



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.



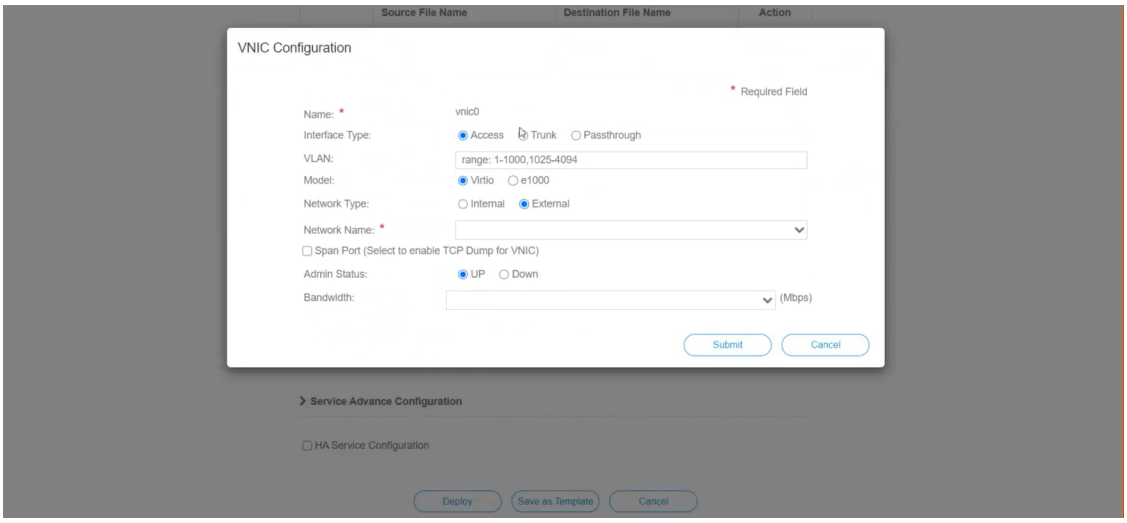
In the Day Zero Config dialog box, do the following:

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:

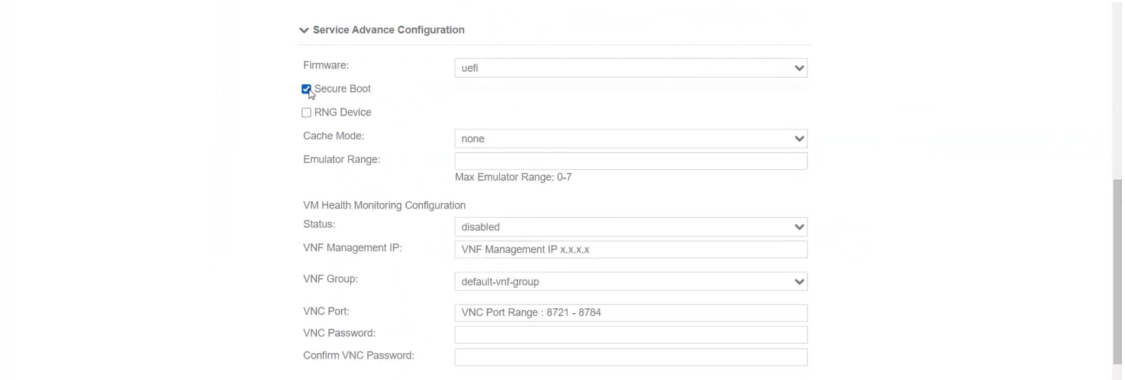
For VNIC...	Select...
vnic0	Eth0-1
vnic1	Eth1-1
vnic2	Eth1-2

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:

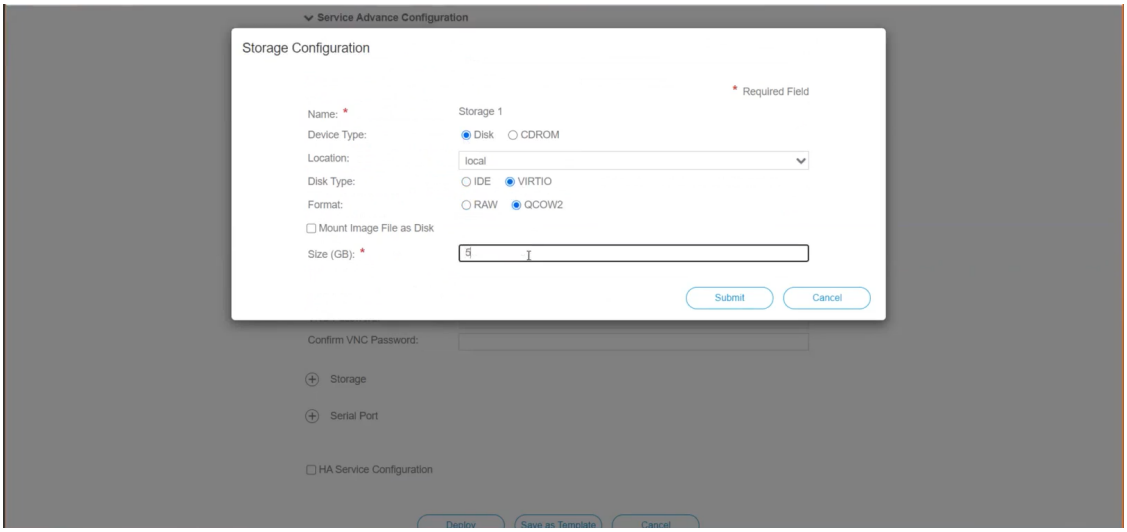
h) Expand the Service Advance Configuration and for Firmware, select uefi from the drop-down.

Check the Secure Boot checkbox.



i) Click Storage.

In the Storage Configuration dialog box, do the following:

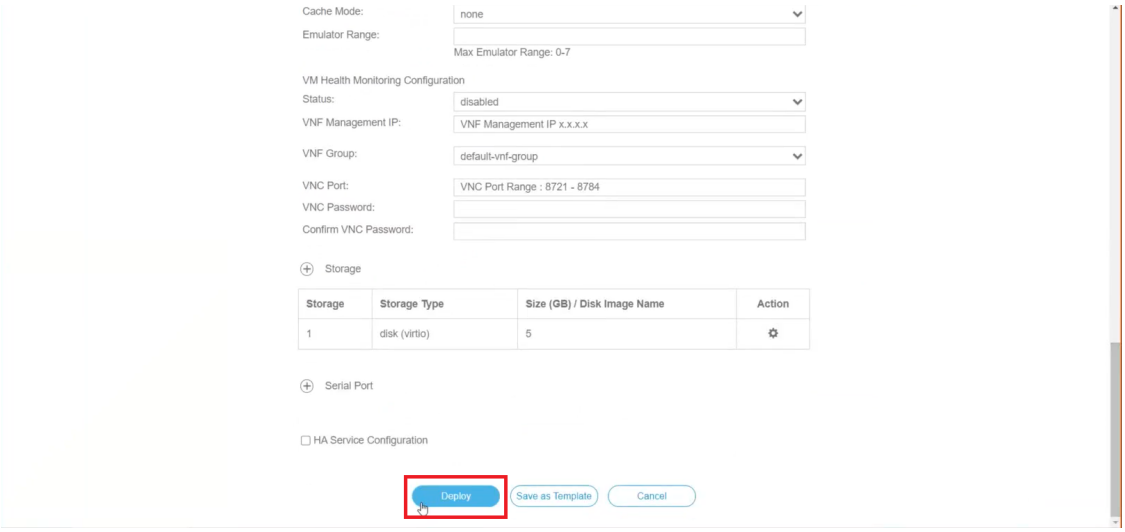


Field	Description
Name	Name of the storage. This is specified by default.

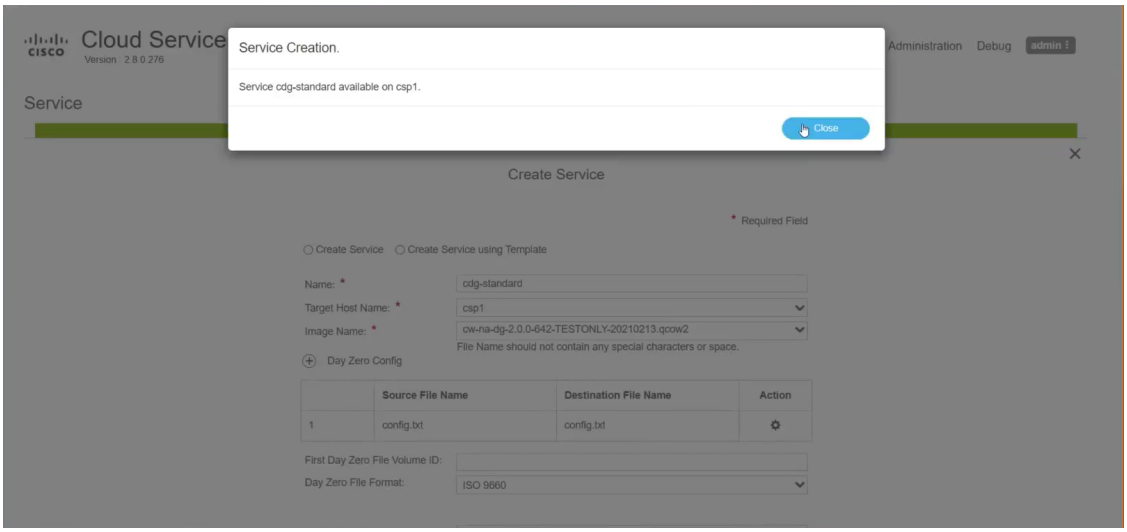
Field	Description
Device Type	Select Disk.
Location	Select local.
Disk Type	Select VIRTIO.
Format	Select QCOW2.
Mount image file as disk?	Leave this unchecked.
Size (GB)	Enter the disk size (5 for Standard and 500 for Extended.)

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

j) Click Deploy.



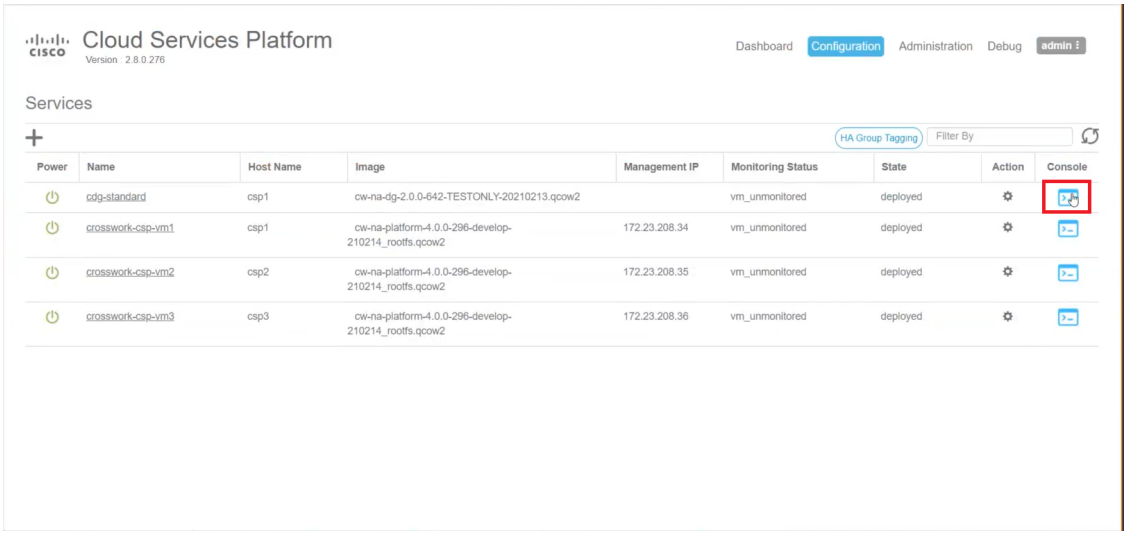
You will see a similar message once the service has successfully deployed. Click Close.



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 82
- Configure Timezone, on page 83
- Log Out, on page 84

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

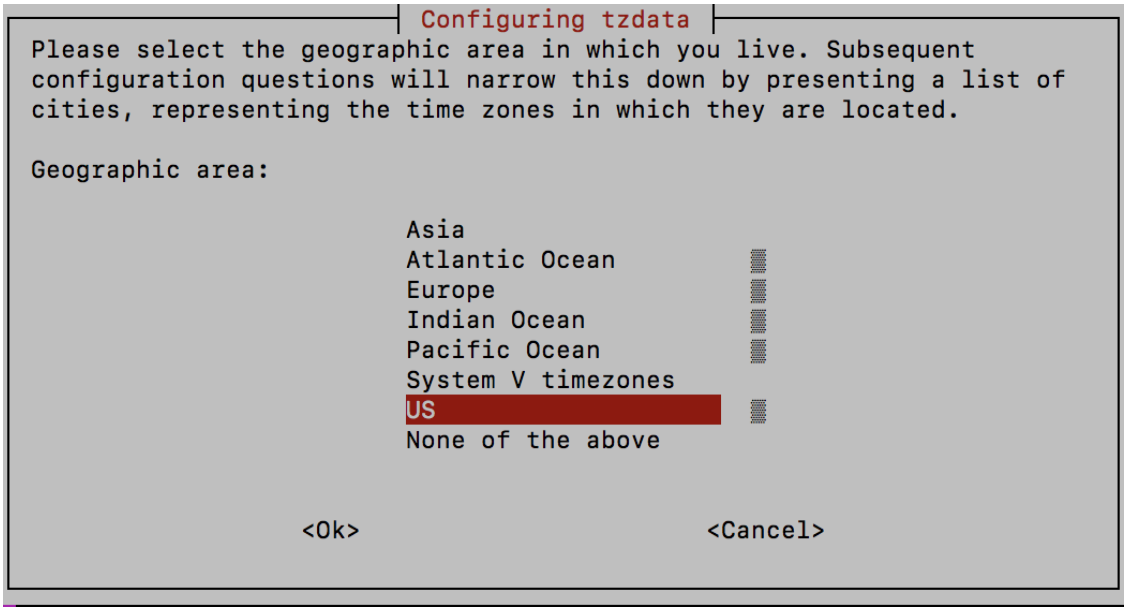
The Crosswork Data Gateway first launches with default timezone as UTC.

Follow the steps to configure timezone:

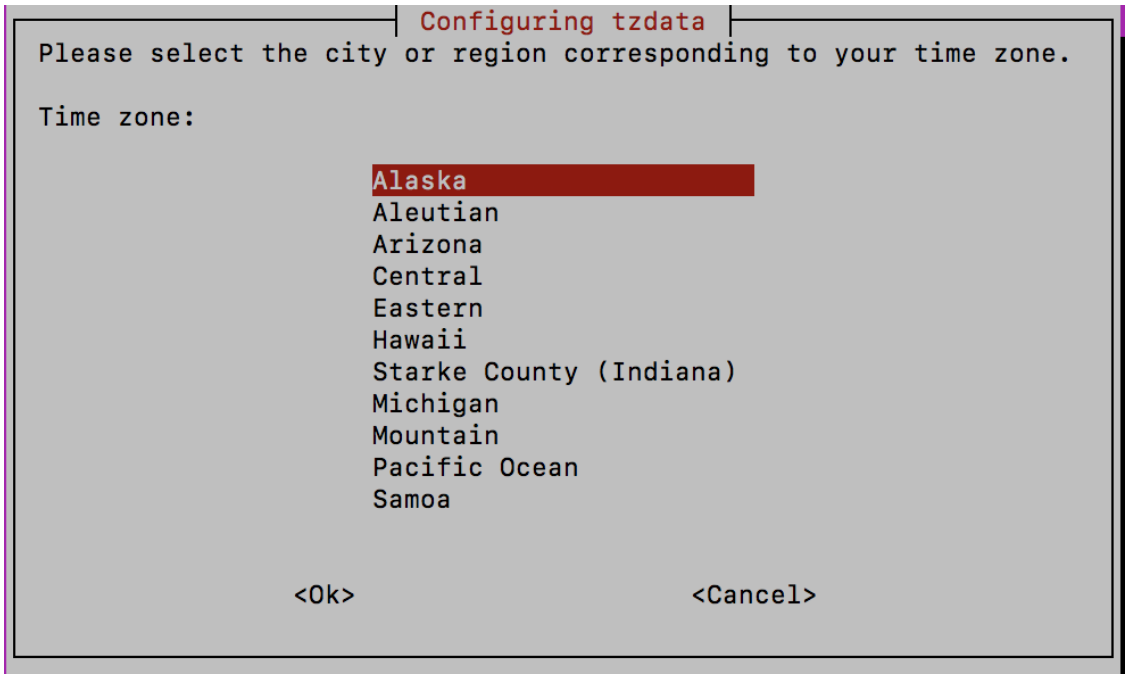
Step 1 In Crosswork Data Gateway VM interactive menu, select Change Current System Settings.

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

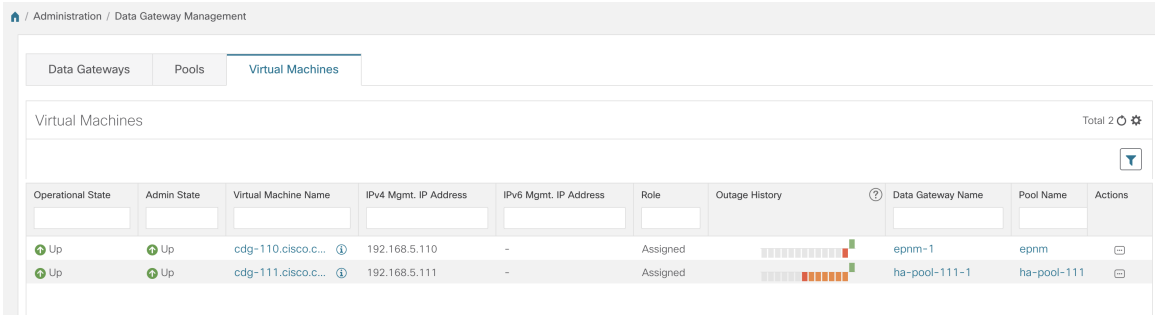
To log out, select option l Logout from the Main Menu and press Enter or click OK.

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:

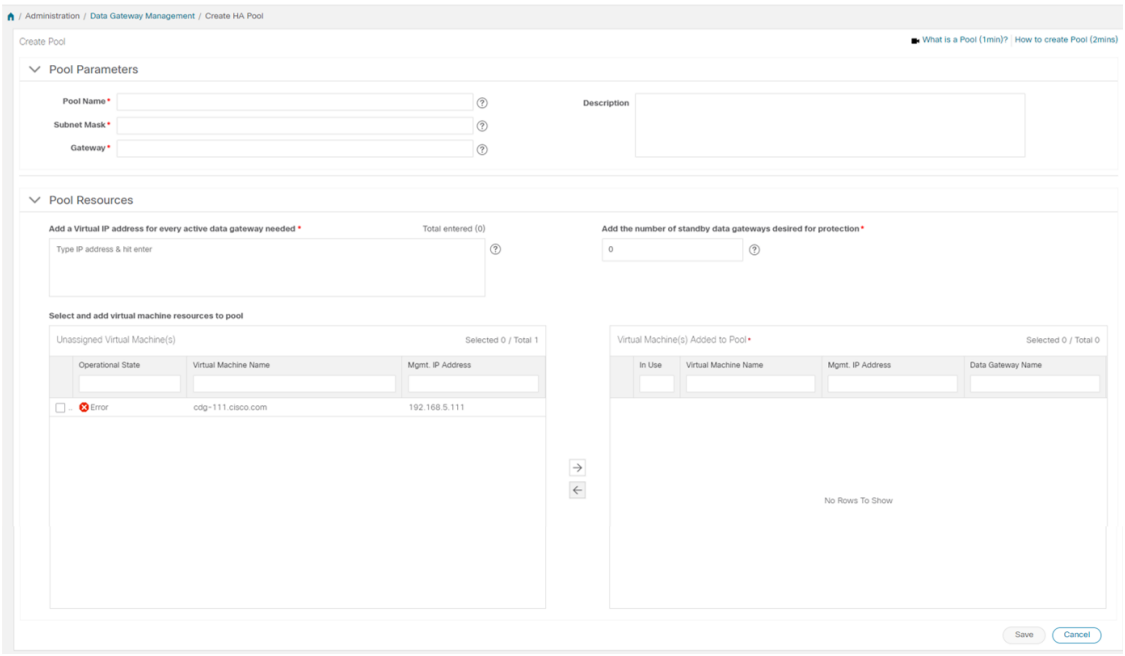
Before you begin

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.

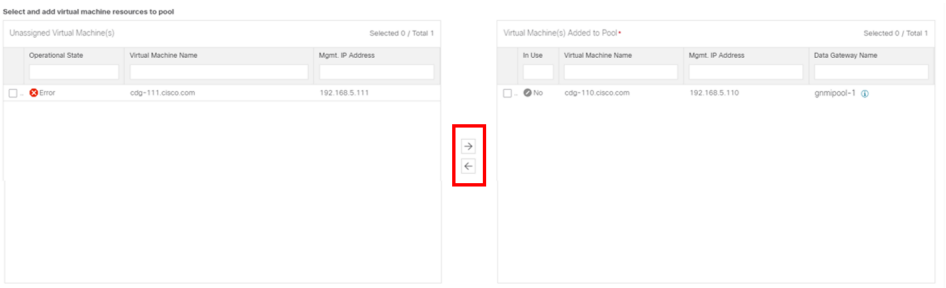
- Number of standby Cisco Crosswork Data Gateways desired for protection. Entering a value greater than 0 in this field enables high availability for the pool.

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 18: 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.

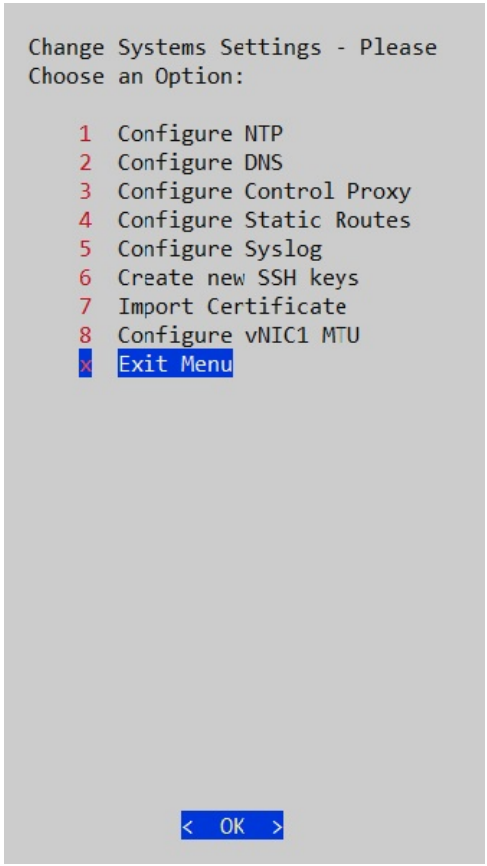
Import Controller Signing Certificate File

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.

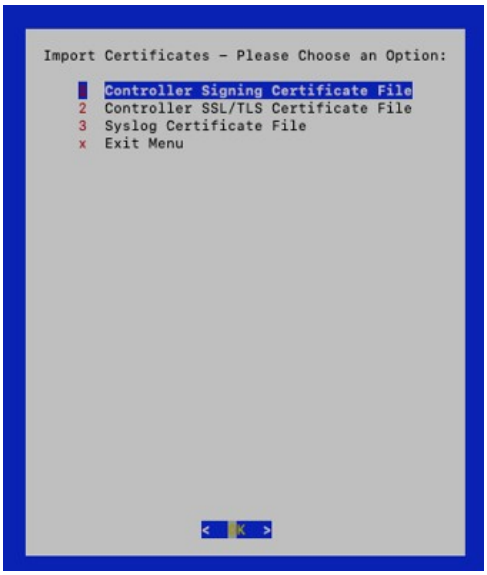
Step 1 From the Cisco Crosswork Data Gateway VM's interactive menu, select 3 Change Current System Settings.

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).

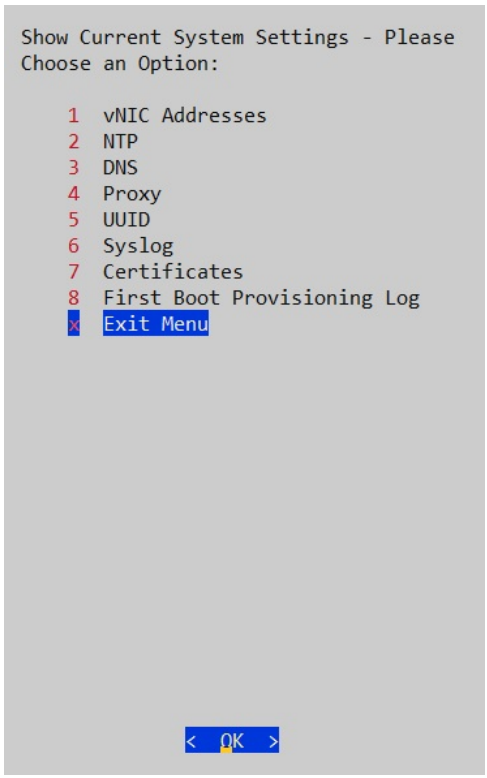
The certificate file is imported.

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.

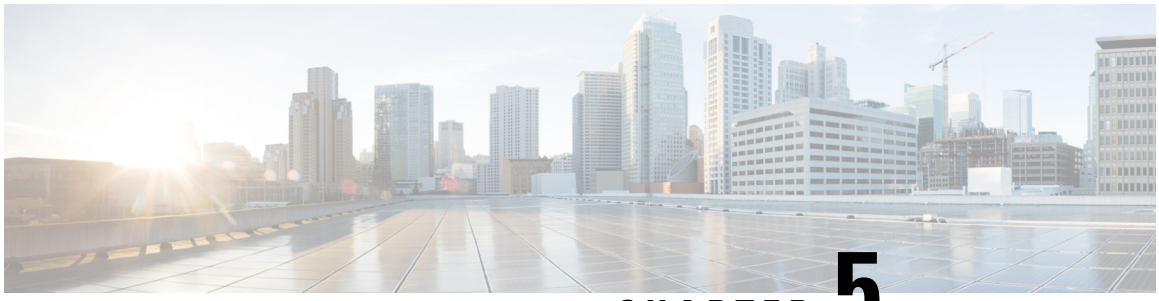
Step 1 From the Crosswork Data Gateway VM's interactive menu, select 2 Show System Settings.



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.



CHAPTER 5

Install Crosswork Applications

This section contains the following topics:

Install Crosswork Applications

This section explains how to install a Cisco Crosswork application from the Cisco Crosswork UI.

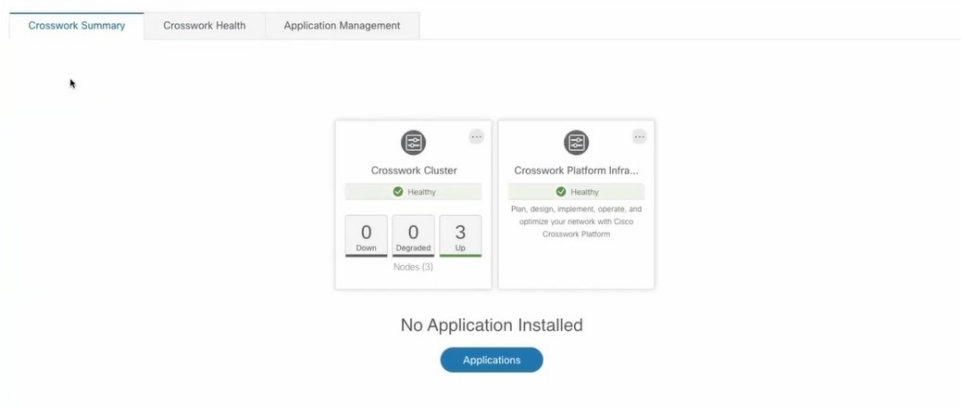
Note

- Every crosswork application is packaged in a particular format unique to Crosswork known as CAPP (Cisco APPlication). The applications CAPP files are downloaded from cisco.com to a machine reachable from the Cisco Crosswork server, and added to the Crosswork UI where it can be installed. You need to have the credentials that will allow you to copy the CAPP files from that machine.
- During installation, Cisco Crosswork will create a special administrative ID (virtual machine (VM) administrator, with the username cw-admin, and the default password cw-admin). The administrative username is reserved and cannot be changed. The first time you log in using this administrative ID, you will be prompted to change the password. Data center administrators use this ID to log in to and troubleshoot the Crosswork application VM. You will use it to verify that the VM has been properly set up.

Step 1 Download or copy the CAPP files from cisco.com to a server that can be reached from the CW server.

Step 2 In the Cisco Crosswork homepage, click on Administration > Crosswork Management. The Crosswork Summary page is displayed with Crosswork Cluster and Crosswork Platform Infrastructure tiles.

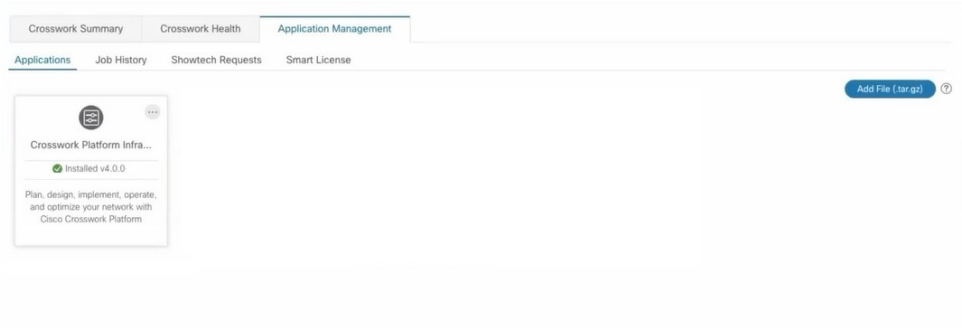
Install Crosswork Applications



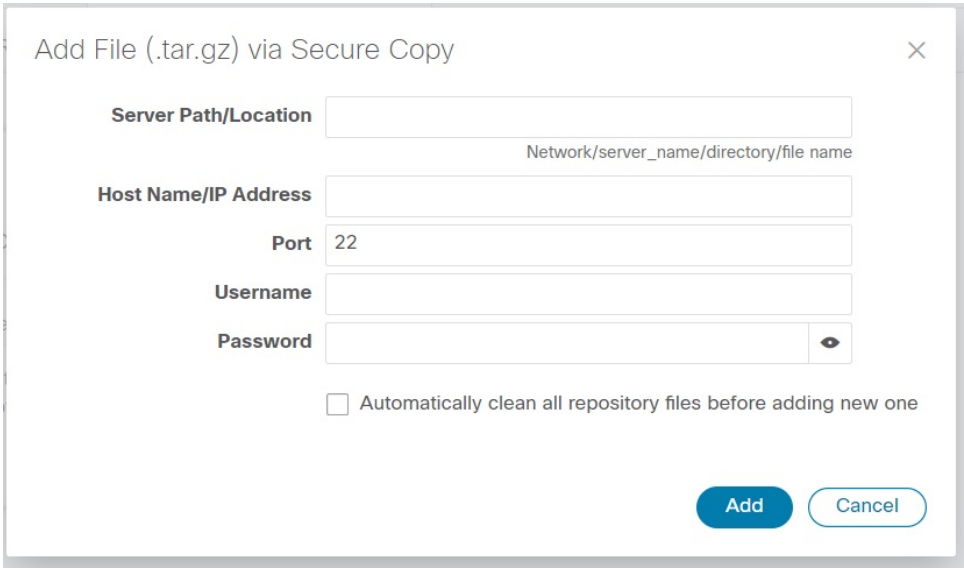
You can click on the tiles to get more information.

Step 3 To install an application, click on Applications button. Alternately, click on the Application Management tab.

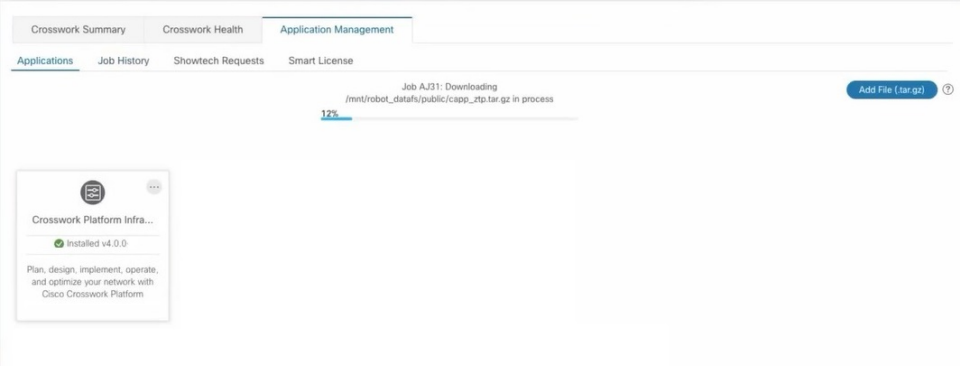
Step 4 In the Application Management screen, select the Applications tab, and click on the Add File (.tar.gz) option to add a CAPP file.



Step 5 In the Add File dialog box, enter the relevant information and click Add.

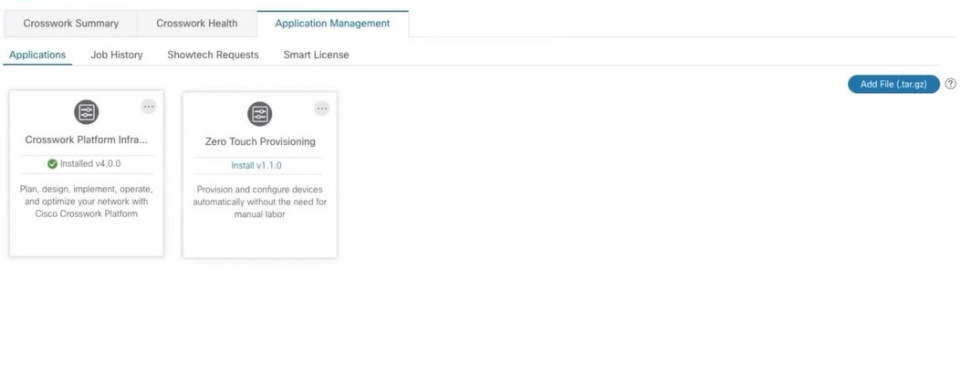


The add operation progress is displayed on the Applications screen.

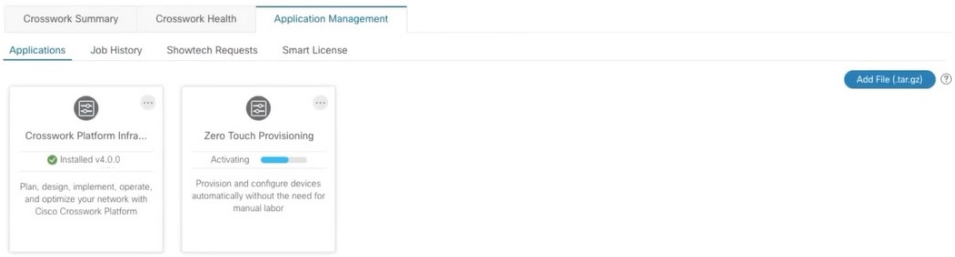


Note You can add a new CAPP file while another CAPP file is being added. The system will add each file in sequence, and the current CAPP file that is added will be displayed on the screen.

Step 6 The newly added application (CAPP file) is displayed as a tile on the Applications screen. To install, click on the Install prompt on the tile. You can also click ··· on the tile, and select the Install option from the drop down list.



The progress of installation is displayed on the application tile. You can also view the installation progress in the Job History tab.

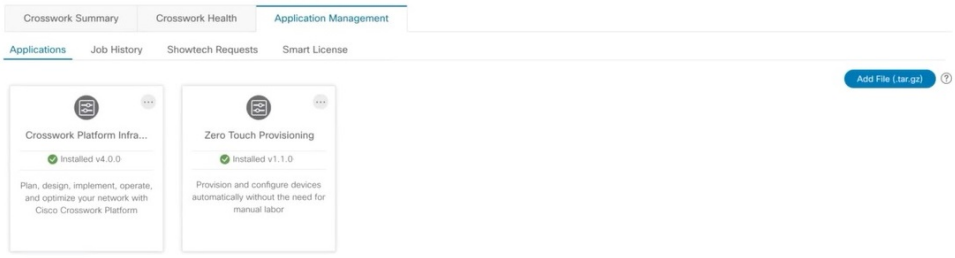


Note The first-time installation also activates a CAPP file.

The application is now installed. You can observe the change in the application tile icon. Once an application is installed, all the related-resources, UI screens and menu options are dynamically loaded in the Crosswork UI.

Install Crosswork Applications

You can initiate multiple installs by clicking the install option in the application tiles. The system will install the CAPP files in sequence, and the progress of current CAPP being will be displayed on the screen. The applications are that are in queue to be installed will have the status as "Install pending"

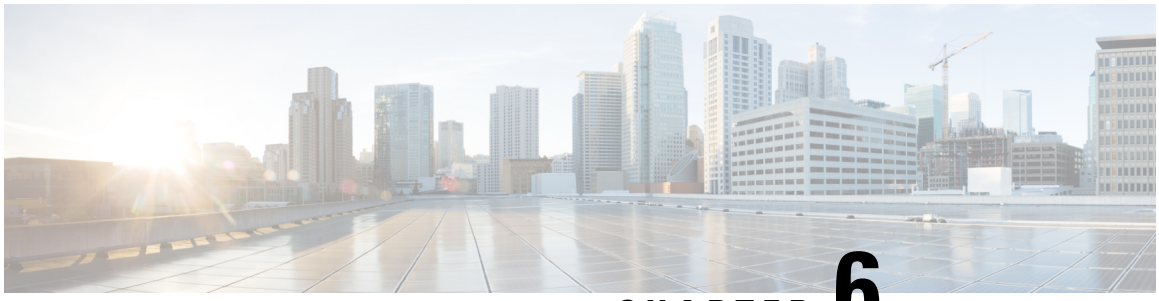


Note Once an application is installed, the 90-day evaluation period will automatically start. You can register the application with your Cisco Smart Account in the the Smart License tab.

Step 7 The first-time installation also activates a CAPP file. However, if the activation fails after a successful installation, you can manually activate the application. To manually activate an applicable, click the ··· on the aplication tile, and select Activate.

Step 8 Repeat steps 6 to 8 for adding more applications.

Step 9 (Optional) Click ··· on the application tile, and select the View Details option to view details of the installed application.



CHAPTER 6

Upgrade

This section contains the following topics:

Upgrade Cisco Crosswork Applications

This section explains how to upgrade the Crosswork Applications from the Crosswork GUI.

Before you begin, ensure that you:

- Take a backup of your data (using the backup/restore functionality) before any critical upgrade.
- Download the latest version of the Crosswork Application file (CAPP) from cisco.com to your local machine.

Note Crosswork does not support the downgrade operation of a CAPP file. However, if you want to go back to an older application version, you can uninstall the application and install the older version of the application. In case of a downgrade, you are advised to take a backup of your data prior to the operation.

Step 1 Click on Administration > Crosswork Management, and select the Application Management tab.

The Crosswork Platform Infrastructure and any applications that are added are displayed here as tiles.

Step 2 Click on the Add File (.tar.gz) option to add the application CAPP file that you had downloaded.

Step 3 In the Add File dialog box, enter the relevant information and click Add.

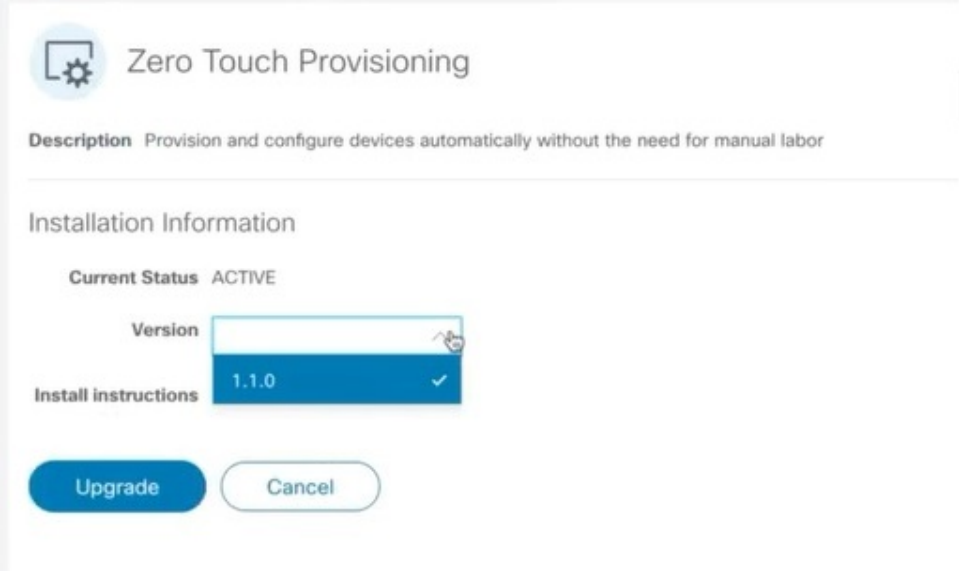
Once the CAPP file is added, you can observe the existing applcation tile (in this example, Zero Touch Provisioning) displaying an upgrade prompt.

Step 4 To upgrade, click the Upgrade prompt and the new version of the application is installed.

The upgrade progress is displayed on the application tile.

Step 5 Alternately, you can click (…) on the tile, and select the Upgrade option from the drop down list.

In the Upgrade screen, select the new version that you want to upgrade to, and click Upgrade.



Step 6 (Optional) Click on Job History to see the progress of the upgrade operation.

Note During an upgrade operation, typically only the components that have changed between the existing CAPP file and the new CAPP file are installed, as the new version may continue to use the most of the resources of the older version. This ensures a quick operation that happens without disruption to the current system and session.

Note During an upgrade, the application that is being updated will be unavailable until the update is completed. During this time, any other users using the application will be notified via an alarm about the upgrade.

Migrate to Cisco Crosswork 4.0

Use Cisco Crosswork backup functionality to migrate your data from earlier versions of Cisco Crosswork to version 4.0. All you need is a backup file from the earlier version.

When migrating your data to Cisco Crosswork 4.0, observe these guidelines:

- The migration shell script supports data migration to Cisco Crosswork 4.0 from Cisco Crosswork Change Automation and Health Insights 3.2.2 or Cisco Crosswork Optimization Engine 1.2.1 only. You can’t use it to migrate from any version of Cisco Crosswork Network Controller.
- You also can't migrate both Change Automation and Health Insights 3.2.2 and Optimization Engine 1.2.1. These are two different backups, and can't be merged.
- The script doesn’t support in-place upgrade to Cisco Crosswork version 4.0. First, install Cisco Crosswork version 4.0. You must also install the current version of any Cisco Crosswork applications you use. For example: Migrating Cisco Crosswork Optimization Engine 1.2.1 to Cisco Crosswork 4.0 requires that you first have Cisco Optimization Engine 2.0 installed on the 4.0 cluster. You can then migrate your data to it.

Before you begin, ensure that:

- You have the cw-admin password for Cisco Crosswork 4.0.
- All applications services on the deployed Cisco Crosswork 4.0 main node to which you're migrating your data are up and healthy. You can check the status of services on the main node by selecting from the main menu Administration > Crosswork Manager > Crosswork Health. If any services are down or degraded and you still want to migrate, use the script's "force" flag (`-f true`) to ignore these issues and perform the migration.

Step 1 Create a backup of the data from the previous version of Cisco Crosswork:

a) Click Backup. The Backup dialog box displays the destination server details.
b) Provide a relevant name for the backup in the Job Name field. Record this file name and the remote file path, as you'll need them later in this procedure.
c) (Optional) Click Verify Backup to verify that Cisco Crosswork has enough free resources to complete the backup. If the check is successful, Cisco Crosswork displays a warning message about the time-consuming nature of the operation. Click OK.
d) Click Start Backup to start the backup operation. Cisco Crosswork creates a backup job set and adds it to the job list.

Step 2 If your previous deployment of Cisco Crosswork is still running, detach all your managed devices from the Data Gateway instances of the previous version:

a) From the main menu, choose Admin > Data Gateway Management.
b) Select the Cisco Crosswork Data Gateway instance with attached devices.
c) Click Detach Devices.
d) Click Detach All Devices.
e) Repeat these steps if you're using more than one Cisco Crosswork Data Gateway instance.

Step 3 Delete the Cisco Crosswork Data Gateway VM hosting the previous version:

a) Log in to the VMware vSphere Web Client hosting your Data Gateway VM.
b) In the Navigator pane, right-click the Data Gateway VM that you want to remove and choose Power > Power Off.
c) Once you power down the VM, right-click the VM again and choose Delete from Disk.

Step 4 Deploy version 4.0 of Cisco Crosswork. The deployment must include the Cisco Crosswork 4.0 platform, the Cisco Crosswork Data Gateway, your cluster nodes, and the Cisco Crosswork application whose data you want to migrate (either Change Automation and Health Insights or Optimization Engine).

Step 5 Configure version 4.0 of Cisco Crosswork to use the same secure SCP server you used for the backups of the previous version:

a) From the main menu, choose Administration > Backup and Restore.
b) Click Destination to display the Edit Destination dialog box. Enter the details for the previously used SCP server.
c) Click Save to confirm the backup server details.

Step 6 Use SSH to log in to the Cisco Crosswork Management VIP. Assume root privileges and change to the folder containing the migration shell script, as follows:

```
$> ssh cw-admin@CrossworkHost
Password: password
Cisco Crosswork
$>cw-admin@CrossworkHost:~$ sudo su
[sudo] password for cw-admin: sudo password
root@CrossworkHost: cd /opt/robot/bin
```

Where:

- *CrossworkHost* is the IP address or host name of the server.

- *password* is the Cisco Crosswork cw-admin password, created when you deployed the server.
- *sudo password* is the root password for the server. The sudo password of usually the same as the cw-admin password.

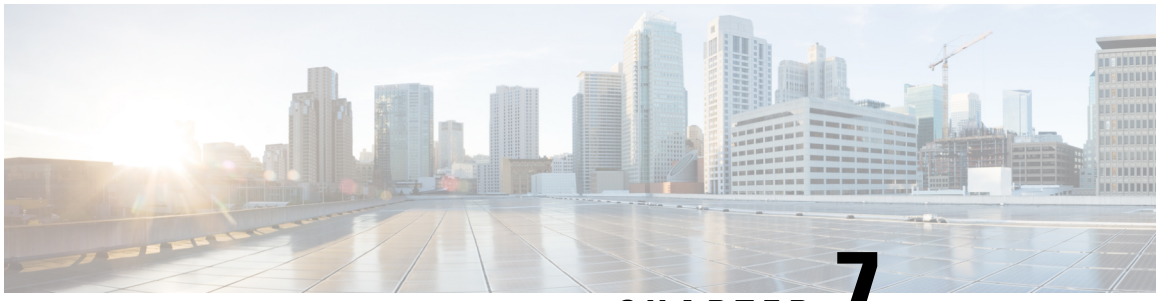
Step 7 Initiate migration of the backup data to the Cisco Crosswork 4.0 deplomen, as follows:

```
root@CrossworkHost: ./migration.sh -i CrossworkIP -u username -p password -n backupFile -f false|true
```

Where:

- *CrossworkIP* is the IP address of the main node of the deployed Cisco Crosswork 4.0 cluster. For example: `-i 192.168.1.1`.
- *username* is the user name of an enrolled, nonadministrative user on the cluster. The script submits the migration job as a nonadmin job. For example: `-u UserTom`.
- *password* is the password for the enrolled user. For example: `-p MyPassword` to force the migration.
- *backupFile* is the file name of the backup. For example: `-n My332BackUp.tar.gz`. Cisco Crosswork assumes that the configured FTP backup server has this file.
- *force* is a boolean flag indicating whether you want to ignore the health status of system services. For example: `-f true` to force the migration.

The migration script initiates the data transfer. The time the migration takes varies, depending on the hardware resources available and the amount of data to be migrated.



CHAPTER 7

Uninstall

This section contains the following topics:

Delete VM using Cluster Installer

In case of a failed installation, the cluster installer tool is used to cleanup or delete any previously created VMs based on the cluster-state. this is a critical activity during failed deployments. Any changes made to the VM settings or the DC host requires a cleanup operation before redeployment.

Note The cleanup procedure is similar for both vCenter and CSP deployments, with the only exception being the addition of "-t csp" option when running a CSP cleanup.

Note The installer cleanup option will delete the cluster deployment based on the inventory in `/data` directory.

Step 1 Enter the directory storing the deployment info.

For example, `_cd ~/cw-cluster`.

Step 2 Run the container on the host.

```
docker run --rm -it -v `pwd`:/data <cw-installer docker container>
```

Note Add the "-t csp" option when running a CSP cleanup.

Step 3 Edit the copy of the template file (for example, `v4.tfvars`) in a text editor, adding the data center access parameters. Remaining parameters can be provided with dummy values, or entered on the command line during the execution of the operation.

Step 4 Run the `_cw-installer.sh install_` script with the clean directive along with the deployment manifest using the `-m` flag. For example:

```
./cw-installer.sh clean -m /data/deployment.tfvars
```

Step 5 Enter "yes" when prompted to confirm the operation.

Step 6 (Optional) In addition to removing the VMs, adding the `-o` option to the clean directive will also remove the Cisco Crosswork image template from the data center.

Example:

```
./cw-installer.sh clean -m/data/deployment.tfvars -o
```

Step 7 (Optional) To clean the cluster quickly (without verification), users can run the installer using the following command:

```
docker run --rm -it -v `pwd`:/data <cw installer docker image> -exec './cw-installer.sh clean -m
/data/deployment.tfvars'
```

Uninstall Crosswork Applications

This section explains how to uninstall a application via the Crosswork GUI.

Note The Uninstall option removes the application, the associated data and services (application-specific menus, UI etc.).

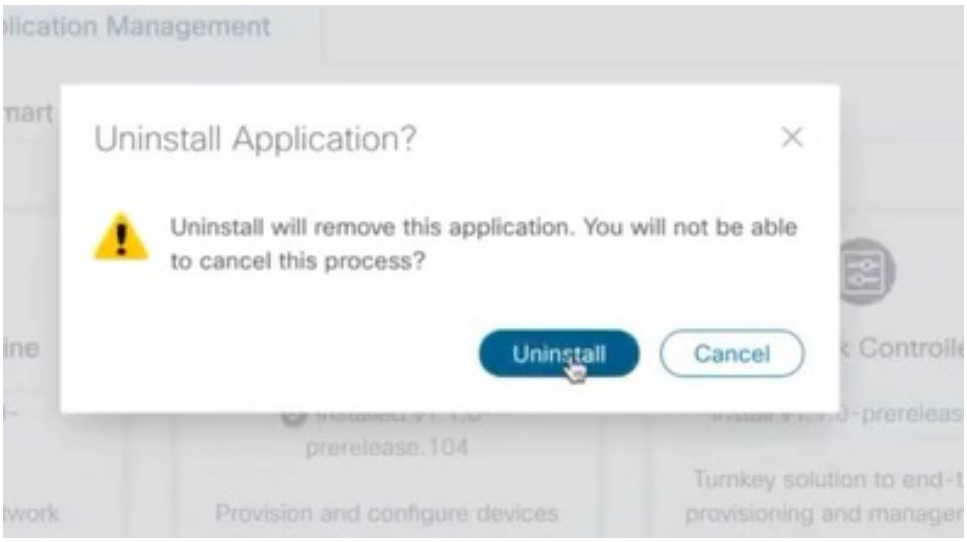
Note Crosswork Platform Infrastructure cannot be deactivated.

Step 1 Click on Admin > Crosswork Management, and select the Application Management tab.

The Crosswork Platform Infrastructure and any applications that are added are displayed here as tiles.

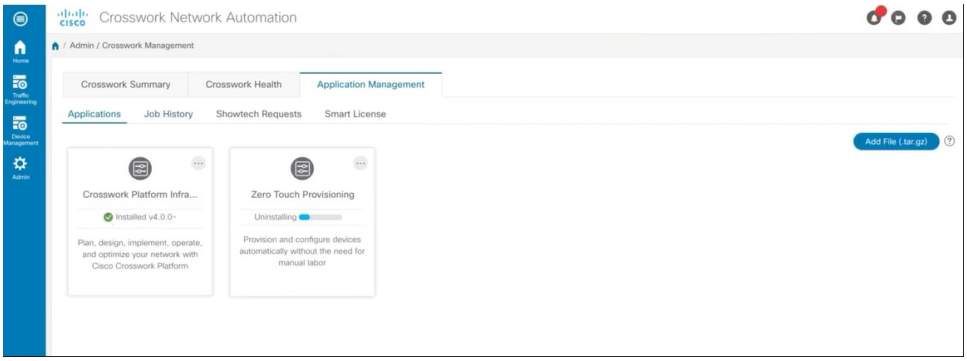
Step 2 Click (…) on the application tile that you want to uninstall, and select the Uninstall option from the drop down list.

A pop-up is displayed to confirm the action.



Step 3 Click Uninstall to confirm.

The selected application is uninstalled and the application tile is modified to reflect the same.



Note Uninstall operation does not remove the CAPP file from the repository. The CAPP file will remain visible in the UI, in case user wants to install in the future.

Delete Crosswork Data Gateway VM from Cisco Crosswork

Before you begin

The Crosswork Data Gateway VM you want to delete must be in maintenance mode.

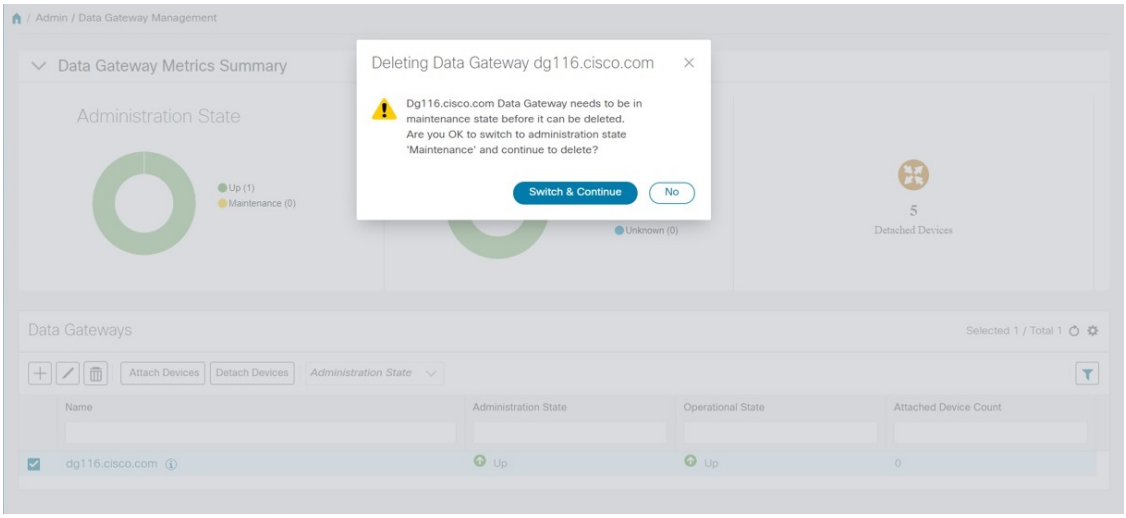
Step 1 Log in to Cisco Crosswork.

Step 2 From the navigation panel, select Administration > Data Gateway Management.

Click on the Virtual Machines tab.

Step 3 In the Virtual Machines list, find the Crosswork Data Gateway VM you want to delete and click ⋯ under Actions column. Click Delete.

Step 4 If the Crosswork Data Gateway VM is not in maintenance state, Cisco Crosswork prompts you to switch it to maintenance state. Click Switch to maintenance & continue.



The Crosswork Data Gateway VM is deleted.

Delete VM using vSphere UI

This section explains the procedure to delete a VM from vCenter. This procedure is used to delete any Cisco Crosswork application VM.

Note

- Be aware that this procedure deletes all your app data.
- If you want to delete Crosswork Data Gateway only, ensure you have done the following:
  - Detach the devices from the Crosswork Data Gateway VM you want to delete. The procedure to detach devices from a Crosswork Data Gateway is described in the Section: Delete Cisco Crosswork Data Gateway VM from Cisco Crosswork in Cisco Crosswork Infrastructure 4.0 and Applications Administration Guide.
  - Delete the Crosswork Data Gateway VM from Cisco Crosswork as described in Delete Crosswork Data Gateway VM from Cisco Crosswork, on page 105.

Step 1 Log in to the VMware vSphere Web Client.

Step 2 In the Navigator pane, right-click the app VM that you want to remove and choose Power > Power Off.

Step 3 Once the VM is powered off, right-click the VM again and choose Delete from Disk.

The VM is deleted.

Delete Crosswork Data Gateway Service from Cisco CSP

Follow the steps to delete the Crosswork Data Gateway Service from Cisco CSP:

Before you begin

Before deleting the Crosswork Data Gateway VM, ensure you have done the following:

Step 1 Log in to your Cisco CSP.

Step 2 Go to Configuration > Services.

The Service table shows the current status of the services.

Step 3 Find your service instance in the Service Name column and click Delete under the Action column.