



Cisco Crosswork Network Controller 7.1 Device Lifecycle Management

First Published: 2025-06-25

Americas Headquarters

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



CONTENTS

PART I

Onboard Devices 9

CHAPTER 1

Add and Configure Devices 1

- Add devices to the inventory 1
- Configuration prerequisites for new devices 2
- Sample Configuration for Cisco NSO Devices 10
- Add devices through the UI 11
- Add devices by importing from CSV file 16
- Export Device Information to a CSV File 18

CHAPTER 2

Zero Touch Provisioning 19

- Zero Touch Provisioning Concepts 19
 - ZTP and Evaluation Licenses 22
 - Platform Support for ZTP 22
 - Provisioning Support for Third-Party Devices 22
 - ZTP Implementation Decisions 23
 - ZTP Processing Logic 24
- ZTP Setup Workflow 28
 - Meet ZTP Prerequisites 29
 - Assemble the ZTP Assets 29
 - Loading Software Images 31
 - Prepare and Load Configuration Files 31
 - Load ZTP Assets 43
 - Find and Load SMUs 45
 - Create Credential Profiles for ZTP 46
 - Find and Load Device Serial Numbers 47

Update the PDC, Owner Certificates, and Owner Key	48
Load Ownership Vouchers	50
Prepare and Load the SUDI Root Certificate	51
Create ZTP Profiles	52
Prepare ZTP Device Entry Files	53
Prepare Single ZTP Device Entries	59
ZTP Provisioning Workflow	59
Upload ZTP Device Entries	60
Set Up DHCP for ZTP	60
Set Up DHCP for Classic ZTP	60
Set Up DHCP for Secure ZTP	64
Set Up DHCP and TFTP for PnP ZTP	65
Classic ZTP DHCP Setup Scripts for Cisco Prime Network Registrar (CPNR)	66
Trigger ZTP Device Bootstrap	80
Complete Onboarded ZTP Device Information	83
Reconfigure Onboarded ZTP Devices	84
Retire or Replace Devices Onboarded with ZTP	84
ZTP Asset Housekeeping	85
Troubleshoot ZTP Issues	85
Diagnose ZTP Issues Using the Alarms Window	86
Diagnose ZTP Issues Using the Status Column	86
Diagnose ZTP Issues Using Error Logs	87
Troubleshoot Common ZTP Issues	88
Troubleshoot Classic ZTP Issues	91
Troubleshoot PnP ZTP Issues	91
Troubleshoot ZTP: Alarms and Events Reference	92

PART II
Manage Devices 93

CHAPTER 3
View and Manage Devices 95

Manage onboarded devices	95
Monitor Device States	96
Filter Network Devices by Tags	98
Edit Devices	99

Delete Devices	100
View Detailed Inventory Collection Status	100
Enable or Disable Granular Inventory	101
Perform detailed inventory sync	102
Use Device Groups to Filter your Topology Map	102
Create Device Groups	102
Create Rules for Dynamic Device Grouping	103
Modify Device Groups	104
Delete Device Groups	104
Move Devices from One Group to Another	104
Import Multiple Device Groups	105
Export Multiple Device Groups	106
View Device Details from the Topology Map	106
View Basic Device Details	106
View All Device Details	107
Identify Device Routing Details	108
Identify the Links on a Device	109
View Detailed Device Inventory	110
Get Details About Topology Links	113
View Link Details	114
View Link Interface Metrics	116
Link States and Discovery Methods	116
Protocols Used for Topology Services	117
Enable or Disable Topology Link Discovery	118
View the network inventory	120
Export Inventory Results	123
View Device Job History	124
Manage Port Groups	125
Add Ports Manually to a Group	125
Add Ports Dynamically to a Group	126
Edit Port Group Properties	126
Create User-defined Port Group	126
Delete a Port Group	127
Import Port Groups	127

Export Port Groups 128

CHAPTER 4

Use Templates to Configure Similar Devices 129

Key benefits of configuration templates 130

Configuring devices using templates 130

Identify and group devices for deploying templates 131

Define configuration preferences for templates and backup and restore 132

Specify template details 133

Select device types 134

Define variables 134

Configuration template commands 136

Enable mode commands 136

Multi-line commands 136

Interactive commands 137

Mixed commands 138

Apache VTL: syntax and examples 139

Create template script 139

Deploy templates 140

Manage template jobs 142

Monitor and manage templates 143

Deploy templates from detailed inventory 144

Sample configuration scripts for templates 146

CHAPTER 5

Configuration Backup and Restore 147

Schedule a configuration backup 147

Restore a configuration backup 148

View a device configuration 149

Pin a device configuration 150

Compare device configurations 150

Export device configuration 151

Delete a device configuration 151

CHAPTER 6

Manage Software Images 153

Set up software image management (SWIM) 153

Add a software image to the image repository	154
Deploy a new software image to devices	155
Activate a new software image on devices	156
Delete software image files from the image repository	157

PART III

Monitor the Network 159

CHAPTER 7

Set Up and Monitor Alarms and Events 161

What Are Alarms and Events?	162
Interpret Event and Alarm Badges and Colors	162
Which Events Are Supported?	162
Set Alarm Thresholds to Manage How Alarms are Triggered	163
Configure the Settings for Alarms and Events	163
Customize Alarm Auto Clear	163
Customize Alarm Severity	164
Manage cleanup options for alarms, events, and audit logs	165
Customize device alarm manager settings	165
Customize Device Notifications	166
Customize gNMI Settings	167
Configure Alarms Notification Destination	167
Create a Notification Policy for Network and Devices	168
Manage Alarm Suppression Policy	169
Manage Alarms	169
Clear Alarms	170
Annotate Alarms	171
Export Alarms	171

CHAPTER 8

Monitor Device and Inventory Health 173

How are device and inventory health monitored?	173
Parameters monitored by each policy	174
Manage default policies	175
Configure gNMI based polling for interface health and LSP traffic policies	175
Create monitoring policies	176
View collection jobs for performance monitoring	176

Customize metrics for network analysis	177
Customize metric health settings	178
Set data retention periods for monitored metrics	179
View key metrics	180

APPENDIX A

Manage Unsupported Devices	181
Manage unsupported devices	181



PART I

Onboard Devices

- [Add and Configure Devices, on page 1](#)
- [Zero Touch Provisioning, on page 19](#)



CHAPTER 1

Add and Configure Devices

This section contains the following topics:

- [Add devices to the inventory, on page 1](#)
- [Configuration prerequisites for new devices, on page 2](#)
- [Sample Configuration for Cisco NSO Devices, on page 10](#)
- [Add devices through the UI, on page 11](#)
- [Add devices by importing from CSV file, on page 16](#)
- [Export Device Information to a CSV File, on page 18](#)

Add devices to the inventory

There are different ways to add devices to Crosswork. Each has its own set of prerequisites, which you must fulfill if the device addition is to succeed. As Cisco Crosswork Network Controller supports dual-stack deployment, you can onboard devices with both IPv4 and IPv6 addresses. It is recommended to onboard such devices only once, selecting either the IPv4 or IPv6 address.

Ensure that your devices are configured properly for communication and telemetry. See guidelines and example configurations in [Configuration prerequisites for new devices, on page 2](#) and [Sample Configuration for Cisco NSO Devices, on page 10](#).

In order of preference for most users, the methods and their prerequisites are:

1. **Importing devices using the Crosswork APIs:** This is the fastest and most efficient of all the methods, but requires programming skills and API knowledge.

For more information, see the [CNC 7.1 API documentation](#).

2. **Importing devices from a Devices CSV file:** This method can be time-consuming. To succeed with this method, you must first:

- Create corresponding credential profiles for all of the devices and providers listed in the CSV file.
- Create the provider(s) that will be associated with the devices.
- Create tags for use in grouping the new devices.
- Download the CSV template file from Crosswork and populate it with all the devices you plan to add.

For more information about adding providers, credential profiles and creating tags, refer to the *Cisco Crosswork Network Controller 7.1 Administration Guide*.

For information about adding devices using a CVS file, see [Add devices by importing from CSV file, on page 16](#).

3. **Adding them via the UI:** This method is the least error-prone of the three methods, as all data is validated during entry. It is also the most time-consuming, being suitable only for adding a few devices at a time. Note that the providers, credential profiles and tags you want to apply to them must exist beforehand. For more information, see [Add devices through the UI, on page 11](#).
4. **Auto-onboarding from a Cisco SR-PCE provider:** This method is highly automated and relatively simple. Note that the device and provider credential profiles and tags you want to apply to these devices must exist beforehand. The auto-onboarding method does not create or assign this information automatically. Devices are initially discovered and added with partial information. To complete the onboarding process, you will need to supplement the missing details. You can provide the additional information by uploading a CSV file or manually adding it using the API or UI.

For more information, see the provider properties described in the section, *Add Cisco SR-PCE Providers* in the *Cisco Crosswork Network Controller 7.1 Administration Guide*.



Note If a device onboarded in Cisco Crosswork is on the same subnet as a Crosswork Data Gateway interface, then it must be on the data gateway's southbound network. This is because Crosswork Data Gateway implements Reverse Path Forwarding (RPF) checks and the source address of devices cannot be on the management or northbound networks if multiple NICs (2 or 3 NIC) are deployed.

Configuration prerequisites for new devices

Before you onboard the new devices, ensure that the devices are properly configured in order to be managed by the Cisco Crosswork Network Controller.

For SR-PM configurations, refer to the *Segment Routing Configuration* documentation specific to your platform and release. Configuration requirements may vary between platforms.

For configurations related to LLDP, CDP, and LAG protocols, see the *Set Up and Use Your Topology Map for Network Visualization* chapter in the [Cisco Crosswork Network Controller 7.1 Administration Guide](#). The link discovery process is closely related to the onboarding process, though it is not strictly required for onboarding. However, we recommend that you plan for link discovery as part of the onboarding workflow. This approach allows you to complete all necessary configuration work upfront, rather than addressing it incrementally. This is especially important if you want to leverage configuration templates. You can onboard devices without all the desired configurations initially and later push a standardized configuration to the devices. This ensures they are fully compatible with Crosswork Network Controller.

The following sections provide sample configurations for several protocols, including SNMP, NETCONF, SSH, gNMI, syslog and TELNET. Use them as a guide to configuring the devices that you plan to manage.



Note If you are using TELNET in your network environments, we recommend implementing security measures, such as firewall protections and ACLs to reduce any potential risks.

**Note**

- SNMPv2 and SNMPv3 (Auth/Priv) traps are supported.
- The SNMP EngineID generated or configured in the device should be unique in the network.
- For the credentials to work, SNMP users should be re-created if the SNMP EngineID is reconfigured in the device.
- In the sample configurations, *cdg_virtualIP* denotes the virtual IP address of the Data Gateway in a Data Gateway pool. The *cdg_virtualIP* varies for each pool.
- When devices are onboarded with *Sys Object ID* contact the Cisco Customer Experience team as the platform may not be certified by Cisco.

Configure Devices To Forward Events to Crosswork Network Controller

To ensure that the Crosswork Network Controller can receive events and notifications from devices, configure the devices to forward events to the Crosswork server. For most devices, this means you must configure the devices to forward SNMP traps and syslogs to the Data Gateway using its virtual IP as the receiver IP.

If you have a geo high availability deployment, configure devices to forward events to both Data Gateway on the primary and secondary data center.

**Note**

When you configure a Data Gateway pool with spare Data Gateway, failover is handled without changing the IP address that devices use for forwarding traffic:

- If a Data Gateway fails, the spare Data Gateway automatically inherits the IP address of the failed Data Gateway.
- If your configuration uses an FQDN, traffic continues to route without disruption even if a Data Gateway in the pool fails because the FQDN remains unchanged.

We recommend using a common configuration file for all your devices to allow Crosswork Network Controller to perform a reachability check and collect trap information.

For example, you can configure a device to forward events to the Crosswork Network Controller server using the **snmp-server host** command.

```
snmp-server host 192.168.90.135 traps version 2c public udp-port 1062
snmp-server community public RO
snmp-server community private RW
snmp-server traps snmp linkup
snmp-server traps snmp linkdown
```

To set the SNMP view:

```
snmp-server view { group name } include
```

Configure Devices for Pre-Onboarding Tasks

The following commands provide a sample pre-onboarding device configuration that sets the correct SNMPv2 and NETCONF configuration, and SSH and TELNET rate limits. The NETCONF setting is only needed if the device is MDT-capable.

```

logging console debugging
logging monitor debugging
telnet vrf default ipv4 server max-servers 100
telnet vrf default ipv6 server max-servers 100
crypto key generate rsa
  exec-timeout 0 0
  width 107
  length 37
  absolute-timeout 0
!
snmp-server community public RO
snmp-server community robot-demo2 RO
snmp-server ifindex persist
ntp
  server NTPServerIPAddress
!
ssh server v2
ssh server vrf default
ssh server netconf vrf default
ssh server logging
ssh server rate-limit 100
ssh server session-limit 100
!
netconf-yang agent
  ssh
!
netconf agent tty
!
xml agent tty
!

```

Configure SNMPv3 Devices

If you want to enable SNMPv3 data collection, repeat the SNMPv2 configuration commands in the previous section, and add the following commands:

```

snmp-server group grpauthpriv v3 priv notify vldefault
snmp-server user <user-ID> grpauthpriv v3 auth md5 password priv aes 128 password

```

Configure SNMPv2 and SNMPv3 traps

To configure the device to send SNMP traps, use the following commands:

For SNMP v2 traps:

```

snmp-server trap link ietf
snmp-server host cdg_virtualIP traps version 2c Community String udp-port 1062
snmp-server community Community String
snmp-server traps snmp linkup
snmp-server traps snmp linkdown

```

For SNMP v3 traps:

```

snmp-server trap link ietf
snmp-server host cdg_virtualIP traps version 3 Community String udp-port 1062
snmp-server community Community String
snmp-server traps snmp linkup
snmp-server traps snmp linkdown

```

Configure MDT sensor groups

```

telemetry model-driven
!
destination-group Crosswork

```

```

vrf mgmt
address-family ipv4 x.x.x.x port 9010
encoding self-describing-gpb
protocol tcp
!
sensor-group Crosswork
sensor-path Cisco-IOS-XR-infra-tc-oper:traffic-collector/afs/af/counters/tunnels/tunnel
!
subscription Crosswork
sensor-group-id Crosswork
destination-id Crosswork
!
!

```

Configure gNMI or gRPC

```

grpc
vrf mgmt
port 57500
no-tls
max-streams 128
max-streams-per-user 128
address-family dual
max-request-total 256
max-request-per-user 32
!

tpa
vrf mgmt
address-family ipv4
default-route mgmt
!
address-family ipv6
default-route mgmt
!
!
!

```

Configure required settings for Cisco IOS XR device operating system

Note that <SystemOwner> is a user-supplied variable.

```

snmp-server community community_name SystemOwner
snmp-server community community_name RO
snmp-server entityindex persist
snmp-server ifindex persist

logging cdg_virtualIP
logging on
logging buffered 307200-125000000

logging source-interface interface_name

logging trap informational
logging events level informational
logging events link-status
logging events link-status software-interfaces

no cli whitespace completion
domain ipv4 host server_name cdg_virtualIP

```

Set up VTY options:

```

line default
exec-timeout 10
session-limit 10
session-timeout 100
transport input ssh
transport output ssh
vty-pool default 0 99 line-template default

```

TELNET and SSH Settings:

```

telnet ipv4 server max-servers no-limit
telnet vrf default ipv4 server max-servers 100
ssh server v2
ssh server rate-limit 60
cinetd rate-limit 60

```

Configure the NetConf and XML agents:

```

xml agent tty
netconf agent tty

```

Monitor device with Virtual IP address :

```

ipv4 virtual address use-as-src-addr
ipv4 virtual address Virtual_IP_Address/Subnet_Mask

```

Enable CFM modeling:

```

snmp-server view all 1.3.111.2.802.1.1.8 included

```

For SNMPv2 only, configure the community string:

```

snmp-server community ReadonlyCommunityName RO SystemOwner

```

For SNMPv3 only, configure the following settings:

```

snmp-server user User Group v3 auth sha encrypted Password priv des56 encrypted
Password SystemOwner
snmp-server view Group 1.3.6 included
snmp-server view Group 1.0.8802.1.1.2 included
snmp-server group Group v3 priv notify Group read Group
snmp-server group Group v3 priv read vldefault write vldefault notify vldefault

```

Configure the following to improve the SNMP interface stats response time:

```

snmp-server ifmib stats cache

```

Configure SNMP traps for physical interfaces to ensure that link-down scenarios are captured:

```

snmp-server interface subset 2 regular-expression Forty*
notification linkupdown
!
snmp-server interface subset 3 regular-expression Ten*
notification linkupdown
!
snmp-server interface subset 1 regular-expression Hun*
notification linkupdown
!
snmp-server interface subset 1 regular-expression TwoHun*
notification linkupdown
!
snmp-server interface subset 1 regular-expression FourHun*
notification linkupdown

```

Enable SNMP entity field replaceable unit (FRU) control traps:

```

snmp-server traps fru-ctrl

```


Syslogs are used by Crosswork Network Controller for alarm and event management. NTP settings ensure that Crosswork Network Controller receives the correct timestamps for events. To configure syslogs on the device, add the following settings:

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server NTP_Server
logging facility local7
logging cdg_virtualIP vrf name
```

Configure Required Settings for Cisco IOS and IOS-XE Device Operating System

```
snmp-server host cdg_virtualIP
snmp-server community public-cmtty RO
snmp-server community private-cmtty RW
snmp-server ifindex persist
```

```
logging cdg_virtualIP
logging on
logging buffered 64000 informational
```

```
logging source-interface interface_name
logging trap informational
logging event link-status default
```

Disable domain lookups to avoid delay in TELNET/ SSH command response:

```
no ip domain-lookup
```

Enable SSH

```
crypto key generate rsa
ip ssh rsa keypair-name keypair-name
crypto key generate rsa usage-keys label key-label modulus modulus-size
ip ssh version [1 | 2]
```

Setup VTY options:

```
line vty <number of vty>
exec-timeout
session-timeout
transport input ssh (required only if ssh is used)
transport output ssh (required only if ssh is used)
```

For SNMPv2 only, configure the community string:

```
snmp-server community ReadonlyCommunityName RO
```

For SNMPv3 only, configure the following settings:

```
snmp-server user User Group v3 auth sha Password priv des Password
snmp-server view Group 1.3.6 included
snmp-server view Group 1.0.8802.1.1.2 included
snmp-server group Group v3 priv notify Group read Group
```

```
snmp-server group Group v3 priv read vldefault write vldefault notify vldefault
snmp-server group Group v3 priv
snmp-server group Group v3 priv notify crosswork read crosswork
```

Configure the cache settings at a global level to improve the SNMP interface response time using the configuration:

```
snmp-server cache
```

Syslogs are used by the Crosswork Network Controller for alarm and event management. NTP settings ensure that Crosswork Network Controller receives the correct timestamps for events. To configure syslogs on the device, add the following settings:

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server NTP_Server
update-calendar
logging facility local7
logging cdg_virtualIP vrf default severity info [port default]
```

Configure Required Settings for Nexus Operating System

The following commands provide a sample pre-onboarding device configuration for Nexus devices that sets the correct SNMPv2 and NETCONF configuration, and SSH rate limits. The NETCONF setting is only needed if the device is MDT-capable.

```
logging console 7
logging monitor 7
!
ntp server <NTPServerIPAddress>
ntp server <10.10.10.11> use-vrf <management or configured vrf>.
!
ssh idle-timeout
logging level security
!
feature netconf
feature openconfig
!
snmp-server user <User> auth md5 <String> priv aes-256 <String>
!
snmp-server enable traps link linkDown
snmp-server enable traps link linkUp

snmp-server community community_name RO
!
logging server <IP>
logging source-interface interface_name
logging event link-status default
logging event link-status enable
```

- User privileges can be configured as either `network-admin` or `network-operator`
- In Nexus OS, the `ifIndex` for an interface is persistent.
- To retrieve the SNMP interface index (ifmib index), use the following command:

```
show interface snmp-index
```

- To configure logging for link status or trunk status changes, use the following command in configuration mode:

```
logging event link-status default
logging event link-status enable
```

Set up VTY options:

```
line vty
exec-timeout 10
session-limit 10
```

Forward events to the Crosswork Network Controller server using the `snmp-server host` command:

```
snmp-server host <192.168.90.135> traps version 2c public udp-port 1062
snmp-server community public RO
snmp-server community private RW
snmp-server enable traps link linkDown
snmp-server enable traps link linkUp
```

Configure the following to improve the SNMP interface stats response time:

```
snmp-server counter cache enable
snmp-server counter cache timeout <1-3600>
```

Enable SNMP entity field replaceable unit (FRU) control traps:

```
snmp-server enable traps entity
```

Syslogs are used by Crosswork Network Controller for alarm and event management. NTP settings ensure that Crosswork Network Controller receives the correct timestamps for events. To configure syslogs on the device, add the following settings:

```
clock timezone TimeZone
ntp server NTP_Server
logging level ntp 7
logging server <IP> use-vrf <vrf name>
```

The `service timestamps` feature is not supported in Nexus OS. To set the logging level for a specific facility (e.g., NTP), use the following command:

```
logging level ntp 7
```

Configure IGP Protocol to Generate the Router ID

Based on your device configuration, use the appropriate sample configuration for either ISIS or OSPF. For detailed configurations, see the platform-specific documentation.

ISIS router ID:

```
router isis 1
net 49.0010.0100.0004.00
distribute link-state instance-id 100
log adjacency changes
affinity-map top bit-position 101
affinity-map bottom bit-position 102
address-family ipv4 unicast
metric-style wide
mpls traffic-eng level-2-only
mpls traffic-eng router-id Loopback0
router-id 198.19.1.4
segment-routing mpls
#show mpls traffic-eng igp-areas
Fri Oct 4 03:53:16.117 UTC
```

MPLS-TE IGP Areas

```
Global router-id:          198.19.1.4
Global optical router-id: Not available
```

IS-IS 1

```
IGP ID:                    0010.0100.0004
TE router ID configured:   198.19.1.4
                        in use: 198.19.1.4
Connection:                up
```

OSPF router ID:

```
router ospf
  distribute link-state instance-id 6
  router-id 1.1.1.20
  segment-routing global-block 16000 17999
  segment-routing forwarding mpls
  segment-routing sr-prefer
#show mpls traffic-eng igp-areas
Fri Oct  4 03:53:28.091 UTC
```

MPLS-TE IGP Areas

```
Global router-id:      1.1.1.20
Global optical router-id: Not available
```

OSPF

```
IGP ID:                1.1.1.20
TE router ID configured: 1.1.1.20
                        in use:  1.1.1.20
Connection:            up
```

Sample Configuration for Cisco NSO Devices

When using Cisco Network Services Orchestrator (Cisco NSO) as a provider to configure devices managed by Cisco Crosswork, make sure that the Cisco NSO device configurations observe the guidelines in the following example.

This example shows a Cisco NSO configuration that uses the hostname as the device ID. If you are using a CSV file to import devices, use **ROBOT_PROVDEVKEY_HOST_NAME** as the enum value for the `provider_node_key` field. The example hostname **RouterFremont** used here must match the hostname for the device in the CSV file.

```
configure
set devices device RouterFremont address 198.18.1.11 port 22
```

In the following example, we are creating an authgroup called "cisco", with a remote name and password of "cisco". Next, we are setting all the devices that have a name starting with "Router" to a device type of "netconf" using the `ned-id` "cisco-iosxr-nc-6.6". Finally, we are assigning all of the devices with a name starting with "Router" to the "cisco" authgroup. Edit these settings to match your environment:

```
set devices authgroups group cisco default-map remote-name cisco remote-password cisco
set devices device Router* device-type netconf ned-id cisco-iosxr-nc-6.6
set devices device Router* authgroup cisco
```

The following CLI commands unlock and retrieve the SSH keys from all of the devices. Cisco NSO synchronizes itself with the devices by uploading each device's current configuration and then storing the present configuration. It is important to use these commands to ensure that the devices, Cisco NSO, and your Cisco Crosswork applications are starting from a common configuration:

```
set devices device Router* state admin-state unlocked
request devices device Router* ssh fetch-host-keys
request devices device Router* sync-from
```

commit

Add devices through the UI

Follow the steps below to add devices one by one, using the user interface. This method is mostly used when adding a few devices only.

Procedure

- Step 1** From the main menu, choose **Device Management > Network Devices**.
- Step 2** Click .
- Step 3** Enter the values for the new device, as listed in [Table 1: Add new device Window \(*=Required\)](#), on page 11.
- Step 4** Click **Save**. The **Save** button is disabled until all mandatory fields are completed.
- Step 5** (Optional) Repeat these steps to add more devices.

Attention

The **Device type** field is deprecated in Crosswork Network Controller version 7.1.

Table 1: Add new device Window (*=Required)

Field	Description
Device info	
* Admin state	The management state of the device. Options are • UNMANAGED—Crosswork Network Controller is not monitoring the device. • DOWN—The device is being managed and is down. • UP—The device is being managed and is up.
* Reachability check	Determines whether Crosswork Network Controller performs reachability checks on the device. Options are: • ENABLE (In CSV: REACH_CHECK_ENABLE)—Checks for reachability and then updates the Reachability State in the user interface automatically. • DISABLE (In CSV: REACH_CHECK_DISABLE)—The device reachability check is disabled. Cisco recommends that you always set this to ENABLE. This field is optional if Configured State is marked as UNMANAGED.
Serial number	Serial number for the device.
Host name	The hostname of the device.

Field	Description
Tags	The available tags to assign to the device for identification and grouping purposes. Use device tags to group devices for monitoring, and to provide additional information that might be of interest to other users, such as the device's physical location or its administrator's email ID.
Software type	Software type of the device. Note Some third-party vendor devices require a specific string to be entered as part of the Software Type field. These are the required strings for different vendors: • Juniper devices: JUNOS • Huawei devices: VRP • Nokia devices: TIMOS
Software version	Software version of the operating system.
UUID	Universally unique identifier (UUID) for the device.
MAC address	MAC address of the device.
Inventory ID	Inventory ID value for the device. The value can contain a maximum of 128 alphanumeric characters, and can include dots (.), underscores ("_"), colons (":"), or hyphens ("-"). No other special characters are allowed. Choose the device host name or an easily identifiable name for Inventory ID as this will be used to sync the device to Crosswork Network Controller with the Inventory ID used as the device name.
Product type	Product type of the device.
Syslog format	The format in which syslog events received from the device should be parsed by the syslog collector. The options are: • UNKNOWN - Choose this option if you are uncertain or if you do not want any parsing to be done by the syslog collector. The Syslog Collection Job output contains syslog events as received from the device. • RFC5424 - Choose this option to parse syslog events received from the device in RFC5424 format. • RFC3164 - Choose this option to parse syslog events received from the device in RFC3164 format.
CLI cache enabled	Click the checkbox if you wish to enable CLI cache.
Connectivity details	
* Credential Profile	The name of the credential profile to be used to access the device for data collection and configuration changes. Select the profile for which the device is configured from the dropdown list. For example: ns023 or srpce123 . This field is optional if Administration State is marked as UNMANAGED .

Field	Description
Protocol	The connectivity protocols used by the device. Choices are: SNMP, NETCONF, TELNET, HTTP, HTTPS, GNMI, TL1, and GRPC. Note Toggle the Secure Connection slider to secure the GNMI protocol that you have selected. In this documentation, the secured gNMI protocol is referred to as GNMI_Secure. To add more connectivity protocols for this device, click  at the end of the first row in the Connectivity Details panel. To delete a protocol you have entered, click  shown next to that row in the panel. You can enter as many sets of connectivity details as you want, including multiple sets for the same protocol. Enter details for at least SSH and SNMP. If you do not configure SNMP, the device will not be added. If you want to manage the device (or you are managing XR devices), you must enter details for NETCONF. TELNET connectivity is optional.
* IP Address / Subnet Mask	Enter the device's IP address (IPv4 or IPv6) and subnet mask. Note If you have multiple protocols with the same IP address and subnet mask, you can instruct Crosswork Network Controller to autofill the details in the other fields. Note Please ensure that the subnets chosen for the IP networks (including devices and destinations) do not have overlapping address space (subnets/supernets) as it may result in unpredictable connectivity issues.
* Port	The port used for this connectivity protocol. For each protocol enabled on the device, the default port is automatically provided. This default value works correctly in most cases. However, if your network uses non-standard ports, you must update the port settings to match the ones configured in your network. GNMI and GNMI_SECURE: When using gNMI the value is not automatically populated. You must instead enter the value configured on your network devices. The port values range between 57344 to 57999. Ensure that the port number you enter here matches with the port number configured on the device.
Timeout	The elapsed time (in seconds) before communication attempts using this protocol times out. The default value is 30 seconds. While the default value is 30 seconds, a minimum timeout value of 90 seconds is recommended for XE devices using NETCONF. For all other devices and protocols, the recommended minimum timeout value is 60 seconds.
Encoding Type	This field is only applicable for GNMI and GNMI_SECURE protocols. The options are JSON, BYTES, PROTO, ASCII, and JSON IETF. Based on device capability, only one encoding format is supported at a time in a device.

Field	Description
Encryption	This field is applicable only to the SNMP protocol. From the drop-down list, choose the appropriate SNMPv3 protocol supported by the device. The default value is NONE. The drop-down list presents several Advanced Encryption Standard (AES) options, including Counter mode (CTR), Galois/Counter mode (GCM), and Cipher Block Chaining mode (CBC), each supporting various key lengths (128-bit, 192-bit, and 256-bit). The credential profile supports the generic privacy types such as AES-192 and AES-256. For Cisco devices, these are specified as CiscoAES192 and CiscoAES256 protocols. On Cisco devices, the protocols appear as aes256-ctr, aes256-gcm@openssh.com, aes256-cbc, aes192-ctr, and aes192-cbc. To ensure compatibility with Crosswork Network Controller polling, Cisco devices must use these updated protocol variations. On non-Cisco devices, select the encryption that the device supports or use NONE if the device does not use encryption for SNMP.
Trap source IP	This field is available only when the SNMP protocol is selected. Use this field to specify the source IP address that the device will use to report SNMP traps if it differs from the default management interface IP address. For consistent trap collection, ensure that the IP address entered in the Trap source IP field matches the <code>trap-source</code> parameter configured on the network device to avoid any issues with SNMP trap handling. Note - If the Trap source IP field is not specified, Crosswork defaults to using the management interface IP address. For devices added via CSV or API, this field also defaults to the management interface IP address unless explicitly specified. - Ensure that the trap source uses the same IP stack (IPv4 or IPv6) as the device connectivity protocol to maintain consistent communication and avoid mismatches.
SNMP Disable Trap Check	This check box appears when the protocol field is set to SNMP. Selecting this check box disables the SNMPv2 community string validation between the network device and Data Gateway. Disabling the SNMPv2 community string validation might be a requirement when you want to use a different community string for traps than the one in the credential profile.
* Capability	The capabilities that allow collection of device data and that are configured on the device. You must select at least SNMP as this is a required capability. The device will not be onboarded if SNMP is not configured. Other options are YANG_MDT, YANG_CLI, TL1, and GNMI. The capabilities that you select will depend on the device software type and version. Note - For devices with MDT capability, do not select YANG_MDT at this stage. - To enable Crosswork Network Controller to receive the syslog-based data, select YANG_CLI.
Providers and access	
Provide the provider information.	
Provider family	Provider type used for topology computation. Choose a provider from the list.

Field	Description
Provider name	Provider name used for topology computation. Choose a provider from the list. Note For Cisco NSO LSA deployment, select the resource-facing service (RFS) node to which you want to assign the device.
Credential	The credential profile used for the provider. This field is read-only and is autopopulated based on the provider you select.
Device key	The hostname used to link this device record to its corresponding record on the provider. This is typically the device's full hostname, including the domain.
Routing info	
ISIS system ID	The device's IS-IS system ID. This ID identifies the router in an IS-IS topology, and is required for SR-PCE integration. This field is a configurable parameter, and cannot be autodiscovered by Crosswork Network Controller.
OSPF router ID	The device's OSPF router ID. This ID identifies the router in an OSPF topology, and is required for SR-PCE integration. This field is a configurable parameter, and cannot be autodiscovered by Crosswork Network Controller.
*TE router ID	The traffic engineering router ID for the respective IGP. Note For visualizing L3 links in topology, devices should be onboarded to Crosswork Network Controller with the TE Router ID field populated.
IPv6 router ID	IPv6 router ID for the device. This field is a configurable parameter, and cannot be autodiscovered by Crosswork Network Controller.
Streaming telemetry config	
VRF	Name of the VRF within which Model Driven Telemetry (MDT) traffic is routed.
Source interface	The range of loopback address for the device type. This field is optional. However, we recommend specifying the loopback associated with the VRF by using the selector in the adjacent box. Note This field can be edited only when the device is in a DOWN or UNMANAGED state.
Opt out MDT config	When enabled, Crosswork Network Controller will not push telemetry configuration to the device via NSO. The default setting state is Disabled (which allows Crosswork Network Controller to push telemetry configuration to the device via NSO). The device must be in ADMIN DOWN state to toggle this setting. Any out of band configuration setup must be cleared before moving the setting from Enabled to Disabled.
Location	
Provide location information if you want to see your devices on the geographical map.	

Field	Description
Building	Enter the name of the building.
Street	Enter the name of the street.
City	Enter the name of the city.
State	Enter the name of the state.
Country	Enter the name of the country.
Region	Enter the name of the region.
Zip	Enter the zip code of the region.
Longitude	Longitude value is required so that the geographical map can present the correct geographical location of the device and its links to other devices. Enter the longitude in Decimal Degrees (DD) format.
Latitude	Latitude value is required so that the geographical map can present the correct geographical location of the device and its links to other devices. Enter the latitude in Decimal Degrees (DD) format.
Altitude	The altitude at which the device is located. If you do not know the altitude or do not wish to track it, you can leave this field blank. Alternatively, you may use this field to specify the floor of the building where the device is installed. The value must be a numeric entry.

Add devices by importing from CSV file

To add multiple devices to the Crosswork Network Controller, you can create and import a CSV file. This approach allows you to add several devices at once, avoiding the need to add each device individually.

Understanding the behavior of CSV import:

- Importing devices from a CSV file adds the devices that are not already present in the database.
- You can use more than one CSV file for importing devices. However, ensure that duplicate devices are not included in the new CSV file.
- If a device in the CSV matches an existing device's **Inventory key type** field (excluding the UUID, which is system generated), the existing record is overwritten with data from the CSV.
- If certain fields require unique values such as `VRF`, `router loopback`, or `loopback ID`, you must explicitly include these values in the CSV. This helps prevent any unintended configurations.
- To avoid accidental data loss, we recommend to export a backup copy of your current device list before performing an import.

Handling non-required fields: For fields that are not required in the CSV, the following can occur:

- The field may be left blank.

- The field may be set to a default value.
- The field may be populated with values retrieved from the device once communication is established, such as model, type, or software version.

Before adding devices from a CSV file, we recommend that you:

- Add a few devices using the Crosswork Network Controller UI and confirm they are functioning properly.
- Export the current device configuration to generate a CSV file. This serves as a template tailored to your environment.
- Use this exported CSV file as a baseline for adding additional devices to ensure compatibility and reduce errors.



Attention

- You cannot directly import a file that was just exported from the Crosswork Network Controller UI without making edits to it first.
- If there are any errors in the import file, they are not reported all at once. Instead, the system identifies and displays errors one at a time, starting with the first error it encounters.
- Importing devices using CSV or API methods will fail if the CSV file contains data gateway information. To successfully import the devices, ensure that the Crosswork Data Gateway and UUID columns in the CSV file are empty before you proceed.
- The CSV file used to import devices differs between cluster deployments and single VM deployments.

To add devices by importing from CSV file, follow these steps:

Procedure

Step 1 From the main menu, choose **Device Management > Network Devices**. The **Network Devices** tab is displayed by default.

Step 2 Click  to open the **Import CSV File** dialog box.

Step 3 If you have not already created a device CSV file to import:

- Click the **Download sample 'Device Management template (*.csv)' file** link and save the CSV file template to a local storage resource.
- Open the template using your preferred tool. Begin adding rows to the file, one row for each device.

Note

- Ensure that the TE router ID value for each device is populated. This value uniquely identifies the device within the topology as provided by SR-PCE.
- The CSV files created on a Windows machine should contain a new line (marked with a 'newline' character) for the file to be processed as expected. Any newline created using the "carriage return" option will not work.

Use a semicolon to separate multiple entries in the same field. Use two semicolons with no space between them to indicate that you are leaving the field blank. When you separate multiple entries with semicolons, remember that the order in which you enter values in each field is important. For example, if you enter **SSH ; SNMP ; NETCONF** in the

Connectivity Type field and you enter **22 ; 161 ; 830** in the **Connectivity Port** field, the order of entry determines the mapping between the two fields:

- SSH: port 22
- SNMP: port 161
- NETCONF: port 830

- c) Delete the sample data rows before saving the file, or they will be imported along with your data. You can keep the column header row, as it is ignored during the import process.
- d) Save the new CSV file.

Step 4 Click **Browse** to navigate to the CSV file you created in the previous steps and then click **Open** to select it.

Step 5 With the CSV file selected, click **Import** and wait for the import to complete.

Step 6 Resolve any errors and confirm device reachability.

It is normal for devices to show as unreachable or not operational when they are first imported. However, if they are still displayed as unreachable or not operational after 30 minutes, there may be an issue that needs to be investigated. To investigate, select **Device Management > Job History** and click on any error icon you see in the **Status** column. Common issues include failure to ensure the associated credential profile contains the correct credentials. You can test this by opening a terminal window on the server and then trying to access the device using the protocol and credentials specified in the associated credential profile.

Step 7 Once you have successfully onboarded the devices, you must map them to a data gateway instance.

Export Device Information to a CSV File

Exporting the device list is a handy way to keep a record of all devices in the system at one time. You can also edit the CSV file as needed, and re-import it to overwrite existing device data.

Procedure

Step 1 From the main menu, choose **Device Management > Network Devices**. The **Network Devices** tab is displayed by default.

Step 2 (Optional) Filter the device list as needed.

Step 3 Check the check boxes for the devices you want to export.

Step 4 Click . Your browser will prompt you to select a path and the file name to use when saving the CSV file, or to open it immediately.



CHAPTER 2

Zero Touch Provisioning

This section contains the following topics:

- [Zero Touch Provisioning Concepts, on page 19](#)
- [ZTP Setup Workflow, on page 28](#)
- [ZTP Provisioning Workflow, on page 59](#)
- [Reconfigure Onboarded ZTP Devices, on page 84](#)
- [Retire or Replace Devices Onboarded with ZTP, on page 84](#)
- [ZTP Asset Housekeeping, on page 85](#)
- [Troubleshoot ZTP Issues, on page 85](#)

Zero Touch Provisioning Concepts

The ZTP allows you to ship factory-fresh devices to a branch office or remote location and provision them when physically installed. Local operators can cable these devices to the network without installing an image or the need to fully configure them. To use ZTP, you first establish an entry for each device in the DHCP server and in ZTP. You can then activate ZTP processing by connecting the device to the network and powering it on or reloading it. The device will download and apply a software image and configurations to the device automatically (you can also apply configurations only). When configured, ZTP onboards the new device to the Cisco Crosswork device inventory. You can then use other Crosswork Network Controller functionalities to monitor and manage the device.

ZTP uses the following basic terms and concepts:

- **Classic ZTP:** A process to download and apply software and configuration files to devices. It uses iPXE firmware and HTTP to boot the device and perform downloads. As it does not use secure communications, it is not suitable for use over public networks.
- **Secure ZTP:** A secure process to download and apply software images and configuration files to devices. It uses secure transport protocols and certificates to verify devices and perform downloads, which makes it more suitable for use over public networks.
- **PnP ZTP:** A secure process to download and apply software images and configuration files to Cisco IOS-XE devices. It uses Cisco Plug and Play (Cisco PnP) to verify devices and perform downloads over a secure, encrypted channel. It offers much the same level of security as Secure ZTP, but only for Cisco IOS-XE devices.
- **Evaluation License Countdown:** You can use ZTP to onboard devices without licenses for 90 days. After this evaluation period expires, you cannot use ZTP to onboard new devices until you purchase and

install a license bundle with enough capacity to cover all prior devices onboarded using ZTP, as well as your projected future needs.

- **Image file:** A binary software image file, used to install the network operating system on a device. For Cisco devices, these files are the supported versions of Cisco IOS images. Software image installation is an optional part of ZTP processing. When configured to do so, the ZTP process downloads the image from the Crosswork Network Controller to the device, and the device installs it. If you must also install SMUs, ZTP can install them as part of configuration processing in Classic and Secure ZTP (SMUs are not supported in PnP ZTP).
- **Cisco Plug and Play (Cisco PnP):** Cisco's proprietary ZTP, bundled in most IOS software images. Cisco PnP uses a software PnP agent and a PnP server to distribute images and configurations to devices. To ensure that communications are secure, the server and agent communicate using HTTPS.
- **Configuration file:** A file used to set the operating parameters of the newly imaged or re-imaged device. Depending on the ZTP mode you plan to use, the file may be a Python script, Linux shell script, or a sequence of Cisco IOS CLI commands stored as ASCII text (not all of these are supported in all ZTP modes). The ZTP process downloads the configuration file to the newly imaged device, which then executes it. The ZTP process requires a single configuration file. The secure ZTP process supports up to three different configuration files, which are applied during onboarding in the following order:
 - **Pre-configuration:** A preconfiguration file is a file used to set the initial operating parameters of a newly imaged or re-imaged device. The preconfiguration file is essential for automating the setup process, allowing the device to be configured without manual intervention.
 - **Day-zero:** A day-zero file is a configuration file that is used to set up a newly imaged or re-imaged device right from the start, often referred to as "day zero." The day-zero file is crucial for automating the initial configuration process, enabling the device to be operational without manual setup.
 - **Post-configuration:** A post-configuration file is used to apply additional settings and configurations to a device after the initial setup has been completed. This file can include advanced configurations, updates, or custom scripts that further refine the device's operation. The post-configuration file ensures that the device meets specific operational requirements and is fully optimized for its intended use.

The pre-configuration and post-configuration may have references to the day-zero configuration file, which indicates that the pre and post- configuration files require the UUID from the day-zero file.

- **Configuration handling method:** A Secure ZTP user option. It allows you to specify whether you want to merge a new configuration into the existing device configuration or to overwrite it.
- **Credential profile:** Collections of passwords and community strings that are used to access devices via SNMP, SSH, HTTP, and other network protocols. Crosswork Network Controller uses credential profiles to access your devices, automating device access. All credential profiles store passwords and community strings in encrypted format.
- **Bootfile name:** The explicit path to and name of a software image that is stored in the ZTP repository. For each device you plan to onboard using ZTP, specify the bootfile name as part of the device configuration in DHCP.
- **HTTPS/TLS:** Hypertext Transport Protocol Secure (HTTPS) is a secure form of the HTTP protocol. It wraps an encrypted layer around HTTP. This layer is the Transport Layer Security (TLS) (formerly Secure Sockets Layer, or SSL).

- **iPXE:** The [open-source boot firmware iPXE](#) is the popular implementation of the Preboot eXecution Environment (PXE) client firmware and boot loader. iPXE allows devices without built-in PXE support to boot from the network. The iPXE boot process is a normal part of Classic ZTP processing.
- **Owner Certificate:** The Certificate Authority (CA)-signed end-entity certificate for your organization, which binds a public key to your organization. You install Owner Certificates on your devices as part of Secure ZTP processing.
- **Ownership Voucher:** The Ownership Voucher is used to identify the owner of the device by verifying the Owner Certificate that is stored in the device. Cisco supplies Ownership Vouchers in response to requests from your organization. For information on how to get the Ownership Vouchers from Cisco, see [Load Ownership Vouchers, on page 50](#).
- **Cisco PnP agent:** A software agent embedded in Cisco IOS-XE devices. Whenever a device that supports the PnP agent powers up for the first time without a startup configuration file, the agent tries to find a Cisco PnP server. The agent can use various means to discover the server's IP address, including DHCP and DNS.
- **Cisco PnP server:** A central server for managing and distributing software images and configurations to Cisco PnP-enabled devices. ZTP has an embedded PnP server, which is configured to communicate with PnP agents using HTTPS.
- **SUDI:** The [Secure Unique Device Identifier \(SUDI\)](#) is a certificate with an associated key pair. The SUDI contains the device's product identifier and serial number. Cisco inserts the SUDI and key pair in the device hardware Trust Anchor module (TAM) during manufacturing, giving the device an immutable identity. During Secure ZTP processing, the back-end system challenges the device to validate its identity. The router responds using its SUDI-based identity. This exchange, and the TAM encryption services, permit the back-end system to provide encrypted image and configuration files. Only the validated router can open these encrypted files, ensuring confidentiality in transit over public networks.
- **SUDI Root CA certificates:** A root authority certificate for SUDIs, issued and signed by a Certificate Authority (CA), used to authenticate subordinate SUDI certificates.
- **UUID:** The Universal Unique Identifier (UUID) identifies a device when it is onboarded.
- **Image ID:** The image ID uniquely identifies an image file that you have uploaded to Crosswork Network Controller. You use the image ID of the software image file in the DHCP bootfile URL with Classic and Secure ZTP.
- **ZTP asset:** ZTP requires access to several types of files and information in order to onboard new devices. We refer to these files and information collectively as "ZTP assets." You load these assets as part of the ZTP setup, before initiating ZTP processing.
- **ZTP profile:** Crosswork Network Controller storage construct that combines (normally) one image and one configuration into a single unit. Crosswork Network Controller uses ZTP profiles to automate imaging and configuration processes. Using ZTP profiles is optional, but we recommended them. They are an easy way to organize ZTP images and configurations around device families, classes, and roles, and help maintain consistency.
- **ZTP repository:** The location where the Crosswork Network Controller stores image and configuration files.

ZTP and Evaluation Licenses

The ZTP licensing follows a consumption-based model with licenses that are sold in blocks. To regain the ability to onboard devices using ZTP, you must install a license block that covers both the number of devices you onboarded during the trial period as well as the new devices you expect to onboard with ZTP in the future. For example: If you onboard 10 devices during the trial and then install a license bundle for 10 devices on day 91, you have no licenses that are left to use, and must install at least one more license block before onboarding another device. You can add more license blocks as needed. Operators should monitor license consumption to avoid running out of licenses unexpectedly. To see how many licenses you have used and are still available, check [Cisco Smart Licensing site](#).

Your onboarded ZTP devices are always associated with either:

- A serial number, or
- For IOS-XR devices: The values of the Option 82 location ID attributes (remote ID and circuit ID).

Serial numbers and location IDs form an "allowed" list. ZTP uses this list when deciding to onboard a device and assign it a license. If you delete an onboarded ZTP device from inventory, and then onboard it again later, use the same serial number or location ID. If you use a different serial number or location ID, you may consume an extra license. The current release provides no workaround for this scenario. In any case, you can't have two different ZTP devices with the same serial number or location ID active at the same time.

Platform Support for ZTP

For the most accurate and up-to-date list of hardware and software versions that Classic ZTP, Secure ZTP, and PNP ZTP supports, refer to the [Cisco Crosswork Network Controller Essentials Supported Devices](#).



Important ZTP does not support third-party devices.

Provisioning Support for Third-Party Devices

Secure ZTP supports provisioning for third-party devices only if the third-party devices:

- Are 100 percent compliant with the Secure ZTP [RFC 8572](https://tools.ietf.org/html/rfc8572) (<https://tools.ietf.org/html/rfc8572>).
- Match the Cisco format guidelines for serial numbers in device certificates and ownership vouchers. See [Secure ZTP: Guidelines for Third-Party Device Certificates and Ownership Vouchers, on page 22](#).

Secure ZTP: Guidelines for Third-Party Device Certificates and Ownership Vouchers

Secure ZTP processing for any device starts with a successful HTTPS/TLS handshake between the device and Cisco Crosswork. After the handshake, Secure ZTP must extract a serial number from the device certificate. Secure ZTP then validates the extracted serial number against its internal "allowed" list of serial numbers. You create the allowed list by uploading device serial numbers to Cisco Crosswork. A similar serial-number validation step occurs later, when Crosswork uses ownership vouchers to validate downloads.

Unlike Cisco IOS-XR devices, the format of the serial number in third-party vendors' device certificates is not standardized across vendors. Typically, a third-party vendor's device certificate has a Subject field or section. The `Subject` contains multiple key-value pairs that the vendor decides upon. One of the keys is usually `serialNumber`. This key's value contains the actual device serial number as a string, which is preceded by the

string `SN:`. For example: Let's suppose that the third-party device certificate's Subject section contains the following key and value: `serialNumber = PID:NCS-5501 SN:FOC2331R0CW`. Secure ZTP will take the value after the `SN:` string and attempt to match that to one of the serial numbers in the allowed list.

If the third-party vendor's device certificate has a different format, validation failures can occur. The degree of failure depends on the degree of difference. The vendor certificate may not match this format at all. The certificate's `Subject` field may not contain a `serialNumber` key with a value that contains the `SN:` string. In this case, Secure ZTP processing falls back to using the whole string value of the `serialNumber` key (if present) as the device serial number. It will then try to match that value to one in the allowed list of serial numbers. These two methods – string matching and the fallback – are the only means Secure ZTP has for determining the third-party device's serial number. If the vendor certificate differs from this expectation, Secure ZTP is unable to validate the device.

Secure ZTP has similar format expectations for ownership vouchers (OVs). Cisco tools generate ownership vouchers with filenames in the format `SerialNumber.vcj`, where `SerialNumber` is the device's serial number.

Secure ZTP extracts the serial number from the filename and then attempts to match it to one in the allowed list. For multivendor support, we assume that third-party vendor tools generate OV files with file names in the same format. If this expectation isn't met, validation fails.

ZTP Implementation Decisions

As a best practice, always choose the most secure implementation that is supported by your devices. That said, ZTP offers a range of implementation choices and cost vs. benefit tradeoffs worth considering in advance:

- **When to Use Classic ZTP:** Classic ZTP is easier to implement than Secure ZTP. It needs no Pinned Domain Certificate (PDC), owner certificates, or ownership vouchers. It's less subject to processing errors, as device and server verification is less stringent and setup is less complex. It's your only choice if your Cisco devices run IOS-XR versions earlier than 7.3.1, as Secure and PnP ZTP are not supported on earlier versions of the software. Although Classic ZTP includes a device serial-number check, it remains unsecured at the transport layer. It's not recommended if routes to your remote devices cross a metro or otherwise unsecured network.
- **When to Use Secure ZTP:** Use Secure ZTP when:
 - Your ZTP traffic must traverse unsecured public networks.
 - Your Cisco IOS-XR devices support Secure ZTP and are at the required software level (see [#unique_13 unique_13_Connect_42_section_fdw_ybm_3vb](#)).

The additional security that Secure ZTP provides requires a more complex setup than either Classic or PnP ZTP. This complexity can make configuration error-prone if you're new to the setup tasks. Secure ZTP setup also requires a PDC, owner certificates and ownership vouchers from Cisco.

Consider using Secure ZTP if your devices are from third-party manufacturers; Classic and PnP ZTP don't support third-party hardware. Third-party devices and their software must be 100 percent compliant with RFCs [8572](#) and [8366](#). Device certificates for third-party devices must contain the device serial number. Third-party ownership vouchers must be in a format that uses the device serial number as the filename. Cisco doesn't guarantee Secure ZTP compatibility with all third-party devices. For more details on third-party device support, see [Platform Support for ZTP, on page 22](#).

- **When to Use PnP ZTP:** Use PnP ZTP when you want a secure provisioning setup for Cisco IOS-XE devices that support the Cisco PnP protocol. PnP ZTP is less complicated to set up than Secure ZTP, but only slightly more complicated than Classic ZTP.

- **When to Use ZTP With Imaged Devices:** You do not have to specify a software image when using any of the ZTP modes. This feature allows you the option of shipping to your remote location one or more devices on which you have already installed a software image. Later, connect to these devices and trigger the ZTP processing remotely. You can then apply:

- A configuration file
- One or more images or SMUs, with more configurations.

- **How ZTP processes support script execution:** Secure ZTP offers more flexibility with compatible devices because it offers pre-configuration, day-zero, and post-configuration script execution capability. While both Classic and Secure ZTP modes can chain configuration files, Classic ZTP's ability to execute additional scripts is limited to the support for script execution allowed on specific devices. PnP ZTP can only execute CLI commands, which don't allow for script execution.

In all cases, the result is to onboard the device. Once onboarded to Crosswork Network Controller, you want to avoid using ZTP to configure the device again (see [Reconfigure Onboarded ZTP Devices, on page 84](#) for details).

- **Organize Your Configurations:** Keep your configurations as consistent as possible across devices. Start by ensuring that all devices from the same device family and with similar roles have the same or similar basic configurations.

How you define the role that a device plays depends on your organization, its operational practices, and the complexity of your network environment. For example: Suppose that your organization is a financial services enterprise. It has three types of branches: Sidewalk ATMs, retail branches open during standard business hours, and private trading offices. You could define three sets of basic profiles covering all the devices at each type of branch. You can map your configuration files to each of these profiles.

Another method of enforcing consistency is to develop basic script configurations for similar types of devices, then use the script logic to call, or chain, other scripts for devices with special roles. If you're using Classic ZTP, the script is in the specified configuration file. To extend our example, that script would apply a common configuration, then download and apply other scripts depending on the branch type. If using Secure ZTP, you have even more flexibility, as you can specify pre-configuration and post-configuration scripts in addition to the day-zero configuration script.

ZTP Processing Logic

ZTP processing differs depending on the Classic ZTP, Secure ZTP, or PnP ZTP implementation. Following are details on each step of ZTP processing for each ZTP mode.

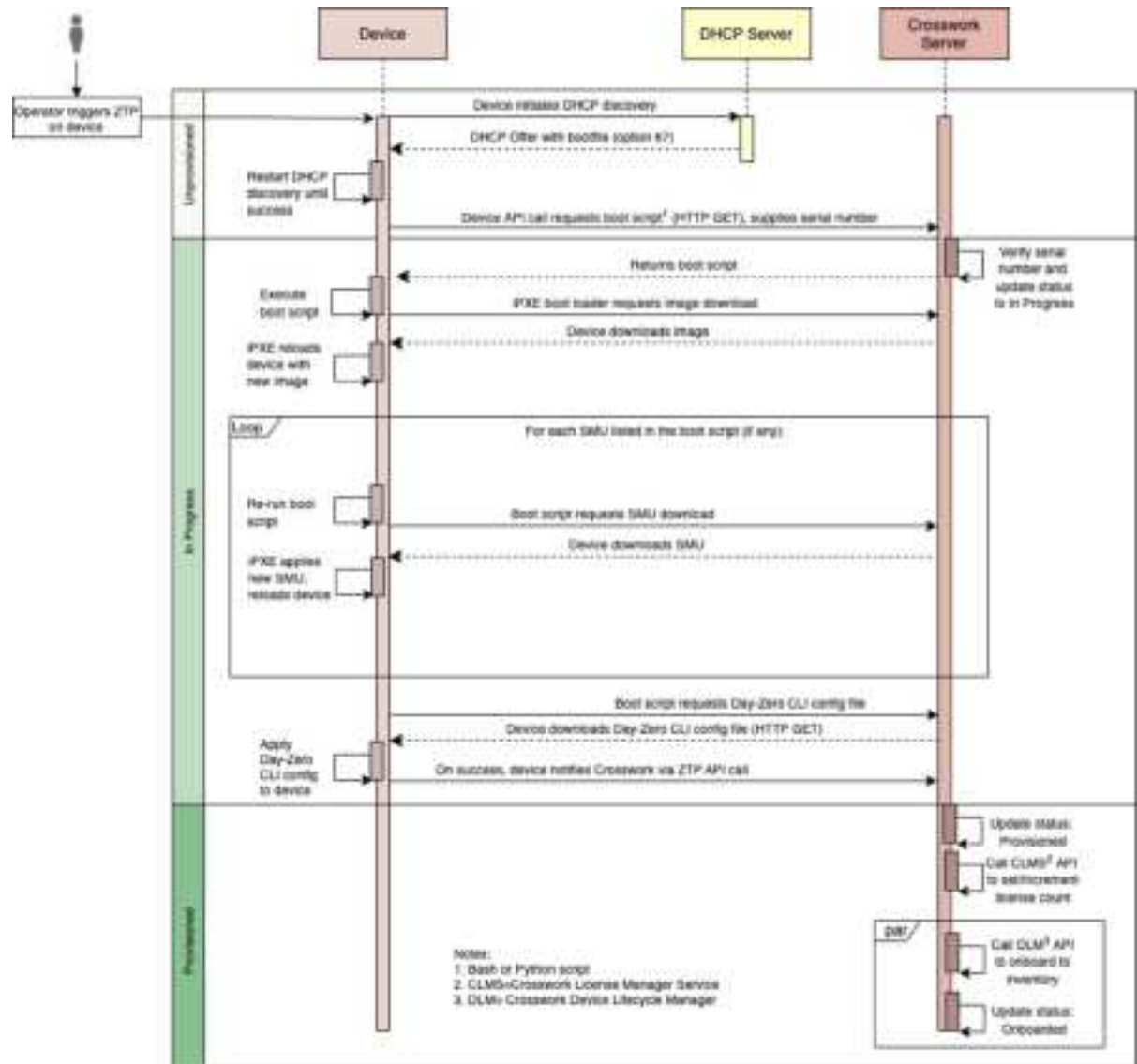
When initiated by a device reset or reload, the ZTP process proceeds automatically. Crosswork Network Controller also updates the Devices window with status messages showing the state that each device reaches as it is processed. When a device has reached the Onboarded state, there are additional steps to perform that are beyond the scope of ZTP processing (see, for example, [Complete Onboarded ZTP Device Information, on page 83](#)).

The scripts used to configure the devices must include notifications of state changes in order for Crosswork Network Controller to accurately report progress as shown in the diagrams. To see examples of these calls, select **Device Management > Zero Touch Provisioning > Configuration files**, then click **Download sample script (XR)**. For information on the sample configuration file, see the Download the Sample Configuration File section in [Prepare and Load Configuration Files](#).

Classic ZTP Processing

The following illustration shows the process logic that Classic ZTP uses to provision and onboard devices. The device state transitions are represented by blocks in the shades of green, positioned on the left side of the illustration.

Figure 1: Classic ZTP Processing

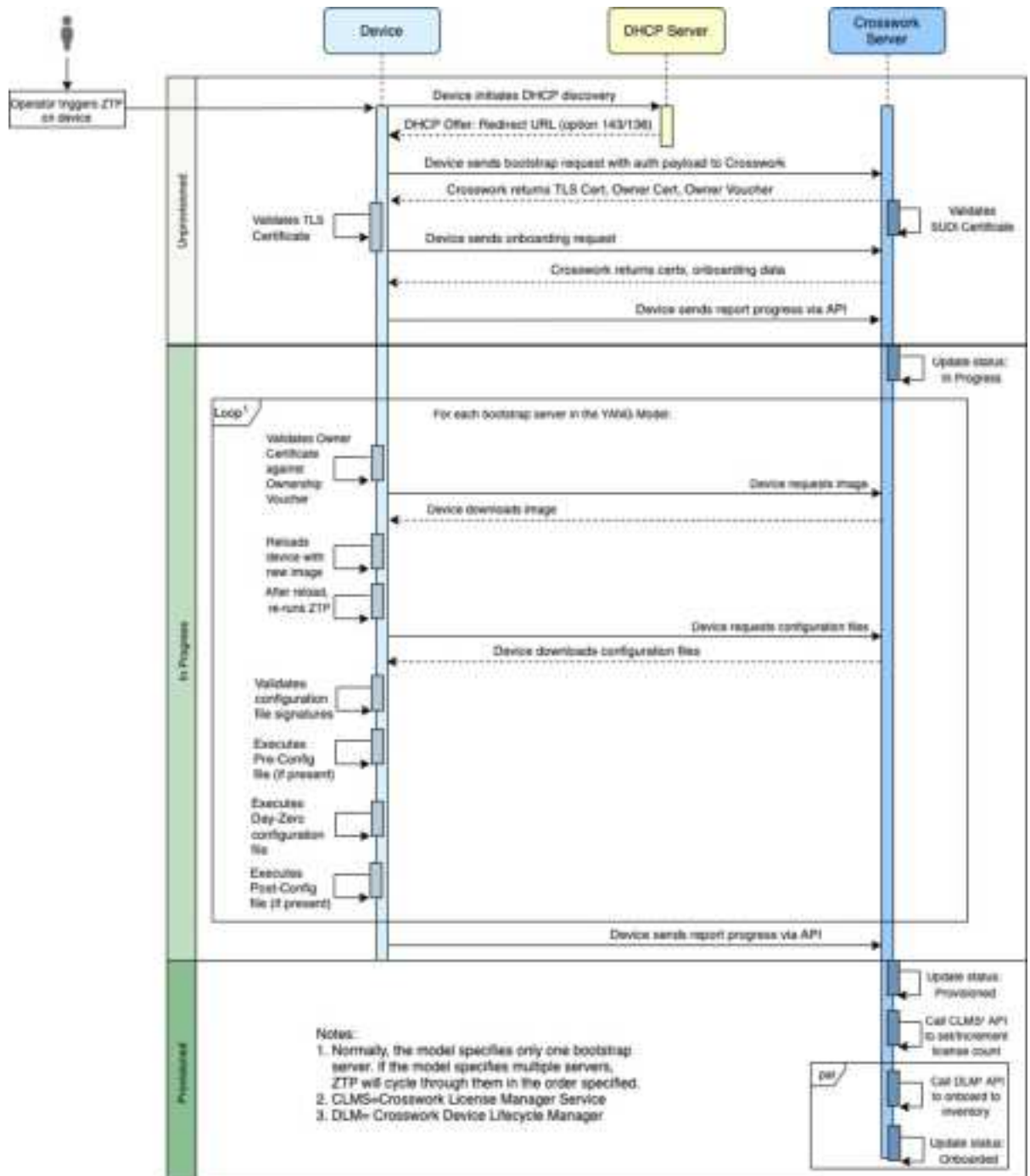


The DHCP server verifies the device identity based on the device serial number, then directs the device to download the boot file and image. Once ZTP images the device, the device downloads the configuration file and executes it.

Secure ZTP Processing

The following illustration shows the process logic that Secure ZTP uses to provision and onboard devices. The device state transitions are represented by blocks in the shades of green, positioned on the left side of the illustration.

Figure 2: Secure ZTP Processing



The device and the ZTP bootstrap server authenticate each other using the Secure Unique Device Identifier (SUDI) on the device and server certificates over TLS/HTTPS. Over a secure HTTPS channel, the bootstrap server lets the device download-signed image and configuration artifacts. These artifacts must adhere to the [RFC 8572 YANG schema](https://tools.ietf.org/html/rfc8572#section-6.3) (<https://tools.ietf.org/html/rfc8572#section-6.3>). When the device installs the new image (if any) and reloads, the device downloads configuration scripts and executes them.

The following illustration shows the process logic that PnP ZTP uses to provision and onboard devices. The device state transitions are represented by blocks in the shades of green, positioned on the left side of the illustration.

The diagram illustrates the initial device onboarding process, divided into three phases: Unauthenticated, In Progress, and Provisioned.

Participants:

- Cisco IOS-XE device:** The device being onboarded.
- DHCP + TFTP Servers:** Provide network configuration and boot files.
- Crosswork Server:** Manages device lifecycle and licenses.

Sequence of Events:

- Unauthenticated Phase:**
 - Operator triggers ZTP on device.
 - ZTP process, VLAN discovery occurs on the device.
 - DHCP process on the device receives DHCP offer and lease from the DHCP + TFTP servers.
 - Initial PoP discovery occurs on the device.
 - The device sends an **httpWORK-REQUEST** (external) to the Crosswork Server.
 - The Crosswork Server responds with an **httpWORK-REQUEST** (capacity service request).
 - The device receives an **httpWORK-RESPONSE** (success=0) with supported capabilities.
- In Progress Phase:**
 - The device sends an **httpWORK-RESPONSE** (send bye request) to the Crosswork Server.
 - The Crosswork Server responds with an **httpWORK-REQUEST** (external).
 - The device sends an **httpWORK-REQUEST** (inventory request) to the Crosswork Server.
 - The Crosswork Server responds with an **httpWORK-RESPONSE** (success=0) with device info.
 - The device sends an **httpWORK-RESPONSE** (send bye request) to the Crosswork Server.
 - The Crosswork Server responds with an **httpWORK-REQUEST** (external).
 - The device sends an **httpWORK-REQUEST** (configure initial service) to the Crosswork Server.
 - The Crosswork Server responds with an **httpCERT-OCSP-040** response.
 - The device sends an **httpHELLO** response to the Crosswork Server.
 - The Crosswork Server responds with an **httpWORK-RESPONSE** (success=0).
 - The device sends an **httpWORK-RESPONSE** (send bye request) to the Crosswork Server.
 - The Crosswork Server responds with an **httpWORK-REQUEST** (external).
 - The device sends an **httpWORK-REQUEST** (device self challenge) to the Crosswork Server.
 - The Crosswork Server responds with an **httpWORK-RESPONSE** (success=0) with SUDI certificate.
 - The device sends an **httpWORK-RESPONSE** (work into request submission) to the Crosswork Server.
 - The Crosswork Server responds with an **httpWORK-REQUEST** (external).
 - The device sends an **httpWORK-REQUEST** (image request request) to the Crosswork Server.
 - The Crosswork Server responds with a **Download image from image repo service** message.
 - The device sends an **httpWORK-RESPONSE** (success=0) with status.
 - The Crosswork Server responds with an **httpWORK-RESPONSE** (work into bye request) to the device.
 - The device sends an **httpWORK-REQUEST** (external).
 - The Crosswork Server responds with an **httpWORK-REQUEST** (config upgrade request) to the device.
 - The device sends a **Download boot config from config repo service** message to the Crosswork Server.
 - The Crosswork Server responds with an **httpWORK-RESPONSE** (success=0) with status.
 - The device sends an **httpWORK-RESPONSE** (work into bye request) to the Crosswork Server.
- Provisioned Phase:**
 - The Crosswork Server updates the status to **Provisioned**.
 - The Crosswork Server calls the **CLMS API** to synchronize device count.
 - The Crosswork Server calls the **CLMS API** to onboard to inventory.
 - The Crosswork Server updates the status to **Onboarded**.

Handshake Messages:

- Red:** Initial HTTP work request from device, asking the server which service to perform.
- Blue:** Server tells device which PoP service to perform.
- Green:** Device downloads file or reports status.
- Black:** Server acknowledges or tells the device the handshake is done.

Notes:

- CLMS: Crosswork License Manager Service
- CLM: Crosswork Device Lifecycle Manager

Once an operator triggers PnP ZTP processing, the device performs VLAN discovery and creates a BDI interface, on which DHCP discovery is initiated. The DHCP discovery response provided to the device during DHCP must include Option 150 which directs the device to the TFTP server hosted on the CNC. The device downloads the PnP Profile from the TFTP server without authentication and copies it to the device's running configuration. The PnP Profile is a CLI text file. The profile activates the device's PnP agent and sends work requests to the embedded Crosswork Network Controller PnP server over HTTP on port 30620. The PnP server then validates the device's serial number against Crosswork Network Controller's "allowed" list of serial numbers (previously uploaded to Crosswork Network Controller) and then initiates a PnP capability service request. A successful PnP work response from the device changes the device provisioning status from Unprovisioned to In Progress. Thereafter, the PnP server initiates a series of service requests, including requests for device information, certificate installation, image installation, configuration upgrade, and so on. Each of these service requests involves a four-way handshake between the PnP server and the PnP agent. As part of the certificate-install request, the Crosswork Network Controller PnP server shares its certificate with the device. Successful installation of this trustpoint on the device changes the PnP profile configuration to start using HTTPS and port 30603 on Crosswork Network Controller. Subsequent image and config download requests use HTTPS to secure transactions. There is currently no SUDI certificate authentication support on the device. Once the device downloads and installs a new image (if any) and reloads, the PnP process continues to download CLI configuration files and apply them to device running configuration. The device status is then set to Provisioned and the license count is updated in Crosswork Network Controller. The device status is then set to Onboarded, and the device stops communicating with the PnP server.

ZTP Setup Workflow

ZTP requires you to complete the following setup tasks and configuration:

1. Make sure that your environment meets ZTP prerequisites for security, provider configuration, and device connectivity. See [Meet ZTP Prerequisites, on page 29](#).
2. Assemble and load the types of assets that ZTP needs for processing to Crosswork Network Controller. When uploading a configuration file that references additional files or assets, ensure that those files or assets are also uploaded to Crosswork Network Controller. See [Assemble the ZTP Assets, on page 29](#).
3. Optional: Create ZTP Profiles, which can help you simplify and standardize device imaging and configuration during the onboarding process. See [Create ZTP Profiles, on page 52](#).
4. Create ZTP device entries. ZTP uses these device entries as database "anchors" when onboarding devices to the Crosswork Network Controller device inventory. If you have many devices to onboard, create the entries in bulk by importing a CSV file (see [Upload ZTP Device Entries, on page 60](#)). If you have only a few devices to onboard, it's more convenient to prepare these entries one by one, using the Crosswork Network Controller UI (see [Prepare Single ZTP Device Entries, on page 59](#)). You can also use Crosswork APIs to onboard devices (see the ZTP API reference on the [Cisco Crosswork DevNet Page](#)).



Note

To perform ZTP activities such as adding a device, create a configuration file, or establish a ZTP profile, it's essential that you have the read/write access permissions for both ZTP-related roles and Inventory APIs.

Meet ZTP Prerequisites

For compatibility with ZTP in a multicluster and single VM deployment, your setup must meet the following prerequisites:

1. **Onboard to NSO:** If you want ZTP to onboard your devices to Cisco NSO, configure NSO as a Crosswork Network Controller provider. Be sure to set the NSO provider property key to `forward` and the property value to `true`.
2. **Confirm device reachability:** The Crosswork Network Controller cluster nodes must be reachable from the devices, and the nodes from the devices, over either an out-of-band management network or an in-band data network. For a general indication of the scope of these requirements, see the [Cisco Crosswork Installation Guide for your version of the product](#). Enabling this kind of access may require you to change firewall configurations.
3. **Set up static routes:** If your Crosswork Network Controller cluster nodes and the devices you want to onboard using ZTP are in different subnets, you need to set up one or more static routes from your Crosswork Network Controller cluster nodes to each separate device subnet. To do this from the Crosswork Network Controller main menu, select **Administration > Settings > Device connectivity management > Routes**. Click , enter the destination subnet IP address and mask (in slash notation), then click **Add**.
4. **Set up TFTP server for PnP ZTP:** If you plan to use PnP ZTP, you must add a TFTP server as a Crosswork Network Controller provider. The TFTP server can be configured with a generic profile like the one following:

```
pnp profile test-profile
transport http ipv4 192.168.100.205 port 30620
```

5. **Set boot-level license levels on IOS-XE devices:** If you plan on using PnP ZTP, check that the minimum license boot-level on each IOS-XE device is set to **metroipaccess** or **advancedmetroipaccess**. Be sure to perform this check **before** you trigger ZTP processing. If the boot level has been set properly, the output of the IOS-XE `#sh run | sec license` CLI command on the device should contain statements showing either of these two license levels: `license boot level advancedmetroipaccess` or `license boot level metroipaccess`. If the command output shows any other license level, especially one lower than these two, the Cisco PnP cryptographic functionality will not be enabled. This will cause certificate installation to fail, which will then cause PnP ZTP device provisioning to fail.
6. **Avoid IPv6 SLAAC IP address conflicts:** Incorrect DHCPv6 and IPv6 gateway configuration can cause IP address assignment conflicts with Stateless Address Autoconfiguration (SLAAC). These conflicts result in a variety of ZTP failures, including preventing image upgrade on a destination device. If you plan to use ZTP on an IPv6 network, ensure that:
 - Your DHCPv6 subnet range specifies a `/64 prefixlen`. This simple specification can prevent many failures.
 - The default gateway is configured to avoid SLAAC IP assignment and uses DHCPv6 and stateful IP configuration only.
 - The VMs used to host DHCPv6 allow Router Advertisements but do not allow autoconfig IPs.

Assemble the ZTP Assets

The term "ZTP Assets" refers to the software and configuration files, credentials, certificates, and other assets. The number of assets you need to prepare and load into Crosswork Network Controller will vary, depending

on whether they are required for the ZTP mode you want to use, the state of your devices at the time you begin onboarding them, and other factors.

For your convenience, we recommend that you prepare and load these assets in the order that is given in the [checklist](#). For details on how to prepare and then load each asset, including optional assets like software images, see the linked topic in the checklist's last column. If an asset references additional files or assets, make sure that those files or assets are also loaded into Crosswork Network Controller to prevent errors when applying configuration files to a device.

Many organizations maintain libraries of ZTP assets such as serial numbers and configuration files. If your organization has libraries like this, ensure that they are easily accessible from your desktop. Doing so makes it easier for you to complete the ZTP setup.

For more background on using Secure ZTP with IOS-XR devices, see the [Securely Provision Your Network Devices](#) chapter of the *System Setup and Software Installation Guide for Cisco NCS 540 Series Routers, IOS XR Release 7.3.x*.

Crosswork Network Controller supplies its own TLS certificate, with Crosswork Network Controller as the Certificate Authority, for IOS-XR devices. You need not supply or upload your own TLS CA certificate chain, as IOS-XR devices do not perform X.509 validation on the Crosswork TLS server certificate.

Table 2: ZTP Asset Checklist

Order	Asset	Classic ZTP	Secure ZTP	PnP ZTP	For Details, see
1	Software image	Optional	Optional	Optional	A software image is required if the device has no software image installed. Loading Software Images, on page 31
2	Configurations	Required	Required. Supports multiple configurations.	Required	Prepare and Load Configuration Files, on page 31
3	Software Maintenance Updates (SMUs)	Optional	Optional	Not Supported	Find and Load SMUs, on page 45
4	Device Credentials	Required	Required	Required	Create Credential Profiles for ZTP, on page 46
5	Serial Numbers	Required	Required	Required	Find and Load Device Serial Numbers, on page 47
6	Pinned Domain Certificate (PDC), Owner Certificates (OCs) and Owner Key	Not Used	Required	Not used	Update the PDC, Owner Certificates, and Owner Key, on page 48.

Order	Asset	Classic ZTP	Secure ZTP	PnP ZTP	For Details, see
7	Ownership Vouchers	Not Used	Required	Not used	Load Ownership Vouchers, on page 50.
8	SUDI Root Certificate	Not used	Required	Required for IOS-XE devices only	Prepare and Load the SUDI Root Certificate, on page 51

Loading Software Images

A software image is a file containing the installable network operating system software (such as Cisco IOS-XR or, for PnP ZTP, Cisco IOS-XE) that enables a network device to function.

Software image loading is optional for all ZTP modes, although it is required if the device you are onboarding has no software image installed. You are not required to apply a software image to a device that is already imaged. You can also apply configuration files to a device without loading an image. Loading images is required only when the device you want to onboard does not have an image that is installed on it, or when you want to upgrade the network OS at the same time as you onboard the device.

Cisco distributes IOS-XR images as TAR, ISO, BIN, or RPM files. Cisco distributes IOS-XE images as BIN files only. Each Cisco image file represents a single release of the given network OS for a given device platform or family.

Download software image files from the [Cisco Support & Downloads page](#). During the download, record the file's MD5 checksum. You can also generate your own MD5 checksum for an image file you want to upload. Crosswork Network Controller uses the MD5 checksum to validate the integrity of the file.

Load software image files to Crosswork Network Controller one at a time, and enter the MD5 checksum for each file during the load.

To load software images to Crosswork Network Controller:

1. Log in to Crosswork Network Controller.
2. From the main menu, select **Device Management > Software Management**.
3. Click .
4. Enter the name of, or click **Browse** and select, the file you want to upload.
5. Click **Add** to finish adding the file.
6. Repeat as needed until you have loaded all the files to be used in the planned ZTP run.

Prepare and Load Configuration Files

Configuration files are script files that configure the features of the installed software image on a given device. They are required for all ZTP modes.

Configuration files that are used with Classic and Secure ZTP modes can be Linux shell scripts (SH), Python scripts (PY), or device operating system CLI commands stored in an ASCII text file (TXT). For Cisco IOS-XR devices and with Classic or Secure ZTP only, you can also use configuration files to upgrade an installed network OS software version using an SMU (see [Find and Load SMUs, on page 45](#)).

Classic ZTP supports only one day-zero configuration file per device. Secure ZTP allows you to apply up to three configuration files during onboarding: one for preconfiguration preparation, a second that is the day-zero or main configuration, and a third postconfiguration file to be applied after the day-zero configuration is complete. Only the day-zero configuration is required. The order of application is fixed.

Cisco PnP ZTP supports only day-zero configuration TXT files on Cisco ASR 900 and Cisco NCS 520 devices. Your PnP ZTP configuration files must use IOS-XE CLI commands. PnP ZTP does not support Linux shell (SH) or Python (PY) script files.

Your organization or Cisco consultants can create configuration files. The following sections provide guidelines for preparing configuration files for use when onboarding devices using any of the ZTP modes, as well as how to load these files into the Crosswork Network Controller.



Note When entering configuration filenames in Crosswork Network Controller, be sure to enter the filename *extension* in lowercase letters only (for example: myConfig.py, not myConfig.PY). The Crosswork Network Controller screens for and will only accept configuration filenames with all-lowercase filename extensions.

Download the Sample Configuration File

The contents of your configuration script file varies greatly, depending on the devices you use and how your organization uses them. A complete description of all the options available to you is therefore beyond the scope of this document.

The main guidelines to remember are:

1. Your custom configuration code can use both default and custom replaceable (or "placeholder") parameters. This allows you to insert values at run-time using the **Configuration details** field when importing device entries in bulk or creating them one at a time.
2. You can create new, custom replaceable parameters as needed. You can name them anything that you like, as long as they do not use the same names as the default parameters and follow the variable naming conventions that are discussed in this topic. If you do use the default replaceable parameters, their run time values will be inserted from the sources described in the "Use Default Replaceable Parameters in Configuration Files" section of this topic, instead of the values you set in the device entry's **Configuration details** field.
3. Replaceable parameter names are case-sensitive, and must include the braces and dollar sign. They must not include spaces (use underscores instead).
4. Be sure all your custom replaceable parameters have a run-time value that is specified in the **Configuration details** field. If you fail to specify a run-time value for even one of your custom replaceable parameters, the device configuration process fails.
5. If you're using Secure ZTP, you can use custom replaceable parameters for the day-zero configuration only. Custom replaceable parameters are not supported for pre-configuration and post-configuration files.
6. If your configuration file refers to another asset or file, ensure that the referred assets or files are uploaded before loading the original file. For example, when devices are located at the network edge, the operator uses a configuration script that is called Edge_Script to load a configuration file named Edge_Config. The operator must add the Edge_Config file to the system, and Crosswork Network Controller will assign a UUID to the file. After which, the operator enters the UUID into the configuration script. When

that's done, the configuration script can be loaded into the Crosswork Network Controller, which creates a UUID for the script.

7. Your configurations must use Cisco Crosswork API calls to complete some tasks. In particular, the code must use API calls to notify the Crosswork Network Controller server when the device transitions from one ZTP state to another.
8. While any configuration file can call another configuration file and run it (if it can be successfully downloaded to the device), only Secure ZTP lets you specify separate pre-configuration, post-configuration, and day-zero configuration files as part of the initial, secure download.
9. Configuration filenames cannot contain more than one period, and must use underscores in place of spaces.
10. Additional file restrictions are noted in the sample configuration file that is discussed below.
11. Review the comments in the configuration file to understand which substitutions are allowed. If the comments are unclear to you, [contact Cisco Support](#).

For examples of how to use the replaceable parameters and API calls, see the sample ZTP configuration file for Cisco IOS-XR devices supplied with ZTP. To download the sample ZTP configuration file from Crosswork Network Controller, select **Device Management > Zero Touch Provisioning > Configuration files**, then click **Download sample script (XR)**. The sample configuration script is commented and provides examples of the more commonly used API calls and replaceable parameters.

For more details on replaceable parameters, see the following sections, "Use Default Replaceable Parameters in Configuration Files", and "Use Custom Replaceable Parameters in Configuration Files".

For more details on Crosswork API calls, see the section on ZTP device and configuration APIs in the "Crosswork API References" menu, available on the [Cisco Developer Network \(DevNet\) site for Cisco Crosswork](#).

The section "Sample ZTP Configuration Scripts", later in this topic, provides examples of how to use replaceable parameters and APIs.

Preview Configuration Files

To preview the contents of any configuration file previously uploaded to Crosswork Network Controller, select **Device Management > Zero Touch Provisioning > Configuration files**, then click the configuration filename. The pop-up preview includes code syntax styling for important code features, as shown in the following table.

Table 3: Code Syntax Colors in ZTP Config File Preview

These code features...	... are shown in this color
Punctuation, Operator, Entity, URL, Variable, Class Name, Constant	Black
Comment	Gray
Property, Tag, Boolean, Function Name, Symbol	Orange
Selector, Attribute Name, Char, Builtin, Inserted	Dark Green
Function	Purple

These code features...	... are shown in this color
Keyword, Attribute Value	Blue
Regex, Important	Brown
String	Green
Number, Ethernet Address, MAC Address	Magenta

Use Default Replaceable Parameters in Configuration Files

The following table lists the default replaceable parameters you can use in your custom configuration files. At runtime, for each of these placeholders, Crosswork Network Controller substitutes the appropriate values for each device. For an example of the use of these placeholders, download the sample configuration script from Crosswork Network Controller: **Device Management > Zero Touch Provisioning > Configuration files > Download sample script (XR)**. For examples showing how to use these default replaceable parameters, see the section later in this topic, "Sample ZTP Configuration Scripts".

Table 4: Default Parameters in ZTP Configuration Files

Crosswork Network Controller substitutes this placeholder...	...Using the value from the...
<code>{ \$HOSTNAME }</code>	Host name of the device as specified in the ZTP device entry.
<code>{ \$IP_ADDRESS }</code>	IP address of the device as specified in the ZTP device entry.
<code>{ \$SSH_USERNAME }</code>	The value of the User Name field in the credential profile (when the Connectivity Type is SSH).
<code>{ \$SSH_PASSWORD }</code>	The value of the Password field in the credential profile (when the Connectivity Type is SSH).
<code>{ \$SSH_ENPASSWORD }</code>	The value of the Enable Password field in the credential profile (when the Connectivity Type is SSH).
<code>{ \$SNMP_READ_COM }</code>	The value of the Read Community field in the credential profile (when the Connectivity Type is SNMPv2).
<code>{ \$SNMP_WRITE_COM }</code>	The value of the Write Community field in the credential profile (when the Connectivity Type is SNMPv2).
<code>{ \$SNMP_SEC_LEVEL }</code>	The value of the Security Level field in the credential profile (when the Connectivity Type is SNMPv3).
<code>{ \$SNMP_USERNAME }</code>	The value of the User Name field in the credential profile (when the Connectivity Type is either SNMPv2 or SNMPv3).
<code>{ \$SNMP_AUTH_TYPE }</code>	The value of the User Name field in the credential profile (when the Connectivity Type is SNMPv3 and Security Level is AUTH_NO_PRIV or AUTH_PRIV).

Crosswork Network Controller substitutes this placeholder...	...Using the value from the...
<code>{ \$SNMP_AUTH_PASS }</code>	The value of the User Name field in the credential profile (when the Connectivity Type is SNMPv3 and Security Level is AUTH_NO_PRIV or AUTH_PRIV).
<code>{ \$SNMP_PRIV_TYPE }</code>	The value of the User Name field in the credential profile (when the Connectivity Type is SNMPv3 and Security Level is AUTH_PRIV).
<code>{ \$SNMP_PRIV_PASS }</code>	The value of the Priv Password field in the credential profile (when the Connectivity Type is SNMPv3 and Security Level is AUTH_PRIV).

Use Custom Replaceable Parameters in Configuration Files

You can create your own custom replaceable parameters in configuration files, as shown in the following sample. You can use custom and default replaceable parameters in the same configuration file, as shown in the sample.

You can assign any name you want to a custom replaceable parameter, so long as you:

- Follow the given variable definition format (for example, `{ $MyParm }`)
- Substitute an underline character in place of spaces in the parameter name.
- Don't re-use the same names and capitalization as any of the default replaceable parameters.
- Supply values for each of your custom parameters in the **Configuration details** field in the device entry file. To use the following sample CLI configuration file and its custom parameters with a ZTP device entry file, you would need to specify a value for the `{ $LOOPBACK0_IP }` custom parameter in each device's **Configuration details** field in the ZTP device entry file. If you forget to specify values for any custom parameter, the configuration fails.

If you're using Secure ZTP, custom replaceable parameters are supported for the day-zero configuration file only.

The first line in this sample script is required in CLI scripts for IOS-XR devices. It allows ZTP to verify whether the file is a CLI script or a bash/Python script. Be sure to update the version number as appropriate. No such line is required for IOS-XE devices.

In these scripts, the mandatory parameters are in **bold**.

Figure 4: Sample IOS-XR CLI Configuration Script with Mixed Replaceable Parameters

```
!! IOS XR Configuration 7.3.1
!
hostname { $HOSTNAME }
username { $SSH_USERNAME }
  group root-lr
  group cisco-support
  password 0 { $SSH_PASSWORD }
!
cdp
!
line console
exec-timeout 0 0
!
line default
```

```

exec-timeout 0 0
session-timeout 120
!

call-home
  service active
  contact smart-licensing
  profile CiscoTAC-1
  active
  destination transport-method http
!
!
interface Loopback0
  ipv4 address {${LOOPBACK0_IP}} 255.255.255.255
!
interface MgmtEth0/RP0/CPU0/0
  description OOB Management ZTP
  ipv4 address {${IP_ADDRESS}}
!
end

```

Sample ZTP Configuration Scripts

This section provides examples of configuration scripts for ZTP.

Figure 5: Classic ZTP: Day-Zero Configuration Script for IOS XR Devices

```

#!/bin/bash

#####
#
# ztpSampleScriptFile.sh
#
# Purpose: This sample script is required to notify Crosswork of the status of
# ZTP processing on an IOS XR device, and to update the device's IP address and
# hostname in Crosswork. It is also used to download a day0 config file from
# Crosswork config repository and apply this initial configuration to the device.
#
# To use: Modify the sample script as needed, following the comment guidance.
# Then upload the modified script to the Crosswork config repository.
# Next, copy the URL of this file from the repository and set that
# value in the DHCP server boot filename for ZTP config download. When ZTP is
# triggered on the device, it will download and run the script, then notify
# Crosswork.
#
# Replace the following variables with valid values & upload to Crosswork config
# repository. Sample values are provided for reference.
# - XRZTP_INTERFACE_NAME: e.g., MgmtEth0/RP0/CPU0/0 interface where ZTP triggered
# - CW_HOST_IP: Crosswork VM management or data network IP address
# - CW_PORT: 30604 for HTTP & 30603 only for HTTPS download of config file
# - CW_CONFIG_UUID: Replace with UUID of day0 config file from Crosswork repo,
#   assuming user has already uploaded device day-0 config file.
#
# This script has been tested and is known to work on Cisco NCS5501, NCS5401,
# ASR9901, and 8800 routers.
#
#####

export LOGFILE=/disk0:/ztp/customer/user-script.log

XRZTP_INTERFACE_NAME="MgmtEth0/RP0/CPU0/0"
# ZTP helper library is assumed to be installed in IOS-XR linux shell
source /pkg/bin/ztp_helper.sh

```

```

interfacedata=$(xrcmd "show interface ${XRZTP_INTERFACE_NAME}")

CW_HOST_IP="<EnterIPv4AddressHere>"
CW_PORT="<30604>"
CW_CONFIG_UUID="<e04661f8-0169-4ad3-82b8-a7c26c4f2565>"

# Send logging information to log file on device disk0:/ztp/user-script.log
function ztp_log() {

    echo "$(date +"%b %d %H:%M:%S")" "$1" >> $LOGFILE
}

#
# Get chassis serial number of the device, required by ZTP process.
# This works on Cisco NCS5501, NCS5401, 8800 series routers.
#
function get_serialkey(){

    local sn=$(dmidecode | grep -m 1 "Serial Number:" | awk '{print $NF}');
    if [ "$sn" != "Not found" ]; then
        ztp_log "Serial $sn found.";
        # The value of $sn from dmidecode should be same as serial number
        # of XR device chassis.
        DEVNAME=$sn;
        return 0
    else
        ztp_log "Serial $sn not found.";
        return 1
    fi
}

#
# Get chassis serial number of the device, required by ZTP process.
# This is tested and works on Cisco ASR 9901, but not other devices.
#
function get_serialkey_asr9901(){

    udi=$(xrcmd "show license udi")
    sn=$(cut -d':' -f4 <<<"$udi")
    pid=$(cut -d':' -f3 <<<"$udi")
    pid=$(cut -d',' -f1 <<<"$pid")
    echo "Serial Number $sn"
    echo "product id $pid"
}

#
# Get IP address and subnet mask from device. IP address is assigned from DHCP
# server on interface where ZTP was triggered.
#
function get_ipaddress(){

    local ipvar=$(echo $interfacedata | awk -F "Internet address is " '{sub(/
.*/,"",$2);print $2}');
    local ipv4addr=$(xrcmd "sh run interface ${XRZTP_INTERFACE_NAME} | i ipv4 address" |
awk '{print $3}')
    local ipv6addr=$(xrcmd "sh run interface ${XRZTP_INTERFACE_NAME} | i ipv6 address" |
awk '{print $3}')
    local ipaddress=$(echo $ipvar | awk -F "/" '{sub(/ .*/,"",$1);print $1}');
    local mask=$(echo $ipvar | awk -F "/" '{sub(/ .*/,"",$2);print $2}');
    local maskv6=$(echo $ipv6addr | awk -F "/" '{sub(/ .*/,"",$2);print $2}');

    ztp_log "### Value of interfacedata => $interfacedata ###"
    ztp_log "### Value of ipvar => $ipvar ###"
    ztp_log "#####IPv4 address $ipaddress and mask $mask found. #####";
}

```

```

        IPADDR=$ipaddress
        MASK=$mask
        MASKV6=$maskv6

        return 0
    }

    #
    # Fetch hostname from device configuration.
    #
    function get_hostname(){

        hostnamedata=$(xrcmd "show running-config hostname")
        local hostname=$(echo $hostnamedata | awk -F "hostname " '{sub(/ .*/, ""); print $2}');

        ztp_log "#####hostname $hostname found.";
        HOSTNAME=$hostname;
        return 0;
    }

    #
    # Download day-0 config file from Crosswork config repository using values
    # set for CW_HOST_IP, CW_PORT and CW_CONFIG_UUID.
    # The MESSAGE variable is optional, can be used to display a suitable message
    # based on the ZTP success/failure log.
    #
    function download_config(){

        ztp_log "### Downloading system configuration ::: ${DEVNAME} ###";
        ztp_log "### ip address passed value ::: ${IPADDR} ###";
        ip netns exec global-vrf /usr/bin/curl -k --connect-timeout 60 -L -v --max-filesize
104857600
http://${CW_HOST_IP}:${CW_PORT}/crosswork/configsvc/v1/configs/device/files/${CW_CONFIG_UUID}
-H X-cisco-serial*:${DEVNAME} -H X-cisco-arch*:x86_64 -H X-cisco-uuid*: -H
X-cisco-oper*:exr-config -o /disk0:/ztp/customer/downloaded-config 2>&1

        if [[ "$?" != 0 ]]; then
            STATUS="ProvisioningError"
            ztp_log "### status::: ${STATUS} ###"
            ztp_log "### Error downloading system configuration, please review the log ###"
            MESSAGE="Error downloading system configuration"
        else
            STATUS="Provisioned"
            ztp_log "### status::: ${STATUS} ###"
            ztp_log "### Downloading system configuration complete ###"
            MESSAGE="Downloading system configuration complete"
        fi
    }

    #
    # Apply downloaded configuration to the device and derive ZTP status based on
    # success/failure of ZTP process. The MESSAGE variable is optional, can be used
    # to display a suitable message based on the ZTP success/failure log.
    #
    function apply_config(){
        ztp_log "### Applying initial system configuration ###";
        xrapplly_with_reason "Initial ZTP configuration" /disk0:/ztp/customer/downloaded-config
2>&1 >> $LOGFILE;
        ztp_log "### Checking for errors ###";
        local config_status=$(xrcmd "show configuration failed");
        if [[ $config_status ]]; then
            echo $config_status >> $LOGFILE
        fi
    }

```



```

        STATUS="ProvisioningError"
        ztp_log "### status::: ${STATUS} ###"
        ztp_log "!!! Error encountered applying configuration file, please review the log
!!!";
        MESSAGE="Error encountered applying configuration file, ZTP process failed"
    else
        STATUS="Provisioned"
        ztp_log "### status::: ${STATUS} ###"
        ztp_log "### Applying system configuration complete ###";
        MESSAGE="Applying system configuration complete, ZTP process completed"
    fi
}

#
# Call Crosswork ZTP API to update device ZTP status, IP address, hostname.
# Without this function, device status will remain in "In Progress" and not
# be updated in Crosswork.
#
# Using this API, device SSH/SNMP connectivity details can also be updated.
# Values for connectivity details values can be added as part of
# "connectivityDetails" array in below curl command. Sample snippet provided:
#
# "connectivityDetails": [{
#     "protocol": "SSH",
#     "inetAddr": [{
#         "inetAddressFamily": "IPv4/IPv6",
#         "ipaddrs": "<ssh/snmp ipaddress>",
#         "mask": <ipaddress mask(Integer).>,
#         "type": "CONNECTIVITYINFO"
#     }],
#     "port": <ssh/snmp port(Integer)>,
#     "timeout": <ssh/snmp timeout(Integer). default to 60sec>
# }]
#
function update_device_status() {

    echo "'"$IPADDR"'
    echo "'"$MASK"'
    echo "'"$DEVNAME"'
    echo "'"$STATUS"'
    echo "'"$HOSTNAME"'
    echo "'"$MESSAGE"'

    curl -d '{
        "ipAddress":{
            "inetAddressFamily": "IPv4",
            "ipaddrs": "'"$IPADDR"'",
            "mask": "'"$MASK'"
        },
        "serialNumber": "'"$DEVNAME"'",
        "status": "'"$STATUS"'",
        "hostName": "'"$HOSTNAME"'",
        "message": "'"$MESSAGE"'
    }' -H "Content-Type: application/json" -X PATCH
    http://${CW_HOST_IP}:${CW_PORT}/crosswork/ztp/v1/deviceinfo/status
}

# ==== Script entry point ====
STATUS="InProgress"
get_serialkey;
#get_serialkey_asr9901; // For Cisco ASR9901, replace get_serialkey with
get_serialkey_asr9901.

```

```

ztp_log "Hello from ${DEVNAME} !!!";
get_ipaddress;
ztp_log "Starting autoprovision process...";
download_config;
apply_config;
get_hostname;
update_device_status;

ztp_log "Autoprovision complete...";
exit 0

```

Figure 6: Secure ZTP: Simple Day-Zero Configuration Script

```

!! IOS XR
!
hostname ztpdevice1
!
interface MgmtEth0/RP0/CPU0/0
  ipv4 address dhcp
!

```

Figure 7: Secure ZTP: Day-Zero Configuration Script Using Replaceable Parameters

```

!! IOS XR
!
hostname ${hname}
!
interface MgmtEth0/RP0/CPU0/0
  ipv4 address ${mgmt_ipaddr} ${mgmt_subnet_mask}
!

```

Figure 8: Secure ZTP: Post-Configuration Script

```

#!/bin/bash

#####
#
#SZTP post script to update hostname and ipaddress for the device
# input - serial key and crosswork host and port
#
#####

export LOGFILE=/disk0:/ztp/customer/user-script.log

XRZTP_INTERFACE_NAME="MgmtEth0/RP0/CPU0/0"
# ZTP helper library is assumed to be installed in IOS-XR linux shell
source /pkg/bin/ztp_helper.sh
interfacedata=$(xrcmd "show interface ${XRZTP_INTERFACE_NAME}")

CW_HOST_IP="<EnterIPv4AddressHere>" #update from the post script prepare code
CW_PORT="<30603>" #update from the post script prepare code

# Send logging information to log file on device disk0:/ztp/user-script.log
function ztp_log() {

    echo "$(date +"%b %d %H:%M:%S")" "$1 >> $LOGFILE"

}

#
# Get IP address and subnet mask from device. IP address is assigned from DHCP
# server on interface where ZTP was triggered.
#

```

```

function get_ipaddress(){

    local ipvar=$(echo $interfacedata | awk -F "Internet address is " '{sub(/
.*/,"",$2);print $2}');
    local ipv4addr=$(xrcmd "sh run interface ${XRZTP_INTERFACE_NAME} | i ipv4 address" |
awk '{print $3}')
    local ipv6addr=$(xrcmd "sh run interface ${XRZTP_INTERFACE_NAME} | i ipv6 address" |
awk '{print $3}')
    local ipaddress=$(echo $ipvar | awk -F "/" '{sub(/ .*/,"",$1);print $1}');
    local mask=$(echo $ipvar | awk -F "/" '{sub(/ .*/,"",$2);print $2}');
    local maskv6=$(echo $ipv6addr | awk -F "/" '{sub(/ .*/,"",$2);print $2}');

    ztp_log "### Value of interfacedata => $interfacedata ###"
    ztp_log "### Value of ipvar => $ipvar ###"
    ztp_log "#####IPv4 address $ipaddress and mask $mask found. #####";

    IPADDR=$ipaddress
    MASK=$mask
    MASKV6=$maskv6

    return 0
}

#
# Fetch hostname from device configuration.
#
function get_hostname(){

    hostnamedata=$(xrcmd "show running-config hostname")
    local hostname=$(echo $hostnamedata | awk -F "hostname " '{sub(/ .*/,"",$2);print
$2}');

    ztp_log "#####hostname $hostname found.";
    HOSTNAME=$hostname;
    return 0;
}

#
# Call Crosswork ZTP API to update device ZTP status, IP address, hostname.
# Without this function, device status will remain in "In Progress" and not
# be updated in Crosswork.
#
# Using this API, device SSH/SNMP connectivity details can also be updated.
# Values for connectivity details values can be added as part of
# "connectivityDetails" array in below curl command. Sample snippet provided:
#
# "connectivityDetails": [{
#   "protocol": "SSH",
#   "inetAddr": [{
#     "inetAddressFamily": "IPv4/IPv6",
#     "ipaddrs": "<ssh/snmp ipaddress>",
#     "mask": "<ipaddress mask(Integer).>",
#     "type": "CONNECTIVITYINFO"
#   }],
#   "port": "<ssh/snmp port(Integer)>",
#   "timeout": "<ssh/snmp timeout(Integer). default to 60sec>"
# }]
#
function update_device_status() {

    echo ""$IPADDR""
    echo ""$MASK""

```

```

echo ""$SERIAL_KEY""
echo ""$HOSTNAME""

curl -d '{
  "ipAddress":{
    "inetAddressFamily": "IPv4",
    "ipaddrs": ""$IPADDR"",
    "mask": '$MASK'
  },
  "serialNumber": ""$SERIAL_KEY"",
  "hostName": ""$HOSTNAME"",
  "message": "Post config script updated succssfully"
}' -H "Content-Type: application/json" -X PATCH
http://${CW_HOST_IP}:${CW_PORT}/crosswork/ztp/v1/deviceinfo/status
}

function get_sudi_serial() {
  local rp_card_num=`ip netns exec xrnns /pkg/bin/show_platform_sysdb | grep Active | cut
-d ' ' -f 1`
  echo $rp_card_num
  xrcmd "show platform security tam all location $rp_card_num" > tamfile.txt
  local sudi_serial=$(sed -n -e '/Device Serial Number/ s/.*\s- */p' tamfile.txt)
  echo $sudi_serial
  SERIAL_KEY=$sudi_serial
  return 0
}

function ztp_disable()
{
  xrcmd "ztp disable noprompt"
}

function ztp_enable()
{
  xrcmd "ztp enable noprompt"
}

# ==== Script entry point ====
get_sudi_serial;
ztp_log "Hello from ${SERIAL_KEY} !!!";
get_ipaddress;
get_hostname;
update_device_status;

ztp_log "Autoprovision complete...";
ztp_log "Disabling secure mod"
ztp_disable;
exit 0

```

Load Configuration Files

The configuration file can become lengthy if it includes many different settings. If this file fails to load, it can be challenging to determine where the failure occurred. To address this, we recommend building and testing the script in smaller sections before fully loading it into the Crosswork Network Controller.

To load configuration files to the Crosswork Network Controller:

1. Launch Crosswork Network Controller.
2. From the main menu, select **Device Management > Zero Touch Provisioning > Configuration files**.
3. Click 

4. Click **Browse** to select a configuration file.
5. Enter the required configuration information:
For Classic and PnP ZTP, always select **Day0-config** in the **Type** drop-down.
If you're using Secure ZTP, use the **Type** drop-down to specify whether the configuration file you are adding is a **Pre-config**, **Day0-config**, or **Post-config**.
6. Click **Add** to finish adding the configuration file.
7. Repeat as needed until you have loaded all the configuration files to be used in the planned ZTP run.

Load ZTP Assets

Upload the ZTP assets that you assembled, per the requirements of the ZTP mode you want to use.

Classic ZTP requires you to load:

- Configuration files (TXT, SH, or PY files)
- Device serial numbers

Secure ZTP requires you to load:

- Configuration files (TXT, SH, or PY files)
- Device serial numbers
- Pinned domain certificate
- Ownership certificates
- Ownership Vouchers
- SUDI Root Certificates

PnP ZTP requires you to load:

- Configuration files (TXT files only)
- Device serial numbers

If you plan to image, reimage, or update the device operating system software as part of ZTP onboarding, you must also load software images and SMUs, as follows:

- Classic ZTP: TAR, ISO, BIN, or RPM image files, and SMUs
- Secure ZTP: TAR, ISO, BIN, or RPM image files, and SMUs
- PnP ZTP: BIN only. SMUs are not supported.

You may use a mapped network drive to upload software images, SMUs, and configuration files.

Crosswork Network Controller checks uploaded serial numbers for duplicates and merges them into single entries automatically. Crosswork Network Controller also associates all uploaded ownership vouchers with existing serial numbers automatically.

You can upload images, SMUs, configuration files, and serial numbers in any order. Load certificates and ownership vouchers only after loading serial numbers.



Note When entering filenames in Crosswork Network Controller, be sure to enter the filename *extension* in lowercase letters only (for example: myConfig.py, not myConfig.PY). Crosswork Network Controller screens for and will only accept configuration filenames with all-lowercase filename extensions.

Procedure

Step 1 (Optional) Upload software images and SMUs:

- a) From the main menu, select **Device Management** > **Software Management** and then click .
- b) Enter the required image or SMU file information and then click **Add**.

(Optional) Enter the MD5 checksum for the file.

You can also click **Browse** to select the software image file.

- c) Click  again and repeat step 1b until you have loaded all the image and SMU files.

Step 2 Upload configuration files:

- a) From the main menu, select **Device Management** > **Zero Touch Provisioning** > **Configuration files** and then click .

- b) Enter the required configuration information and then click **Add**.

Click **Browse** to select a configuration file.

If you're implementing Secure ZTP, use the **Type** drop-down to specify whether the configuration file you are adding is a **Pre-config**, **Day0-config**, or **Post-config**. For Classic and PnP ZTP, always select **Day0-config**.

- c) Click  again and repeat step 2b until you have loaded all the configuration files.

Step 3 (Optional) Copy the UUID of the configuration file that you have uploaded.

Step 4 (Optional) Edit the configuration scripts to include the UUID or image ID for any configuration files, images, or SMUs that are uploaded.

Step 5 Upload device serial numbers:

- a) From the main menu, select **Device Management** > **Zero Touch Provisioning** > **Serial Numbers & Ownership Vouchers**, then click **Add serial number(s)**.
- b) Click **Upload CSV**, then click the **serialnumber.csv** link to download the sampleSerialnumber.csv template file.
- c) Using your choice of CSV file editor, enter into the template the serial numbers for all the devices you plan to onboard using ZTP. Save the updated CSV template under a new filename.
- d) Select **Add serial number(s)** again and select the **Upload CSV** radio button. Click **Browse** to select the updated CSV file, then click **Add serial number(s)** to import the serial numbers from the updated CSV template file.

Step 6 Continue with the following steps only if you plan to implement Secure ZTP.

Step 7 Update the pre-installed default Secure ZTP ownership certificate with your Pinned Domain Certificate, Owner Certificate, Owner Key, and Owner Passphrase:

- a) From the main menu, select **Administration** > **Certificate Management**.
- b) In the **Name** column, find the pre-installed **Crosswork-ZTP-Owner** certificate.
- c) Click ******* in the same row as **Crosswork-ZTP-Owner**, then click **Update certificate**.

- d) Next to the **Pin domain CA certificate** field, click **Browse**. Browse to and select the PDC file (PEM or CRT) and then click **Save**.
- e) Next to the **Owner certificate** field, click **Browse**. Browse to and select the Owner Certificate file (PEM or CRT) and then click **Save**.
- f) Next to the **Owner key** field, click **Browse**. Browse to and select the Owner Key file (PEM, KEY, CRT), then click **Save**.
- g) In the **Owner passphrase** field, enter the owner passphrase.
- h) Click **Save** to update the default owner certificate with your uploads.

Step 8

Update the preinstalled default Secure ZTP SUDI device certificate with your SUDI certificate:

- a) From the main menu, select **Administration > Certificate Management**.
- b) In the **Name** column, find the preinstalled **Crosswork-ZTP-Device-SUDI** certificate.
- c) Click **---** in the same row as **Crosswork-ZTP-Device-SUDI**, then click **Update certificate**.
- d) Next to the **Cisco M2 CA certificate** field, click **Browse**. Browse to and select the Cisco M2 CA certificate file (PEM or CRT), then click **Save**.

Step 9

Upload additional ownership vouchers, as needed:

- a) From the main menu, select **Device Management > Zero Touch Provisioning > Serial Numbers & Ownership Vouchers**.
- b) Click **Add voucher(s)**.
- c) Click **Browse** to browse to and select the TAR or VCJ voucher files you want to upload. Note that Crosswork Network Controller supports both compressed and uncompressed TAR files.

When uploading vouchers, ensure that the uploaded VCJ file or files in the TAR follow the name convention *serial.vcj*, where *serial* is the serial number of the corresponding device. Crosswork Network Controller requires this type of naming to map the ownership voucher to the device.

- d) Click **Upload**.

Find and Load SMUs

A Software Maintenance Update (SMU) is a Cisco software package file that provides point fixes for critical issues in a given release of a Cisco network operating system software image. Cisco distributes SMUs in nonbootable format with a *readme.txt* file explaining the issues associated with the SMU. Cisco rolls SMU contents into the next maintenance release of a software image. For more information, see the *Cisco IOS XR documentation*.

Applying an SMU to a device during ZTP onboarding is supported for Classic and Secure ZTP only, and then only during application of a configuration file (see [Prepare and Load Configuration Files, on page 31](#)). SMUs are not supported for Cisco IOS-XE devices or for PnP ZTP.

As with software images, download SMU files from the [Cisco Support & Downloads page](#). During the download, record the SMU file's MD5 checksum. Crosswork Network Controller uses the MD5 checksum to validate the integrity of the SMU file. Load SMUs to Cisco Crosswork one at a time, and enter the MD5 checksum for each SMU file during the load.

To load SMUs to Crosswork Network Controller:

1. Launch Crosswork Network Controller.
2. From the main menu, select **Device Management > Software Management**.

3. Click .
4. In the **Software image** field, enter or click **Browse** to select, the name of the SMU file you want to upload (ISO, TAR, or RPM).
5. In the **MD5 checksum** field, enter the checksum you recorded when you downloaded the SME file.
Then complete the other fields as required.
6. Click **Add** to finish adding the SMU.
7. Repeat these steps as needed until you have loaded all the SMU files to be used in the planned ZTP run.

Create Credential Profiles for ZTP

Cisco Crosswork ZTP requires credential profiles in order to access and configure your devices. The following steps show how to add them in bulk using a CSV file.

You can also add credential profiles one at a time. To do so, select **Device Management > Credential Profiles**, then click .

Credential profiles allow you to specify different credentials for each protocol the device supports. When creating device credential profiles that contain SNMP credentials, we recommend that the profile contain credentials for the version of SNMP actually enabled on the device, and that version only. For example: If SNMPv3 is not enabled in the device configuration, do not include SNMPv3 credentials in the device credential profile.

Procedure

-
- Step 1** From the main menu, choose **Device Management > Credential Profiles**.
 - Step 2** Click .
 - Step 3** Click the **Download sample 'credential template (*.csv)' file** link and save the CSV file template locally.
 - Step 4** Open the CSV template using your preferred editor. Begin adding rows to the file, one row for each credential profile you want to create.
As you do, observe these guidelines:
 - If the **Password** column for any credential profile is blank, you can't import the CSV file. If you wish, you can enter the actual passwords in these fields. Cisco Crosswork stores them in encrypted form. If you choose this method, be sure to destroy the CSV file immediately after upload. We recommend using asterisks to fill the **Password** column in the CSV file and then importing it. After successful import, you can use the Cisco Crosswork GUI to edit each profile and enter the actual passwords, as explained in the following steps.
 - Use a semicolon to separate multiple entries in the same field.
 - When you separate multiple entries with semicolons, remember that the order in which you enter values in each field is important. The first entry in one column will map to the first entry in the next column, and so on. For example: Suppose you enter in **Password type** this list of password types: **ROBOT_USERPASS_SSH;ROBOT_USERPASS_TELNET;ROBOT_USERPASS_NETCONF**. You then enter in the **User name** column **Tom;Dick;Harry**; and in the **Password** column **root;MyPass;Turtledove**; . The order of entry in these columns sets the following mapping between the three password types and the three user names and three passwords you entered:

- ROBOT_USERPASS_SSH; Tom ; root
- ROBOT_USERPASS_NETCONF; Dick ; MyPass
- ROBOT_USERPASS_TELNET; Harry; Turtledove

- Be sure to delete sample data rows before saving the file. You can ignore the column header row.

Step 5 When you're finished, save the CSV file to a new name.

Step 6 If necessary, choose **Device Management > Credential Profiles** again, then click .

Step 7 Click **Browse** to navigate to the CSV file and select it.

Step 8 With the CSV file selected, click **Import**.

Step 9 When the import is complete:

- With the **Credential Profiles** window displayed, click the selection box next to the profile you want to update, then click .
- Enter the passwords and community strings for the credential profile and then click **Save**.
- Repeat these steps as needed until you have entered all passwords and community strings for all the credential profiles needed to access your devices.

Find and Load Device Serial Numbers

Device serial numbers are required for all ZTP modes.

Most organizations maintain a database of network device serial numbers as part of their non-sales inventory records. When adding new devices to the network, they will typically add the new device serial numbers to the same database at the time of purchase. This is the first place to look for serial numbers for devices you plan to onboard using ZTP.

You can also [Contact Cisco Support](#) for help getting the serial numbers for newly purchased devices.

As a last resort, and for a Cisco IOS device that is already imaged, log in to the device console and run the `show inventory` CLI command. In the command output, look for a device name and description section like the one shown in the following illustration. In the case of devices with line cards or other options (as shown in this example), you will want to load both the serial numbers for both the chassis and card.

```
RP/0/RP0/CPU0:ios#sh inv
Wed May 18 13:33:53.674 UTC
NAME: "0/RP0", DESCR: "NC5501 w/o TCAM Route Processor Card"
PID: NCS-5501 , VID: V01, SN: FOC23297HGS

NAME: "Rack 0", DESCR: "NCS5501 w/o TCAM 1RU Chassis"
PID: NCS-5501 , VID: V01, SN: FOC2332R014
...
```

To load device serial numbers to Crosswork Network Controller :

1. Launch Crosswork Network Controller.
2. From the main menu, select **Device Management > Zero Touch Provisioning > Serial Numbers & Ownership Vouchers**.
3. Click **Add serial number(s)**.

4. Click **Upload CSV**, then click the **serialnumber.csv** link to download the `sampleSerialnumber.csv` template file.
5. Using your choice of CSV file editor, enter into the template the serial numbers for all the devices you plan to onboard using ZTP. Save the updated CSV file template under a new name.
6. Select **Add serial number(s)** again.
7. Click **Browse** to select the updated CSV file.
8. Click **Add serial number(s)** to import the serial numbers.

Update the PDC, Owner Certificates, and Owner Key

The Pinned domain certificate, Owner certificate, and Owner key are required only for Secure ZTP. They are not used with Classic ZTP and PnP ZTP.

In a test environment, you can use the default Pinned Domain Certificate (PDC), Owner Certificates (OCs) and Owner key that Cisco Crosswork generates when ZTP is first installed. These credentials rely on Cisco as the Certificate Authority (CA) and are offered solely for the convenience of product testing. Cisco assumes that when you are using these default credentials, you are testing Cisco Crosswork in a protected "sandbox" environment that does not expose your network to security risks.

For production use, you must pin the Domain Certificate, generate intermediate OCs, and sign the Owner Key. You can then update the default versions of these credentials using the steps in the following section, "Update the Default PDC, OCs and Owner Key".

Organizations with their own certificate management staff and procedures will be familiar with how to generate a PDC, OCs and Owner Key using their chosen CA. Organizations that need more assistance with these tasks should see the examples and advice in the later section of this topic, "Pin the Domain Certificate, Generate Owner Certificates and Sign the Owner Key".

Update the Default PDC, OCs and Owner Key

To update the default Pinned Domain Certificate (PDC), Owner Certificate (OCs), and Owner Key:

1. Launch Crosswork.
2. From the main menu, select **Administration > Certificate Management**.
3. Under the **Name** column, find the **Crosswork-ZTP-Owner** certificate. Then click the ******* in the same row and select **Update certificate**.
4. Next to the **Pin domain CA certificate** field, click **Browse** and select your Pinned Domain Certificate file (PEM or CRT only). With the file selected, click **Save**.
5. Next to the **Owner certificate** field, click **Browse** and select your Owner Certificate file (PEM or CRT only). With the file selected, click **Save**.
6. Next to the **Owner key** field, click **Browse** and select your Owner Key file (PEM, KEY, CRT). With the file selected, click **Save**.
7. Click **Save** to update the default certificates and key.

Pin the Domain Certificate, Generate Owner Certificates and Sign the Owner Key

The following steps provide a series of examples showing how to use OpenSSL and the Linux Bash shell to generate a PDC, OCs and a signed Owner Key using your own Certificate Authority. You can find additional explanations and examples of this process at the following public resource: [OpenSSL Certificate Authority](#). Once you've generated these credentials, follow the procedure in the preceding section, "Update the Default PDC, OCs and Owner Key".

1. Create a set of directories to manage the certificate and other files you will use or generate. For example:

```
#!/bin/sh
mkdir ./ca
mkdir ./ca/certs
mkdir ./ca/crl
mkdir ./ca/newcerts
mkdir ./ca/private
chmod 700 ./ca/private
touch ./ca/index.txt
echo 1000 > ./ca/serial
mkdir ./ca/intermediate
mkdir ./ca/intermediate/certs
mkdir ./ca/intermediate/crl
mkdir ./ca/intermediate/csr
mkdir ./ca/intermediate/newcerts
mkdir ./ca/intermediate/private
chmod 700 ./ca/intermediate/private
touch ./ca/intermediate/index.txt
echo 1000 > ./ca/intermediate/serial
echo 1000 > ./ca/intermediate/crlnumber
```

2. Generate the root key. For example:

```
#!/bin/bash
cd ca
openssl genrsa -aes256 -out private/ca.key.pem 4096
chmod 400 ./private/ca.key.pem
```

3. Create the root certificate. For example:

```
#!/bin/bash
cd ca
##-subj "/C=us/ST=nc/L=rtp/O=cisco/OU=cx/CN=cisco.com" \
openssl req -config openssl.cnf -key ./private/ca.key.pem -new -x509 -days 7300 -sha256 \
-subj "/C=us/ST=nc/L=rtp/O=cisco/OU=cx/CN=cisco.com" -extensions v3_ca -out \
certs/ca.cert.pem
chmod 444 ./certs/ca.cert.pem
```

4. Verify the root certificate. For example:

```
#!/bin/bash
cd ca
openssl x509 -noout -text -in certs/ca.cert.pem
```

5. Generate the intermediate key. For example:

```
#!/bin/bash
cd ca
openssl genrsa -aes256 -out intermediate/private/intermediate.key.pem 4096
chmod 400 ./intermediate/private/intermediate.key.pem
```

6. Create the intermediate certificate. For example:

```
#!/bin/bash
cd ca
##-subj "/C=us/ST=nc/L=rtp/O=cisco/OU=cx/CN=cisco.com" \
```

```
openssl req -config intermediate/openssl.cnf -new -sha256 \
-key intermediate/private/intermediate.key.pem \
-out intermediate/csr/intermediate.csr.pem \
-subj "/C=us/ST=nc/L=rtp/O=cisco/OU=cx/CN=intermediate.cisco.com"
chmod 444 ./certs/ca.cert.pem
© 2022 GitHub, Inc.
```

7. Sign the intermediate key. For example:

```
#!/bin/bash
cd ca
openssl ca -config openssl.cnf -extensions v3_intermediate_ca \
-days 3650 -notext -md sha256 \
-in intermediate/csr/intermediate.csr.pem \
-out intermediate/certs/intermediate.cert.pem
chmod 444 ./intermediate/certs/intermediate.cert.pem
```

8. Verify the intermediate certificate. For example:

```
#!/bin/bash
cd ca
openssl x509 -noout -text -in intermediate/certs/intermediate.cert.pem
```

9. Create the certificate chain. For example:

```
#!/bin/bash
cd ca
cat intermediate/certs/intermediate.cert.pem \
certs/ca.cert.pem > intermediate/certs/ca-chain.cert.pem
chmod 444 intermediate/certs/ca-chain.cert.pem
```

10. Sign the Certificate Revocation List (CRL). For example:

```
#!/bin/bash
mycsr=$1
myip=$2
export SAN="IP:${myip}"
echo $SAN
cd ca
openssl ca -config intermediate/openssl.cnf \
-extensions usrSrv_cert -days 750 -notext -md sha256 \
-in intermediate/csr/${mycsr}.csr.pem \
-out intermediate/certs/${mycsr}.cert.pem
chmod 444 intermediate/certs/${mycsr}.cert.pem
```

Load Ownership Vouchers

Ownership Vouchers (OVs) are required for Secure ZTP only. They are not used with Classic or PnP ZTP.

Cisco supplies OV's to customers either on request or via download in the form of VCJ (containing a single voucher) or TAR (an archive of multiple vouchers) files. Once you have the voucher files in either format, you can upload them directly to Crosswork.

Get Ownership Vouchers From Cisco

You can download OV's in bulk from Cisco's MASA (Manufacturer Authorized Signing Authority) server at <https://masa.cisco.com>. You will need a customer login to access the MASA server securely.

If you would rather request OV's from Cisco, [contact Cisco Support](#). You must provide the following with your request:

- Pinned Domain Certificate (PDC): A trusted digital certificate issued by a Certificate Authority (CA) and pinned by you. For details on pinning the PDC, see [Update the PDC, Owner Certificates, and Owner Key, on page 48](#).
- The serial number of each device you plan to onboard using Secure ZTP (see [Find and Load Device Serial Numbers, on page 47](#)).

Here is an example request for a single device:

```
{
  "expires-on": "2016-10-21T19:31:42Z",
  "assertion": "verified",
  "serial-number": "JADA123456789",
  "idevid-issuer": "base64encodedvalue==",
  "pinned-domain-cert": "base64endvalue==",
  "last-renewal-date": "2017-10-07T19:31:42Z"
}
```

Cisco Support will respond to your request for a single OV by sending you a VCJ file. If you requested OVs for more than one device, Cisco will send you multiple VCJs in a TAR file instead of a single VCJ file. We recommend that you perform the VCJ or TAR file exchange using a secure method that you have agreed upon with Cisco Support.

Remember that individual VCJ files, whatever the source, must have the device serial number as the file name. Following the example request given above, Cisco would return a file with this name: JADA123456789.VCJ.

Get Ownership Vouchers From Third Parties

If you want to use Secure ZTP to onboard third-party devices, you must request VCJ files from the third-party manufacturer. VCJ files the manufacturer supplies must follow the naming convention *serial.vcj*, where *serial* is the serial number of the third-party device. Cisco Crosswork requires this file naming convention in order to map the Ownership Voucher to the device. For background about restrictions on vouchers from third-party manufacturers, see *Platform Support for Secure ZTP* in [Platform Support for ZTP, on page 22](#).

Load Ownership Vouchers

To load Ownership Vouchers:

1. Launch Cisco Crosswork.
2. From the main menu, select **Device Management > Zero Touch Provisioning > Serial Numbers & Ownership Vouchers**.
3. Click **Add voucher(s)**.
4. Enter the name of, or click **Browse** to select, the VCJ or TAR file containing the vouchers you want to upload.
5. Click **Upload** to finish uploading the OVs.

If you upload a TAR file, Crosswork will extract each of the VCJ files from the archive during the load.

Prepare and Load the SUDI Root Certificate

The SUDI Root Certificate is required for Secure ZTP, and for PnP ZTP when onboarding IOS-XE devices. It is not used for Classic ZTP.

There are two types of "SUDI certificates":

- The device **SUDI Certificate** (also known as the Trust Anchor Certificate). Every Cisco IOS-XR and IOS-XE device has a SUDI Certificate stored on the device. The device SUDI certificate cannot be modified.
- The **SUDI Root Certificate**. This is the root CA certificate that enables the SUDI Certificate on each device.

Uploading the SUDI Root Certificate to Crosswork enables the Secure ZTP process (and, for IOS-XE devices, the PnP ZTP process) to authenticate each device by comparing the SUDI Root Certificate with the device's stored SUDI Certificate. This is required before the PnP ZTP or Secure ZTP processes can provide bootstrap information to the device.

To prepare the SUDI Root Certificate and upload it to Cisco Crosswork:

1. Download the "Cisco Root CA 2048" and "Cisco Root CA 2099" files, in PEM format, from [Cisco PKI: Policies, Certificates, and Documents](https://www.cisco.com/security/pki/policies/index.html) (<https://www.cisco.com/security/pki/policies/index.html>).
2. Use an ASCII text editor to combine the two downloaded PEM files into a single PEM file, as in the example below:


```
-----BEGIN CERTIFICATE-----
MIIDQzCCAiuGAWIBAgIQX/h7KctU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
....
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDITCCAgmgAWIBAgIJAZozWHjOFsHBMA0GCSqGSIb3DQEBCwUAMC0xDjAMBgNV
....
PKkmBlNQ9hQcNM3CSzVvEAK0CCEo/NJ/xzZ6WX1/f8Df1eXbFg==
-----END CERTIFICATE-----
```
3. Launch Cisco Crosswork.
4. From the main menu, select **Administration > Certificate Administration**.
5. Under the **Name** column, find the **Crosswork-ZTP-Device-SUDI** certificate. Then click the *** in the same row and select **Update certificate**.
6. In the **Cisco M2 CA certificate** field: Either enter, or click **Browse** and select, the SUDI Root Certificate file (PEM or CRT only) you prepared.
7. With the file name entered, click **Save**. Crosswork stores the SUDI Root Certificate.

Create ZTP Profiles

Cisco Crosswork uses ZTP profiles to automate imaging and configuration processes. While ZTP profiles are optional, we strongly recommend creating them, as they can help simplify and routinize the ZTP imaging and configuration process. You can use ZTP profiles to help organize defined sets of image and configuration files that you can then apply to devices in a particular class or device family.

If you're implementing Classic ZTP, each ZTP profile can have only one image file and one configuration file associated with it. Secure ZTP allows you to specify preconfiguration, postconfiguration, and day-zero configuration files.

ZTP profiles don't require that you specify a software image file.

You can create as many ZTP profiles as you like. We recommend that you create only one ZTP profile for each device family, use case, or network role.

Procedure

-
- Step 1** From the main menu, choose **Device Management > Zero Touch Provisioning > ZTP profiles**.
- Step 2** Click **+ Create ZTP Profile**.
- Step 3** Enter the required values for the new ZTP profile. You don't need to specify a software image for the profile.
- Step 4** If you're implementing Secure ZTP, select the **Secure ZTP** check box. Then enter the names of the pre- and postconfiguration files.
- The **Secure ZTP** check box is unselected by default. The check box selection is not available if you select **IOS-XE** in the **OS platform** field.
- Step 5** Click **Save** to create the new ZTP profile.
-

Prepare ZTP Device Entry Files

Cisco Crosswork uses ZTP device entries to let you specify in advance and then import the IP addresses, protocols, and other information for the devices you want to provision. Cisco Crosswork populates these imported entries with more information once ZTP processing completes successfully.

The fastest way to create multiple ZTP device entries is to import them in bulk, using a device-entry CSV file. You can download a template for this CSV file from Crosswork. We recommend that you experiment with the device entry CSV file format until you get used to it. Download and make a copy of the template, modify the copy to add just one or two device entries, then import it. You can then see how to get the results you want.

The following topics explain how to download and use a device entry CSV file to create properly formatted ZTP device entries in bulk.

You can also create ZTP device entries one by one, using the Cisco Crosswork UI, as explained in [Prepare Single ZTP Device Entries, on page 59](#).

Download and Edit the ZTP Device Entry CSV Template

1. From the main menu, choose **Device Management > Zero Touch Provisioning > Devices**.
2. Click .
3. Click the **Download 'devices import' template (.csv)** link and then **Save** it to a local storage resource. Click **Cancel** to clear the dialog box.
4. Open the CSV template with the application of your choice and save it to a new name. In each row of the template copy, create an entry for each device you plan to onboard using ZTP. Refer to the next topic, "ZTP Device Entry CSV Template Reference", for help with the values to enter in each column.
5. Once you have completed preparing your ZTP device entry files, load them to Crosswork using the steps in [Upload ZTP Device Entries, on page 60](#).

ZTP Device Entry CSV Template Reference

The following table explains how to use the columns in the device entry template. We mark columns that require entries with an asterisk (*) next to the column name.

The four "Connectivity" columns allow multiple entries, so you can specify multiple connectivity protocols for a single device. If you use this option, use semicolons between entries, and enter the values in the next three columns in the same order. For example: Suppose you enter **SSH;NETCONF;** in the **Connectivity Protocol** column. If you enter **23;830;** in the **Connectivity Port** column, the entries in the two columns map like this:

- SSH: 22
- NETCONF: 830

Table 5: ZTP Device Entry Template Column Reference

Template Column	Usage
Serial Number *	Enter the device serial number. You can enter up to three serial numbers for the same device. These must be the same serial number for each device that you loaded into Cisco Crosswork previously. ZTP requires a serial number entry for all normal deployments. If you're using DHCP option 82 to implement a relay agent, you can leave this field blank, but you must specify a Remote Id and Circuit ID to identify the device.
Location Enabled	Enter TRUE if you plan to identify the device using a location ID. Enter FALSE if you plan to identify it by serial number. If you enter TRUE, enter a Remote ID and a Circuit ID in the corresponding columns. If you enter FALSE, enter a Serial Number in the corresponding column.
Remote ID *	If implementing Secure ZTP and using option 82: Identify the name of the remote host acting as the bootstrap server. If you're using DHCP option 82 to implement a relay agent, this entry is required. You must enter a combination of the device RemoteID and CircuitID. If you're not using option 82, you can leave this field blank but you must specify the device serial number.
Circuit ID *	If implementing Secure ZTP and using option 82: Identify the interface or VLAN on which the bootstrap server receives requests. If you're using DHCP option 82 to implement a relay agent, this entry is required. You must enter a combination of the device RemoteID and CircuitID. If you're not using option 82, you can leave this field blank but you must specify the device serial number.
Host Name *	Enter the host name you want to assign to the device.
Credential Profile *	Enter the name of the credential profile you want Cisco Crosswork to use to access and configure the device. The name you enter must match the name of the credential profile as specified in Cisco Crosswork.

Template Column	Usage
OS Platform *	Enter the OS platform for the device. For example: IOS XR. Note that you must enter Cisco IOS platform names with a space, not a hyphen.
Version *	Enter the OS platform version for the device software image. The platform version should be the same version as the ones specified for the image and configuration files you use to provision it. Required only if you don't specify a ZTP profile in the Profile Name column.
Device Family *	Enter the device family for the device. The device family must match the device family in the image and configuration files ZTP uses to provision it. Required only if you don't specify a ZTP profile in the Profile Name column.
Config ID *	Enter the Cisco Crosswork-assigned ID for the configuration file you want to use when configuring the device. Cisco Crosswork assigns a unique ID for every configuration file during upload. Required only if you don't specify a ZTP profile in the Profile Name column.
Profile Name *	Enter the name of the ZTP profile you want to use to provision this device. Required only if you want to use a ZTP profile to specify things like the configuration ID, image ID, OS platform, and so on.
Product ID *	Enter the Cisco-assigned PID (product identifier) coded into the device hardware. You can retrieve the PID from the UDI (Unique Device Identifier) information printed on the label affixed to every Cisco networking device when it leaves the factory. Please note that, in this release, no verification is performed on the PID. We recommend that you supply a correct PID anyway, in case of future requirements.
UUID	You can choose to generate and specify a Universally Unique Identifier (UUID) to be assigned to the device when it is onboarded. If you choose this option, enter the 128-bit UUID in this column. Otherwise, leave the field blank and Cisco Crosswork will assign a random UUID when it onboards the device.
MAC Address	Enter the device's MAC address.
IP Address	Enter the device's IP address (IPv4 or IPv6), along with its subnet mask in slash notation.
Configuration Attributes	Enter the values you want Cisco Crosswork to use for the custom replaceable parameters in the configuration file for the device. If you are using only the default replaceable parameters, leave this field blank. If you're using Secure ZTP, you can use custom replaceable parameters only for day-zero configuration file parameters. For help using replaceable parameters, see Prepare and Load Configuration Files, on page 31 .

Template Column	Usage
Connectivity Protocol	The connectivity protocols needed to monitor the device or to support Cisco Crosswork applications and features. Choices are: SSH , SNMPv2 , NETCONF , TELNET , HTTP , HTTPS , GRPC , and SNMPv3 . For help selecting the correct mix of protocols, see the table in the following topic, "Crosswork Connectivity Protocol Requirements".
Connectivity IP Address	Enter the IP address (IPv4 or IPv6) and subnet mask for the connectivity protocol. Required only if you chose to set up a connectivity protocol.
Connectivity Port	Enter the port used for this connectivity protocol. Each protocol maps to a port. Be sure to enter the port number that maps to the protocol you chose. Specify at least one port and protocol for every device, except if you want to: • Set the status of the onboarded device as unmanaged or down. • Disable Cisco Crosswork reachability checks for the onboarded device. You may need to specify more than one protocol and port per device. The number of protocols and ports you specify depends on how you have configured Cisco Crosswork and the Crosswork applications you're using. For help selecting the correct mix of protocols, see the table in the following section, "Crosswork Connectivity Protocol Requirements".
Connectivity Timeout	Enter the elapsed time (in seconds) before an attempt to communicate using this protocol times out. The default value is 30 seconds; the recommended timeout value is 60 seconds.
Provider Name	Enter the name of the provider to which you want to onboard the new ZTP devices. The name you enter must match exactly the name of the provider managing the device, as specified in Cisco Crosswork.
Inventory ID	Enter the inventory ID you want to assign to the device.
Secure ZTP Enabled	Enter TRUE if you want to provision the device using Secure ZTP, or FALSE if not.
Secure ZTP Encrypted	Currently unsupported. Enter FALSE.
Image ID	Cisco Crosswork assigns a unique ID for every software image file during upload. Enter the Cisco Crosswork-assigned ID for the software image file you want to install on the device. Required only if you want to include installation of a software image during onboarding, and you did not specify a ZTP profile with this software image in the Profile Name column.
PreConfig ID	Cisco Crosswork assigns a unique ID for every configuration file during upload. Enter the Cisco Crosswork ID of the configuration script you want to run before running the configuration file specified in the Config ID column. Required only if you want to run a pre-configuration file during onboarding.

Template Column	Usage
PostConfig ID	Cisco Crosswork assigns a unique ID for every configuration file during upload. Enter the Cisco Crosswork ID of the configuration script you want to run immediately after running the configuration file specified in the Config ID column. Required only if you want to run a post-configuration file during onboarding.
SZTP Config Mode	Enter merge if you want Secure ZTP to merge the configuration files you specify in the Config ID, PreConfig ID, and PostConfig ID columns with a pre-existing configuration on the device. Leave this column blank if you want to overwrite any existing configuration with the content of the specified configuration files (overwrite is the default specified by leaving the column blank).
Version ID	The version ID of the configuration. Required only if you specified a pre-configuration and a post-configuration file to run during onboarding.
routingInfo.globalospfrouterid	If implementing OSPF on the device: Enter the OSPF Router ID for the device. Otherwise, leave this field blank.
routingInfo.globalisssystemid	If implementing IS-IS on the device: Enter the IS-IS System ID for the device. Otherwise, leave this field blank.
routingInfo.teRouterid	If implementing Traffic Engineering on the device: Enter the TE router ID for the device. Otherwise, leave this field blank.

Crosswork Connectivity Protocol Requirements

Cisco Crosswork applications require you to enable a range of connectivity protocols for each device. The following table identifies these requirements for each supported connectivity protocol. If you use the applications listed in this table, be sure to enable these protocols on your devices. You must enable at least one of these protocols on each device in order to onboard it; you cannot onboard a device without at least one of these protocols.

Table 6: Connectivity Protocol Requirements for Applications and Features

Protocol	Port	Crosswork Application	Application Feature
GRPC	9090	- Cisco Crosswork Network Controller - Cisco Crosswork Change Automation and Health Insights - Cisco Crosswork Optimization Engine	Cisco Crosswork API communication

Protocol	Port	Crosswork Application	Application Feature
HTTP	80	• Cisco Crosswork Network Controller • Cisco Crosswork Change Automation and Health Insights • Cisco Crosswork Optimization Engine	Onboarding of the device to Cisco Network Services Orchestrator
HTTPS	443	• Cisco Crosswork Network Controller	Onboarding of the device to Cisco Network Services Orchestrator
NETCONF	830	• Cisco Crosswork Network Controller • Cisco Crosswork Change Automation and Health Insights • Cisco Crosswork Optimization Engine	Onboarding of the device to Cisco Network Services Orchestrator
SNMPv2	161	• Cisco Crosswork Network Controller • Cisco Crosswork Change Automation and Health Insights • Cisco Crosswork Optimization Engine	SNMPv2 data collection
SNMPv3	161	• Cisco Crosswork Network Controller • Cisco Crosswork Change Automation and Health Insights • Cisco Crosswork Optimization Engine	SNMPv3 data collection
SSH	22	• Cisco Crosswork Network Controller • Cisco Crosswork Change Automation and Health Insights • Cisco Crosswork Optimization Engine	• CLI data collection • SSH access to devices

Prepare Single ZTP Device Entries

If you have only a few devices to onboard using ZTP, you may find it easiest to create the device entries one by one. Use the ZTP user interface and the following instructions to create single ZTP device entries.

The ZTP device entries you create using this method always appear in the **Devices** tab with their **Status** set to **Unprovisioned**. They remain **Unprovisioned** until you trigger ZTP processing.

After ZTP onboards your device entries, Cisco Crosswork will display fields calling for more information about the device, such as its geographical location. You will need to supply this additional information by editing the device's inventory record, as explained in [Complete Onboarded ZTP Device Information, on page 83](#).

Procedure

Step 1 From the main menu, choose **Device Management > Zero Touch Provisioning > Devices**.

Step 2 Click the **Add devices** tab.

Step 3 Enter values for the new ZTP device entry.

For help with the types of information called for in each device entry field, see the template reference in [Prepare ZTP Device Entry Files, on page 53](#).

Step 4 Click **Save**.

ZTP Provisioning Workflow

When you complete ZTP setup, you can provision your devices and maintain them as follows:

1. Set up DHCP so that the Crosswork Network Controller can download image and configuration software securely after you trigger ZTP processing.
2. Upload the ZTP device entry CSV file that you created to Crosswork Network Controller. Importing the file creates the device entries that ZTP populates during onboarding. If you're onboarding only a few ZTP devices, create device entries using the ZTP user interface instead.
3. Trigger ZTP processing by power-cycling or performing a CLI reboot for each device.
4. Complete the information for the onboarded devices. Edit them and supply (for example) geographical location information that ZTP couldn't discover during provisioning.

After completing this core workflow, you can perform ongoing maintenance of your ZTP devices using the advice and methods in the following topics:

- Update ZTP devices with additional information.
- Reconfigure your ZTP devices after onboarding, using other applications or by deleting and re-onboarding the devices.
- Retire or replace ZTP devices without consuming more device licenses.
- Perform housekeeping on the ZTP assets that you used to onboard your devices.

- Troubleshoot issues with ZTP processing and devices.

Upload ZTP Device Entries

The following steps explain how to create multiple ZTP device entries by importing ZTP device-entry CSV files. If you plan to use this method for creating ZTP device entries, you must prepare these files in advance, as explained in [Prepare ZTP Device Entry Files, on page 53](#).

Imported ZTP device entries always appear in the **Devices** tab with their **Status** set to **Unprovisioned**. They remain **Unprovisioned** until you trigger ZTP processing.

After ZTP onboards your device entries, Cisco Crosswork will display fields calling for more information about each device, such as its geographical location. You will need to supply this additional information by editing the device's inventory record, as explained in [Complete Onboarded ZTP Device Information, on page 83](#)

Procedure

-
- Step 1** From the main menu, choose **Device Management > Zero Touch Provisioning > Devices**.
- Step 2** Click .
- Step 3** Click **Browse** to navigate to the ZTP device entry CSV file you created and then select it.
- Step 4** With the CSV file selected, click **Import**.
-

Set Up DHCP for ZTP

Before triggering the ZTP process, update the configuration of your DHCP server (and, for PnP only, your TFTP server) with information that permits Crosswork Network Controller to communicate with your devices and respond to their requests for downloads.

The following topics provide examples showing how to update your server configurations to meet this requirement. The instructions and examples you choose to follow will depend on the ZTP mode you have chosen to use:

- For Classic ZTP, see [Set Up DHCP for Classic ZTP, on page 60](#).
- For Secure ZTP, see [Set Up DHCP for Secure ZTP, on page 64](#).
- For PnP ZTP, see [Set Up DHCP and TFTP for PnP ZTP, on page 65](#).

For a set of configuration scripts for Classic ZTP and Cisco PNR, see [Classic ZTP DHCP Setup Scripts for Cisco Prime Network Registrar \(CPNR\), on page 66](#)

Set Up DHCP for Classic ZTP

Before triggering Classic ZTP processing, update your DHCP configuration file with information that identifies your ZTP devices and the software that is applied to them. This information permits Crosswork Network Controller and DHCP to identify the ZTP devices and respond to requests for network connection and file downloads.

The following topics provide examples showing how to update DHCP server configurations to meet this requirement. The examples in these topics assume the DHCP context settings that are shown in the following figure. The figure shows example settings for the Internet Systems Consortium DHCP server.

Figure 9: Classic ZTP DHCP Context (ISC)

```
#
authoritative;

default-lease-time 7200;
max-lease-time 7200;

subnet 192.168.100.0 netmask 255.255.255.0 {
    option routers 192.168.100.1;
    option domain-name "cisco.com";
    option domain-name-servers 171.70.168.183;
    option subnet-mask 255.255.255.0;
    range 192.168.100.105 192.168.100.195;
}
```

Examples: DHCP Setup for Classic ZTP

We strongly recommend that you use Classic ZTP to provision devices over secure network domains only.

Cisco devices that are supported by Classic ZTP allow iPXE software image downloads via HTTP only. These same devices support download of configuration files via either HTTP or HTTPS. These options require entry of DHCP bootfile URLs in the DHCP server configuration for your organization.

If you want to use HTTP for both image and configuration file downloads, these URLs must specify the HTTP protocol and port 30604. For help, see the examples in figures 1 and 2.

If you want to use HTTPS for configuration file downloads only, the URL must specify the HTTPS protocol and port 30603. Specify the -k option before the HTTPS protocol in the URL. For help, see the examples in figures 3 and 4.

ZTP permits the use of DHCP option 82 for configuration downloads. Option 82, also known as the DHCP Relay Agent Information Option, helps protect your devices from attacks using IP and MAC spoofing or DHCP address starvation. Option 82 allows you to specify an intermediary, or relay, router located between the device you're onboarding and the DHCP server resolving device requests. To use this option, specify a location ID. The location ID consists of a circuit ID (interface or VLAN ID) and remote ID (hostname). Specify these values as parameters of the configuration download URL, as shown in the examples in figures 2 and 4. For more information about option 82, see [RFC 3046](http://tools.ietf.org/html/rfc3046) (<http://tools.ietf.org/html/rfc3046>).

When following these examples:

- Be sure to replace `<CW_HOST_IP>` with the IP address of your Crosswork Network Controller cluster.
- Replace `<IMAGE_ID>` with the image ID of the software image file in the ZTP repository. For help with using bootfile names and image ID, see the later section in this topic, "Copy Bootfile Names and Image IDs for DHCP Setup".
- Configuration files do not require image IDs.

Figure 10: Classic ZTP DHCP Setup, Using HTTP

```
host cztpl {
    hardware ethernet 00:a7:42:86:54:f1;
    if exists user-class and option user-class = "iPXE" {
        filename = "http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/<IMAGE_ID>";
    } else if exists user-class and option user-class = "exr-config" {
```

```

        filename = "http://<CW_HOST_IP>:30604/crosswork/configsvc/v1/file";
    }
}

```

Figure 11: Classic ZTP DHCP Setup, Using HTTP and Option 82

```

host cztp2 {
    hardware ethernet 00:a7:42:86:54:f2;
    if exists user-class and option user-class = "iPXE" {
        filename = "http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/<IMAGE_ID>";
    } else if exists user-class and option user-class = "exr-config" {
        filename =
"http://<CW_HOST_IP>:30604/crosswork/configsvc/v1/file?circuitid=Gig001&remoteid=MAR1";
    }
}

```

Figure 12: Classic ZTP DHCP Setup, Using HTTPS

```

host cztp3 {
    hardware ethernet 00:a7:42:86:54:f3;
    if exists user-class and option user-class = "iPXE" {
        filename = "http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/<IMAGE_ID>";
    } else if exists user-class and option user-class = "exr-config" {
        filename = "-k https://<CW_HOST_IP>:30603/crosswork/configsvc/v1/file";
    }
}

```

Figure 13: Classic ZTP DHCP Setup, Using HTTPS and Option 82

```

host cztp4 {
    hardware ethernet 00:a7:42:86:54:f4;
    if exists user-class and option user-class = "iPXE" {
        filename = "http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/<IMAGE_ID>";
    } else if exists user-class and option user-class = "exr-config" {
        filename = "-k
https://<CW_HOST_IP>:30603/crosswork/configsvc/v1/file?circuitid=Gig001&remoteid=MAR1";
    }
}

```

Examples: Generic Internet Systems Consortium (ISC) DHCP Setup for Classic ZTP

The following figures show examples of the type of host entries that you would make for Classic ZTP in the `/etc/dhcp/dhcp.conf` configuration file of an [Internet Systems Consortium \(ISC\) DHCP server](#).

Other third-party DHCP servers differ in overall implementation, but many use options and formats similar to these ISC examples.

Be sure to reload or restart the ISC DHCP server when you have finished creating these new entries.

Figure 14: Classic ZTP ISC IPv4 DHCP Configuration Example

```

host NCS5k-1
{
    option dhcp-client-identifier "FOC2302R09H";
    hardware ethernet 00:cc:fc:bb:be:6a;
    fixed-address 105.1.1.16;
    if exists user-class and option user-class = "iPXE" {
        filename = "http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/
        <IMAGE_ID>";
    } else if exists user-class and option user-class = "exr-config" {
        filename = "http://<CW_HOST_IP>:30604/crosswork/configsvc/v1/file";
    }
}

```


Figure 15: Classic ZTP ISC IPv6 DHCP Configuration Example

```

host 5501
{
    host-identifier option dhcp6.client-id
00:02:00:00:00:09:46:4f:43:32:33:30:38:52:30:53:33:00;
    fixed-address6 fc00:15:2::36;
    if exists dhcp6.user-class and substring(option dhcp6.user-class, 2, 4) = "iPXE" {
        option dhcp6.bootfile-url "http://<CW_HOST_IP>:30604/crosswork/imagesvc/v1/device/files/
        <IMAGE_ID>";
    } else {if exists dhcp6.user-class and substring(option dhcp6.user-class, 0, 10) =
"exr-config" {
        option dhcp6.bootfile-url
"http://<CW_HOST_IP>:30604/crosswork/crosswork/configsvc/v1/file";
    }
}

```

The following table describes each line in the IPv4 ISC DHCP device entry examples that are given, and the source of the values used. Descriptions for the entries in the IPv6 example are identical, but adapted for the IPv6 addressing scheme.

Table 7: ISC IPv4 DHCP Configuration Host Entries and Values (Classic ZTP)

IPv4 Entry	Description
host NCS5k-1	The device entry hostname. The hostname can be the same as the actual assigned hostname, but need not be.
option dhcp-client-identifier	The unique ID of the device entry. The value "FOC2302R09H" shown in the IPv4 example is the serial number of the device. You can find the serial number on the device chassis. If you don't have physical access to the device, the IOS-XR <code>show inventory</code> command provides the serial number.
hardware ethernet 00:cc:fc:bb:be:6a	The MAC address of the Ethernet NIC port on the device. This address is the address on which you trigger the ZTP process. The address can be a management or data port, as long as it's reachable from Crosswork Network Controller .
fixed-address 105.1.1.16	The IP address to be assigned to the device during configuration. The example is for a static IP, but you can also use standard DHCP IP pool assignment commands.
option user-class = "iPXE" and filename =	This line checks that the incoming ZTP request contains the "iPXE" option. Classic ZTP uses this option to image the device. If the request includes this option, then the device downloads the image file matching the image ID and path specified in the <code>filename =</code> parameter.
option user-class = "exr-config" and ffl filename =	This line checks that the incoming ZTP request contains the "exr-config" option. ZTP uses this option to configure the device. If the request includes this option, then the device downloads the configuration file matching the path that is specified in the <code>filename =</code> parameter.

Copy Bootfile Names and Image IDs for DHCP Setup

When modifying your DHCP server configuration file, specify the bootfile name and image ID for each software image. You can quickly copy both to your clipboard directly from the list of software images that you have already uploaded to Crosswork Network Controller. No ID or image ID is required for configuration files.

To copy software image bootfile names and image ID:

1. From the main menu, choose **Device Management > Software Management**.
2. If you want to copy:
 - The bootfile name and image ID of the software image: Click  in the **Configuration Name** column.
 - Only the Image ID of the software image: Click  in the **Image ID** column.

Crosswork Network Controller copies the bootfile name or image ID, or both to your clipboard. You can now paste it into your DHCP host entry.

When using the copied file path to create DHCP host entries, replace the *IP* variable with the IP address and port of your Crosswork Network Controller server.

Set Up DHCP for Secure ZTP

Before triggering the Secure ZTP process, update your DHCP configuration file with information that identifies your ZTP devices and the software that is applied to them. This information permits Crosswork Network Controller and DHCP to identify the ZTP devices and respond to requests for network connection and file downloads.

The following provides an example showing how to update the DHCP server configuration file to meet this requirement. The example assumes you are using an Internet Systems Consortium (ISC) DHCP server. The line enabling the `sztg-redirect` option is required for Secure ZTP.

The device sends the user-class option `xr-config` along with the option 143, so this needs to be configured as shown as part of the `host` block.

Figure 16: Secure ZTP DHCP Configuration File (ISC)

```
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
# Attention: If /etc/ltsp/dhcpd.conf exists, it will be used as the
# configuration file instead of this file.
#

# option definitions common to all supported networks...
option domain-name "cisco.com";
option domain-name-servers 192.168.100.101, 171.70.168.183;
option sztp-redirect code 143 = text;
option subnet-mask 255.255.255.0;
default-lease-time 600;
max-lease-time 7200;
INTERFACES="ens192";

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none'), since DHCP v2 does not
# have support for DDNS.
```

```
#ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, uncomment the "authoritative" directive below.
#authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
#log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

subnet 192.168.100.0 netmask 255.255.255.0 {
    option routers 192.168.100.100;
    range 192.168.100.105 192.168.100.150;
}

host sztpdevice {
    hardware ethernet 08:4f:a9:0e:43:c8;
    fixed-address 192.168.100.153;
    if exists user-class and option user-class = "xr-config" {
# If you want to use a remote circuit ID to identify a remote host
# comment out the first option line and uncomment the second.
        option sztp-redirect
        "https://<CrossworkHostIP>:30617/restconf/operations/ietf-sztp-bootstrap-server:get-bootstrap-data";

        #option sztp-redirect
        "https://<CrossworkHostIP>:30617/restconf/operations/ietf-sztp-bootstrap-server:get-bootstrap-data?remoteid=VAP1&circuitid=Gig001";
    }
}
```

Set Up DHCP and TFTP for PnP ZTP

Before triggering the PnP ZTP process, you must:

1. Set up an external TFTP server that is reachable by your IOS-XE devices.
2. Upload PnP profile to the external TFTP server.
3. Update your DHCP configuration file with information pointing to the location of the PnP server.

The following topics provide examples showing how to perform each of these tasks.

Set Up the External TFTP server

An external TFTP server is required for all of the supported IOS-XE routers. The server must be active on port 69 UDP. If your organization does not already have a TFTP server, [see \(for example\) the guidance here](#).

Upload the PnP Profile to TFTP

The PnP profile is a simple generic configuration file. Uploading the PnP profile to the configuration service on the TFTP repository is a one-time activity.

The profile's contents must specify use of the Crosswork Network Controller cluster's virtual data port. In this example, the IP address 192.168.100.211 is the data VIP for the embedded PnP server and 30620 is the PnP server external port.

Figure 17: Example: Generic PnP Profile

```

pnp profile cwpnp-data
transport http ipv4 192.168.100.211 port 30620

```

Configure the DHCP Server

The DHCP entry redirects traffic from the PnP agent on the device to the IP address of the external TFTP server.

Figure 18: Sample PnP ZTP DHCP Setup

```

option tftp code 150 = text;
host cztpl {
  hardware ethernet 00:a7:42:86:54:f1;
  option tftp150 "192.168.100.205";
}

```

Classic ZTP DHCP Setup Scripts for Cisco Prime Network Registrar (CPNR)

Following are two sets of scripts that allow you to add Classic ZTP device, image and configuration file entries to the CPNR DHCP server configuration file. There is one set of three scripts for IPv4, and a separate set of five scripts for IPv6.



Note The following scripts are for use with Classic ZTP only. You can't use them with Secure ZTP or PnP ZTP.

To use these scripts:

1. Copy and paste the contents of the scripts into local text files with the names given here.
2. Modify the device, image, and configuration entries in the `ztp-v4-setup-vi-nrcmd.txt` script, or the `ztp-v6-setup-vi-nrcmd.txt` script, to fit your needs, as explained in the script comments.
3. Copy the script files you want to use to the root folder of your local CPNR server.
4. Execute the scripts on the CPNR server using the following command:

```

[root@cpnr-local ~]#/opt/nwreg2/local/usrbin/nrcmd -N username -P password
<ztp-IPVersion-setup-via-nrcmd.txt

```

Where:

- *username* is the name of a user ID with administrator privileges on the CPNR server.
- *password* is the password for the corresponding CPNR admin user ID.
- *IPVersion* is either `v4` for the IPv4 version of the scripts, or `v6` for the IPv6 version of the scripts.

Figure 19: IPv4 Script 1 of 3: ztp-v4-setup-vi-nrcmd.txt

```

#
# Create the scope
#
scope ztp-ncs-5501-mgmt create 192.0.20.0/24

# Add the dynamic range
scope ztp-ncs-5501-mgmt addrange 200 225

```

```

# Default the routers option. Note: No need to do subnet-mask. It is automatically provided.
scope-policy ztp-ncs-5501-mgmt setoption routers 10.10.10.1

# Set the lease time for clients on this scope
scope-policy ztp-ncs-5501-mgmt setoption dhcp-lease-time 216000
#
# Load the option 43 definitions
import option-set ztp-v4-option-set.txt
#
# Set the client classing expression and enable use of client-class
dhcp set client-class-lookup-id=@ztp-v4-client-class-expr.txt
dhcp enable client-class
#
# Load the client classes - these are used to lookup the correct client details
# depending on whether an iso or script is requested by the client.
client-class ztp-iso create
client-class ztp-iso set client-lookup-id="(or (try (concat (as-string
    (request get option 61)) \"-iso\")) (request macaddress-string))"
#
client-class ztp-script create
client-class ztp-script set client-lookup-id="(or (try (concat (as-string
    (request get option 61)) \"-script\")) (request macaddress-string))"
#
# Clients that are not ztp will fall into the ztp-none class
# and should not be offered service so they are excluded.
#
client-class ztp-none create
client-class ztp-none set action=exclude
#
# Create a default client that will prevent service to unknown clients.
client default create
client default set action=exclude
#
# Create some ZTP clients
#
# For each ZTP client we create two clients based on their serial number.
# (See above for the client-lookup-id expressions.)
# One has "-iso" added to the end that will be used when the client's
# request includes "iPXE" in option 77.
# The other has "-script" added to the end that will be used when the
# client's request includes "exr-config" in option 77.
#

### Device-1 Settings ###
client <device-1-serial-num>-iso create
client-policy <device-1-serial-num>-iso set packet-file-name=
"http://<cw-ipv4-address>:30604/crosswork/imagesvc/v1/device/files/cw-image-id-d3930e13-b081-4905-b2e5-051249d9b0cb"

client <device-1-serial-num>-script create
client-policy <device-1-serial-num>-script set packet-file-name=
"http://<cw-ipv4-address>:30604/crosswork/configsvc/v1/configs/device/files/d1d7b441-3a27-47d1-aef0-39c3087d34c1"
client-policy <device-1-serial-num>-script setvendoroption 43 Cisco-ZTP "(1 exr-config) (2
0)"

### Device-2 Settings ###
client <device-2-serial-num>--iso create
client-policy <device-2-serial-num>-iso set packet-file-name=
"http://<cw-ipv4-address>:30604/crosswork/imagesvc/v1/device/files/cw-image-id-d3930e13-b081-4905-b2e5-051249d9b0cb"

```

```

client <device-2-serial-num>-script create
client-policy <device-2-serial-num>-script set packet-file-name=

"http://<cw-ipv4-address>:30604/crosswork/configsvc/v1/configs/device/files/d1640deb-8252-47b6-aab1-a843c0c7757b"
client-policy <device-2-serial-num>-script setvendoroption 43 Cisco-ZTP "(1 exr-config)(2
0)"

#
# Create more as needed using the above as models.
# Note: For those that need option 67 (boot file), you can use:
#   client-policy <name> setoption boot-file "<file-url>"
#
# The next line is optional. Uncomment it if you want to log what the script is doing.
# dhcp set log-settings+=incoming-packet-detail,outgoing-packet-detail,client-detail

# Assure that the server is up-to-date with this configuration
dhcp reload

```

Figure 20: IPv4 Script 2 of 3: ztp-v4-setup-vi-nrcmd.txt

```

#
# Create the scope
#
scope ztp-ncs-5501-mgmt create 192.0.20.0/24

# Add the dynamic range
scope ztp-ncs-5501-mgmt addrange 200 225

# Default the routers option. Note: No need to do subnet-mask. It is automatically provided.
scope-policy ztp-ncs-5501-mgmt setoption routers 10.10.10.1

# Set the lease time for clients on this scope
scope-policy ztp-ncs-5501-mgmt setoption dhcp-lease-time 216000
#
# Load the option 43 definitions
import option-set ztp-v4-option-set.txt
#
# Set the client classing expression and enable use of client-class
dhcp set client-class-lookup-id=@ztp-v4-client-class-expr.txt
dhcp enable client-class
#
# Load the client classes - these are used to lookup the correct client details
# depending on whether an iso or script is requested by the client.
client-class ztp-iso create
client-class ztp-iso set client-lookup-id="(or (try (concat (as-string
(request get option 61)) \"-iso\")) (request macaddress-string))"
#
client-class ztp-script create
client-class ztp-script set client-lookup-id="(or (try (concat (as-string
(request get option 61)) \"-script\")) (request macaddress-string))"
#
# Clients that are not ztp will fall into the ztp-none class
# and should not be offered service so they are excluded.
#
client-class ztp-none create
client-class ztp-none set action=exclude
#
# Create a default client that will prevent service to unknown clients.
client default create
client default set action=exclude
#
# Create some ZTP clients
#
# For each ZTP client we create two clients based on their serial number.
# (See above for the client-lookup-id expressions.)

```

```
# One has "-iso" added to the end that will be used when the client's
# request includes "iPXE" in option 77.
# The other has "-script" added to the end that will be used when the
# client's request includes "exr-config" in option 77.
#

### Device-1 Settings ###
client <device-1-serial-num>-iso create
client-policy <device-1-serial-num>-iso set packet-file-name=
"http://<cw-ipv4-address>:30604/crosswork/imagesvc/v1/device/files/cw-image-id-d3930e13-b081-4905-b2e5-051249d9b0cb"

client <device-1-serial-num>-script create
client-policy <device-1-serial-num>-script set packet-file-name=
"http://<cw-ipv4-address>:30604/crosswork/configsvc/v1/configs/device/files/d1d7b441-3a27-47d1-aef0-39c3087d34c1"
client-policy <device-1-serial-num>-script setvendoroption 43 Cisco-ZTP "(1 exr-config) (2
0)"

### Device-2 Settings ###
client <device-2-serial-num>--iso create
client-policy <device-2-serial-num>-iso set packet-file-name=
"http://<cw-ipv4-address>:30604/crosswork/imagesvc/v1/device/files/cw-image-id-d3930e13-b081-4905-b2e5-051249d9b0cb"

client <device-2-serial-num>-script create
client-policy <device-2-serial-num>-script set packet-file-name=
"http://<cw-ipv4-address>:30604/crosswork/configsvc/v1/configs/device/files/d1640deb-8252-47b6-aab1-a843c0c7757b"
client-policy <device-2-serial-num>-script setvendoroption 43 Cisco-ZTP "(1 exr-config) (2
0)"

#
# Create more as needed using the above as models.
# Note: For those that need option 67 (boot file), you can use:
#   client-policy <name> setoption boot-file "<file-url>"
#
# The next line is optional. Uncomment it if you want to log what the script is doing.
# dhcp set log-settings=+incoming-packet-detail,outgoing-packet-detail,client-detail

# Assume that the server is up-to-date with this configuration
dhcp reload
```

Figure 21: IPv4 Script 3 of 3: ztp-v4-client-class-expr.txt

```
(or
  (if (equal (as-string (request get-blob option 77)) "iPXE") "ztp-iso")
  (if (equal (as-string (request get-blob option 77)) "exr-config") "ztp-script")
  "ztp-none"
)
```

Figure 22: IPv6 Script 1 of 5: ztp-v6-setup-vi-nrcmd.txt

```
#
# create prefix for mgmt
prefix prefix-for-mgmt create 2001:DB8:10e:201a::/64
#
# Set the client classing expression and enable use
# of client-class
#
dhcp set v6-client-class-lookup-id=@ztp-v6-client-class-expr.txt
```

```

dhcp enable client-class
#
# Load the client classes - these are used to lookup the correct
# client details depending on whether an iso or script is requested
# by the client.
#
client-class ztp-iso create
client-class ztp-iso set v6-client-lookup-id=@ztp-v6-iso-lookup-expr.txt
#
client-class ztp-script create
client-class ztp-script set v6-client-lookup-id=@ztp-v6-script-lookup-expr.txt
client-class-policy ztp-script set v6-reply-options=17
#
# Delete option set (may not exist and ok if fails)
#
option-set dhcp6-cisco-custom delete
#
import option-set ztp-v6-options.txt
#
# Clients that are not ztp will fall into the ztp-none class
# and should not be offered service so they are excluded.
#
client-class ztp-none create action=exclude
#
# Create a default client that will prevent service to
# unknown clients.
#
client default create
client default set action=exclude
#
# Create some ZTP clients
#
# For each ZTP client we create two clients based on their mac-address.
# One has "-iso" added to the end that will be used when the client's
# request does not include the "exr-config" in option 77.
# The other has "-script" added to the end that will be used when the
# client's request does include "exr-config" in option 77.
#
client <device-serial-no>-iso create
# Set the vendor options using blob format as option definitions are for different data
client-policy <device-serial-no>-iso setV6VendorOption 17 dhcp6-cisco-custom "(1 exr-config) (2
0)"
# Escape the [ and ] as nrcmd (which uses tcl interpreter) will otherwise fail command
client-policy <device-serial-no>-iso setv6option bootfile-url
"http://\[cw-ipv6-address\]:30604/crosswork/imagesvc/v1/device/files/cw-image-id-aec596
a1-7847-4254-966a-2456aa5"
#
client <device-serial-no>-script create
# Set the vendor options using blob format as option definitions are for different data
client-policy <device-serial-no>-script setV6VendorOption 17 dhcp6-cisco-custom "(1
exr-config) (2 0)"
# Escape the [ and ] as nrcmd (which uses tcl interpreter) will otherwise fail command
client-policy <device-serial-no>-script setv6option bootfile-url
"http://\[cw-ipv6-address\]:30604/crosswork/configsvc/v1/configs/device/files/8eb6b7e1
-bd54-40bb-84e0-89f11a60128b"
#
#
# Assure the server is up-to-date with this configuration
dhcp reload

```

Figure 23: IPv6 Script 2 of 5: ztp-v6-client-class-expr.txt

```

(or (try (if (equal (as-string (request get option 15)) "exr-config") "ztp-script"))

```



```

        (try (if (equal (as-string (request get option 15)) "iPXE") "ztp-iso"))
        "ztp-none"
    )
)

```

Figure 24: IPv6 Script 3 of 5: ztp-v6-iso-lookup-expr.txt

```

(let (id)
  (setq id (request get option 1))
  (or
    # First try extracting the serial number from DUID
    (try (if (equali (substring id 0 6) 00:02:00:00:00:09)
      (concat (as-string (substring id 6 128)) "-script")
    )
    # If that fails, use normal client-id (DUID) lookup
    (concat (to-string id) "-iso")
  )
)
)

```

Figure 25: IPv6 Script 4 of 5: ztp-v6-script-lookup-expr.txt

```

(let (id)
  (setq id (request get option 1))
  (or
    # First try extracting the serial number from DUID
    (try (if (equali (substring id 0 6) 00:02:00:00:00:09)
      (concat (as-string (substring id 6 128)) "-script")
    )
    # If that fails, use normal client-id (DUID) lookup
    (concat (to-string id) "-script")
  )
)
)

```

Figure 26: IPv6 Script 5 of 5: ztp-v6-options.txt

```

# Option Definition Set Export/Import Utility
# Version: 1
#
{
  ( name = dhcp6-cisco-custom )
  ( desc = Cisco Systems, Inc. )
  ( vendor-option-enterprise-id = 9 )
  ( id-range = 2 )
  ( option-list = [
    {
      ( name = cisco-17 )
      ( id = 17 )
      ( base-type = AT_VENDOR_OPTS )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
      ( option-list = [
        {
          ( name = clientID )
          ( id = 1 )
          ( base-type = AT_NSTRING )
          ( sepstr = , )
          ( desc = ZTP - clientID )
        }
        {
          ( name = authCode )

```

```

( id = 2 )
( base-type = AT_INT8 )
( sepstr = , )
( desc = ZTP - authCode )
}
{
( id = 3 )
( name = md5sum )
( base-type = AT_NSTRING )
( desc = ZTP - md5sum )
}
{
( name = cnr-leasequery )
( id = 13 )
( base-type = AT_BLOB )
( flags = AF_IMMUTABLE )
( sepstr = , )
( option-list = [
{
( name = oro )
( id = 1 )
( base-type = AT_SHORT )
( flags = AF_IMMUTABLE )
( repeat = ZERO_OR_MORE )
( sepstr = , )
}
{
( name = dhcp-state )
( id = 2 )
( base-type = AT_INT8 )
( flags = AF_IMMUTABLE )
( sepstr = , )
}
{
( name = data-source )
( id = 3 )
( base-type = AT_INT8 )
( flags = AF_IMMUTABLE )
( sepstr = , )
}
{
( name = start-time-of-state )
( id = 4 )
( base-type = AT_TIME )
( flags = AF_IMMUTABLE )
( sepstr = , )
}
{
( name = base-time )
( id = 5 )
( base-type = AT_DATE )
( flags = AF_IMMUTABLE )
( sepstr = , )
}
{
( name = query-start-time )
( id = 6 )
( base-type = AT_DATE )
( flags = AF_IMMUTABLE )
( sepstr = , )
}
{
( name = query-end-time )
( id = 7 )

```

```

    ( base-type = AT_DATE )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = client-class-name )
    ( id = 8 )
    ( base-type = AT_NSTRING )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = partner-last-transaction-time )
    ( id = 9 )
    ( base-type = AT_TIME )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = client-creation-time )
    ( id = 10 )
    ( base-type = AT_TIME )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = limitation-id )
    ( id = 11 )
    ( base-type = AT_BLOB )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = binding-start-time )
    ( id = 12 )
    ( base-type = AT_TIME )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = binding-end-time )
    ( id = 13 )
    ( base-type = AT_STIME )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = fwd-dns-config-name )
    ( id = 14 )
    ( base-type = AT_NSTRING )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = rev-dns-config-name )
    ( id = 15 )
    ( base-type = AT_NSTRING )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = lookup-key )
    ( id = 16 )
    ( base-type = AT_BLOB )

```

```

        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = user-defined-data )
        ( id = 17 )
        ( base-type = AT_NSTRING )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = prefix-name )
        ( id = 18 )
        ( base-type = AT_NSTRING )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = failover-state-serial-number )
        ( id = 19 )
        ( base-type = AT_INT )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = reservation-key )
        ( id = 20 )
        ( base-type = AT_BLOB )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = failover-partner-lifetime )
        ( id = 21 )
        ( base-type = AT_STIME )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = failover-next-partner-lifetime )
        ( id = 22 )
        ( base-type = AT_STIME )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = failover-expiration-time )
        ( id = 23 )
        ( base-type = AT_STIME )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = client-oro )
        ( id = 24 )
        ( base-type = AT_SHORT )
        ( flags = AF_IMMUTABLE )
        ( repeat = ZERO_OR_MORE )
        ( sepstr = , )
    }
    ] )
}
{
    ( name = failover )

```

```

( id = 21 )
( base-type = AT_BLOB )
( flags = AF_NO_CONFIG_OPTION,AF_SUPPORTS_ENCAP_OPTION,AF_IMMUTABLE )
( sepstr = , )
( option-list = [
{
  ( name = server-state )
  ( id = 1 )
  ( base-type = AT_INT8 )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = server-flags )
  ( id = 2 )
  ( base-type = AT_INT8 )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = binding-status )
  ( id = 3 )
  ( base-type = AT_INT8 )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = binding-flags )
  ( id = 4 )
  ( base-type = AT_INT8 )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = start-time-of-state )
  ( id = 5 )
  ( base-type = AT_DATE )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = state-expiration-time )
  ( id = 6 )
  ( base-type = AT_DATE )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = failover-expiration-time )
  ( id = 7 )
  ( base-type = AT_DATE )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = bndupd-serial )
  ( id = 8 )
  ( base-type = AT_INT )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = bndack-serial )
  ( id = 9 )

```

```

    ( base-type = AT_INT )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
{
  ( name = client-flags )
  ( id = 10 )
  ( base-type = AT_INT )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = vpn-id )
  ( id = 11 )
  ( base-type = AT_INT )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = lookup-key )
  ( id = 12 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
  ( option-list = [
    {
      ( name = type )
      ( id = 0 )
      ( base-type = AT_INT8 )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = data )
      ( id = 0 )
      ( base-type = AT_BLOB )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
  ] )
}
{
  ( name = user-defined-data )
  ( id = 13 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
}
{
  ( name = reconfigure-data )
  ( id = 14 )
  ( base-type = AT_BLOB )
  ( flags = AF_IMMUTABLE )
  ( sepstr = , )
  ( option-list = [
    {
      ( name = time )
      ( id = 0 )
      ( base-type = AT_DATE )
      ( flags = AF_IMMUTABLE )
      ( sepstr = , )
    }
    {
      ( name = key )

```

```

        ( id = 0 )
        ( base-type = AT_BLOB )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
] )
}
{
    ( name = requested-fqdn )
    ( id = 15 )
    ( base-type = AT_BLOB )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
    ( option-list = [
        {
            ( name = flags )
            ( id = 0 )
            ( base-type = AT_INT8 )
            ( flags = AF_IMMUTABLE )
            ( sepstr = , )
        }
        {
            ( name = domain-name )
            ( id = 0 )
            ( base-type = AT_DNSNAME )
            ( flags = AF_IMMUTABLE )
            ( sepstr = , )
        }
    ] )
}
{
    ( name = forward-dnsupdate )
    ( id = 16 )
    ( base-type = AT_NSTRING )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = reverse-dnsupdate )
    ( id = 17 )
    ( base-type = AT_NSTRING )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = partner-raw-cltt )
    ( id = 18 )
    ( base-type = AT_DATE )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = client-class )
    ( id = 19 )
    ( base-type = AT_NSTRING )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}
{
    ( name = status-code )
    ( id = 20 )
    ( base-type = AT_BLOB )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
}

```

```

    ( option-list = [
      {
        ( name = status-code )
        ( id = 0 )
        ( base-type = AT_SHORT )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
      }
      {
        ( name = status-message )
        ( id = 0 )
        ( base-type = AT_NSTRING )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
      }
    ] )
  }
  {
    ( name = dns-info )
    ( id = 21 )
    ( base-type = AT_BLOB )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
    ( option-list = [
      {
        ( name = flags )
        ( id = 0 )
        ( base-type = AT_SHORT )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
      }
      {
        ( name = host-label-count )
        ( id = 0 )
        ( base-type = AT_INT8 )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
      }
      {
        ( name = name-number )
        ( id = 0 )
        ( base-type = AT_INT8 )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
      }
    ] )
  }
  {
    ( name = base-time )
    ( id = 22 )
    ( base-type = AT_DATE )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = relationship-name )
    ( id = 23 )
    ( base-type = AT_NSTRING )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = protocol-version )
    ( id = 24 )
  }

```



```

    ( base-type = AT_INT )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = mclt )
    ( id = 25 )
    ( base-type = AT_INT )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = dns-removal-info )
    ( id = 26 )
    ( base-type = AT_BLOB )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
    ( option-list = [
      {
        ( name = host-name )
        ( id = 1 )
        ( base-type = AT_RDNSNAME )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
      }
      {
        ( name = zone-name )
        ( id = 2 )
        ( base-type = AT_DNSNAME )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
      }
      {
        ( name = flags )
        ( id = 3 )
        ( base-type = AT_SHORT )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
      }
      {
        ( name = forward-dnsupdate )
        ( id = 4 )
        ( base-type = AT_NSTRING )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
      }
      {
        ( name = reverse-dnsupdate )
        ( id = 5 )
        ( base-type = AT_NSTRING )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
      }
    ] )
  }
  {
    ( name = max-unacked-bndupd )
    ( id = 27 )
    ( base-type = AT_INT )
    ( flags = AF_IMMUTABLE )
    ( sepstr = , )
  }
  {
    ( name = receive-timer )

```

```

        ( id = 28 )
        ( base-type = AT_INT )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = hash-bucket-assignment )
        ( id = 29 )
        ( base-type = AT_BLOB )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = partner-down-time )
        ( id = 30 )
        ( base-type = AT_DATE )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = next-partner-lifetime )
        ( id = 31 )
        ( base-type = AT_DATE )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = next-partner-lifetime-sent )
        ( id = 32 )
        ( base-type = AT_DATE )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    {
        ( name = client-oro )
        ( id = 33 )
        ( base-type = AT_SHORT )
        ( flags = AF_IMMUTABLE )
        ( repeat = ZERO_OR_MORE )
        ( sepstr = , )
    }
    {
        ( name = requested-prefix-length )
        ( id = 34 )
        ( base-type = AT_INT8 )
        ( flags = AF_IMMUTABLE )
        ( sepstr = , )
    }
    ] )
}
] )
}

```

Trigger ZTP Device Bootstrap

With device entries imported to Cisco Crosswork and DHCP configured, you can initiate ZTP processing by restarting each of the devices.

Before you begin

Before triggering ZTP bootstrap on any of your devices, ensure that you have finished:

- All of the preliminary setup tasks explained in [ZTP Setup Workflow, on page 28](#).
- Creating ZTP device entries for the devices you want to bootstrap, as explained in [Prepare ZTP Device Entry Files, on page 53](#) and [Prepare Single ZTP Device Entries, on page 59](#).
- DHCP (and TFTP, if using PnP ZTP) setup, as appropriate for your choice of ZTP mode, as explained in the corresponding topic in [Set Up DHCP for ZTP, on page 60](#).

If you are using Secure ZTP:

1. Telnet to the console on each of the device(s) you want to onboard: `telnet <device IP> <userID><password>`.
2. Check if Secure ZTP is enabled on the device:
 - a. For IOS-XR versions 7.5.2 or earlier: Enter Bash run mode and issue the following command:
`[xr-vm_node:~]$pyztp2 --ztp-mode ZTP Mode: Secure`
 - b. For IOS-XR versions later than 7.5.2: Go to the IOS CLI command prompt and enter the following command `show ztp information`.

3. Issue the following commands to clean logs and configurations:

```
ios#ztp clean

ios#config terminal

ios(config)#commit replace

ios(config)#end
```

If you are using PnP ZTP: Be sure to set the minimum license boot-level on each IOS-XE device to **metroipaccess** or **advancedmetroipaccess** before you trigger ZTP processing. If the boot level has been set properly, the output of the IOS-XE `#sh run | sec license` CLI command on the device should contain statements showing either of these two license levels: `license boot level advancedmetroipaccess` or `license boot level metroipaccess`. If the command output shows any other license level lower than these two, the Cisco PnP cryptographic functionality will not be enabled. This will cause certificate installation to fail, which will then cause PnP ZTP device provisioning to fail.

Procedure

Step 1 Initiate ZTP processing as appropriate for the ZTP mode you are using:

- For Classic ZTP, use one of these options:
 - Power-cycle the device to restart it.
 - Using a pin, press the chassis reset button at the back of the device. Press for 15 seconds, or until the power light on the device starts flashing.
 - For a previously imaged device: Connect to the device console via Telnet, then issue the **ztp initiate** command.

- For Secure ZTP, use one of these options:
 - Power-cycle the device to restart it.
 - Using a pin, press the chassis reset button at the back of the device. Press for 15 seconds, or until the power light on the device starts flashing.
 - For a previously imaged device: Connect to the device console via Telnet, then issue the following commands (the `ztp initiate interface` value given here starts Secure ZTP on the device management port):

```
ztp enable noprompt
```

```
ztp initiate debug verbose interface MgmtEth 0/RP0/CPU0/0
```

- For PnP ZTP, use the option appropriate for your devices:
 - On Cisco ASR 903, ASR 907, and NCS 520 devices: Connect to it via Telnet, then issue a **write erase** command, followed by a **reload** command.
 - On Cisco ASR 920 devices: Press the ZTP button on the chassis for 8 seconds.

Repeat this step as needed for each of the devices you plan to provision during this session. You can restart all or as few devices as needed during a single session.

Step 2

Monitor the progress of ZTP processing using the Zero Touch Provisioning status tile shown in the following figure. To view the tile, click the **Dashboard** on the main menu.



The tile provides a summary view of your current ZTP processing status. It gives a count of all the ZTP profiles, images, and configuration files currently in use. The tile also shows the number of devices in each of the possible ZTP processing states.

Complete Onboarded ZTP Device Information

The ZTP devices, once onboarded, are automatically part of the shared Crosswork Network Controller device inventory. You can edit them like any other device. The following steps explain two ways to add information to devices onboarded using ZTP.

Before editing any device, it's always good practice to export a CSV backup of the devices you want to change. You can do this using the export function described in Step 2.

Before you begin

Some information needed for a complete device inventory record is either not necessary or not available via automation. For example: Geographical data, indicating that a device is located in a building at a given address, or at a set of GPS coordinates.

Other types of inventory information are useful when managing your network with different tools and functionalities. For example, using tags makes it easier to apply specific performance metrics to individual devices. Similarly, associating policies with devices streamlines integration with network management or optimization processes. Additionally, certain network management solutions leverage this extended device information to enhance automation and simplify operational tasks.

You can add this kind of information using functions in the other Crosswork Network Controller applications and providers. For more information on this topic, see the user documentation for the application. You can also add much of it using ZTP.

Procedure

Step 1 To update the inventory record for a ZTP device:

- a) From the main menu, choose **Device Management > Zero Touch Provisioning > Devices**.
- b) Select the device you want to change, then click .
- c) Change the value of the **Status** field to **Unprovisioned**.
- d) Edit the other values configured for the device, as needed.
- e) Click **Save**.

Step 2 To update the inventory records for devices in bulk, including devices onboarded using ZTP:

- a) From the main menu, choose **Device Management > Zero Touch Provisioning > Devices**.
 - b) Click . Save the CSV file.
 - c) Open the CSV template with the application of your choice and edit the device information you want to add or update. It's a good idea to delete rows for devices you don't want to update.
 - d) When you're finished, save the edited CSV file.
 - e) Click .
 - f) Click **Browse** to navigate to the CSV file you created and then select it.
 - g) With the CSV file selected, click **Import**.
-

Reconfigure Onboarded ZTP Devices

The purpose of ZTP is to onboard new devices quickly and easily, without requiring you to send experts to the same site as the new devices. ZTP performs imaging and configuration as part of that task, and can run scripts as part of device configuration. However, it is not designed as an all-purpose device configuration utility, and shouldn't be used in that way.

If you must reconfigure a device onboarded using ZTP, use:

- A Change Automation Playbook, which allows you to roll out configuration changes to devices on demand.
- The configuration change functions of Cisco Network Services Orchestrator (Cisco NSO), or any of the other Cisco Crosswork providers you're using.
- A direct connection to the device and the device OS CLI.

If you can't use any of these methods, the best approach is to delete the device. You can onboard the device again, this time with the correct configuration.

To delete a ZTP device, select **Device Management > Devices > Zero Touch Provisioning > Devices**, select the device in the table, then click .

Retire or Replace Devices Onboarded with ZTP

Sometimes you must retire a Cisco device that was onboarded using ZTP. Device licenses are associated with the device serial number that you entered at the time of onboarding. ZTP permits the association of a single device with up to three different serial numbers. You can use this fact to remove a failed or obsolete device from your network and from Crosswork Network Controller inventory. You can replace it later without consuming an extra license.

This rule applies not only to devices with a chassis, but also to line cards and other pluggable device modules. Each of these modules has its own serial number. If you must RMA a module, associate the old license with the serial number of the new module. But first remove the old line card and its serial number from the inventory, as explained in the following steps.

1. Select **Device Management > Zero Touch Provisioning > Devices**.
2. Find the old device in the table and make a record of its serial number.
3. Select the device and then click  to delete it.

After you delete the device, Crosswork Network Controller will still count the license that is associated with this serial number as consumed. Track this license as part of any new or RMA replacement device purchase, so you can return the license for the old device to active use.

Crosswork Network Controller won't allow two active devices with the same license. Delete the old device before you can onboard a new or replacement device.

4. When it's time to onboard the new device:
 - a. When you create a ZTP device entry for the new device, enter both the new and old serial numbers.

- b. If you're using Secure ZTP: Submit both the old and new device serial numbers with the Ownership Voucher request for the new device. Crosswork Network Controller associates the old and new serial numbers with the in-use license in the regenerated Ownership Voucher.
- c. Onboard the new device as you would any other ZTP device. Only the old device license is consumed.

ZTP Asset Housekeeping

When you have completed onboarding your devices with ZTP, you can delete offline copies of some of the ZTP assets you assembled. Retain others, depending on the policies and best practices of your organization. We recommend:

- **ZTP profiles:** Usually, it's safe to delete ZTP profiles after onboarding is complete. To delete a ZTP profile, select **Device Management > Zero Touch Provisioning > ZTP profiles**. On the tile representing the ZTP profile you want to delete, click  and then select **Delete** from the dropdown menu.
- **ZTP device entry CSV file:** You may want to retain an offline copy of this file for use as a template. This file can be handy if, say, you have many branch offices sharing the same network architecture and device types. Otherwise, you can simply delete it from the file system. You can download the CSV file template at any time. You may find it more useful to export a backup CSV file containing all the data for your ZTP devices, including data you entered after onboarding. To export a CSV device backup, select **Device Management > Zero Touch Provisioning > Devices**. Then click  and save the CSV file.
- **Software images and SMUs:** Save the production versions of these files offline, and delete older ones per the policies of your organization. Don't delete the uploaded image files from Cisco Crosswork if you plan to use them to image more devices of the same family. To delete obsolete images, select **Device Management > Software Management**, select the file in the table, then click .
- **Configuration files:** You need not retain configurations you already uploaded to Cisco Crosswork, but the policy of your organization may differ. Don't delete uploaded configuration files if you plan to configure more devices of the same family using ZTP. When configurations change, you can easily update the stored version. Prepare the new configuration file or script, select **Device Management > Zero Touch Provisioning > Configuration files**, select the file in the table, and then click . You can then browse to the new script file you created, and copy/paste the new configuration. If a configuration becomes obsolete, delete it: Select **Device Management > Zero Touch Provisioning > Configuration files**, select the file in the table, then click .
- **Credential profiles:** You can delete an imported credential profile CSV file immediately. Don't delete the uploaded credential profiles. When user names and passwords change, update the credential profiles: Select **Device Management > Credentials**, select the credential profile in the table, then click .

Troubleshoot ZTP Issues

Normally, ZTP provisioning and onboarding happen quickly and automatically. Issues do occur at times, so the following topics explain how to diagnose and remedy issues, including common issues and issues specific

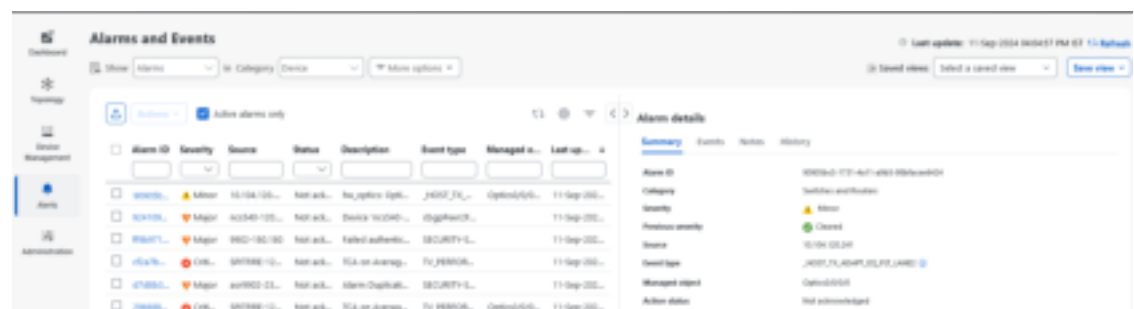
to ZTP modes. For reference, this section also supplies a comprehensive index of ZTP errors indicated in Crosswork alarms or events.

Diagnose ZTP Issues Using the Alarms Window

You can use the Crosswork Alarms window to view summary and detail information for any ZTP-related error, whether propagated as an alarm or an event. The alarm details contain information about the likely cause of the error and, where appropriate, how to recover from it.

1. Select **Administration > Alerts** to display the **Alarms and Events** window.
2. If the ZTP error is propagated only as an event: From the Show drop-down, choose **Events** to view the event. If the event has a correlated alarm, view the **Correlated** column. To view the details for the correlated alarm, click the event ID.
3. For ZTP errors propagated as alarms: From the Show drop-down, choose **Alarms** to view the alarms. Click the alarm in the Alarms ID column to view the ZTP error whose details you want to see. The **Alarms** window displays **Alarm details** on the right panel, as shown in the illustration below.

Figure 27: Alarms View with Detail Window



For a comprehensive list of ZTP errors and how they are propagated, see [Troubleshoot ZTP: Alarms and Events Reference, on page 92](#).

Diagnose ZTP Issues Using the Status Column

You can use the **Devices** tab on the **Zero Touch Provisioning** window to view summary and detail information for any ZTP-related error. The alarm details contain information about the likely cause of the error and, where appropriate, how to recover from it.

1. Select **Device Management > Zero Touch Provisioning > Devices**. The **Devices** window displays a list of all the devices that were onboarded using ZTP.

The **Status** column displays the  next to every device entry which ZTP processing finished with a **Provisioning Error**, **Onboarding Error** or (for Secure ZTP only) **ZTP Error**.

2. Click  to display a pop-up window with information about the error, like the one shown in the following example.

Figure 28: Error pop-up window



For a comprehensive list of ZTP-related errors, see [Troubleshoot ZTP: Alarms and Events Reference](#), on page 92.

Diagnose ZTP Issues Using Error Logs

You can diagnose ZTP issues by viewing ZTP error logs. You can view or request error logs directly from the Crosswork user interface, using a `showtech` request. You can also download error logs using an SSH login to one or more of the virtual machines running Crosswork and the instance of the Crosswork ZTP service running on that VM.

To view or request copies of ZTP error log files using a `showtech` request from the Crosswork user interface, follow these steps:

1. Using an ID with administrator privileges, log into the Crosswork user interface.
2. Select **Administration > Crosswork Manager**.
3. With the **Crosswork Summary** page displayed, click on the **Element Management Functions** tile. Crosswork displays details for ZTP.
4. With the application details displayed, select **Showtech options > Request logs**. Then select **Showtech requests**. You can retrieve your log files from the dashboard when the request is completed.

You can also choose to simply view the most recent log files by selecting **Showtech options > View Showtech logs**.



Tip If ZTP processing seems to be completing successfully but you are having issues with the onboarding phase, you may want to see logs for the Crosswork device inventory manager application (known as `dlminvmgr`) in addition to the logs for the ZTP service. You can do that by selecting **Platform Infrastructure** instead of **Element Management Functions** on the **Crosswork Summary** page (during step 3, above).

To download error log files from the Crosswork ZTP service, follow these steps:

1. Log in to the VM using an Secure Shell command like the following:

```
ssh admin@VMIP
```

Where:

- `admin` is the Crosswork administrator ID. For example: `cw-admin`.
- `VMIP` is the IP address of the virtual machine running Crosswork. For example: `192.168.100.102`.

2. Access the `cw-ztp-service` Kubernetes pod using a command like the following:

```
# kubectl exec -it PodID# bash
```

Where `PodID#` is the ID of the `cw-ztp-service` Kubernetes pod. Change the pod ID number as needed to match the number of the pod you want to access (pod 0 is always the first). For example: `cw-ztp-service-0`, `cw-ztp-service-1`, `cw-ztp-service-2`, and so on.

3. Change to the log folder with a command like the following: `cd /var/log/robot/`. You can then open any of the following ZTP-specific files in the folder:

- `cw-image-service_stdout.log`
- `cw-image-service_stderr.log`
- `cw-config-service_stdout.log`
- `cw-config-service_stderr.log`

Troubleshoot Common ZTP Issues

The following table identifies remedies for common issues that can occur with any of the ZTP modes. For details on ZTP processing for all three ZTP modes, see [ZTP Processing Logic, on page 24](#).

Table 8: Common ZTP Issues and Remedies

Phase	Issue	Symptoms	Remedy
Setup	Image, configuration, or SMU file upload fails	Error messages displayed in the user interface during upload	Make sure that the MD5 checksum for the file is correct. If the file information is correct, image uploads can still fail due to slow network connections. If you're running into this problem, retry the upload.
	Uploaded files aren't in the drop-down menu when creating ZTP device entries or ZTP profiles	Files missing from the dropdown list	The drop-down menu selects files based on the device family and IOS release number you specify in your device entry or ZTP profile. Make sure that the file information matches the information for the device entry or profile you're creating.
	Errors during device entry CSV file import	Varies; see error log	If devices in inventory have the same serial numbers as the devices you're importing, check that the devices are in the Unprovisioned state before import. All the devices imported using CSV files have their status set to Unprovisioned on import. Before import, make sure the configurations, images, and ZTP profiles mentioned in the CSV file exist. You can edit device image and configuration files by exporting a device CSV file and reimporting it with changes. If you use this edit method, make sure the CSV file has the correct UUIDs before import.
Unprovisioned	DHCP is unresponsive or offer execution fails	ZTP processing hangs	Test access to the DHCP server from the Cisco Crosswork server, using ping and similar tools

Phase	Issue	Symptoms	Remedy
In Progress	Image or SMU file download fails	ZTP processing hangs	Check that there's network connectivity between Cisco Crosswork and the device. Make sure that the device is getting its IP address from the DHCP server. Ensure that the image ID of the software image given in the configuration file of the DHCP server is correct. If you must correct the image ID specified in the configuration file, make sure you restart the DHCP server before initiating ZTP processing again.
	Configuration file download fails	Logged errors	Check that there's network connectivity between Cisco Crosswork and the device. Make sure that the device is getting its IP address from the DHCP server. Ensure that the image ID of the software image given in the DHCP server configuration file is correct. If you must correct the image ID specified in the DHCP configuration file, make sure you restart the DHCP server before re-initiating ZTP processing. Make sure that the device serial number matches the serial number on the chassis of the device. Ensure that the status of the device is either Unprovisioned or In Progress before initiating ZTP processing. Configuration downloads continue to fail as long as the device is in any other state.
Onboarded	Device state is showing Onboarded and not Provisioned	Status column did not show Provisioned	Provisioned is an intermediate state in ZTP processing. When the device state changes to Provisioned , Cisco Crosswork attempts to onboard the device immediately. The status changes to Onboarded or Onboarding Error after.
	Onboarding Error	Status column shows Onboarding Error	The default Cisco Crosswork device life-cycle management (DLM) policy for identifying devices uniquely is the IP address. If you import a new device with an IP address that matches an existing device, the device status changes to Provisioned, then to Onboarding Error. If the IP address of the new device is blank, you get the same result. These same issues apply if your installation uses an OSPF ID, ISIS ID, or other DLM policy for determining device IDs. Onboarding can only succeed when you fill all the DLM policy fields with unique, non-blank values. If onboarding fails, inspect the popup error message, update the corresponding fields and retry onboarding.

Troubleshoot Classic ZTP Issues

The following table identifies remedies for issues that can occur during Classic ZTP processing. For details on processing steps during each phase of Classic ZTP processing, see [ZTP Processing Logic, on page 24](#).

Table 9: Classic ZTP Issues and Remedies

Phase	Issue	Symptoms	Remedy
Unprovisioned	Crosswork cannot verify the device serial number	Status column does not show "In Progress"	ZTP supports addition of multiple serial numbers irrespective of how many devices there are to be added. While creating a device entry, make sure to assign the correct serial number. ZTP is initiated based on the serial number, and the connected device entry will start to show state changes based on it.
In Progress	Boot script execution fails	Processing hangs. See error log.	Examine the boot script for errors, correct them and try again.
	iPXE reload fails	Processing hangs. See error log.	This is likely due to an temporary issue with the device. Try again. If the process fails repeatedly, contact the Cisco device support team.
Unprovisioned, In Progress	Device progress report API call fails	Processing hangs. See error log.	Make sure the API call is properly formatted and has correct values. Correct them and try again. May also be the result of temporary connectivity loss due to network issues.

Troubleshoot PnP ZTP Issues

The following table identifies remedies for issues that can occur during PnP ZTP processing. For details on steps during each phase of PnP ZTP processing, see [ZTP Processing Logic, on page 24](#).

Table 10: PnP ZTP Issues and Remedies

Phase	Issue	Symptoms	Remedy
Unprovisioned	PnP profile download fails	Device stays in Unprovisioned state	The download may have failed due to packets being dropped or similar network traffic issues. First ensure that the PnP profile has the correct file name, protocol, IP address, and port specified. Ensure that the TFTP server is up and reachable. Then try triggering ZTP from the device again.
Unprovisioned, In Progress	Capability service request fails	ZTP device entry is moved to error state with the message "service 'capability check' failed". Reason: Device doesn't support the minimum required capabilities.	For PnP ZTP to work, the XE device being provisioned must support the following minimum Cisco IOS-XE capabilities: • device-info • certificate-install • image-install • config-upgrade • backoff If you are having trouble with this requirement, contact the Cisco device support team.
In Progress	Certificate install fails	ZTP device goes into error state with the message "certificate installation service failed."	First, log in to the XE device and clean up trustpoint "CrossworkPnP" if it already exists. Then, from the Crosswork GUI, move the device back to the UnProvisioned state and re-trigger ZTP from the beginning.

Troubleshoot ZTP: Alarms and Events Reference

To view the supported alarms and events within ZTP, access the [Cisco Crosswork Supported Alarms and Events](#). This document contains a detailed list of the alarms and events that are compatible with the Cisco Crosswork platform.



PART II

Manage Devices

- [View and Manage Devices, on page 95](#)
- [Use Templates to Configure Similar Devices, on page 129](#)
- [Configuration Backup and Restore, on page 147](#)
- [Manage Software Images, on page 153](#)



CHAPTER 3

View and Manage Devices

This section contains the following topics:

- [Manage onboarded devices, on page 95](#)
- [Use Device Groups to Filter your Topology Map, on page 102](#)
- [View Device Details from the Topology Map, on page 106](#)
- [Get Details About Topology Links, on page 113](#)
- [View the network inventory, on page 120](#)
- [View Device Job History, on page 124](#)
- [Manage Port Groups, on page 125](#)

Manage onboarded devices

The **Network Devices** window gives you a consolidated list of all your devices that you have onboarded, and their status.

To view the **Network Devices** window, select **Device Management > Network Devices** from the main menu.

Figure 29: Network Devices

IP address	Host name	Admin state	Operational state	Link status	Last updated time	Product type	Software type	Software version
10.10.10.1	10.10.10.1	On	Up	Up	20-Aug-2020 10:10:10	10.10.10.1	10.10.10.1	10.10.10.1
10.10.10.2	10.10.10.2	On	Up	Up	20-Aug-2020 10:10:10	10.10.10.2	10.10.10.2	10.10.10.2
10.10.10.3	10.10.10.3	On	Up	Up	20-Aug-2020 10:10:10	10.10.10.3	10.10.10.3	10.10.10.3
10.10.10.4	10.10.10.4	On	Up	Up	20-Aug-2020 10:10:10	10.10.10.4	10.10.10.4	10.10.10.4

Clicking on the IP address link of a device displays information about each device in the pop-up window.

- A **Details** tab with device specifications, onboarding time, connectivity details, routing information and detailed inventory collection. On this tab, devices with a supported SysOID are marked as *Certified*. If

the SysOID is missing from the certified list, the support type is *Uncertified*. Incomplete discovery or no CDG connection sets it to *Unknown*.

Refer to the [Cisco Crosswork Network Controller Essentials Supported Devices](#) for a list of supported OIDs for devices.

- An **Alarms** tab with detailed information on alarms, including their severity, the source (Syslog, Trap, or gNMI), the category, and the current condition of each alarm. The tab allows you to customize the displayed columns.
- An **Inventory** tab displaying the product name, product ID, admin status, operational status, and serial number. You can customize the columns according to your preferences.



Note A component of a device lacking a serial number is not displayed in the **Inventory** tabs within the Crosswork UI. Additionally, the tree structure in the **Detailed Inventory** window also excludes components without serial numbers.

- A **History** tab with detailed information about device performance, including various performance metrics.



Note Average values for all performance metrics are displayed under the **History** tabs in the Crosswork Network Controller UI. However, the relevance of the average values may vary across different metrics. Assess the context of each metric before using the average values in your analysis.

Within the **Network Devices** window, you can perform the following tasks:

- [Monitor Device States, on page 96](#)
- [Filter Network Devices by Tags, on page 98](#)
- [Edit Devices, on page 99](#)
- [Delete Devices, on page 100](#)
- [View Detailed Inventory Collection Status, on page 100](#)
- [Enable or Disable Granular Inventory, on page 101](#)
- [Perform detailed inventory sync, on page 102](#)

For controlling or restricting device access for users, see the section **Manage Device Access Groups** in the *Cisco Crosswork Network Controller 7.1 Administration Guide*.

Monitor Device States

Cisco Crosswork Network Controller computes the reachability state of the devices it manages, as well as the operational and NSO states of reachable managed devices. It indicates these states using the icons in the following table. By monitoring the reachability and operational states of devices, you can get real-time

information about their connectivity status, enabling you to quickly identify and resolve any connectivity issues.

At the top of the **Network Devices** window, you can view a summary of the reachability status of your devices. Additionally, the list of devices displays the reachability state, admin state, and operational state for each device.

Table 11: Device Status Icons

This Icon...	Indicates...
Reachability State icons indicate if a device is reachable. This state is computed when the device is configured as UP. It is not computed if the device is DOWN or UNMANAGED. • REACHABLE: At least one route and the device is discoverable. • UNREACHABLE: No routes or the device does not respond. • UNKNOWN: The device is UNMANAGED.	
	Reachable: The device can be reached by all configured protocols.
	Reachability Degraded: The device can be reached by at least one protocol, but is not reachable by one or more of the other protocols configured for it.
	Unreachable: The device cannot be reached by any protocol configured for it.
	Reachability Unknown: Crosswork Network Controller cannot determine if the device is reachable.
Operational State icons show if a device is operational. • Computed only if the device is UP, not if DOWN or UNMANAGED. • It can be either OK or ERROR. • Operational=OK if the device is REACHABLE and discoverable; otherwise, it is ERROR.	
	The device is operational and under management, and all individual protocols are "OK" (also known as "up").
	The device is not operational ("down"). The same icon is used when the device has been set "administratively down" by an operator.
	The device's operational state is unknown.
	The device's operational state is degraded.
	The device's operational state is in an error condition. It is either not up, or unreachable, or both, due to errors encountered while attempting to reach it and compute its operational state. The number in the circle shown next to the icon indicates the number of recent errors. Click on the number to see a list of these errors. (Note that the icon badging for errors is not available in the topology map.)

This Icon...	Indicates...
	The device's operational state is currently being checked.
	The device is being deleted.
	The device is unmanaged.
NSO State icons show whether a device is synced with Cisco NSO. Note In the initial sync between Crosswork Network Controller and NSO after onboarding a device, the NSO state column in the device remains blank. This occurs because Crosswork has not determined if the device needs to sync with NSO based on the policy, and cannot select the default state in the initial sync.	
	The device is in sync with Cisco NSO.
	The device is out of sync with Cisco NSO.

**Note**

- For XR or XE devices only, Operational=OK also requires that clock drift difference between the Crosswork Network Controller host and the device clocks is less than or equal to the default drift value of 2 minutes.
- Some timezone settings are known to result in clock drift errors when no clock drift actually exists. To work around this issue set your devices to use UTC time.

Filter Network Devices by Tags

By creating a tag and assigning it to a particular device, you can easily provide additional information that might be of interest to other users, such as the device's physical location and its administrator's email ID. You can also use tags to find and group devices with the same or similar tags in any window that lists devices.

To filter devices by tags:

Procedure

- Step 1** From the main menu, choose **Device Management > Network Devices**.
- Step 2** In the **Type to filter by tags** bar at the top of the user interface, type all or part of the name of a tag.
The **Type to filter by Tags** bar has a type-ahead feature: As you start typing, the field shows a drop-down list of tags that match all the characters you have typed so far. To force the drop-down list to display all available tags, type *****.
- Step 3** Choose the name of the tag you want to add to the filter. The filter appears in the **Type to filter by tags** filter bar. The table or map shows only the devices with that tag.
- Step 4** If you want to filter on more than one tag:

- a) Repeat Steps 2 and 3 for each additional tag you want to set as part of the filter.
- b) When you have selected all the tags you want, click **Apply Filters**. The table or map shows only the devices with tags that match **all** the tags in your filter.

Step 5 To clear all tag filters, click the **Clear Filters** link. To remove a tag from a filter containing multiple tags, click the **X** icon next to that tag's name in the filter.

To see how tags can be managed for assignment to the devices in your network, refer to the section **Manage Tags** in the *Cisco Crosswork Network Controller 7.1 Administration Guide*.

Edit Devices

Editing a device allows you to modify various device settings for onboarded devices. Ensure that you have administrative access and consider any network impact when you make changes. For a list of the fields you can edit, see the "Add New Device" field table in [Add devices through the UI, on page 11](#).

These are the steps of updating a device's information.

Before you begin

Before editing any device, it is always good practice to export a CSV backup of the devices you want to change.

Procedure

Step 1 From the main menu, choose **Device Management > Network Devices**.

Step 2 (Optional) Filter the list of devices by filtering specific columns.

Step 3 Select the check box of the device you want to change, then click .

Step 4 Edit the values configured for the device, as needed.

Note

- User-configured parameters like ISIS System ID and OSPF Router ID are not autodiscovered by Crosswork Network Controller for onboarded devices. These fields may appear blank when you edit the device, however, the topology page for the same device displays the parameters.
- In addition to the existing fields, you can also view the **Data Gateway** configured for the selected device. This field is read-only.
- The TE Router ID should not be changed after importing or onboarding a device. If it is necessary to change the TE Router ID, follow these steps:
 - a. Remove the device from Crosswork Network Controller.
 - b. Remove all SR-PCE Providers.
 - c. Onboard the device again with the new TE Router ID.
 - d. Add the SR-PCE providers again.
 - e. Update the TE Router ID under the **Routing info** segment.

Step 5 Click **Save**. The **Save** button remains dimmed until all required fields are completed.

Step 6 Resolve any errors and confirm device reachability.

Delete Devices

When you delete a device from Crosswork Network Controller, it is removed from its monitoring and management framework. You might delete a device if it is being withdrawn, reassigned, replaced, or if it was added by mistake.

Complete the following procedure to delete the devices.

Before you begin

- Export a backup CSV file containing the devices that you plan to delete.
- If you set the **auto-onboard** property as **managed** or **unmanaged** for an SR-PCE provider, set **auto-onboard** as **off** for one or more SR-PCEs.
- Confirm that the device is disconnected and powered off before deleting the device.
- If devices are mapped to Cisco NSO with MDT capability, and a telemetry configuration is pushed, then those configurations will be removed from the device.
- If **auto-onboard** is not **off** and it is still functional and connected to the network, the device will be rediscovered as unmanaged when it is deleted.

Procedure

Step 1 From the main menu, choose **Device Management > Network Devices**.

Step 2 (Optional) In the **Devices** window, filter the list of devices by entering text in the **Search** field or filtering specific columns.

Step 3 Check the check box for the devices that you want to delete.

Step 4 Click the .

Step 5 In the confirmation dialog box, click **Delete**.

View Detailed Inventory Collection Status

Cisco Crosswork Network Controller computes the detailed inventory collection status of the devices it manages. At the top of the **Network Devices** window, you can view a summary of the detailed inventory collection status for your devices. Additionally, when you click on a device's link, you can view the detailed inventory collection information under the **Details** tab.

It indicates the status of a device using the icons in the following table.

Table 12: Inventory Collection Status

This Icon	Indicates
	Completed: The device inventory collection process has finished.
	Failed: The device inventory collection process has encountered an error and did not complete.
	In Progress: The device inventory collection is in progress and the system is currently in the process of collecting and updating inventory data for network elements.
	Maintenance: Operation for detailed inventory collection is suspended. It may not be possible to initiate new inventory collection processes, or the data displayed might not reflect the most recent state of the network elements.
	Warning: The inventory collection process has encountered some issues that may not have completely prevented the process from completing but could still affect the accuracy or completeness of the data collected. After addressing the causes of the warnings, the inventory collection process may need to be rerun to confirm that all issues have been resolved and that the collected data is both accurate and complete.

Enable or Disable Granular Inventory

Granular inventory in Cisco Crosswork Network Controller provides detailed device data for enhanced monitoring and troubleshooting. While enabling it offers deeper insights and supports proactive maintenance, it can also consume significant system resources and storage. Disabling it can improve performance, especially in large networks.

The inventory sync process includes several automated steps. A nightly sync updates the inventory system, while any failed features for devices prompt a sync attempt every 30 minutes. Newly added devices in the UP state and existing devices transitioning from DOWN to UP state also trigger inventory syncs. The automatic synchronization occurs when there are configuration or state changes on a device. The device notifies these changes through traps or syslogs.

You can enable the granular inventory at the device level by selecting the required device in the **Network Devices** page, and then choosing **Actions > Enable Granular Inventory**.

To disable granular inventory, choose **Actions > Disable Granular Inventory**. This will disable the granular inventory for the selected device only, and will not impact the granular inventory processing of any other devices in the system.

You can apply these actions to multiple devices simultaneously, but all selected devices must be in the same state (either all enabled or all disabled) for these options to be available.

Perform detailed inventory sync

Perform a detailed inventory sync to maintain an up-to-date view of the network devices. If there are changes in the network, such as new devices being added, existing devices being removed, or configurations being updated, an on-demand inventory sync captures these changes and updates the system accordingly.

Procedure

- Step 1** From the main menu, choose **Device Management > Network Devices**.
- Step 2** Select one more devices for which you want to perform the detailed inventory synchronization.
- Step 3** Click **Actions > Detailed inventory sync** to sync and reflect the current state of the network devices.

Note

- If a device is attached to a Data Gateway during a pool change, detailed inventory collection for devices that have synced in the last 60 minutes is not performed. This ensures that devices with recent inventory data are not processed unnecessarily. Devices requiring synchronization still undergo detailed inventory collection as usual.
 - If the inventory collector pods go down during a device sync, the devices in the process of syncing remain in their previous state. To resolve this, you can manually re-sync these devices, or they automatically recover during the nightly sync.
-

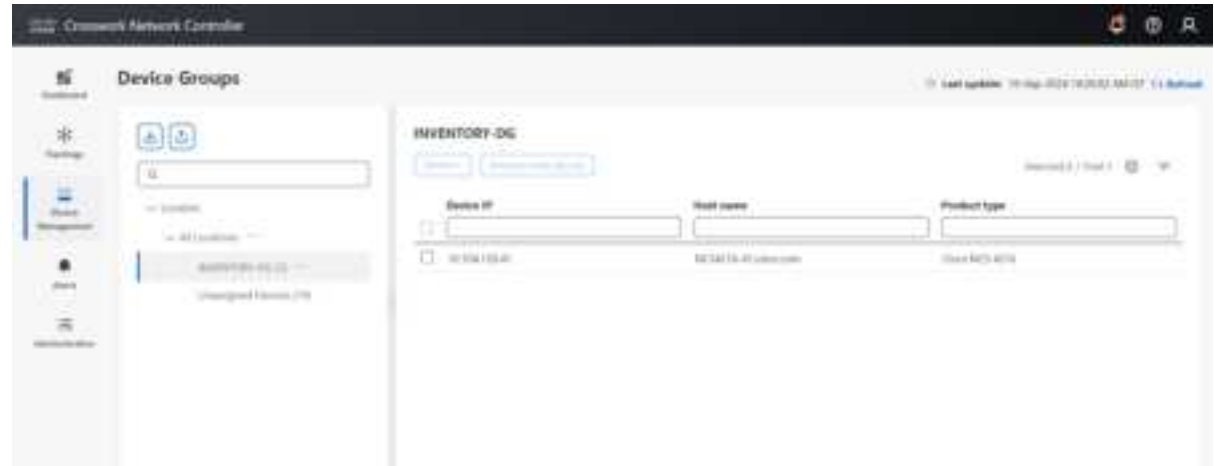
Use Device Groups to Filter your Topology Map

Device groups let you organize and manage your devices according to your needs. You can use device groups to filter and display data from specific devices on your dashboard. Device groups also allow you to visualize and zoom in on data specific to a particular group of devices. It reduces the clutter on your screen and allows you to focus on data that is most important to you.

Create Device Groups

You can create device groups and add devices to the groups either manually (as described in this section) or automatically, as described in [Create Rules for Dynamic Device Grouping, on page 103](#). A device can belong to only one device group.

Figure 30: Device Groups



Procedure

-
- Step 1** From the main menu choose **Device Management > Device Groups**. We see that a device group has been selected. Also note that only the devices belonging to that device group are listed in the devices table in the right pane.
- Step 2** To add a new sub-group, click the three dots next to any group and then click **Add a Sub-group**.
- Step 3** Fill in the details and click **Create**.
A new sub-group is added under the selected parent group.
-

Create Rules for Dynamic Device Grouping

You can create a rule to dynamically create device groups and automatically add unassigned devices to these groups using a Regular Expression (regex) on the device host name or IP address. Any newly added or discovered devices that match the rule will be placed in the appropriate group.

Dynamic rules do not apply to devices that already belong to groups. You must move them to Unassigned Devices if you want them to be considered by the rule.

Before you begin

While you can follow examples given in the Dynamic Groups dialog, it is helpful to be familiar with Regular Expressions.

Procedure

-
- Step 1** From the main menu choose **Device Management > Device Groups**.
- Step 2** Click next to **All Locations > Manage Location Dynamic Groups**.
- Step 3** Click **Show more details and examples** to help you fill out the required host name or IP address.

- Step 4** If there are any existing devices in the Unassigned Devices group, click **Test Rule** to view a sampling of what type of group names will be created.
- Step 5** Turn the **Enable Rule** toggle ON to enable the rule. After the rule is enabled, the system checks for unassigned devices every minute and will assign them to the appropriate group based on the rule.
- Step 6** Click **Save**.
- Step 7** Groups that are created this way initially appear under Unassigned Groups (created when a rule is enabled for the first time). Move newly created groups to the desired group hierarchy.
-

Modify Device Groups

You can modify device groups to add or edit the device group details. You can change the group name, or assign a different parent group.

Procedure

-
- Step 1** From the main menu choose **Device Management > Device Groups**.
- Step 2** To edit the group details, click the three dots next to the group name and then click **Edit Group Properties**. You can update the parent group, group name and the description.
- Step 3** Click **Save**.
-

Delete Device Groups

You can delete a device groups from the system. This will unassign all the devices that belong to that group and make them available for other groups.

Procedure

-
- Step 1** From the main menu choose **Device Management > Device Groups**.
- Step 2** To delete the device group, click the three dots next to the group name and then click **Delete Group**.
- Step 3** On the **Delete Group** pop-up, click **Delete** to confirm your deletion.
-

Move Devices from One Group to Another

If you need to reorganize your devices, you can move them from one group to another.

Procedure

-
- Step 1** From the main menu choose **Device Management > Device Groups**.

- Step 2** Select the group from which you wish to move the devices.
- Step 3** Select the devices from the right pane.
- Step 4** From the **Move** drop-down, select the appropriate group and click **Move**. You can also create a new group to which you can move your selected devices. For more information refer to [Create Device Groups, on page 102](#)

Sometimes, certain devices in a service or policy may not appear on the map if they are not part of the selected device group. To address this, navigate to **Administration > Settings**. Click the **User Settings** tab, where you have the following options:

- **Automatically switch to the device group that will show all participating devices**- This option ensures that all devices involved in the service or policy are displayed, providing a complete view without manual intervention.
- **Don't switch the device group automatically**- With this option, the map remains unchanged, preserving your current device group selection, even if all devices are not shown.
- **Ask me each time**- Selecting this option prompts you to decide whether to switch the device group whenever devices are missing, offering flexibility and control over your view.

Import Multiple Device Groups

When you import device groups from a CSV file, the import process creates new device groups that does not exist in the database, and updates the existing device groups that have the same data as the imported ones. This means that you might lose some of your original data if you import device groups without backing them up first. Therefore, we recommend that you export a copy of all your current device groups before you perform an import.

Procedure

- Step 1** From the main menu, choose **Device Management > Device Groups**.
- Step 2** Click  to open the **Import Groups** dialog box.
- Step 3** If you have not already created a device groups CSV file to import:
- a) Click the **Download device groups (*.csv)' template** link and save the CSV file template to a local storage resource.
 - b) Open the template using your preferred tool. Begin adding rows to the file, one row for each device group.

Use a semicolon to separate multiple entries in the same field. Use two semicolons with no space between them to indicate that you are leaving the field blank.

Be sure to delete the sample data rows before saving the file, or they will be imported along with the data you want. The column header row can stay, as it is ignored during import.
 - c) When you are finished, save the new CSV file.
- Step 4** Click **Browse** to navigate to the CSV file you just created and then click **Open** to select it.
- Step 5** With the CSV file selected, click **Import**.

Note

- While importing device groups using a CSV file, you should wait for the operation to complete. Clicking the **Import** button while the operation is in progress will lead to duplicate entries.

Export Multiple Device Groups

You can export the device groups details to a CSV file. This is useful for creating a record of all the device groups in the system at a given time. You can also modify the CSV file as you wish, and import it back to update the existing data.

Procedure

- Step 1** From the main menu, choose **Device Management > Device Groups**.
- Step 2** Click  to export the device groups in CSV format. The CSV file is then downloaded in your systems download folder.
-

View Device Details from the Topology Map

The topology map lets you view the information of any device in your network. You can see various details, such as device specifications, routing configurations, and device links. The topology map enables you to monitor and manage your network devices with ease and efficiency.

View Basic Device Details

You can view the basic device details and its connections in a graphical way. The map also allows you to adjust the view of the device by zooming in and out, panning, and rotating.

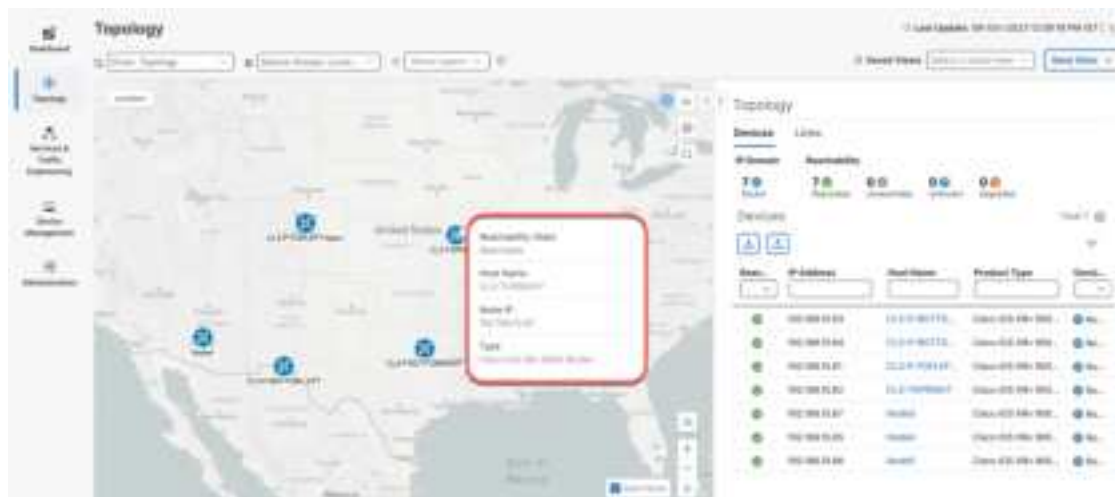


Note If you are viewing the HTML version of this guide, click on the images to view them in full-size.

Procedure

- Step 1** From the main menu choose **Topology**.
- Step 2** Hover the mouse over the device icon, to quickly view the host name, reachability state, IP address and type of device.

Figure 31: Basic Device Details



View All Device Details

The device icon on your topology map lets you view more details about your device, such as where it is located, what kind of device it is, when it was last updated and more.

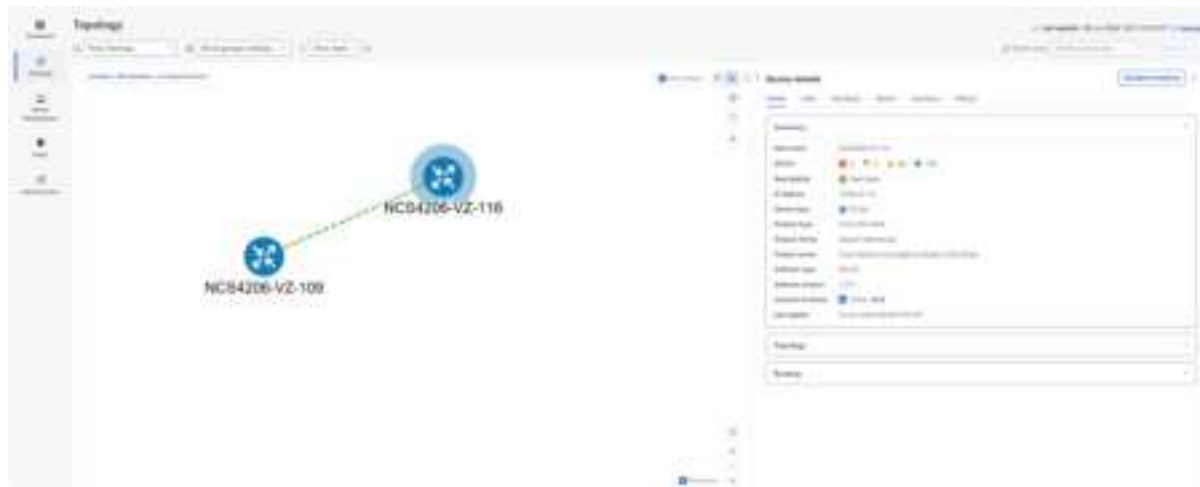
Procedure

Step 1 From the main menu choose **Topology**.

Step 2 To view device details, click on the device icon. The following details are displayed.

- Alarm information under Summary in the **Details** tab.
- An **Interfaces** tab with name, and operational and admin status for each associated interface.
- A **Links** tab with the details of the links on the selected device.
- An **Alarms** tab displaying information such as severity, source, category, and condition of the alarms. The columns can be customized based on your preferences.
- An **Inventory** tab displaying the product name, product ID, admin status, operational status, and serial number. The columns can be customized based on your preferences.
- A **History** tab with detailed information about device performance, including various performance metrics for CPU utilization, device memory utilization, device availability and environmental temperature. For each trend, you can choose the required time frame and dates using the Zoom and Date options on the graph. You also have the option to download the details in a PNG or CSV file.

Figure 32: Device Details



Identify Device Routing Details

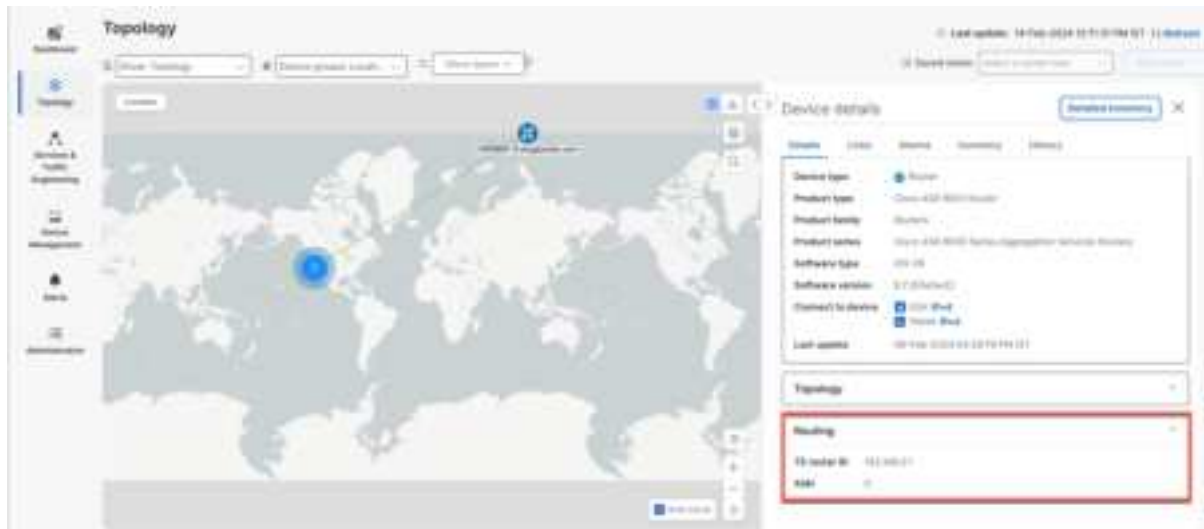
Device routing determines how data packets are transmitted from one device to another in the network and ensures that data packets reach their intended destination, avoiding congestion or loops in the network.



Note If you are viewing the HTML version of this guide, click on the images to view them in full-size.

Procedure

- Step 1** From the main menu choose **Topology**.
- Step 2** To view the device routing details, on the topology map, click the device icon. You can view the routing details in the right pane.

Figure 33: Device Routing Details

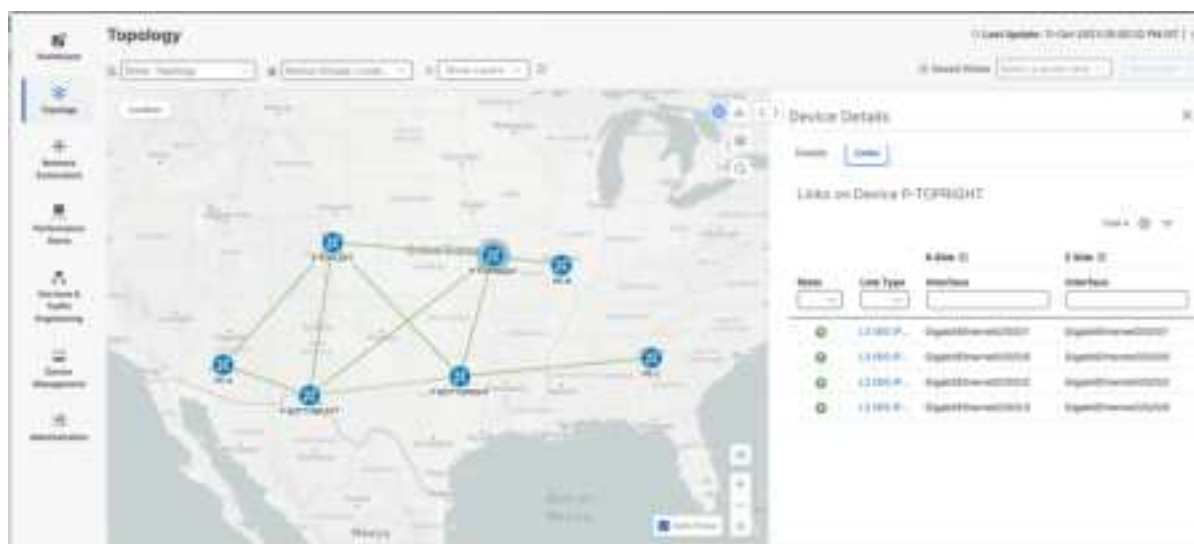
Identify the Links on a Device

You can see which links are connected to the device in the Links tab in the Device Details pane.

Procedure

- Step 1** From the main menu choose **Topology**.
- Step 2** To view links on the device, click on the device icon.
- Step 3** In the right pane, click the **Links** tab and expand the right panel to view all the link details.

Figure 34: Links on a Device



View Detailed Device Inventory

You can get a simplified, consolidated view of detailed inventory data for the devices in your network. This includes details of modules, chassis, cards and interfaces.

Procedure

- Step 1** From the main menu, choose **Topology**.
- Step 2** Click the device icon to view the **Device details** pane for the device.
- Step 3** Click the **Detailed inventory** button on the **Device details** pane to open the detailed inventory window for the chosen device. You can see the Topology tree view on the left.

Figure 35: Topology Tree View



Under the **Details** tab, you can view detailed device information, including the device summary and interface properties.

Figure 36: Extended view of the Details tab

Manage configuration

Summary

Name	Optics0/8/0/18
Product ID	DP04QSD0-ULH-188
Device name	nc5006-12428
Operational state	Up
Serial number	ACA2912030F
Type	Module
Version	01
CLI code	INXIANEAA
Part number	DP04QSD0-ULH-188

Interface properties

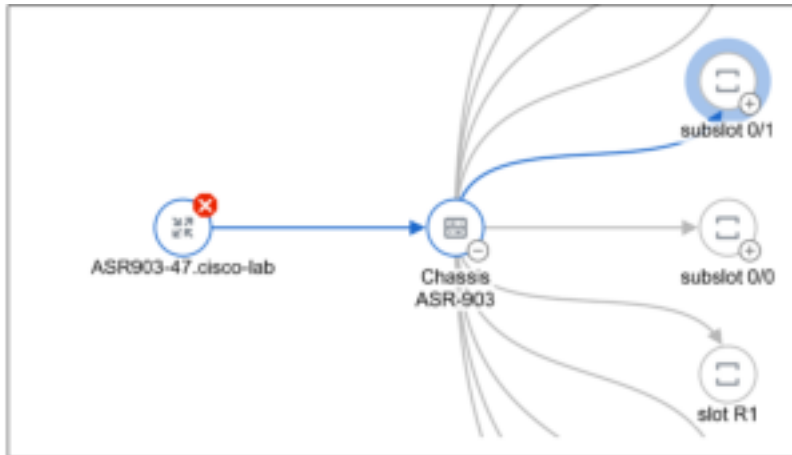
Name	Optics0/8/0/18
Admin state	Up
Operational state	Up
Description	-
MTU	-
Speed	-

Optics properties

Type	DWDM
Framing type	NONE
Port mode	NONE
Mapping mode	NONE
Wavelength	NOT SET
Actual wavelength	1532.528 nm
Modulation type	QPSK

Step 4 Zoom in to view the different modules and click one for which you need detailed information.

Figure 37: Zoomed modules on the Topology Map



You can view detailed information on the **Details**, **Interface**, **Alarms**, **Inventory** and **History** tabs for the chosen module.

Note

In the **Detailed inventory** view in topology:

- Slot, bay, and container are not shown.
- The Optics Controller and pluggable components are combined and presented as a single merged port.
- Only the entities with the Serial Number (SN) are shown. An entity without a SN is hidden, and its child is attached to the parent of the hidden entity.
- Optical ports for XR devices are merged with the corresponding SFP and the RSIP. Note that the merging of ethernet ports for XR devices is not supported.
- When clicking on the device node or the chassis node in the topology tree view, both physical and logical interfaces can be viewed. If you click on other nodes, only the physical interfaces can be viewed.

Get Details About Topology Links

You can view detailed information about any link on the topology map, such as the link name, source and destination devices, link status, bandwidth, latency, and link details. You can also view link utilization to see how much bandwidth the link is using, as well as packet drops and traffic volume.



Note

Delay and jitter metrics are available only when Segment Routing Performance Monitoring (SR-PM) is enabled. This comes with the Crosswork Network Controller Advantage package. For details on enabling SR-PM for links, refer to the *Enable SR-PM Monitoring for Links and TE Policies* section in the [Cisco Crosswork Network Controller 7.1 Service Health Monitoring](#) guide.

View Link Details

You can view the link details such as name, state, type, and endpoint interface information for each link. For more information on the link state, refer to [Link States and Discovery Methods](#), on page 116

Procedure

Step 1 From the main menu choose **Topology**.

Step 2 Select a link to view details in any of the following ways:

- By clicking a link on the topology map
- By clicking a link from the **Links** tab in the topology map
- By clicking a link from the **Links** tab in the **Device Details** page.

Figure 38: Link Details



The **History** tab provides useful insights into the performance and trends of the network. You can select the time interval to analyze the data.

Step 3 View aggregate link details.

Click on a dashed line in the topology map. A dashed line indicates an aggregated link that represents more than one link.

Step 4 View IPv4 unnumbered interface information (if available).

IPv4 unnumbered interfaces information is displayed as a combination of the TE Router ID and the index.

View Link Interface Metrics

Link interface metrics are a set of indicators that measure the performance and quality of the communication between two or more network devices. They include parameters such as bandwidth, delay, jitter, packet loss. Link interface metrics can help network administrators to monitor and troubleshoot network issues, optimize network resources, and plan for future network expansion or upgrade.

Procedure

- Step 1** From the main menu choose **Topology**.
- Step 2** Click a link on the topology map.
- Step 3** To view interface metrics, expand **A side** or **Z side**.

The utilization shown for IPv4 and IPv6 links represents the total traffic and packet drops for the interface as a whole, not specific to each address family. The traffic metrics are also reported as a combined value.

Figure 39: Link Interface Metrics

Links

Total 0

A side (1)

Z side (1)

State	Link type	Interface	Utilization (1)	In packet dr...	Out packet ex...	Delay	Jitter	Interface	Utilizat... (1)	In packet ...	Out packet ...	Delay	Jitter
	L3 link IP...	TwentyFiveGig...	0.000% (3...	0%	0%			TwentyFiveGigG0/0/0/34	0.000%...	0%	0%		
	L3 link IP...	TenGigE0/0/0/0	0.000% (3...	0%	0%			TenGigE0/0/0/0	0.0000% ...	0%	0%		
	L3 link IP...	TenGigE0/0/0/0	0.000% (3...	0%	0%			TenGigE0/0/0/0	0.0000% ...	0%	0%		
	L3 link IP...	TwentyFiveGig...	0.000% (3...	0%	0%			TwentyFiveGigG0/0/0/34	0.000%...	0%	0%		
	L3 link IP...	TwentyFiveGig...	0.000% (3...	0%	0%			TwentyFiveGigG0/0/0/34	0.000%...	0%	0%		
	L3 link IP...	TwentyFiveGig...	0.000% (3...	0%	0%			TwentyFiveGigG0/0/0/34	0.000%...	0%	0%		
	L3 link IP...	TenGigE0/0/0/0	0.000% (3...	0%	0%			TenGigE0/0/0/0	0.0000% ...	0%	0%		
	L3 link IP...	TenGigE0/0/0/0	0.000% (3...	0%	0%			TenGigE0/0/0/0	0.0000% ...	0%	0%		

Link States and Discovery Methods

Table 13: Link Types, Discovery and States

Link Type	Discovery	Link State
L3 link (ISIS, OSPF and eBGP)	via SR-PCE	- SR-PCE set it to UP or DOWN based on the link operational state - When one direction of a link is operational while the other direction is down, then the link state is set as degraded.

Link Type	Discovery	Link State
L2 link (CDP, LLDP, LAG)	via SNMP MIB: CDP, LLDP and LAG	The link state is based on the two link endpoints operational states (via IF MIB). • Link state is UP when initially discovered. • When one of the endpoint interfaces is operationally down, then the link state is set to DOWN. • When both endpoint interfaces are operationally up, then the link state is set to UP. • When one direction of a link is operational while the other direction is down, then the link state is set as degraded.

Protocols Used for Topology Services

The following table lists the protocols and methods used for obtaining the topology information.

Protocol/Method	Provides	Use Cases
IGP/ BGP-LS (via SR-PCE)	Real time topology (nodes, links, link metrics, and so on.)	L3 topology visualization
PCEP (via SR-PCE)	Real time LSP status and CRUD of SR-PCE initiated LSPs	• SR/SRv6, RSVP-TE LSP visualization • SR-PCE initiated LSP create/update/delete
SNMP (SNMPv2-MIB, IP-MIB, IF-MIB, LLDP-MIB, (CISCO CDP-MIB) (via CDG)	System info, interface table (interface and SR-TE/RSVP-TE traffic Utilization) IP address table, L2 adjacency information	Device management and details and Crosswork Optimization Engine model building: • L2/L3 topology • Interface name, admin/oper status • Interface and SR policy and RSVP-TE tunnel utilization
CLI (via CDG) - show mpls	TE router ID and so on.	To match the DLM node with the same TE router ID that is learned from the SR-PCE

Enable or Disable Topology Link Discovery

To control the visibility of L2 topology links on the maps, you can change the system settings for the discovery of LLDP, CDP and LAG protocols. These protocols are used to identify the neighboring devices and their connections. The discovery option is disabled by default, which means the links of these protocols, including the ones that were already discovered, will not show up on the maps. You can enable the discovery option to see the links of the selected protocols on the maps.

To enable topology discovery:

Before you begin

- Make sure all pods are healthy before changing the settings.

Procedure

- Step 1** From the main menu, choose **Administration > Settings > System Settings**.
- Step 2** Under **Topology**, click the **Discovery** option.
- Step 3** Select the checkbox of the protocols for which you want to enable discovery.
- Step 4** Click **Save** to save your changes.

When you enable discovery, the collection jobs will be created. The table below lists the collections jobs created for each protocol setting along with the sensor paths.

Table 14: Collection Jobs for each setting

L2 Configuration Setting	Helios collection Jobs ID	Context ID	MIBs collected	Sensor paths
None (default)	cw.topo_svc	cw.toposvc.snmp cw. toposvc.snmptraps	IF-MIB, IP-MIB, LAG-MIB IF-MIB:notification Note IF-MIB is required, but it is collected in the ICON jobs.	IP - MIB : IP-MIB / ipAddressTable / ipAddressEntry IF-MIB:notifications
CDP	cw.topo_svc	cw.toposvc.cdp	IF-MIB, CDP-MIB, LAG-MIB	CISCO - CDP - MIB : CISCO - CDP - MIB / cdpCacheTable / cdpCacheEntry CISCO - CDP - MIB : CISCO - CDP - MIB / cdpInterfaceTable / cdpInterfaceEntry

L2 Configuration Setting	Helios collection Jobs ID	Context ID	MIBs collected	Sensor paths
LLDP	cw.topo_svc	cw.toposvc.lldp	IF-MIB, LLDP-MIB, LAG-MIB	LLDP - MIB : LLDP - MIB / lldpLocPortTable / lldpLocPortEntry LLDP - MIB : LLDP - MIB / lldpRemTable / lldpRemEntry
LAG	cw.topo_svc	cw.toposvc.lag	IF-MIB, LAG-MIB	IEEE8023 - LAG - MIB : IEEE8023 - LAG - MIB / dot3adAggTable / dot3adAggEntry IEEE8023 - LAG - MIB : IEEE8023 - LAG - MIB / dot3adAggPortTable / dot3adAggPortEntry

The table below lists the common errors when enabling or disabling topology discovery:

Table 15: Common error scenarios:

Possible Error Scenario	Cause	Cause Recommended Action
After disabling, some of the disabled links are displayed in the maps.	A protocol that is disabled soon after being enabled may cause a problem. The system may stop the collection job for the previous enabled job before it finishes processing the SNMP data. This may lead to a mismatch between the actual and the displayed status of the links. The links that are disabled may still appear as enabled.	Enable and disable the protocol again with sufficient wait time in between, or restart robot-topo-svc.

Possible Error Scenario	Cause	Cause Recommended Action
When you try to enable discovery, the helios job fails and settings are disabled from further editing.	A possible cause of the collection job being stuck in an unsuccessful state is that the helios pod is unhealthy. Crosswork prevents users from modifying the L2 discovery settings while the collection job is in progress. This means that the collection job cannot be canceled or restarted until the helios pod is healthy again.	Ensure that the pods are healthy, and then enable and disable the protocol with sufficient wait time in between, or restart robot-topo-svc.
When you change the discovery settings, the topology UI or topology service crashes resulting in an unpredictable status.	The mechanism to disable users from further editing while the collection job is being created or deleted, relies on pods communicating via Postgres flag. If any pod crashes during this time, the Postgres flag key is not set correctly.	

View the network inventory

The **Network Inventory** window provides a comprehensive list of the network elements and devices that are part of your managed network. This list includes device names and types. It also details hardware specifics like serial numbers, manufacture dates, and lists each device's operational state. You can also see a high-level overview of the alarm status across your network inventory to monitor network health.

Procedure

Step 1 To view device-level information:

- a. From the main menu, go to **Device Management > Network Inventory**. The **Network Inventory** page is displayed. You can see a list of the different **Product Types** like chassis, chassis extender, compute blade, fan, memory module, pluggable transceiver and power supply.
- b. Use the quick filter to locate specific devices. For example, to list the information for all ASR devices, enter ***ASR*** in the **Product ID** field.

You can also click the alarm icons at the top of the page to filter the inventory.

Figure 40: Network Inventory

Network Inventory

Inventory with Alarms

0 Critical, 0 Major, 2 Minor, 0 Warning

Selected 0 / Total 238

Product ID	Product name	Product type	Operational s...	Vendor	Device name	Serial number	Version	CLEI code	Part number
8011-2X2XP4L	Rack 0	Chassis	Up	Cisco Systems...	Modeline 55...	FOC26510E7F	V00	UNASSIGNED	68-7627-02
8011-2X2XP4L	QRPSCPU0	Module	Up	Cisco Systems...	Modeline 55...	FOC26510E7F	V00	UNASSIGNED	68-7627-02
8011-4G24N4H1	QRPSCPU0	Module	Up	Cisco Systems...	Glendon-62	FOC2700019G	V00	UNASSIGNED	68-7462-05
8011-4G24N4H1	Rack 0	Chassis	Up	Cisco Systems...	Glendon-62	FOC2700019G	V00	UNASSIGNED	68-7462-05
8011	Rack 0	Chassis	Up	Cisco Systems...	SPYRE-120...	FOC4037P5BA	V02	UNASSIGNED	68-6825-07
8011	QRPSCPU0	Module	Up	Cisco Systems...	SPYRE-120...	FOC4037P5BA	V02	UNASSIGNED	68-6825-07

For each product, you can view the product name, device name, type and version, vendor name, the operational state of the device, its serial and part number, manufacturing date, and CLEI code. You can filter the displayed information using the *settings* icon by selecting the inventory information that you want to display.

Step 2

To view element-level information, click the link on the product ID of the device. You can see the pop window with the following tabs. Filter the displayed information under each tab using the *settings* icon by selecting the information that you want to view.

- Details:** This tab includes network inventory information for each device. It displays the **device name** and **product name** to identify the specific device and model while the **product ID** provides a unique identifier. The **operational state** indicates whether the device is currently active or experiencing issues. The **serial number** is the unique code assigned to each device for inventory. The **type** and **version** indicate the device functionality and its specific release. The **CLEI** (Common Language Equipment Identifier) code is the standardized identification of the equipment. The **part number** helps in identifying specific components or assemblies of the device and the **physical path** details the exact location of the device within the network.

Figure 41: Network Inventory Details

Network Inventory

Inventory with Alarms

0 Critical, 0 Major, 2 Minor, 0 Warning

Selected 0 / Total 238

Product ID	Product name	Product type	Operational s...
8011-2X2XP4L	Rack 0	Chassis	Up
8011-2X2XP4L	QRPSCPU0	Module	Up
8011-4G24N4H1	QRPSCPU0	Module	Up
8011-4G24N4H1	Rack 0	Chassis	Up
8011	Rack 0	Chassis	Up
8011	QRPSCPU0	Module	Up

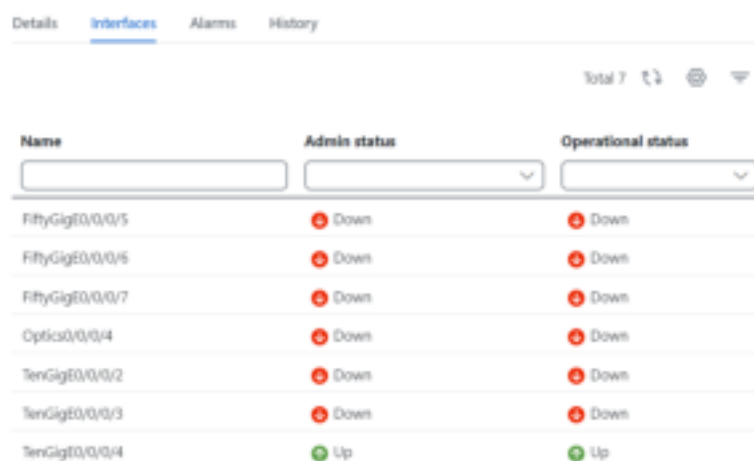
8011-2X2XP4L

Summary

Name	Rack 0
Product ID	8011-2X2XP4L
Device name	Modeline 55...
Operational state	Up
Serial number	FOC26510E7F
Type	Chassis
Version	V00
CLEI code	UNASSIGNED
Part number	68-7627-02
Physical path	Rack 0

- b) **Interfaces:** This tab displays information about the network interfaces of the device. It includes the name of each interface, the administrative status, indicating whether the interface is up or down and the operational status, which reflects the current working condition of the interface, such as whether it is up and running or experiencing issues.

Figure 42: Network Inventory Interface Details



The screenshot shows the 'Interfaces' tab in the Network Inventory. At the top, there are tabs for 'Details', 'Interfaces' (selected), 'Alarms', and 'History'. Below the tabs, there is a search bar and a 'Total 7' indicator. The table below lists the interfaces and their statuses.

Name	Admin status	Operational status
FiftyGigE0/0/0/5	Down	Down
FiftyGigE0/0/0/6	Down	Down
FiftyGigE0/0/0/7	Down	Down
Optics0/0/0/4	Down	Down
TenGigE0/0/0/2	Down	Down
TenGigE0/0/0/3	Down	Down
TenGigE0/0/0/4	Up	Up

- c) **Alarms:** This tab provides information about the alarms that have been raised on a device, a card, or a port. It includes the event type, severity, source and description of the alarm, the date the alarm was created and last updated, the category of the device and the managed object that is monitored.

Figure 43: Network Inventory Alarms

Details

Interfaces

Alarms

History

Total 1

🔍

⚙️

☰

Severity	Source	Description	Event type	Last update
Critical	TenGigabitEthernet0/0/0/4	IOSXE_RP_ALAR...	04-Sep-2024 10:57:24...	

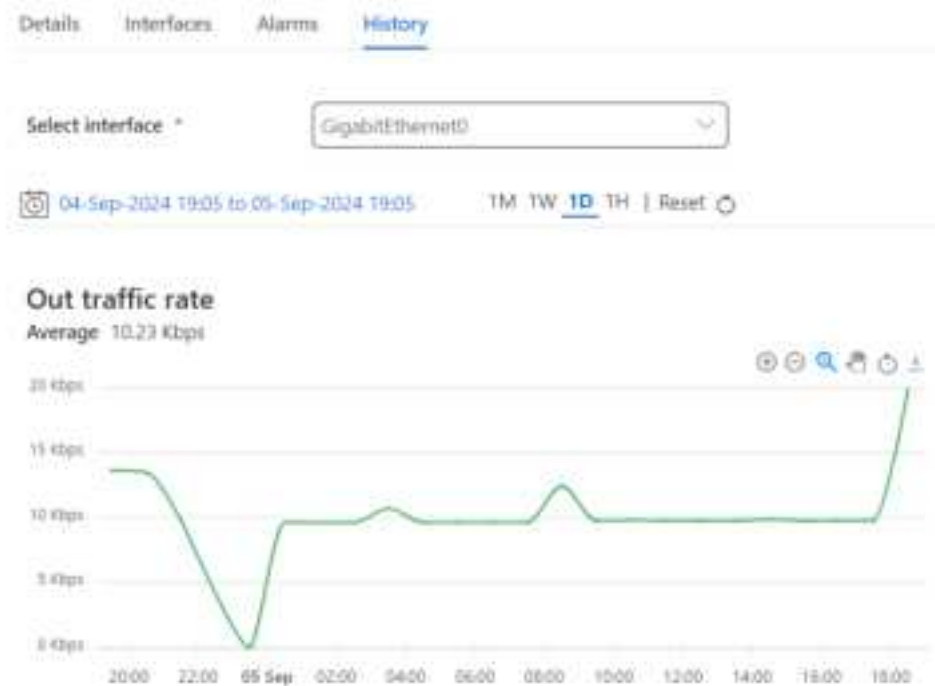
- d) **History:** Provides graphs that reflect various aspects of network performance since the device was discovered or deployed.

Select the interface from the dropdown option to choose the interface type. Depending on the monitoring policy that you have chosen, you can view the tabular representation of interface details. For example, if you have activated the Interface Health policy, you can view details like in-traffic rate, out-traffic rate, in-utilization, out-utilization, in-errors,

out-errors, in-discards, out-discards, in-packets rate, out-packets rate and CRC errors percentage. If you have activated an optical policy, you can view details like optical Rx power, optical Tx power, voltage, temperature and current.

You can select the time ranging from one month to one hour. In the figure below, you can see a snippet of the average outbound traffic rate for a Gigabit Ethernet interface over a period of one day. You can scroll through the pop-up window to view the other detailed graphs. Additionally, you can click the button labeled with the policy name to expand or collapse its details.

Figure 44: Network inventory history details



Click the *download* icon to download the data as a pdf file or a csv file.

Note

- To see the relevant data displayed in the graphs, activate the monitoring policy for the relevant devices. For steps to create monitoring policies, refer to the section [Create monitoring policies, on page 176](#).
- Average values are available for all performance metrics on the **History** tabs. However, the relevance of average values may vary across different metrics. Assess the context of each metric before using the average values in your analysis.

Export Inventory Results

You can export the inventory search results to a CSV file. This is useful to maintain a record of all your inventory in the system at a given time.

Step 1 From the main menu, choose **Device Management** > **Network Inventory**.

Step 2 Select the devices you want to include in the export. Based on your requirements, you can:

- Export the entire inventory- upto 1 million records.
- Apply filters and export only filtered inventory items- upto 1 million records.
- Export only the manually selected items, with a limit of upto 1,000 records. The export can include rows filtered by your criteria and the columns you have chosen. If you select more than 1,000 items, the export option is disabled.

Step 3 Click to export the inventory details in CSV format. The CSV file is then downloaded in your system's download folder.

View Device Job History

Crosswork Network Controller collects and stores information about device-related jobs. Follow the steps below to track all create, update and delete activities.

Procedure

Step 1 From the main menu, choose **Device Management** > **Inventory Jobs**. The **Inventory Jobs** window opens displaying a log of all device-related jobs, like the one shown below.

Figure 45: Inventory Jobs window

Status	Description	Impact	Start time	End time	Job name
Completed	Adding device 'Cisco-1000-1' to the network	Low	11-Sep-2024 01:00:00 PM GMT	11-Sep-2024 01:00:00 PM GMT	InventoryJob-1000-1
Completed	Adding device 'Cisco-1000-2' to the network	Low	11-Sep-2024 01:00:00 PM GMT	11-Sep-2024 01:00:00 PM GMT	InventoryJob-1000-2
Completed	Adding device 'Cisco-1000-3' to the network	Low	11-Sep-2024 01:00:00 PM GMT	11-Sep-2024 01:00:00 PM GMT	InventoryJob-1000-3
Completed	Adding device 'Cisco-1000-4' to the network	Low	11-Sep-2024 01:00:00 PM GMT	11-Sep-2024 01:00:00 PM GMT	InventoryJob-1000-4
Completed	Adding device 'Cisco-1000-5' to the network	Low	11-Sep-2024 01:00:00 PM GMT	11-Sep-2024 01:00:00 PM GMT	InventoryJob-1000-5
Completed	Adding device 'Cisco-1000-6' to the network	Low	11-Sep-2024 01:00:00 PM GMT	11-Sep-2024 01:00:00 PM GMT	InventoryJob-1000-6
Completed	Adding device 'Cisco-1000-7' to the network	Low	11-Sep-2024 01:00:00 PM GMT	11-Sep-2024 01:00:00 PM GMT	InventoryJob-1000-7
Completed	Adding device 'Cisco-1000-8' to the network	Low	11-Sep-2024 01:00:00 PM GMT	11-Sep-2024 01:00:00 PM GMT	InventoryJob-1000-8
Completed	Adding device 'Cisco-1000-9' to the network	Low	11-Sep-2024 01:00:00 PM GMT	11-Sep-2024 01:00:00 PM GMT	InventoryJob-1000-9
Completed	Adding device 'Cisco-1000-10' to the network	Low	11-Sep-2024 01:00:00 PM GMT	11-Sep-2024 01:00:00 PM GMT	InventoryJob-1000-10
Completed	Adding device 'Cisco-1000-11' to the network	Low	11-Sep-2024 01:00:00 PM GMT	11-Sep-2024 01:00:00 PM GMT	InventoryJob-1000-11
Completed	Adding device 'Cisco-1000-12' to the network	Low	11-Sep-2024 01:00:00 PM GMT	11-Sep-2024 01:00:00 PM GMT	InventoryJob-1000-12

The jobs display in descending order of creation time. The most recent job is shown first. To sort the data in the table, click a column heading. Click the column heading again to toggle between ascending and descending sort order.

Step 2 The **Status** column shows the types of states: completed, failed, running, partial, and warning. For any failed or partial job, click ⓘ shown next to the error for more information.

Note

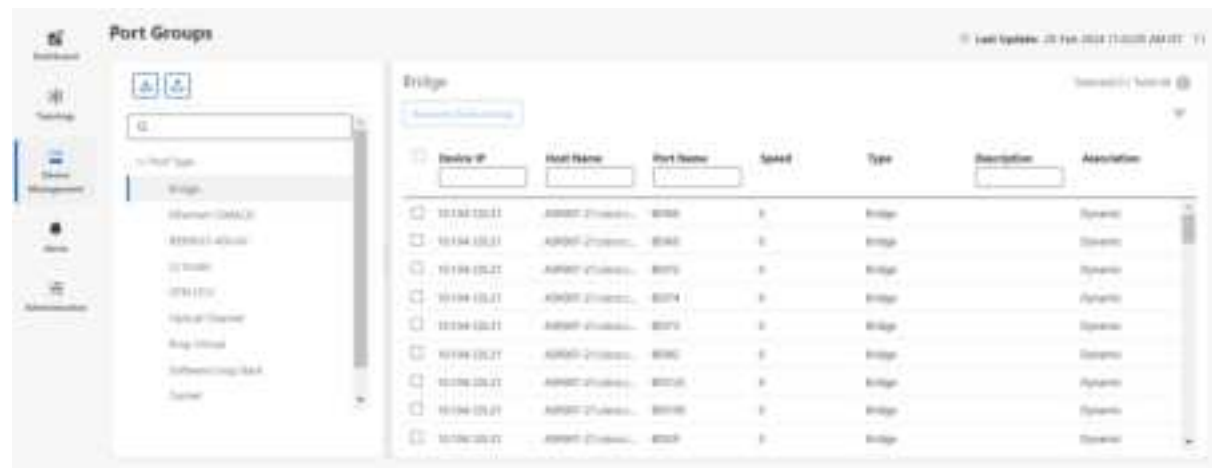
The status may be displayed as **Completed** even when the device is not reachable. You can verify that the status of the jobs that is displayed is correct by also looking into the status of the device (**Device Management > Network Devices**).

Manage Port Groups

Cisco Crosswork Network Controller allows you to manage multiple port groups for applying configurations and monitoring policies to sets of ports on devices. You can implement policies like Quality of Service (QoS), security settings, and traffic management rules across multiple ports simultaneously, and set up monitoring and performance tracking for these groups to oversee network health and identify issues.

Ports on new devices are automatically assigned to the appropriate port group. You can see these ports listed under Port Type as a read-only list. This list categorizes ports according to their types, such as Ethernet, Fiber Channel, or other interface types, without the need for you to enter them manually. You cannot create Port Type groups directly but you can use device criteria to create a user-defined group, and create subgroups under the user-defined group. If the group is dynamic and a port matches the criteria, it is added to the group. A port can belong to one or more port groups.

Figure 46: Port Groups



Add Ports Manually to a Group

You can add ports manually to an existing group. To add a port:

Procedure

Step 1 From the main menu choose **Device Management > Port Groups**.

Step 2 To add a port manually, click the three dots next to any group and then click **Add ports manually**.

- Step 3** Click the **Add ports** button. You can see the ports contained in the selected port groups.
- Step 4** Select the ports you want to add and click **Save**. The ports that you select will be added to the parent port group.

Add Ports Dynamically to a Group

You can automate the inclusion of ports in port groups by adding ports dynamically based on predefined rules, reducing the need for manual intervention. You can define specific rules to automatically add ports to these groups. Note that you can create a maximum number of 10 rules.

Procedure

- Step 1** From the main menu, choose **Device Management > Port Groups**.
- Step 2** To add a port automatically, click the three dots next to any group and then click **Add ports dynamically**.
- Step 3** Click **Add new rule** and enter the conditions that you want for the rule based on name, admin status, speed, port type or operational status.
- For a detailed list of *ifType* values and their descriptions to identify interface types and type identifiers, refer to the IANAifType-MIB document available at [IANA Interface Types](#).
- Step 4** Click **Save**. The port group rule is updated and the rule becomes available within 10 minutes.
- Step 5** Click **Test rule** to view a sample of the expected result for the rule you create.

Edit Port Group Properties

You can edit the properties for the port groups you have created. To edit the properties:

Procedure

- Step 1** From the main menu choose **Device Management > Port Groups**.
- Step 2** Locate and select the port group you wish to edit from the list of existing port groups. Click the three dots next to the group and then click **Edit group properties**.
- Step 3** Fill in the details under the **Group details** tab and click **Save**.

Create User-defined Port Group

You can create custom groups of ports, known as user-defined port groups. These groups allow you to organize ports according to your needs. The port groups listed under **Port Type** are automatically generated by Crosswork based on ports discovered from your onboarded devices and are read-only. In contrast, you can create your own port groups under the **User-Defined** section.

To create a user-defined port group:

Procedure

-
- Step 1** From the main menu choose **Device Management > Port Groups**.
- Step 2** To add a new port group, click the three dots next to a user-defined group and then click **Add a Sub-Group**.
- Step 3** Add a name and description for the new port and click **Create**.
A new user-defined port group will appear under the selected category.
-

Delete a Port Group

You can delete a port group from the system. This will unassign all the ports that belong to that group.

Procedure

-
- Step 1** From the main menu choose **Device Management > Port Groups**.
- Step 2** To delete the port group, click the three dots next to the group name and then click **Delete Group**.
- Step 3** On the **Delete Group** pop-up, click **Delete** to confirm your deletion.
-

Import Port Groups

By importing predefined port groups, you can quickly apply configurations and policies to sets of ports without manually defining each group. When you import port groups from a CSV file, the process creates new port groups that do not exist in the database and updates existing port groups with matching data. This could result in the loss of original data if you import port groups without backing them up first. Therefore, we recommend exporting a copy of all your current port groups before proceeding with the import.

Procedure

-
- Step 1** From the main menu, choose **Device Management > Port Groups**.
- Step 2** Click  to open the **Import Groups** dialog box.
- Step 3** If you have not created a CSV file for imported port groups:
- Click the **Download port groups (*.csv)' template** link and save the CSV file template to a local storage resource.
 - Open the template using your preferred tool. Begin adding rows to the file, one row for each port group.

Use a semicolon to separate multiple entries in the same field. Use two semicolons with no space between them to indicate that you are leaving the field blank.

Make sure to delete the sample data rows before saving the file, or they will be imported along with your intended data. The column header row can remain, as it is ignored during import.
 - When you are finished, save the new CSV file.

Step 4 Click **Browse** to navigate to the CSV file you just created and then click **Open** to select it.

Step 5 With the CSV file selected, click **Import**.

Note

While importing port groups using a CSV file, you should wait for the operation to complete. Clicking the **Import** button while the operation is in progress will lead to duplicate entries.

Export Port Groups

You can export the port groups detail to a CSV file. This is useful for creating a record of all the port groups in the system at a given time. You can also modify the CSV file as you wish, and import it back to update the existing data.

Procedure

Step 1 From the main menu, choose **Device Management > Port Groups**.

Step 2 Click  to export the port groups in CSV format. The CSV file is then downloaded in your systems download folder.



CHAPTER 4

Use Templates to Configure Similar Devices

You can deploy templates for quick and consistent application of settings across your network devices. Templates help you to update configurations by applying changes to multiple devices simultaneously. You can also onboard devices without all the desired configurations initially and later push a standardized configuration to the devices using templates.



Note

- For template operations such as creating, editing, or deleting, you must have Global API Permissions enabled for **Device Configurations**.
- For support with configuring templates for any non-Cisco devices, contact the Cisco Customer Experience team.

The types of templates available with Crosswork are:

- **System templates:** These are predefined configuration templates bundled with Crosswork, ready for deployment on your network devices.
- **User-defined templates:** Create and customize these templates, making them available for others to use.

You can use a combination of these templates on your devices to:

- Streamline and manage existing device settings.

OR

- Design templates to provision new settings on devices for ease of deployment.

This section contains the following topics:

- [Key benefits of configuration templates, on page 130](#)
- [Configuring devices using templates, on page 130](#)
- [Monitor and manage templates, on page 143](#)
- [Deploy templates from detailed inventory, on page 144](#)
- [Sample configuration scripts for templates, on page 146](#)

Key benefits of configuration templates

Using configuration template as a network management tool offers the following benefits:

- Ensures uniformity across devices.
- Reduces manual errors and ensures consistent network configurations.
- Saves time by applying pre-defined settings to multiple devices simultaneously.
- Allows granular control from the topology view for device-level management.
- Integrates with inventory using APIs to display pre-configured values in the UI for device-level configurations.
- Efficiently manages up to 1,000 devices per template in a SVM environment and 3000 devices per template in a cluster setup.

Configuring devices using templates

Follow these steps to configure a template for devices with similar configurations.

Prepare for template deployment

1. Choose a device group or list of devices for template deployment. Consider your network and device similarities carefully to ensure correct template application. Refer to the section, [Identify and group devices for deploying templates, on page 131](#) for more details.
2. If you select the device group option, ensure that all devices within the chosen group are compatible with the selected template, as Crosswork Network Controller does not perform any validation or compatibility checks.
3. Ensure your devices are configured for Crosswork Network Controller for template deployment. Check network settings and compatibility requirements. Refer to the section, [Configuration prerequisites for new devices, on page 2](#) to verify and complete device configurations for Crosswork Network Controller.
4. The templates are executed by Crosswork Network Controller VMs. Ensure that the VM has direct reachability to the managed devices before deploying templates. If NSO is integrated with Crosswork Network Controller, a *sync-from* operation is automatically performed to keep NSO aligned with the device configuration.

Backup and restore device configuration

Use the backup and restore capabilities to protect your device configurations and maintain the templates applied to your onboarded devices. For more information, see [Configuration Backup and Restore, on page 147](#).

Create and deploy templates

Navigate to **Device Management > Configuration Templates > Create Template** in the Crosswork Network Controller UI and proceed with the following steps for your selected devices.

1. Define configuration preferences for the templates that you create. Refer to the section, [Set configuration preferences](#).
2. Enter the template information. Refer to the section, [Specify template details, on page 133](#).
3. Define the variables and input methods. Refer to the section, [Define variables, on page 134](#).
4. Convert variable inputs into CLI commands using different code syntax. Refer to the section, [Configuration template commands, on page 136](#).
5. Configure the script for a template. Refer to the section, [Create template script, on page 139](#).
6. Apply the configuration template to selected devices. Refer to the section, [Deploy templates, on page 140](#).
7. Check the status and results of the deployed configuration template. Refer to the section, [Monitor template jobs](#).
8. Use the topology map to modify or replace templates on devices that already have templates applied. Refer to the section, [Deploy templates from detailed inventory, on page 144](#).

Identify and group devices for deploying templates

Group devices by network role and refine groups based on attributes.

1. Identify and standardize shared protocols and features across similar devices.

Grouping examples:

- Routers running the same version of IOS-XE with similar routing configurations.
- Interface settings such as security parameters and routing protocols, variables like MTU size, NAT, or DNS configurations.
- Protocols like OSPF or BGP, shared QoS policies, and security measures like ACLs.
- Common elements such as VLAN configurations, SNMP settings, and logging policies across similar devices.

2. Identify the configurations on your devices that you want to standardize with templates, such as:

- **Common settings:** These are basic configurations that are standardized across many devices, with role-specific variations.

Example: A SNMP configuration, where the core settings are the same, but the target server may differ. Other examples include configuring user accounts, banners, and PCE.

- **Free-form variable input:** These configurations require you to enter specific values, such as descriptions, names, port descriptions, and IP addresses.

Example: Setting an interface description or defining a service name such as:

```
interface GigabitEthernet0/0/0/1 description "Uplink to Core Router"
```

- **Interactive configurations:** These configurations allow you to make choices that influence the configuration. You can use UI elements like radio buttons, checkboxes or dropdown lists.

Example: Enabling or disabling a specific feature on an interface such as:

```
shutdown OR no shutdown
```

Define configuration preferences for templates and backup and restore

Customize your configuration preferences to tailor your template setup. Define settings like session timeouts backup configurations and retention policies to manage resources and ensure data compliance effectively. You can set your preferences before deploying a template or before scheduling configuration backup.

Procedure

Step 1 From the main menu, navigate to **Device Management > Configuration Preferences**.

Step 2 Set your preferences for templates, as well as backup and restore operations. Refer to the *Configuration preferences* table to view the options available for customization.

Table 16: Configuration preferences

Field	Enter or select
Timeout (seconds)	Specify the duration in seconds before a session times out due to inactivity. The valid range is from 60 to 900 seconds.
Maximum backup versions	Choose the maximum number of configuration backup versions to retain per device, ensuring you have sufficient historical data for rollback or audit purposes without excessive storage usage. Note that this limit applies to each device individually, not the total number of backups in Crosswork Network Controller. The valid range is from 0 to 52.
Maximum retention days	Set the number of days to retain configuration backups. The valid range is from 0 to 365 days.
If both Maximum backup version and Maximum days are configured, Crosswork Network Controller uses both the settings to determine how long backups are kept.	
Alarm threshold	Define the number of backup failures to trigger an alarm. The valid range is from 1 to 10.
Job retention days	Specify the number of days to retain data and logs for template jobs, backup jobs, and restore jobs. The valid range is from 7 to 14 days.
Archive configuration while adding a device	Enable or disable automatic archiving of the device configuration upon its addition. This option safeguards against failed configurations during the initial setup.
Collect configuration backup when the configuration changes	This option enables automatic backups upon configuration changes to maintain a secure, up-to-date archive.

Field	Enter or select
Hold Off Timer (seconds)	This option becomes visible if you select Collect configuration backup when the configuration changes. When a configuration change occurs on a device, a notification is sent from the device to Crosswork Network Controller. After receiving the notification, the system activates a hold off timer to wait for a specific duration before proceeding with further actions. If there is a configuration change on the device, the system will wait for the time you specify to check if another backup request is triggered for the same device. If additional backup requests are received within this time, they will be grouped into a single backup process for the device. The valid range is from 60 to 600 seconds.
Initiate the copy function using the EMS server	Select to specify whether the EMS server should transfer the configuration to the device during the restore operation.
Enable syslog and traps on devices	Select this option to enable monitoring and receive status updates from devices. When this option is activated, Crosswork Network Controller automatically configures the device to send syslog and traps to the Crosswork Data Gateway virtual IPs after the device is onboarded. This allows the system to receive and process important network events and device status updates.
Synchronize with NSO	Select to trigger device synchronization with NSO whenever a configuration is pushed to the device, including template deployments, restore operations, or syslog or trap configurations.

Specify template details

Provide template details to define and set it up on the **Specify template details** page.

Procedure

- Step 1** In the **Specify template details** section, enter a template name and description. Template name can only contain letters, numbers, hyphens and underscores. Spaces and special characters are not allowed.
- The default transport protocol for connecting to a device is set to CLI in the current release and this option cannot be modified. Future implementations may support additional protocols for configuration templates.
- Step 2** In the **Labels** field, enter a label name. You can enter more than one label.
- Assigning a label to a configuration template helps you to:

- Search a template using the label name in the search field.
- Use the labeled template as a reference to configure more devices.

Step 3 If you want to configure a troubleshooting template, enable the **Read template for troubleshooting** slider.

This option creates a **read** template with a set of commands, such as show commands, to gather information from devices without altering their configurations. These show commands are visible under the **Configuration Templates > Jobs** tab.

Use a troubleshooting template to:

- Execute multi-show commands for a single device or a group of devices for easy and quick diagnostics.
- Deploy schedule based execution for better network management.
- To gather data over time for offline comparison.

Choosing the **Read template for troubleshooting** option automatically tags the template as a **Read template** for easy identification. We recommend that you maintain the default tag of these templates to distinguish them from other templates.

Step 4 Choose the users that you wish to authorize to deploy the template from the **Users** dropdown menu. Note that administrator users are not displayed in the list.

Select device types

Choose the device types for template deployment on the **Select device types** page.

Procedure

- Step 1** Select a category from the dropdown to specify the type of device, interface, or module the template applies to, and to differentiate it from system templates. This step is optional.
- The template utilizes these device types to configure settings or retrieve data. However, Crosswork Network Controller does not validate if the template is compatible with a specific device type.
- Step 2** Select the device types for template deployment from the available list.

Define variables

Add rows to specify variables to be used in CLI commands on the **Define variables** page. For a new template this task is optional.

Procedure

- Step 1** Click **Add row** to add one or more variables and enter their details.
- Step 2** Select the variable to be a mandatory or non-mandatory field.

Refer to the table *Data types and usage in configuration templates* for examples of data types you can use to define variables.

Table 17: Data Types and usage in configuration templates

Data type	Usage	Code snippet
String	Creates a text box for entering text values.	<code>hostname \${deviceName}</code>
Integer	Creates a text box that accepts only numeric values.	<code>interface \${interfaceName}mtu \${mtu} !</code>
IPv4 address	Creates a text box that accepts only IPv4 addresses.	<code>interface \${interfaceName} ip address \${ipAddress} !</code>
Dropdown	Creates a list of options.	<code>interface \${interfaceName} #if\ (\${speed}=="10_Mbps"\) speed 10 #elseif\ (\${speed}=="100_Mbps"\) speed 100 #elseif\ (\${speed}=="1000_Mbps"\) speed 1000 #end !</code>
Checkbox	Creates a checkbox for selection.	<code>interface \${interfaceName} #if\ (\${shutdown}=="true"\) shutdown #else no shutdown #end !</code>
Radio button	Creates a radio button for choices.	<code>interface \${interfaceName} #if\ (\${adminStatus}=="Down"\) shutdown #elseif\ (\${adminStatus}=="Up"\) no shutdown #end !</code>
Text area	Creates a text area that allows multiple-line values.	<code>banner motd ^C\${bannerText}^C</code>

The figure *Define variables* shows some more examples of functions such as strings, integers, and dropdown lists that you can use within configuration templates.

Figure 47: Define variables

Name	Display name	Type	Network ID	Description ID	Monitoring ID
hostname	hostname	string			
hostname-optional	hostname-optional	string			
hostname-optional-2	hostname-optional-2	string			
hostname-optional-3	hostname-optional-3	string			
ip	IP	ipaddress	192.168.1.1		
hostname-optional-4	hostname-optional-4	string			
hostname-optional-5	hostname-optional-5	string			
hostname-optional-6	hostname-optional-6	string			
hostname-optional-7	hostname-optional-7	string			
hostname-optional-8	hostname-optional-8	string			
hostname-optional-9	hostname-optional-9	string			
hostname-optional-10	hostname-optional-10	string			
hostname-optional-11	hostname-optional-11	string			
hostname-optional-12	hostname-optional-12	string			
hostname-optional-13	hostname-optional-13	string			
hostname-optional-14	hostname-optional-14	string			
hostname-optional-15	hostname-optional-15	string			
hostname-optional-16	hostname-optional-16	string			
hostname-optional-17	hostname-optional-17	string			
hostname-optional-18	hostname-optional-18	string			
hostname-optional-19	hostname-optional-19	string			
hostname-optional-20	hostname-optional-20	string			

Configuration template commands

This section explains the different CLI commands you can use with variables while creating the configuration script.

- [Enable mode commands, on page 136](#)
- [Multi-line commands, on page 136](#)
- [Interactive commands, on page 137](#)
- [Mixed commands, on page 138](#)

To make your templates more flexible you can also use Apache VTL. It enables you to create more dynamic templates by adding conditional logic, loops, and calculations. Refer to the section, [Apache VTL: syntax and examples, on page 139](#) for more information on incorporating VTL syntax to your CLI commands.

Enable mode commands

Certain functions like connecting to remote devices and changing terminal settings require you to use EXEC mode.

Use the following syntax to enter EXEC mode commands:

```
#MODE_ENABLE<<commands >>#MODE_END_ENABLE
```

Multi-line commands

Multi-line commands allow you to define text areas within CLI templates that accommodate multiple lines of values.

Table 18: Multi-line commands

Command type	Description	Syntax and example
Multi-line Commands	Allows creation of multiline text areas	Use <MLTCMD> and </MLTCMD> tags
Example 1	Banner creation	<MLTCMD>banner motd Welcome to Cisco. You are using Multi-line commands.</MLTCMD>
Example 2	Banner message	<MLTCMD>banner motd ~ \${message}</MLTCMD> where {message} is a multi line input variable.

Where:

- <MLTCMD> and </MLTCMD> tags are case-sensitive and must be entered as uppercase.
- The multi-line commands must be inserted between the <MLTCMD> and </MLTCMD> tags.
- The tag cannot start with a space.
- The <MLTCMD> and </MLTCMD> tags cannot be used in a single line.



Restriction For using multi-line banner commands

Multi-line banner commands are not supported directly. Instead, use the banner file format as shown in the example:

```
#conf t
Enter configuration commands, one per line. End with Ctrl-Z.
(config)#parameter-map type webauth global
(config-params-parameter-map)# type webauth
(config-params-parameter-map)#banner file tftp://209.165.202.10/banner.txt
(config-params-parameter-map)#^Z
#more tftp://192.168.0.0/banner.txt
Disclaimer:
Usage of this wireless network is restricted to authorized users only.
Unauthorized access is strictly forbidden.
All accesses are logged and can be monitored.
#
```

Interactive commands

Interactive commands allow real-time engagement with network devices, requiring user inputs to proceed with configuration tasks. These commands facilitate interactions to ensure configurations are applied correctly based on user responses.

To enter an interactive command in the CLI content, use the following syntax:

```
#INTERACTIVE
commands<IQ>interactive question<R>response
#ENDS_INTERACTIVE
```

The <IQ> tag utilizes regular expressions for interactive questions. Use valid regular expressions for matching patterns.

Refer to the table **Interactive commands** for syntax and examples.

Table 19: Interactive commands

	Description	Syntax and examples
General syntax	Enter interactive commands	CLI Command<IQ>interactive question 1<R>command response 1 <IQ>interactive question 2<R>command response 2 Where, <IQ> and <R> tag are case-sensitive and must be entered as uppercase.
Invalid content	Example with invalid interactive question usage	#INTERACTIVE save config<IQ>Are you sure you want to save? \ (y/n\)<R>y #ENDS_INTERACTIVE A question mark in between a command is invalid and does not match the pattern.
Valid content	Example with valid interactive question usage	#INTERACTIVE save config<IQ>\ (y/n\)<R>y #ENDS_INTERACTIVE
Example 1	No new line required	Replace the <IQ> tag with the <IQNONEWLINE> tag for interactive questions in which the default <return> or new line character is not required in the command. #INTERACTIVE transfer download start <IQNONEWLINE>y/N<R>y<IQNONEWLINE>y/N<R>y #ENDS_INTERACTIVE
Example 2	RSA key generation	#INTERACTIVE crypto key generate rsa general-keys <IQ>yes/no<R> no #ENDS_INTERACTIVE

Mixed commands

Mixed commands combine elements of different command types, such as using interactive prompts within a multi-line command configuration, or integrating VTL templates to generate CLI commands for a given setup. This approach allows flexibility and control when managing complex network requirements.

Combining enable mode and multi-line commands

Combine interactive and enable mode commands for tasks involving both configuration changes and interactive input.

Table 20: Enable mode and interactive commands

Syntax	#MODE_ENABLE #INTERACTIVE commands<IQ>interactive question<R>response #ENDS_INTERACTIVE #MODE_END_ENABLE
Example	#MODE_ENABLE #INTERACTIVE mkdir <IQ>Create directory<R>XXX #ENDS_INTERACTIVE #MODE_END_ENABLE

Combining interactive and multi-line commands

Interactive multi-line commands allow complex interactions with multiline configurations. Combine interactive commands and multi-line commands in scenarios where the execution of a command requires both user interaction and spans multiple lines.

```
#INTERACTIVE
macro name EgressQoS<IQ>Enter macro<R><MLTCMD>mls qos trust dscp
wrr-queue queue-limit 10 25 10 10 10 10
wrr-queue bandwidth 1 25 4 10 10 10 10
priority-queue queue-limit 15
wrr-queue random-detect 1
wrr-queue random-detect 2
wrr-queue random-detect 3
wrr-queue random-detect max-threshold 1 100 100 100 100
wrr-queue random-detect min-threshold 1 80 100 100 100
wrr-queue random-detect max-threshold 2 100 100 100 100
wrr-queue random-detect min-threshold 2 80 100 100 100
wrr-queue random-detect max-threshold 3 80 90 100 100
wrr-queue random-detect min-threshold 3 70 80 90 100
@</MLTCMD>
#ENDS_INTERACTIVE
```

Apache VTL: syntax and examples

Apache VTL enables you to create configuration scripts that dynamically incorporate input variables. Use VTL to add conditional logic, loops, or calculations to your template. This will enable you to structure and automate the generation of commands within CLI templates.

The table **Apache VTL examples for CLI templates** shows different variable types that you can use to dynamically insert values into command templates.

Additionally, see <https://velocity.apache.org/engine/devel/vtl-reference.html> for more details on VTL syntax.

Table 21: Apache VTL examples for CLI templates

Variable Type	Example Code Snippet
Normal variable	<code>#set\(\$hostname = "Router1"\) configure terminal \n hostname \$hostname</code>
Array of integers	<code>#set\(\$ports = \[1, 2, 3\]\) interface GigabitEthernet0/\$ports\[0\]</code>
Array of strings	<code>#set\(\$users = \["admin", "guest", "operator"\]\) username \$users\[1\]</code>
Map	<code>#set\(\$interface = {"name" : "GigabitEthernet0/0", "ip" : "192.168.1.1"}\)\n interface \${interface.name} \n ip address \${interface.ip}</code>

Create template script

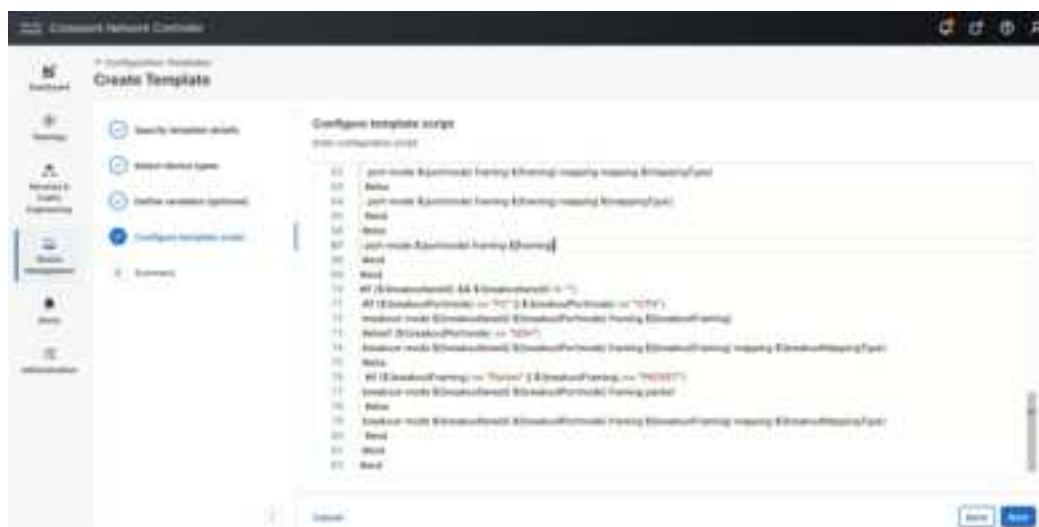
This step transforms the variable inputs and the CLI commands that you create into valid executable configurations. If no variables have been defined, you can directly enter the script into the configlet.

Procedure

Step 1 Navigate to the **Configure template script** page.

Step 2 Enter the configuration script in the configlet.

Figure 48: Example of a template script



Refer to the section [Sample configuration scripts for templates, on page 146](#) for a collection of template scripts.

Deploy templates

Deploy templates across multiple devices with similar configurations.

Procedure

Step 1 From the main menu, navigate to **Device Management > Configuration Templates**.

Step 2 Select a template and click **Deploy**. The **Specify device details** page is displayed where you can view the general details about the template.

Step 3 Select a device group or a list of devices from the **Device selection** section. This is a crucial step as you must take into account the compatibility of the devices.

Step 4 If you have defined variables when creating a user-defined template, assign values to the variable settings on the **Assign variables** page.

Example:

- Interface name-GigabitEthernet0/1/1
- Description-This is an uplink interface
- MTU-1,500

d) Admin state- Up

Step 5 You can assign these values either individually to devices or to a group of devices. To assign values individually, toggle the slider to **Yes** for the option labeled **Assign values to devices individually** and click **Assign variables**.

If variables are set as mandatory on the **Define variables** page, the **Next** button is not enabled when selecting **Assign values to devices individually**. You must provide inputs at the global level first, after which the **Next** button will become active.

Setting default values for variables in templates can significantly simplify the deployment process. Defining these values in advance removes the need for manual input during each deployment.

Step 6 On the **Preview configuration** page, select the device from the **Select device** dropdown and verify the template details you have provided. Whether you have made changes to an existing template or want to review the current configurations, click **Preview Config Changes** to view the details. If there are configuration changes, they are displayed under the **Updated Config** section.

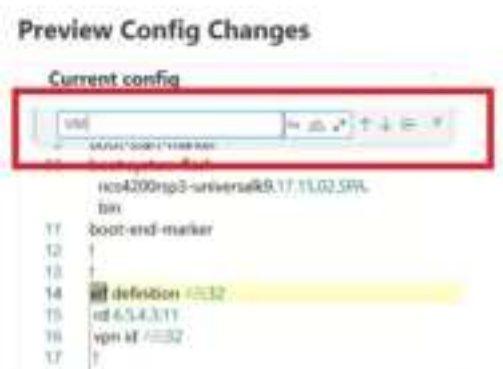
Figure 49: Preview configuration changes



Note

Sensitive data such as passwords and SNMP community strings are masked under the **Current Config** section.

To search for a variable or value, place your cursor in the config section and type your search term.



Step 7 On the **Manage settings** page:

a. Select the recovery and backup settings.

If..	Then..
You are deploying the template on IOS-XR or Nexus devices	Select Backup configuration before deployment . This ensures that if a template fails to deploy, the configuration can be restored to the last backup taken.
You are deploying the template on IOS-XE devices	Select Rollback configuration upon failure . For IOS- XE devices, configuration sessions are automatically locked, preventing simultaneous edits. If a template fails to deploy, the backup version created prior to the deployment attempt is restored.

- b. Schedule the deployment for immediate execution or at a later time.

Step 8 On the **Summary** page, review the details of your template, and if needed, make changes before clicking **Deploy template**.

Manage template jobs

Template jobs provide details on configuration tasks associated with templates. Use the **Jobs** page to track and manage template executions, filter by status, examine error details, and schedule jobs.

Navigate to the main menu and select **Device Management > Configuration Templates > Jobs**. The **Deployed jobs** section is displayed.

- At the top of the **Jobs** tab, you can see the types of states that deployed jobs can be in: **Success**, **In progress**, **Partial**, and **Failed**.
- The page lists all the current jobs with their details such as job ID, status of the job, deployed time and name of the template creator.

Use the **Jobs** page to track and manage template jobs.

Procedure

- Step 1** Use filters such as status or deployed time to narrow down specific jobs based on a criteria.
- Step 2** Click the **Job ID** in the **Deployed Jobs** section to see detailed information about the job, such as device names and time deployed. Under the **Action** column, click the three dots menu, then choose either **Re-run** to execute the job again or **Delete** to remove the job. The re-run option applies only to the same devices with the same configuration. If the template has been modified, you must deploy it again.
- Step 3** Click on the job ID to view a summary of the job, including details such as device name, job ID, and scheduled time. In the **Configlet** column, click **view** to see the configuration script associated with the template. You can see the commands pushed to device for a successful job or the reason for a failed job
- Step 4** **Handling failed and partial jobs:**
- To monitor the status of a job, apply a filter to display **Failed** jobs.
 - Click on the job ID to examine the error details of the failed job.

- c. Edit the template from the **Configuration Template** page to address any configuration errors identified in the error details.
- d. After correcting the template, go to the **Jobs** page and locate the failed job ID. Under the **Action** column, click the three dots menu, then choose either **Re-run** to execute the job again or **Delete** to remove the job.

Step 5 Scheduling jobs:

- a. To view and manage jobs scheduled for a later time, click on **Scheduled jobs**. This will display a list of all scheduled jobs.
- b. To reschedule a job, locate the job ID under **Scheduled jobs**. Under the **Action** column, click the three dots menu, then choose **Reschedule**. Select the date and time of the job and click **Reschedule**.

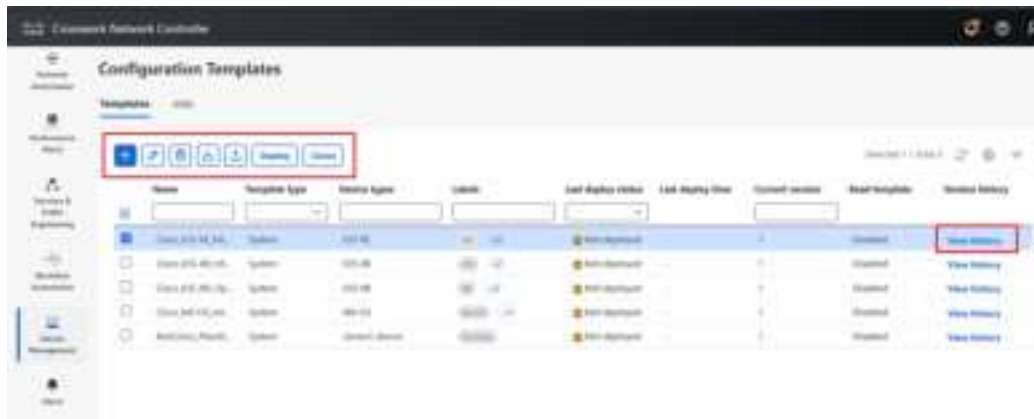
Monitor and manage templates

Ensure templates run smoothly and maintain efficiency.

Procedure

- Step 1** From the main menu, navigate to **Device Management > Configuration Templates** page. You can see a list of all the available templates.

Figure 50: Configuration templates



- Step 2** On this page, you can do the these tasks:

Task	Steps
Create a new template	Click + to create a new template.
Edit a template	Select a template and click the Edit icon. Make sure to review the edited template details before clicking Update template .

Task	Steps
Delete a template	Select a template and click the Delete icon. Only user defined templates can be deleted.
Check the different versions of a template	Select the device and click View history .
Compare versions of a template to review changes in the configuration script	Click View history for a selected template. On the Version history page, choose a specific version of the template and click Compare version . Use the dropdown menu to select a version to compare. Note that only one version can be selected for comparison at a time.
Import a template	Click the Import icon, browse for a template and click Import .
Export a template	Select a template and click Export . The templates are generated in JSON format and compressed into a .zip file before being exported. If you export without selecting one or more templates, all the available templates are exported.
Create a new template from an existing one	Select a template and click Clone to duplicate the selected template. Modify any of the template attributes to create a new version tailored to your needs. You can also clone a system template, customize its attributes as needed and transform it into a user-defined template. Ensure that you adhere to guidelines provided for creating and editing templates. Check any constraints or dependencies related to template properties before you deploy a cloned template.
Use filters to view templates	Explore various templates by filtering based on template name, type, associated device types, labels, deployment status, and version history.

Deploy templates from detailed inventory

Use the **Detailed inventory** view of a device to update or modify templates on any Gigabit interface such as IOS XR, IOS XE, NX-OS or Optics Controller with pluggables like RON devices. Follow these steps:

Before you begin

Back up your current configurations and ensure compatibility of new updates or templates with your device interface.

Procedure

- Step 1** From the main menu, navigate to the **Topology** page.
- Step 2** Click the **Host name** of a device and then click the **Detailed inventory** button in the **Device details** pane to access the detailed inventory for the chosen device.
- Step 3** Focus on the interface or optics controller that you want to manage using the **Device groups** or **Show layers** filters. For all supported modules, the **Manage configuration** option will be visible in the device details pane.

Figure 51: Manage configuration



- Step 4** **Update or change template from the same category:** On the **Manage configuration** page, you have the option to either update the current template details or select another template for deployment.
- a) **Update current template:** Modify the existing template configuration by updating the current details. Use **Preview config changes** to review and compare current and updated settings, then click **Save** to finalize the changes.

OR

- b) **Choose another template:** Click **Select another template**. View the available options and select a new template.
- c) Use the **show run** command to check current configurations.

For example:

```
show running-config interface GigabitEthernet0/1
```

This command displays the current configuration settings applied to the specified interface, such as:

```
interface GigabitEthernet0/1
description Link to Router
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
mtu 1500
```

Use the output of the `show run` command to understand existing settings that might need to be preserved or updated when deploying the new template. Note that if the input command in **Select another template** is **show run**, sensitive data, such as passwords and SNMP community strings, are masked in the **Current config** section.

- d) Apply your changes with **Save** or cancel them with **Discard changes**.

Sample configuration scripts for templates

This section provides a collection of sample configuration scripts you can use for your reference.

Configure an interface via VTL templates

```
#if (${interfaceName})
    interface ${interfaceName}

    #if (${shutdown}=="true")
        shutdown
    #else
        no shutdown
    #end

    #if (${description} != "")
        description ${description}
    #end

    #if (${mtu} != "")
        mtu ${mtu}
    #end

    #if (${ipAddress} != "")
        ip address ${ipAddress}
    #end

    #if (${speed}=="10_Mbps")
        speed 10
    #elseif (${speed}=="100_Mbps")
        speed 100
    #elseif (${speed}=="1000_Mbps")
        speed 1000
    #end
#end
```

Configure a banner

```
<MLTCMD>banner exec %
-----
This system is private property of Cisco.
Any unauthorized access is strictly prohibited and will be
prosecuted to the full extent of applicable local and international law.
-----
% </MLTCMD>
```

Configure password encryption

```
#MODE_ENABLE
#INTERACTIVE
<MLTCMD>key config-key password-encryption<IQ>Enter new key :<R>${key}<IQ>Enter confirm key
:<R>${key}
</MLTCMD>
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```



CHAPTER 5

Configuration Backup and Restore

Crosswork Network Controller's device configuration backup and restore features help prevent data loss and preserve the configuration templates on your onboarded devices.

This chapter contains the following topics:

- [Schedule a configuration backup, on page 147](#)
- [Restore a configuration backup, on page 148](#)
- [View a device configuration, on page 149](#)
- [Pin a device configuration, on page 150](#)
- [Compare device configurations, on page 150](#)
- [Export device configuration, on page 151](#)
- [Delete a device configuration, on page 151](#)

Schedule a configuration backup

This section explains how to schedule a configuration backup.

Procedure

-
- Step 1** From the main menu, choose **Device Management > Configuration Backup and Restore**.
The **Configuration Backup & Restore** page is displayed.
- Step 2** Click **Schedule backup**. The **Schedule Configuration Backup** page is displayed with the first step, **Select devices**, highlighted.
- Step 3** Choose either **Device groups** or **Devices**. Based on your selection, device group(s) or individual devices are displayed in the selection pane at the bottom. Select the required devices, and click **Next**.
- Step 4** The **Schedule Configuration Backup** page is refreshed with the next step, **Configure & schedule**, highlighted.
- a) Provide a **Backup name**.
 - b) Select the backup **Type**.

If you selected the **Type** as **Recurring**, provide relevant values for these fields:

- **Frequency**: Select the frequency of the backup. The values are Daily, Hourly, Weekly, and Monthly.

- **Repeat every:** Select the duration for repeating the backup based on the frequency you have chosen. You can specify the duration as a number of days, a number of hours, specific days of the week, or a specific day of the month. For example, if you select a monthly frequency, choose a specific day of the month.
- **Starting date and time:** Enter the starting date and time for the backup.

If you selected the **Type** as **One time**, provide relevant values for these fields:

- **Schedule:** Choose **Now** or **Later**.
- **Starting date and time:** This field is applicable only if you have chosen to schedule the backup for a later time. Enter the starting date and time for the backup.

Click **Next** to proceed.

Step 5 The **Schedule Configuration Backup** page is refreshed with the final step, **Summary**, highlighted. Review your selections, and click **Schedule backup** to proceed.

A backup job is created and added to the job list.

Step 6 To view the progress of a job, navigate to the **Jobs** tab on the **Configuration Backup & Restore** page. Enter job details, such as the job name or status, in the search fields within the table. Then, click on the job name to view detailed information about the job.

On the **Job details** page, you can edit, pause, or delete the backup job by selecting the corresponding options in the UI.

Restore a configuration backup

This section explains how to restore a configuration backup on a device.

Procedure

Step 1 From the main menu, choose **Device Management > Configuration Backup and Restore**.

The **Configuration Backup & Restore** page is displayed.

Step 2 Click on the device to which you want to restore the backup. The **Device Configuration Details** page is displayed.

Step 3 Click **Restore**. The **Restore Configuration** page is displayed with the first step, **Select backup file**, highlighted.

- Select **Backup files** to select from the list of configuration backups.
- Select **Upload** to upload the configuration file from your local machine.

Click **Next** to continue.

Step 4 The **Restore Configuration** page is refreshed with the next step, **Configure & schedule**, highlighted.

- Under **Configurations to restore**, choose the relevant configuration you need. Based on the device type and version, the available configurations may include **Admin**, **Running**, and/or **Startup** configurations.
- Select the relevant configuration checkboxes.
 - Reboot

Note

The **Reboot** checkbox is enabled only when **Startup** configuration is being restored.

- Save to startup

Note

The **Save to startup** checkbox is enabled only when **Running** configuration is being restored on IOS, IOS XE, or NX-OS devices.

- Archive before restore
- Continue restore on archive failure
- VRF name

c) Under **Schedule**, choose **Now** or **Later**.

- **Starting date and time:** This field is applicable only if you have chosen to schedule the restore operation for a later time.

Click **Next** to continue.

Step 5 The **Restore Configuration** page is refreshed with the final step, **Summary**, highlighted. Review your selections, and click **Restore** to proceed.

A restore job is created and added to the job list.

Step 6 To view the progress of a job, navigate to the **Jobs** tab on the **Configuration Backup & Restore** page. Enter job details, such as the job name or status, in the search fields within the table. Then, click on the job name to view detailed information about the job.

On the **Job details** page, you can edit, pause, or delete the restore job by selecting the corresponding options in the UI.

View a device configuration

This section outlines the steps to view a device backup configuration.

Procedure

Step 1 From the main menu, choose **Device Management > Configuration Backup and Restore**.

The **Configuration Backup & Restore** page is displayed.

Step 2 To view the latest backup configuration, click **View** under the **Last backup configuration** column to view the latest configuration backup of the selected device.

Step 3 To view an older backup configuration, click on the device. The **Device Configuration Details** page is displayed with the list of backup configurations performed on the device.

Note

When new non-empty backups are created for a device, old non-pinned backups, including empty backups, are purged based on the configured preferences (maximum backup versions or maximum retention days). Old backups are removed only after successfully creating a new backup for the same device.

- Step 4** Click on the required backup configuration file, and the configuration details are displayed in a drawer panel window.
-

Pin a device configuration

This section outlines the steps to pin a device configuration.

Procedure

- Step 1** From the main menu, choose **Device Management > Configuration Backup and Restore**.

The **Configuration Backup & Restore** page is displayed.

- Step 2** Click on the required device. The **Device Configuration Details** page is displayed.

- Step 3** Under the **Actions** column, click *** and select **Pin** to pin a configuration file.

Note

A pinned configuration cannot be deleted.

- Step 4** (Optional) To unpin a pinned configuration, click *** and select **Unpin**.
-

Compare device configurations

This section outlines the steps to compare your device backup configurations.

Procedure

- Step 1** From the main menu, choose **Device Management > Configuration Backup and Restore**.

The **Configuration Backup & Restore** page is displayed.

- Step 2** Click on the device you want to view. The **Device Configuration Details** page is displayed with the list of backup configurations performed on the device.

- Step 3** Click **Compare** and the latest backup configuration version is displayed.

- Step 4** Click the **Configuration versions** dropdown lists to select the configuration versions to compare.
-

Export device configuration

This section outlines the steps for exporting your device configuration.

Procedure

-
- Step 1** From the main menu, choose **Device Management > Configuration Backup and Restore**.
The **Configuration Backup & Restore** page is displayed.
- Step 2** Click on the device you want to view. The **Device Configuration Details** page is displayed with the list of backup configurations performed on the device.
- Step 3** Under the **Actions** column, click ******* and select **Export**.
The **Export** drawer panel window is displayed.
- Step 4** Choose the **Type**.
- Select **Sanitized** if you want to mask device passwords (credentials) in the downloaded file.
 - Select **Unsanitized** if you want to keep device passwords (credentials) visible in the downloaded file.
- Step 5** Click **Export**, and the device configuration is exported as a ZIP archive file.
- Note**
- Exporting sanitized or unsanitized configurations is done at the device and configuration level. Multi-selection is not allowed.
 - Only one configuration can be exported at a time.
- Step 6** (Optional) You can also export configuration backup activity history for one or more devices.
- **Export for multiple devices:** On the **Configuration Backup & Restore** page, select the devices and click . In the popup window, provide a file name and click **Export** to export the configuration activity history as a CSV file.
 - **Export for all devices:** On the **Configuration Backup & Restore** page, click . In the popup window, provide a file name and click **Export** to export the configuration activity history as a CSV file.
-

Delete a device configuration

This section outlines the steps to delete a device configuration.

Procedure

-
- Step 1** From the main menu, choose **Device Management > Configuration Backup and Restore**.

The **Configuration Backup & Restore** page is displayed.

Step 2 Click on the required device. The **Device Configuration Details** page is displayed.

Step 3 Under the **Actions** column, click *** and select **Delete** to delete a configuration file.



CHAPTER 6

Manage Software Images

Software image management helps you ensure that all devices in your network run on the latest, most secure software versions.



Note If you are a premiere license user interested in using the *Fleet Upgrade* feature, refer to the *Cisco Crosswork Workflow Manager Solutions 2.0 Fleet Upgrade Guide* for instructions on the automated image upgrade workflow.

This section contains the following topics:

- [Set up software image management \(SWIM\), on page 153](#)
- [Add a software image to the image repository, on page 154](#)
- [Deploy a new software image to devices, on page 155](#)
- [Activate a new software image on devices, on page 156](#)
- [Delete software image files from the image repository, on page 157](#)

Set up software image management (SWIM)

The **Software Image Management** page, located under **Device Management > Software Management**, offers a comprehensive overview of image management functionalities. Key features include adding and deploying images, exporting images, deleting image summaries, and viewing job details. Before you upload software images:

- Ensure your devices are configured correctly with the right credentials.
- To perform any SWIM related activities such as viewing image information or performing install-related operations, it's essential that you have read and write access permissions for both SWIM related roles and inventory APIs.
- If you are utilizing FTP, SFTP, or SCP, make sure these protocols are enabled and properly configured.
- Set your image transfer and distribution preferences. From the main menu, navigate to **Device Management > Software Management Preferences**. Under the **Basic** tab, choose the following preferences.

Basic Settings	Description	Default Setting
Backup running image	Backs up the running image to the software image repository before image distribution.	Disabled
Smart flash delete	Deletes unnecessary files from flash to free up memory space before distribution.	Disabled
Insert boot command	Inserts the boot command into the running image after image distribution.	Disabled
Continue on failure	If distributing images to multiple devices and distribution to a device fails, continues the distribution to other devices.	Enabled
Remove the option to activate software during distribution jobs	Select to remove the option to activate the software during distribution jobs.	Disabled
Copy operation to be initiated by the Crosswork Network Automation Manager server	Select if you want the software images to be copied by the Crosswork server.	Enabled

- Click the **Protocols** tab and drag and drop to specify the default protocol Crosswork should use when transferring images in the Image Transfer Protocol Order. Arrange the protocols in order of preference. If the first protocol listed fails, Crosswork will use the next protocol in the list.



Note Refer to the [Cisco Crosswork Network Controller Essentials Supported Devices](#) for more information about support for SWIM on different devices.

Add a software image to the image repository

To add a software image, follow these steps:

Procedure

-
- Step 1** From the main menu, navigate to **Device Management > Software Management**.
- Step 2** Click the **Add** icon under the **Images** tab.
- Step 3** Select the method for adding software images.
- **From a client machine:** Choose the **File** radio button, browse to select the image, and click **Add**.
 - **From a server:** Choose the **URL** radio button, ensuring the file adheres to the recommended naming convention.

Example: `image family-*-image version.tar`, where the image family is in capital case, like `NCS540-iosxr-k9-7.0.0.tar`.

- **From a managed device:** Choose the **Device** radio button, select the device name.

Step 4 Opt to **Run Now** or **Schedule Later**, and click **Schedule**.

Step 5 Verify that the image is listed on the **Software Images** page under **Device Management > Software Management**.

Deploy a new software image to devices

The image distribution process requires transferring a new software image to a designated location on a device. You can deploy images across multiple similar devices within a single deployment, customizing options for each device as needed. Crosswork Network Controller ensures that only devices compatible with the selected image are displayed, facilitating a seamless deployment experience.

When setting up the distribution job, you have the flexibility to choose whether Crosswork Network Controller should deploy the image immediately or schedule it for a later time. You can manage up to five concurrent distribution operations, excluding active operations, and provides real-time feedback and status updates throughout the process. For large-scale deployments, we recommend to stagger device reboots to ensure continuous service during upgrades.

Pre-deployment checklist

- **Memory and disk space:** Ensure sufficient memory and clear disk space for distributing the image.
- **Device compatibility:** Verify the suitability of the device for the chosen image.
- **Secure protocols:** Use the most secure protocols supported by the device for distribution.
- **Geographical considerations:** Ensure the device and server are in the same geographical location to optimize efficiency and reduce errors due to slow network speeds.

Procedure

Step 1 From the main menu, select **Device Management > Software Management**.

Step 2 **Select an image:** Under the **Image ID** tab, view the list of available software images in your repository. Select the **Image ID** that you want to distribute. When you create a distribution job, you can configure the image for each device or do a bulk distribution for a type of devices.

Note

If the required device is not listed, verify that the image family associated with the file matches the family of the selected device.

Step 3 Select the device for image distribution.

Step 4 **Verify compatibility:** In the **Verification** window, check the details of the software image on the device. Compatible devices will display a SUCCESS message in the Status column. The UI suggests compatible software and storage partitions. You can also choose to deploy the images on a device or on an external server.

Step 5 **Configure deployment:** Select the various settings according to your preferences. The image deployment options that are available are:

a. Distribution settings:

- Smart flash delete: Recover disk space by deleting non-running files.
- Erase running image: Option to erase the device's current image.

b. Activation settings:

- Boot command insertion: Insert the boot command after distribution.
- Image activation: Choose sequential or parallel deployment for multiple images.
- Commit: Option to commit the image post-distribution for XR devices.
- FPD image upgrade: Enable to automatically upgrade Field Programmable Devices during distribution.

c. Device running mode:

- Bundle mode: Use a monolithic image to boot. Requires device reload post-activation.
- Install mode: Activate image in subpackage mode without reloading (ISSU).
- Currently exists: Activate the image using the device's current mode.

d. Advanced settings:

- Continue on failure: Opt to continue activation or distribution on other devices if one fails.
- Interface module delay: Select to adjust the delay between the Online Insertion and Removal (OIR) of each interface module.
- Distribute via default VRF: Enable image distribution through VRF.

Step 6 **Scheduling:** On the **Schedule** page, choose to run the job immediately or at a later time, then click **Schedule**.

Step 7 **Monitoring:** To view details about the image distribution job, access the **Jobs** tab under **Software Management**.

Activate a new software image on devices

When a new image is activated on a device, it becomes the running image on the disk. Deactivated images are not removed when a new image is activated. You must manually delete the image from the device.

To activate an image without distributing a new image to a device—for example, when the device has the image you want to activate—use the following procedure.

Procedure

Step 1 From the main menu, go to **Device Management > Software Management**.

- Step 2** Click the **Jobs** tab to view details about the image distribution jobs that you have created. This section lists job details such as job type, status, and run time. For more information on a specific job instance, click on the corresponding hyperlink.
- Step 3** Select a software image distribution job which has been run successfully and click the **Activate** button,
- Step 4** Select the devices for the image distribution and click **Next**.
- Step 5** In the **Activation settings** window, choose the settings according to your preference.
- Step 6** Click **Next** and choose **Run Now** or **Schedule Later** to activate the software image in the selected devices.
- Step 7** Click the **Schedule** button to submit the changes.

See the table *Cisco devices and supported image distribution Protocols* for information on Cisco devices and the protocols that they support for image distribution:

Table 22: Cisco devices and supported image distribution protocols

Cisco Devices	FTP	SCP	SFTP	HTTPS
Cisco ASR 1000 series routers	Yes	No	Yes	No
Cisco ASR 9000 series routers	No	No	Yes	No
Cisco IOS-XR (except Cisco ASR 9000 series routers)	Yes	Yes	Yes	No
Cisco ASR 900 series routers	Yes	Yes	No	No

Delete software image files from the image repository

Software images can only be manually deleted from the image repository. With the right privileges, you can use the following procedure to delete software image files from the image repository.

Procedure

- Step 1** Choose **Device Management > Software Management**.
- Step 2** From the **Images** window, select one or more images that you want to delete.
- Step 3** Click the **Delete** icon to delete the image.

■ Delete software image files from the image repository



PART **III**

Monitor the Network

- [Set Up and Monitor Alarms and Events, on page 161](#)
- [Monitor Device and Inventory Health, on page 173](#)



CHAPTER 7

Set Up and Monitor Alarms and Events

By configuring alarms and events, you can effectively manage system performance and promptly address emerging issues. Navigate to **Alerts > Alarms and Events** page from the main menu. The **Alarms and Events** window is displayed.

Navigating alarms and events

- **Switch views:** On the **Alarms and Events** page, use the **Alarms** or **Events** button next to the **Show** option to toggle between the Alarms and Events windows.
- **Alarm categories:** Access the **Category** drop-down list to view different alarm types, including system, network, and device alarms.
 - **System alarms:** Concerned with overall system infrastructure. For information on system alarms, refer to the *View system alarms* section in the *Cisco Crosswork Network Controller 7.1 Administrator Guide*.
 - **Network alarms:** Related to network performance and connectivity.
 - **Device alarms:** Specific to individual network devices.

Customizing alarms using REST APIs:

- You can use the Crosswork Representational State Transfer (REST) APIs to access system, network and device fault information, configure syslogs, and set up trap and packet infrastructure (PKT-FM-INFRA) alarms.
- See the [Crosswork Alarms and Events APIs](#) and [Crosswork Element Management Functions Fault APIs](#) documentation for instructions on how to create, update, acknowledge, and clear alarms using REST APIs.

This section contains the following topics:

- [What Are Alarms and Events?, on page 162](#)
- [Interpret Event and Alarm Badges and Colors, on page 162](#)
- [Which Events Are Supported?, on page 162](#)
- [Set Alarm Thresholds to Manage How Alarms are Triggered, on page 163](#)
- [Configure the Settings for Alarms and Events , on page 163](#)
- [Manage Alarms, on page 169](#)
- [Clear Alarms, on page 170](#)

- [Annotate Alarms, on page 171](#)
- [Export Alarms, on page 171](#)

What Are Alarms and Events?

An *event* is a distinct incident that occurs at a specific point in time, such as a port status change, or a device becoming unreachable. Events can indicate an error, failure, or exceptional condition in the network. Events can also indicate the *clearing* of those errors, failures, or conditions.

An *alarm* is a response to one or more related events. Only certain events generate alarms. Alarms have a state (cleared or not cleared) and a severity (Critical, Major, Minor, and so forth). An alarm inherits the severity of its most recent event. Alarms remain open until a clearing event is generated (or if the alarm is manually cleared).

Interpret Event and Alarm Badges and Colors

When there is a problem in the network, Crosswork flags the problem by displaying an alarm or event icon with the element that is experiencing the problem. The following table lists the icons and their colors.

The table below lists the alarm colors and their respective severity levels for the icons displayed in various parts of the web GUI.

Severity Icon	Description	Color
	Critical alarm	Red
	Major alarm	Orange
	Minor alarm	Yellow
	Warning alarm	Light Blue
	Alarm cleared; normal, OK	Green
	Informational alarm	Medium Blue

Which Events Are Supported?

To view the supported alarms and events within Cisco Crosswork, access the following link: [Cisco Crosswork Supported Alarms and Events](#). This document contains a detailed list of the alarms and events that are compatible with the Cisco Crosswork platform.

Set Alarm Thresholds to Manage How Alarms are Triggered

You can modify performance policies to customize how often information is gathered (polling interval), the threshold value that indicates a problem, and whether Crosswork Network Controller should generate an informational event or an alarm (of a severity) when a problem is detected. Not all policies have all of these settings; for example, a policy may only collect statistics, so it would not have any thresholds or alarms associated with it.

Procedure

-
- Step 1** Choose **Device Management** > **Performance Policies** and select the policy you want to edit.
 - Step 2** Click on the **Threshold** tab and locate the parameter you want to change.
 - Step 3** Click on the **Actions** tab and select **Edit**.
 - Step 4** Choose the device or the device group or the port group for the polling interval and click **Next**.
 - Step 5** To adjust the polling interval, select the new interval from the **Polling Frequency** drop-down list. To disable polling, choose **No Polling**. Note that some polling frequencies are applied to groups of parameters. Changing the group interval will change the polling for all settings in the group.
 - Step 6** To change a threshold value, expand the parameter and choose a value from the parameter's drop-down list.
 - Step 7** To specify what Crosswork Network Controller should do when the threshold is surpassed, choose an alarm value from the parameter's drop-down list. You can configure Crosswork Network Controller to generate an alarm of a specified severity, generate an informational event, or do nothing (if no reaction is configured).
 - Step 8** Click **Save**.
-

Configure the Settings for Alarms and Events

Configure and customize your settings for alarms and events in Crosswork Network Controller to effectively monitor your devices. You can customize alarm notification destinations, device notifications, or adjust gNMI settings, among other available options. These customizations allow you to receive timely alerts and tailor notifications to specific devices.

Customize Alarm Auto Clear

Crosswork lets you customize whether an alarm can be automatically cleared and how many minutes to wait before automatically clearing it.

Procedure

-
- Step 1** From the main menu, choose **Administration** > **Settings** > **Alarms and Events** > **Severity and auto clear**. Crosswork displays the **Severity and auto clear** window, showing the list of all the standard alarm types.

- Step 2** (Optional) Filter the list of alarms by entering or selecting values in one or more of the **Name**, **Category**, **Severity**, and **Auto clear duration** column filter fields. You can toggle the filter fields on and off by clicking on the .
- Step 3** To assign a time after which an alarm will be automatically cleared, click on the check box shown next to that alarm's name in the list. Then click **Alarm auto clear**.
- Step 4** With the **Alarm auto clear** window displayed, enter the number of minutes to wait before clearing in the **Clear alarms after** field. Then click **OK**.

Figure 52: Alarm Auto Clear Window



- Step 5** To stop an alarm from being automatically cleared, first select it in the list and then click **Revert auto clear**.
- Step 6** When you are finished making changes, click **Save** to apply them.

Customize Alarm Severity

You can customize the Crosswork alarm database to assign your choice of severity levels to particular alarms.

Procedure

- Step 1** From the main menu, choose **Administration > Settings > Alarms and Events > Severity and auto clear**. Crosswork displays the **Severity and auto clear** window, showing the list of all the standard alarm types.
- Step 2** (Optional) Filter the list of alarms by entering or selecting values in one or more of the **Name**, **Category**, **Severity**, and **Auto clear duration** column filter fields. You can toggle the filter fields on and off by clicking on the .
- Step 3** To customize the severity of an alarm, click on the check box shown next to that alarm's name in the list. Then click **Actions > Severity configuration** to display **Severity Configuration Page**.

Figure 53: Severity Configuration Page



Step 4 Click on the severity level you want to assign to the alarm. Then click **OK**.

Step 5 When you are finished making changes, click **Save** to apply them. Changes to severity levels will only affect new alarms generated after the update.

Manage cleanup options for alarms, events, and audit logs

Alarms, events, and audit logs are automatically deleted based on the default settings that is configured in the **Cleanup options** page. The settings are enabled by default and are designed to maintain efficiency. When adjusting these settings, exercise caution, especially if managing a very large network. To access and modify these settings, follow these steps:

Procedure

Step 1 From the main menu, choose **Administration > Settings > Alarm and events settings > Alarms and events > Cleanup options**.

You can see the default values and the valid range for each setting.

Step 2 Review and choose to retain these default values or adjust them within the permissible range specified in the UI.

Step 3 Click **Save** to apply any changes.

Customize device alarm manager settings

Crosswork Network Controller lets you customize the set of Cisco devices from which you want to receive alerts. These alarms are generated by the Device alarm manager for Cisco IOS XR devices. Crosswork Network Controller polls the alarm manager within these devices to detect any outstanding alarms or events.

- The devices for which the alarm manager has been enabled are polled every five minutes.
- The `show alarms` command is executed during the polling process to retrieve all open alarms currently present on the device. Using the data retrieved by this command, the Crosswork Network Controller performs a comparison process. This process matches the alarms reported by the device with the alarms already recorded in the Crosswork Network Controller, ensuring synchronization.

- As part of this comparison, the Crosswork Network Controller clears alarms that have been resolved or creates new alarms to accurately reflect the device's current state.
- These alarms have a fixed severity level that cannot be overridden in the system settings.
- Alarms raised by the alarm manager are displayed with the source labeled as Synthetic_Event.

Procedure

-
- Step 1** From the main menu, choose **Administration > Settings > Alarms and events > Device alarm manager**. Crosswork displays a list of all the supported Cisco devices from which Crosswork can receive alerts.
- Step 2** (Optional) Filter the list of devices by filtering on the **Name** and **Status** column filter fields. You can toggle the filter fields on and off by clicking on the .
- Step 3** To start receiving alerts from a device type, click the checkbox shown next to the device type's name and then click **Enable**.
- When enabled, all alarms generated by the device alarm manager will appear in the UI.
- Step 4** To stop receiving alerts from a device type, click the selection checkbox shown next to the device type's name and then click **Disable**.
- When disabled, Crosswork Network Controller will no longer poll the devices. However, the device manager alarms will be visible in the UI. You can clear these alarms manually.
- Step 5** Click **Save**.
-

Customize Device Notifications

Crosswork lets you customize the notifications received for traps and syslogs.

Procedure

-
- Step 1** From the main menu, choose **Administration > Alarm and Events > General**.
- Step 2** Enable or Disable the **Trap processing** slider to handle trap notifications from your network devices.
- Step 3** Enable or Disable the **Syslog processing** slider to handle event notification messages or syslog messages from the devices in your network.
- Step 4** When you are finished making changes, click **Save** to apply them.
- Click **Discard Changes** if you do not want to save the changes you made.
-

Customize gNMI Settings

Crosswork lets you customize the set of Cisco devices from which you want to receive gNMI alerts. Note that this feature is enabled for third-party platforms. If you want to enable this functionality for Cisco platforms, you have to activate it manually.



Note gNMI support is not available on Cisco IOS XE devices and limited to the `openconfig-system/alarms` path on Nexus devices.

Procedure

- Step 1** From the main menu, choose **Administration > Settings > Alarms and Events Settings > Alarms and Events > GNMI**. Crosswork displays the **GNMI** window, with a list of supported vendors from which Crosswork Network Controller can receive alerts.
- Step 2** (Optional) Filter the list of vendors by filtering on the **Name** and **Status** column filter fields. You can toggle the filter fields on and off by clicking on the .
- Step 3** To start receiving alerts from a vendor, click the checkbox shown next to the vendor's name and then click **Enable**.
- Step 4** To stop receiving alerts from a vendor, click the selection checkbox shown next to the vendor's name and then click **Disable**.
- Step 5** Click **Save** to apply the changes.

Configure Alarms Notification Destination

You can configure the Northbound trap or syslog receiver settings to forward the alarms generated by Crosswork Network Controller. You can also forward your notifications to an external Kafka server.

Procedure

- Step 1** From the main menu, choose **Administration > Settings > Alarms and Events Settings > Notification Destination**.
- Step 2** Click the **Add** icon to create a new notification destination.
- Step 3** To configure a Northbound trap receiver using IP Address, do the following:
 - a) From the **Destination** dropdown, choose **Trap receiver**.
 - b) Select the **IP address** radio button and enter the **IP address**.
 - c) Enter the **Port number**, and choose the **SNMP version**.
 - d) If you choose the **SNMP Version** as **v2c**, enter the **Community** settings as required.
 - e) If you choose the **SNMP version** as **v3**, enter the **Username**, **Mode**, **Auth. type**, **Auth.Password**, **Confirm auth. password**, **Privacy type**, **Privacy password** and **Confirm privacy password**.
 - f) Click **Save**.
- Step 4** To configure a Northbound trap receiver using DNS, do the following:
 - a) From the **Select contact type**, choose **Northbound trap receiver**.

- b) Select the **DNS** radio button and enter the **DNS Name**.
- c) Choose the required **Receiver Type** and **Notification type**.
- d) Enter the **Port number**, and choose the **SNMP version**.
- e) If you choose the **SNMP version** as **v2c**, enter the **Community** settings as required.
- f) If you choose the **SNMP Version** as **v3**, enter the **Username**, **Mode**, **Auth. type**, **Auth. password**, **Confirm Auth. password**, **Privacy type**, **Privacy password** and **Confirm Privacy password**.
- g) Click **Save**.

Step 5 To publish notification messages for alarms to external Kafka server, configure a External Kafka as the destination by doing the following:

- a) From the **Destination** drop-down list, choose **External Kafka**.
- b) Select a Kafka topic name created by Crosswork Network Controller REST API.
- c) Click **Save**.

Note

- While updating the Notification Destination Trap Receiver, the operational status that the previous Trap Receiver status until the status is updated by the next polling.
- You cannot delete Notification Destinations which are associated with Notification Policies.
- If you reinstall an already existing external Kafka data destination with the same IP address, then the collectors need to be restarted for changes to take place.
- If your external data destination requires a TLS connection, keep the public certificate ready or if it requires client authentication, keep the client certificate and key files ready. The client key might be password-encrypted which will need to be configured as part of the data destination provisioning. Currently, Crosswork supports IP-based certificates only.
- Ensure that the certificates are PEM encoded and the key file is in PKCS#8 format when generating them with your Certificate Authority.
- Crosswork logs may display exceptions related to non-existent topics during the dispatching of collected data to an external Kafka. These exceptions can occur if the specified topic within the external Kafka has not been created or was deleted before the data collection job was completed and the data dispatch began.
- The alarm notifications are filtered based on the alarm policy that you have configured for the destination.

Create a Notification Policy for Network and Devices

This topic explains the steps to create a notification policy for network and devices. With these policies, you can control the alarms and events generated based on conditions you specify.

For information on notification policies for system events, see the *Create Notification Policy for System Event* section in the *Cisco Crosswork Network Controller 7.0 Administration Guide*.

Procedure

Step 1 From the main menu, choose **Alerts > Notification Policies**.

The **Notification Policies** window is displayed.

Step 2 Click **Create** and select **Devices alarms and events** or **System/Network events**.

The **Create** window is displayed.

Step 3 Under **Policy attributes**, enter relevant values for the following fields:

- Policy name
- Description

Step 4 Click **Next**.

Step 5 If you have selected **Devices alarms and events**:

- Under **Alarm/Event types**, select the event type(s) for the notification policy and click **Next**.
- Select one of the device groups to be part of the alarm policy.

Step 6 Under **Destination**, select the destination(s) for the notification policy. The destination can be a trap receiver, syslog receiver, or an external kafka. Add the details of the notification destination and click **Save**.

If there are no destinations available, click the *Add* icon to add a destination. Refer to the next section, [Configure Alarms Notification Destination, on page 167](#) in this guide.

Step 7 Click **Next** and review the summary details.

Step 8 Click **Save** to confirm the policy details.

Manage Alarm Suppression Policy

When you need to temporarily disable notifications for specific conditions such as system maintenance or known issues, you can implement an alarm suppression policy to prevent unnecessary alerts. To create a new Alarm Suppression Policy:

Procedure

Step 1 From the main menu, go to **Alerts > Alarm Suppression Policy**.

Step 2 Give your policy a name and description and choose if you want to suppress **Alarms** or **Alarms and Events**. Click **Next**.

Step 3 Select the device groups to which you want the policy applied and click **Next**.

Step 4 Select one or more event types for your policy and click **Next**.

Step 5 You can see the summary of your policy in the **Summary** window. Click **Save** to save your alarm suppression policy.

Manage Alarms

Manage your alarms effectively to maintain network health and ensure prompt responses to potential issues. Crosswork allows you to acknowledge, unacknowledge, clear, and annotate alarms within the controller.

Procedure

-
- Step 1** From the main menu, choose **Alerts > Alarms and Events**. Crosswork displays the **Alarms and Events** window.
- Step 2** (Optional) Filter the list of alarms by filtering columns, or by adding or removing columns using the  and then filtering again. Use the **More options** dropdown to choose whether you want to see only current alarms, and how often the window syncs the displayed list with the Crosswork database. Check the **Active alarms only** checkbox to show all alarms.
- Step 3** Check the check box next to the ID of the alarm(s) for which you want to take action.
- Step 4** Click **Actions** and select one of following the options:
- **Acknowledge:** Acknowledge alarms to indicate that they have been recognized and are being addressed. Acknowledging an alarm clears it permanently, but the alarm will still be listed in the **Alarms and Events** window.
 - **Unacknowledge:** Unacknowledge alarms to revert their status to indicate they need further attention.
 - **Clear:** Clear alarms once the issues have been resolved, ensuring your dashboard reflects current network status. Clearing an alarm removes it from the **Alarms and Events** window, but the alarm will be generated again if the triggering event recurs.
 - **Notes:** Annotate alarms by adding notes and comments for better tracking. Notes are permanently attached to the alarm and are retrievable until the alarm is cleared from the database or deleted by a user. The user ID of the note taker is stored with the note.
- Step 5** Enter an appropriate note and click the applicable button to complete the action.
-

Clear Alarms

Follow these steps to clear device alarms. You can clear one or multiple alarms by selecting their check boxes. You can also choose to clear all alarms reporting the same alarm condition (such as "lostFlow" or "mplsTunnelDown").

Clearing an alarm removes it from the **Device Alarms** window, but the alarm will be generated again if the triggering event recurs.

Procedure

-
- Step 1** From the main menu, choose **Alerts > Alarms and Events**. Crosswork displays the **Alarms and Events** window.
- Step 2** (Optional) Filter the list of alarms by filtering columns, changing the **Active Alarms Only** slider to show all alarms, or by adding or removing columns using the . Use the **More Options** dropdown to choose whether you want to see only current alarms or all alarms, and how often the window syncs the displayed list with the Crosswork database.
- Step 3** Check the check box next to the ID of the alarm(s) you want to clear, then select **Actions > Clear**.
- Step 4** Click **OK** to complete the clear action.
- Step 5** To clear all alarms sharing the same condition:

- a) Check the check box next to the ID of one or more alarms sharing the conditions you want to clear (you may select alarms with different conditions).
 - b) Select **Actions > Clear all of this condition**.
 - c) Click **OK** to complete the clear-all action.
-

Annotate Alarms

Alarm notes are a handy way to share information and record important information missed by automated monitoring. Notes are permanently attached to the alarm and are retrievable until the alarm is cleared from the database or deleted by a user. The user ID of the note taker is stored with the note.

Follow the steps below to annotate device alarms. You can annotate multiple alarms at the same time by selecting their check boxes before choosing to add a note. Notes support entries in plain text only.

Procedure

- Step 1** From the main menu, choose **Alerts > Alarms and Events**. Crosswork displays the **Alarms and Events** window.
 - Step 2** (Optional) Filter the list of alarms by filtering columns, changing the **Active Alarms Only** slider to show all alarms, or by adding or removing columns using the . Use the **More Options** dropdown to choose whether you want to see only current alarms or all alarms, and how often the window syncs the displayed list with the Crosswork database.
 - Step 3** Check the check box next to the ID of the alarm(s) you want to annotate.
 - Step 4** Select **Actions > Notes**. Crosswork displays the **Add annotation** popup.
 - Step 5** Enter the text of the note you want to add to the selected alarm(s).
 - Step 6** Click **Add** to add the note.
-

Export Alarms

Follow these steps to export device alarms for offline storage and analysis.

You must be viewing alarms to export alarms, or events if you want to export events. You can choose to export alerts to comma-separated values (CSV) or PDF file formats.

By default, Crosswork Network Controller exports all the alarms currently visible in the **Alarms and Events** list. You can limit the contents of the exported file to just the alerts you want by filtering the list, or selecting the checkbox next to the alerts you want, before clicking the .

Procedure

- Step 1** From the main menu, choose **Alerts > Alarms and Events**. Crosswork displays the **Alarms and Events** window.
If you want to export events instead of alarms: In the **Show** dropdown, select **Events**.

- Step 2** (Optional) Filter the list of events to be exported by filtering columns, or by adding or removing columns using the  and then filtering again. Use the **More options** dropdown to choose whether you want to see only current alerts or all alerts, and how often the window syncs the displayed list with the Crosswork database.
- For alarms only: Check the **Active alarms only** checkbox. You can also check the check box next to the ID of the alerts you want to export.
- Step 3** Click . Crosswork displays an export popup window appropriate for the type of alert you want to export.
- Step 4** In the **File name** field, enter the name of the destination file (don't include a filename extension).
- Step 5** Using the **Format** button, select **CSV** or **PDF**.
- Step 6** Click **Export** to begin the export, and specify the storage location for the new file.
- If you manually select the alarms, only 100 records can be exported. If no alarms are selected, 20,000 records can be exported at a time.
-



CHAPTER 8

Monitor Device and Inventory Health

This section contains the following topics:

- [How are device and inventory health monitored?, on page 173](#)
- [Create monitoring policies, on page 176](#)
- [View collection jobs for performance monitoring, on page 176](#)
- [Customize metrics for network analysis, on page 177](#)

How are device and inventory health monitored?

Monitoring policies determine how the Crosswork Network Controller monitors your network by specifying the following:

- What is monitored: The network and device attributes.
- How often it is monitored: The rate at which parameters are polled.
- When to indicate a problem: Acceptable values for the polled attributes.
- How to indicate a problem: Trigger an alarm if a threshold is exceeded and set its severity.

Monitoring policies are important as they allow you to select what to monitor without making any changes to devices. These steps summarize how to set up a monitoring policy and configure metrics visualizations:

1. **Select a policy type:** Choose the appropriate policy type for your monitoring needs and select the devices you wish to monitor.
2. **Configure polling frequencies and TCAs:** Set the policy polling frequencies and specify the Threshold Crossing Alarms (TCAs) that Crosswork should generate when a threshold parameter is exceeded.
3. **Configure Top N metrics:** Categorize the health parameters, establish data retention periods, and configure visualization for Top N metrics.
4. **Customize your dashboard:** Tailor the metrics dashboard to track and display critical metrics.

To view and administer monitoring policies, navigate to **Device Management > Performance Policies**. This page displays both default and user-created policies. From here, you can activate, deactivate, edit, or delete a policy.

Parameters monitored by each policy

This section outlines the specific parameters monitored by each policy type. Each policy targets specific aspects of device health and functionality, providing focused monitoring solutions.

The table lists the different parameters a policy monitors for a particular policy type.

Policy type	Parameters the policy monitors
Device health	The device health monitoring policy monitors Cisco devices and third-party devices. For Cisco devices, the policy checks managed devices for CPU utilization, memory pool utilization, environment temperature, and device availability. For third party devices, the policy checks devices for device availability only. This policy also specifies thresholds for utilization and temperature which, if surpassed, trigger alarms that are displayed in the UI. Parameters- Memory pool utilization, CPU utilization, environmental temperature, device availability Note The device health monitoring policy excludes Cisco NCS 2000 and Cisco ONS devices. Optical monitoring policies should be used for these device types.
GNSS	A GNSS (Global Navigation Satellite System) monitoring policy monitors the performance and reliability of GNSS receivers within a network. It polls status and signal quality of satellites. Parameters- • Antenna open alarm, antenna short alarm, module lock, module presence, satellite lock count, module slot info, module slot state, module visibility status
Interface health	An interface health policy monitors attributes to assess interface operational status and performance in a network. Parameters- Statistics and CRC
LSP traffic	A LSP traffic policy tracks traffic routed through an MPLS (Multiprotocol Label Switching) network and ensures that data packets are being efficiently routed. Parameters- • Outgoing traffic rate and outgoing packets rate
Optical SFP	An optical SFP policy polls health and performance information for optical SFP (Small Form-Factor Pluggable) interfaces. It is available for all Cisco pluggable devices supporting DOM (Cisco Digital Optical Monitoring). Parameters- Received optical power, temperature, transmitted bias current, current, transmitted optical power, voltage

Policy type	Parameters the policy monitors
Optical ZRP	An optical ZR pluggable policy polls health and performance information for ZR optical transceivers within a network. Parameters- • Optics lane- Maximum, minimum, and average transmit and receive power levels. • OTU controllers- Error corrected bits, Post-Fec-Ber, Pre-Fec-Ber, Q-factor, Q -margin, uncorrectable words
PTP/ SyncE	A PTP/SyncE policy monitors the Precision Time Protocol (PTP) and Synchronous Ethernet (SyncE) within a network. The PTP/ SyncE policy monitors clock synchronization of primary clocks on devices and the quality of clock signals. Parameters- • PTP- Clock class, clock state and clock UTC offset • Input quality level

Manage default policies

LSP traffic and **Interface health** policies are enabled by default on Crosswork version 7.1. Manage the default policies based on these considerations:

- **Viewing default policies:** Access and review the default policies on the **Performance Policies** page.
- **Upgrade considerations:** During the upgrade from Crosswork Network Controller version 7.0 to version 7.1, if no LSP traffic or interface health policies were configured, these policies are created by default.
- **Customizing default policies:** You can customize the default policies according to your preferences. Changes to default policies may impact Crosswork Optimization Engine (COE) operations if COE is installed.
- **Impact of deactivating or deleting default policies:** Deactivating or deleting default policies may impact COE functionalities. It may also affect visualizations and data displays within the topology user interface. Evaluate the impact of the default policies carefully before making changes.

Configure gNMI based polling for interface health and LSP traffic policies

SNMP is the default protocol used for data polling in Crosswork Network Controller. You can also enable gNMI based polling for interface health and LSP traffic policies. To enable gNMI polling, the device must have the `pm-openconfig` tag assigned, and gNMI capability must be configured. Once you enable gNMI, the tagging and configuration changes take effect in the next polling cycle.

If a device is tagged with `pm-openconfig` but lacks gNMI capability, polling will switch to SNMP to ensure data collection.

To enable gNMI protocol for interface health or LSP traffic monitoring policies, complete these actions:

Procedure

- Step 1** Navigate to the **Tag Management** page in the Crosswork Network Controller UI and create the `pm-openconfig` tag.
- Step 2** Assign the tag to the intended devices. The tag can belong to any category and be added or removed at any time.
- Step 3** Configure gNMI capability on the required devices.

See the *Cisco Crosswork Network Controller 7.1 Administration Guide* for instructions to create and assign tags and configure gNMI for your devices.

Note

Refer to the section, [Manage default policies](#) before you customize any default policies.

Create monitoring policies

To set up and enable a monitoring policy, go to the main menu, select **Device Management > Performance Policies** and click on **Create new policy**.

Procedure

- Step 1** **Select policy type:** Choose a policy type from the **Select policy type** drop-down list.
- Step 2** **Enter policy details:** Provide the policy name and other relevant details.
- Step 3** **Select devices:** Choose the appropriate radio button for the device or device groups you want to monitor. For specific policies like interface health, optical SFP, or optical ZRP, you can also select port groups for monitoring.
- Step 4** **Set polling frequency:** Adjust how often the devices are polled by selecting a value from the **Polling frequency** drop-down list. Some policies allow different polling frequencies for various parameters, while others apply a single frequency to all parameters.
- Step 5** **Configure alarm thresholds:** If the policy supports TCA customization, enable the **Configure alarm threshold** slider to set thresholds. You can add multiple thresholds.
- Step 6** **Activate monitoring:** Click **Activate** to start monitoring. The policy and its details will be listed under **Performance Policies > View details**.
- Step 7** **Manage policies:** To manage a policy, click **View details**, then select **Actions** to deactivate, edit, or delete a policy. You can edit a performance policy during maintenance mode, but changes may not immediately reflect due to maintenance activities. They are fully deployed once Crosswork exits maintenance mode.

View collection jobs for performance monitoring

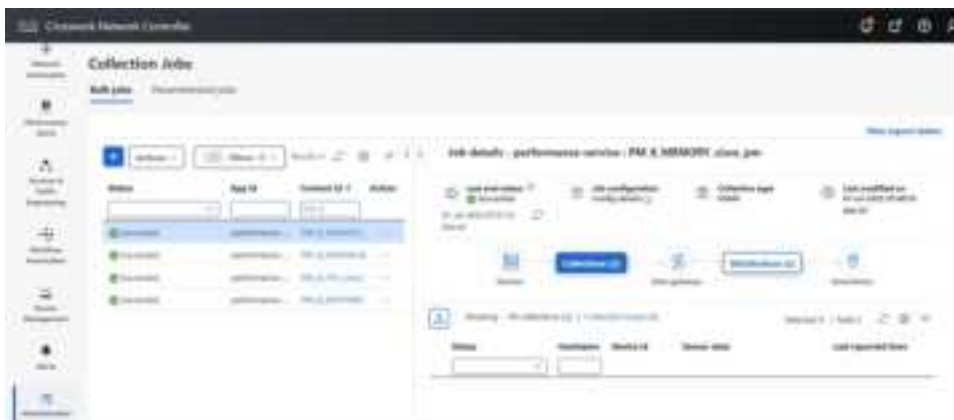
You can monitor the status of collection jobs associated with active performance policies. These jobs are displayed on the **Collection Jobs** page.

To view the collection job for a monitoring policy, follow these steps.

Procedure

- Step 1** Go to **Device Management > Performance Policies**.
- Step 2** Switch to the list view to display the **ID** column.
- Step 3** Identify and note the **ID** of the specific performance policy you want to monitor.
For example, if the policy ID is 6, all collection jobs with the prefix PM_6 will be related to this policy.
- Step 4** To view the collection job, go to **Administration > Collection Jobs**.
All the collection jobs with the app id **performance-service** are related to performance monitoring.
- Step 5** Use the **Context ID** filter to locate jobs related to the specified performance policy. For example PM_6, PM_2.
This applies to both bulk and parameterized jobs.
- Step 6** Click on the **Context ID** link for the chosen performance policy to access detailed job information.

Figure 54: Collection jobs for monitoring policies



Customize metrics for network analysis

Crosswork Network Controller enables you to analyze a wide range of metrics related to the monitoring policies you define.

Within the UI, you can access these metrics across all **History** tabs, providing insights into network performance. Crosswork Network Controller processes the data over a one hour period before running a preprocessing task to calculate the histogram and summary. In the histogram graphs, the time shown represents the start of the one-hour period. For instance, if the hourly report displays 8:00, it means the data corresponds to the time range from 8:00 to 9:00.

Additionally, you can configure Top N metrics to monitor the key metrics you wish to track, and customize your dashboard to visualize these essential metrics across your network. This enables you to effectively focus on key performance indicators and streamline network management.

There are four levels at which you can investigate metrics:

- **Network aggregation:** Analyze data across the entire network to identify overall patterns and trends.
- **Trend analysis:** Examine historical data to detect changes and trends over time.
- **Top element identification:** Identify the highest-performing or most critical elements within the network.
- **Individual element trend viewing:** Focus on specific elements to track their performance trends and changes.

Refer to the following sections to define Top N metrics for your network:

- [Customize metric health settings, on page 178](#)
- [Set data retention periods for monitored metrics, on page 179](#)
- [View key metrics, on page 180](#)

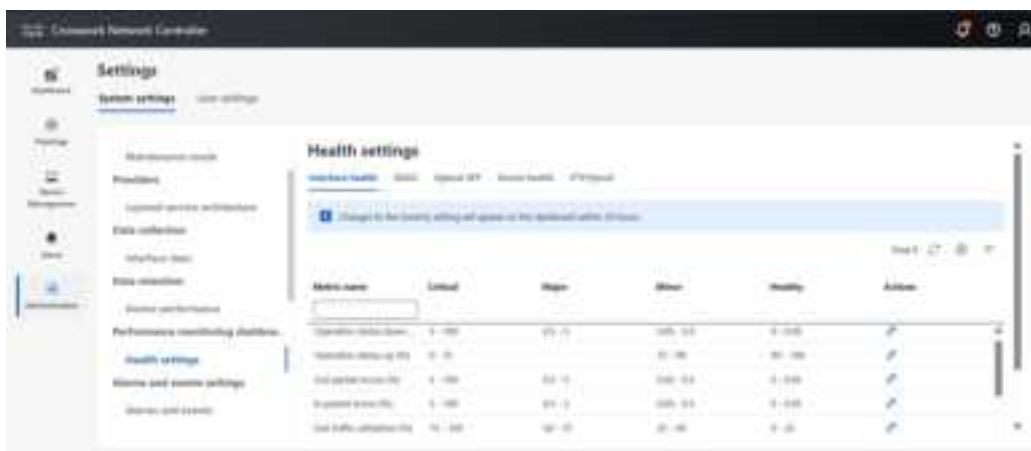
Customize metric health settings

Before setting up metrics visualization, define the metric health categories. Set thresholds for each metric to determine what is considered healthy, major, minor, or critical. While default categories and thresholds are available, you can customize them to suit your needs.

Procedure

Step 1 From the main menu, navigate to **Administration > Settings > Performance monitoring dashboard > Health settings**.

Figure 55: Health settings



Under the **System settings** tab, explore the different metrics tabs by policies you have created. Each tab displays all metrics related to that policy.

Step 2 Set metric health thresholds:

- Click the **Edit** button under the **Actions** column to define the severity of the collected metrics.

- b. You can reset thresholds to default values individually or for all metrics under a single policy at once.

Example:**1 Setting threshold values for interface health policy parameters**

- a. Click on the policy tab to view the listed metrics.
- b. Click the **Edit** button under **Actions** for **Out Packet Drops**.
- c. Set severity ranges for healthy, minor, major, and critical.
- d. Click **Save**.

Example:**2 Setting threshold values for PTP/ SyncE policy parameters**

Select each parameter to define the values.

- **Clock class:** Enter the PTP clock class values (0–255) to configure severity levels which ensures accurate timing synchronization.
- **Clock state:** Configure the clock state settings to identify synchronization status.
 - Freerun: Operates independently without synchronization.
 - Holdover: Maintains the last known good state temporarily.
 - Acquiring: In the process of obtaining synchronization.
 - Frequency locked: Frequency is synchronized, but phase alignment is not achieved.
 - Phase aligned: Fully synchronized in both frequency and phase.
- **Input quality level:** Select from one or more quality parameters like DNU (Do Not Use), PRC (Primary Reference Clock), UNC (Uncertain), UNK (Unknown) to assesses the reliability of the clock source.
- **Clock UTC offset:** Set the time difference between the local clock and UTC to account for time zone differences.

Note

The new settings are applied to future reports, while past or previously calculated periods will continue to use the old settings.

Set data retention periods for monitored metrics

Define the retention periods for metrics data. This ensures that your network analysis aligns with your specific monitoring needs and storage capabilities. Follow these steps to access and modify data retention settings.

Procedure

-
- Step 1** Navigate to **Administration > Settings > Data retention > Device performance**.
 - Step 2** Use the policy type dropdown menu to filter the desired policy type.

Step 3 For a selected policy, choose the performance metrics you wish to edit and click the edit icon.

Default data retention values are provided. You can customize the retention period by specifying it for raw data, hourly data, daily data, and weekly data.

View key metrics

Customize the **Top Metrics** view and monitor the critical metrics of your choice.

Procedure

Step 1 From the main menu, navigate to **Device Management > Top Metrics**.

Step 2 **Select metrics and filters:**

- a) **Choose a category:** From the **Select Metrics** dropdown, choose from the categories: Device health, GNSS, Interface health, LSP traffic, Optical SFP, Optical ZRP, and PTP/SyncE. The categories depend on the monitoring policies you have set.
 - b) **Adjust filter settings:** Select categories such as critical, major, minor, and healthy. Filter by device groups or port groups or by choosing metrics ranging from the top 10 to top 500.
 - c) **View trends:** Under the **Actions** tab, click the three dots for a device and select **View trends**. You can use this feature to identify when an error began occurring.
-



APPENDIX **A**

Manage Unsupported Devices

This section contains details on managing unsupported devices in Crosswork Network Controller. It contains the following topics:

- [Manage unsupported devices, on page 181](#)

Manage unsupported devices

You can manage unsupported devices by enabling the necessary configurations on them to facilitate inventory management, fault management, and performance metric collection. While these devices are not officially supported, Cisco Crosswork Network Controller offers limited capabilities to help you manage them effectively.

Table 23: Available options on unsupported devices

Features	Inventory Fault Performance metrics LLDP/ LAG links
MIBs	SNMPv2 ENTITY-MIB IF-MIB LLDP-MIB
Fault	SNMP based alarms Linkup/ Linkdown (IF-MIB) Warm start (SNMPv2-MIB) Cold start (SNMPv2-MIB) Authentication Failure (SNMPv2-MIB) gNMI based alarms gNMI- openconfig-system:/system/messages gNMI- openconfig-system:system/alarms

APIs	Inventory APIs Fault APIs Notification APIs
Performance monitoring metrics	<u>Cisco Devices</u> For Cisco devices the following performance metrics are supported- CPU Utilization CISCO-PROCESS-MIB/cpmCPUTotalTable/ cpmCPUTotalEntry ENTITY-MIB/entPhysicalTable/entPhysicalEntry Memory Pool Utilization CISCO-ENHANCED-MEMPOOL-MIB/cempMemPoolTable/cempMemPoolEntry ENTITY-MIB/entPhysicalTable/entPhysicalEntry Environment Temperature CISCO-ENTITY-SENSOR-MIB/ entSensorValueTable/entSensorValueEntry ENTITY-MIB/entPhysicalTable/entPhysicalEntry Device availability SNMPv2-MIB/system/sysUpTime Interface Statistics IF-MIB/ifTable/ifEntry <u>Non-Cisco Devices</u> For non-Cisco devices the following performance metrics are supported- • Device availability SNMPv2-MIB/system/sysUpTime • Interface Statistics IF-MIB/ifTable/ifEntry • Memory Pool Utilization gNMI-openconfig-platform/components/component • CPU Utilization gNMI- openconfig-platform/components/component/cpu • Environment Temperature gNMI- openconfig-platform/components/component

**Note**

For unsupported devices, the functionality is best-effort. For official support and certified device management functions, contact your Cisco account representative.

