



Cisco Crosswork Network Controller 5.0 Installation Guide

First Published: 2023-05-08

Last Modified: 2023-07-07

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023–2023 Cisco Systems, Inc. All rights reserved.



CONTENTS

PART I

Get Started 9

CHAPTER 1

Overview 1

- About this guide 1
- Audience 1
- Introduction 2
- Cisco Crosswork Network Controller Packages 3
- Security 4

CHAPTER 2

Plan Your Deployment 5

- Before You Begin 5
 - Determine the Applications You Need 5
 - Identify the Resource Footprint 7
 - Special Considerations 9

CHAPTER 3

Choose Your Installation Workflow 11

- Overview 11
- Install Cisco Crosswork Network Controller on VMware vCenter 11
- Install Cisco Crosswork Network Controller on AWS EC2 13

PART II

Install Cisco Crosswork Network Controller on VMware vCenter 17

CHAPTER 4

Installation Prerequisites for VMware vCenter 19

- Overview 19
- Supported Network Topology Models 19
- VMware Settings 25

Host VM Requirements 26

 Crosswork Cluster VM Requirements 26

 Crosswork Data Gateway VM Requirements 28

TCP/UDP Port requirements 30

IP Address Restrictions 34

Supported Web Browsers 36

CHAPTER 5

Install Crosswork Cluster on VMware vCenter 37

 Installation Overview 37

 Installation Parameters 37

 Install Cisco Crosswork on VMware vCenter using Cluster Installer Tool 42

 Sample manifest template for VMware vCenter 47

 Set seed node explicitly 49

 Troubleshoot the Cluster 49

 Manual Installation of Cisco Crosswork using vCenter vSphere UI 52

 Build the OVF template 53

 Deploy the template 59

 Monitor the Installation 62

 Log into the Cisco Crosswork UI 64

CHAPTER 6

Install Cisco Crosswork Data Gateway on VMware vCenter 67

 Cisco Crosswork Data Gateway Installation Workflow 67

 Cisco Crosswork Data Gateway Parameters and Deployment Scenarios 68

 Install Cisco Crosswork Data Gateway using vCenter vSphere Client 82

 Install Cisco Crosswork Data Gateway via OVF Tool 95

 Sample Script for Crosswork Data Gateway IPv4 Deployment 97

 Sample Script for Crosswork Data Gateway IPv6 Deployment 98

 Log in and Log out of Crosswork Data Gateway VM 100

 Access Crosswork Data Gateway VM from SSH 100

 Access Crosswork Data Gateway through vCenter 101

 Log Out of Crosswork Data Gateway VM 101

 Cisco Crosswork Data Gateway Authentication and Enrollment 102

 Crosswork Data Gateway Post-installation Tasks 103

 Configure Timezone of the Crosswork Data Gateway VM 103

Troubleshoot Crosswork Data Gateway Installation and Enrollment	104
Import Controller Signing Certificate File	107
View the Controller Signing Certificate File	108

PART III

Install Cisco Crosswork Network Controller on AWS EC2 109

CHAPTER 7
Installation Prerequisites for AWS EC2 111

Overview	111
Amazon EC2 Settings	111
Host VM Requirements	114
Crosswork Cluster VM Requirements	114
Crosswork Data Gateway VM Requirements	115
TCP/UDP Port requirements	118
IP Address Restrictions	123
Supported Web Browsers	124

CHAPTER 8
Install Cisco Crosswork Network Controller on AWS EC2 125

Installation Overview	125
Extract CF Template Image	125
Roles and Policy Permissions	127
Configure the CloudFormation (CF) Template Parameters	127
CF Template Parameters for Installing Cisco Crosswork Cluster VMs	128
CF Template Parameters for Installing Crosswork Data Gateway	134
CF Template Parameters for Installing NSO	137
CF Template Parameters for Installing Single Hybrid Cluster or Worker Node	138
Install Using Module Deployment Method	140
Install Cisco Crosswork Cluster on Amazon EC2	140
Install Crosswork Data Gateway on Amazon EC2	141
Auto-Configuration for Deploying Crosswork Data Gateway	143
Install Cisco NSO on Amazon EC2	145
Deploy an Additional Crosswork Cluster Node	146
Manage CF Template Deployment	147
Deploy a CF Template	147
Monitor the Installation	148

Accessing the Crosswork UI 149

Crosswork Data Gateway Post-installation Tasks 150

- Configure Timezone of the Crosswork Data Gateway VM 150
- Log in and Log out of Crosswork Data Gateway VM 152
 - Access Crosswork Data Gateway VM from SSH 152
 - Log out of Crosswork Data Gateway VM 152
- Troubleshoot Crosswork Data Gateway Installation and Enrollment 152
 - Import Controller Signing Certificate File 155
 - View the Controller Signing Certificate File 156

PART IV **Install Crosswork Applications 157**

CHAPTER 9 **Install Crosswork Applications 159**

- Install Crosswork Applications 159

PART V **Integrate Cisco NSO and SR-PCE with Cisco Crosswork Network Controller 165**

CHAPTER 10 **Integrate Cisco NSO 167**

- NSO Integration Workflow 167
- Install Cisco NSO Function Packs using Ansible playbook 168
 - LSA 170
 - LSA HA (High Availability) 171
 - Standalone 173
 - Standalone HA (High Availability) 174
 - Install Cisco NSO Function Packs manually 175
- Add Cisco NSO Providers 175
- (Optional) Set up Cisco NSO Layered Service Architecture 178

CHAPTER 11 **Integrate SR-PCE 179**

- SR-PCE Integration Workflow 179
- Configure SR-PCE 179
 - Sample SR-PCE config 182
- Add Cisco SR-PCE Providers 182

PART VI**Upgrade Cisco Crosswork Network Controller 187**

CHAPTER 12**Upgrade Cisco Crosswork 189**

Upgrade Overview 189

Upgrade Requirements 190

Upgrade Using Existing Hardware 191

Shut Down Cisco Crosswork Data Gateway VMs 192

Create Backup and Shut Down Cisco Crosswork 193

Install the latest version of the Cisco Crosswork Cluster 195

Install the Cisco Crosswork Applications 196

Migrate Cisco Crosswork Backup 196

Upgrade Crosswork Data Gateway 197

Troubleshoot Crosswork Data Gateway Upgrade Issues 200

Post-upgrade Checklist 200

Upgrade Using Parallel Hardware 201

Deploy a new Cisco Crosswork Cluster 202

Backup Cisco Crosswork Cluster 203

Update DNS Server and Run Migration 205

Add Crosswork Data Gateway to Cisco Crosswork 206

Shut Down the old Cisco Crosswork Cluster 208

Update a Crosswork Application (standalone activity) 208

PART VII**Uninstall Cisco Crosswork Network Controller 213**

CHAPTER 13**Uninstall Cisco Crosswork 215**

Uninstall the Crosswork Cluster 215

Delete the VM using the Cluster Installer 215

Delete the VM using the vSphere UI 216

Uninstall Crosswork Data Gateway 216

Delete Crosswork Data Gateway VM from Cisco Crosswork 217

Delete Crosswork Data Gateway from the Crosswork Cluster 217

Uninstall Crosswork Applications 218



PART I

Get Started

- [Overview, on page 1](#)
- [Plan Your Deployment, on page 5](#)
- [Choose Your Installation Workflow, on page 11](#)



CHAPTER 1

Overview

This chapter contains the following topics:

- [About this guide, on page 1](#)
- [Audience, on page 1](#)
- [Introduction, on page 2](#)
- [Cisco Crosswork Network Controller Packages, on page 3](#)
- [Security, on page 4](#)

About this guide

This guide explains the requirements and processes to install or upgrade Crosswork Network Controller solution.

This document does not cover the installation of integrated components (such as Cisco NSO, Cisco SR-PCE, or Cisco WAE) that may already be installed or can be used independently. For more details about these components, please refer to their respective installation documentation.



Note While this guide includes instructions for installing or upgrading Crosswork Network Controller on Amazon EC2 platform, it is only available as a limited-release feature. Please contact your Cisco representative for assistance.

Audience

This guide is for experienced network users and operators who want to install Crosswork Network Controller solution in their network. This guide assumes that you are familiar with the following:

- Using a Docker container
- Running scripts in Python
- Deploying OVF templates using VMware vCenter
- Deploying using OVF tool
- Amazon Web Services (AWS), Amazon EC2 concepts, and creation of CloudFormation templates

Introduction

Cisco Crosswork Network Controller

Cisco Crosswork Network Controller is an integrated solution (consisting of Cisco Crosswork Infrastructure, Cisco Crosswork Data Gateway and the Crosswork applications) that enables you to proactively manage your end-to-end networks, by providing intent-based and closed-loop automation solutions to ensure faster innovation, optimal user experience, and operational excellence.

Cisco Crosswork Infrastructure

Cisco Crosswork Infrastructure is a microservices-based platform and is the foundation required for running Crosswork applications. It employs a cluster architecture to be extensible, scalable, and highly available. The Crosswork cluster consists of three VMs or nodes operating in a hybrid configuration. Additional VMs or nodes (maximum up to 2 nodes) in a Worker configuration can be added, as needed, to match the requirements of the deployed applications. A Hybrid node can run infrastructure and application pods, while a Worker node can run only application pods. The total number of Hybrid and Worker nodes varies based on the size of the network and the applications being run. Please work with the Cisco Customer Experience team to determine the number of nodes required for your network.



Note Hereafter in this guide, Cisco Crosswork Infrastructure is referred to as "Cisco Crosswork".

Cisco Crosswork Data Gateway

Cisco Crosswork integrates with one or more Cisco Crosswork Data Gateway(s) to gather information from the managed devices and forward it to Cisco Crosswork as well as external destinations. The information is then analyzed and processed by the Crosswork applications and used to manage the network or respond to changes in the network. The number of Crosswork Data Gateways deployed in your network depends on the number of devices, the amount of data being collected, the overall topology, and your redundancy requirements. Each Crosswork Data Gateway is deployed on an individual VM. Please consult with the Cisco Customer Experience team for guidance on your deployment to best meet your needs.

Crosswork Data Gateway is an integral part of the Crosswork solution being deployed. For this reason, this document explains Crosswork Data Gateway as a foundational component that must be installed in tandem with the Crosswork Infrastructure.

Crosswork Applications

See [Cisco Crosswork Network Controller Packages](#), on page 3 for details.

Other Integrated Components

Cisco Network Services Orchestrator functions as the provider for Cisco Crosswork to configure the devices according to their expected functions, including optionally configuring MDT sensor paths for data collection. Cisco NSO provides the important functions of device management, configuration and maintenance services.

Cisco Segment Routing Path Computation Element (SR-PCE) is an IOS-XR multi-domain stateful PCE supporting both Segment Routing Traffic Engineering (ST-TE) and Resource Reservation Protocol Traffic

Engineering (RSVP-TE). Cisco Crosswork uses the combination of telemetry and data collected from the Cisco SR-PCE to analyze and compute optimal paths for TE tunnels and/or to discover devices in the network.

Cisco Crosswork can also integrate with other providers (such as Cisco WAE, Syslog, and Alert), external servers (TACACS+, LDAP, and RADIUS), DHCP server (when using Crosswork ZTP), and external Kafka (for external data collection destinations). The details about these specific integrations are addressed in *Cisco Crosswork Network Controller 5.0 Administration Guide* or in the application guides.

Cisco Crosswork Network Controller Packages

The following table describes the Crosswork applications that can be deployed on the Crosswork Network Controller and the way they are packaged:



Note Cisco Crosswork Optimization Engine can be installed independently without any of the other Crosswork Network Controller applications. For more details, see [Install Crosswork Applications, on page 159](#).

Table 1: Cisco Crosswork Network Controller Packages

Package	Contents	Description
Essentials Package	Cisco Crosswork Optimization Engine	An application that provides closed-loop tracking of the network state and real-time network optimization in response to changes in network state, allowing operators to effectively maximize network capacity utilization, as well as increase service velocity.
	Cisco Crosswork Active Topology	A component of Crosswork Network Controller that enables visualization of topology and services on logical and geographical maps.
	Element Management Functions	A library of functions that provides deep inventory collection, alarm management and image management using Inventory, Fault, and Software Image Management (SWIM) functions.
Advantage Package	Cisco Crosswork Service Health	An application that overlays a service level view of the environment and makes it easier for operators to monitor if services (for example, L2/L3 VPN) are healthy based on the rules established by the operator.

Package	Contents	Description
Add-on Package	Cisco Crosswork Change Automation	An application that automates the process of deploying changes to the network. Orchestration is defined via an embedded Ansible Playbook and then configuration changes are pushed to Cisco Network Services Orchestrator (NSO) to be deployed to the network.
	Cisco Crosswork Health Insights	An application that performs real-time Key Performance Indicator (KPI) monitoring, alerting, and troubleshooting. Cisco Crosswork Health Insights enables programmable monitoring and analytics, and builds dynamic detection and analytics modules that allow operators to monitor and alert on network events based on user-defined logic.
	Cisco Crosswork Zero Touch Provisioning	An application that streamlines onboarding and provisioning of Day 0 configuration resulting in faster deployment of IOS-XR devices at a lower operating cost.

Security

Cisco takes great strides to ensure that all our products conform to the latest industry recommendations. We firmly believe that security is an end-to-end commitment and are here to help secure your entire environment. Please work with your Cisco account team to review the security profile of your network.

For details on how we validate our products, see [Cisco Secure Products and Solutions](#) and [Cisco Security Advisories](#).

If you have questions or concerns regarding the security of any Cisco products, please open a case with the Cisco Customer Experience team and include details about the tool being used and any vulnerabilities it reports.



CHAPTER 2

Plan Your Deployment

This chapter contains the following topics:

- [Before You Begin, on page 5](#)

Before You Begin

This section explains the setup options you need to make before installing Crosswork Network Controller solution on your preferred platform.

1. [Determine the Applications You Need, on page 5](#)
2. [Identify the Resource Footprint, on page 7](#)
3. [Special Considerations, on page 9](#)

After completing the planning in the above steps, follow the relevant installation workflow steps for your platform:

- **For VMware vCenter:** [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)
- **For AWS EC2:** [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)

Starting with the Crosswork Network Controller version 4.1, Crosswork deployment is no longer supported for the Cisco CSP platform. For more information, see [End-of-Life Announcement for the Cisco Cloud Services Platform Operating System](#).

Determine the Applications You Need

The first decision is to select the Crosswork applications that meet the needs of your production environment. This is a crucial step as each Crosswork application can impact the overall resources needed.



Note Crosswork Network Controller supports only "Large" deployment profile for customer deployments.

Crosswork Network Controller is available in the following packages (see [Cisco Crosswork Network Controller Packages, on page 3](#) for details):

Table 2: Crosswork Network Controller packages

Package 1	Contents	Crosswork Data Gateway Deployment 2	Recommended number of cluster VMs 3
Cisco Crosswork Network Controller Essentials	Cisco Crosswork Optimization Engine	On-Premise Standard (default): Collectors only.	When Essentials package is installed WITHOUT Element Management Functions: • 3 Hybrid nodes
	Cisco Crosswork Active Topology	On-Premise Standard (default): Collectors only.	
	Element Management Functions	On-Premise Standard (default): Collectors only.	When Essentials package is installed WITH Element Management Functions: • 3 Hybrid nodes + 1 Worker node
Cisco Crosswork Network Controller Advantage	Cisco Crosswork Service Health	On-Premise Extended: Collectors and offload services.	3 Hybrid nodes + 2 Worker nodes
Add-on Package 4	Cisco Crosswork Change Automation	On-Premise Extended: Collectors and offload services.	3 Hybrid nodes + 2 Worker nodes
	Cisco Crosswork Health Insights	On-Premise Extended: Collectors and offload services.	
	Cisco Crosswork Zero Touch Provisioning	On-Premise Standard (default): Collectors only.	

- ¹ There are licensing implications for different packages, please consult your Cisco Account team to understand which packages and licenses are required for your use cases.
- ² The VM resource requirements for Crosswork Data Gateway are different for each type and cannot be modified. Therefore, if your requirements change, you must re-deploy the Crosswork Data Gateway to move from one type to another. For more information, see the *Redeploy a Crosswork Data Gateway VM* section in the *Cisco Crosswork Network Controller 5.0 Administration Guide*.
- ³ The number of VMs mentioned is the recommended count. You can add more Worker nodes (maximum up to 2 worker nodes) as needed. If your requirements exceed the recommended count, please contact the Cisco Customer Experience team.
- ⁴ The cluster resource estimation is under the assumption that you are using the add-on applications with the Crosswork Network Controller packages.

Ensure that you have sufficient worker nodes in your cluster. You can always check the load in your cluster and choose to add new worker nodes post installation. For more information, see the *Deploy New Cluster Nodes* section in the *Crosswork Network Controller 5.0 Administration Guide*.

Identify the Resource Footprint

Once you determine the Crosswork applications you want and the number of VMs you will need to deploy to host them, ensure that you have the resources needed for them. The resources required per VM such as CPU, Memory, and Storage vary based on the datacenter where your VMs will be hosted (VMware or AWS).

The tables in this topic explain the resource requirements per VM to deploy Crosswork Hybrid or Worker nodes, Crosswork Data Gateways, NSO, and SR-PCE (refer to the table relevant to your platform).



Note

- The resources listed for NSO are higher than for other NSO use cases due to the additional requirements Crosswork Network Controller places on NSO.
- The NSO footprint depends on the type of deployment, standalone or LSA.
- The SR-PCE count will depend on the number of head-ends that need to be managed
- The types of VM and the number of each type of VM should be decided based on the use cases and scale. Please consult with your Cisco Account team and Cisco Customer Experience team for assistance.
- The values in **Storage** column is the space needed for storing Crosswork files and does not consider any additional overhead that may be required (for example, RAID configuration).
- The storage required for each backup will vary based on the your cluster size, applications in the cluster, and the scale requirements.
- Upgrade of the cluster temporarily requires double the total disk space used by the cluster.
- The number of data gateways needed depends on the number of devices you have in your network and the level of redundancy you want (1:n up to 1:1). To determine the number of Crosswork Data Gateways needed, contact the Cisco Customer Experience team.

Crosswork Resource Footprint for VMware



Note

- Ensure that you have a docker-capable host to load the Crosswork installer tool.

Table 3: Crosswork Resource Footprint for VMware

Component	vCPU	Clock Freq (GHz)	Memory (RAM)	Network Interface Controller (NIC)	Storage (Boot disk + Data disk)
Crosswork Hybrid or Worker node	12 Minimum clock reservation: 18 GHz	>= 2.20	96 GB	10 Gbps	1 TB
CDG On-Premise Standard	12	>= 2.20	48 GB	10 Gbps	70 GB (50 GB + 20 GB)

Component	vCPU	Clock Freq (GHz)	Memory (RAM)	Network Interface Controller (NIC)	Storage (Boot disk + Data disk)
CDG On-Premise Extended	20	>= 2.20	112 GB	10 Gbps	570 GB (50 GB + 520 GB)
Cisco NSO	16	>= 2.20	128 GB	10 Gbps	1 TB
Cisco SR-PCE	8	>= 2.20	24 GB	10 Gbps	70 GB
Basic SCP Server (for storing backups)	-	-	-	-	At least 25 GB (recommended)

Crosswork Resource Footprint for AWS EC2



Note In case of AWS EC2, the additional storage server may be in the AWS cloud or your local environment (must be reachable from the AWS cloud).

Table 4: Crosswork Resource Footprint for AWS EC2

Component	vCPU	Memory (RAM)	Network Interface Controller (NIC)	Storage (Boot disk + Data Disk)
Crosswork Hybrid or Worker node	12 Minimum clock reservation: 18 GHz	96 GB	10 Gbps	1 TB
CDG On-Premise Standard	12	64 GB	10 Gbps	70 GB (50 GB + 20GB)
CDG On-Premise Extended	24	128 GB	10 Gbps	570 GB (50 GB + 520 GB)
Cisco NSO	16	128 GB	10 Gbps	1 TB
Cisco SR-PCE	8	24 GB	10 Gbps	70 GB
Basic SCP Server (for storing backups)	-	-	-	At least 25 GB (recommended)

Additional Resource Requirements:

- 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 15,000 RPM.

- The VM data store(s) need to have disk access latency < 10 ms or > 5000 IOPS.

Special Considerations

In addition to the above instructions, there may be certain setup options that you need to consider before you begin the installation.

- **Are you going to use self-signed certificates?** – if yes, you need to make the certificates available. For more information on the type of certificates supported and how to manage them, see the *Manage Certificates* section in the *Crosswork Network Controller 5.0 Administration Guide*.
- **Do you plan to integrate Crosswork with external authentication servers?**– Integration with TACACS+ or other external authentication servers will require you to have credentials created for the Crosswork user accounts and roles.
- **Do you want to use a URL of an optional Management network proxy server?**– If your environment requires an HTTP or HTTPS proxy to access the URLs on the public Internet, you must configure a proxy server for Crosswork Data Gateway to connect to Cisco Crosswork.
- **In Crosswork Data Gateway, do you want to configure a Syslog server to collect the syslog?**– if yes, then provide the host name or IPv4 or IPv6 address of an external syslog server.
- **In Crosswork Data Gateway, do you want to configure an Auditd Server to collect the event logs?**– if yes, then provide the host name or IPv4 or IPv6 address of an external auditd server.
- **Do you plan to enable the automatic execution of linked playbooks?** – If yes, you must enable Playbook Job Scheduling and disable Credential Prompting for playbook execution in the Network Automation settings window. For more information, see the *Enable Automatic Playbook Execution* topic in the *Crosswork Change Automation and Health Insights 5.0 User Guide*.



CHAPTER 3

Choose Your Installation Workflow

This chapter contains the following topics:

- [Overview, on page 11](#)
- [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)
- [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)

Overview

This chapter provides the installation workflows for each of the supported environments (VMware and AWS).

The workflows give a high level description of the tasks necessary to install the Crosswork Network Controller and to integrate it with the required components of the solution. Integration with optional components is addressed in the *Crosswork Network Controller 5.0 Administration Guide*.

These workflow steps should be used as your primary installation guidepost and roadmap for the end to end installation of Crosswork Network Controller. After completing each detailed step, it is recommended that you refer back to the workflow chart for the next step to perform.



Note The time taken for the entire installation can vary based on size of your deployment profile and the performance characteristics of your hardware.

Install Cisco Crosswork Network Controller on VMware vCenter

Before you begin:

- Ensure you have identified the Crosswork components you need and arranged for the resources required to complete the installation. If not, please refer to the guidelines in [Plan Your Deployment, on page 5](#).
- Please see the *Crosswork Network Controller 5.0 Release Notes* to know the NSO and SR-PCE versions compatible with Crosswork Network Controller.

The following table describes the stages to install Crosswork Network Controller on VMware vCenter.

Table 5: Crosswork Installation Workflow

Step	Action
Prepare for installation	
1. Ensure that your VMware environment meets all the requirements.	Refer to the guidelines in Installation Prerequisites for VMware vCenter , on page 19.
Install the Crosswork cluster	
2. Install the Cisco Crosswork cluster on VMware vCenter.	Install using your preferred method: <ul style="list-style-type: none"> • <i>Using cluster installer tool:</i> Install Cisco Crosswork on VMware vCenter using Cluster Installer Tool, on page 42 • <i>Manual Installation:</i> Manual Installation of Cisco Crosswork using vCenter vSphere UI, on page 52
3. Verify if the installation was successful, and log into the Cisco Crosswork UI.	Refer to the guidelines in: <ul style="list-style-type: none"> • Monitor the Installation, on page 62 • Log into the Cisco Crosswork UI, on page 64
Install the Crosswork Data Gateway	
4. Install one or more Crosswork Data Gateway instances on VMware vCenter.	Choose the profile for the Cisco Crosswork Data Gateway VM (Standard or Extended) and install as per your preferred method: <ul style="list-style-type: none"> • <i>Using vSphere:</i> Install Cisco Crosswork Data Gateway using vCenter vSphere Client, on page 82 • <i>Using OVF tool:</i> Install Cisco Crosswork Data Gateway via OVF Tool, on page 95 <p>Note If you plan to install multiple Cisco Crosswork Data Gateway VMs due to load or scale requirements, or you wish to leverage Cisco Data Gateway High Availability, you are recommended to install all the Crosswork Data Gateway VMs first and then proceed with adding them to a Data Gateway pool.</p>
5. Complete the Crosswork Data Gateway post-installation tasks.	Follow the steps in Crosswork Data Gateway Post-installation Tasks , on page 103.
6. Verify that the Crosswork Data Gateway VM or multiple VMs have enrolled successfully with Cisco Crosswork.	Follow the steps in Cisco Crosswork Data Gateway Authentication and Enrollment , on page 102. After verifying that the Crosswork Data Gateway VM has enrolled successfully with Cisco Crosswork, set up the Crosswork Data Gateway for collection by creating a Crosswork Data Gateway pool. See the <i>Create a Crosswork Data Gateway Pool</i> section in Cisco Crosswork Network Controller 5.0 Administration Guide .

Step	Action
Install the Cisco Crosswork Applications	
7. Install the Crosswork Applications	Follow the instructions in Install Crosswork Applications, on page 159 .
Integrate NSO with Crosswork	
8. Do you have Cisco NSO already installed?	If yes, proceed to step 9. If no, please follow the install instructions in the NSO Installation Guide .
9. Install the NSO Function Packs	Follow the instructions in Install Cisco NSO Function Packs using Ansible playbook, on page 168 .
10. Add NSO Provider and verify that it is reachable	Follow the instructions in Add Cisco NSO Providers, on page 175 .
Integrate SR-PCE with Crosswork	
11. Is your SR-PCE installed?	If yes, please proceed to step 12. If no, please choose the type of SR-PCE you wish to use (physical or virtual device) and follow the appropriate instructions to get the device (or virtual device) deployed. For more information, see the Cisco IOS XRv 9000 Router Installation Guide .
12. Configure SR-PCE	Follow the instructions in Configure SR-PCE, on page 179 .
13. Add SR-PCE Provider and verify that it is reachable.	Follow the instructions in Add Cisco SR-PCE Providers, on page 182 .
14. (Recommended) Create a backup of your Crosswork Network Controller.	Follow the instructions in <i>Manage Backups</i> chapter in Cisco Crosswork Network Controller 5.0 Administration Guide .

Install Cisco Crosswork Network Controller on AWS EC2

Before you begin:

- Ensure you have identified the Crosswork components you need and arranged for the resources required to complete the installation. If not, please refer to the guidelines in [Plan Your Deployment, on page 5](#).
- Please see the *Crosswork Network Controller 5.0 Release Notes* to know the NSO and SR-PCE versions compatible with Crosswork Network Controller.

Crosswork Network Controller supports **Module deployment** which allows you to pick and choose to install the components of the Cisco Crosswork solution (hybrid and worker nodes needed for Crosswork cluster, one or more Crosswork Data Gateway(s), and NSO) you wish to deploy.

The following table describes the stages to install Crosswork Network Controller on AWS EC2 using CloudFormation (CF) templates.

Table 6: Crosswork Installation Workflow

Step	Action
Prepare for installation	
1. Ensure that your AWS EC2 environment meets all the requirements.	Refer to the guidelines in Installation Prerequisites for AWS EC2 , on page 111.
2. Extract the CF template package	Follow the instructions in Extract CF Template Image , on page 125.
Install Crosswork components	
3. Module deployment: Install the Cisco Crosswork components using module deployment.	<p>Install the Crosswork components individually:</p> <ul style="list-style-type: none"> • Install the Crosswork cluster: Install Cisco Crosswork Cluster on Amazon EC2, on page 140 • Install one or more Crosswork Data Gateway(s): Install Crosswork Data Gateway on Amazon EC2, on page 141 <p>Crosswork Data Gateway is deployed with the default parameter values if you missed configuring the values during deployment. For more information, see Auto-Configuration for Deploying Crosswork Data Gateway, on page 143.</p> <ul style="list-style-type: none"> • Install Cisco NSO: Install Cisco NSO on Amazon EC2, on page 145
4. Verify the installation and access Crosswork UI	Refer to the guidelines in Accessing the Crosswork UI , on page 149
Install the Crosswork Applications	
5. Install the Crosswork Applications	Follow the instructions in Install Crosswork Applications , on page 159.
Integrate NSO with Crosswork	
6. Install the NSO Function Packs	Follow the instructions in Install Cisco NSO Function Packs using Ansible playbook , on page 168.
7. Add NSO Provider and verify that is reachable.	Follow the instructions in Add Cisco NSO Providers , on page 175.
Integrate SR-PCE with Crosswork	
8. Is your SR-PCE installed?	<p>If yes, please proceed to step 9.</p> <p>If no, please select the SR-PCE type (for AWS) and follow the relevant install instructions in the Cisco IOS XRv 9000 Router Installation Guide.</p>
9. Configure SR-PCE	Follow the instructions in Configure SR-PCE , on page 179.

Step	Action
10. Add SR-PCE Provider and verify that SR-PCE is reachable.	Follow the instructions in Add Cisco SR-PCE Providers, on page 182 .
11. (Recommended) Create a backup of your Crosswork Network Controller.	Follow the instructions in <i>Manage Backups</i> chapter in the <i>Cisco Crosswork Network Controller 5.0 Administration Guide</i> .



PART II

Install Cisco Crosswork Network Controller on VMware vCenter

- [Installation Prerequisites for VMware vCenter, on page 19](#)
- [Install Crosswork Cluster on VMware vCenter, on page 37](#)
- [Install Cisco Crosswork Data Gateway on VMware vCenter, on page 67](#)



CHAPTER 4

Installation Prerequisites for VMware vCenter

This chapter contains the following topics:

- [Overview, on page 19](#)
- [Supported Network Topology Models, on page 19](#)
- [VMware Settings, on page 25](#)
- [Host VM Requirements, on page 26](#)
- [TCP/UDP Port requirements, on page 30](#)
- [IP Address Restrictions, on page 34](#)
- [Supported Web Browsers, on page 36](#)

Overview

This chapter explains the general (such as VM requirements, port requirements, application requirements, etc.) and platform-specific prerequisites to install each Crosswork component.

The data center resources needed to operate other integrated components or applications (such as WAE, DHCP, and TFTP servers) are not addressed in this document. Refer to the respective installation documentation of those components for more details.

Supported Network Topology Models

This section introduces the different topology models supported when deploying Cisco Crosswork and the other solution components on a datacenter using VMware.

Routed and Device Networks

The following table describes the types of traffic that comes from the Crosswork Network Controller. This traffic can use a single NIC (typically in lab installs) or dual NICs.

Table 7: Types of Crosswork Network Traffic

Traffic	Description
Management	For accessing the UI and Crosswork Network Controller command line, and passing information between servers (for example, Cisco Crosswork to Crosswork Data Gateway or NSO).

Traffic	Description
Data	Data and configuration transfer between Cisco Crosswork and Crosswork Data Gateway and other data destinations (external Kafka/gRPC).
Device Access	The device access that the servers (Crosswork, NSO, Crosswork Data Gateway, or others) use to communicate with the managed devices in the network.

Connectivity between the various components should be accomplished via an external routing entity. The Network Topology figures in this section 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.



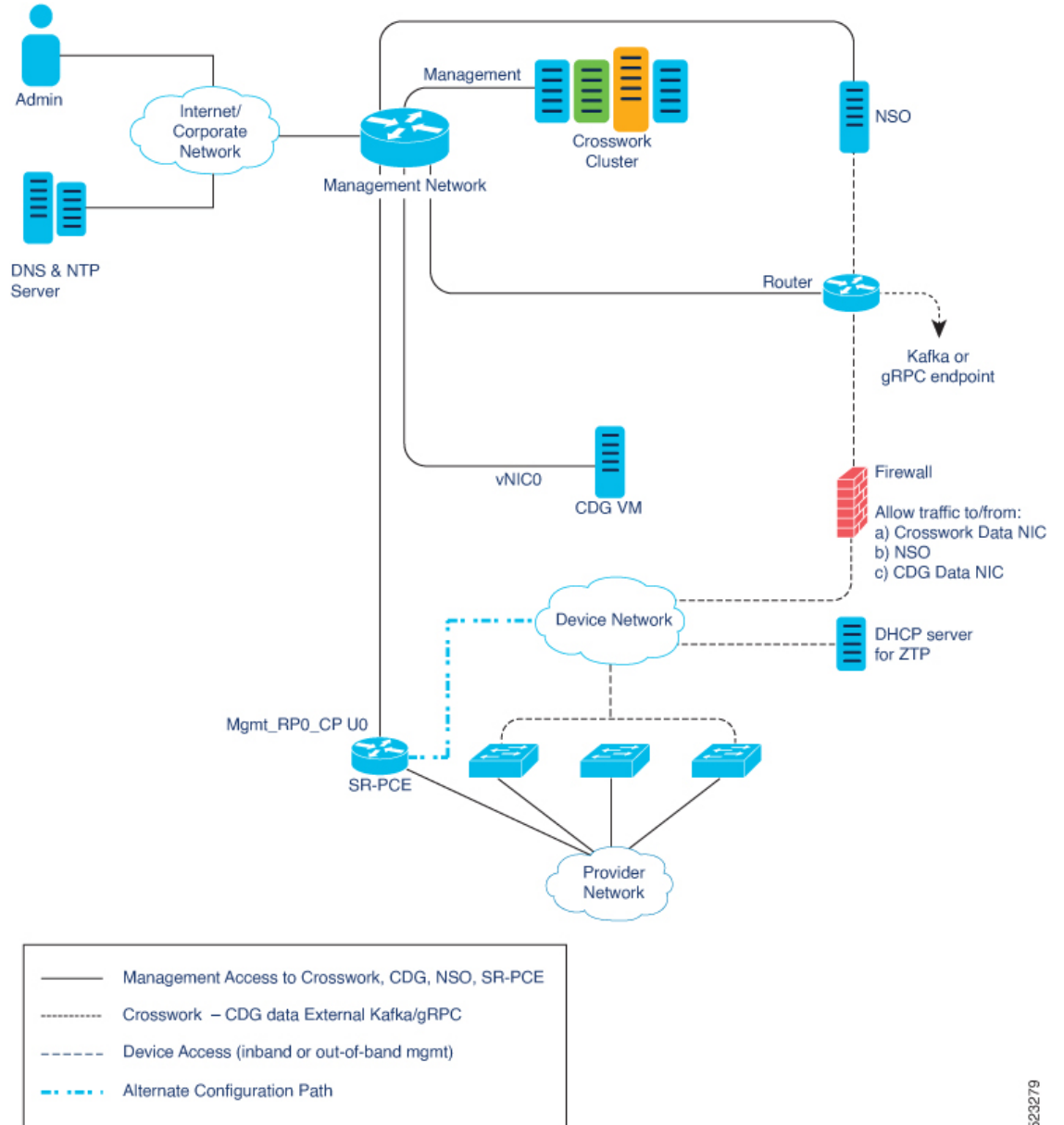
Important

- It is vital to have secure firewalls between Crosswork Network Controller and the network devices. However, the firewalls are not provided by Crosswork Network Controller and must be set up separately by the user. This topic highlights what application flows need to be allowed through the user-provided firewall system.
- 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.

The three supported configurations are:

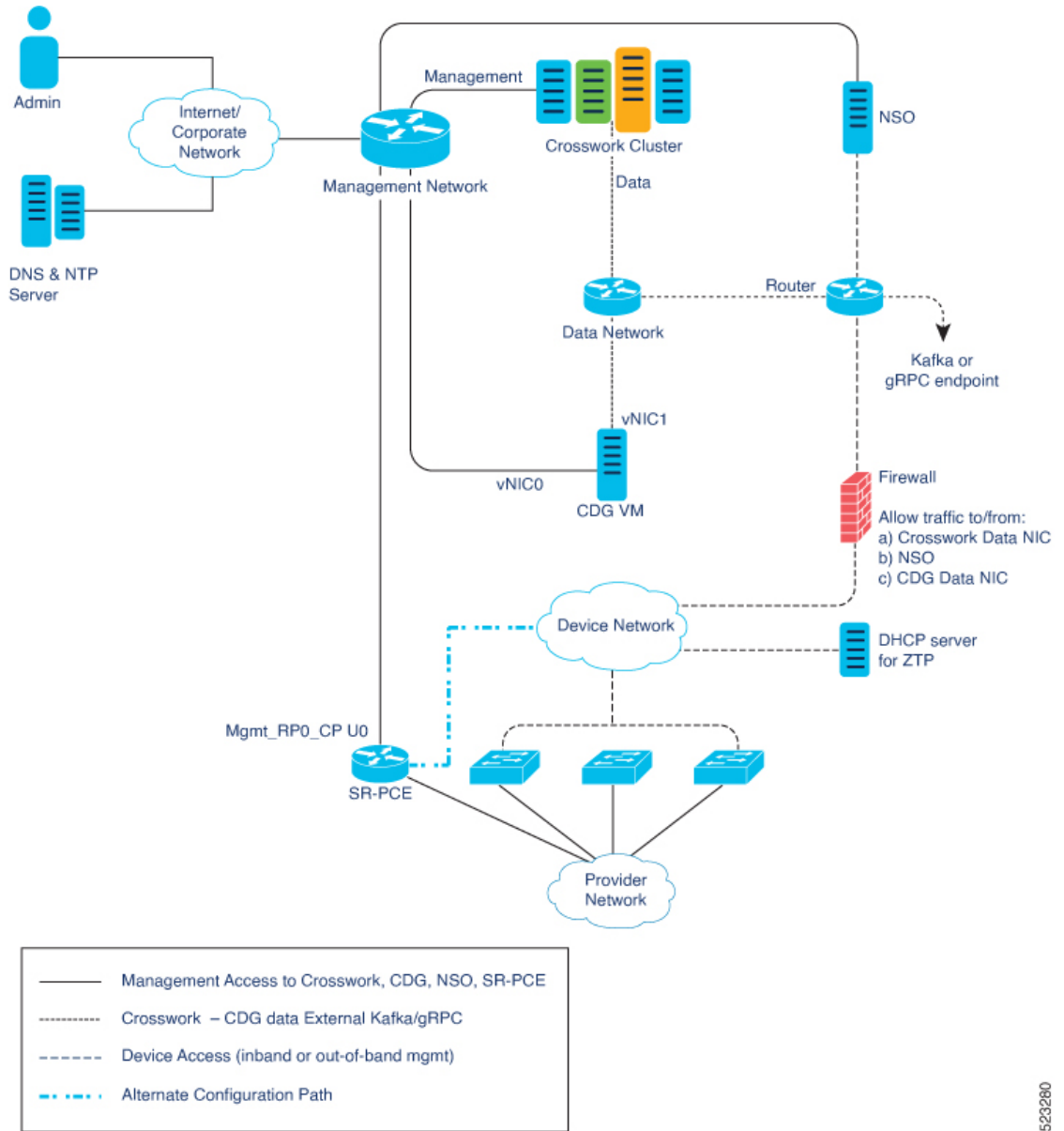
- **1 NIC Network Topology:** The Crosswork cluster, Crosswork Data Gateway, NSO, and SR-PCE use one network interface to communicate between each other and a routed interface to communicate with the network devices.
- **2 NIC Network Topology:** The Crosswork cluster, Crosswork Data Gateway, NSO, and SR-PCE use one network interface to communicate between their management interfaces, a second interface to pass the data between Crosswork Network Controller and Crosswork Data Gateway, and a routed interface to communicate with the network devices.
- **3 NIC Network Topology:** The Crosswork cluster, Crosswork Data Gateway, NSO, and SR-PCE use one network interface to communicate between their management interfaces, a second interface to pass the data between Crosswork Network Controller and Crosswork Data Gateway, and a third interface for Crosswork Data Gateway to communicate with the network devices. NSO may use either the third interface or a routed interface to communicate with the network devices.

Figure 1: Cisco Crosswork - 1 NIC Network Topology



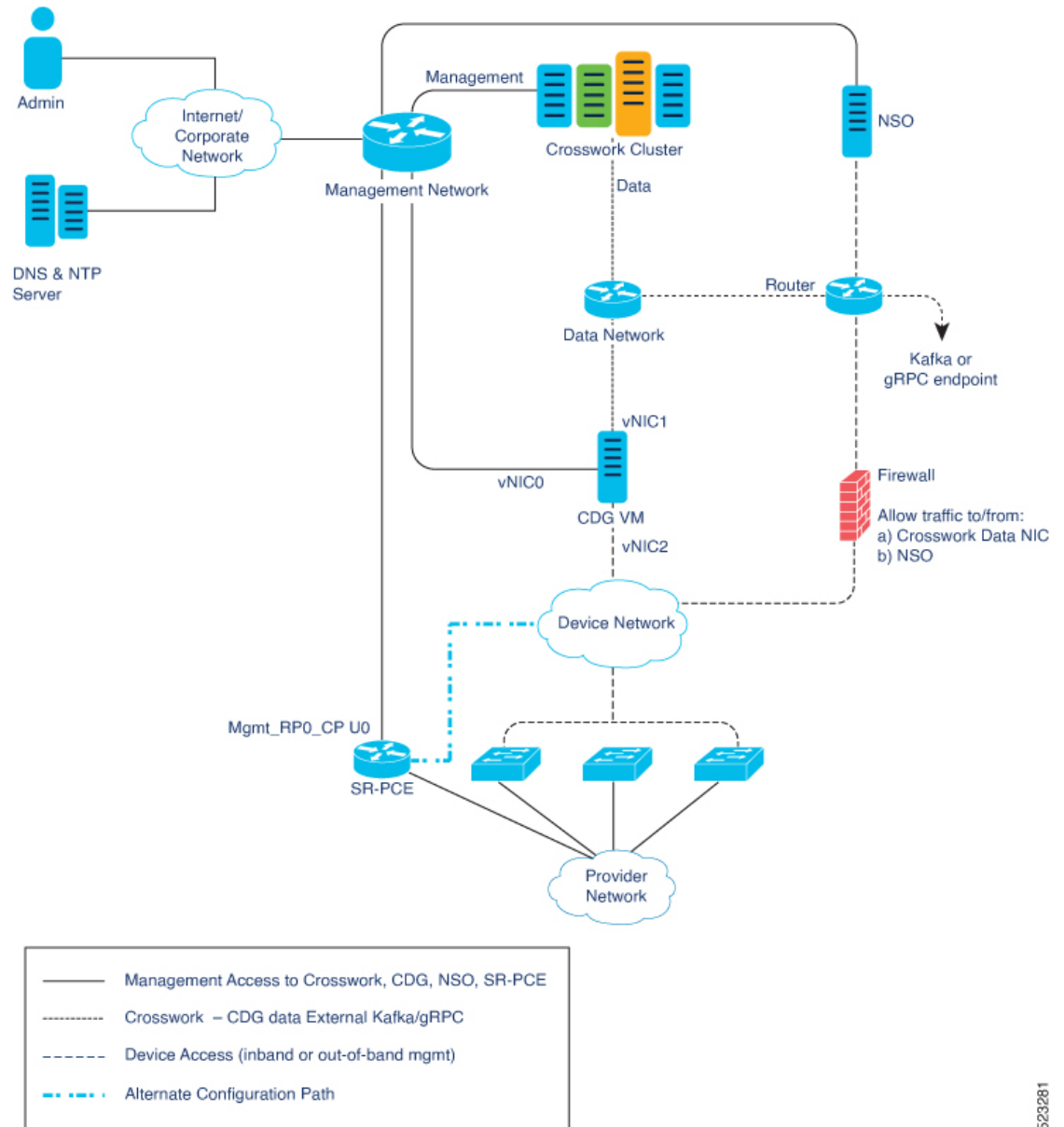
523279

Figure 2: Cisco Crosswork - 2 NIC Network Topology



523260

Figure 3: Cisco Crosswork - 3 NIC Network Topology



523281

Cisco Crosswork Virtual Machine (VM)

The Cisco Crosswork VM has the following vNIC deployment options:

Table 8: Cisco Crosswork vNIC deployment modes

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

No. of vNICs	vNIC	Description
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:



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.

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

Table 9: Cisco Crosswork Data Gateway default vNIC deployment modes

No. of vNICs	vNIC	Type of Traffic
1	vNIC0	Default Gateway, Administration, External Logging, and Management traffic passing through a single NIC.
2	vNIC0	Default Gateway, Administration, External Logging, and Management traffic.
	vNIC1	Control and Northbound External Data traffic.
3	vNIC0	Default Gateway, Administration, External Logging, and Management traffic.
	vNIC1	Control and Northbound External Data traffic.
	vNIC2	Southbound Data traffic

SR-PCE Configuration

The 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). For more information on enabling Crosswork access to an SR-PCE instance as a device on the device network (shown as alternate path in the figures), please refer to [Add Cisco SR-PCE Providers, on page 182](#).

ZTP Requirements

If you plan to use Zero Touch Provisioning, the device network needs to be equipped with a DHCP server (not provided as part of Cisco Crosswork). Some forms of ZTP also require a TFTP server (not provided as part of Cisco Crosswork). Additionally, all devices that use ZTP must have network connectivity to the Crosswork cluster as they will pull files (software and/or configuration) directly from the Crosswork cluster. For more information on Zero Touch Provisioning concepts and features, please refer to the *Zero Touch Provisioning* chapter in the *Cisco Crosswork Network Controller 5.0 Administration Guide*.

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).

VMware Settings

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. For more information on manual installation, see [Manual Installation of Cisco Crosswork using vCenter vSphere UI, on page 52](#).

- Hypervisor and vCenter supported:
 - VMware vCenter Server 7.0 and ESXi 7.0.
 - VMware vCenter Server 6.7 (Update 3g or later) and ESXi 6.7 (Update 1).
- If you plan to use the Crosswork installer tool, the machine where you run the installer must have network connectivity to the vCenter data center where you plan to install the cluster. If this mandatory requirement cannot be met, you must manually install the cluster. For more information on manual installation, see [Manual Installation of Cisco Crosswork using vCenter vSphere UI, on page 52](#).
- Cisco Crosswork cluster VMs (Hybrid nodes and Worker nodes) must be hosted on hardware with Hyper Threading disabled.
- As Cisco Crosswork cluster nodes place high demands on the VMs, ensure that you have not oversubscribed CPU or memory resources on the machines hosting the nodes.
- 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. This prevents the host from being a single point of failure and improves solution resilience.
- The networks required for the Crosswork Management and Data networks need to be built and configured in the data centers, and must allow low latency L2 communication.



Note The same network names must be used and configured on all the ESXi host machines hosting the Crosswork VMs.

- To allow use of VRRP, DVS Port group needs to be set as follows:

Property	Value
Promiscuous mode	Reject
MAC address changes	Reject

To edit the settings in vCenter, navigate to the **Host > Configure > Networking > Virtual Switches**, and select the virtual switch. In the virtual switch, select **Edit > Security** and confirm the settings as suggested. Repeat the process for each virtual switch used in the cluster.

- Ensure the user account you use for accessing vCenter has 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 (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 data center tree level.
- We also recommend you to enable vCenter storage control.

Host VM Requirements

This section explains the resource requirements per VM to deploy the Crosswork Cluster and Crosswork Data Gateway.

- [Crosswork Cluster VM Requirements, on page 26](#)
- [Crosswork Data Gateway VM Requirements, on page 28](#)

Crosswork Cluster VM Requirements

The Crosswork cluster consists of three VMs or nodes operating in a hybrid configuration. This is the minimum configuration necessary to support the applications in a standard network. Additional VMs or nodes (maximum up to 2 worker nodes) in a worker configuration can be added later to scale your deployment, as needed, to match the requirements of your network, or as other applications are introduced (see [Table 2: Crosswork Network Controller packages, on page 6](#) for more information on VM count for each Crosswork Network Controller package). Please consult with the Cisco Customer Experience team for guidance on your deployment to best meet your needs.

The table below explains the network requirements per VM host:

Table 10: Network Requirements (per VM)

Requirement	Description
Network Connections	<p>For production deployments, we recommend that you use dual interfaces, one for the Management network and one for the Data network.</p> <p>For optimal performance, the Management and Data networks should use links configured at a minimum of 10 Gbps.</p>
IP Addresses	<p>When using dual NICs (one for the Management network and one for the Data network): A management and data IP address (IPv4 or IPv6) for each node being deployed (Hybrid or Worker) and two additional IP addresses to be used as the Virtual IP (VIP) address (one for the Management network and one for the Data network).</p> <p>When using single NIC: One IP address (IPv4 or IPv6) for each node being deployed (Hybrid or Worker) and one additional IP address to be used as the Virtual IP (VIP) address.</p> <p>For example, in the case of a cluster with 3 hybrid VMs and 1 worker VM with a single NIC, you need 5 IP addresses, and in the case of the same configuration with dual NIC, you need 10 IP addresses (5 for management network and 5 for data network).</p> <p>Note</p> <ul style="list-style-type: none"> • 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 the Cisco Customer Experience team.
NTP Servers	<p>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.</p> <p>Ensure that the NTP servers are reachable on the network before attempting installation. The installation will fail if the servers cannot be reached.</p>
DNS Servers	<p>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.</p> <p>Ensure that the DNS servers are reachable on the network before attempting installation. The installation will fail if the servers cannot be reached.</p>
DNS Search Domain	<p>The search domain you want to use with the DNS servers, for example, cisco.com. You can have only one search domain.</p>

Requirement	Description
Backup Server	Cisco Crosswork will back up the configuration of the system to an external server using SCP. The SCP server storage requirements will vary slightly but you must have at least 25 GB of storage.

- Cisco Crosswork Infrastructure and applications are built to run as a distributed collection of containers managed by Kubernetes. 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.

Crosswork Data Gateway VM Requirements

This section provides information about the general guidelines and minimum requirements for installing Crosswork Data Gateway.

- [Selecting the Crosswork Data Gateway Deployment Type, on page 28](#)
- [Crosswork Data Gateway VM Requirements, on page 29](#)

Selecting the Crosswork Data Gateway Deployment Type

The following table lists the deployment profile that must be used for installing Crosswork Data Gateway in each Crosswork product:



Note The VM resource requirements for Crosswork Data Gateway are different for each type and cannot be modified. Therefore, if your requirements change, you must re-deploy the Crosswork Data Gateway to move from one type to another. For more information, see the *Redeploy a Crosswork Data Gateway VM* section in [Cisco Crosswork Network Controller 5.0 Administration Guide](#).

Table 11: Crosswork Data Gateway deployment types

Cisco Crosswork Product	Crosswork Data Gateway Deployment
Crosswork Network Controller (combination of Crosswork Active Topology & Crosswork Optimization Engine)	On-Premise Standard
Crosswork Optimization Engine	On-Premise Standard
Crosswork Zero Touch Provisioning	On-Premise Standard
Crosswork Change Automation	On-Premise Extended
Crosswork Health Insights	On-Premise Extended
Crosswork Service Health	On-Premise Extended

Crosswork Data Gateway VM Requirements

The VM requirements for Crosswork Data Gateway are listed in the following table.

Table 12: Crosswork Data Gateway Requirements for on-premise applications

Requirement	Description			
Data Center	VMware. See Installation Prerequisites for VMware vCenter, on page 19 .			
Interfaces	Minimum: 1 Maximum: 3 Cisco Crosswork Data Gateway can be deployed with either 1, 2, and 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.		
	No. of NICs	vNIC0	vNIC1	vNIC2
	1	<ul style="list-style-type: none"> • Management Traffic • Control/Data Traffic • Device Access Traffic 	—	—
	2	Management Traffic	<ul style="list-style-type: none"> • Control/Data Traffic • Device Access Traffic 	—
3	Management Traffic	Control/Data Traffic	Device Access Traffic	
	<ul style="list-style-type: none"> • Management traffic: for accessing the Interactive Console and passing the Control/Data information between servers (for example, a Crosswork application to Crosswork Data Gateway). • 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 access and data collection. 			
Note	Due to security policies, traffic from subnets of a vNIC received on other vNICs is dropped. For example, in a 3 vNIC model setup, all device traffic (incoming and outgoing) must be routed through default vNIC2. Crosswork Data Gateway drops device traffic received over vNIC0 and vNIC1.			

Requirement	Description
IP Addresses	<p>1 or 2 IPv4 or IPv6 addresses based on the number of interfaces you choose to use.</p> <p>An additional IP address to be used as the Virtual IP (VIP) address. For each active data gateway, a unique VIP is required.</p> <p>For more information, refer to the <i>Interfaces</i> section in the Table 24: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 69.</p> <p>Note Crosswork does not support dual stack configurations. Therefore, all addresses for the environment must be either IPv4 or IPv6.</p> <p>In a 3-NIC deployment, you need to provide an IP address for Management interface (vNIC0) and Control/Data interface (vNIC1) during installation. A virtual IP address for Device Access Traffic (vNIC2) is assigned when you create a Crosswork Data Gateway to a pool as explained in the <i>Create a Crosswork Data Gateway Pool</i> section in Cisco Crosswork Network Controller 5.0 Administration Guide.</p>
NTP Servers	<p>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 devices, clients, and servers across your network. Verify that the NTP IP address or host name is reachable on the network else the installation fails.</p> <p>Also, the ESXi hosts that 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.</p>
DNS Servers	<p>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 fails if the servers cannot be reached.</p>
DNS Search Domain	<p>The search domain you want to use with the DNS servers, for example, cisco.com. You can have only one search domain.</p>
Internet Control Message Protocol (ICMP)	<p>The Crosswork uses ICMP in the communications with Crosswork Data Gateway. Ensure that the firewall between Crosswork and the Crosswork Data Gateway passes this traffic.</p>

TCP/UDP Port requirements

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



Note All IP addresses (including Virtual IP addresses) between Crosswork Cluster, Crosswork applications, and Crosswork Data Gateway need to be reachable (to be pinged to/from) between each other.

Crosswork Cluster Port Requirements

The following TCP/UDP port numbers need to be allowed through any external firewall or access-list rules deployed by the data center administrator. Depending on the NIC deployment, these ports may be applicable to only one or both NICs.



Note Crosswork cluster ports allow bidirectional flow of information.

Table 13: External Ports used by Crosswork Cluster

Port	Protocol	Used for	Location (in 2 NIC deployment)
22	TCP	Remote SSH traffic	Management Network / vNIC0
111	TCP/UDP	GlusterFS (port mapper)	Management Network / vNIC0
179	TCP	Calico BGP (Kubernetes)	Management Network / vNIC0
80, 443	TCP	Accessing the EC2 API	Management Network / vNIC0
500	UDP	IPSec	Management Network / vNIC0
2379/2380	TCP	Kubernetes etcd	Management Network / vNIC0
4500	UDP	IPSec	Management Network / vNIC0
6443	TCP	kube-apiserver (Kubernetes)	Management Network / vNIC0
9100	TCP	Kubernetes metamonitoring	Management Network / vNIC0
10250	TCP	kubelet (Kubernetes)	Management Network / vNIC0
24007	TCP	GlusterFS	Management Network / vNIC0
30603	TCP	User interface (NGINX server listens for secure connections on port 443)	Management Network / vNIC0
30606	TCP	Docker Registry	Management Network / vNIC0
30621	TCP	For FTP (available on data interface only). The additional ports used for file transfer are 31121 (TCP), 31122 (TCP), and 31123 (TCP). This port is available only when the supported application is installed on Cisco Crosswork and the FTP settings are enabled.	Management Network / vNIC0
30622	TCP	For SFTP (available on data interface only) This port is available only when the supported application is installed on Cisco Crosswork and the SFTP settings are enabled.	Management Network / vNIC0
49152 49370	TCP	GlusterFS	Management Network / vNIC0

Table 14: Ports used by other Crosswork components

Port	Protocol	Used for	Location (in 2 NIC deployment)
30602	TCP	To monitor the installation (Crosswork Network Controller)	Management Network / vNIC0
30603	TCP	Crosswork Network Controller Web User interface (NGINX server listens for secure connections on port 443)	Management Network / vNIC0
30604	TCP	Used for Classic Zero Touch Provisioning (Classic ZTP) on the NGINX server	Management Network / vNIC0
30607	TCP	Crosswork Data Gateway vitals collection	Data Network / vNIC1
30608	TCP	Data Gateway gRPC channel with Data Gateway VMs	Data Network / vNIC1
30609	TCP	Used by the Expression Orchestrator (Crosswork Service Health)	Management Network / vNIC0
30610	TCP	Used by the Metric Scheduler (Crosswork Service Health)	Management Network / vNIC0
30611	TCP	Used by the Expression Tracker component (Crosswork Service Health)	Management Network / vNIC0
30617	TCP	Used for Secure Zero Touch Provisioning (Secure ZTP) on the ZTP server	Management Network / vNIC0
30620	TCP	Used to receive plug-and-play HTTP traffic on the ZTP server	Management Network / vNIC0
30649	TCP	To set up and monitor Crosswork Data Gateway collection status	Data Network / vNIC1
30650	TCP	The astack gRPC channel with astack-client running on Data Gateway VMs	Data Network / vNIC1
30993, 30994, 30995	TCP	Crosswork Data Gateway sending the collected data to Crosswork Kafka destination	Data Network / vNIC1

Table 15: Destination Ports used by Crosswork Cluster

Port	Protocol	Used for	Location (in 2 NIC deployment)
7	TCP/UDP	Discover endpoints using ICMP	Management Network / vNIC0
22	TCP	Initiate SSH connections with managed devices	Management Network / vNIC0
53	TCP/UDP	Connect to DNS	Management Network / vNIC0
123	UDP	Network Time Protocol (NTP)	Management Network / vNIC0

Port	Protocol	Used for	Location (in 2 NIC deployment)
830	TCP	Initiate NETCONF	Management Network / vNIC0
2022	TCP	Used for communication between Crosswork and Cisco NSO (for NETCONF)	Management Network / vNIC0
8080	TCP	REST API to SR-PCE	Management Network / vNIC0
8888	TCP	Used for communication between Crosswork and Cisco NSO (for HTTPS)	Management Network / vNIC0
20243	TCP	Used by the DLM Function Pack for communication between DLM and Cisco NSO	Management Network / vNIC0
20244	TCP	Used to internally manage the DLM Function Pack listener during a Reload Packages scenario on Cisco NSO	Management Network / vNIC0

Crosswork Data Gateway Port Requirements

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

Inbound: Crosswork Data Gateway listens on the specified ports.

Outbound: Crosswork Data Gateway connects to external destination IP on the specified ports.

Table 16: 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



Note SCP port can be tuned.

Table 17: Ports to be Opened for Device Access Traffic

Port	Protocol	Used for	Direction
161	UDP	SNMP Collector	Outbound

Port	Protocol	Used for	Direction
1062	UDP	SNMP Trap Collector This is the default value. You can change this value after installation from the Cisco Crosswork UI. See Configure Crosswork Data Gateway Global Parameters for more information.	Inbound
9010	TCP	MDT Collector	Inbound
22	TCP	CLI Collector	Outbound
6514	TLS	Syslog Collector	Inbound
9898	TCP	This is the default value. You can change this value after installation from the Cisco Crosswork UI. See Configure Crosswork Data Gateway Global Parameters for more information.	
9514	UDP		
Site Specific Check the platform-specific documentation.	TCP	gNMI Collector	Outbound

Table 18: Ports to be Opened for Control/Data Traffic

Port	Protocol	Used for	Direction
30649	TCP	Crosswork Controller	Outbound
30993 30994 30995	TCP	Crosswork Kafka	Outbound
Site Specific	Site Specific	Kafka and gRPC Destination	Outbound

IP Address Restrictions

Crosswork cluster uses the following IP ranges for internal communications. This cannot be changed. As a result, these subnets cannot be used for devices or other purposes within your network.

You are recommended to isolate your Crosswork cluster to ensure all the communications stay within the cluster. Please also ensure that address spaces do not overlap for any of the external integration points (e.g. connections to devices, connections to external servers that Crosswork is sending data to, connections to the NSO server, etc.).



Note This is applicable for cluster installation and for adding a static route.

Table 19: Protected IP Subnets

IP Type	Subnet	Remarks
IPv4	172.17.0.0/16	Docker Subnet (Infrastructure)
	169.254.0.0/16	Link local address block
	127.0.0.0/8	Loopback address
	192.88.99.0/24	Reserved, previously used for relay servers to do IPv6 over IPv4
	240.0.0.0/4	Reserved for future use (previously class E block)
	224.0.0.0/4	MCAST-TEST-NET
	0.0.0.0/8	Current network, valid as source address only
IPv6	2001:db8:1::/64	Docker Subnet (Infrastructure)
	fdfb:85ef:26ff::/48	Pod Subnet (Infrastructure)
	fd08:2eef:c2ee::/110	Service Subnet (Infrastructure)
	::1/128	Loopback address
	fe80::/10	Link local
	ff00::/8	IPv6 Multicast
	2002::/16	Reserved, previously used for relay servers to do IPv6 over IPv4
	2001:0000::/32	Terredo tunnel and relay
	2001:20::/28	Used by ORCHID and not IPv6 routable
	100::/64	Discard prefix, used in specific use-cases not applicable to Crosswork Zero Touch Provisioning
	::/128	Unspecified address, cannot be assigned to hosts
	::ffff:0:0/96	IPv4 mapped addresses
	::ffff:0:0:0/96	IPv4 translated addresses

Supported Web Browsers

To access the Crosswork UI after installing the infrastructure, we recommend using either of the browsers which have been validated:

Table 20: Supported Web Browsers

Browser	Version
Google Chrome (recommended)	92 or later
Mozilla Firefox	70 or later

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

In addition to using a supported browser, all client desktops accessing geographical maps in the Crosswork applications must be able to reach the mapbox.com site. Customers not wishing to have Cisco Crosswork access an external site can choose to install the map files locally.

What to do next:

Return to the installation workflow: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)



CHAPTER 5

Install Crosswork Cluster on VMware vCenter

This chapter contains the following topics:

- [Installation Overview, on page 37](#)
- [Installation Parameters, on page 37](#)
- [Install Cisco Crosswork on VMware vCenter using Cluster Installer Tool , on page 42](#)
- [Manual Installation of Cisco Crosswork using vCenter vSphere UI, on page 52](#)
- [Monitor the Installation, on page 62](#)
- [Log into the Cisco Crosswork UI, on page 64](#)

Installation Overview

Crosswork Network Controller Crosswork Cluster can be installed using the following methods:

Crosswork Cluster can be installed using the following methods:

- **Installation using Installer:** The cluster installer tool 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.
- **Manual Installation (via the VMware UI):** This option is available for deployments that cannot use the installer tool.

The installer tool method is the preferred option as it is faster and easier to use.



Note Secure ZTP and Secure Syslog require the Crosswork cluster to be deployed with FQDN.

Installation Parameters

This section explains the important parameters that must be specified while installing the Crosswork cluster. Kindly ensure that you have relevant information to provide for each of the parameters mentioned in the table and that your environment meets all the requirements specified under [Installation Prerequisites for VMware vCenter, on page 19](#).



Note Some of the below parameters may be named differently depending upon the installation method (automated or manual) and IP stack (IPv4 or IPv6) you choose.



Attention Please use the latest template file that comes with the Crosswork installer tool.

Table 21: General parameters

Parameter Name	Description
ClusterName	Name of the cluster file
ClusterIPStack	The IP stack protocol: IPv4 or IPv6
ManagementIPAddress	The Management IP address of the VM (IPv4 or IPv6).
ManagementIPNetmask	The Management IP subnet in dotted decimal format (IPv4 or IPv6).
ManagementIPGateway	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.
ManagementVIPName	Name of the Management Virtual IP for the cluster. This is an optional parameters used to reach Crosswork cluster Management VIP via DNS name. If this parameter is used, the corresponding DNS record must exist in the DNS server and must match the ManagementVIP and ManagementVIPName.
DataIPAddress	The Data IP address of the VM (IPv4 or IPv6).
DataIPNetmask	The Data IP subnet in dotted decimal format (IPv4 or IPv6).
DataIPGateway	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.
DataVIPName	Name of the Data Virtual IP for the cluster. This is an optional parameters used to reach Crosswork cluster Data VIP via DNS name. If this parameter is used, the corresponding DNS record must exist in the DNS server and must match the DataVIP and DataVIPName.
DNS	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	The domain name used for the cluster.

Parameter Name	Description
CWusername	Username to log into Cisco Crosswork. This is an optional parameter.
CWPassword	Password to log into Cisco Crosswork. Use a strong VM Password (8 characters long, including upper & lower case letters, numbers, and one special character). Avoid using passwords similar to dictionary words (for example, "Pa55w0rd!") or relatable words (for example, C!sco123 or Cwork321!). While they satisfy the criteria, such passwords are weak and will result in the failure of VM setup.
VMSize	VM size for the cluster. Value is <code>large</code> .
VMName	Name of the VM You will require at least 3 unique names (one for each VM). See
NodeType	Indicates the type of VM. Choose either "Hybrid" or "Worker". Note The Crosswork cluster for 5.0 release requires at least three VMs operating in a hybrid configuration.
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. This parameter is optional for installing using the cluster installer tool.
InitNodeCount	Total number of nodes in the cluster including Hybrid and Worker nodes. The default value is 3. Set this to match the number of VMs (nodes) you are going to deploy. For more information on VM count, see Table 2: Crosswork Network Controller packages, on page 6 . This parameter is optional for installing using the cluster installer tool.
InitMasterCount	Total number of Hybrid nodes in the cluster. The default value is 3. This parameter is optional for installing using the cluster installer tool.
BackupMinPercent	Minimum percentage of the data disk space to be used for the size of the backup partition. The default value is 50 (valid range is from 1 to 80). Please use the default value unless recommended otherwise. Note The final backup partition size will be calculated dynamically. This parameter defines the minimum.
ManagerDataFsSize	Refers to the data disk size for Hybrid nodes (in Giga Bytes). This is an optional parameter and the default value is 450 (valid range is from 450 to 8000), if not explicitly specified. Please use the default value unless recommended otherwise.

Parameter Name	Description
WorkerDataFsSize	Refers to the data disk size for Worker nodes (in Gigabytes). This is an optional parameter and the default value is 450 (valid range is from 450 to 8000), if not explicitly specified. Please use the default value unless recommended otherwise.
ThinProvisioned	Set to "false" for production deployments.
EnableHardReservations	Determines the enforcement of VM CPU and Memory profile reservations (see Installation Prerequisites for VMware vCenter, on page 19 for more information). This is an optional parameter and the default value is <code>true</code> , if not explicitly specified. If set as <code>true</code> , the VM's resources are provided exclusively. In this state, the installation will fail if there are insufficient CPU cores, memory or CPU cycles. If set as <code>false</code> (only set for lab installations), the VM's resources are provided on best efforts. In this state, the installation will fail if there are insufficient CPU cores.
RamDiskSize	Size of the Ram disk. This parameter is only used for lab installations (value must be at least 2). When a non-zero value is provided for <code>RamDiskSize</code> , the <code>HSDatastore</code> value is not used.
OP_Status	This optional parameter is used (uncommented) to import inventory post manual deployment of Crosswork cluster. The parameter refers to the state for this VM. To indicate a running status, the value must be 2 (<code>#OP_Status = 2</code>).
SchemaVersion	The configuration Manifest schema version. Schema version should map to the version packaged with sample template in installer tool.
LogFsSize	Log partition size (in Giga Bytes). Minimum value is 10 GB and Maximum value is 1000 GB. You are recommended to use the default value.
Timezone	Enter the timezone. Input is a standard IANA time zone (for example, "America/Chicago"). If left blank, the default value (UTC) is selected. This is an optional parameter. Note The timestamp in Kafka log messages represents the NSO server time. If you change the <code>Timezone</code> parameter in Crosswork without updating the NSO server time, there will be a mismatch between the Crosswork server time and the NSO event time.

Parameter Name	Description
EnableSkipAutoInstallFeature	Any pods marked as skip auto install will not be brought up until a dependent application/pod explicitly asks for it. If left blank, the default value ("False") is selected.
EnforcePodReservations	Enforces minimum resource reservations for the pod. If left blank, the default value ("True") is selected.
K8sServiceNetwork	The network address for the kubernetes service network. The CIDR range is fixed to '/16'. This is an optional parameter.
K8sPodNetwork	The network address for the kubernetes pod network. The CIDR range is fixed to '/16'. This is an optional parameter.

Table 22: VMware template parameters

Parameter Name	Description
vCentreAddress	The vCenter IP or host name.
vCentreUser	The username needed to log into vCenter.
vCentrePassword	The password needed to log into vCenter.
DCname	The name of the Data Center resource to use. Example: DCname = "WW-DCN-Solutions"
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 ONLY the vcenter cluster/resource group name where the VM is to be deployed. The primary option is to use the host IP or name (all the hosts should be under the Datacentre). If the hosts are under a cluster in the Datacentre, only provide the cluster name (all hosts within the cluster will be picked up). The subsequent option is to use a resource group. In this case, a full path should be provided. Example: Host = "Main infrastructure/Resources/00_trial"
Datastore	The datastore name available to be used by this host or resource group. The primary option is to use host IP or name. The subsequent option is to use a resource group. Example: Datastore = "SDRS-DCNSOL-prodexsi/bru-netapp-01_FC_Prodesx_ds_15"

Parameter Name	Description
HSDatastore	The high speed datastore available for this host or resource group. When not using a highspeed data store, set to same value as Datastore.
DCfolder	The resource folder name on vCenter. To be used if you do not have root access as a VMware user, or when you need to create VMs in separate folders for maintenance purposes. You must provide the complete path as value for the DCfolder. Example: DCfolder = "/WW-DCN-Solutions/vm/00_trial" Please contact your VMware administrator for any queries regarding the complete folder path. Leave as empty if not used.
Cw_VM_Image	The name of Crosswork cluster VM image in vCenter.
HostedCwVMs	The IDs of the VMs to be hosted by the ESXi host or resource.

After you have decided the installation parameters values for Crosswork Network Controller, choose the method you prefer and begin your deployment:

- [Install Cisco Crosswork on VMware vCenter using Cluster Installer Tool](#) , on page 42
- [Manual Installation of Cisco Crosswork using vCenter vSphere UI](#), on page 52

Install Cisco Crosswork on VMware vCenter using Cluster Installer Tool

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



Note The time taken to create the cluster can vary based on the size of your deployment profile and the performance characteristics of your hardware.

Before you begin

Few pointers to know when using the cluster installer tool:

- Make sure that your environment meets all the vCenter requirements specified in [Installation Prerequisites for VMware vCenter](#), on page 19.
- The edited template in the /data directory will contain sensitive information (VM passwords and the vCenter password). The operator needs to manage access to this content. Store them in a secure environment or edit them to remove the passwords.

- 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.
- The install script is safe to run multiple times. Upon error, input parameters can be corrected and re-run. You must remove the `install.log`, `install_tf.log`, and `tfstate` files before each re-run. Please note that running the tool multiple times may result in the deletion and re-creation of VMs.
- 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 the deployment state files to be independent. The simplest way for doing so is to create a local directory for each deployment on the host machine and map each one to the container accordingly.
- Docker version 19 or higher is required while using the cluster installer option. For more information on Docker, see <https://docs.docker.com/get-docker/>
- 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 Crosswork 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. For more information, see [Delete the VM using the Cluster Installer, on page 215](#).
- A VM redeployment will delete the VM's data, hence caution is advised. We recommend you perform VM parameter changes from the Crosswork 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.

Known limitations:

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

- The vCenter host VMs defined must use the same network names (vSwitch) across all hosts in the data center.
- The vCenter storage folders or datastores organized under a virtual folder structure, are not supported currently. Please ensure that the datastores referenced are not grouped under a folder.
- 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. When making modifications after the initial deployment of the cluster, ensure that you capture the inventory information. For more information, see the *Manage Clusters* chapter in the *Crosswork Network Controller 5.0 Administration Guide*.
- 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.



Note The installer tool will deploy the software and power on the virtual machines. If you wish to power on the virtual machines yourself, use the manual installation.

Step 1 In your vCenter datacenter, go to **Host > Configure > Networking > Virtual Switches** and select the virtual switch. In the virtual switch, select **Edit > Security**, and configure the following DVS port group properties:

- Set **Promiscuous mode** as *Reject*
- Set **MAC address changes** as *Reject*

Confirm the settings and repeat the process for each virtual switch used in the cluster.

Step 2 In your Docker capable machine, create a directory where you will store everything you will use during this installation.

Note If you are using a Mac, please ensure that the directory name is in lower case.

Step 3 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-5.0.0-signed-installer.tar.gz** and **cw-na-platform-5.0.0-81-release-230502.ova** respectively.

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

Step 4 Use the following command to unzip the installer bundle:

```
tar -xvf cw-na-platform-5.0.0-signed-installer.tar.gz
```

The contents of the installer bundle is unzipped to a new directory (e.g. `cw-na-platform-5.0.0-signed-installer`). This new directory will contain the installer image (**cw-na-platform-installer-5.0.0-81-release-230502.tar.gz**) and files necessary to validate the image.

Step 5 Change the directory to the directory created by opening the file and then review the contents of the README file in order to understand everything that is in the package and how it will be validated in the following steps.

Step 6 Use the following command to verify the signature of the installer image:

Note Use `python --version` to find out the version of python on your machine.

If you are using python 2.x, use the following command to validate the file:

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

If you are using python 3.x, use the following command to validate the file:

```
python cisco_x509_verify_release.py3 -e <.cer file> -i <.tar.gz file> -s <.tar.gz.signature file>
-v dgst -sha512
```

Note If you do not have python installed, go to python.org and download the version of python that is appropriate for your work station.

Step 7 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-5.0.0-81-release-230502.tar.gz
```

Step 8

Run Docker image list or Docker images command to get the "image ID" (which is needed in the next step).

For example:

```
docker images
```

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

```
My Machine% docker images
REPOSITORY              TAG                IMAGE ID
CREATED                SIZE
dockerhub.cisco.com/cw-installer  cw-na-platform-installer-5.0.0-81-release-230502  a4570324fad30
  7 days ago          276MB
```

Note Pay attention to the "CREATED" time stamp in the table presented when you run `docker images`, as you might have other images present from the installation of prior releases. If you wish to remove these, the `docker image rm {image id}` command can be used.

Step 9

Launch the Docker container using the following command:

```
docker run --rm -it -v `pwd`:/data {image id of the installer container}
```

To run the image loaded in our example, the command would be:

```
docker run --rm -it -v `pwd`:/data a4570324fad30
```

- Note**
- You do not have to enter that full value. In this case, "docker run --rm -it -v `pwd`:/data a45" was adequate. Docker requires enough of the image ID to uniquely identify the image you want to use for the installation.
 - In the above command, we are using the backtick (`). Do not use the single quote or apostrophe (') as the meaning to the shell is very different. By using the backtick (recommended), the template file and OVA will be stored in the directory where you are on your local disk when you run the commands, instead of inside the container.
 - 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, using the following method:
 - **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>
```
 - 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>
```

Note The Docker command provided will use the current directory to read the template and the ova files, and to write the log files used during the install. If you encounter either of the following errors you should move the files to a directory where the path is in lowercase (all lowercase, no spaces or other special characters).

Error 1:

```
% docker run --rm -it -v `pwd`:/data a45
docker: invalid reference format: repository name must be lowercase.
See 'docker run --help'
```

Error 2:

```
docker: Error response from daemon: Mounts denied: approving /Users/Desktop: file does
not exist
ERRO[0000] error waiting for container: context canceled
```

Step 10 Navigate to the directory with the VMware template.
`cd /opt/installer/deployments/5.0.0/vcentre`

Step 11 Copy the template file found under
`/opt/installer/deployments/5.0.0/vcentre/deployment_template_tfvars` to the `/data` folder using a different name.

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

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

Step 12 Edit the template file located in the `/data` directory in a text editor, to match your planned deployment. Refer to the [Installation Parameters, on page 37](#) table for details on the required and optional fields and their proper settings. The [Sample manifest template for VMware vCenter, on page 47](#) includes an example that you can reference for proper formatting. The example is more compact due to the removal of descriptive comments:

Step 13 From the `/opt/installer` directory, 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-5.0.0-81-release-230502.ova
```

Step 14 Read, and then enter "yes" if you accept the End User License Agreement (EULA). Otherwise, exit the installer and contact your Cisco representative.

Step 15 Enter "yes" when prompted to confirm the operation.

Note It is not uncommon to see some warnings like the following during the install:

```
Warning: Line 119: No space left for device '8' on parent controller '3'.
Warning: Line 114: Unable to parse 'enableMPTSupport' for attribute 'key' on element 'Config'.
```

If the install process proceeds to a successful conclusion (see sample output below), these warnings can be ignored.

Sample output:

```

cw_cluster_vms = <sensitive>
INFO: Copying day 0 state inventory to CW
INFO: Waiting for deployment status server to startup on 10.90.147.66. Elapsed time 0s,
retrying in 30s
Crosswork deployment status available at
http://{VIP}:30602/d/NK1bwVxGk/crosswork-deployment-readiness?orgId=1&refresh=10s&theme=dark

Once deployment is complete login to Crosswork via: https://{VIP}:30603/#/logincontroller
INFO: Cw Installer operation complete.
```

Note If the installation fails due to a timeout, you should try rerunning the installation (step 13) without the `-p` option. This will deploy the VMs serially rather than in parallel.

If the installer fails for any other reason (for example, mistyped IP address), correct the error and rerun the install script.

If the installation fails (with or without the `-p`), open a case with Cisco and provide the `.log` files that were created in the `/data` directory (and the local directory where you launched the installer docker container), to Cisco for review. The two most common reasons for the install to fail are: (a) password that is not adequately complex, and (b) errors in the template file.

What to do next

- See [Monitor the Installation, on page 62](#) to know how you can check the status of the installation.
- See [Troubleshoot the Cluster, on page 49](#) for common troubleshooting scenarios.

Return to the installation workflow: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)

Sample manifest template for VMware vCenter

The following example deploys a Crosswork cluster containing 3 Hybrid nodes (IDs 0,1, 2) and 2 worker nodes (IDs 3, 4).



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
*****
```

```

ClusterIPStack = "IPv4"
ManagementVIP = "172.25.87.94"
ManagementIPNetmask = "255.255.255.192"
ManagementIPGateway = "172.25.87.65"
DataVIP = "192.168.123.94"
DataIPNetmask = "255.255.255.0"
DataIPGateway = "0.0.0.0"
DNS = "171.70.168.183"
DomainName = "cisco.com"
CWPassword = "*****"
VMSize = "Large"
NTP = "ntp.cisco.com"
CloneTimeOut = 90
ManagerDataFsSize = 450
ThinProvisioned = true
BackupMinPercent = 50
EnableHardReservations = false
ManagerDataFsSize = 450
WorkerDataFsSize = 450

CwVMs = {
  "0" = {
    VMName = "vm0",
    ManagementIPAddress = "172.25.87.82",
    DataIPAddress = "0.0.0.0",
    DataIPAddress = "192.168.123.82",
    NodeType = "Hybrid"
  },
  "1" = {
    VMName = "vm1",
    ManagementIPAddress = "172.25.87.83",
    DataIPAddress = "0.0.0.0",
    DataIPAddress = "192.168.123.83",
    NodeType = "Hybrid"
  },
  "2" = {
    VMName = "vm2",
    ManagementIPAddress = "172.25.87.84",
    DataIPAddress = "0.0.0.0",
    DataIPAddress = "192.168.123.84",
    NodeType = "Hybrid"
  },
  "3" = {
    VMName = "vmworker0",
    ManagementIPAddress = "172.25.87.85",
    DataIPAddress = "0.0.0.0",
    DataIPAddress = "192.168.123.84",
    NodeType = "Worker"
  },
  "4" = {
    VMName = "vmworker1",
    ManagementIPAddress = "172.25.87.86",
    DataIPAddress = "0.0.0.0",
    DataIPAddress = "192.168.123.86",
    NodeType = "Worker"
  },
}

/***** vCentre Resource Data with Cw VM assignment *****/

```

```

VCenterDC = {
  VCenterAddress = "172.25.87.90",
  VCenterUser = administrator@vsphere.local,
  VCenterPassword = "*****",
  DCname = "dc-cr",
  MgmtNetworkName = "VM Network",
  DataNetworkName = "DPortGroup10",
  VMs = [
    {
      HostedCwVMs = [
        "0",
        "1",
        "2",
        "3", "4"
      ],
      Host = "172.25.87.93",
      Datastore = "datastore3",
      HSDatastore = "datastore3",
    },]
}

```

Set seed node explicitly

The cluster installer tool, by default, selects the first VM (VM 0) as the seed node. You can set the seed node explicitly by adding the following section to the manifest template (.tfvars file) indicating the unique key of the seed node.



Note You are recommended not to modify the default seed node value unless advised to do so by the Cisco Customer Experience team.

```

cluster_settings = {
#Default Minimum number of nodes in inventory
  min_inventory = 3
#Default Max number of nodes in inventory
  max_inventory = 9
#Default Min number of manager nodes
  min_mgr_nodes = 2
#Default Max number of manager nodes
  max_mgr_nodes = 3
#Default seed node key name
  default_seed_node = "0"
}

```

Troubleshoot the Cluster

By default, the installer displays progress data on the command line. The install log is fundamental in identifying the problems, and it is written into the /data directory.

Scenario	Possible Resolution
Missing or invalid parameters	<p>The installer provides a clue as regards to the issue; however, in case of errors in the manifest file HCL syntax, these can be misleading. If you see "Type errors", check the formatting of the configuration manifest.</p> <p>The manifest file can also be passed as a simple JSON file. Use the following converter to validate/convert: https://www.hcl2json.com/</p>
Certificate Error	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.
Image upload takes a long time or upload is interrupted.	The image upload duration depends on the link and datastore performance and can be expected to take around 10 minutes or more. If an upload is interrupted, the user needs 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 Installation Prerequisites for VMware vCenter , on page 19.
Floating VIP address is not reachable	The VRRP protocol requires unique router_id advertisements 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. A symptom of conflict, if it arises, 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 log in	The password specified is not strong enough. Change the configuration manifest and redeploy.
<p>Error conditions such as:</p> <p><i>Error: Error locking state: Error acquiring the state lock: resource temporarily unavailable</i></p> <p><i>Error: error fetching virtual machine: vm not found</i></p> <p><i>Error: Invalid index</i></p>	<p>These errors are common when re-running the installer after an initial run is interrupted (Control C, or TCP timeout, etc). Remediation steps are:</p> <ol style="list-style-type: none"> 1. Run the clean operation (<code>./cw-installer.sh clean -m <your manifest here></code>) OR remove the VM files manually from the vCenter. 2. Remove the state file (<code>rm /data/crosswork-cluster.tfstate</code>) and retry.
Deployment fails with: <i>Failed to validate Crosswork cluster initialization.</i>	<p>The clusters' seed VM is either unreachable or one or more of the cluster VMs have failed to get properly configured.</p> <ol style="list-style-type: none"> 1. Check whether the VM is reachable, and collect logs from <code>/var/log/firstBoot.log</code> and <code>/var/log/vm_setup.log</code> 2. Check the status of the other cluster nodes.

Scenario	Possible Resolution																				
<p>The VMs are deployed but the Crosswork cluster is not being formed.</p>	<p>A successful deployment allows the operator logging in to the VIP or any cluster IP address to run the following command to get the status of the cluster:</p> <pre>sudo kubectl get nodes</pre> <p>A healthy output for a 3-node cluster is:</p> <table border="1"> <thead> <tr> <th>NAME</th> <th>STATUS</th> <th>ROLES</th> <th>AGE</th> <th>VERSION</th> </tr> </thead> <tbody> <tr> <td>172-25-87-2-hybrid.cisco.com</td> <td>Ready</td> <td>master</td> <td>41d</td> <td>v1.16.4</td> </tr> <tr> <td>172-25-87-3-hybrid.cisco.com</td> <td>Ready</td> <td>master</td> <td>41d</td> <td>v1.16.4</td> </tr> <tr> <td>172-25-87-4-hybrid.cisco.com</td> <td>Ready</td> <td>master</td> <td>41d</td> <td>v1.16.4</td> </tr> </tbody> </table> <p>In case of a different output, collect the following logs: /var/log/firstBoot.log and /var/log/vm_setup.log</p> <p>In addition, for any cluster nodes not displaying the Ready state, collect:</p> <pre>sudo kubectl describe node <name of node></pre>	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
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																	
<p>The following error is displayed while uploading the image:</p> <p><i>govc: The provided network mapping between OVF networks and the system network is not supported by any host.</i></p>	<p>The Dswitch on the vCenter is misconfigured. Please check whether it is operational and mapped to the ESXi hosts.</p>																				
<p>The VMs take a long time to deploy</p>	<p>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.</p>																				
<p>VMs deploy but install fails with <i>Error: timeout waiting for an available IP address</i></p>	<p>Most likely cause would be an issue in the VM parameters provided or network reachability. Enter the VM host through the vCenter console. and review and collect the following logs: /var/log/firstBoot.log and /var/log/vm_setup.log</p>																				
<p>On cluster node failure, the VIP is not transferred to the remaining nodes</p>	<p>Ensure that switch or the vCenter Dswitch connected the VMs allows IP address movement (Allow Forged Transmits in vCenter). For more information, see VMware Settings, on page 25.</p>																				

Scenario	Possible Resolution
<p>When deploying on a vCenter, the following error is displayed towards the end of the VM bringup:</p> <p>Error processing disk changes post-clone: <i>disk.0: ServerFaultCode: NoPermission: RESOURCE (vm-14501:2000), ACTION (queryAssociatedProfile): RESOURCE (vm-14501), ACTION (PolicyIDByVirtualDisk)</i></p>	<p>Enable Profile-driven storage. Query permissions for the vCenter user at the root level (i.e. for all resources) of the vCenter.</p>
<p>Installer reports plan to add more resources than the current number of VMs</p>	<p>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.</p>
<p>On running or cleaning, installer reports <i>Error: cannot locate virtual machine with UUID "xxxxxxx": virtual machine with UUID "xxxxxxx" not found</i></p>	<p>To resolve, remove the <code>/data/crosswork-cluster.tfstate</code> file.</p> <p>The installer uses the <code>tfstate</code> file stored as <code>/data/crosswork-cluster.tfstate</code> to maintain the state of the VMs it has operated upon. If a VM is removed outside of the installer, that is through the vCenter UI, this state is out of synchronization.</p>

Manual Installation of Cisco Crosswork using vCenter vSphere UI

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

The manual installation workflow is broken into two parts:

1. [Build the OVF template, on page 53](#)
2. [Deploy the template, on page 59](#)

In the first part, you create a template. In the second part, you deploy the template as many times as needed to build the cluster of 3 Hybrid nodes (typically) along with any Worker nodes that your environment requires.



Note If the template already exists and you need to rebuild or deploy a Worker node, you can directly go to deploying the template (the second part of this procedure).



Important In case of manual installation of Crosswork Cluster, you must import a cluster inventory file (.tfvars file) to the Crosswork UI. The inventory file (a sample can be downloaded from the Crosswork UI) will contain information about the VMs in your cluster along with the data center parameters. You must set the parameter `OP_Status = 2` to enable manual import of the inventory.

Cisco Crosswork cannot deploy or remove VM nodes in your cluster until you complete this operation. For more information, see the *Import Cluster Inventory* topic in the *Cisco Crosswork Network Controller 5.0 Administration Guide*.

Before you begin:

- Make sure that your environment meets all the vCenter requirements specified under [Crosswork Cluster VM Requirements, on page 26](#) and [Installation Prerequisites for VMware vCenter, on page 19](#).

Build the OVF template

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

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

Step 3 In the vSphere UI, go to **Host > Configure > Networking > Virtual Switches** and select the virtual switch. In the virtual switch, select **Edit > Security**, and configure the following DVS port group properties:

- Set **Promiscuous mode** as *Reject*
- Set **MAC address changes** as *Reject*

Confirm the settings and repeat the process for each virtual switch used in the cluster.

Step 4 Review and confirm that your network settings meet the requirements.

Step 5 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 document the choices (such as IP address, gateway, DNS server, etc.) so that you can enter the information quickly and avoid any issues with the VMware configuration.

Step 6 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 7 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 6.0 Build 152.

Step 8 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 9** 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 10** Review the OVF template that you are deploying. Note that this information is gathered from the OVF, and cannot be modified.
- Step 11** Click **Next**. The **Deploy OVF Template** window is refreshed, with **5 - License agreements** highlighted. Review the End User License Agreement and if you agree, click the **I accept all license agreements** checkbox. Otherwise, contact your Cisco Experience team for assistance.
- Step 12** Click **Next**. The **Deploy OVF Template** window is refreshed, with **6 - Configuration** highlighted. Choose the desired deployment configuration.

Figure 4: Select a deployment configuration

Deploy OVF Template

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

Configuration
Select a deployment configuration

	Description
<input checked="" type="radio"/> IPv4 Network	Use IPv4 network stack for management and data traffic.
<input type="radio"/> IPv6 Network	
<input type="radio"/> IPv4 Network on a Single Interface	
<input type="radio"/> IPv6 Network on a Single Interface	

4 Items

CANCEL BACK NEXT

Note If Cisco Crosswork is deployed using a single interface, then Cisco Crosswork Data Gateway must be deployed using a single interface as well (only recommended for lab deployments).

- Step 13** 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 5: Select Storage

Deploy OVF Template

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

Select storage
Select the storage for the configuration and disk files

Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thin Provision

VM Storage Policy: Datastore Default

Name	Capacity	Provisioned	Free	Type	Cluster
datastore62	2.17 TB	1.66 GB	2.17 TB	VMFS 5	
datastore62-hdd-1	1.64 TB	1.43 GB	1.63 TB	VMFS 6	
datastore62-ssd-1	1.09 TB	1.42 GB	1.09 TB	VMFS 6	
datastore62-ssd-2	371.5 GB	1.41 GB	370.09 GB	VMFS 6	

Compatibility

Compatibility checks succeeded.

CANCEL BACK NEXT

Note For production deployment, choose the **Thick Provision Eager Zeroed** option because this will preallocate disk space and provide the best performance. For lab purposes, we recommend the **Thin Provision** option because it saves disk space.

Step 14 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.

Important Admin Network and NBI Network are not applicable for Crosswork Network Controller deployments.

Step 15 Click **Next**. The **Deploy OVF Template** window is refreshed, with **9 - Customize template** highlighted.

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

Figure 6: Customize template settings

Deploy OVF Template

4 properties have invalid values

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

Network	Settings
Management Network	3 settings
Management IPv4 Address	Please enter the VM's IPv4 management address. 10.10.100.101
Management IPv4 Netmask	Please enter the VM's IPv4 management netmask. 255.255.255.0
Management IPv4 Gateway	Please enter the VM's IPv4 management gateway. 10.10.100.1
Data Network	3 settings
Data IPv4 Address	Please enter the VM's IPv4 data address. 10.10.200.101
Data IPv4 Netmask	Please enter the VM's IPv4 data netmask. 255.255.255.0
Data IPv4 Gateway	Please enter the VM's IPv4 data gateway. 10.10.200.1
Deployment Credentials	2 settings
Original VM Username	Default custom administrator username: cwa-admin

CANCEL BACK NEXT

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.

Note Use a strong VM Password (8 characters long, including upper & lower case letters, numbers, and one special character). Avoid using passwords similar to dictionary words (for example, "Pa55w0rd!") or relatable words (for example, C!sco123 or Cwork321!). While they satisfy the criteria, such passwords are weak and will result in the failure of VM setup.

- 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.

Deploy OVF Template

<ul style="list-style-type: none"> ✓ 1 Select an OVF template ✓ 2 Select a name and folder ✓ 3 Select a compute resource ✓ 4 Review details ✓ 5 License agreements ✓ 6 Configuration ✓ 7 Select storage ✓ 8 Select networks <li style="background-color: #005596; color: white; padding: 2px;">9 Customize template 10 Ready to complete 	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #e6f2ff; padding: 2px; margin-bottom: 5px;"> Deployment Credentials 2 settings </div> <div style="padding: 5px;"> <p>Original VM Username Default system administrator username: cw-admin</p> <p><input type="text" value="cw-admin"/></p> </div> <hr/> <div style="padding: 5px;"> <p>VM Password Password for the default system administrator account</p> <p>Password <input type="password" value="....."/></p> <p>Confirm Password <input type="password" value="....."/></p> </div> </div> <div style="background-color: #e6f2ff; padding: 2px; margin-bottom: 5px;"> DNS and NTP Servers 3 settings </div> <div style="padding: 5px;"> <p>DNS IPv4 Address</p> <p style="font-size: 0.8em;">Please enter the DNS server's IPv4 address. Multiple DNS server IPs can be provided space separated.</p> <p><input type="text" value="8.8.8.8 8.8.4.4"/></p> </div> <div style="padding: 5px;"> <p>NTP Servers</p> <p style="font-size: 0.8em;">Please enter NTP server hostname. Multiple NTP servers can be provided space separated.</p> <p><input type="text" value="ntp.crosswork.com"/></p> </div> <div style="padding: 5px;"> <p>DNS Search Domain Please enter the DNS search domain.</p> <p><input type="text" value="crosswork.com"/></p> </div>
--	--

Disk Configuration 5 settings

Logfs Disk Size Please enter the size of the logfs disk in GB.

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) The default **Disk Configuration** settings should work for most environments. Change the settings only if you are instructed to by 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 and Management Virtual IP DNS name.
 - **Crosswork Data Cluster Virtual IP:** Enter the Data Virtual IP address. and the Data Virtual IP DNS name.
 - **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.

Deploy OVF Template

<ul style="list-style-type: none"> ✓ 1 Select an OVF template ✓ 2 Select a name and folder ✓ 3 Select a compute resource ✓ 4 Review details ✓ 5 License agreements ✓ 6 Configuration ✓ 7 Select storage ✓ 8 Select networks 9 Customize template 10 Ready to complete 	<div style="text-align: right; margin-bottom: 10px;">Hybrid ▾</div> <p>Cluster seed node</p> <p>True/False: Is this the CW cluster seed node? There can be at most 1 in a cluster</p> <p>True ▾</p> <p>Crosswork Management Cluster Virtual IP Please enter virtual IP on the management network</p> <p style="text-align: center;">10.10.100.100</p> <p>Crosswork Data Cluster Virtual IP Please enter virtual IP on the data network</p> <p style="text-align: center;">10.10.200.100</p> <p>Initial node count</p> <p>The TOTAL number of nodes in the cluster including worker and hybrid nodes</p> <p style="text-align: center;">3</p> <p>Initial leader node count The total initial number of hybrid nodes</p> <p style="text-align: center;">3</p> <p>Location of VM A user configurable string</p> <p style="text-align: center;">default</p> <p>Installation type Was the VM installed by the CW installer?</p> <p style="text-align: center;"><input type="checkbox"/></p>
--	---

CANCEL
BACK
NEXT

Step 16 Click **Next**. The **Deploy OVF Template** window is refreshed, with **10 - Ready to Complete** highlighted.

Step 17 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 18 To finalize the template creation, 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.

This is the end of the first part of the manual installation workflow. In the second part, use the newly created template to build the cluster VMs.

Deploy the template

- Step 1** To build the VM, right-click on the newly created template and select **New VM from This Template**.
- Step 2** 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 3** 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 4** 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).

The recommended configuration for the nodes uses a combination of high-speed (typically SSD based) and normal (typical disks) storage. If you are following the recommended configuration follow the steps for two data stores. Otherwise, follow the steps for using a single data store.

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

- Enable **Configure per disk** option.
- Select same data store (regular) as the **Storage** setting for disks 1 through 5. This data store must have 916 GB of space.
- Select the host's high speed (ssd) data store as the **Storage** setting for disk 6. The high speed data store must have at least 50 GB of space.

Figure 7: Select Storage - Configure per disk

cw-template - Deploy From Template

1 Select a name and folder
 2 Select a compute resource
 3 Select storage
 4 Select clone options
 5 Customize vApp properti...
 6 Ready to complete

Select storage
Select the storage for the configuration and disk files

Configure per disk

Virtual Machine	File	Storage	Disk format	VM Storage Poli
cw-1	Configuration File	datastore62-hdd-1	N/A	Datastore Defa
cw-1	Hard disk 1 (50.00 GB)	datastore62-hdd-1	Same format as source	Datastore Defa
cw-1	Hard disk 2 (156.00 GB)	datastore62-hdd-1	Same format as source	Datastore Defa
cw-1	Hard disk 3 (10.00 GB)	datastore62-hdd-1	Same format as source	Datastore Defa
cw-1	Hard disk 4 (450.00 GB)	datastore62-hdd-1	Same format as source	Datastore Defa
cw-1	Hard disk 5 (250.00 GB)	datastore62-hdd-1	Same format as source	Datastore Defa
cw-1	Hard disk 6 (50.00 GB)	datastore62-ssd-2	Same format as source	Datastore Defa

Compatibility

Compatibility checks succeeded.

CANCEL BACK NEXT

- Click **Next**.

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

1 Select a name and folder

2 Select a compute resource

3 Select storage

4 Select clone options

5 Customize vApp properties

6 Ready to complete

Select storage

Select the storage for the configuration and disk files

Configure per disk

Select virtual disk format: Same format as source

VM Storage Policy: Keep existing VM storage policies

Name	Capacity	Provisioned	Free	Type
LocalDataStore-01	922.75 GB	55.05 GB	867.7 GB	VM
LocalDataStore-02	1.36 TB	641.54 GB	750.71 GB	VM

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

Step 5 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:

Note For non-lab environments, you need to reconfigure the hardware to use the proper amount of memory and CPU resources.

- 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 [Crosswork Cluster VM Requirements, on page 26](#)) for **CPU** and **Memory**.
- Under **VM Options** tab, expand **Boot Options**, select **EFI** as the Firmware, and check the **Secure Boot** checkbox.

Step 6 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 (Optional) Use the **Reservation** field under the **Virtual Hardware** tab to set reservation for the VM's CPU allocation (in MHz) and memory profile (in MB).

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

Step 7 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 8 Repeat from **Step 1** to **Step 7** to deploy the remaining VMs in the cluster.

Step 9 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**.

Step 10 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 62](#) 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).

Note If you are using this process to build a new Worker node, no additional work is required after the node is powered on. The node will register with the existing Kubernetes cluster.

For more information on how the resources are allocated to the Worker node, see the *Rebalance Cluster Resources* topic in the *Cisco Crosswork Network Controller 5.0 Administration Guide*.

What to do next

After you login to Crosswork UI, please import a cluster inventory file (.tfvars file) to the Crosswork UI. The inventory file (a sample can be downloaded from the Crosswork UI) will contain information about the VMs in your cluster along with the data center parameters. You must set the parameter `OP_Status = 2` to enable manual import of the inventory. Cisco Crosswork cannot deploy or remove VM nodes in your cluster until you complete this operation. For more information, see the *Import Cluster Inventory* topic in the *Cisco Crosswork Network Controller 5.0 Administration Guide*.

Return to the installation workflow: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)

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 possible errors will be logged in either `installer.log` or `installer_tf.log`. If the VMs get built and are able to boot, the errors in applying the operator specified configuration will be logged on the VM in the `/var/log/firstboot.log`.



Note During installation, Cisco Crosswork will create a special administrative ID (**virtual machine (VM) administrator**, `cw-admin`, with the password that you provided in the manifest template. In case the installer is unable to apply the password, it creates the administrative ID with the default password `cw-admin`). The first time you log in using this administrative ID, you will be prompted to change the password.

The administrative username is reserved and cannot be changed. Data center administrators use this ID to log into and troubleshoot the Crosswork application VM.

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) to the vCenter data center.



Note 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.

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 each VM is created, it is powered on (either automatically when the installer completes, or after you power on the VMs during the manual installation). The parameters specified in the template are applied to the VM, and it is rebooted. The VMs are then registered by Kubernetes to form the cluster.
4. Once the cluster is created and becomes accessible, a success message (e.g. "Crosswork Installer operation complete") will be displayed and the installer script will exit and return you to a prompt on the screen.

You can monitor startup progress using the following methods:

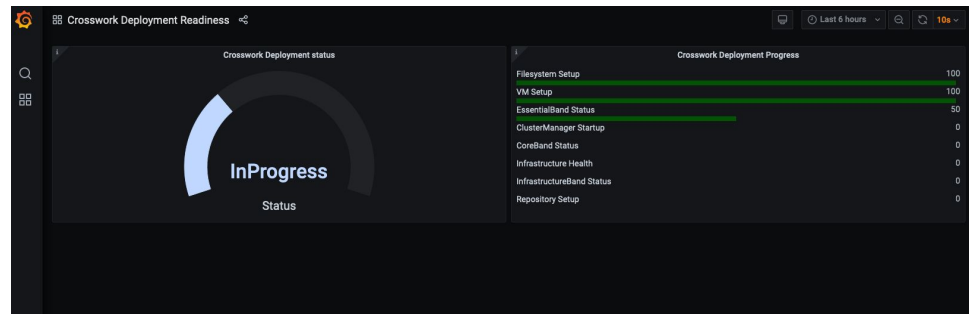
- **Using browser accessible dashboard:**

1. While the cluster is being created, monitor the setup process from a browser accessible dashboard.
2. The URL for this grafana dashboard (in the format `http://{VIP}:30602/d/NK1bwWxGk/crosswork-deployment-readiness?orgId=1&refresh=10s&theme=dark`)

is displayed once the installer completes. 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, use the SSH console described in this section to monitor the installation process.

Figure 9: Crosswork Deployment Readiness



- **Using the console:**

- Check the progress from the console of one of the hybrid VMs or by using SSH to the Virtual IP address.
- In the latter case, login using the *cw-admin* user name and the password you assigned to that account in the install template.
- Switch to super user using `sudo su -` command.
- Run `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 into the Cisco Crosswork UI, on page 64](#).

Failure Scenario

In the event of a failure scenario (listed below), contact the Cisco Customer Experience team and provide the `installer.log`, `installer_tf.log`, and `firstBoot.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 `/var/log/firstBoot.log` or `/opt/robot/bin/firstBoot.log` file.

What to do next:

Return to the installation workflow: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)

Log into the Cisco Crosswork UI

Once the cluster activation and startup have been completed, 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 into the Cisco Crosswork UI and check the cluster health:



Note If the Cisco Crosswork UI is not accessible, during installation, please access the host's console from the VMware or AWS 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 36](#)).

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.

Note You can also log into the Crosswork UI using the Crosswork FQDN name.

The **Log In** window opens.

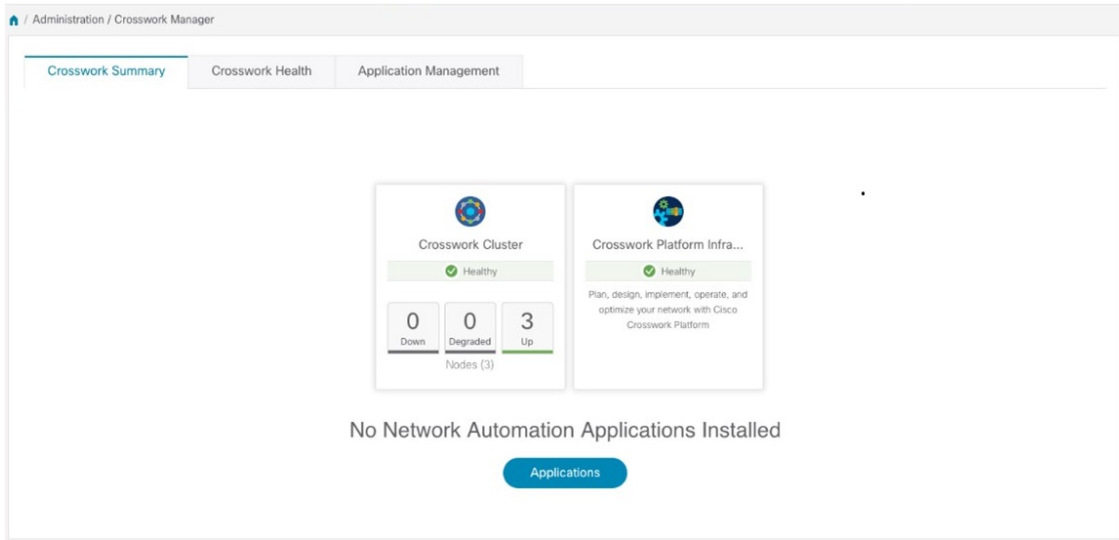
Note When you access the Cisco Crosswork for the first time, some browsers display a warning that the site is untrusted. When this happens, follow the prompts to add a security exception and download the self-signed certificate from the Cisco Crosswork server. After you add a security exception, the 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* topic in the *Cisco Crosswork Network Controller 5.0 Administration Guide*.

Step 3 Log into the Cisco Crosswork as follows:

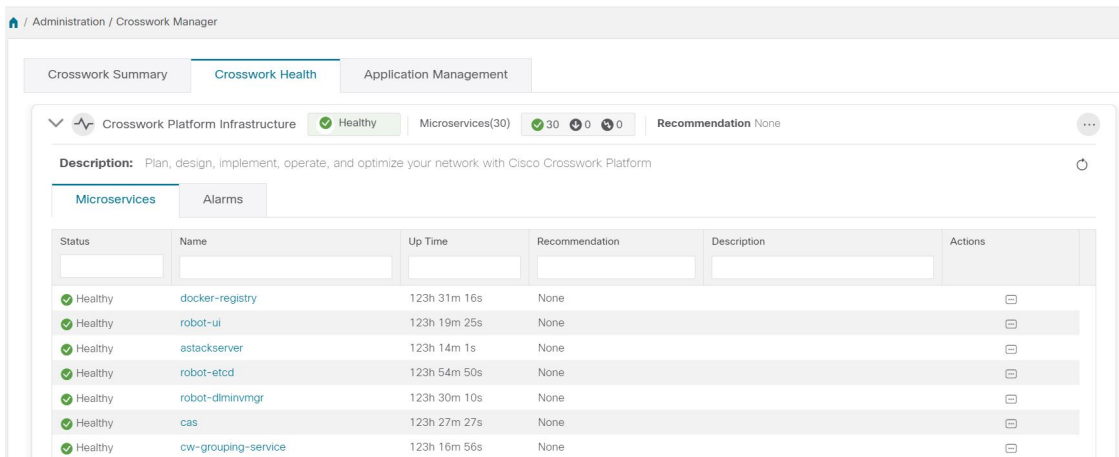
- a) Enter the Cisco Crosswork administrator username **admin** and the default password **admin**.
- b) Click **Log In**.
- c) When prompted to change the administrator's default password, enter the new password in the fields provided and then click **OK**.

Note Use a strong VM Password (minimum 8 characters long, including upper & lower case letters, numbers, and one special character). Avoid using passwords similar to dictionary words (for example, "Pa55w0rd!") or relatable words (for example, C!sco123 or Cwork321!).

The **Crosswork Manager** window is displayed.



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



What to do next

Return to the installation workflow: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)



CHAPTER 6

Install Cisco Crosswork Data Gateway on VMware vCenter

This chapter contains the following topics:

- [Cisco Crosswork Data Gateway Installation Workflow, on page 67](#)
- [Log in and Log out of Crosswork Data Gateway VM, on page 100](#)
- [Cisco Crosswork Data Gateway Authentication and Enrollment, on page 102](#)
- [Crosswork Data Gateway Post-installation Tasks, on page 103](#)
- [Troubleshoot Crosswork Data Gateway Installation and Enrollment, on page 104](#)

Cisco Crosswork Data Gateway Installation Workflow

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



Note If you are redeploying the same Cisco Crosswork Data Gateway with Cisco Crosswork, delete the previous Crosswork Data Gateway entry from the Virtual Machine table under Data Gateway Management. For information on how to delete a Crosswork Data Gateway VM, see [Delete Crosswork Data Gateway VM from Cisco Crosswork, on page 217](#).

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

1. Choose the deployment profile for the Crosswork Data Gateway VM. See [Crosswork Data Gateway VM Requirements, on page 28](#).
2. Review the installation parameters at [Cisco Crosswork Data Gateway Parameters and Deployment Scenarios](#) and make sure that you have all the required information to install Crosswork Data Gateway using your the preferred deployment scenario.
3. Install Cisco Crosswork Data Gateway using yours preferred method:

Table 23: Crosswork Data Gateway installation options

VMware	Install Cisco Crosswork Data Gateway using vCenter vSphere Client, on page 82
	Install Cisco Crosswork Data Gateway via OVF Tool, on page 95

- Complete the post-installation tasks mentioned in the section [Crosswork Data Gateway Post-installation Tasks, on page 103](#)



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

- Verify that the Crosswork Data Gateway VM has enrolled successfully with Cisco Crosswork. For information on how to verify the enrollment process, see [Cisco Crosswork Data Gateway Authentication and Enrollment, on page 102](#).

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

Cisco Crosswork Data Gateway Parameters and Deployment Scenarios

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

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

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

- Cisco Crosswork Data Gateway administrator, with the username, dg-admin, and the password set during installation. The administrator uses this ID to log in and troubleshoot Cisco Crosswork Data Gateway.
- Cisco Crosswork Data Gateway operator, with the username, dg-oper and the password set during installation. The dg-oper user has permissions to perform all 'read' operations and limited 'action' commands.

To know what operations an admin and operator can perform, see the *Supported User Roles* topic in the [Cisco Crosswork Network Controller 5.0 Administration Guide](#).

The **dg-admin** and **dg-oper** user accounts are reserved user names and cannot be changed. You can change the password in the console for both the accounts. For more information, see the *Change Passphrase* section in [Cisco Crosswork Network Controller 5.0 Administration Guide](#). In case of lost or forgotten passwords, destroy the current VM, you have to create a new VM, and re-enroll the new VM with Cisco Crosswork, if required.

In the following table:

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

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

Table 24: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios

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

Label	Key	Description	Additional Information
Profile*	Profile	<p>Parameter conveys the VM resource profile. For an on-premise installation, choose either:</p> <ul style="list-style-type: none"> • Standard • Extended <p>The default value is Standard.</p>	For VMware vCenter, you cannot configure this parameter. The OVF tool configures this parameter with the default value.
AllowRFC8190*	AllowRFC8190	Choose how to validate interface addresses that fall in a usable RFC 8190 range. Options are: Yes, No, or Ask, where the initial configuration scripts prompts for confirmation.	The default value is Yes to automatically allow interface addresses in an RFC 8190 range.
Private Key URI	DGCertKey	SCP URI to private key file for session key signing. You can retrieve this using SCP (user@host:path/to/file).	Cisco Crosswork uses self-signed certificates for handshake with Cisco Crosswork Data Gateway. These certificates are generated at installation.
Certificate File and Key Passphrase	DGCertChainPwd	Passphrase of the SCP user to retrieve the Cisco Crosswork Data Gateway PEM formatted certificate file and private key.	<p>However, if you want to use third party or your own certificate files, then enter these parameters.</p> <p>Certificate chains override any preset or generated certificates in the Cisco Crosswork Data Gateway VM and are given as an SCP URI (user:host:/path/to/file).</p> <p>The host with the URI files must be reachable on the network (from the vNIC0 interface via SCP) and files must be present at the time of install.</p>

Label	Key	Description	Additional Information
Data Disk Size	DGAppdataDisk	Indicates the size in GB of a second data disk. The default value of this parameter in each profile is: <ul style="list-style-type: none"> • 20 GB for Standard. • 520 GB for Extended. 	
HA Network Mode*	HANetworkMode	Indicates the mode for the HA network. Options are: <ul style="list-style-type: none"> • L2 • L3 The default value is L2.	
Passphrase			
dg-admin Passphrase*	dg-adminPassword	The password you have chosen for the dg-admin user. Password must be 8-64 characters.	
dg-oper Passphrase*	dg-operPassword	The password you have chosen for the dg-oper user. Password must be 8-64 characters.	
Interfaces			
<p>In a 3-NIC deployment, you need to provide IP address for Management Traffic (vNIC0) and Control/Data Traffic (vNIC1) only. IP address for Device Access Traffic (vNIC2) is assigned during Crosswork Data Gateway pool creation as explained in the <i>Create a Crosswork Data Gateway Pool</i> section in Cisco Crosswork Network Controller 5.0 Administration Guide.</p> <p>Note Selecting None in both IPv4 Method and the IPv6 Method fields of the vNIC results in a nonfunctional deployment.</p>			

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

Label	Key	Description	Additional Information
NicSBData*	NicSBData	The interface used to collect data from the devices. Options are <code>eth0</code> , <code>eth1</code> , or <code>eth2</code> . The default value is <code>eth2</code> .	
<p>vNIC IPv4 Address (vNIC0, vNIC1, and vNIC2 based on the number of interfaces you choose to use)</p> <p>Important If you plan on using 1 NIC, you must configure Crosswork Data Gateway to get an IPv4 or IPv6 address assigned to vNIC0. When using 2 NICs, specify Method (None or Static) and Type (Ipv4 or IPv6) values for vNIC0 and vNIC1. For 3 NICs, specify the Method and Type for vNIC0 and vNIC0. If you're not using a vNIC, choose None as the Method value.</p>			
vNIC IPv4 Method*	Vnic0IPv4Method Vnic1IPv4Method Vnic2IPv4Method	Method in which the interface is assigned an IPv4 address - None or Static. The default value is None.	<p>If you have selected Method as:</p> <ul style="list-style-type: none"> • None: Skip the rest of the fields for the vNIC IPv4 parameters. Proceed to enter information in the vNIC IPv6 Address parameters. • Static: Enter information in Address, Netmask, Skip Gateway, and Gateway fields
vNIC IPv4 Address	Vnic0IPv4Address Vnic1IPv4Address Vnic2IPv4Address	IPv4 address of the interface.	
vNIC IPv4 Netmask	Vnic0IPv4Netmask Vnic1IPv4Netmask Vnic2IPv4Netmask	IPv4 netmask of the interface in dotted quad format.	
vNIC IPv4 Skip Gateway	Vnic0IPv4SkipGateway Vnic1IPv4SkipGateway Vnic2IPv4SkipGateway	The default value is False. Setting this to <code>True</code> skips configuring a gateway.	
vNIC IPv4 Gateway	Vnic0IPv4Gateway Vnic1IPv4Gateway Vnic2IPv4Gateway	IPv4 address of the vNIC gateway.	
<p>vNIC IPv6 Address (vNIC0, vNIC1, and vNIC2 based on the number of interfaces you choose to use)</p>			

Label	Key	Description	Additional Information
vNIC IPv6 Method*	Vnic0IPv6Method Vnic1IPv6Method Vnic2IPv6Method	Method in which the vNIC interface is assigned an IPv6 address - None, Static, or SLAAC. The default value is None.	<p>If you have selected Method as:</p> <ul style="list-style-type: none"> • None: Skip the rest of the fields for the vNIC IPv6 parameters. Enter information in the vNIC IPv4 Address parameters. • Static: Enter information in Address, Netmask, Skip Gateway, and Gateway fields <p>Do not change the VnicxIPv6Address default values.</p>
vNIC IPv6 Address	Vnic0IPv6Address Vnic1IPv6Address Vnic2IPv6Address	IPv6 address of the interface.	
vNIC IPv6 Netmask	Vnic0IPv6Netmask Vnic1IPv6Netmask Vnic2IPv6Netmask	IPv6 prefix of the interface.	
vNIC IPv6 Skip Gateway	Vnic0IPv6SkipGateway Vnic1IPv6SkipGateway Vnic2IPv6SkipGateway	Options are True or False. Selecting True skips configuring a gateway.	
vNIC IPv6 Gateway	Vnic0IPv6Gateway Vnic1IPv6Gateway Vnic2IPv6Gateway	IPv6 address of the vNIC gateway.	
vNIC Roles			

Label	Key	Description	Additional Information
Default Gateway	DEFAULT_GATEWAY	<p>The interface that allows all types of traffic to flow. This interface is configured using the route metrics.</p> <p>The DNS and NTP traffic uses the DEFAULT_GATEWAY role.</p> <p>The default value is eth0.</p>	<p>For information on the type of roles that you must assign to the vNICs, see Table 9: Cisco Crosswork Data Gateway default vNIC deployment modes, on page 24.</p>
Administration	ADMINISTRATION	<p>The SSH traffic uses the Administration role to access the console menu.</p> <p>The default value is eth0.</p>	
External Logging	EXTERNAL_LOGGING	<p>The interface that allows a connection to an external syslog and auditd servers for sending logs.</p> <p>The default value is eth0.</p>	
Management	MANAGEMENT	<p>The interface that allows a connection to dg-manager for enrollment and other management traffic.</p> <p>The default value is eth0.</p>	
Control	CONTROL	<p>The interface that allows a connection to collection service for destination, device, and collection configuration.</p> <p>The default value is eth1.</p>	
NB System Data	NB_SYSTEM_DATA	<p>As the system destinations share the same IP as interface that allows connection to the collection service, the northbound data for system destinations uses the Control role's interface.</p>	
NB External Data	NB_EXTERNAL_DATA		

Label	Key	Description	Additional Information
		The interface that allows connection to the destinations provided by the user. The default value is <code>eth1</code> .	
SB Data	SB_DATA	The interface that allows a connection to collect the device data. An interface with only the SB Data role does not need an IP during the deployment. The default value is <code>eth2</code> .	
DNS Servers			
DNS Address*	DNS	Space delimited list of IPv4 or IPv6 addresses of the DNS servers accessible from the management interface.	
DNS Search Domain*	Domain	DNS search domain. The default value is <code>localdomain</code> .	
DNS Security Extensions*	DNSSEC	Options are <code>False</code> , <code>True</code> , or <code>Allow-Downgrade</code> . The default value is <code>False</code> . Select <code>True</code> to use DNS security extensions.	
DNS over TLS*	DNSTLS	Options are <code>False</code> , <code>True</code> , and <code>Opportunistic</code> . The default value is <code>False</code> . Select <code>True</code> to use DNS over TLS.	
Multicast DNS*	mDNS	Options are <code>False</code> , <code>True</code> , and <code>Resolve</code> . Select <code>True</code> to use multicast DNS. The default value is <code>False</code> .	If you choose <code>Resolve</code> , only resolution support is enabled. Responding is disabled.

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

Label	Key	Description	Additional Information
Remote Syslog Server			

Label	Key	Description	Additional Information
Use Remote Syslog Server*	UseRemoteSyslog	Options are <code>True</code> and <code>False</code> . Select <code>True</code> to send Syslog messages to a remote host. The default value is <code>False</code> .	Configuring an external syslog server sends service events (CLI/MDT/SNMP/gNMI) to the external syslog server. Otherwise, they are logged only to the Cisco Crosswork Data Gateway VM. If you want to use an external syslog server, specify the following settings: <ul style="list-style-type: none"> • Use Remote Syslog Server • Syslog Server Address • Syslog Server Port • Syslog Server Protocol
Syslog Server Address	SyslogAddress	Hostname, IPv4, or IPv6 address of a syslog server accessible in the management interface.	
Syslog Server Port	SyslogPort	Port number of the syslog server. The default port number is 514.	
Syslog Server Protocol	SyslogProtocol	Options are <code>UDP</code> , <code>RELp</code> , or <code>TCP</code> to send the syslog. The default value is <code>UDP</code> .	
Syslog Multiserver Mode	SyslogMultiserverMode	Multiple servers in the failover or simultaneous mode. This parameter is applicable only when the protocol is set to a non-UDP value. UDP must use the simultaneous mode. Options are <code>Simultaneous</code> or <code>Failover</code> . The default value is <code>Simultaneous</code> .	
Use Syslog over TLS?	SyslogTLS	Select <code>True</code> to use TLS to encrypt syslog traffic. The default value is <code>False</code> .	
Syslog TLS Peer Name	SyslogPeerName	Syslog server hostname exactly as entered in the server certificate <code>SubjectAltName</code> or subject common name.	
Syslog Root Certificate File URI	SyslogCertChain		

Label	Key	Description	Additional Information
		<p>PEM formatted root cert of syslog server retrieved using SCP.</p> <p>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.</p>	
Syslog Certificate File Passphrase	SyslogCertChainPwd	Password of SCP user to retrieve Syslog certificate chain.	
Remote Auditd Server			
Use Remote Auditd Server*	UseRemoteAuditd	Options are <code>True</code> and <code>False</code> . The default value is <code>False</code> . Select <code>True</code> to send auditd messages to a remote host.	<p>If desired, you can configure an external Auditd server. Cisco Crosswork Data Gateway sends audit notifications to the Auditd server when configured and present on the network.</p> <p>Specify these three settings to use an external Auditd server.</p>
Auditd Server Address	AuditdAddress	Hostname, IPv4, or IPv6 address of an optional Auditd server.	
Auditd Server Port	AuditdPort	<p>Port number of an optional Auditd server.</p> <p>The default port is 60.</p>	
Controller and Proxy Settings			
Crosswork Controller IP*	ControllerIP	<p>The Virtual IP address or the host name of Cisco Crosswork Cluster.</p> <p>Note If you are using an IPv6 address, it must be surrounded by square brackets ([1::1]).</p>	<p>This is required so that the Crosswork Data Gateway can enroll with the Crosswork server during the installation and initial start up. Excluding this step will require you to manually ingest the certificate. For more information, see Import Controller Signing Certificate File, on page 107.</p>
Crosswork Controller Port*	ControllerPort	<p>Port of the Cisco Crosswork controller.</p> <p>The default port is 30607.</p>	

Label	Key	Description	Additional Information
Controller Signing Certificate File URI*	ControllerSignCertChain	<p>PEM formatted root cert of Cisco Crosswork to validate signing certs retrieved using SCP. Cisco Crosswork generates the PEM file and is available at the following location:</p> <pre> cw-admin@<Crosswork_VM_Management_VIP_Address> :/home/cw-admin /controller.pem </pre>	<p>Crosswork Data Gateway requires the Controller Signing Certificate File to enroll automatically with Cisco Crosswork.</p> <p>If you specify these parameters during the installation, the certificate file is imported once Crosswork Data Gateway boots up for the first time.</p> <p>If you do not specify these parameters during installation, then import the certificate file manually by following the procedure Import Controller Signing Certificate File, on page 107.</p>
Controller SSL/TLS Certificate File URI	ControllerTlsCertChain	Cisco Crosswork Controller PEM formatted SSL/TLS certificate file retrieved using SCP.	
Controller Certificate File Passphrase*	ControllerCertChainPwd	Password of SCP user (cw-admin) to retrieve Cisco Crosswork certificate chain.	

Label	Key	Description	Additional Information
Proxy Server URL	ProxyURL	URL of the HTTP proxy server.	The proxy parameters apply to the Crosswork Data Gateway cloud deployment. Crosswork Data Gateway must connect to the Internet via TLS, and a proxy server may be required if it is not present in your environment. If you want to use a proxy server, specify these parameters.
Proxy Server Bypass List	ProxyBypass	Comma-delimited list of addresses and hostnames that will not use the proxy server.	
Authenticated Proxy Username	ProxyUsername	Username for authenticated proxy servers.	
Authenticated Proxy Passphrase	ProxyPassphrase	Passphrase for authenticated proxy servers.	
HTTPS Proxy SSL/TLS Certificate File URI	ProxyCertChain	HTTPS proxy PEM formatted SSL/TLS certificate file retrieved using SCP.	
HTTPS Proxy SSL/TLS Certificate File Passphrase	ProxyCertChainPwd	Password of SCP user to retrieve proxy certificate chain.	

vNIC Role Assignment

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

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

Install Cisco Crosswork Data Gateway using vCenter vSphere Client

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



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

Step 1

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

Warning The default VMware vCenter deployment timeout is 15 minutes. If the time taken to fill the OVF template exceeds 15 minutes, vCenter times out and you have to start over again. To prevent this, it is recommended that you plan for the installation by having the necessary parameters and requirements ready. Refer to the [Table 24: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 69](#) for list of mandatory and optional parameters.

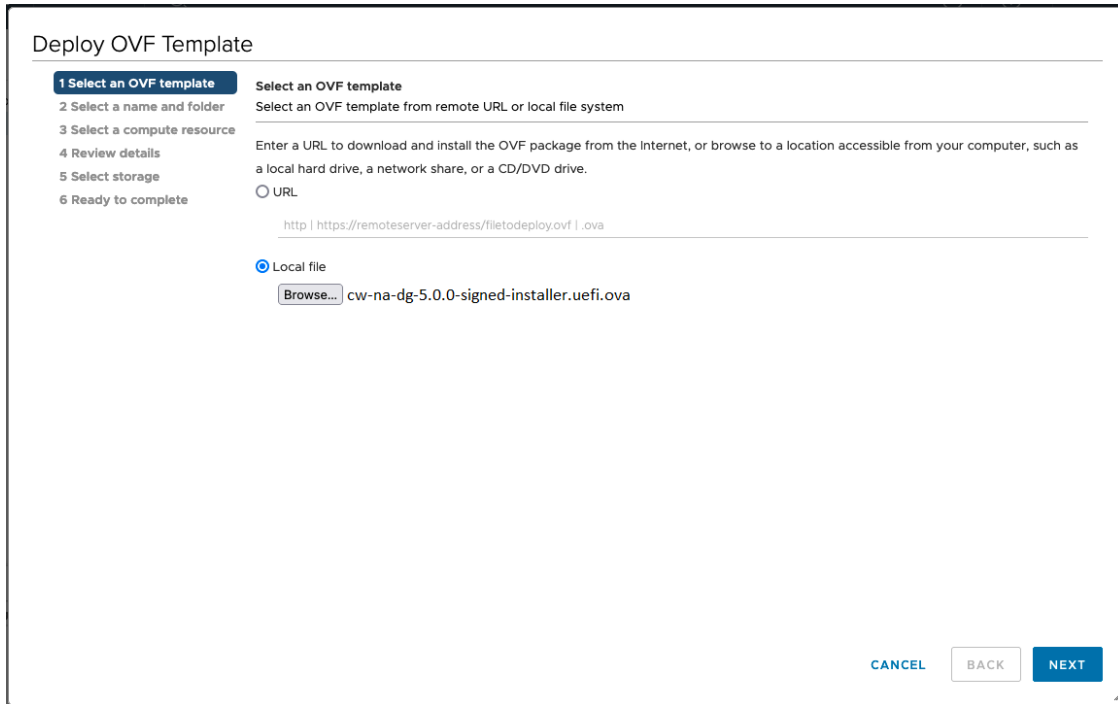
Step 2 Connect to vCenter vSphere Client and select **Actions > Deploy OVF Template**.

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

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

Once selected, the file name is displayed in the window.

Figure 10: Deploy OVF Template - Select an OVF Template Window



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

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

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

Figure 11: Deploy OVF Template - Name and Folder Selection Window

Deploy OVF Template

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

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

Virtual machine name:

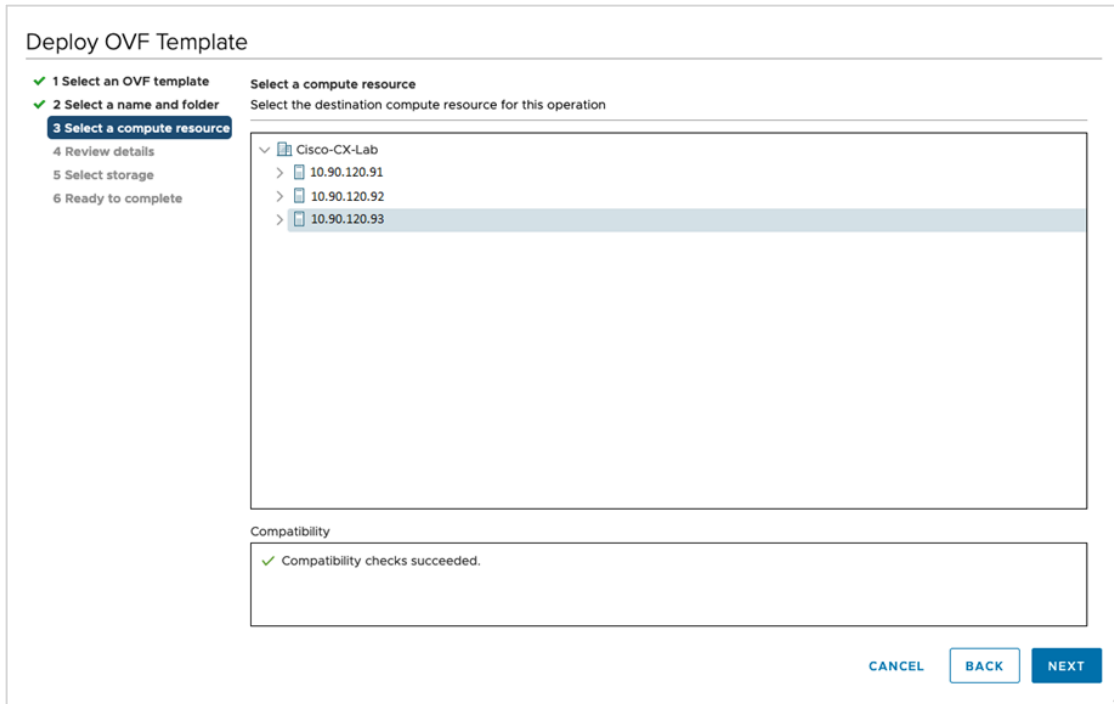
Select a location for the virtual machine.

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

CANCEL BACK NEXT

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

Figure 12: Deploy OVF Template - Select a computer resource Window



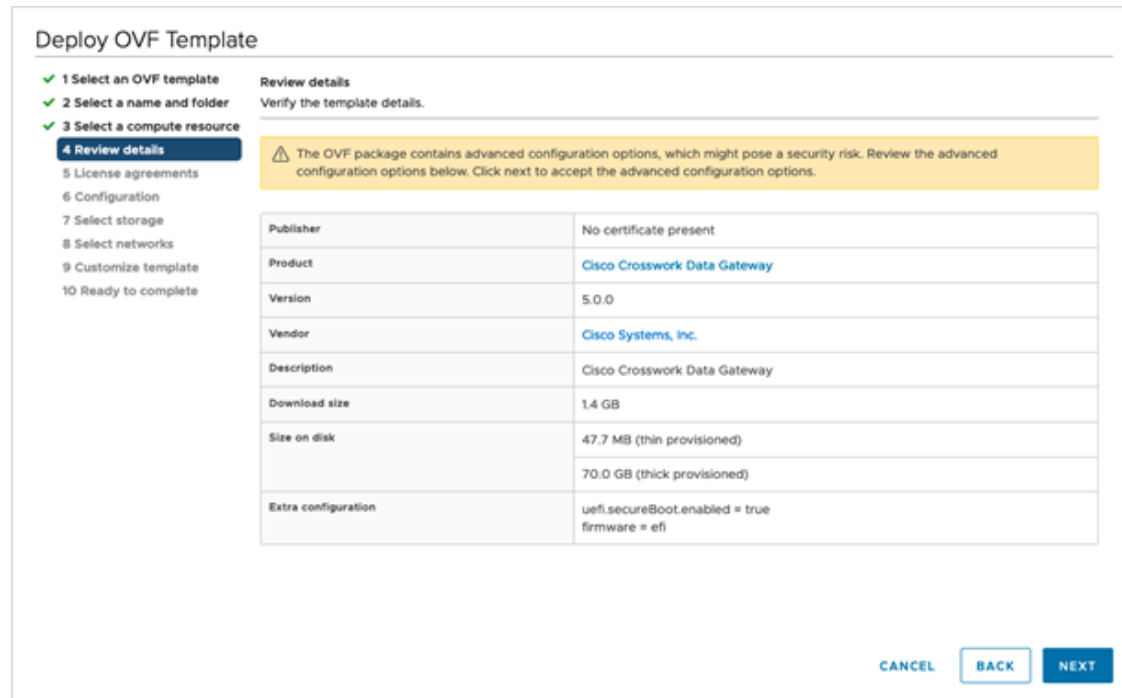
Step 6

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

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

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

Figure 13: Deploy OVF Template - Review details Window



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

Step 8 Click **Next** to go to **6 Configuration**, as shown in the following figure. Select **Crosswork On-Premise Standard** or **Crosswork On-Premise Extended**. See [Selecting the Crosswork Data Gateway Deployment Type, on page 28](#) for more information.

Figure 14: Deploy OVF Template - Configuration Window

Deploy OVF Template

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

Configuration
Select a deployment configuration

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

4 Items

CANCEL BACK NEXT

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

Step 9

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

- Cisco recommends that you select **Thick provision lazy zeroed** from the **Select virtual disk format** drop-down list.
- From the **Datastores** table, choose the data store you want to use and review its properties to ensure there is enough available storage.

Figure 15: Deploy OVF Template - Select storage Window

Deploy OVF Template

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

Select storage
Select the storage for the configuration and disk files

Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thick Provision Lazy Zeroed

VM Storage Policy: Datastore Default

Name	Capacity	Provisioned	Free	Type	Cluster
<input checked="" type="checkbox"/> Datastore2	4.5 TB	3.69 TB	3.66 TB	VMFS 6	
<input type="checkbox"/> Small datastore	213.5 GB	714 GB	206.36 GB	VMFS 6	

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

Figure 16: Deploy OVF Template - Select storage Window

Deploy OVF Template

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

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format:

Thick Provision Lazy Zeroed ▾

VM Storage Policy:

Datastore Default ▾

Name	Capacity	Provisioned	Free	Type
Local Datastore	2.45 TB	1.19 TB	1.46 TB	VM

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

Step 10

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

Figure 17: Deploy OVF Template - Select networks Window

Deploy OVF Template

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

Select networks

Select a destination network for each source network.

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

4 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL
BACK
NEXT

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

Step 11 Click **Next** to go to **9 Customize template**, with the **Host information** already expanded. Enter the information for the parameters as explained in [Table 24: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 69](#).

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

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

Figure 18: Deploy OVF Template - Customize template > Host information Window

Deploy OVF Template

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

01. Host Information 10 settings

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

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

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

d. Allow Usable RFC 8190 Addresses
If an address for vNIC0, vNIC1, vNIC2, or vNIC3 falls into a usable range identified by RFC 8190 or its predecessors, reject, accept, or request confirmation during initial configuration
Yes

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

f. Crosswork Data Gateway Certificate File URI

CANCEL BACK NEXT

Crosswork Data Gateway supports the following pool mode options:

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

Figure 19: Deploy OVF Template - Customize template > Host information Window > High Availability Network Mode

Deploy OVF Template

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

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

Password _____

Confirm Password _____

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

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

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

02. Passphrases 2 settings

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

- a. Configure the vNIC role assignment based on the number of NICs that you have decided to use.

Based on the number of NICs, refer to the following:

- See [Deploy OVF Template - Customize Template for 1 vNIC deployment](#).
- See [Deploy OVF Template - Customize Template for 2 vNICs deployment](#).
- See [Deploy OVF Template - Customize Template for 3 vNICs deployment](#).

Figure 20: Deploy OVF Template - Customize Template for 1 vNIC deployment

Deploy OVF Template

<ul style="list-style-type: none"> ✓ 1 Select an OVF template ✓ 2 Select a name and folder ✓ 3 Select a compute resource ✓ 4 Review details ✓ 5 License agreements ✓ 6 Configuration ✓ 7 Select storage ✓ 8 Select networks 9 Customize template 10 Ready to complete 	<table border="1"> <thead> <tr> <th style="text-align: left;">03. vNIC Role Assignment</th> <th style="text-align: left;">7 settings</th> </tr> </thead> <tbody> <tr> <td>a. Default Gateway</td> <td>The interface used as the Default Gateway and for DNS and NTP traffic <input type="text" value="eth0"/></td> </tr> <tr> <td>b. Administration</td> <td>The interface used for SSH access to the VM <input type="text" value="eth0"/></td> </tr> <tr> <td>c. External Logging</td> <td>The interface used to send logs to an external logging server <input type="text" value="eth0"/></td> </tr> <tr> <td>d. Management</td> <td>The interface used for enrollment and other management traffic <input type="text" value="eth0"/></td> </tr> <tr> <td>e. Control</td> <td>The interface used for destination, device, and collection configuration <input type="text" value="eth0"/></td> </tr> <tr> <td>g. Northbound External Data</td> <td>The interface used to send collection data to external destinations <input type="text" value="eth0"/></td> </tr> <tr> <td>h. Southbound Data</td> <td>The interface used collect data from all devices <input type="text" value="eth0"/></td> </tr> </tbody> </table>	03. vNIC Role Assignment	7 settings	a. Default Gateway	The interface used as the Default Gateway and for DNS and NTP traffic <input type="text" value="eth0"/>	b. Administration	The interface used for SSH access to the VM <input type="text" value="eth0"/>	c. External Logging	The interface used to send logs to an external logging server <input type="text" value="eth0"/>	d. Management	The interface used for enrollment and other management traffic <input type="text" value="eth0"/>	e. Control	The interface used for destination, device, and collection configuration <input type="text" value="eth0"/>	g. Northbound External Data	The interface used to send collection data to external destinations <input type="text" value="eth0"/>	h. Southbound Data	The interface used collect data from all devices <input type="text" value="eth0"/>
03. vNIC Role Assignment	7 settings																
a. Default Gateway	The interface used as the Default Gateway and for DNS and NTP traffic <input type="text" value="eth0"/>																
b. Administration	The interface used for SSH access to the VM <input type="text" value="eth0"/>																
c. External Logging	The interface used to send logs to an external logging server <input type="text" value="eth0"/>																
d. Management	The interface used for enrollment and other management traffic <input type="text" value="eth0"/>																
e. Control	The interface used for destination, device, and collection configuration <input type="text" value="eth0"/>																
g. Northbound External Data	The interface used to send collection data to external destinations <input type="text" value="eth0"/>																
h. Southbound Data	The interface used collect data from all devices <input type="text" value="eth0"/>																

Figure 21: Deploy OVF Template - Customize Template for 2 vNICs deployment

Deploy OVF Template

<ul style="list-style-type: none"> ✓ 1 Select an OVF template ✓ 2 Select a name and folder ✓ 3 Select a compute resource ✓ 4 Review details ✓ 5 License agreements ✓ 6 Configuration ✓ 7 Select storage ✓ 8 Select networks 9 Customize template 10 Ready to complete 	<table border="1"> <thead> <tr> <th style="text-align: left;">03. vNIC Role Assignment</th> <th style="text-align: left;">7 settings</th> </tr> </thead> <tbody> <tr> <td>a. Default Gateway</td> <td>The interface used as the Default Gateway and for DNS and NTP traffic <input type="text" value="eth0"/></td> </tr> <tr> <td>b. Administration</td> <td>The interface used for SSH access to the VM <input type="text" value="eth0"/></td> </tr> <tr> <td>c. External Logging</td> <td>The interface used to send logs to an external logging server <input type="text" value="eth0"/></td> </tr> <tr> <td>d. Management</td> <td>The interface used for enrollment and other management traffic <input type="text" value="eth0"/></td> </tr> <tr> <td>e. Control</td> <td>The interface used for destination, device, and collection configuration <input type="text" value="eth1"/></td> </tr> <tr> <td>g. Northbound External Data</td> <td>The interface used to send collection data to external destinations <input type="text" value="eth1"/></td> </tr> <tr> <td>h. Southbound Data</td> <td>The interface used collect data from all devices <input type="text" value="eth1"/></td> </tr> </tbody> </table>	03. vNIC Role Assignment	7 settings	a. Default Gateway	The interface used as the Default Gateway and for DNS and NTP traffic <input type="text" value="eth0"/>	b. Administration	The interface used for SSH access to the VM <input type="text" value="eth0"/>	c. External Logging	The interface used to send logs to an external logging server <input type="text" value="eth0"/>	d. Management	The interface used for enrollment and other management traffic <input type="text" value="eth0"/>	e. Control	The interface used for destination, device, and collection configuration <input type="text" value="eth1"/>	g. Northbound External Data	The interface used to send collection data to external destinations <input type="text" value="eth1"/>	h. Southbound Data	The interface used collect data from all devices <input type="text" value="eth1"/>
03. vNIC Role Assignment	7 settings																
a. Default Gateway	The interface used as the Default Gateway and for DNS and NTP traffic <input type="text" value="eth0"/>																
b. Administration	The interface used for SSH access to the VM <input type="text" value="eth0"/>																
c. External Logging	The interface used to send logs to an external logging server <input type="text" value="eth0"/>																
d. Management	The interface used for enrollment and other management traffic <input type="text" value="eth0"/>																
e. Control	The interface used for destination, device, and collection configuration <input type="text" value="eth1"/>																
g. Northbound External Data	The interface used to send collection data to external destinations <input type="text" value="eth1"/>																
h. Southbound Data	The interface used collect data from all devices <input type="text" value="eth1"/>																

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

Figure 22: Deploy OVF Template - Customize Template for 3 vNICs deployment

03. vNIC Role Assignment		7 settings
a. Default Gateway	The interface used as the Default Gateway and for DNS and NTP traffic	eth0
b. Administration	The interface used for SSH access to the VM	eth0
c. External Logging	The interface used to send logs to an external logging server	eth0
d. Management	The interface used for enrollment and other management traffic	eth0
e. Control	The interface used for destination, device, and collection configuration	eth1
g. Northbound External Data	The interface used to send collection data to external destinations	eth1
h. Southbound Data	The interface used collect data from all devices	eth2

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

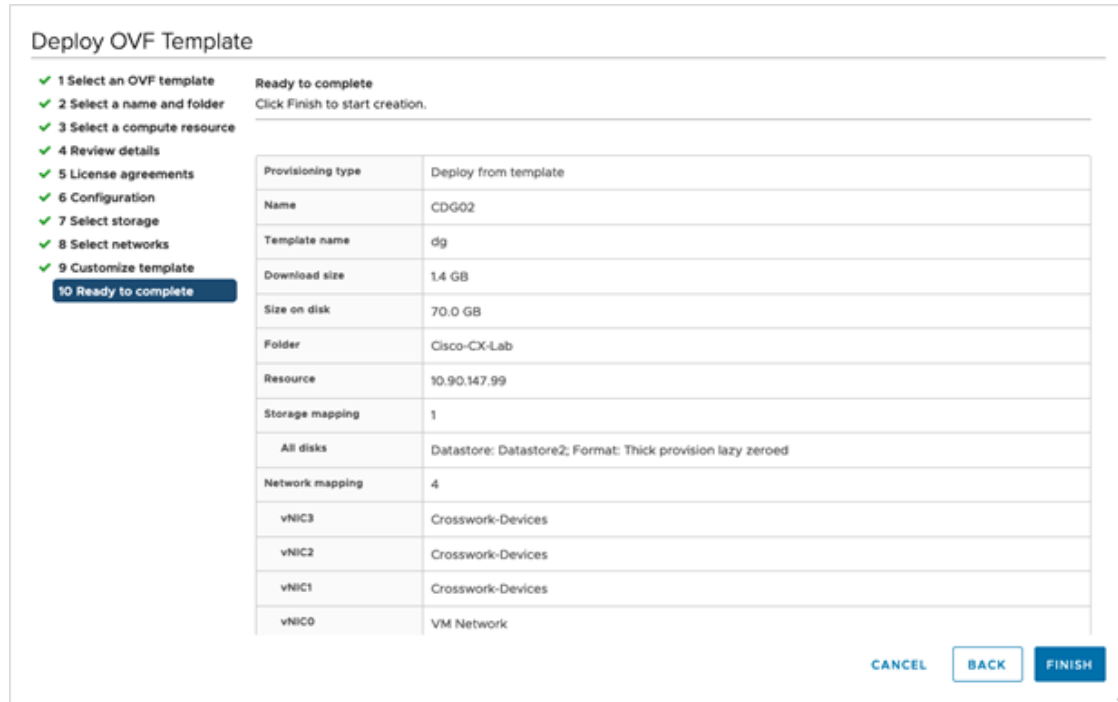
- In the **16. Controller Setting** > **a. Crosswork Controller IP** section, enter the IP address of the cluster of the DNS host name you assigned to the cluster in your DNS server configuration.
- In the **16. Controller Setting** > **b. Crosswork Controller Port** section, set the port number to 30607.

Figure 23: Deploy OVF Template - Customize Template > Controller Settings

16. Controller Settings		11 settings
a. Crosswork Controller IP *	Please enter the hostname, IPv4 address, or IPv6 address of the Crosswork Controller accessible from the Default Gateway role	
b. Crosswork Controller Port *	Please enter the port number of the Crosswork Controller	30607
c. Controller Signing Certificate File URI	Please enter the optional Crosswork Controller PEM formatted signing certificate file URI retrieved using SCP (user@host:/path /to/file)	
d. Controller SSL/TLS Certificate File URI	Please enter the optional Crosswork Controller PEM formatted SSL/TLS certificate file URI retrieved using SCP (user@host:/path /to/file)	
e. Controller Certificate File Passphrase	Please enter the SCP user passphrase to retrieve the Crosswork Controller PEM formatted certificate file	Password

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

Figure 24: Deploy OVF Template - Ready to Complete Window



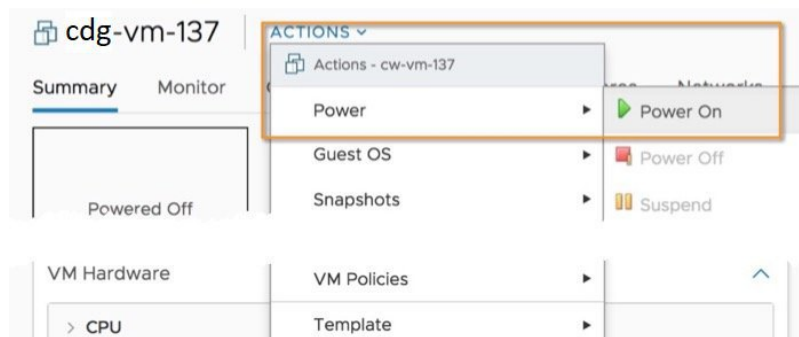
Step 13 Wait for the deployment to finish before continuing. To check the deployment status:

- Open the vCenter vSphere client.
- In the **Recent Tasks** tab for the host VM, view the status for the **Deploy OVF template** and **Import OVF package** jobs.

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

Step 14 Once the deployment status is 100%, power on the VM to complete the deployment process. Expand the host's entry so you can click the VM and then choose **Actions > Power > Power On**, as shown in the following figure:

Figure 25: Power On Action



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

Warning Changing the VM's network settings in vCenter may have significant unintended consequences, including but not limited to the loss of static routes and connectivity. The settings have been validated to provide the best network performance. Make changes to these settings at your own risk.

What to do next

After you log in, the Crosswork Data Gateway should present you with the welcome screen and options menu indicating that the installation completed successfully. For information on how to log in, see [Log in and Log out of Crosswork Data Gateway VM, on page 100](#).

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

Return to the installation workflow: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)

Install Cisco Crosswork Data Gateway via OVF Tool

You must modify the list of mandatory and optional parameters in the script as per your requirements and run the OVF Tool. Refer to [Table 24: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 69](#) for the list of installation parameters and their default values.



Note The file names mentioned in this topic are sample names and may differ from the actual file names on [cisco.com](https://www.cisco.com).

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

Before you begin

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

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

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

```
ovftool --version
```

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

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

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

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

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

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

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

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

Sample scripts for 3 vNIC deployment are included in this document. For more information, see [Sample Script for Crosswork Data Gateway IPv4 Deployment, on page 97](#) and [Sample Script for Crosswork Data Gateway IPv6 Deployment, on page 98](#).

Step 7 Use the following command to make the script executable:

```
chmod +x {filename}
```

Step 8 Use the following command to execute the script from the directory where the OVA and script files are stored:

```
./{script name} {path and ova file name}
```

For example:

```
./<script name> <Absolute path to cw-na-dg-5.0.0-45-release-20230418.uefi.ova>
```

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

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

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

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

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

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

What to do next

Log in to the VM. For more information, see [Log in and Log out of Crosswork Data Gateway VM, on page 100](#). After you log in, the Crosswork Data Gateway should present you with the welcome screen, and options menu indicating that the installation is complete. Log out and proceed with the postinstallation tasks explained in [Crosswork Data Gateway Post-installation Tasks, on page 103](#).

Sample Script for Crosswork Data Gateway IPv4 Deployment

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



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

```
#!/usr/bin/env bash
DM="

```

Sample Script for Crosswork Data Gateway IPv6 Deployment

```

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

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

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

```

Sample Script for Crosswork Data Gateway IPv6 Deployment

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



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

```

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

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

```

```

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

ROBOT_OVA_PATH=$1

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

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

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

```

```

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

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

```

Log in and Log out of Crosswork Data Gateway VM

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

- [Access Crosswork Data Gateway VM from SSH, on page 100](#)
- [Access Crosswork Data Gateway through vCenter, on page 101](#)

To log out of the Crosswork Data Gateway VM, see [Log Out of Crosswork Data Gateway VM, on page 101](#).

Access Crosswork Data Gateway VM from SSH

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

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

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

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

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

For example,

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

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

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

The Crosswork Data Gateway flash screen opens prompting for password.

Figure 26: Crosswork screen

```

Cisco Crosswork Data Gateway

#####  #####  #####  #####  #####  #  #  #####  #####  #  #
#  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #
#  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #
#  #####  #  #  #####  #####  #  #  #  #  #  #####  ###
#  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #
#  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #
#####  #  #  #####  #####  #####  ##  ##  #####  #  #  #

```

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

Access Crosswork Data Gateway through vCenter

Follow these steps to log in via vCenter:

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

The Crosswork Data Gateway console comes up.

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

The Crosswork Data Gateway flash screen opens prompting for password.

Figure 27: Crosswork screen

```

Cisco Crosswork Data Gateway

#####  #####  #####  #####  #####  #  #  #####  #####  #  #
#  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #
#  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #
#  #####  #  #  #####  #####  #  #  #  #  #  #####  ###
#  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #
#  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #
#  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #  #
#####  #  #  #####  #####  #####  ##  ##  #####  #  #  #

```

Log Out of Crosswork Data Gateway VM

To log out, select option **1 Logout** from the Main Menu and press Enter or click **OK**.

Cisco Crosswork Data Gateway Authentication and Enrollment

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

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

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

1. Log in to the Cisco Crosswork UI. See [Log into the Cisco Crosswork UI, on page 64](#).
2. Navigate to **Administration > Data Gateway Management**.
3. Click on the **Data Gateway Instances** tab.

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

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

For information about the different operational states of the VMs, see the *Overview of Cisco Crosswork Data Gateway* section in [Cisco Crosswork Network Controller 5.0 Administration Guide](#).



Note Cisco Crosswork Data Gateway VMs that were previously onboarded and still have the **Operational State** as **Degraded** need to be investigated. Contact Cisco Customer Experience team for assistance.

For information about the different operational states of the VMs, see the *Overview of Cisco Crosswork Data Gateway* section in [Cisco Crosswork Network Controller 5.0 Administration Guide](#).



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

What to do next:

Return to the installation workflow: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)

Crosswork Data Gateway Post-installation Tasks

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

- [Configure Timezone of the Crosswork Data Gateway VM, on page 103](#)

What to do next:

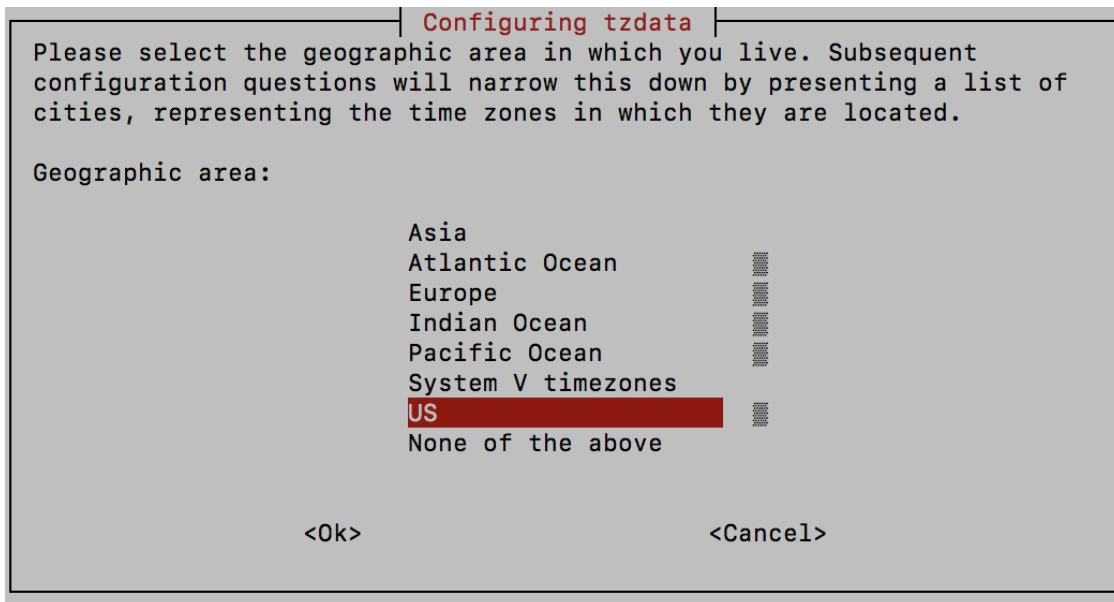
Return to the installation workflow: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)

Configure Timezone of the Crosswork Data Gateway VM

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

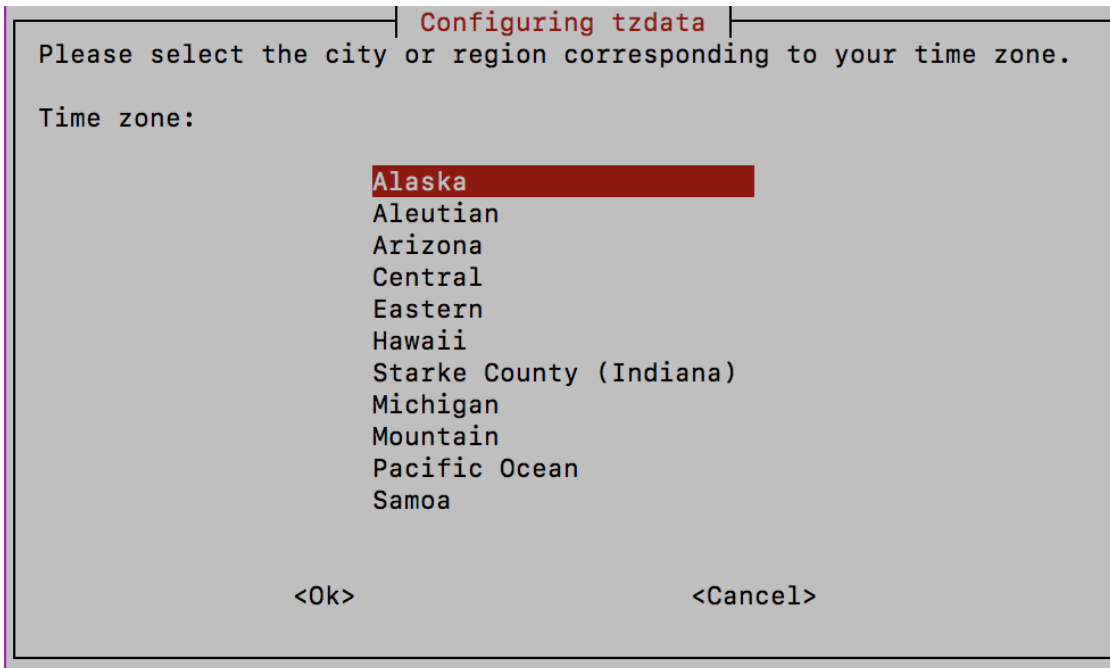
- Step 1** Log in to the Crosswork Data Gateway VM.
- Step 2** In the Crosswork Data Gateway VM interactive menu, select **3 Change Current System Settings**.
- Step 3** From the menu, select **9 Timezone**.
- Step 4** Select the geographic area in which you live.

Figure 28: Timezone Settings - Geographic Area Selection



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

Figure 29: Timezone Settings - Region Selection



- Step 6** Select **OK** to save the settings.
- Step 7** Reboot the Crosswork Data Gateway VM so that all processes pick up the new timezone. See *Reboot Crosswork Data Gateway VM* section in [Cisco Crosswork Network Controller 5.0 Administration Guide](#).
- Step 8** Log out of the Crosswork Data Gateway VM.

Troubleshoot Crosswork Data Gateway Installation and Enrollment

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

For more information on how to collect show-tech logs, see the *Collect show-tech logs from the Interactive Console* section in [Cisco Crosswork Network Controller 5.0 Administration Guide](#). If there are session establishment or certificate-related issues, ensure that the `controller.pem` certificate is uploaded using the Interactive Console.



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

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

Table 25: Troubleshooting the Installation/Enrollment

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

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

Issue	Action
Crosswork Data Gateway goes into Error state	Check the vNIC values in the OVF template in case of vCenter.
Crosswork Data Gateway enrollment with 1 NIC Cisco Crosswork fails	<p>Check the vNIC values in the OVF template in case of vCenter. If ActiveVnics property is missing for 1 NIC and 2 NIC, Crosswork Data Gateway tries to deploy 3 NICs by default.</p> <p>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.</p>
Crosswork Data Gateway deploys Standard profile instead of Extended profile	Check the <code>Deployment</code> parameter in the OVF template in case of vCenter. If <code>Deployment</code> parameter mismatches or does not exist for an Extended profile, then Crosswork Data Gateway deploys the Standard profile by default.
During a Crosswork upgrade, some of the Crosswork Data Gateways may not get upgraded or reenrolled leading to logging multiple error messages in the dg-manager logs.	Reenroll or redeploy the Crosswork Data Gateways. For more information, see the <i>Redeploy a Crosswork Data Gateway Instance</i> and <i>Reenroll Crosswork Data Gateway</i> sections in Cisco Crosswork Network Controller 5.0 Administration Guide .
If a Crosswork Data Gateway instance that was previously attached to Crosswork is now reattached to a different Crosswork version 4.x or 5.0, the operational state of the instance may be Degraded with the robot-astack-influxdb error.	<ol style="list-style-type: none"> 1. Log in to the Crosswork UI from the SSH. 2. Run the Docker executive commands to access the robot-astack-influxdb pod. 3. In the pod, navigate to the following directory and delete it: <code>/mnt/dataafs/influxdb</code> 4. Restart the service using the following command: <code>supervisorctl restart all</code>
If Data Gateway is redeployed without moving the gateway to the Maintenance mode, Crosswork enrollment will be unsuccessful and errors will be logged in the dg-manager and controller-gateway logs.	Move the Data Gateway to the Maintenance mode or manually reenroll the gateway. For more information, see the <i>Reenroll Crosswork Data Gateway</i> section in Cisco Crosswork Network Controller 5.0 Administration Guide .

Import Controller Signing Certificate File

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

- You have not specified **Controller Signing Certificate File URI** under the **Controller Settings** during installation.

- Cisco Crosswork was upgraded or reinstalled and you need to authenticate and enroll Crosswork Data Gateway with Cisco Crosswork.

Follow these steps to import controller signing certificate file:

-
- Step 1** From the Cisco Crosswork Data Gateway VM's Interactive Menu, select **3 Change Current System Settings**.
The **Change System Settings** menu opens.
- Step 2** Select **7 Import Certificate**.
- Step 3** From **Import Certificates** menu, select **1 Controller Signing Certificate File**.
- Step 4** Enter the SCP URI for the certificate file.
An example URI is given below:
`cw-admin@{server ip}:/home/cw-admin/controller.pem`
- Step 5** Enter the SCP passphrase (the SCP user password).
The certificate file is imported.
- Step 6** Verify that the certificate was installed successfully. See [View the Controller Signing Certificate File, on page 108](#).
-

View the Controller Signing Certificate File

Follow these steps to view the signing certificate:

-
- Step 1** From the Crosswork Data Gateway VM's interactive menu, select **2 Show System Settings**.
- Step 2** From the **Show Current System Settings** menu, select **7 Certificates**.
- Step 3** Select **2 Controller Signing Certificate File**.
Crosswork Data Gateway displays the default certificate if no new certificate has been imported. Otherwise, it displays the new certificate if it was successfully imported.
-



PART **III**

Install Cisco Crosswork Network Controller on AWS EC2

- [Installation Prerequisites for AWS EC2, on page 111](#)
- [Install Cisco Crosswork Network Controller on AWS EC2, on page 125](#)



CHAPTER 7

Installation Prerequisites for AWS EC2

This chapter contains the following topics:

- [Overview, on page 111](#)
- [Amazon EC2 Settings, on page 111](#)
- [Host VM Requirements, on page 114](#)
- [TCP/UDP Port requirements, on page 118](#)
- [IP Address Restrictions, on page 123](#)
- [Supported Web Browsers, on page 124](#)

Overview

This chapter explains the general (such as VM requirements, port requirements, application requirements, etc.) and platform-specific prerequisites to install each Crosswork component.

The data center resources needed to operate other integrated components or applications (such as WAE, DHCP, and TFTP servers) are not addressed in this document. Refer to the respective installation documentation of those components for more details.

Amazon EC2 Settings

This section describes the settings that must be configured to install Crosswork Network Controller on Amazon EC2.

Crosswork can be deployed in Amazon Elastic Compute Cloud (EC2). Amazon EC2 is a web service that provides compute resources in the cloud to host your Crosswork applications.

Crosswork is deployed in Amazon EC2 using CloudFormation (CF) templates. The CloudFormation process is faster and less error-prone than the manual procedure to build the cluster, however you must have the necessary skills to prepare a CloudFormation template with details of the cluster deployment.

Installing Crosswork and its components in the AWS environment requires you to review and meet the following prerequisites:



Attention Most of the requirements discussed in this section are AWS concepts and not imposed exclusively by Crosswork.

Table 26: AWS Prerequisites and Settings

Requirement	Description
VPC and Subnets	<p>Virtual Private Cloud (VPC) is created and configured with dedicated subnets for Crosswork interfaces (Management and Data) and Crosswork Data Gateway (Management, Data, and Device) interfaces.</p> <p>Direct IP connectivity is required between all subnets.</p>
Endpoints	<p>An endpoint is created in your VPC with the following parameters:</p> <ul style="list-style-type: none"> • Service name: EC2 service for the region (availability zone) where you are deploying. • Private DNS names: Enabled • Endpoint type: Interface • Under Subnets, specify the management subnet that you intend to use for the installation. If you are using different management subnets for the Crosswork VM and the Crosswork Data Gateway VM, ensure that you specify both the management subnets so that the endpoint has access to both the subnets. <p>Important The interface subnet should not conflict with the Network Load Balancer (NLB).</p> <p>For information on how to configure the endpoints, refer to the AWS documentation.</p>
IAM role	<p>A role is created in Identity and Access Management (IAM) with relevant permission policies. An IAM role is an identity that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.</p> <p>Note</p> <ul style="list-style-type: none"> • The minimum permissions required for a Crosswork role are ec2:DescribeNetworkInterfaces, ec2:AssignPrivateIpAddresses and ec2:UnassignPrivateIpAddresses. • The trust policy for your role must have the "Action": "sts:AssumeRole" condition.
Key pairs	Key pairs (private keys used to log into the VMs) are created and configured.
Placement Groups	<p>A placement group of <i>Cluster</i> strategy is created.</p> <p>In a <i>cluster</i> placement group, instances are logically grouped in a single availability zone that benefit from low network latency and high network throughput.</p> <p>This requirement is required only for launching the Crosswork cluster instances.</p>

Requirement	Description
IP addresses	<p>Crosswork cluster: When using single NIC, you require one IP address (IPv4 or IPv6) for each node being deployed (Hybrid or Worker) and one additional IP address to be used as the Virtual IP (VIP) address. When using dual NICs (one for the Management network and one for the Data network), you require a management and data IP address (IPv4 or IPv6) for each node being deployed (Hybrid or Worker) and two additional IP addresses to be used as the management and data Virtual IP (VIP) address.</p> <p>For example, in the case of a 3 VM cluster with a single NIC, you need 4 IP addresses, and in the case of a 3 VM cluster with dual NIC, you need 8 IP addresses (4 for management network and 4 for data network).</p> <p>Crosswork Data Gateway: IP addresses for Management Traffic and Data Traffic only. IP address for Device Access Traffic is assigned during Crosswork Data Gateway pool creation as explained in the Section: <i>Create a Crosswork Data Gateway Pool</i> in the <i>Cisco Crosswork Network Controller 5.0 Administration Guide</i>.</p> <ul style="list-style-type: none"> • 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 fails. • At this time, your IP allocation is permanent and cannot be changed without redeployment. For more information, contact the Cisco Customer Experience team.
Security group	A security group must be created and configured to specify which ports or traffic are allowed.
Instance type	<p>The resource profile for your instance deployment. The AWS Instance type should be selected to conform with the VM resource and network requirements listed in Plan Your Deployment, on page 5.</p> <ul style="list-style-type: none"> • Crosswork Cluster: <ul style="list-style-type: none"> • Select m5.4xlarge for demos or lab deployments. • Select m5.8xlarge for production deployments. • Crosswork Data Gateway (production and lab deployments): <ul style="list-style-type: none"> • Standard - Select m5.4xlarge • Extended - Select m5.8xlarge
CloudFormation (CF) template	The CF template (.yaml) files for the Crosswork components that must be uploaded during the installation. For more information, see Extract CF Template Image, on page 125 .
Route53DomainName	Domain name configured for Route53 DNS hosted zone.
User data	The VM-specific parameters script that must be specified during the manual installation procedure.

Requirement	Description
Hosted Zone ID	The Hosted Zone ID must be provided with the domain name (Route53DomainName). The Network Load Balancer (NLB) deployments require a predefined Route53 hosted zone.

Host VM Requirements

This section explains the resource requirements per VM to deploy the Crosswork Cluster and Crosswork Data Gateway.

- [Crosswork Cluster VM Requirements, on page 26](#)
- [Crosswork Data Gateway VM Requirements, on page 28](#)

Crosswork Cluster VM Requirements

The Crosswork cluster consists of three VMs or nodes operating in a hybrid configuration. This is the minimum configuration necessary to support the applications in a standard network. Additional VMs or nodes (maximum up to 2 worker nodes) in a worker configuration can be added later to scale your deployment, as needed, to match the requirements of your network, or as other applications are introduced (see [Table 2: Crosswork Network Controller packages, on page 6](#) for more information on VM count for each Crosswork Network Controller package). Please consult with the Cisco Customer Experience team for guidance on your deployment to best meet your needs.

The table below explains the network requirements per VM host:

Table 27: Network Requirements (per VM)

Requirement	Description
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.
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.
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.

Requirement	Description
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.
Backup Server	Cisco Crosswork will back up the configuration of the system to an external server using SCP. The SCP server storage requirements will vary slightly but you must have at least 50 GB of storage.

- Cisco Crosswork Infrastructure and applications are built to run as a distributed collection of containers managed by Kubernetes. 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.

Crosswork Data Gateway VM Requirements

This section provides information about the general guidelines and minimum requirements for installing Crosswork Data Gateway.

- [Selecting the Crosswork Data Gateway Deployment Type, on page 115](#)
- [Crosswork Data Gateway VM Requirements, on page 116](#)

Selecting the Crosswork Data Gateway Deployment Type

The following table lists the deployment profile that must be used for installing Crosswork Data Gateway in each Crosswork product:



Note The VM resource requirements for Crosswork Data Gateway are different for each type and cannot be modified. Therefore, if your requirements change, you must re-deploy the Crosswork Data Gateway to move from one type to another. For more information, see the *Redeploy a Crosswork Data Gateway VM* section in [Cisco Crosswork Network Controller 5.0 Administration Guide](#).

Table 28: Crosswork Data Gateway deployment types

Cisco Crosswork Product	Crosswork Data Gateway Deployment
Crosswork Network Controller (combination of Crosswork Active Topology & Crosswork Optimization Engine)	On-Premise Standard
Crosswork Optimization Engine	On-Premise Standard
Crosswork Zero Touch Provisioning	On-Premise Standard
Crosswork Change Automation	On-Premise Extended
Crosswork Health Insights	On-Premise Extended

Cisco Crosswork Product	Crosswork Data Gateway Deployment
Crosswork Service Health	On-Premise Extended

Crosswork Data Gateway VM Requirements

The VM requirements for Crosswork Data Gateway are listed in the following table.

Table 29: Crosswork Data Gateway Requirements for on-premise applications

Requirement	Description
Data Center	VMware. See Installation Prerequisites for VMware vCenter , on page 19.

Requirement	Description			
Interfaces	<p>Minimum: 1 Maximum: 3</p> <p>Cisco Crosswork Data Gateway can be deployed with either 1, 2, and 3 interfaces as per the combinations below:</p> <p>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.</p>			
	No. of NICs	vNIC0	vNIC1	vNIC2
	1	<ul style="list-style-type: none"> • Management Traffic • Control/Data Traffic • Device Access Traffic 	—	—
	2	Management Traffic	<ul style="list-style-type: none"> • Control/Data Traffic • Device Access Traffic 	—
	3	Management Traffic	Control/Data Traffic	Device Access Traffic
	<ul style="list-style-type: none"> • Management traffic: for accessing the Interactive Console and passing the Control/Data information between servers (for example, a Crosswork application to Crosswork Data Gateway). • 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 access and data collection. <p>Note Due to security policies, traffic from subnets of a vNIC received on other vNICs is dropped. For example, in a 3 vNIC model setup, all device traffic (incoming and outgoing) must be routed through default vNIC2. Crosswork Data Gateway drops device traffic received over vNIC0 and vNIC1.</p>			

Requirement	Description
IP Addresses	<p>1 or 2 IPv4 or IPv6 addresses based on the number of interfaces you choose to use.</p> <p>An additional IP address to be used as the Virtual IP (VIP) address. For each active data gateway, a unique VIP is required.</p> <p>For more information, refer to the <i>Interfaces</i> section in the Table 24: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 69.</p> <p>Note Crosswork does not support dual stack configurations. Therefore, all addresses for the environment must be either IPv4 or IPv6.</p> <p>In a 3-NIC deployment, you need to provide an IP address for Management interface (vNIC0) and Control/Data interface (vNIC1) during installation. A virtual IP address for Device Access Traffic (vNIC2) is assigned when you create a Crosswork Data Gateway to a pool as explained in the <i>Create a Crosswork Data Gateway Pool</i> section in Cisco Crosswork Network Controller 5.0 Administration Guide.</p>
NTP Servers	<p>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 devices, clients, and servers across your network. Verify that the NTP IP address or host name is reachable on the network else the installation fails.</p> <p>Also, the ESXi hosts that 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.</p>
DNS Servers	<p>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 fails if the servers cannot be reached.</p>
DNS Search Domain	<p>The search domain you want to use with the DNS servers, for example, cisco.com. You can have only one search domain.</p>
Internet Control Message Protocol (ICMP)	<p>The Crosswork uses ICMP in the communications with Crosswork Data Gateway. Ensure that the firewall between Crosswork and the Crosswork Data Gateway passes this traffic.</p>

TCP/UDP Port requirements

Crosswork Cluster Port Requirements

The following TCP/UDP port numbers need to be allowed through any external firewall or access-list rules deployed by the data center administrator. Depending on the NIC deployment, these ports may be applicable to only one or both NICs.



Note Crosswork cluster ports allow bidirectional flow of information.

Table 30: External Ports used by Crosswork Cluster

Port	Protocol	Used for
22	TCP	Remote SSH traffic
111	TCP/UDP	GlusterFS (port mapper)
179	TCP	Calico BGP (Kubernetes)
80, 443	TCP	Accessing the EC2 API.
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)
30606	TCP	Docker Registry
30621	TCP	For FTP (available on data interface only). The additional ports used for file transfer are 31121 (TCP), 31122 (TCP), and 31123 (TCP). This port is available only when the supported application is installed on Cisco Crosswork and the FTP settings are enabled.
30622	TCP	For SFTP (available on data interface only) This port is available only when the supported application is installed on Cisco Crosswork and the SFTP settings are enabled.
49152:49370	TCP	GlusterFS

Table 31: Ports used by other Crosswork components

Port	Protocol	Used for
30602	TCP	to monitor the installation (Crosswork Network Controller)
30603	TCP	Crosswork Network Controller Web 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.
30607	TCP	Crosswork Data Gateway vitals collection
30608	TCP	Data Gateway gRPC channel with Data Gateway VMs
30609	TCP	Used by the Expression Orchestrator (Crosswork Service Health)
30610	TCP	Used by the Metric Scheduler (Crosswork Service Health)
30611	TCP	Used by the Expression Tracker component (Crosswork Service Health)
30617	TCP	Used for Secure Zero Touch Provisioning (Secure ZTP) on the ZTP server.
30620	TCP	Used to receive plug-and-play HTTP traffic 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.

Table 32: Destination Ports used by Crosswork Cluster

Port	Protocol	Used for
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).

Port	Protocol	Used for
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

Crosswork Data Gateway Port Requirements

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

Inbound: Crosswork Data Gateway listens on the specified ports.

Outbound: Crosswork Data Gateway connects to external destination IP on the specified ports.

Table 33: 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



Note SCP port can be tuned.

Table 34: Ports to be Opened for Device Access Traffic

Port	Protocol	Used for	Direction
161	UDP	SNMP Collector	Outbound

Port	Protocol	Used for	Direction
1062	UDP	SNMP Trap Collector Note This is the default value. You can change this value after installation from the Cisco Crosswork UI. See Configure Crosswork Data Gateway Global Parameters for more information.	Inbound
9010	TCP	MDT Collector	Inbound
22	TCP	CLI Collector	Outbound
6514	TLS	Syslog Collector	Inbound
9898	TCP	This is the default value. You can change this value after installation from the Cisco Crosswork UI. See Configure Crosswork Data Gateway Global Parameters for more information.	
9514	UDP		
Site Specific Default ports differ from XR, XE to vendor. Check platform-specific documentation.	TCP	gNMI Collector	Outbound

Table 35: Ports to be Opened for Control/Data Traffic

Port	Protocol	Used for	Direction
30649	TCP	Crosswork Controller	Outbound

Port	Protocol	Used for	Direction
30993 30994 30995	TCP	Crosswork Kafka	Outbound
Site Specific	Site Specific	Kafka and gRPC Destination	Outbound

IP Address Restrictions

Crosswork cluster uses the following IP ranges for internal communications. This cannot be changed. As a result, these subnets cannot be used for devices or other purposes within your network.

You are recommended to isolate your Crosswork cluster to ensure all the communications stay within the cluster. Please also ensure that address spaces do not overlap for any of the external integration points (e.g. connections to devices, connections to external servers that Crosswork is sending data to, connections to the NSO server, etc.).



Note This is applicable for cluster installation and for adding a static route.

Table 36: Protected IP Subnets

IP Type	Subnet	Remarks
IPv4	172.17.0.0/16	Docker Subnet (Infrastructure)
	169.254.0.0/16	Link local address block
	127.0.0.0/8	Loopback address
	192.88.99.0/24	Reserved, previously used for relay servers to do IPv6 over IPv4
	240.0.0.0/4	Reserved for future use (previously class E block)
	224.0.0.0/4	MCAST-TEST-NET
	0.0.0.0/8	Current network, valid as source address only

IP Type	Subnet	Remarks
IPv6	2001:db8:1::/64	Docker Subnet (Infrastructure)
	fdfb:85ef:26ff::/48	Pod Subnet (Infrastructure)
	fd08:2eef:c2ee::/110	Service Subnet (Infrastructure)
	::1/128	Loopback address
	fe80::/10	Link local
	ff00::/8	IPv6 Multicast
	2002::/16	Reserved, previously used for relay servers to do IPv6 over IPv4
	2001:0000::/32	Terredo tunnel and relay
	2001:20::/28	Used by ORCHID and not IPv6 routable
	100::/64	Discard prefix, used in specific use-cases not applicable to Crosswork Zero Touch Provisioning
	::/128	Unspecified address, cannot be assigned to hosts
	::ffff:0:0/96	IPv4 mapped addresses
	::ffff:0:0:0/96	IPv4 translated addresses

Supported Web Browsers

To access the Crosswork UI after installing the infrastructure, we recommend using either of the browsers which have been validated:

Table 37: Supported Web Browsers

Browser	Version
Google Chrome (recommended)	92 or later
Mozilla Firefox	70 or later

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

In addition to using a supported browser, all client desktops accessing geographical maps in the Crosswork applications must be able to reach the mapbox.com site. Customers not wishing to have Cisco Crosswork access an external site can choose to install the map files locally.

What to do next:

Return to the installation workflow: [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)



CHAPTER 8

Install Cisco Crosswork Network Controller on AWS EC2

This chapter contains the following topics:

- [Installation Overview, on page 125](#)
- [Extract CF Template Image, on page 125](#)
- [Roles and Policy Permissions, on page 127](#)
- [Configure the CloudFormation \(CF\) Template Parameters, on page 127](#)
- [Install Using Module Deployment Method, on page 140](#)
- [Manage CF Template Deployment, on page 147](#)
- [Accessing the Crosswork UI, on page 149](#)
- [Crosswork Data Gateway Post-installation Tasks, on page 150](#)

Installation Overview

This section provides an overview of how Cisco Crosswork is installed on Amazon EC2.

Cisco Crosswork uses the CloudFormation (CF) templates to deploy the cluster stacks. The CF process is faster and less error-prone than the manual procedure to build the cluster, however you must have the necessary skills to prepare a CF template with details of the cluster deployment.



Note The terms 'stack' and 'instance' refers to cluster and VM respectively.



Important The CF templates (.yaml file) provided are samples that must be customized according to your production preferences and executed as per the steps mentioned in this chapter.

Extract CF Template Image

This section explains the procedure to extract and validate the Cisco Crosswork CF template image.



Attention The file names mentioned in this topic are sample names and may differ from the actual file names in release version.

Step 1 Download the CF template package (**`cw-na-platform-cft-5.0.0-signed.tar.gz`**).

Step 2 Use the following command to unzip the package:

```
tar -xzvf cw-na-platform-cft-5.0.0-signed.tar.gz
```

The contents of the package is unzipped to a new directory. This new directory contains the CF template image and files necessary to validate the image.

For example:

```
tar -xzvf cw-na-platform-cft-5.0.0-signed.tar.gz
x CFT-5.0.0_release500_2.tar.gz
x CFT-5.0.0_release500_2.tar.gz.signature
x README
x CW-CCO_RELEASE.cer
x cisco_x509_verify_release.py3
x cisco_x509_verify_release.py
```

Step 3 Review the contents of the README file in order to understand everything that is in the package and how it will be validated in the following steps.

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

Note Use `python --version` to find out the version of Python on your machine.

If you are using Python 2.x, use the following command to validate the file:

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

If you are using Python 3.x, use the following command to validate the file:

```
python cisco_x509_verify_release.py3 -e <.cer file> -i <.tar.gz file> -s <.tar.gz.signature file>
-v dgst -sha512
```

For example:

```
python cisco_x509_verify_release.py3 -e CW-CCO_RELEASE.cer -i CFT-5.0.0_release450_2.tar.gz -s
CFT-5.0.0_release450_2.tar.gz.signature -v dgst -sha512
Retrieving CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from CW-CCO_RELEASE.cer.
Successfully verified the signature of CFT-5.0.0_release450_2.tar.gz using CW-CCO_RELEASE.cer
```

The contents of the package is extracted and validated successfully.

Step 5 In the directory, locate the `install-cnc-templates` file and follow the instructions provided within its **Description** section. Customize the CF templates in the directory to install Cisco Crosswork on Amazon EC2.

What to do next

Return to the installation workflow: [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)

Roles and Policy Permissions

This section describes the roles and the policy permissions that you must have when deploying the CF template on Amazon. For information on how to create and manage the roles, refer to the Amazon documentation.

Table 38: Amazon EC2 Roles and Actions Assigned to the Roles

Role	Actions
EC2	DescribeInternetGateways, DescribeNetworkInterfaces, DescribeImages, DeleteLaunchTemplate, DescribeSubnets, DescribeAccountAttributes, DescribeSecurityGroups, RunInstances, DescribeVpcs, DescribeInstances, CreateNetworkInterface, CreateTags, DescribeKeyPairs, CreateLaunchTemplate, DeleteNetworkInterface, TerminateInstances
ELB	DescribeLoadBalancers, CreateLoadBalancer, ModifyLoadBalancerAttributes, AddTags, DeleteLoadBalancer
ELB v2	DescribeLoadBalancers, CreateLoadBalancer, AddTags, DeleteLoadBalancer, CreateTargetGroup, CreateListener, DeleteListener, DescribeTargetGroups, ModifyLoadBalancerAttributes, DescribeListeners, RegisterTargets, DeleteTargetGroup, ModifyTargetGroupAttributes, DescribeTargetHealth
IAM	CreateNodegroup, DescribeNodegroup, DeleteNodegroup

Configure the CloudFormation (CF) Template Parameters

This section explains the important parameters that must be specified for module deployments.

- [CF Template Parameters for Installing Cisco Crosswork Cluster VMs, on page 128](#)
- [CF Template Parameters for Installing Crosswork Data Gateway, on page 134](#)
- [CF Template Parameters for Installing NSO, on page 137](#)
- [CF Template Parameters for Installing Single Hybrid Cluster or Worker Node, on page 138](#)



Important

- The parameters that are mandatory for creating the templates are indicated explicitly. Parameters without this indication are optional and are populated with the default values, which you can alter based on your deployment requirement.
- All IP addresses you enter as parameters should be available.

CF Template Parameters for Installing Cisco Crosswork Cluster VMs

This section describes the parameters that are required for deploying Cisco Crosswork Cluster VMs with 3 hybrid VMs on Amazon EC2. It also describes the Management and Data NLB parameters.

Once you have determined the subnet for your cluster nodes and any other virtual machines you are going to deploy, confirm that there are enough available IP addresses to support the number of VMs (and virtual IP addresses) needed.

Table 39: Cisco Crosswork Cluster VMs Deployment Parameters

Parameter	Description
VpcId	The virtual private cloud (VPC) ID of your existing VPC. For example, vpc-0f83aac74690101a3.
SecGroup	Precreated security group that must be applied to the stack. For example, sg-096ff4bc355af16a0. The group must allow ingress access to ports 22, 30160:31560.
CwSSHPassword	The SSH password of the Crosswork Network Controller. Important We recommend using an external secret store for the password.
CwAmiId	The Crosswork AMI ID. This is a mandatory parameter.
CwMgmtSubnet1Id	Management subnet for Crosswork VM 1. This is a mandatory parameter.
CwMgmtSubnet2Id	Management subnet for Crosswork VM 2. This is a mandatory parameter.
CwMgmtSubnet3Id	Management subnet for Crosswork VM 3. This is a mandatory parameter.
CwMgmtSubnet1Netmask	The first management subnet netmask in the dotted-decimal form. For example, 255.255.255.0. This parameter is ignored when deploying on a single interface. This is a mandatory parameter.
CwMgmtSubnet2Netmask	The second management subnet netmask in the dotted-decimal form. For example, 255.255.255.0. This parameter is ignored when deploying on a single interface. This is a mandatory parameter.

Parameter	Description
CwMgmtSubnet3Netmask	The third management subnet netmask in the dotted-decimal form. For example, 255.255.255.0. This parameter is ignored when deploying on a single interface. This is a mandatory parameter.
CwMgmtSubnet1Gateway	The management default gateway on the selected data subnet. Typically, the first address on the subnet. This parameter is ignored when deployed on single interface mode. This is a mandatory parameter.
CwMgmtSubnet2Gateway	The management default gateway on the selected data subnet. Typically, the first address on the subnet. This parameter is ignored when deployed on single interface mode. This is a mandatory parameter.
CwMgmtSubnet3Gateway	The management default gateway on the selected data subnet. Typically, the first address on the subnet. This parameter is ignored when deployed on single interface mode. This is a mandatory parameter.
ManagementVIPName	Crosswork Management VIP name. For example, dev1-cwmgnt. This will be the host name to access the Crosswork cluster.
DataVIPName	Crosswork Data VIP name. For example, dev1-cwdata.
Route53DomainName	Domain name used for all Route53 objects. This is the DNS domain name for the Crosswork cluster. This is a mandatory parameter.
HostedZoneId	The Hosted Zone ID provided with the domain name (Route53DomainName). The Network Load Balancer (NLB) deployments require a predefined Route53 hosted zone. This is a mandatory parameter.
UseExternalNLB	Determines whether to use an external NLB for the Crosswork cluster (multi-AZ or subnet) or a Crosswork VIP (only single AZ or subnet). Options are <code>True</code> or <code>False</code> . This is a mandatory parameter.
CwClusterPlacementStrategy	The EC2 instance placement strategy that is valid for single availability zone. Default 'cluster' ensures maximum throughput. Options are: <ul style="list-style-type: none"> • cluster • partition • spread

Parameter	Description
CwNodeType	<p>The Crosswork Node Type for deployment. Options are <code>Hybrid</code> or <code>Worker</code>.</p> <p>A replacement Hybrid node must reuse the same IP addresses as the Hybrid node it is replacing.</p> <p>Default value is <code>Worker</code>.</p> <p>This is a mandatory parameter.</p>
InterfaceDeploymentMode	<p>The deployment mode.</p> <p>Options are <code>1</code> to deploy the Management interface or <code>2</code> to deploy the Management and Data interface.</p>
CwDataSubnet1Id	<p>Data subnet of Crosswork VM 1.</p> <p>In a single interface, the deployments happen on the subnet where the Management interface is deployed.</p> <p>This is a mandatory parameter.</p>
CwDataSubnet2Id	<p>Data subnet of Crosswork VM 2.</p> <p>In a single interface, the deployments happen on the subnet where the Management interface is deployed.</p> <p>This is a mandatory parameter.</p>
CwDataSubnet3Id	<p>Data subnet of Crosswork VM 3.</p> <p>In a single interface, the deployments happen on the subnet where the Management interface is deployed.</p> <p>This is a mandatory parameter.</p>
CwDataSubnet1Netmask	<p>The first data subnet netmask in the dotted-decimal form. For example, <code>255.255.255.0</code>. This parameter is ignored when deploying in a single interface mode.</p> <p>This is a mandatory parameter.</p>
CwDataSubnet1Gateway	<p>The first default data gateway on the selected data subnet. Typically, the value is the first address on the subnet. This parameter is ignored when deploying in a single interface mode.</p> <p>This is a mandatory parameter.</p>
CwDataSubnet2Netmask	<p>The second data subnet netmask in the dotted-decimal form. For example, <code>255.255.255.0</code>. This parameter is ignored when deploying in a single interface mode.</p> <p>This is a mandatory parameter.</p>
CwDataSubnet2Gateway	<p>The second data subnet netmask in the dotted-decimal form. This parameter is ignored when deploying in a single interface mode.</p> <p>This is a mandatory parameter.</p>

Parameter	Description
CwDataSubnet3Netmask	The third data subnet netmask in the dotted-decimal form. For example, 255.255.255.0. This parameter is ignored when deploying in a single interface mode. This is a mandatory parameter.
CwDataSubnet3Gateway	The third data subnet netmask in the dotted-decimal form. This parameter is ignored when deploying in a single interface mode. This is a mandatory parameter.
CwMgmtVIP	The current Crosswork Management VIP address.
CwDataVIP	The current Crosswork Data VIP address. When using an external NLB, you can leave this parameter empty.
Cw1MgmtIP	A free address on the management subnet. If not specified, an address is automatically assigned.
Cw1DataIP	A free address on the data subnet. If not specified, an address is automatically assigned.
Cw2MgmtIP	A free address on the management subnet. If not specified, an address is automatically assigned .
Cw2DataIP	A free address on the data subnet. If not specified, an address is automatically assigned.
Cw3MgmtIP	A free address on the management subnet. If not specified, an address is automatically assigned.
Cw3DataIP	A free address on the data subnet. If not specified, an address is automatically assigned .
OtherCwMgmtIP1	The Management IP address \#1 of the existing Crosswork node. This is used when the deployment happens with an external load balancer.
OtherCwMgmtIP2	The Management IP address \#2 of the existing Crosswork node. This parameter is used when the deployment happens with an external load balancer.
OtherCwDataIP1	The Data IP address \#1 of the existing Crosswork node. This parameter is used when the deployment happens with an external load balancer.
OtherCwDataIP2	The Data IP address \#2 of the existing Crosswork node. This parameter is used when the deployment happens with an external load balancer.

Table 40: Crosswork VM Customization

Parameter	Description
InstanceType	The EC2 instance type for the node instances. This is a mandatory parameter.
RunAsSpotInstance	A spot instance. Options are: <ul style="list-style-type: none"> • True: to enable the feature • False: to disable the feature Default value is False. This is a mandatory parameter.
DataDiskSize	Crosswork data disk size. The default is 450 GB and should be fine for most deployments. Enter the default unless otherwise directed by Cisco Customer Experience team. This is a mandatory parameter.
K8sServiceNetwork	The network address for the Kubernetes service network. The CIDR range is fixed to '/16'. If not provided, the default will be taken, that is, 10.96.0.0. This is a mandatory parameter.
K8sPodNetwork	The network address for the Kubernetes pod network. The CIDR range is fixed to '/16'. This is a mandatory parameter.
SkipAutoInstall	Configures the Skip Auto Install feature. Options are: <ul style="list-style-type: none"> • True: to enable the feature • False: to disable the feature Default value is False. This is a mandatory parameter.

Table 41: Cisco Crosswork Cluster Management NLB Deployment Parameters

Parameter	Description
VpcId	The virtual private cloud (VPC) ID of your existing VPC. For example, vpc-0f83aac74690101a3.
CwTargetSubnetIdList	This is a list of the Crosswork management subnets. This is a mandatory parameter.
CwTargetIP1	This is a Crosswork VM management IP. In this template, this is a mandatory parameter.

Parameter	Description
CwTargetIP2	This is a Crosswork VM management IP. In this template, this is a mandatory parameter.
CwTargetIP3	This is a Crosswork VM management IP. In this template, this is a mandatory parameter.
Route53DomainName	Domain name used for all Route53 objects. This is a mandatory parameter.
HostName	The domain name used for all Route53 objects. This is a mandatory parameter.
HostedZoneId	The hosted zone ID. This is a mandatory parameter.

Table 42: Data NLB Deployment Parameters

Parameter	Description
VpcId	The virtual private cloud (VPC) ID of your existing VPC. For example, vpc-0f83aac74690101a3.
CwTargetSubnetIdList	The first management subnet for the Crosswork VMs. This is a mandatory parameter.
CwTargetIP1	A free address on the management subnet. If not specified, an address is automatically assigned.
CwTargetIP2	A free address on the management subnet. If not specified, an address is automatically assigned.
CwTargetIP3	A free address on the management subnet. If not specified, an address is automatically assigned.
Route53DomainName	Domain name used for all Route53 objects. This is a mandatory parameter.
HostName	The domain name used for all Route53 objects. This is a mandatory parameter.
HostedZoneId	The hosted zone ID. This is a mandatory parameter.

CF Template Parameters for Installing Crosswork Data Gateway

This section describes the parameters that are required when creating the Crosswork Data Gateway control plane, node, pool, and other important containers. It also has parameters that are required for creating EC2 Crosswork Data Gateway NLB stack.

Table 43: Crosswork Data Gateway Deployment Parameters

Parameter	Description
VpcId	The virtual private cloud (VPC) ID of your existing VPC. For example, vpc-0f83aac74690101a3.
SecGroup	Precreated security group that must be applied to the stack. For example, sg-096ff4bc355af16a0. The group must allow ingress access to all ports that Crosswork, NSO, Crosswork Data Gateway, and IOS-XR uses.
CDGSSHPassword	The SSH password to be configured on the Crosswork Data Gateway node.
CDGOperPassword	The password to be configured on the Crosswork Data Gateway for Dg-Oper user.
CDGAmiId	The Crosswork Data Gateway AMI ID.
InstanceType	The EC2 instance type for the node instances. This is a mandatory parameter.
CNCControllerIP	Host address or name of the Crosswork Data Gateway controller. In a multi-AZ deployments, this value must be the name. This is a mandatory parameter.
CNCControllerPassword	The cw-admin user password used to access Crosswork or CNC Controller.
InterfaceDeploymentMode	Crosswork Data Gateway deployment mode. The options are: <ul style="list-style-type: none"> • 1: to deploy all the interfaces. • 2: to deploy the Management and Data interfaces. • 3: to deploy the Management, Data, and Control interfaces.
CDGInterface0IPAddress	A free IP address on the subnet. If set to 0.0.0.0, the IP address is automatically allocated. This is a mandatory parameter.
CDGInterface0SubnetId	The first interface subnet for the Crosswork Data Gateway VM.
CDGInterface0Gateway	The default gateway on the selected subnet. Typically, the first address on the subnet.

Parameter	Description
CDGInterface0SubnetNetmask	The first interface subnet netmask in the dotted-decimal form. For example, 255.255.255.0. This is a mandatory parameter.
CDGInterface1IPAddress	A free IP address on the first subnet. If set to 0.0.0.0, the IP address is automatically allocated. This is a mandatory parameter.
CDGInterface1SubnetId	The second interface subnet for the Crosswork Data Gateway. The subnet must be in the same availability zone as the CDGInterface0SubnetId.
CDGInterface1Gateway	The second interface default gateway on the selected subnet. Typically, the first address on the subnet. This is a mandatory parameter.
CDGInterface1SubnetNetmask	The second interface subnet netmask in the dotted-decimal form. For example, 255.255.255.0. This parameter is ignored when dual interface mode is not used. This is a mandatory parameter.
CDGInterface2IPAddress	A free IP address on the second subnet. If set to 0.0.0.0, the IP address is automatically allocated. This is a mandatory parameter.
CDGInterface2SubnetId	The third interface subnet for the Crosswork Data Gateway VM. The subnet must be in the same availability zone as the CDGInterface0SubnetId.
CDGInterface2Gateway	The third interface default gateway on the selected subnet. Typically, the first address on the subnet. This is a mandatory parameter.
CDGInterface2SubnetNetmask	The third interface subnet netmask in the dotted-decimal form. For example, 255.255.255.0. This parameter is ignored when triple interface mode is not used. This is a mandatory parameter.
CNCControllerIP	Host address of the Crosswork Data Gateway controller.

Parameter	Description
HANetworkMode	<p>The Crosswork Data Gateway HA mode.</p> <p>The pool mode options are:</p> <ul style="list-style-type: none"> • L2: Use this option when you specify IP addresses for creating the HA pool. • L3: Use this option when you specify FQDN for creating the HA pool and for multisubnet deployment. <p>For information on the pool types, refer to the <i>Create a Cisco Crosswork Data Gateway Pool</i> section in Cisco Crosswork Network Controller 5.0 Administration Guide.</p> <p>This is a mandatory parameter.</p>
DataDiskSize	<p>Size of the Crosswork data disk. The minimum size is 20. Default size is 50.</p> <p>This is a mandatory parameter.</p>
CDGProfile	<p>The deployment profile of Crosswork Data Gateway.</p> <ul style="list-style-type: none"> • Standard • Extended <p>This is a mandatory parameter.</p>
CdgInstanceHostname	<p>The Crosswork Data Gateway instance name, for example CDG-01.</p>

Table 44: Crosswork Data Gateway and Network Load Balancer (NLB) Stack Parameters

Parameter	Description
VpcId	<p>The VPC ID of the worker instances.</p> <p>This is a mandatory parameter.</p>
SubnetId1	<p>The management ID of subnet 1.</p> <p>This is a mandatory parameter.</p>
SubnetId2	<p>The management ID of subnet 2.</p> <p>This is a mandatory parameter.</p>
DomainName	<p>The domain name.</p> <p>This is a mandatory parameter.</p>
HostedZoneId	<p>The hosted zone ID.</p> <p>This is a mandatory parameter.</p>

Parameter	Description
CdgPoolHostname	Name of the Route53 record. This is a mandatory parameter.
CdgTargetIP1	The IP address 1 of the Management node. In the event of a single Crosswork Data Gateway, one target IP must be configured.
CdgTargetIP2	The IP address 2 of the Management node.
LBIPAddress1	The first LB IP address on subnet. This is a mandatory parameter.
LBIPAddress2	The second LB IP address on subnet. This is a mandatory parameter.

CF Template Parameters for Installing NSO

This section describes the parameters that are required for deploying NSO on Amazon EC2.

Table 45: NSO Deployment Parameters

Parameter	Description
VpcId	The virtual private cloud (VPC) ID of your existing VPC. For example, vpc-0f83aac74690101a3.
SecGroup	Precreated security group that must be applied to the stack. For example, sg-096ff4bc355af16a0. The group must allow ingress access to ports 22, 30160:31560.
NSOSubnetId	The subnet for the NSO VM.
KeyName	Name of an existing EC2 KeyPair to enable SSH access to the instance.
NSOAmiId	The NSO AMI ID. This is a mandatory parameter.
NSOInterface0IPAddress	A free IP address on the second subnet. If set to 0.0.0.0, the IP address is automatically allocated. This is a mandatory parameter.
InstanceType	The EC2 instance type for the node instances. This is a mandatory parameter.

CF Template Parameters for Installing Single Hybrid Cluster or Worker Node

This section describes the parameters that are required for deploying a single cluster node (Hybrid or Worker).



Attention

- A replacement hybrid node must reuse the same IP addresses as the hybrid VM it is replacing.
- As you will be adding another node (worker or hybrid) to the existing cluster determine the subnet that is being used and find an additional available IP on that subnet.

Table 46: Single Hybrid Cluster or Worker Cisco Crosswork Nodes Deployment Parameters

Parameter	Description
VpcId	The virtual private cloud (VPC) ID of your existing VPC. For example, vpc-0f83aac74690101a3.
SecGroup	Precreated security group that must be applied to the stack. For example, sg-096ff4bc355af16a0. The group must allow ingress access to ports 22, 30160:31560.
EC2ENIRole	Existing role name for the Crosswork cluster. The role must permit EC2 access.
CwAmiId	The Crosswork AMI ID. This is a mandatory parameter.
CwSSHPassword	The SSH password of the Crosswork Network Controller. Important We recommend using an external secret store for the password.
InstanceType	The EC2 instance type for the node instances. This is a mandatory parameter.
ManagementVIPName	Crosswork Management VIP name. For example, dev1-cwmgmt.
DataVIPName	Crosswork Data VIP name. For example, dev1-cwdata.
Route53DomainName	Domain name used for all Route53 objects. This is a mandatory parameter.
UseExternalNLB	Determines whether to use an external NLB for the Crosswork cluster (multi-AZ or subnet) or a Crosswork VIP (only single AZ or subnet). Options are <code>True</code> or <code>False</code> . This is a mandatory parameter.
CwMgmtSubnetId	The management subnet for the Crosswork VMs.

Parameter	Description
CwMgmtSubnetNetmask	The management subnet netmask in dotted decimal form. For example, 255.255.255.0. This parameter is ignored when deploying in a single interface mode. This is a mandatory parameter.
CwDataSubnetGateway	The management default gateway on the selected data subnet. Typically, the first address on the subnet. This parameter is ignored when deployed on single interface mode. This is a mandatory parameter.
CwDataSubnetId	The data subnet for the Crosswork VMs.
CwDataSubnetNetmask	The data subnet netmask in dotted decimal form. For example, 255.255.255.0. This parameter is ignored when deploying in a single interface mode. This is a mandatory parameter.
CwDataSubnetGateway	The data default gateway on the selected data subnet. Typically, the first address on the subnet. This parameter is ignored when deployed on single interface mode. This is a mandatory parameter.
CwNodeType	The Crosswork Node Type for deployment. Options are <code>Hybrid</code> or <code>Worker</code> . A replacement Hybrid node must reuse the same IP addresses as the Hybrid node it is replacing. This is a mandatory parameter.
DataDiskSize	Crosswork data disk size. The default is 450 (in GB) and should be fine for most deployments. Enter the default unless otherwise directed by Cisco Customer Experience team. This is a mandatory parameter.
K8sServiceNetwork	The network address for the Kubernetes service network. The CIDR range is fixed to '/16'. If not provided, the default (10.96.0.0) is taken.
K8sPodNetwork	The network address for the Kubernetes pod network. The CIDR range is fixed to '/16'. If not provided, the default (10.244.0.0) is taken.

Table 47: Optional VM parameters

Parameters	Description
CwMgmtVIP	The current Crosswork Management VIP address.
CwDataVIP	The current Crosswork Data VIP address. When using an external NLB, you can leave this parameter empty.

Parameters	Description
CwlMgmtIP	A free address on the management subnet. If not specified, an address is automatically assigned.
CwlDataIP	A free address on the data subnet. If not specified, an address is automatically assigned.
OtherCwMgmtIP1	The first Management IP address of the existing Crosswork node. This is used when the deployment happens with an external load balancer.
OtherCwMgmtIP2	The second Management IP address of the existing Crosswork node. This parameter is used when the deployment happens with an external load balancer.
OtherCwDataIP1	The first Data IP address of the existing Crosswork node. This parameter is used when the deployment happens with an external load balancer.
OtherCwDataIP2	The second Data IP address of the existing Crosswork node. This parameter is used when the deployment happens with an external load balancer.

Install Using Module Deployment Method

The module-based deployment procedures involve deploying each resource separately. Each resource has its own template file, which can be used to deploy them individually. For more information, see the following topics:

- [Install Cisco Crosswork Cluster on Amazon EC2, on page 140](#)
- [Install Crosswork Data Gateway on Amazon EC2, on page 141](#)
- [Install Cisco NSO on Amazon EC2, on page 145](#)
- [Deploy an Additional Crosswork Cluster Node, on page 146](#)

Install Cisco Crosswork Cluster on Amazon EC2

This section provides an overview of how Cisco Crosswork cluster is installed on Amazon EC2.

Cisco Crosswork uses a set of CF templates to deploy Crosswork cluster.

Crosswork Cluster Deployment Workflow

The Crosswork cluster deployment procedure involves deploying various Crosswork resources using the corresponding YAML files.

Table 48: Resources Deployed During Crosswork Cluster Deployment

Resource	Description
EC2 Cluster	The main stack (cw-cluster.yaml) which will deploy other nested stacks for creating EC2 CW NLBs.

Resource	Description
Management NLB	The cw-mgmt-nlb.yaml file creates Network Load Balancer, Target Groups, Listeners and Route53Record for EC2 CW Management Nodes.
Data NLB	The cw-data-nlb.yaml file creates Network Load Balancer, Target Groups, Listeners and Route53Record for EC2 CW Data Nodes

Installation Parameters

For list of important parameters that you must specify in the CF templates that are used to deploy Crosswork cluster, see [CF Template Parameters for Installing Cisco Crosswork Cluster VMs, on page 128](#). Crosswork cluster is deployed on Amazon EC2 based on the parameters specified in the templates.



Note Once you have determined the subnet for your cluster nodes and any other virtual machines you are going to deploy, confirm that there are enough available IP addresses to support the number of VMs (and virtual IP addresses) needed.

Deploy the CF Templates

You can install the Crosswork cluster on Amazon EC2 by customizing the CF templates. For the list of CF templates that are used for Crosswork cluster deployment, see [Crosswork Cluster Deployment Workflow, on page 140](#).

For instructions on how to deploy the CF templates on Amazon EC2, see [Deploy a CF Template, on page 147](#).

Verify the Installation

Verify that the Crosswork cluster installation is successful by following the steps in [Monitor the Installation, on page 148](#).

Deploy an Additional Crosswork Cluster Node

For instructions on how to deploy an additional worker/hybrid node on the Crosswork cluster, see [Deploy an Additional Crosswork Cluster Node, on page 146](#).

What to do next

Return to the installation workflow: [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)

Install Crosswork Data Gateway on Amazon EC2

This section provides an overview of how Crosswork Data Gateway is installed on Amazon EC2.

Crosswork Data Gateway Deployment Workflow

The Crosswork Data Gateway deployment procedure involves deploying various Crosswork resources using the corresponding YAML files.

The main file **cdg-stack-ec2.yaml** deploys the stacks for one CDG NLB (**cdg-nlb.yaml**) and two CDG (**cdg.yaml**).

- An additional Crosswork Data Gateway VM to the Crosswork Data Gateway high availability pool is deployed using the **cdg.yaml** file. For each additional VM deployment, you must repeat the deployment procedure.
- An additional NLB and Crosswork Data Gateway high availability pool is deployed using the **cdg-nlb.yaml** file.

The following table provides information about the components are installed:

Table 49: Resources Deployed During Crosswork Data Gateway Deployment

Resource	Description
EC2 Crosswork Data Gateway	The resources related to EC2 node are created by deploying the cdg.yaml file.
Crosswork Data Gateway Network Load Balancer	The EC2 NLB components (target groups, network load balancer, data listeners, and NLB route 53 record) are created by deploying the cdg-nlb.yaml file.

Installation Parameters

For list of important parameters in the Crosswork Data Gateway CF templates, see [CF Template Parameters for Installing Crosswork Data Gateway, on page 134](#).

Crosswork Data Gateway is deployed on Amazon EC2 based on the parameters specified in the CF templates. For list of CF templates that are used for Crosswork Data Gateway deployment, see [Crosswork Data Gateway Deployment Workflow, on page 141](#).

Deploy the CF Templates

For instructions on how to deploy the CF templates on Amazon EC2, see [Deploy a CF Template, on page 147](#).



Note Amazon EC2 mandates entering an IP address for the vNIC2 interface when Crosswork Data Gateway is deployed using 3 NICs. This is an AWS EC2 requirement and not imposed by Crosswork.

Verify the Installation

Verify that the Crosswork Data Gateway installation is successful by following the steps in [Monitor the Installation, on page 148](#).

What to do next

Return to the installation workflow: [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)

Auto-Configuration for Deploying Crosswork Data Gateway

The auto-configuration procedure discovers the configuration parameters that are missing, and it automatically defines the mandatory parameters to install Base VM. The configuration parameters are passed using the Dynamic Host Configuration Protocol (DHCP) framework. In the Day 0 configuration, the auto-configuration mechanism defines only the essential parameters with the default values.

A default password is provided during the auto-configuration to comply with the security policies. On the initial log in, the dg-admin and dg-oper users must change the default password. The Crosswork Data Gateway services are inactive until the default password is changed.

The auto-configuration process supports the default 3 NIC deployment. In particular, only eth0 is configured for the Management network.

The DHCP interaction takes place over the eth0 interface. The auto-configuration procedure uses the default values stored on the DHCP server. After Base VM is deployed, you can configure or modify the default values using the Interactive Console. For more information about the console, see [Cisco Crosswork Network Controller 5.0 Administration Guide](#).



Important The auto-configuration mechanism is not supported for deploying Crosswork Data Gateway on the VMware platform.

Parameters used during Auto-Configuration

The auto-configuration utility configures the following parameters with the default values. For more information about these parameters, see [Cisco Crosswork Data Gateway Parameters and Deployment Scenarios, on page 68](#).

Table 50: Cisco Crosswork Data Gateway Mandatory Deployment Parameters

Name	Parameter	Default Value
AllowRFC8190	AllowRFC8190	The default value is Yes.
Auditd Server Port	AuditdPort	The default port is 60.
Crosswork Controller Port	ControllerPort	The default port is 30607.
Description	Description	The default value is CDG auto configure.
dg-admin Passphrase	dg-adminPassword	The default password is changeme. Reset the default value with the password that you have chosen for the dg-admin user. Password must be 8-64 characters.
dg-oper Passphrase	dg-operPassword	The default password is changeme. Reset the default value with the password you have chosen for the dg-oper user. Password must be 8-64 characters.

Name	Parameter	Default Value
Data Disk Size	DGAppdataDisk	The default value of this parameter is 5.
DNS Address	DNS	The default values of this parameter are 208.67.222.222 208.67.220.220
DNS Security Extensions	DNSSEC	The default value of this parameter is False.
DNS over TLS	DNSTLS	The default value of this parameter is False.
DNS Search Domain	Domain	The default value of this parameter is localdomain.
Crosswork Data Gateway HA mode	HANetworkMode	The default value of this parameter is L2.
Hostname	Hostname	The default value of this parameter is dg-<eth0 address>. Where <eth0-address> is the address of vNIC0.
Link-Local Multicast Name Resolution	LLMNR	The default value of this parameter is False.
Multicast DNS	mDNS	The default value of this parameter is False.
NicAdministration	NicAdministration	The default value of this parameter is eth0.
NicControl	NicControl	The default value of this parameter is eth1.
NicDefaultGateway	NicDefaultGateway	The default value of this parameter is eth0.
NicExternalLogging	NicExternalLogging	The default value of this parameter is eth0.
NicManagement	NicManagement	The default value of this parameter is eth0.
NicNBExternalData	NicNBExternalData	The default value of this parameter is eth1.
NicNBSystemData	NicNBSystemData	The default value of this parameter is eth1.
NicSBData	NicSBData	The default value of this parameter is the last active interface such as eth0 for 1-NIC deployment, eth1 for 2-NIC.
NTPv4 Servers	NTP	The default values of this parameter are 162.159.200.1 65.100.46.164 40.76.132.147 104.131.139.195

Name	Parameter	Default Value
Use NTPv4 Authentication	NTPAuth	The default value of this parameter is <code>False</code> .
Profile	Profile	The default value of this parameter is <code>Standard</code> .
Syslog Multiserver Mode	SyslogMultiserverMode	The default value of this parameter is <code>Simultaneous</code> .
Syslog Server Port	SyslogPort	The default value of this parameter is <code>514</code> .
Syslog Server Protocol	SyslogProtocol	The default value of this parameter is <code>UDP</code> .
Use Syslog over TLS	SyslogTLS	The default value of this parameter is <code>False</code> .
Use Remote Auditd Server	UseRemoteAuditd	The default value of this parameter is <code>False</code> .
Use Remote Syslog Server	UseRemoteSyslog	The default value of this parameter is <code>False</code> .
vNIC IPv4 Method	Vnic0IPv4Method	The default value of this parameter is <code>DHCP</code> .
vNIC IPv4 Skip Gateway	Vnic0IPv4SkipGateway	The default value of this parameter is <code>False</code> .
vNIC IPv6 Method	Vnic0IPv6Method	The default value is <code>None</code> .
vNIC IPv6 Skip Gateway	Vnic0IPv6SkipGateway	The default value is <code>False</code> .
vNIC IPv4 Method	Vnic1IPv4Method	The default value is <code>DHCP</code> .
vNIC IPv4 Skip Gateway	Vnic1IPv4SkipGateway	The default value is <code>False</code> .
vNIC IPv6 Method	Vnic1IPv6Method	The default value is <code>None</code> .
vNIC IPv6 Skip Gateway	Vnic1IPv6SkipGateway	The default value is <code>False</code> .
vNIC IPv4 Method	Vnic2IPv4Method	The default value is <code>DHCP</code> .
vNIC IPv4 Skip Gateway	Vnic2IPv4SkipGateway	The default value is <code>False</code> .
vNIC IPv6 Method	Vnic2IPv6Method	The default value is <code>None</code> .
vNIC IPv6 Skip Gateway	Vnic2IPv6SkipGateway	The default vale is <code>False</code> .

Install Cisco NSO on Amazon EC2

This section provides an overview of how Cisco NSO is installed on Amazon EC2.

Cisco Crosswork uses a set of CF templates to deploy NSO.

NSO Deployment Workflow

The NSO deployment procedure involves deploying various Crosswork resources using the corresponding YAML files.

The **nso-stack-ec2.yaml** file deploys stacks for one NSO NLB (**nso-nlb-ec2.yaml**) and two NSOs (**nso.yaml**). See below table for more information.

Table 51: Resources Deployed During NSO Deployment

Resource	Description
EC2 NSO	The nso.yaml file is deployed to create the EC2 node resources (network interface and an instance) in the stack.
NSO NLB	The nso-nlb-ec2.yaml file is deployed to create the EC2 NLB resources (target groups, network load balancer, data listeners, and NLB route 53 record) in the stack.

Installation Parameters

For list of important parameters that you must specify in the CF templates that are used to deploy NSO, see [CF Template Parameters for Installing NSO, on page 137](#). NSO is deployed on Amazon EC2 based on the parameters specified in the templates.



Note While deleting the NSO setup, delete the NSO Route53 Record (NsoRoute53RecordName) manually.

Deploy the CF Templates

You can install NSO on Amazon EC2 by customizing the CF templates. For list of CF templates that are used for NSO deployment, see [NSO Deployment Workflow, on page 145](#).

For instructions on how to deploy the CF templates on Amazon EC2, see [Deploy a CF Template, on page 147](#).

Verify the Installation

Verify that the NSO installation is successful by following the steps in [Monitor the Installation, on page 148](#).

What to do next

Return to the installation workflow: [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)

Deploy an Additional Crosswork Cluster Node

This section explains how to deploy an additional worker/hybrid node on the Crosswork cluster.

Deploying an additional node on the Crosswork cluster involves deploying the Crosswork network configuration and VM customization resources using the **cw-add-vm.yaml** file.



Important Before deploying an additional worker node, ensure that the Crosswork cluster and Crosswork application have been created.



Note A new hybrid node **MUST** reuse the same IP addresses as the hybrid VM it is replacing, and a maximum of 3 hybrid nodes are allowed.

Installation Parameters

For list of important parameters that you must specify in the CF template that is used to deploy an additional node on the Crosswork cluster, see [CF Template Parameters for Installing Single Hybrid Cluster or Worker Node, on page 138](#). Additional nodes are deployed on the Crosswork cluster based on the parameters specified in the templates.

Deploy the CF Templates

You can install an additional worker/hybrid node on the Crosswork cluster by customizing the CF template. For instructions on how to deploy the CF templates on Amazon EC2, see [Deploy a CF Template, on page 147](#).

Verify the Installation

Verify that the nodes are attached to the Crosswork cluster. On the EC2 console, select the Crosswork cluster and make sure that the nodes that you added appear under the **Compute** section. For more information, see [Monitor the Installation, on page 148](#).

What to do next

Return to the installation workflow: [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)

Manage CF Template Deployment

The following sections explain how to deploy a CF template on Amazon EC2 and verify its installation:

- [Deploy a CF Template, on page 147](#)
- [Monitor the Installation, on page 148](#)

Deploy a CF Template

You can install Crosswork on Amazon EC2 with custom resources. Depending on the configured parameters, the needed components with the capabilities are also installed.

Before you begin

- Make sure that you have met the [Table 26: AWS Prerequisites and Settings](#) and [Amazon EC2 Settings](#) prescribed for installing Crosswork on Amazon EC2.
- Ensure that you have access to the CloudFormation templates that are stored in the S3 bucket or on your local machine. If the template is in Amazon S3, keep the URL of the template file copied.

-
- Step 1** Log in to the AWS account and navigate to the S3 bucket. If the CF template is on your local computer, you can upload the template.
- Step 2** In the AWS CloudFormation console, navigate to the **Stacks** page and choose **Create stack > With new resources (standard)**. The **Create stack** page opens.
- Step 3** Enter the following details:
- a. Under **Prerequisite - Prepare template**, select **Template is ready**.
 - b. Under **Specify template > Template source**, select one of the following options:
 - If you have the YAML or JSON file URL directing to the S3 bucket where the CF template is located, select **Amazon S3 URL**. In the **Amazon S3 URL** field, enter the URL and click **Next**.
 - If the CF template is saved on your local computer, select **Upload a template file** and click **Choose File** to select the file that you want to upload. After you have selected the template, Amazon uploads the file and displays the S3 URL. Click **Next**.
- Note** (Optional) Click **View in Designer** to view a visual representation of the execution flow in your CF template.
- Step 4** In the **Specify stack details** page, enter the relevant values for the stack name and parameter values. Click **Next**.
- Note** The parameter field names visible in this window are defined by the parameters in the CF template.
- Step 5** Review the parameter values that you have configured.
- Step 6** Under the **Capabilities**, select the check boxes next to:
- **I acknowledge that AWS CloudFormation might create IAM resources with custom names.**
 - **I acknowledge that AWS CloudFormation might require the following capability: CAPABILITY_AUTO_EXPAND.**
- Step 7** Click **Submit**.
-

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 148](#) to know how you can check the status of the installation.

Monitor the Installation

This section describes how to verify if the deployment is complete without errors.

- Step 1** In the CloudFormation console, from the left-hand side **Stacks** pane, select the stack that you have deployed.
- Step 2** The stack details are displayed on the right. Click on each tab in this window to view details of the stack. If the stack creation is in progress, the status of the stack in the **Events** tab is `CREATE_IN_PROGRESS`.
- Step 3** After the stack is created:

- The status of the stack changes to `CREATE_COMPLETE` and the **Logical ID** displays the stack name.
- The **Resources** tab displays details of the all the resources that the CF template has created, including the physical IDs.
- The **Outputs** tab has details of the VM's interface IP addresses.

What to do next

After the stack creation is complete, you can access the Crosswork UI and monitor the health of your cluster. For more information on how to log in to the Crosswork UI, see [Accessing the Crosswork UI, on page 149](#).

Accessing the Crosswork UI

After the stacks are created, you can check if all the nodes are up and running in the cluster from the Cisco Crosswork UI.

Before you begin

- Ensure that you have a spare Network Load Balancer (NLB). To access Crosswork UI, use an external NLB that routes requests to its targets using the protocol DNS and port number that you specify.
- Verify that the Crosswork cluster and pods are in the running state. For information on how to view the status of the cluster, see [Monitor the Installation, on page 148](#).
- Make sure to keep the IP address of the Management node copied. This IP address is used to access the Crosswork UI. You can copy the IP address from the **Outputs** tab of the CloudFormation console. For information on accessing the **Outputs** tab, see [Monitor the Installation, on page 148](#).

Step 1 Log in to the AWS console and navigate to **Target Groups** to register the targets.

Step 2 Under **Targets**, click **Register targets**. The **Register targets** page opens.

Step 3 In the **IPv4 address**, specify the Management IP address that you copied from the CloudFormation console.

Step 4 Specify the port as 30603. Click **Include as pending below**

Step 5 Click **Register pending targets**.

To deregister the targets that are no longer in use, select the target and click **Deregister**.

Step 6 After the target is in the healthy state, click on the load balancer name under **Details**. The **Load balancer** page opens.

Step 7 Copy the DNS name from the **DNS name** column.

Step 8 Launch as supported browser and enter the following in the address bar:

```
https://<DNS_name>:30603/
```

Note When you access 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 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 *Crosswork Network Controller 5.0 Administration Guide*.

Step 9 Log in to 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 VM Password (minimum 8 characters long, including upper & lower case letters, numbers, and one special character). Avoid using passwords similar to dictionary words (for example, "Pa55w0rd!") or relatable words (for example, C!sco123 or Cwork321!).

Step 10 (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.

What to do next

Return to the installation workflow: [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)

Crosswork Data Gateway Post-installation Tasks

This section lists the steps that you can complete after you have deployed Crosswork Data Gateway.

Configure Timezone of the Crosswork Data Gateway VM

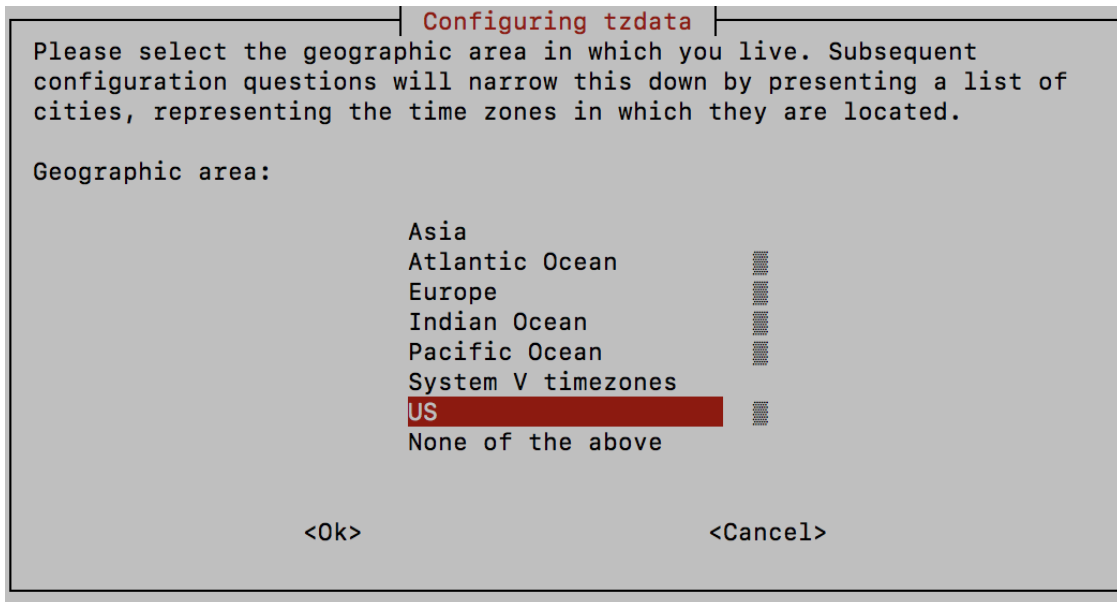
In general, the Crosswork Data Gateway VM launches with the default timezone as UTC. Cisco recommends that you configure the timezone to match your geographical area. With this configuration, all the Crosswork Data Gateway processes including the Showtech logs use the same configured timezone.

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

Step 2 Select **9 Timezone**.

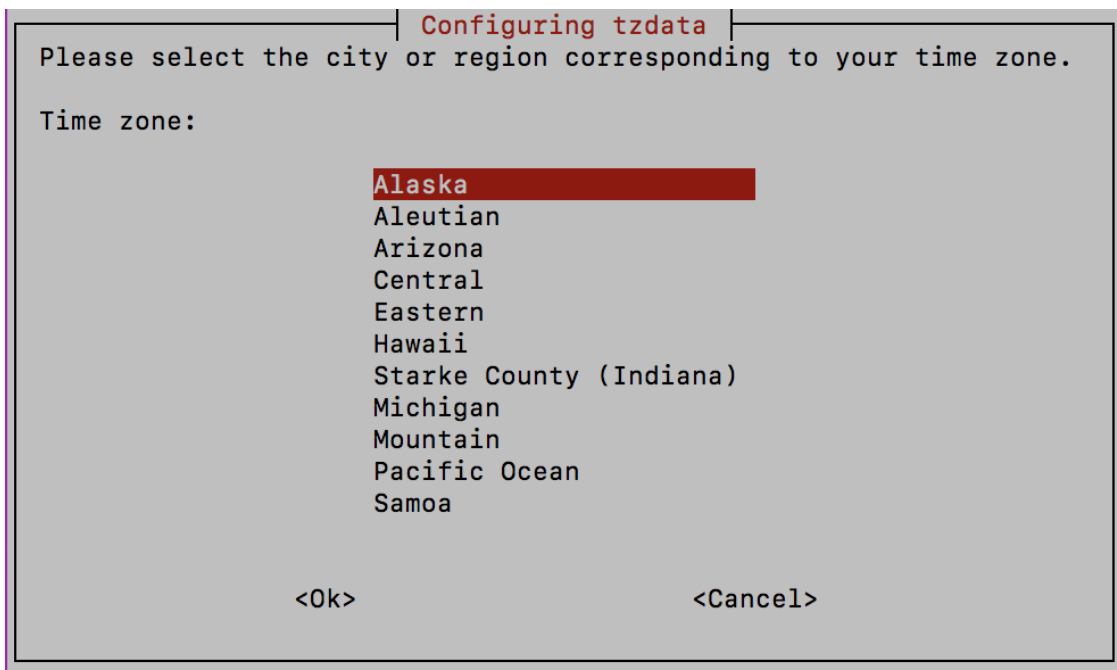
Step 3 Select the geographic area in which you live.

Figure 30: Timezone Settings - Geographic Area Selection



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

Figure 31: Timezone Settings - Region Selection



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.

Step 7 Log out of the Crosswork Data Gateway VM.

Log in and Log out of Crosswork Data Gateway VM

This section describes how to log in and out to the Crosswork Data Gateway VM.

Follow these steps to access and log out of the Crosswork Data Gateway VM:

- [Access Crosswork Data Gateway VM from SSH, on page 152](#)
- [Log out of Crosswork Data Gateway VM, on page 152](#)

Access Crosswork Data Gateway VM from SSH

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

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

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

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

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

For example,

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

To log in 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**.

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

Log out of Crosswork Data Gateway VM

To log out of the VM, from the **Main Menu**, select **1 Logout** and press **Enter** or click **OK**.

Troubleshoot Crosswork Data Gateway Installation and Enrollment

If Crosswork Data Gateway fails to auto-enroll with Cisco Crosswork, you can collect Crosswork Data Gateway show-tech (**Main menu > 5 Troubleshooting > 2 Run show-tech**) and check for the reason in

`controller-gateway` logs. For more information on how to collect show-tech logs, see the *Collect show-tech logs from the Interactive Console* section in *Cisco Crosswork Network Controller 5.0 Administration Guide*. If there are session establishment or certificate-related issues, ensure that the `controller.pem` certificate is uploaded using the Interactive Console.



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

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

Table 52: Troubleshooting the Installation/Enrollment

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

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

Issue	Action
During a Crosswork upgrade, some of the Crosswork Data Gateways may not get upgraded or reenrolled leading to logging multiple error messages in the dg-manager logs.	Reenroll or redeploy the Crosswork Data Gateways. For more information, see the <i>Redeploy a Crosswork Data Gateway Instance</i> and <i>Reenroll Crosswork Data Gateway</i> sections in Cisco Crosswork Network Controller 5.0 Administration Guide .
If a Crosswork Data Gateway instance that was previously attached to Crosswork is now reattached to a different Crosswork version 4.x or 5.0, the operational state of the instance may be Degraded with the robot-astack-influxdb error.	<ol style="list-style-type: none"> 1. Log in to the Crosswork UI from the SSH. 2. Run the Docker executive commands to access the robot-astack-influxdb pod. 3. In the pod, navigate to the following directory and delete it: <code>/mnt/dataafs/influxdb</code> 4. Restart the service using the following command: <code>supervisorctl restart all</code>
If Data Gateway is redeployed without moving the gateway to the Maintenance mode, Crosswork enrollment will be unsuccessful and errors will be logged in the dg-manager and controller-gateway logs.	Move the Data Gateway to the Maintenance mode or manually reenroll the gateway. For more information, see the <i>Reenroll Crosswork Data Gateway</i> section in Cisco Crosswork Network Controller 5.0 Administration Guide .

Import Controller Signing Certificate File

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

- You have not specified **Controller Signing Certificate File URI** under the **Controller Settings** during installation.
- Cisco Crosswork was upgraded or reinstalled and you need to authenticate and enroll Crosswork Data Gateway with Cisco Crosswork.

Follow these steps to import controller signing certificate file:

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

The **Change System Settings** menu opens.

Step 2 Select **7 Import Certificate**.

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

Step 4 Enter the SCP URI for the certificate file.

An example URI is given below:

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

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

The certificate file is imported.

Step 6 Verify that the certificate was installed successfully. See [View the Controller Signing Certificate File, on page 108](#).

View the Controller Signing Certificate File

Follow these steps to view the signing certificate:

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

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

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

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



PART **IV**

Install Crosswork Applications

- [Install Crosswork Applications, on page 159](#)



CHAPTER 9

Install Crosswork Applications

This chapter contains the following topics:

- [Install Crosswork Applications, on page 159](#)

Install Crosswork Applications

This section explains how to install Crosswork applications on the Cisco Crosswork UI.

The Crosswork Network Controller applications are bundled as **Essentials**, **Advantage**, and **Add-on** packages (see [Cisco Crosswork Network Controller Packages, on page 3](#) for more information). Every package contains crosswork applications in a particular format unique to Crosswork known as CAPP (Crosswork APPLICATION). As a first step, the packages containing the application CAPP files (*.tar.gz) must be downloaded from [cisco.com](#) to a machine reachable from the Cisco Crosswork server. The package is then added to the Crosswork UI where the applications within can be installed.

You must first download the relevant Crosswork Network Controller package (Essential or Advantage or Add-on) from [cisco.com](#) and then proceed to install the applications which are part of the package.

Before you begin

Ensure that all requirements of your application are met.

Step 1 Download and validate the CAPP files:

- Navigate to [cisco.com](#) and download the Crosswork Network Controller package that you require and the relevant signature file to a directory in your machine. For the purpose of these instructions, we will use the file names "**cw-na-cncessential-5.0.0-72-release-230502.tar.gz**" and "**cnc-5.0.0-capp-signatures.tar.gz**" respectively.
- Decompress the signature file:

```
tar -xvf <signature file>
```

Example:

```
[test@cw-build sample]% tar -xvf cnc-5.0.0-capp-signatures.tar.gz
README
CW-CCO_RELEASE.cer
cisco_x509_verify_release.py3
cisco_x509_verify_release.py
cw-na-cncessential-5.0.0-72-release-230502.tar.gz.signature
cw-na-cncadvantage-5.0.0-77-release-230425.tar.gz.signature
cw-na-cncaddon-5.0.0-68-release-230502.tar.gz.signature
```

- c) Use python script to validate the signature of each file you plan to use.

Note Use `python --version` to find out the version of Python on your machine.

If you are using Python 2.x, use the following command to validate the file:

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

If you are using Python 3.x, use the following command to validate the file:

```
python cisco_x509_verify_release.py3 -e <.cer file> -i <.tar.gz file> -s <.tar.gz.signature file>
-v dgst -sha512
```

Example:

```
[test@cw-build sample]% python cisco_x509_verify_release.py3 -s
cw-na-cncessential-5.0.0-72-release-230502.tar.gz.signature -i
cw-na-cncessential-5.0.0-72-release-230502.tar.gz -e CW-CCO_RELEASE.cer
Retrieving CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from CW-CCO_RELEASE.cer.
Successfully verified the signature of cw-na-cncessential-5.0.0-72-release-230502.tar.gz using
CW-CCO_RELEASE.cer
```

Note If you do not have python installed, go to python.org and download the version of python that is appropriate for your work station.

- d) If you are planning to download a standalone Crosswork application (for example, Crosswork Optimization Engine), hover over the relevant file and copy the MD5 or SHA512 checksum to your clip board.

Download the CAPP file to a server that can be reached from the Crosswork server. Run a tool of your choice to calculate the checksum, and the compare the checksum value in your downloaded file with the value you copied in the clip board.

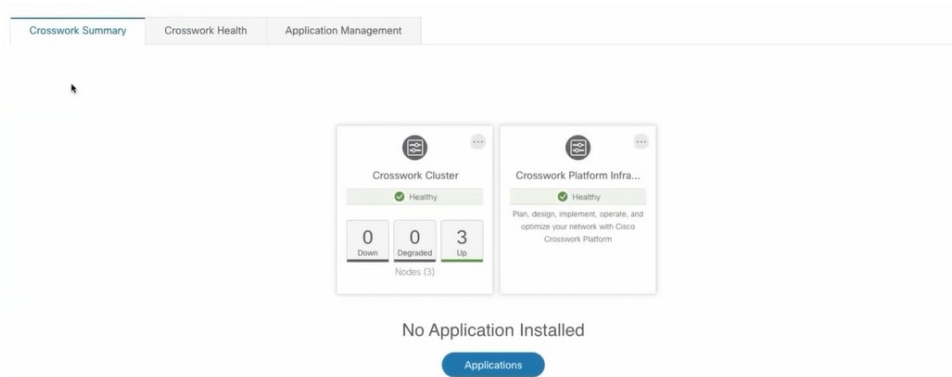
For example, on a MAC you can use the `md5` command to calculate the MD5 sum on a file:

```
md5 <.tar.gz>
```

Verify that the result value matches with the posted value on cisco.com.

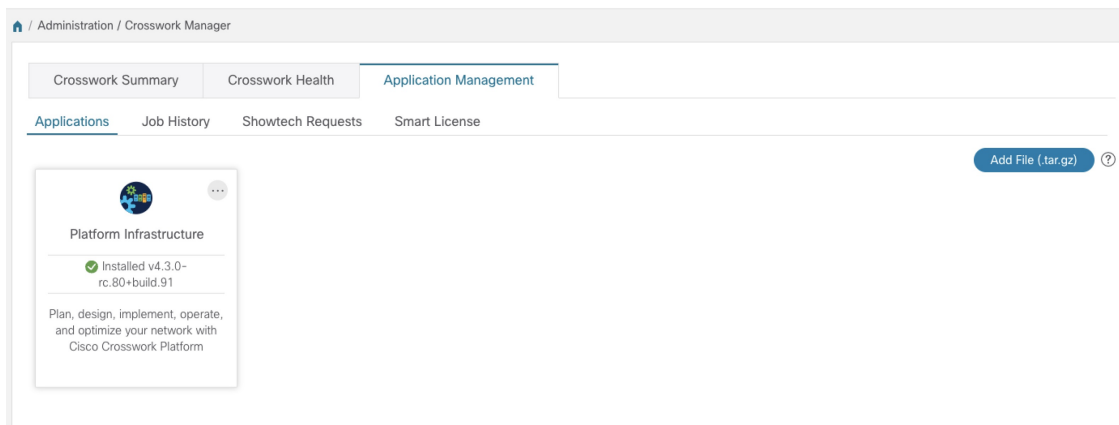
Step 2 Add the downloaded CAPP file to Crosswork:

- a) Log into Cisco Crosswork and in the homepage, click on **Administration** > **Crosswork Manager**. The **Crosswork Summary** page is displayed with Crosswork Cluster and Crosswork Platform Infrastructure tiles.



You can click on the tiles to get more information.

- b) Click on **Application Management** and select the **Applications** tab.



- c) Click on the **Add File (.tar.gz)** option to add the package that contains the CAPP files.

Note When installing a Crosswork Network Controller package, there is no need to untar the package. You can add the package tarball as-is to the Crosswork UI and the applications within are automatically added. You can then install the individual applications as needed.

- d) In the Add File dialog box, enter the relevant information and click **Add**.

Add File (.tar.gz) via Secure Copy ✕

Server Path/Location
Network/server_name/directory/file name

Host Name/IP Address

Port

Username

Password 👁

Automatically clean all repository files before adding new one

Add
Cancel

The add operation progress is displayed on the **Applications** screen. You can also view the installation progress in the **Job History** tab.

Administration / Crosswork Manager


✔ The product file /root/untar/cw-na-cncadvantage-4.0.0-51-release-220809.tar.gz was successfully added, check job id: AJ3. Go to Job History

Crosswork Summary Crosswork Health **Application Management**

Applications Job History Showtech Requests Smart License

Add File (.tar.gz) ?

Job AJ3: Downloading /root/untar/cw-na-cncadvantage-4.0.0-51-release-220809.tar.gz in process
 1%



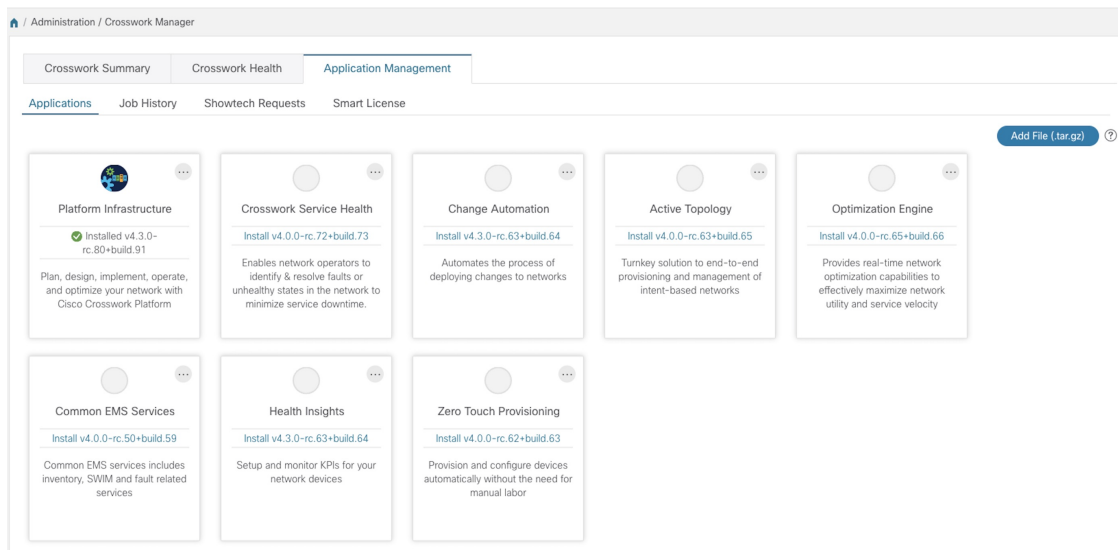
Platform Infrastructure

✔ Installed v4.3.0-rc.80+build.91


Plan, design, implement, operate, and optimize your network with Cisco Crosswork Platform

Note When loading a Crosswork Network Controller package, the loading process may stop at 50% for a while depending on the resources your host platform has available.

The newly added application files are displayed as tiles on the **Applications** screen.



Step 3 Install the Application CAPP file:

- a) Click on the **Install** prompt on the application tile. You can also click  on the tile, and select the **Install** option from the drop down list.

Important After you install Crosswork Cluster and Crosswork Data Gateway, the applications in the Crosswork Network Controller package (Essential or Advantage) need to be installed in the following sequence:

1. Crosswork Optimization Engine
2. Crosswork Active Topology
3. Crosswork Service Health (only available in Advantage package)
4. Element Management Functions (EMF)

Crosswork Change Automation, Crosswork Health Insights, and Crosswork Zero Touch Provisioning can be installed independently in any order and do not require any other application to be installed prior.


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.

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.

- b) After an application is installed, it must be activated to become functional. 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 application, click the  on the application tile, and select **Activate**.

Step 4 Repeat step 3 for installing any remaining applications.

Step 5 (Optional) Click  on the application tile, and select the **View Details** option to view details of the installed application.

Step 6 Once an application (or all applications) have been installed, check the health of the environment to make sure all the applications are healthy. It can take up to an hour for all the processes that make launch and for the applications to report

as healthy. If after an hour a newly installed application is not healthy after an hour, contact the Cisco Customer Experience team.

What to do next

Return to the installation workflow:

- VMware: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)
- AWS EC2: [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)



PART **V**

Integrate Cisco NSO and SR-PCE with Cisco Crosswork Network Controller

- [Integrate Cisco NSO, on page 167](#)
- [Integrate SR-PCE, on page 179](#)



CHAPTER 10

Integrate Cisco NSO

This chapter contains the following topics:

- [NSO Integration Workflow](#), on page 167
- [Install Cisco NSO Function Packs using Ansible playbook](#), on page 168
- [Add Cisco NSO Providers](#), on page 175
- [\(Optional\) Set up Cisco NSO Layered Service Architecture](#), on page 178

NSO Integration Workflow

This section explains the steps in integrating Cisco NSO with Crosswork Network Controller.

1. Install the compatible version of Cisco NSO

Ensure that you have installed the compatible version of Cisco NSO:

- If you are a VMware user, follow the instructions in [NSO documentation](#).
- If you are a AWS EC2 user, follow the instructions in [Install Cisco NSO on Amazon EC2](#), on page 145.

Additionally, for Cisco NSO LSA setup, see [\(Optional\) Set up Cisco NSO Layered Service Architecture](#), on page 178.

Table 53: Cisco NSO - compatible versions

Software/Driver	Version
Cisco Network Services Orchestrator (Cisco NSO)	6.1
Cisco Network Element Driver (NED) Note Cisco NEDs must be installed only for the device types and versions that you are managing. For example, if you are using NETCONF, then you must install the NED that corresponds to your IOS XR version(s). Similarly, Cisco IOS CLI NED must be installed if you have IOS devices in the network.	Cisco IOS XR: <ul style="list-style-type: none"> • CLI: 7.46.3 • NETCONF: 7.3.2, 7.315, 7.4.2, 7.5.2, 7.6.2, 7.7.2, 7.8, 7.9 Cisco IOS: <ul style="list-style-type: none"> • CLI: 6.86.6

2. Install the mandatory NSO core function packs

Depending on the Cisco Crosswork application or solution that you are using, there are mandatory Core Function Packs (CFPs) that must be installed on Cisco NSO to make the products compatible.

The NSO core function packs are bundled in cisco.com as follows:

Table 54: NSO Core Function Packs

Package Name	Contents
Cisco Crosswork Network Controller Essential Function Pack File name: <code>cw-cnc-essential-fp-5.0.0-101-release-230503.tar.gz</code>	<ul style="list-style-type: none"> • Cisco NSO Transport SDN Function Pack Bundle • Cisco NSO DLM Service Pack • Cisco NSO Telemetry Traffic Collector Function Pack
Cisco Crosswork Change Automation Function Pack File name: <code>cw-ca-fp-5.0.0-5-release-230511.tar.gz</code>	<ul style="list-style-type: none"> • Cisco Crosswork Change Automation NSO Function Pack

You can install the CFPs using either of the following methods:

- [Install Cisco NSO Function Packs using Ansible playbook, on page 168](#) (Recommended)
- [Install Cisco NSO Function Packs manually, on page 175](#)



Note The Cisco Crosswork Network Controller Function Pack SDK Application (`cw-na-platform-5.0.0-signed-tdn-sdk.tar.gz`) is also available for download on cisco.com. The SDK provides tools and source-code examples you can use to develop, build, package and deploy the TSDN function pack on Crosswork Network Controller.

3. Add the NSO provider and verify connectivity

Follow the instructions in [Add Cisco NSO Providers, on page 175](#).

Install Cisco NSO Function Packs using Ansible playbook

This section explains how to install the Cisco NSO Core Function Packs (CFPs) using Ansible playbooks.

The Ansible playbook installs the NSO CFPs on existing NSO VM instance(s), running compatible NSO version. The playbook is executed from an Ansible controller with the NSO instance(s) as managed node(s). This feature supports the following NSO deployment configurations:

- [LSA, on page 170](#)
- [LSA HA \(High Availability\), on page 171](#)
- [Standalone, on page 173](#)
- [Standalone HA \(High Availability\), on page 174](#)

See each deployment configuration for information on the required parameters and the scripts for installation and uninstallation.

To install or uninstall a CFP, perform the following:

Before you begin

Assumptions:

- Supports only the clean installation of CFPs.
- Upgrade is not supported.
- NSO is already installed along with HA configuration (per deployment requirement).
- The Ansible script installs all CFP packages (Transport SDN (TSDN), Change Automation (CA), Device Lifecycle Management (DLM), and Telemetry Traffic Controller (TM-TC) and bootstrapping.
- The LSA configuration requires 3 VMs (1 CFS node and 2 RFS nodes).
- NSO is installed in system-install mode (local install is not supported), in standard locations:
 - `ncsdir: /opt/ncs/current`
 - `confdir: /etc/ncs`
 - `rundir: /var/opt/ncs`
 - `logdir: /var/log/ncs`
- As upgrade is not supported, the installation will fail with the presence of the CFP package (for example, `cisco-tdsn-core-fp-common` package) which indicates that the CFP is already installed. This mechanism prevents accidentally installing packages on a working setup.
- If an installation attempt fails or you want to reinstall the CFP, run the uninstallation script first to remove (unlink) old packages.

Prerequisites:

- The latest ansible and ansible-playbook is installed on the host designated as the Ansible controller.
- The Java and Python versions (OpenJDK 11, python3) required for the CFP are already installed in the NSO VM.
- In case of HA deployment, the Cisco Tail-f HCC (Tail-f High Availability Cluster Communications) package must be already installed, configured, and operational prior to executing the CFP installation.

Caveats:

1. If `ssh`, `netconf-north-bound`, or `webui transport` have previously been enabled, running the install will not add the `dual-stack config` and it will need to be manually enabled. The following config is used to add IPv6 listener with the appropriate port:

```
<extra-listen>
  <ip>::</ip>
  <port>2024</port>
</extra-listen>
```

2. Before initiating the uninstallation, you must remove all services and devices added in the CDB; otherwise, NSO will attempt the upgrade process which causes uninstallation failure.

- Do not use an NSO instance as Ansible controller to install CFPs on itself. This deployment configuration is not supported.

Step 1 Edit the `host` and `vars.yml` files with the relevant parameters to configure NSO.

Step 2 To install the CFP, run the installation command (see each deployment configuration for details).

Example:

```
ansible-playbook -v -i hosts tsdn-lsa-ha-install.yml
```

The CFP files are copied to the install directory (`/opt/ncs/packages/`) and symbolic links are created in the runtime directory (`/var/opt/ncs/packages/`). NSO is then restarted to apply the package.

Step 3 To uninstall a CFP, run the uninstallation command (see each deployment configuration for details).

Example:

```
ansible-playbook -v -i hosts tsdn-lsa-ha-uninstall.yml
```

The symbolic links are removed in runtime directory and NSO is restarted without the CFP package.

What to do next

Return to the installation workflow:

- VMware: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)
- AWS EC2: [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)

LSA

This playbook installs the CFP packages and configures LSA cluster as per the node roles described in the `vars.yml` file.

Dir: lsa

Installation: `ansible-playbook -v -i hosts tsdn-lsa-install.yml`

Uninstallation: `ansible-playbook -v -i hosts tsdn-lsa-uninstall.yml`

Required Parameters:

File: `lsa/vars.yml`

Table 55: Required parameters for LSA deployment configuration

Parameter	Description
<code>ansible_user</code>	SSH username
<code>ansible_ssh_pass</code>	SSH password
<code>ansible_sudo_pass</code>	sudo password

Parameter	Description
nbi_port	NSO north bound interface port (Example: 8888)
restconf_port	Restconf interface port (Example: 2022)
lsa_ned_id	NSO Netconf NED ID (Example: cisco-nso-nc-6.1:cisco-nso-nc-6.1)
image_location	CFP package location on Ansible server, Crosswork (Example: /tmp/image)
tsdn_image	TSDN image name (Example: nso-6.1_230124-tsdn-5.0.0-M6)
ca_image	CA image name (Example: cw-na-fp-ca-5.0.0-nso-6.1)
dlm_image	DLM image name (Example: cw-na-dlm-fp-5.0.0-nso-6.1-eng)
tmtc_image	TM-TC image name (Example: cw-na-fp-tmtc-5.0.0-333-nso-6.1)
tmtc_internal	TM-TC internal directory name (Example: TM-TC-5.0.0-333. You may need to untar to get this)
cli_ned_version	IOS XR NED version required by TM-TC (Example: 7.45)
rfs_nodes	- name: rfs-1: ip: <RFS 1 IP address> - name: rfs-2: ip: <RFS 2 IP address> - name: rfs-x: ip: <RFS x IP address>

File: lsa/hosts

```
[all]

[cfs_node]
10.0.0.2

[rfs_node]
10.0.0.3
10.0.0.4
10.0.0.x
```

After you prepare the `host` and `vars.yml` files, follow the instructions in [Install Cisco NSO Function Packs using Ansible playbook, on page 168](#) to complete the CFP installation.

LSA HA (High Availability)

This playbook installs the CFP packages and configures LSA cluster as per the node roles described in the `vars.yml` file.

After you prepare the `host` and `vars.yml` files, follow the instructions in [Install Cisco NSO Function Packs using Ansible playbook, on page 168](#).

Dir: lsa-ha

Installation: `ansible-playbook -v -i hosts lsa-ha-install.yml`

Uninstallation: `ansible-playbook -v -i hosts lsa-ha-uninstall.yml`

Required Parameters:

File: `lsa-ha/vars.yml`

Table 56: Required parameters for LSA HA deployment configuration

Parameter	Description
<code>ansible_user</code>	SSH username
<code>ansible_ssh_pass</code>	SSH password
<code>ansible_sudo_pass</code>	sudo password
<code>nbi_port</code>	NSO north bound interface port (Example: 8888)
<code>restconf_port</code>	Restconf interface port (Example: 2022)
<code>lsa_ned_id</code>	NSO Netconf NED ID (Example: cisco-nso-nc-6.1:cisco-nso-nc-6.1)
<code>image_location</code>	CFP package location on Ansible server, Crosswork (Example: /tmp/image)
<code>tsdn_image</code>	TSDN image name (Example: nso-6.1_230124-tdsn-5.0.0-M6)
<code>ca_image</code>	CA image name (Example: cw-na-fp-ca-5.0.0-nso-6.1)
<code>dlm_image</code>	DLM image name (Example: cw-na-dlm-fp-5.0.0-nso-6.1-eng)
<code>tmtc_image</code>	TM-TC image name (Example: cw-na-fp-tmtc-5.0.0-333-nso-6.1)
<code>tmtc_internal</code>	TM-TC internal directory name (Example: TM-TC-5.0.0-333. You may need to untar to get this)
<code>cli_ned_version</code>	IOS XR NED version required by TM-TC (Example: 7.45)
<code>rfs_nodes</code>	<ul style="list-style-type: none"> - name: rfs-1: ip: <RFS 1 IP address> - name: rfs-2: ip: <RFS 2 IP address> - name: rfs-x: ip: <RFS x IP address>

File: `lsa-ha/hosts`

```
[all]

[cfs_primary]
10.0.0.2

[cfs_secondary]
10.0.0.3

[rfs1_primary]
10.0.0.4

[rfs1_secondary]
```

```

10.0.0.5

[rfs2_primary]
10.0.0.7

[rfs2_secondary]
10.0.0.8

[rfsx_primary]
10.0.0.x1

[rfsx_secondary]
10.0.0.x2

```

After you prepare the `host` and `vars.yml` files, follow the instructions in [Install Cisco NSO Function Packs using Ansible playbook, on page 168](#) to complete the CFP installation.

Standalone

This playbook installs the CFP packages to a standalone NSO node.

Dir: standalone

Installation: `ansible-playbook -v -i hosts standalone-install.yml`

Uninstallation: `ansible-playbook -v -i hosts standalone-uninstall.yml`

Required Parameters:

File: `standalone/vars.yml`

Table 57: Required parameters for standalone deployment configuration

Parameter	Description
<code>ansible_user</code>	SSH username
<code>ansible_ssh_pass</code>	SSH password
<code>ansible_sudo_pass</code>	sudo password
<code>nbi_port</code>	NSO north bound interface port (Example: 8888)
<code>image_location</code>	CFP package location on Ansible server, Crosswork (Example: /tmp/image)
<code>tsdn_image</code>	TSDN image name (Example: nso-6.1_230124-tdsn-5.0.0-M6)
<code>ca_image</code>	CA image name (Example: cw-na-fp-ca-5.0.0-nso-6.1)
<code>d1m_image</code>	DLM image name (Example: cw-na-d1m-fp-5.0.0-nso-6.1-eng)
<code>tmtc_image</code>	TM-TC image name (Example: cw-na-fp-tmtc-5.0.0-333-nso-6.1)
<code>tmtc_internal</code>	TM-TC internal directory name (Example: TM-TC-5.0.0-333. You may need to untar to get this)

Parameter	Description
<code>cli_ned_version</code>	IOS XR NED version required by TM-TC (Example: 7.45)

File: `standalone/hosts`

```
[all]
10.0.0.2
```

After you prepare the `hosts` and `vars.yml` files, follow the instructions in [Install Cisco NSO Function Packs using Ansible playbook, on page 168](#) to complete the CFP installation.

Standalone HA (High Availability)

This playbook installs CFP packages to a NSO node in HA configuration as described in the `vars.yml` file.

In case of HA deployment, the Cisco Tail-f HCC (Tail-f High Availability Cluster Communications) package must be already installed, configured, and operational prior to executing the CFP installation.

Dir: `ha`

Installation: `ansible-playbook -v -i hosts ha-install.yml`

Uninstallation: `ansible-playbook -v -i hosts ha-uninstall.yml`

Required Parameters:

File: `ha/vars.yml`

Table 58: Required parameters for standalone HA deployment configuration

Parameter	Description
<code>ansible_user</code>	SSH username
<code>ansible_ssh_pass</code>	SSH password
<code>ansible_sudo_pass</code>	sudo password
<code>nbi_port</code>	NSO north bound interface port (Example: 8888)
<code>image_location</code>	CFP package location on Ansible server, Crosswork (Example: /tmp/image)
<code>tsdn_image</code>	TSDN image name (Example: nso-6.1_230124-tsdn-5.0.0-M6)
<code>ca_image</code>	CA image name (Example: cw-na-fp-ca-5.0.0-nso-6.1)
<code>dlm_image</code>	DLM image name (Example: cw-na-dlm-fp-5.0.0-nso-6.1-eng)
<code>tmtc_image</code>	TM-TC image name (Example: cw-na-fp-tmtc-5.0.0-333-nso-6.1)
<code>tmtc_internal</code>	TM-TC internal directory name (Example: TM-TC-5.0.0-333. You may need to untar to get this)
<code>cli_ned_version</code>	IOS XR NED version required by TM-TC (Example: 7.45)

Parameter	Description
<code>vip_ip</code>	Virtual IP address
<code>primary_node_ip</code>	Primary node IP address
<code>secondary_node_ip</code>	Secondary node IP address

File: `ha/hosts`

```
[all]

[primary_node]
  10.0.0.2

[secondary_node]
  10.0.0.3
```

After you prepare the `hosts` and `vars.yml` files, follow the instructions in [Install Cisco NSO Function Packs using Ansible playbook, on page 168](#) to complete the CFP installation.

Install Cisco NSO Function Packs manually

If you need to install individual function packs manually, follow the relevant procedure from the below table:

Table 59: List of mandatory Function Packs

Crosswork Product	Required Function Pack documentation
Crosswork Network Controller Essentials OR Crosswork Network Controller Advantage	<ul style="list-style-type: none"> • Cisco NSO Transport SDN Function Pack Bundle 5.0.0 User Guide • Cisco NSO Transport SDN Function Pack Bundle 5.0.0 Installation Guide • Cisco Network Services Orchestrator DLM Service Pack 5.0.0 Installation Guide • Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 5.0.0 Installation Guide • Cisco Crosswork Change Automation NSO Function Pack 5.0.0 Installation Guide
Crosswork Optimization Engine (Standalone)	<ul style="list-style-type: none"> • Cisco Network Services Orchestrator DLM Service Pack 5.0.0 Installation Guide • Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 5.0.0 Installation Guide

Add Cisco NSO Providers

The Cisco Network Services Orchestrator (Cisco NSO) provider supplies the following functionality:

- Network services and device configuration services to Cisco Crosswork applications.
- Device management and configuration maintenance services.



Note Crosswork supports Cisco NSO Layered Service Architecture (LSA) deployment. The LSA deployment is constructed from multiple NSO providers, that function as the customer-facing service (CFS) NSO containing all the services, and the resource-facing service (RFS), which contains the devices. Crosswork automatically identifies the NSO provider as CFS or RFS. Only one CFS is allowed. On the **Manager Provider Access** page, the **Type** column identifies the NSO provider as CFS.



Note The Cisco NSO sample function packs are provided as a starting point for VPN service provisioning functionality in Cisco Crosswork Network Controller. While the samples can be used “as is” in some limited network configurations, they are intended to demonstrate the extensible design of Cisco Crosswork Network Controller. Answers to common questions can be found on Cisco Devnet and Cisco Customer Experience representatives can provide answers to general questions about the samples. Support for customization of the samples for your specific use cases can be arranged through your Cisco account team.

Before you begin

You will need to:

- Create a credential profile for the Cisco NSO provider.
- Know the name you want to assign to the Cisco NSO provider.
- Know the Cisco NSO NED device models and driver versions used in your topology.



Note You can find the Cisco NSO version using the `version` command, as shown in the below example:

```
admin@ncs# show ncs-state version
ncs-state version 6.1
```

- Know the Cisco NSO server IP address and hostname. When NSO is configured with HA, the IP address would be management VIP address.
- Confirm Cisco NSO device configurations.

Follow the steps below to add a Cisco NSO provider through the UI. Note that you can import several providers at the same time by preparing a CSV file with the details of all the providers and importing it into Crosswork.

Step 1 From the main menu, choose **Administration > Manage Provider Access**.

Step 2 Click .

Step 3 Enter the following values for the Cisco NSO provider fields:

a) Required fields:

- **Provider Name:** Enter a name for the provider.
- **Credential Profile:** Select the previously created Cisco NSO credential profile.
- **Family:** Select **NSO**.
- Under Connection Type(s), **Protocol:** Select the protocol that Cisco Crosswork applications will use to connect to the provider. **HTTPS** is usually preferred.
- **IP Address/Subnet Mask:** Enter the IP address and subnet mask of the Cisco NSO server.
Important When you modify or update the NSO provider IP address or FQDN, you need to detach devices from corresponding virtual data gateway, and reattach them. If you fail to do this, the provider changes will not be reflected in MDT collection jobs.
- **Port:** For HTTPS, enter the port that corresponds with what is configured on the NSO VM in etc/ncs/ncs.conf to access NSO using HTTPS. NSO uses 8888 as default port.
- **Model:** Select the model (**Cisco-IOS-XR**, **Cisco-NX-OS**, or **Cisco-IOS-XE**) from the drop-down list and enter its associated NED driver version. Add a model for each type of device that will be used in the topology. If you have more than one, add another supported model.
- **Version:** Enter the NED software version installed for the device model in NSO.


b) Optional values:

- **Timeout:** The amount of time (in seconds) to wait before timing out the connection to the Cisco NSO server. The default is 30 seconds.

Step 4 Under Provider Properties, enter a **Property Key** of **forward** and a **Property Value** of **true**. This property is necessary when using the Cisco Crosswork Network Controller solution to allow provisioning operations within the UI and to enable the northbound interface to NSO via the Crosswork API gateway.

Note Cisco Crosswork provides the option to cross launch the NSO application from the Crosswork UI (this feature is not available for user roles with read-only permissions). To enable the cross launch feature, add Cisco NSO as a provider with one of the following settings:

- The **Property Key** **nso_crosslaunch_url** has a valid URL entered in the **Property Key** field.
- Protocol is **HTTP** or **HTTPS**, and the provider is reachable.

If any of the above settings are present, the cross launch icon () is displayed in the **Provider Name** column. Alternately, you can cross launch the NSO application using the launch icon located at the top right corner of the window.

Step 5 When you have completed entries in all of the required fields, click **Save** to add Cisco NSO as a provider.

Step 6 In the Providers window, select the NSO provider you created and click **Actions > Edit Policy Details**.

The **Edit Policy Details** window for the selected NSO provider is displayed.

Step 7 Edit the configuration fields to match the requirements of your environment. Click **Save** to save your changes.

What to do next

Return to the installation workflow:

- VMware: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)
- AWS EC2: [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)

(Optional) Set up Cisco NSO Layered Service Architecture

This section is applicable only when you have opted for Cisco NSO Layered Service Architecture (LSA) deployment.

Cisco NSO LSA allows you to add arbitrarily many device nodes for improved memory and provisioning throughput. Large service providers or enterprises use Cisco NSO to manage services for millions of subscribers or users, ranging over several hundred thousand managed devices. To achieve this, you can design your services in the layered fashion called LSA.

To position Cisco Crosswork Network Controller for large customers, the solution is made compatible with the existing Cisco NSO LSA architecture.

Follow these steps to decide when to use Cisco NSO LSA:

1. Check if the deployment is stand-alone or Cisco NSO LSA.
2. If the deployment is stand-alone, check the maximum memory that may be utilised. If the maximum memory that may be utilised is more than the current memory state, Cisco NSO LSA needs to be deployed.



Note Migration from stand-alone deployment to Cisco NSO LSA deployment is not currently supported.

To get a detailed information on Cisco NSO LSA and to set up Cisco NSO LSA, see [NSO Layered Service Architecture](#).



CHAPTER 11

Integrate SR-PCE

This chapter contains the following topics:

- [SR-PCE Integration Workflow, on page 179](#)
- [Configure SR-PCE, on page 179](#)
- [Add Cisco SR-PCE Providers, on page 182](#)

SR-PCE Integration Workflow

This section explains the steps in integrating Cisco SR-PCE with Crosswork Network Controller.

The compatible versions of SR-PCE are Cisco IOS XR 7.9.1 and 7.9.2.

1. Install the compatible version of Cisco SR-PCE

Select the type of SR-PCE (for VMware ESXi or AWS) and follow the relevant install instructions in the [Cisco IOS XRv 9000 Router Installation Guide](#).

2. Configure SR-PCE

Follow the instructions in [Configure SR-PCE, on page 179](#).

3. Add SR-PCE provider and verify connectivity

Follow the instructions in [Add Cisco SR-PCE Providers, on page 182](#).

Configure SR-PCE

This section explains how to configure SR-PCE after you have installed it.



Note The Cisco IOS XRv 9000 is the recommended platform to act as the SR-PCE.

Table 60: Configure SR-PCE

Step	Command or Action	Description
1	<code>configure</code> Example: RP/0/RP0/CPU0:router# <code>configure</code>	Enters mode.
2	<code>pce</code> Example: RP/0/RP0/CPU0:router(config)# <code>pce</code>	Enables PCE and enters PCE configuration mode.
3	<code>address ipv4 address</code> Example: RP/0/RP0/CPU0:router(config-pce)# <code>address ipv4 192.168.0.1</code>	Configures a PCE IPv4 address.
4	<code>state-sync ipv4 address</code> Example: RP/0/RP0/CPU0:router(config-pce)# <code>state-sync ipv4 192.168.0.3</code>	Configures the remote peer for state synchronization.
5	<code>tcp-buffer size size</code> Example: RP/0/RP0/CPU0:router(config-pce)# <code>tcp-buffer size 1024000</code>	Configures the transmit and receive TCP buffer size for each PCEP session, in bytes. The default buffer size is 256000. The valid range is from 204800 to 1024000.
6	<code>password {clear encrypted} password</code> Example: RP/0/RP0/CPU0:router(config-pce)# <code>password encrypted pwd1</code>	Enables TCP MD5 authentication for all PCEP peers. Any TCP segment coming from the PCC that does not contain a MAC matching the configured password will be rejected. Specify if the password is encrypted or clear text. Note TCP-AO and TCP MD5 are never permitted to be used simultaneously.

Step	Command or Action	Description
7	<pre>tcp-ao key-chain [include-tcp-options] [accept-ao-mismatch-connection] Example: RP/0/RP0/CPU0:router(config-pce)# tcp-ao pce_tcp_ao include-tcp-options</pre>	<p>Enables TCP Authentication Option (TCP-AO) authentication for all PCEP peers. Any TCP segment coming from the PCC that does not contain a MAC matching the configured key chain will be rejected.</p> <ul style="list-style-type: none"> include-tcp-options—Includes other TCP options in the header for MAC calculation. accept-ao-mismatch-connection—Accepts connection even if there is a mismatch of AO options between peers. <p>Note TCP-AO and TCP MD5 are never permitted to be used simultaneously.</p>
8	<pre>segment-routing {strict-sid-only te-latency} Example: RP/0/RP0/CPU0:router(config-pce)# segment-routing strict-sid-only</pre>	<p>Configures the segment routing algorithm to use strict SID or TE latency.</p> <p>Note This setting is global and applies to all LSPs that request a path from this controller.</p>
9	<pre>timers Example: RP/0/RP0/CPU0:router(config-pce)# timers</pre>	<p>Enters timer configuration mode.</p>
10	<pre>keepalive time Example: RP/0/RP0/CPU0:router(config-pce-timers)# keepalive 60</pre>	<p>Configures the timer value for locally generated keep-alive messages. The default time is 30 seconds.</p>
11	<pre>minimum-peer-keepalive time Example: RP/0/RP0/CPU0:router(config-pce-timers)# minimum-peer-keepalive 30</pre>	<p>Configures the minimum acceptable keep-alive timer that the remote peer may propose in the PCEP OPEN message during session establishment. The default time is 20 seconds.</p>
12	<pre>reoptimization time Example: RP/0/RP0/CPU0:router(config-pce-timers)# reoptimization 600</pre>	<p>Configures the re-optimization timer. The default timer is 1800 seconds.</p>
13	<pre>exit Example: RP/0/RP0/CPU0:router(config-pce-timers)# exit</pre>	<p>Exits timer configuration mode and returns to PCE configuration mode.</p>

What to do next:

Return to the installation workflow:

- VMware: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)
- AWS EC2: [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)

Sample SR-PCE config

This is a sample SR-PCE configuration:

```
pce
address ipv4 1.1.1.98
api
  user cisco {This is the username and password that the
  credential profile used for the PCE will need to have for HTTP}
  password encrypted 032752180500701E1D48
!
```

Add Cisco SR-PCE Providers

Cisco Segment Routing Path Computation Elements (Cisco SR-PCE) providers supply device discovery, management, configuration-maintenance and route-calculation services to the Cisco Crosswork applications. At least one SR-PCE provider is required in order to learn and discover SR policies, Layer 3 links, and devices. You have the option to configure a second SR-PCE as a backup. Both SR-PCE devices must be connected to the same network as Crosswork Network Controller does not support managing more than one domain.



Note To enable Cisco Crosswork application access to an SR-PCE as an SDN controller on the management domain, SR-PCE needs to be added as a provider.

Follow the steps below to add (through the UI) one or more instances of Cisco SR-PCE as providers.

Before you begin

You will need to:

- Configure a device to act as the SR-PCE. See SR configuration documentation for your specific device platform to enable SR (for IS-IS or OSPF protocols) and configure an SR-PCE (for example: [Segment Routing Configuration Guide for Cisco NCS 540 Series Routers](#)).
- Create a credential profile for the Cisco SR-PCE provider. This should be a basic HTTP text-authentication credential (currently, MD5 authentication is not supported). If the Cisco SR-PCE server you are adding does not require authentication, you must still supply a credential profile for the provider, but it can be any profile that does not use the HTTP protocol.
- Know the name you want to assign to the Cisco SR-PCE provider. This is usually the DNS hostname of the Cisco SR-PCE server.
- Know the Cisco SR-PCE server IP address.

- Know the interface you want to use to communicate between Cisco SR-PCE and the Cisco Crosswork application server.
- Determine whether you want to auto-onboard the devices that Cisco SR-PCE discovers and, if so, whether you want the new devices to have their management status set to **off**, **managed** or **unmanaged** when added.
- If you plan to auto-onboard devices that the Cisco SR-PCE provider discovers, and set them to a managed state when they are added to the database:
 - Assign an existing credential profile for communication with the new managed devices.
 - The credential profile must be configured with an SNMP protocol.
- For high availability, ensure that you set up two separate Cisco SR-PCE providers with unique names and IP addresses, but with matching configurations.

Step 1 From the main menu, choose **Administration > Manage Provider Access**.

Step 2 Click .

Step 3 Enter the following values for the SR-PCE provider fields:

a) Required fields:

- **Provider Name:** Name of the SR-PCE provider.
- **Credential Profile:** Select the previously created Cisco SR-PCE credential profile.
- **Family:** Select **SR_PCE**. All other options should be ignored.
- **Protocol:** Select **HTTP**.
- **IP Address/ Subnet Mask:** Enter the IP address (IPv4 or IPv6) and subnet mask of the server.
- **Port:** Enter **8080** for the port number.
- **Provider Properties:** Enter one of the following key/value pairs in the first set of fields:

Property Key	Value
auto-onboard	off Note Use this option if you plan to manually (via UI or CSV import) enter all of your network devices. When devices are discovered, the device data is recorded in the Cisco SR-PCE database, but is not registered in Cisco Crosswork Inventory Management database.

Property Key	Value
auto-onboard	<p>unmanaged</p> <p>If this option is enabled, all devices that Cisco Crosswork discovers will be registered in the Cisco Crosswork Inventory Management database, with their configured state set to unmanaged. SNMP polling will be disabled for these devices, and no management IP information will be included. To get these devices into the managed state later, you will need to either edit them via the UI or export them to a CSV make modifications and then import the updated CSV. You can also assign credential profiles by adding them to the device CSV file before import (the credential profiles must already exist).</p>
auto-onboard	<p>managed</p> <p>If this option is enabled, all devices that Cisco SR-PCE discovers will be registered in the Cisco Crosswork Inventory Management database, with their configured state set to managed. SNMP polling will be enabled for these devices, and Cisco SR-PCE will also report the management IP address (TE Router ID for IPv4, or IPv6 Router ID for IPv6 deployment). The devices will be added with the credential profile associated with the device-profile key in the SR-PCE provider configuration.</p>
device-profile	<p>The name of a credential profile that contains SNMP credentials for all the new devices.</p> <p>Note This field is necessary only if auto-onboard is set to managed or unmanaged.</p>
outgoing-interface	<p>eth1</p> <p>Note You have to set this only if you want to enable Cisco Crosswork application access to SR-PCE via the data network interface when using the two NIC configuration.</p>
topology	<p>off or on.</p> <p>This is an optional property. If not specified, the default value is on.</p> <p>If value is specified as off, it means that L3 topology is not accessible for the SR-PCE provider.</p>
pce	<p>off or on.</p> <p>This is an optional property. If not specified, the default value is on.</p> <p>If value is specified as off, it means that LSPs and policies are not accessible for the SR-PCE provider.</p>

Figure 32: Provider Property Key and Value Example

Property Key [?]	Property Value [?]
auto-onboard	off
outgoing-inter	eth1

Note If **managed** or **unmanaged** options are set and you want to delete a device later, you must do one of the following:

- Reconfigure and remove the devices from the network before deleting the device from Cisco Crosswork. This avoids Cisco Crosswork from rediscovering and adding the device back.
- Set auto-onboard to **off**, and then delete the device from Cisco Crosswork. However, doing so will not allow Cisco Crosswork to detect or auto-onboard any new devices in the network.

b) Optional values:

- **Timeout:** The amount of time (in seconds) to wait before timing out the connection to the SR-PCE server. The default is 30 seconds.

Step 4 When you have completed entries in all of the required fields, click **Save** to add the SR-PCE provider.

Step 5 Confirm that the SR-PCE provider shows a green Reachability status without any errors. You can also view the Events window (**Administration** > **Events**) to see if the provider has been configured correctly.

Step 6 Repeat this process for each SR-PCE provider.



Note It is not recommended to modify auto-onboard options once set. If you need to modify them, do the following:

1. Delete the provider and wait until deletion confirmation is displayed in the Events window.
2. Re-add the provider with the updated auto-onboard option.
3. Confirm the provider has been added with the correct auto-onboard option in the Events window.

What to do next

- If you entered the **auto-onboard/off** pair, navigate to **Device Management** > **Network Devices** to add a devices.
- If you opted to automatically onboard devices, navigate to **Device Management** > **Network Devices** to view the device list. To add more node information such as geographical location details, export the device list (.csv), update it, and import it back. If geographical location data is missing, you will only be able to see device topology using the logical map.

Return to the installation workflow:

- VMware: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)

- AWS EC2: [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)



PART VI

Upgrade Cisco Crosswork Network Controller

- [Upgrade Cisco Crosswork, on page 189](#)



CHAPTER 12

Upgrade Cisco Crosswork

This chapter contains the following topics:

- [Upgrade Overview, on page 189](#)
- [Upgrade Requirements, on page 190](#)
- [Upgrade Using Existing Hardware, on page 191](#)
- [Upgrade Using Parallel Hardware, on page 201](#)
- [Update a Crosswork Application \(standalone activity\) , on page 208](#)

Upgrade Overview

This section provides the high-level overview for upgrading Cisco Crosswork Network Controller to the latest version. This includes upgrading Cisco Crosswork cluster, Cisco Crosswork Data Gateway and Crosswork Applications within a single maintenance window.

You can upgrade Cisco Crosswork in the following methods:

1. [Upgrade Using Existing Hardware, on page 191](#)
2. [Upgrade Using Parallel Hardware, on page 201](#)

The time taken for the entire upgrade window can vary based on size of your deployment profile and the performance characteristics of your hardware.



Warning Migration of Cisco Crosswork from an earlier version has the following limitations:

- License tags are not auto-registered as part of the upgrade operation. You must register them manually after the upgrade.
- Third-party device configuration in Device Lifecycle Management (DLM) and Cisco NSO is not migrated, and needs to be re-applied on the new Cisco Crosswork version post migration.
- Custom user roles (Read-Write/Read) created in earlier version of Cisco Crosswork are not migrated, and need to be updated manually on the new version post migration.
- Any user roles with administrative privileges in the earlier version of Cisco Crosswork must be assigned new permissions after the upgrade to continue being administrative users.
- Crosswork Health Insights KPI alert history is not retrieved as part of the migration.
- After a successful migration, you must perform a hard refresh or browser cache deletion before proceeding to use the system. Failing to do this step can result in data discrepancy.

Crosswork applications can be independently updated from the Cisco Crosswork UI in case of minor updates or patch releases. For more information, see [Update a Crosswork Application \(standalone activity\)](#), on page 208.

Upgrade Requirements

This section explains the requirements for upgrading the Cisco Crosswork if you are using the Crosswork Optimization Engine.

If you have enabled feature packs (LCM, Bandwidth Optimization, or BWoD) in an earlier version of Crosswork Optimization Engine and want to upgrade to the latest version, you must perform the following tasks prior to upgrading:

LCM

- From the LCM **Configuration** page:
 1. Set the **Delete Tactical SR Policies when Disabled** option to **False**. This task must be done prior to disabling LCM so that tactical policies deployed by LCM remain in the network after the upgrade.
 2. Set the **Enable** option to **False**. If LCM remains enabled, there is a chance that tactical policies may be deleted after the upgrade.
 3. Note all options (Basic and Advanced) in the LCM **Configuration** page so that you can confirm the same configuration has been migrated after the upgrade.
- Export the current list of interfaces managed by LCM (**Traffic Engineering > Local Congestion Mitigation > Export** icon). Confirm the interfaces are valid by reimporting the CSV file without errors. For more information, see "Add Individual Interface Thresholds" in the [Cisco Crosswork Optimization Engine 5.0 User Guide](#).
- After the upgrade, wait until the **Traffic Engineering** page shows all the nodes and links before enabling LCM

Note:

After the system is stable and before enabling domains for LCM, confirm that the migration of previously monitored interfaces has completed and that each domain has the expected configuration options.

1. Navigate to **Administration > Alarms > All > Events** and enter **LCM** to filter the **Source** column.
2. Look for the following event: "Migration complete. All migrated LCM interfaces and policies are mapped to their IGP domains". If this message does not appear wait for the **Congestion Check Interval** period (set in the **LCM Configuration** page), then restart LCM (**Administration > Crosswork Manager > Optimization Engine > optima-lcm > ... > Restart**).
3. Wait until the **optima-lcm** service changes from Degraded to Healthy state.
4. For each domain, navigate to the **Configuration** page and verify the options have been migrated successfully. If the domain configurations are incorrect, restart LCM (**Administration > Crosswork Manager > Optimization Engine > optima-lcm > ... > Restart**).
5. Check the **Events** page for the event mentioned above and the **Configuration** page to verify the options.

**Note**

- If the confirmation message does not appear or domain configuration options are incorrect, then contact Cisco Technical support and provide them with showtech information and the exported Link Management CSV file.
- You can also manually add missing interfaces that were previously monitored or update domain configuration options *after* the system is stable.

BWoD

- Set the **Enable** option to **False**. If BWoD remains enabled, there is a chance that tactical policies may be deleted after the upgrade.
- Note all options (Basic and Advanced) in the **BWoD Configuration** page so that you can confirm the same configuration has been migrated after the upgrade.
- After the upgrade, wait until the **Traffic Engineering** page shows all the nodes and links before enabling BWoD.

Upgrade Using Existing Hardware

This section explains how to migrate to the latest version of Crosswork Network Controller using the existing cluster.

Each stage in this upgrade workflow must be executed in sequence, and is explained in detail in later sections of this chapter. The stages are:

1. [Shut Down Cisco Crosswork Data Gateway VMs, on page 192](#)
2. [Create Backup and Shut Down Cisco Crosswork, on page 193](#)
3. [Install the latest version of the Cisco Crosswork Cluster, on page 195](#)



Note While the cluster installation is in progress, you must upgrade NSO to version 6.1.0. The process to upgrade NSO is not covered in this document. For more information, see the relevant [Cisco NSO documentation](#). You must also upgrade your SR-PCE to version 7.9.1. For install instructions, see the [Cisco IOS XRv 9000 Router Installation Guide](#).

4. [Install the Cisco Crosswork Applications, on page 196](#)



Note You are recommended to download and validate the application CAPP files (See [Install Crosswork Applications](#)) before starting the actual upgrade process. This will reduce your system downtime as opposed to downloading the CAPP files midway through the upgrade process.

5. [Migrate Cisco Crosswork Backup, on page 196](#)
6. [Upgrade Crosswork Data Gateway, on page 197](#)
7. [Post-upgrade Checklist, on page 200](#)

Shut Down Cisco Crosswork Data Gateway VMs

This is the first stage of the upgrade workflow.



Note When Crosswork Data Gateway VMs are shut down, data will not be forwarded to data destinations. Check with the application providers to determine if any steps are needed to avoid alarms or other problems.

Before you begin

Take screenshots of all the tabs in the **Data Gateway Management** page to keep a record of the list of Crosswork Data Gateways, **Attached Device Count** in the Cisco Crosswork UI. In the **Pools** tab, for each pool listed here, take a screenshot to make a note of the active, spare, and unassigned VMs in the pool. This information is useful during [Upgrade Crosswork Data Gateway, on page 197](#).

Step 1 Check and confirm that all the VMs are healthy and running in your cluster.

Step 2 Shut down the Crosswork Data Gateway VMs.

- a) Log in to the Crosswork Data Gateway VM. See [Access Crosswork Data Gateway VM from SSH, on page 100](#).
Crosswork Data Gateway launches an Interactive Console after you log in successfully.
 - b) Choose **5 Troubleshooting**.
 - c) From the **Troubleshooting** menu, choose **5 Shutdown VM** to shut down the VM.
-

Create Backup and Shut Down Cisco Crosswork

This is the second stage of the upgrade workflow. Creating a backup is a prerequisite when upgrading your current version of Cisco Crosswork to a new version.



Note We recommend that you create a backup only during a scheduled upgrade window. Users should not attempt to access Cisco Crosswork while the backup operation is running.

Before you begin

Follow these guidelines whenever you create a backup:

- Cisco Crosswork will back up the configuration of the system to an external server using SCP. Before you begin you need to have the following configuration in place and information about the SCP server available:
 - The hostname or IP address and the port number of a secure SCP server.
 - A preconfigured path on the SCP server where the backup will be stored.
 - User credentials with file read and write permissions to the directory.
 - The SCP server storage requirements will vary slightly but you must have at least 25 GB of storage.
- Ensure that you have configured a destination SCP server to store the backup files. This configuration is a one-time activity.
- After the backup operation is completed, navigate to the destination SCP server directory and ensure that the backup file is created. You will require this backup file in the later stages of the upgrade process.
- Both the Cisco Crosswork cluster and the SCP server must be in the same IP environment. For example: If Cisco Crosswork is communicating over IPv6, so must the backup server.
- Keep a record of the list of Crosswork applications you have installed in the current version of Cisco Crosswork, as you can only install those applications after migrating to the new version of Cisco Crosswork.
- If you have onboarded a custom MIB package in the current version of Cisco Crosswork, download a copy of the package to your system. You will need to upload the package after you complete migrating to new version of Cisco Crosswork. See [Post-upgrade Checklist, on page 200](#) for more information.
- If you have modified the current version of Cisco Crosswork to include third-party device types, you must download the third-party device configuration file, and re-apply it to the new version of Cisco Crosswork. The device configuration file is located on the cluster node (at `/mnt/cw_glusterfs/bricks/brick3/sys-oids.yaml`) and on the pod (at `/mnt/backup/sys-oids.yaml`).
- If Cisco Crosswork Optimization Engine has feature packs (Local Congestion Mitigation (LCM), Bandwidth Optimization (BWOpt), and Bandwidth on Demand (BWoD)) that are enabled, you must disable them before proceeding. You must also, if available, export the current list of interfaces managed by LCM or BWOpt (**Traffic Engineering > Local Congestion Mitigation > Domain Identifier <domain_id> > Interface Thresholds > Export OR Traffic Engineering > Bandwidth Optimization**

> **Interface Thresholds** > **Export** icon). Follow the steps documented in [Upgrade Requirements](#), on page 190.

Step 1 Check and confirm that all the VMs are healthy and running in your cluster.

Step 2 **Configure an SCP backup server:**

- a) From the Cisco Crosswork main menu, choose **Administration** > **Backup and Restore**.
- b) Click **Destination** to display the **Edit Destination** dialog box. Make the relevant entries in the fields provided.
- c) Click **Save** to confirm the backup server details.

Step 3 **Create a backup:**

- a) From the Cisco Crosswork main menu, choose **Administration** > **Backup and Restore**.
- b) Click **Actions** > **Backup** to display the **Backup** dialog box with the destination server details prefilled.
- c) Provide a relevant name for the backup in the **Job Name** field.
- d) If any of the VMs or applications are not in **Healthy** state, but you want to create the backup, check the **Force** check box.

Note The **Force** option must be used only after consultation with the Cisco Customer Experience team.

- e) Uncheck the **Backup NSO** checkbox if you don't want to include Cisco NSO data in the backup.

If you do want to include Cisco NSO data in the Cisco Crosswork backup process, follow the instructions given in **Backup Cisco Crosswork with Cisco NSO** section in the *Cisco Crosswork Network Controller 5.0 Administration Guide* instead of the instructions here.

- f) Complete the remaining fields as needed.

If you want to specify a different remote server upload destination: Edit the pre-filled **Host Name**, **Port**, **Username**, **Password** and **Remote Path** fields to specify a different destination.

- g) (Optional) Click **Verify Backup Readiness** to verify that Cisco Crosswork has enough free resources to complete the backup. If the verifications are successful, Cisco Crosswork displays a warning about the time-consuming nature of the operation. Click **OK**.

If the verification is unsuccessful, please contact the Cisco Customer Experience team for assistance.

- h) Click **Start Backup** to start the backup operation. Cisco Crosswork creates the corresponding backup job set and adds it to the job list. The Job Details panel reports the status of each backup step as it is completed.
- i) To view the progress of a backup job: Enter the job details (such as Status or Job Type) in the search fields in the **Backup and Restore Job Sets** table. Then click on the job set you want.

The **Job Details** panel displays information about the selected job set, such as the job Status, Job Type, and Start Time. If there's a failed job, hover the mouse pointer over the icon near the **Status** column to view the error details.

Note After the backup operation is completed, navigate to the destination SCP server directory and ensure that the backup file is created. You will require this backup file in the later stages of the upgrade process.

Note If you do not see your backup job in the list, refresh the **Backup and Restore Job Sets** table.

- j) If the backup fails during upload to the remote server: In the **Job Details** panel, just under the Status icon, click the **Upload backup** button to retry the upload.

Note Upload can fail due to connectivity problems with the SCP backup server (for example, incorrect credentials, missing directory or directory permissions, missing path and so on). This is indicated by failure of the task `uploadBackupToRemote`. If this happens, check the SCP server details, correct any mistakes and try again. Alternatively, you can use the **Destination** button to specify a different SCP server and path before clicking **Upload backup**.

Step 4 After a successful backup, shut down the Cisco Crosswork cluster by powering down the VMs hosting each node (start with the Hybrid VMs):

- a) Log into the VMware vSphere Web Client.
- b) In the **Navigator** pane, right-click the VM that you want to shut down.
- c) Choose **Power > Power Off**.
- d) Wait for the VM status to change to **Off**.
- e) Wait for 30 seconds and repeat steps 4a to 4d for each of the remaining VMs.

Step 5 Move Cisco NSO into read-only mode to avoid any unintended updates to Cisco NSO during the upgrade. Use the following command to move NSO to read-only mode:

```
ncs_cmd -c maapi_read_only
```

Install the latest version of the Cisco Crosswork Cluster

After the successful backup of the old version of Cisco Crosswork, proceed to install the latest version of the Cisco Crosswork cluster.



Note The number of VM nodes installed in the new version of Cisco Crosswork must be equal or more than the number of VM nodes in the old version of Cisco Crosswork.



Note While the cluster installation is in progress, you must upgrade NSO to version 6.1.0. The process to upgrade NSO is not covered in this document. For more information, see the relevant [Cisco NSO documentation](#). Additionally, if you are planning to use Cisco Optimization Engine individually or as part of the Cisco Network Controller solution, upgrade your SR-PCE to version 7.9.1 (see [Crosswork Network Controller 5.0 Release Notes](#) for details).

Before you begin

- Make sure that your environment meets all the installation prerequisites (see [Installation Prerequisites for VMware vCenter](#), on page 19 for VMware and [Installation Prerequisites for AWS EC2](#), on page 111 for AWS).

Step 1 Install Cisco Crosswork cluster on your preferred platform (see [Install Crosswork Cluster on VMware vCenter](#), on page 37 for VMware and [Install Cisco Crosswork Network Controller on AWS EC2](#), on page 125 for AWS).

Note 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 into and troubleshoot the Crosswork application VM. You will use it to verify that the VM has been properly set up.

- Step 2** After the installation is completed, log into the Cisco Crosswork UI and check if all the nodes are up and running in the cluster.
- From the Cisco Crosswork main menu, choose **Administration > Crosswork Manager > Crosswork Summary**.
 - Click **Crosswork Cluster** tile to view the details of the cluster such as resource utilization by node, the IP addresses in use, whether each node is a Hybrid or Worker, and so on.

Install the Cisco Crosswork Applications

After successfully installing the new version of the Cisco Crosswork cluster, proceed to install the latest version of the Cisco Crosswork applications.



Note The Cisco Crosswork applications that you install must be the same ones that were backed up during [Create Backup and Shut Down Cisco Crosswork, on page 193](#).

Step 1 Install the Cisco Crosswork applications using the steps described in [Install Crosswork Applications, on page 159](#).

- Step 2** After the applications are successfully installed, check the health of the new Cisco Crosswork cluster.
- From the Cisco Crosswork main menu, choose **Administration > Crosswork Manager > Crosswork Summary**.
 - Click **Crosswork Cluster** tile to view the health details of the cluster.

Migrate Cisco Crosswork Backup

After successfully installing the new versions of the Cisco Crosswork applications, proceed to migrate the Cisco Crosswork backup taken earlier to the new Cisco Crosswork cluster.

Before you begin

Before you begin, ensure that you have:

- The hostname or IP address and the port number of a secure destination SCP server used in [Create Backup and Shut Down Cisco Crosswork, on page 193](#).
- The name and path of the backup file created in [Create Backup and Shut Down Cisco Crosswork, on page 193](#).
- User credentials with file read and write permissions to the directory.

Step 1 Check and confirm that all the VMs are healthy and running in your cluster.

Step 2 **Configure an SCP backup server:**

- a) From the main menu, choose **Administration > Backup and Restore**.
- b) Click **Destination** to display the **Edit Destination** dialog box.
- c) Make the relevant entries in the fields provided.

Note In the **Remote Path** field, please provide the location of the backup created in [Create Backup and Shut Down Cisco Crosswork, on page 193](#).

- d) Click **Save** to confirm the backup server details.

Step 3 **Migrate the previous Cisco Crosswork backup on the new Cisco Crosswork cluster:**

- a) From the Cisco Crosswork main menu, choose **Administration > Backup and Restore**.
- b) Click **Actions > Data Migration** to display the **Data Migration** dialog box with the destination server details prefilled.
- c) Provide the name of the data migration backup (created in [Create Backup and Shut Down Cisco Crosswork, on page 193](#)) in the **Backup File Name** field.
- d) If you want to perform the data migration backup despite any Cisco Crosswork application or microservice issues, check the **Force** check box.
- e) Click **Start Migration** to start the data migration operation. Cisco Crosswork creates the corresponding data migration job set and adds it to the **Backup and Restore Job Sets** table. The Job Details panel reports the status of each backup step as it is completed.

Note If you do not see your job in the list, please wait for a few minutes and refresh the **Backup and Restore Job Sets** table.

- f) To view the progress of a data migration job: Enter the job details (such as Status or Job Type) in the search fields in the **Backup and Restore Job Sets** table. Then click on the job set you want.

The **Job Details** panel displays information about the selected job set, such as the job Status, Job Type, and Start Time. If there's a failed job, hover the mouse pointer over the icon near the **Status** column to view the error details.

Note Crosswork UI might become temporarily unavailable during the data migration operation. When the Crosswork UI is down, you can view the job status in the Grafana dashboard. The Grafana link is available as *View Data Migration Process Dashboard* option on the right side of the Job Details window.

- g) If the data migration fails in between, you need to restart the procedure from step 1.

Step 4 After the data migration is successfully completed, check the health of the new Cisco Crosswork cluster.

- a) From the Cisco Crosswork main menu, choose **Administration > Crosswork Manager > Crosswork Summary**.
 - b) Click **Crosswork Cluster** tile to view the health details of the cluster.
-

Upgrade Crosswork Data Gateway

This is the final stage of the upgrade work flow. Ensure that the migration is complete and the new Cisco Crosswork UI is available before you proceed with installing the latest version of Crosswork Data Gateway.



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

Crosswork Data Gateway functions as a passive device in the network. The Crosswork Data Gateway upgrade process consists of the following steps replacing all the old Crosswork Data Gateway VMs with Crosswork Data Gateway VMs in the network.



Important Step 8 in this procedure requires you log out of Cisco Crosswork and log in again after verifying the deployment and enrollment of the latest Crosswork Data Gateway VMs with Cisco Crosswork. After you log in, an **Action to be taken** window appears prompting you to confirm that the upgrade is complete. Do not click **Acknowledge** unless you have completed all the verification steps mentioned in Step 3, Step 4, and Step 5 in the procedure.

- Step 1** Log out of Cisco Crosswork and log in again.
- Step 2** After you log in, an **Action to be taken** window appears. Close this window and do not click **Acknowledge**.
- Step 3** Install new Cisco Crosswork Data Gateway VMs with the same number and the same information (management interface importantly) as the old Crosswork Data Gateway VMs. Follow the steps in the [Cisco Crosswork Data Gateway Installation Workflow, on page 67](#).
- Step 4** Wait for about 5 minutes and navigate to **Administration > Data Gateway Management**.
- Step 5** Check the **Data Gateway Instances** tab to verify that the new Crosswork Data Gateway VMs are enrolled with Cisco Crosswork and have the **Admin State** as **Up** and **Operational State** as **Not Ready**.

Figure 33: Data Gateway Instances Window

Operational State	Administration State	Data Gateway Instance Name	Role	Outage History	Data Gateway Name	Pool Name	PDG Identifier	High Availability Status	Actions
Not Ready	Up	cdg-147.cisco.com	Spare		pool1	pool1	567837sf-cst1a-4-	Protected	
Up	Up	cdg-148.cisco.com	Assigned		pool1-2	pool1	63405e44-3a20-	Protected	
Not Ready	Up	cdg-149.cisco.com	Unassigned				e2db0cd1-3eba-	Not Protected	

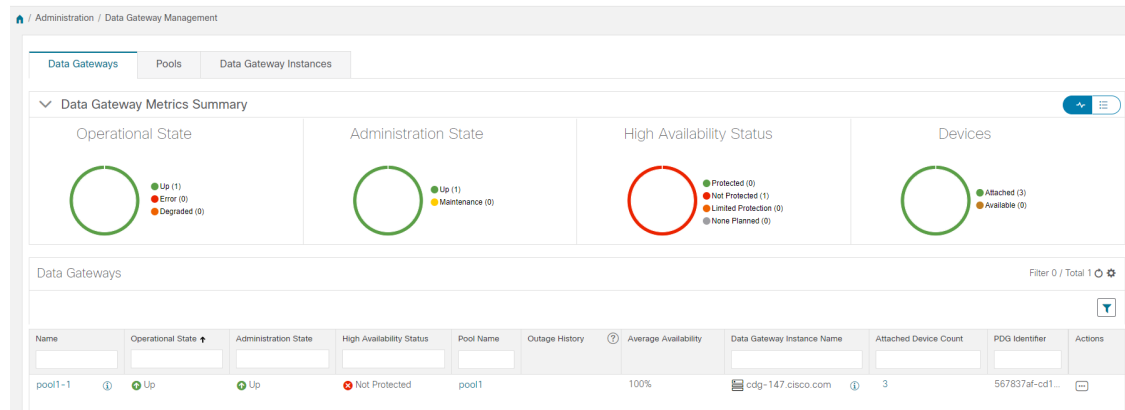
- Step 6** After the **Operational State** of the VMs changes to **Ready**, navigate to the **Pools** tab and verify that all the Crosswork Data Gateway pools from the previous version of Cisco Crosswork, are listed here. Edit each Crosswork Data Gateway pool to verify that the active Crosswork Data Gateway is same as one that you noted in the previous version of Cisco Crosswork.

Note You can also verify the pool details by clicking on the pool name.

- Step 7** **Verify that devices are attached to the Crosswork Data Gateways in the Cisco Crosswork UI.**

- Navigate to the **Administration > Data Gateway Management** page.
- Check the **Attached Device Count** of the Crosswork Data Gateway.

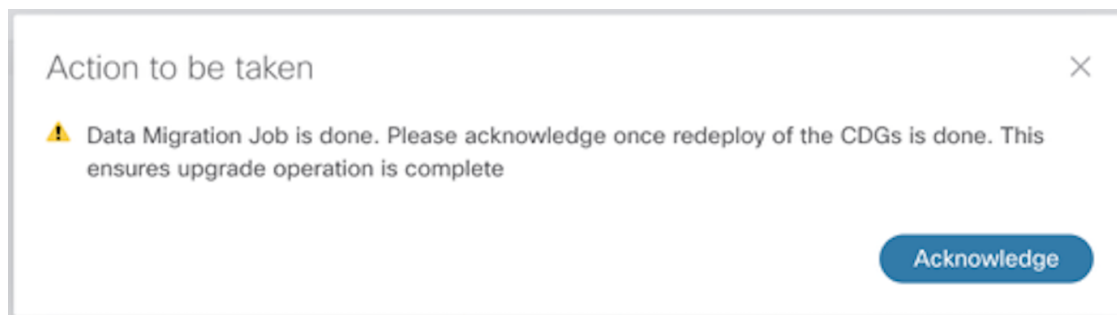
Figure 34: Data Gateway Window



Step 8 Log out of Cisco Crosswork and log in again.

Step 9 After you log in, Cisco Crosswork presents you with the following window prompting for confirmation that the VMs. Click **Acknowledge** in the pop-up that appears.

Figure 35: Acknowledgment Window



Important Do not click **Acknowledge** unless you have verified that the VMs are in the **Up/Not Ready** state. Doing so results in VMs having the state as **Error**. See [Troubleshoot Crosswork Data Gateway Upgrade Issues](#).

Step 10 (Optional) Move Cisco NSO out of maintenance or read-only mode.

```
ncs_cmd -c maapi_read_write
```

After the upgrade is complete:

- Crosswork Data Gateway VMs are enrolled with Cisco Crosswork.
- All destinations, Crosswork Data Gateway pools, device-mapping information can be viewed on the Cisco Crosswork UI with the upgraded Crosswork Data Gateway VMs.
- Collection jobs start again automatically with the new Cisco Crosswork Data Gateway VMs.
- After upgrading the Crosswork Data Gateway VM, you must reconfigure the collector resources and the disabled containers. Global Parameter resources that were configured prior to the upgrade are not retained. To configure the resource parameters, on the Crosswork UI, navigate to **Administration > Data Gateway Global Settings > Data Gateway > Resource**. For more information on the resources, see [Cisco Crosswork Network Controller 5.0 Administration Guide](#).

Troubleshoot Crosswork Data Gateway Upgrade Issues

The following table lists common problems that might be experienced when upgrading the Crosswork Data Gateway, and provides approaches to identifying the source of the problem and solving it.

Issue	Recommended Action
Some of the Crosswork Data Gateway VMs are in Error or Degraded state because you clicked Acknowledge before the VMs came to the Up/Not Ready state	<ol style="list-style-type: none"> 1. Wait for the Crosswork Data Gateway VMs to have the state as Up or Not Ready state. 2. Once the VMs have the state as Up or Not Ready, delete all Crosswork Data Gateway pools and create them again.
Some of the Crosswork Data Gateway VMs are in Error or Degraded state because you clicked Acknowledge before the VMs came to the Up/Not Ready state. The state of the VMs did not change to Up/Ready and they are still in Error .	<ol style="list-style-type: none"> 1. Delete all Crosswork Data Gateway pools. 2. Check if the VMs now have the state as Up or Not Ready. 3. If the VMs are still in a state of Error, manually re-enroll the VMs with the new version of Cisco Crosswork. See Re-enroll Crosswork Data Gateway for more information.
Crosswork Data Gateways VMs are stuck in the Degraded state with Image manager being in exited state. The list of components for the Crosswork Data Gateway either do not show Image manager or show it in an exited state.	<ol style="list-style-type: none"> 1. In the Cisco Crosswork UI, navigate to Data Gateway Management > Virtual Machines. 2. Click the Crosswork Data Gateway that is degraded. 3. Click Actions and click Reboot.

Post-upgrade Checklist

After you upgrade Cisco Crosswork to the latest version, check the health of the new cluster. If your cluster is healthy, perform the following activities:

- Perform a hard refresh or browser cache deletion before proceeding to use the system. Failing to do this step can result in data discrepancy.
- Navigate to **Administration > Collection Jobs** in Cisco Crosswork UI and delete the duplicate system jobs.

Figure 36: Collection Jobs Window

Status	App ID	Context ID	Action
Successful	cw.dminvmgr0	dim/cli-collector/group/reachability/subscription	⊙
Successful	cw.dminvmgr	dim/cli-collector/group/reachability/subscription	⊙
Degraded	cw.dminvmgr	dim/sntp-collector/group/subscription	⊙
Degraded	cw.dminvmgr	dim/cli-collector/group/te-tunnel-id/subscription	⊙
Degraded	cw.dminvmgr0	dim/cli-collector/group/te-tunnel-id/subscription	⊙
Degraded	cw.dminvmgr0	dim/sntp-collector/group/subscription	⊙
Degraded	cw.dminvmgr0	dim/cli-collector/group/showclock/subscription	⊙
Deleting	cw.dminvmgr	dim/cli-collector/group/showclock/subscription	⊙

- Verify that the collection jobs are running on the Crosswork Data Gateway VMs in the **Administration** > **Collection Jobs** page.
- Verify the restored AAA data by logging in using default credentials, and configure custom user roles (Read-Write/Read) in the upgraded Cisco Crosswork.
- (Optional) Based on your network requirements, download the relevant map files from cisco.com and re-upload them to the upgraded Cisco Crosswork.
- (Optional) If any NSO device onboarding policy was set in the previous version of Cisco Crosswork, you must update the policy with new Network Element Drivers (NED) on the NSO.
- (Optional) Re-apply any third-party device configurations (used in the previous version of Cisco Crosswork) to the new version of Cisco Crosswork.
- If you are using Crosswork Change Automation, verify that all the stock and custom playbooks are migrated successfully.
- If you are using Crosswork Health Insights, verify that the collection to the external destination is working. Also, check if the alert dashboard is displaying the correct data.
- If you are using Crosswork Optimization Engine, perform the following actions:
 - Upgrade the software versions in your devices as per the supported Cisco IOS XE/XR versions documented in the [Cisco Crosswork Optimization Engine Release Notes](#).
 - Verify feature packs (Local Congestion Mitigation (LCM), Bandwidth Optimization (BWOpt), and Bandwidth on Demand (BWoD)) using the instructions in [Upgrade Requirements, on page 190](#).

If you encounter errors in any of the above activities, please contact the Cisco Customer Experience team.

Upgrade Using Parallel Hardware

This section explains how to migrate to the latest version of Crosswork Network Controller using new hardware. This method relies on installing the new Cisco Crosswork cluster on new hardware in parallel while the data from the old Cisco Crosswork cluster is being backed up. This method is faster but requires twice the amount of resources for creating the new cluster in parallel.

The stages of the parallel upgrade workflow are:

1. [Deploy a new Cisco Crosswork Cluster, on page 202](#)



Note While the cluster installation is in progress, you must upgrade NSO to version 6.1.0. The process to upgrade NSO is not covered in this document. For more information, see the relevant [Cisco NSO documentation](#). You must also upgrade your SR-PCE to version 7.9.1. For install instructions, see the [Cisco IOS XRv 9000 Router Installation Guide](#).

2. [Backup Cisco Crosswork Cluster, on page 203](#)
3. [Update DNS Server and Run Migration , on page 205](#)
4. [Add Crosswork Data Gateway to Cisco Crosswork, on page 206](#)
5. [Shut Down the old Cisco Crosswork Cluster, on page 208](#)

Deploy a new Cisco Crosswork Cluster

Install the latest version of Cisco Crosswork cluster and applications on a new set of VMs in parallel.



Note The new Cisco Crosswork cluster must be installed with the same FQDN and same number of nodes as in the old version of Cisco Crosswork.

Before you begin

- Make sure that your environment meets all the installation prerequisites (see [Installation Prerequisites for VMware vCenter, on page 19](#) for VMware and [Installation Prerequisites for AWS EC2, on page 111](#) for AWS).

Step 1 Install the new Cisco Crosswork cluster on your preferred platform (see [Install Crosswork Cluster on VMware vCenter, on page 37](#) for VMware and [Install Cisco Crosswork Network Controller on AWS EC2, on page 125](#) for AWS).

Note 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 into and troubleshoot the Crosswork application VM. You will use it to verify that the VM has been properly set up.

Step 2 After the installation is completed, log into the Cisco Crosswork UI by navigating to https://<NEW_VIP>:30603.

Step 3 Check if all the nodes are up and running in the cluster.

- a) From the Cisco Crosswork main menu, choose **Administration > Crosswork Manager > Crosswork Summary**.
- b) Click **Crosswork Cluster** tile to view the details of the cluster such as resource utilization by node, the IP addresses in use, whether each node is a Hybrid or Worker, and so on.

Step 4 Install the applications which were part of the old version of Cisco Crosswork. For more information, see [Install Crosswork Applications, on page 159](#).

Step 5 After the applications are successfully installed, check the health of the new Cisco Crosswork cluster.

Backup Cisco Crosswork Cluster

Before you begin

Follow these guidelines whenever you create a backup:

- Cisco Crosswork will back up the configuration of the system to an external server using SCP. Before you begin you need to have the following configuration in place and information about the SCP server available:
 - The hostname or IP address and the port number of a secure SCP server.
 - A preconfigured path on the SCP server where the backup will be stored.
 - User credentials with file read and write permissions to the directory.
 - The SCP server storage requirements will vary slightly but you must have at least 25 GB of storage.
- Ensure that you have configured a destination SCP server to store the backup files. This configuration is a one-time activity.
- Both the Cisco Crosswork cluster and the SCP server must be in the same IP environment. For example: If Cisco Crosswork is communicating over IPv6, so must the backup server.
- Keep a record of the list of Crosswork applications you have installed in the current version of Cisco Crosswork, as you can only install those applications after migrating to the new version of Cisco Crosswork.
- If you have onboarded a custom MIB package in the previous version of Cisco Crosswork, download a copy of the package to your system. You will need to upload the package after you complete upgrading Cisco Crosswork. See [Post-upgrade Checklist, on page 200](#) for more information.
- If you have modified the previous version of Cisco Crosswork to include third-party device types, you must download the third-party device configuration file, and re-apply it to the upgraded Cisco Crosswork. The device configuration file is located on the cluster node (at `/mnt/cw_glusterfs/bricks/brick3/sys-oids.yaml`) and on the pod (at `/mnt/backup/sys-oids.yaml`).
- If Cisco Crosswork Optimization Engine has feature packs (Local Congestion Mitigation (LCM), Bandwidth Optimization (BWOpt), and Bandwidth on Demand (BWoD)) that are enabled, you must disable them before proceeding. You must also, if available, export the current list of interfaces managed by LCM or BWOpt (**Traffic Engineering > Local Congestion Mitigation > Domain Identifier <domain_id> > Interface Thresholds > Export** OR **Traffic Engineering > Bandwidth Optimization > Interface Thresholds > Export** icon). Follow the steps documented in [Upgrade Requirements, on page 190](#).



Note

We recommend that you create a backup only during a scheduled upgrade window. Users should not attempt to access Cisco Crosswork while the backup operation is running.

-
- Step 1** Launch the Cisco Crosswork UI by using a browser and navigating to `https://<FQDN>:30603`
- Step 2** Check and confirm that all the VMs are healthy and running in your cluster.

Step 3 Configure an SCP backup server:

- a) From the Cisco Crosswork main menu, choose **Administration > Backup and Restore**.
- b) Click **Destination** to display the **Edit Destination** dialog box. Make the relevant entries in the fields provided.
- c) Click **Save** to confirm the backup server details.

Step 4 Create a backup:

- a) From the Cisco Crosswork main menu, choose **Administration > Backup and Restore**.
- b) Click **Actions > Backup** to display the **Backup** dialog box with the destination server details prefilled.
- c) Provide a relevant name for the backup in the **Job Name** field.
- d) If any of the VMs or applications are not in **Healthy** state, but you want to create the backup, check the **Force** check box.

Note The **Force** option must be used only after consultation with the Cisco Customer Experience team.

- e) Uncheck the **Backup NSO** check box if you don't want to include Cisco NSO data in the backup.
If you want to include Cisco NSO data in the Cisco Crosswork backup process, follow the instructions given in **Backup Cisco Crosswork with Cisco NSO** section in the [Cisco Crosswork Network Controller 5.0 Administration Guide](#) instead of the instructions here.
- f) Complete the remaining fields as needed.
If you want to specify a different remote server upload destination: Edit the pre-filled **Host Name**, **Port**, **Username**, **Password** and **Remote Path** fields to specify a different destination.
- g) (Optional) Click **Verify Backup Readiness** to verify that Cisco Crosswork has enough free resources to complete the backup. Cisco Crosswork will also confirm that none of the applications are being updated, if the remote destination is correctly defined and if the applications are healthy. If the verifications are successful, Cisco Crosswork displays a warning about the time-consuming nature of the operation. Click **OK**.

If the verification is unsuccessful, please contact the Cisco Customer Experience team for assistance.

- h) Click **Start Backup** to start the backup operation. Cisco Crosswork creates the corresponding backup job set and adds it to the job list. The Job Details panel reports the status of each backup step as it is completed.
- i) To view the progress of a backup job: Enter the job details (such as Status or Job Type) in the search fields in the **Backup and Restore Job Sets** table. Then click on the job set you want.

The **Job Details** panel displays information about the selected job set, such as the job Status, Job Type, and Start Time. If there's a failed job, hover the mouse pointer over the icon near the **Status** column to view the error details.

Note If you do not see your backup job in the list, refresh the **Backup and Restore Job Sets** table.

- j) If the backup fails during upload to the remote server: In the **Job Details** panel, just under the Status icon, click the **Upload backup** button to retry the upload.

Note Upload can fail due to connectivity problems with the SCP backup server (for example, incorrect credentials, missing directory or directory permissions, missing path and so on). This is indicated by failure of the task **uploadBackupToRemote**. If this happens, check the SCP server details, correct any mistakes and try again. Alternatively, you can use the **Destination** button to specify a different SCP server and path before clicking **Upload backup**.

Update DNS Server and Run Migration

Before you begin

Before you begin, ensure that you have:

- The hostname or IP address and the port number of a secure SCP server.
- The name and path of the backup file created in .
- User credentials with file read and write permissions to the directory.

Step 1 Update the DNS server to point the FQDN of the previous version of Cisco Crosswork cluster to the <VIP> of the new Cisco Crosswork cluster.

Step 2 Navigate to the upgraded Cisco Crosswork UI using `https://<new_VIP>:30603`.

Step 3 **Configure an SCP backup server:**

- a) From the main menu, choose **Administration > Backup and Restore**.
- b) Click **Destination** to display the **Edit Destination** dialog box.
- c) Make the relevant entries in the fields provided.

Note In the **Remote Path** field, please provide the location of the backup created in [Backup Cisco Crosswork Cluster, on page 203](#).

- d) Click **Save** to confirm the backup server details.

Step 4 **Migrate the old Cisco Crosswork backup:**

- a) From the Cisco Crosswork main menu, choose **Administration > Backup and Restore**.
- b) Click **Actions > Data Migration** to display the **Data Migration** dialog box with the destination server details prefilled.
- c) Provide the name of the data migration backup (created in [Backup Cisco Crosswork Cluster, on page 203](#)) in the **Backup File Name** field.
- d) If you want to perform the data migration backup despite any Cisco Crosswork application or microservice issues, check the **Force** check box.
- e) Click **Start Migration** to start the data migration operation. Cisco Crosswork creates the corresponding data migration job set and adds it to the **Backup and Restore Job Sets** table. The Job Details panel reports the status of each backup step as it is completed.

Note If you do not see your job in the list, refresh the **Backup and Restore Job Sets** table.

- f) To view the progress of a data migration job: Enter the job details (such as Status or Job Type) in the search fields in the **Backup and Restore Job Sets** table. Then click on the job set you want.

The **Job Details** panel displays information about the selected job set, such as the job Status, Job Type, and Start Time. If there's a failed job, hover the mouse pointer over the icon near the **Status** column to view the error details.

Note Crosswork UI and Grafana monitoring might become temporarily unavailable during the data migration operation.

- g) If the data migration fails in between, you need to restart the procedure from step 1.

Step 5 After the data migration is successfully completed, check the health of the new Cisco Crosswork cluster.

- a) From the Cisco Crosswork main menu, choose **Administration > Crosswork Manager > Crosswork Summary**.

b) Click **Crosswork Cluster** tile to view the health details of the cluster.

Note After a successful migration, please perform a hard refresh or browser cache deletion before proceeding to use the system. Failing to do this step can result in data discrepancy.

Add Crosswork Data Gateway to Cisco Crosswork

Ensure that the migration is complete and the new Cisco Crosswork UI is available before you proceed with installing the new version of Crosswork Data Gateway.



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

Crosswork Data Gateway functions as a passive device in the network. The Crosswork Data Gateway upgrade process consists of replacing all old Crosswork Data Gateway VMs with new Crosswork Data Gateway VMs (latest version) in the network.



Important Step 6 in this procedure requires you to log out of Cisco Crosswork and log in again after verifying the deployment and enrollment of the new CDG VMs with Cisco Crosswork. After you log in, an **Action to be taken** window appears prompting you to confirm that the upgrade is complete. Do not click **Acknowledge** unless you have completed all the verification steps mentioned in Step 3, Step 4 and Step 5 in the procedure.

- Step 1** Log out of the upgraded Cisco Crosswork and log in again.
- Step 2** After you log in, an **Action to be taken** window appears. Close this window and do not click **Acknowledge**.
- Step 3** Install new Cisco Crosswork Data Gateway VMs (latest version) with the same number and the same information (management interface importantly) as the old Crosswork Data Gateway VMs. Follow the steps in the [Cisco Crosswork Data Gateway Installation Workflow](#), on page 67.
- Step 4** Wait for about 5 minutes and navigate to **Administration > Data Gateway Management**.
- Step 5** Check the **Data Gateway Instances** tab to verify that the new Crosswork Data Gateway VMs are enrolled with the new Cisco Crosswork, and have the **Admin State** as **Up** and **Operational State** as **Not Ready**.

Figure 37: Data Gateway Instances Window

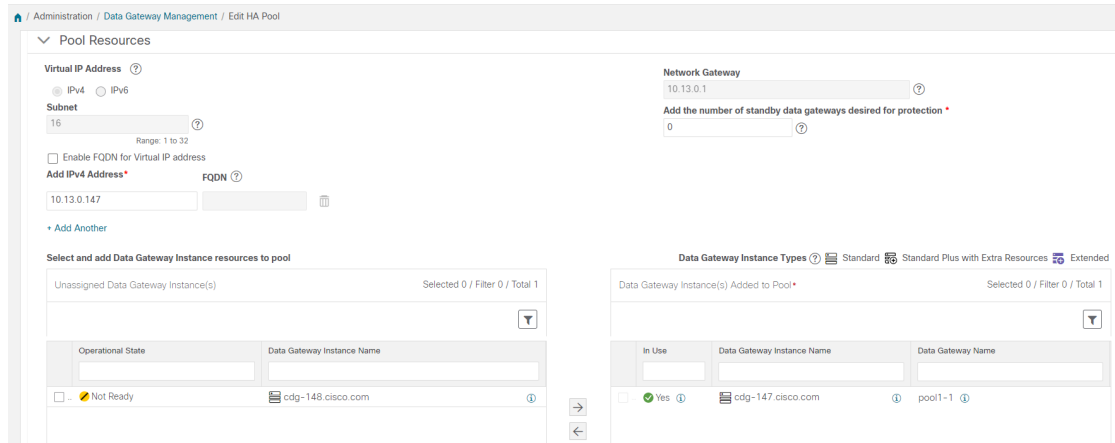
Operational State	Administration State	Data Gateway Instance Name	Role	Outage History	Data Gateway Name	Pool Name	PDG Identifier	High Availability Status	Actions
Not Ready	Up	cdg-147.cisco.com	Spare			pool1	567837af-cd1a-4...	Protected	
Up	Up	cdg-148.cisco.com	Assigned		pool1-2	pool1	63405e44-aa20-...	Protected	
Not Ready	Up	cdg-149.cisco.com	Unassigned				e2db0cd1-3eba-...	Not Protected	

Step 6

After the **Operational State** of the VMs changes to **Ready**, navigate to the **Pools** tab and verify that all the Crosswork Data Gateway pools from the old Cisco Crosswork, are listed here. Edit each Crosswork Data Gateway pool to verify that the active Crosswork Data Gateway is same as one that you noted in the older version of Cisco Crosswork.

For example, the Crosswork Data Gateway pool in the following image contains two VMs, where the active VM is 172.23.247.78

Figure 38: Edit HA Pool Window

**Step 7**

Verify that devices are attached to the new Crosswork Data Gateways in the upgraded Cisco Crosswork UI.

- Navigate to the **Administration > Data Gateway Management** page.
- Check the **Attached Device Count** of the Crosswork Data Gateway.

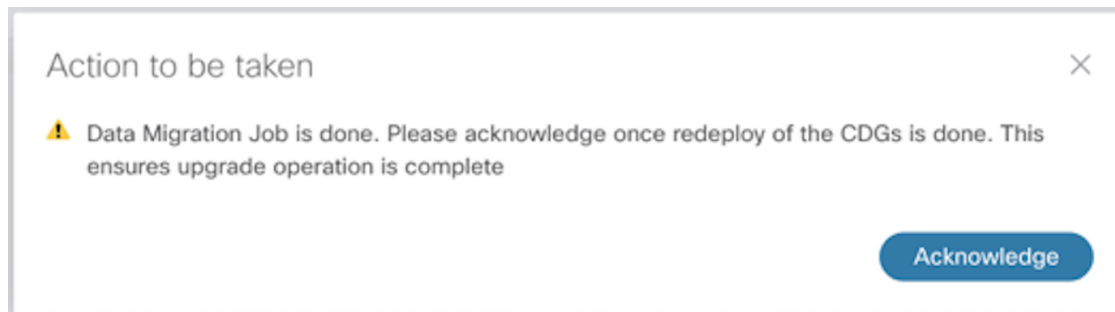
Step 8

Log out of Cisco Crosswork and log in again.

Step 9

After you log in, Cisco Crosswork presents you with the following window prompting for confirmation that the VMs. Click **Acknowledge** in the pop up that appears.

Figure 39: Acknowledgment Window



Important Do not click **Acknowledge** unless you have verified that the VMs are in the **Up/Not Ready** state. Doing so will result in VMs having the state as **Error**. See [Troubleshoot Crosswork Data Gateway Upgrade Issues](#).

Step 10

(Optional) Move Cisco NSO out of maintenance or read-only mode.

```
ncs_cmd -c maapi_read_write
```

After the upgrade is complete:

- The new Crosswork Data Gateway VMs are enrolled with upgraded Cisco Crosswork.
- All destinations, HA Pools, device mapping information can be viewed on the Cisco Crosswork UI with the upgraded Crosswork Data Gateway VMs.
- Jobs start again automatically with the new Cisco Crosswork Data Gateway VMs.

Shut Down the old Cisco Crosswork Cluster

Before you begin

Gather the following information before shutting down the older version of Cisco Crosswork:

- All the IP addresses in the cluster.
- All the IP addresses of the CDGs.

Step 1 After a successful backup, shut down the Cisco Crosswork cluster by powering down the VMs hosting each node (start with the Hybrid VMs):

- Log into the VMware vSphere Web Client.
- In the **Navigator** pane, right-click the VM that you want to shut down.
- Choose **Power > Power Off**.
- Wait for the VM status to change to **Off**.
- Wait for 30 seconds and repeat steps 1a to 1d for each of the remaining VMs.

Step 2 Shut down the Crosswork Data Gateway VMs.

- Log in to the previous version of Crosswork Data Gateway VM. See [Access Crosswork Data Gateway VM from SSH, on page 100](#).

Crosswork Data Gateway launches an Interactive Console after you login successfully.

- Choose **5 Troubleshooting**.
- From the **Troubleshooting** menu, choose **5 Shutdown VM** to shut down the VM.

Step 3 (Optional) Move Cisco NSO into read-only mode to avoid any unintended updates to Cisco NSO during the upgrade. Use the following command to move NSO to read-only mode:

```
ncs_cmd -c maapi_read_only
```

For more information, please refer to the relevant [Cisco NSO documentation](#).

Update a Crosswork Application (standalone activity)

This section explains how to independently update a Crosswork application from the Cisco Crosswork UI in case of minor updates or patch releases. This procedure is not part of the upgrade workflow discussed in the earlier sections.

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](https://www.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 Download and validate the CAPP files:

- Navigate to [cisco.com](https://www.cisco.com) and locate the CAPP files (.tar.gz) that you require.
- Hover over the file and copy the MD5 or SHA512 checksum to your clip board.
- Download the CAPP files to a server that can be reached from the Crosswork server.
- Run a tool of your choice to calculate the checksum, and compare the checksum value in your downloaded file with the value you copied in the clip board.

For example, on a MAC you can use the **md5** command to calculate the MD5 sum on a file:

```
md5 cw-na-ztp-4.0.3-3-release-220614.tar.gz

ff47a72ed7dc4fc4be388db3a43fa13f
```

Verify that the result value matches with the posted value on [cisco.com](https://www.cisco.com).

Step 2 Click on **Administration** > **Crosswork Manager**, and select the **Application Management** tab.

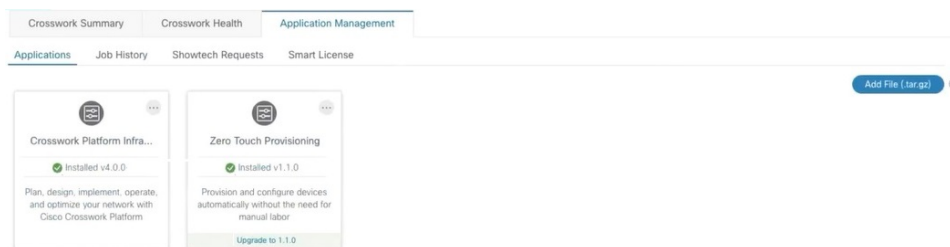
The Crosswork Platform Infrastructure and any applications that are added are displayed here as tiles.

Step 3 Click on the **Add File (.tar.gz)** option to add the application CAPP file that you had downloaded.

Step 4 In the Add File dialog box, enter the relevant information and click **Add**.

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

Figure 40: Applications Window - Upgrade Prompt



Step 5 To upgrade, click the Upgrade prompt and the new version of the application is installed.

Figure 41: Applications Window - Update Progress



The upgrade progress is displayed on the application tile.


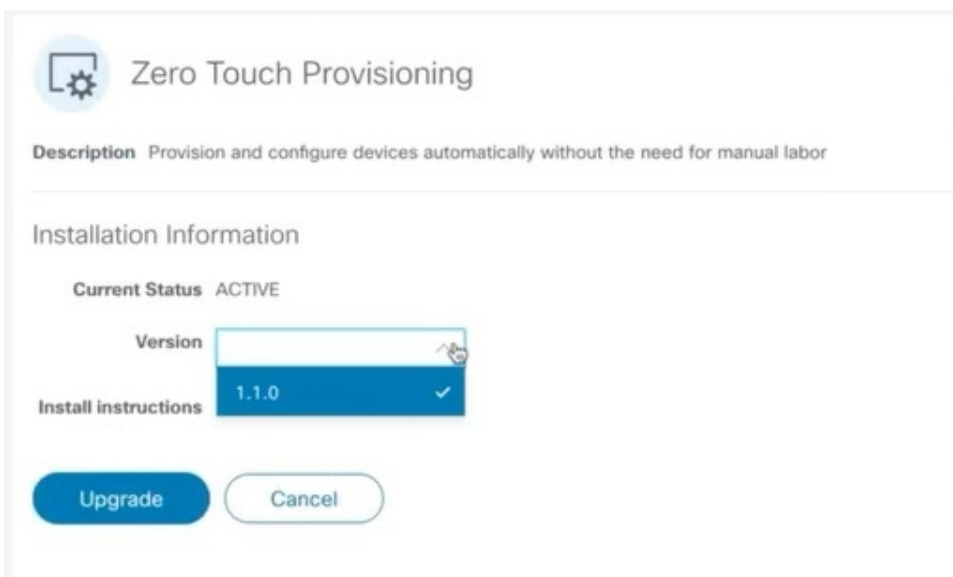
Step 6 Alternately, click  on the tile, and select the **Upgrade** option from the drop down list.

Figure 42: Applications Window - Upgrade Option



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

Figure 43: Upgrade Window



Step 7 (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.
-



PART **VII**

Uninstall Cisco Crosswork Network Controller

- [Uninstall Cisco Crosswork, on page 215](#)



CHAPTER 13

Uninstall Cisco Crosswork

This chapter contains the following topics:

- [Uninstall the Crosswork Cluster, on page 215](#)
- [Uninstall Crosswork Data Gateway, on page 216](#)
- [Uninstall Crosswork Applications, on page 218](#)

Uninstall the Crosswork Cluster

This section explains the various methods to uninstall the Cisco Crosswork cluster.

- [Delete the VM using the Cluster Installer, on page 215](#)
- [Delete the VM using the vSphere UI, on page 216](#)

Delete the VM using the 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 data center host requires a cleanup operation before redeployment.



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>
```

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.

Add `-o` option to remove the Cisco Crosswork image template from the data center.

For example:

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

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

Step 6 (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'
```

Delete the VM using the 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. For more information, see *Delete Cisco Crosswork Data Gateway VM from Cisco Crosswork* topic in the *Cisco Crosswork Network Controller 5.0 Administration Guide*.
 - Delete the Crosswork Data Gateway VM from Cisco Crosswork as described in this chapter.

Step 1 Log into 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.

Uninstall Crosswork Data Gateway

This section explains the methods to remove Cisco Crosswork Data Gateway.

- [Delete Crosswork Data Gateway VM from Cisco Crosswork, on page 217](#)
- [Delete Crosswork Data Gateway from the Crosswork Cluster, on page 217](#)

Delete Crosswork Data Gateway VM from Cisco Crosswork

Before you begin


The Crosswork Data Gateway VM you want to delete:

- Must be in the maintenance mode.
- Must not be a part of a pool or attached to a device.

Step 1 Log into Cisco Crosswork UI.

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

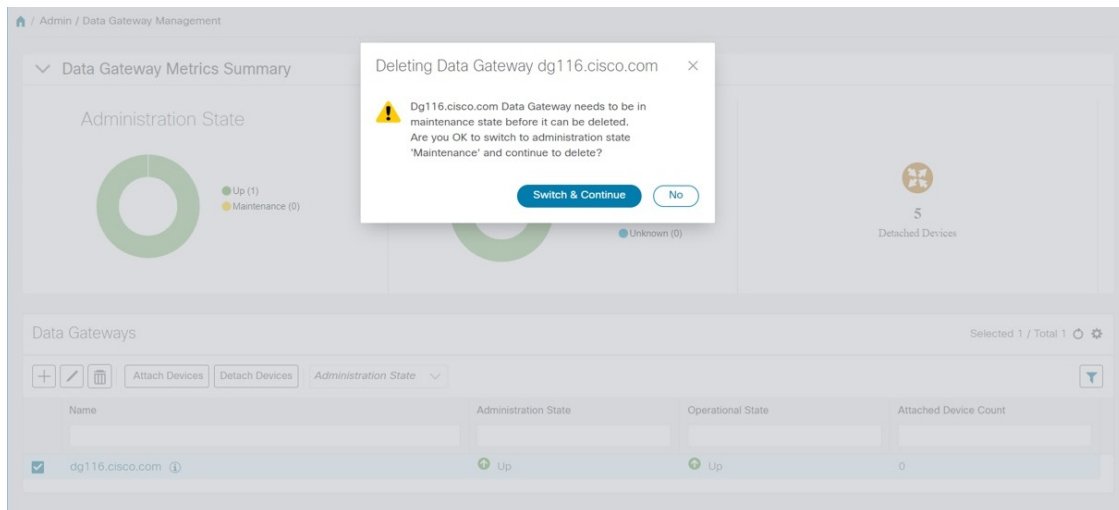
Click the **Data Gateway Instances** tab.

Step 3 In the **Data Gateway Instances** list, find the Crosswork Data Gateway instance you want to delete and click  under **Actions** column.

Click **Delete**.

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

Figure 44: Switch & Continue Pop-up Window



The Crosswork Data Gateway instance is deleted.

Delete Crosswork Data Gateway from the Crosswork Cluster

To remove Crosswork Data Gateway from the Crosswork cluster, follow the below steps:

Step 1 Remove the Crosswork Data Gateway instance from the Crosswork UI. Note down the **Data Gateway Instance Name** and **PDG Identifier** from the Crosswork UI.

Step 2 Execute the following commands to remove the pods from the Crosswork cluster:

- `kubectl edit cdgoperator cdgoperator-cr -n cdg`
 - If there is only one Crosswork Data Gateway in the cluster, remove the CDG array **including** `cdg_dep_plan` under the **spec** section.
 - If there are more than one Crosswork Data Gateway in the cluster, remove only the CDG array entry **under** `cdg_dep_plan` which has to be deleted and save it.
- `kubectl delete infraservices <Data Gateway Instance Name> -n cdg`
For example, `kubectl delete infraservices op-cdg -n cdg`
- `kubectl delete collectors collector-<PDG Identifier> -n cdg`
For example, `kubectl delete collectors collector-26b0053f-5132-4379-a107-f924dfde77f4 -n cdg`
- `kubectl delete icon icon-<PDG Identifier> -n cdg`
For example, `kubectl delete icon icon-26b0053f-5132-4379-a107-f924dfde77f4 -n cdg`
- If offload pods are present, `kubectl delete offload offload-<PDG Identifier> -n cdg`
For example, `kubectl delete offload offload-26b0053f-5132-4379-a107-f924dfde77f4 -n cdg`

Uninstall Crosswork Applications


This section explains how to uninstall an application in the Crosswork UI. The **Uninstall** option removes the application, application-specific menus and associated data.



Attention Crosswork Active Topology (if installed) must be uninstalled before you can uninstall Crosswork Optimization Engine.

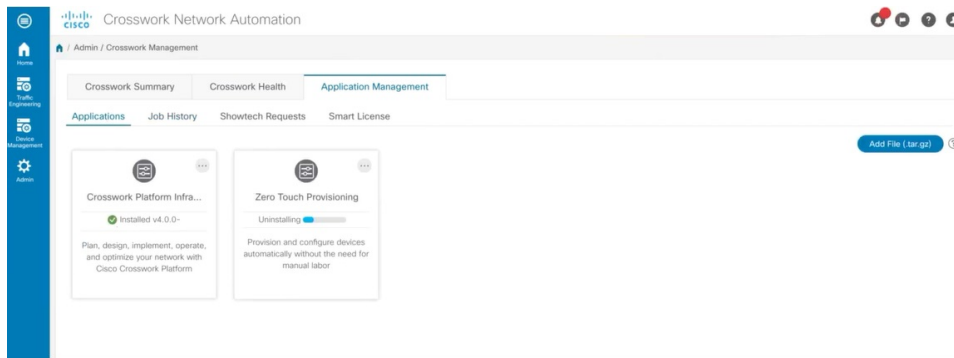
Step 1 Click on **Admin > Crosswork Manager**, and select the **Application Management** tab.

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.

Step 3 Click **Uninstall** to confirm when prompted.

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

Figure 45: Application Management Window

You can also view the progress of uninstallation in the Job History window (**Application Management > Job History**). If the uninstall fails, you can reattempt using the relevant options in the Job History window.

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

