# Add and Configure Devices

This section contains the following topics:



# Device onboarding methods

A device addition is an onboarding mechanism that

- enables registration of network devices into Cisco Crosswork Network Controller,
- offers multiple supported methods tailored for different workflows, and
- requires specific prerequisites for each method to ensure successful onboarding.

Cisco Crosswork Network Controller supports dual-stack deployment. Devices can be onboarded with both IPv4 and IPv6 addresses. To prevent duplicate entries, onboard each device only once using either the IPv4 or IPv6 address.

There are different ways to add devices to Crosswork Network Controller:

1. Importing devices using the Crosswork APIs is the fastest and most efficient method, but it requires programming skills and API knowledge.

   For more information, see the CNC 7.2 API documentation.

2. Importing devices from a Devices CSV file is time-consuming. To use this method, you must first:
   - Create corresponding credential profiles for all of the devices and providers listed in the CSV file.

     For more information, see Manage credential profiles.
   - Create the provider(s) that will be associated with the devices.

     For more information, see Providers.
   - Create tags for use in grouping the new devices.

For more information, see Import multiple tags using a CSV file.

- Download the CSV template file from Crosswork Network Controller and populate it with the devices you plan to add.

For information about adding devices using a CSV file, see CSV device imports, on page 19.

3. Adding devices via the UI is the least error-prone method because all data is validated during entry. However, this approach is time-consuming and is best for adding only a small number of devices at a time. Make sure device and provider credential profiles, as well as tags to be applied to them, are created before onboarding. For more information, see Add devices individually through the UI, on page 13.
4. Auto-onboarding from a Cisco SR-PCE provider is a highly automated and relatively simple method. Create device and provider credential profiles and any required tags before applying them to these devices. The auto-onboarding method does not create or assign device information automatically. Devices are initially discovered and added with partial information. To complete the onboarding process, you must 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 in Provider families.
5. Auto-onboarding using Zero Touch Provisioning is an automated process. First, create device entries and modify your installation's DHCP server. Make sure provider credential profiles and tags are created before use. After onboarding and provisioning, edit each device to supply any information not automatically added.

   For more information, see the *Zero Touch Provisioning*chapter in the *Cisco Crosswork Network Controller 7.2 Device Lifecycle Management Guide*.

**Note** If a device onboarded in Crosswork Network Controller shares a subnet with a Crosswork Data Gateway interface, ensure the device is on the data gateway's southbound network. Reverse Path Forwarding (RPF) checks in Crosswork Data Gateway require source addresses to be on the southbound network. Devices cannot use management or northbound networks if multiple NICs (2 or 3 NIC) are deployed.

# Recommendations for efficient configuration

## Prioritize consistent and secure device configuration

While configuring your devices for onboarding, review these guidelines:

- Use a common configuration file for all devices to enable reachability checks and consistent event collection.
- Plan for link discovery as part of the onboarding workflow. This approach requires necessary configuration work upfront, rather than addressing it incrementally. This is especially important to leverage configuration templates. 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.
- Create unique SNMP EngineIDs for each device in the network.
- If a device's SNMP EngineID is reconfigured, recreate SNMP user accounts for that device.

- Limit NETCONF API access to users with privilege level 15. On XE devices where privilege level 15 is granted via **Enable Password**, do not use NETCONF for reachability or state verification.

### Protect network access and validate device support

- If you are using TELNET in your network environments, implement security measures, such as firewall protections and ACLs to reduce any potential risks.
- If a device is onboarded with an unknown Sys Object ID, contact Cisco Customer Experience as the hardware may not be certified.

# Configuration prerequisites for new devices

A configuration prerequisite is a set of device requirements that

- ensures a new device can be onboarded and managed by Crosswork Network Controller,
- covers key protocols and platforms, and
- prepares a device for streamlined integration into monitoring, telemetry, and orchestration workflows.

Devices need to be properly configured before onboarding to ensure compatibility with Crosswork Network Controller. Configuration details may vary by platform and use case, particularly for protocols such as SNMP, NETCONF, SSH, gNMI, syslog, and TELNET.

For specific protocols like LLDP, CDP, and LAG, see *Set Up and Use Your Topology Map* in the *Cisco Crosswork Network Controller 7.2 Administration Guide*.

**Tip** Planning for link discovery in advance helps complete required configuration upfront and simplifies later management, especially when leveraging configuration templates. You can onboard devices initially with partial configuration, using templates to standardize and complete the configuration later. This approach makes ongoing management and compliance with Crosswork requirements more efficient.

#### Requirements before onboarding devices

- Configure devices for pre-onboarding, on page 3
- Configure devices to forward events to Crosswork Network Controller, on page 4
- Configuration samples for new devices, on page 5

# Configure devices for pre-onboarding

Prepare devices with standard protocol settings and rate limits before onboarding into Crosswork Network Controller.

**Procedure**

**Step 1** Set logging for console and monitoring.

**Step 2** Configure TELNET server limits.

**Step 3** Configure SNMP communities and NTP.

**Step 4** Generate SSH keys and configure session limits.

**Step 5** Set NETCONF and XML agents, if MDT is supported.

The following commands provide a sample pre-onboarding device configuration that sets the correct SNMPv2 and NETCONF configuration, and SSH and TELNET rate limits.

```
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 devices to forward events to Crosswork Network Controller

Enable Crosswork Network Controller to receive SNMP traps and syslogs from managed devices for alarm and event management.

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.

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.

**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.

**Before you begin**

- Confirm the Data Gateway pool virtual IP (*cdg_virtualIP*) addresses.
- In high-availability deployments, gather both primary and secondary Data Gateway addresses.

Configure a device to forward events to the Crosswork Network Controller server using the snmp-server host command:

**Procedure**

**Step 1** Configure the device to send SNMP traps to the Data Gateway virtual IP.

**Example:**

```
snmp-server host 192.168.90.135 traps version 2c public udp-port 1062
```

**Step 2** Set the SNMP community strings.

**Example:**

```
snmp-server community public RO
```

**Step 3** Enable SNMP trap notifications for link status.

**Example:**

```
snmp-server traps snmp linkup
      snmp-server traps snmp linkdown
```

**Step 4** Set the SNMP view group.

**Example:**

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

**Step 5** In geo high-availability scenarios:

a) Add both primary and secondary Data Gateway addresses for redundancy.
b) If using FQDN, ensure the FQDN points to the Data Gateway pool.

# Configuration samples for new devices

Before onboarding devices into Crosswork Network Controller, you must ensure that each device is configured according to the requirements of your platform and protocols.

These sections provide configuration examples for supported protocols and major operating systems. Use these reference samples as starting points and adapt the variable values to match your network environment. Review your platform documentation for version-specific requirements and verify that all configurations meet your organization's security and operational policies.



## Configuration sample for Cisco IOS XR devices

These commands provide a sample pre-onboarding device configuration for IOS-XR devices.

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 all
transport output all
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 v1default write v1default notify v1default
```

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
```

For Cisco ASR 9000 Series devices operating as Large Routers (LRs), configure gNMI using these commands:

```
GNMI Configuration

grpc
 port <port no>
!
```

## Configuration sample for Cisco IOS-XE devices

These commands provide a sample pre-onboarding device configuration for IOS-XE devices.

```
snmp-server host cdg_virtualIP
snmp-server community public-cmty RO
snmp-server community private-cmty 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 all
transport output all
```

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 v1default write v1default notify v1default
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]
```

## Configuration sample for Cisco NSO devices

These commands provide a sample pre-onboarding configuration for a Cisco NSO device used as provider to configure devices managed by Crosswork Network Controller.

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
```

## Configuration sample for Nexus devices

These 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
```

## Configuration sample for gNMI and gRPC

These commands provide a sample pre-onboarding configuration for a device to enable telemetry using gNMI and 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
  !
!
!
```

### gNMI bundling configuration for ASR 9000 series Large Routers

Enabling gNMI bundling is recommended for Cisco ASR 9000 Series devices configured as Large Routers. For inventory collection, gNMI bundling is mandatory to meet requirements. Bundling groups multiple gNMI updates into a single update, which is crucial for inventory collection on high-scale devices.

Sample configuration for gNMI bundling:

```
telemetry model-driven
 gnmi
  bundling
   size 65536
  !
 !
!
```

## Configuration sample for IGP protocol router ID

These commands provide a sample pre-onboarding device configuration for ISIS and OSPF.

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
```

## Configuration sample for MDT sensor group

These commands provide a sample pre-onboarding configuration for a device to stream telemetry data.

```
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
!
!
```

## Configuration sample for SNMPv2 and SNMPv3 traps

These commands provide a sample configuration for a device to send SNMP traps.

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
```

## Configuration sample for SNMPv3 data collection

These commands provide a sample configuration for SNMPv3 data collection. These commands must be added in addition to the SNMPv2 commands referenced in the section, Configuration sample for SNMPv2 and SNMPv3 traps, on page 12.

```
snmp-server group grpauthpriv v3 priv notify v1default
snmp-server user <user-ID> grpauthpriv v3 auth md5 password priv aes 128 password
```

# Add devices individually through the UI

Add devices one by one using the user interface, best suited when adding only a few devices.

**Before you begin**

Gather the required device details, such as name, IP address, and authentication credentials.

Follow these steps to add a device individually through the UI:

**Procedure**

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

**Step 2** Click the add icon.

**Step 3** Enter the values for the new device, as listed in Field descriptions for new device addition, on page 13.

**Step 4** Save your changes.

**Step 5** (Optional) Repeat these steps to add more devices.

# Field descriptions for new device addition

This table lists the fields available when adding a new device through the Crosswork Network Controller user interface, along with each field's description.

**Attention** Starting from version 7.1, the **Device type** field is deprecated in Crosswork Network Controller.

*Table 1: Fields in the Add new device window (*=Required)*

| Field | Description |
|---|---|
| **Device information** | |
| *** Admin state** | The management state of the device. Options are<br>• **UNMANAGED**—Crosswork Network Controller is not monitoring the device.<br>• **DOWN**—The device is being managed and is down.<br>• **UP**—The device is being managed and is up. |
| *** Reachability check** | Determines whether Crosswork Network Controller performs reachability checks on the device. Options are:<br>• **ENABLE** (In CSV: **REACH_CHECK_ENABLE**)—Checks for reachability and then updates the Reachability State in the user interface automatically.<br>• **DISABLE** (In CSV: **REACH_CHECK_DISABLE**)—The device reachability check is disabled.<br>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. |
| **Tags** | The available tags to assign to the device for identification and grouping purposes.<br>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.<br>**Attention**<br>When onboarding Cisco ASR 9000 Large Routers, you must first create the **large-interface-density** tag under the **DeviceClassification** category and subsequently apply this tag to the devices. |
| **Software type** | Software type of the device.<br>**Note**<br>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:<br>• Juniper devices: JUNOS<br>• Huawei devices: VRP<br>• 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. |

| Field | Description |
|---|---|
| **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.<br>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.<br>**Note**<br>For unsupported devices, Crosswork Network Controller reports Manufacturer[sysoid] in the **Product type** column. In cases where unsupported devices do not comply with SNMPv2 MIB, the **Product type** might not show data or may display incorrect data. |
| **Syslog format** | The format in which syslog events received from the device should be parsed by the syslog collector. The options are:<br>• **`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.<br>• **`RFC5424`** - Choose this option to parse syslog events received from the device in RFC5424 format.<br>• **`RFC3164`** - Choose this option to parse syslog events received from the device in RFC3164 format.<br>Refer to Section: Syslog Collection Job Output for more details |
| **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: **`nso23`** or **`srpce123`**.<br>This field is optional if **Administration State** is marked as **`UNMANAGED`**. |
| **Protocol** | The connectivity protocols used by the device. Choices are: **`SNMP`**, **`NETCONF`**, **`TELNET`**,**`HTTP`**, **`HTTPS`**, **`GNMI`**, **`TL1`**, and **`GRPC`**.<br>**Note**<br>Toggle the **Secure Connection** slider to secure the GNMI protocol that you have selected.<br>In this documentation, the secured gNMI protocol is referred to as GNMI_Secure.<br>To add more connectivity protocols for this device, click the add icon at the end of the first row in the **Connectivity Details** panel. To delete a protocol you have entered, click the cross icon shown next to that row in the panel.<br>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. |

| Field | Description |
|---|---|
| *** IP Address / Subnet Mask** | Enter the device's IP address (IPv4 or IPv6) and subnet mask.<br>**Note**<br>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.<br>**Note**<br>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.<br>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.<br>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.<br>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`**.<br>Based on device capability, only one encoding format is supported at a time in a device. |
| **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.<br>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).<br>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.<br>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.<br>On non-Cisco devices, select the encryption that the device supports or use NONE if the device does not use encryption for SNMP. |

| Field | Description |
|---|---|
| **Trap source IP** | This field is available only when the SNMP protocol is selected.<br>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.<br>For consistent trap collection, ensure that the IP address entered in the **Trap source IP** field matches the `trap-source` parameter configured on the network device to avoid any issues with SNMP trap handling.<br>**Note**<br>• If the **Trap source IP** field is not specified, Crosswork Network Controller 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.<br>• 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.<br>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.<br>**Note**<br>• For devices with MDT capability, do not select **YANG_MDT** at this stage.<br>• To enable Crosswork Network Controller to receive the syslog-based data, select **YANG_CLI**. |
| **Providers and access**<br>Provide the provider information. | |
| **Provider family** | Provider type used for topology computation. Choose a provider from the list. |
| **Provider name** | Provider name used for topology computation. Choose a provider from the list.<br>**Note**<br>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** | |

| Field | Description |
|---|---|
| **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.<br>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.<br>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.<br>**Note**<br>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.<br>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.<br>**Note**<br>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).<br>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**<br>Provide location information if you want to see your devices on the geographical map. | |
| **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. |

| Field | Description |
|---|---|
| **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.<br>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. |

# CSV device imports

A CSV device import is a bulk onboarding method that:

- enables users to add multiple devices to the Crosswork Network Controller in a single action,
- allows avoidance of repetitive manual entry, and
- updates existing records when matching inventory key types are found (excluding system-generated UUIDs).

CSV import is most useful in large environments where device addition efficiency and accuracy are critical.

### CSV file behavior

- Import only adds devices not already present in the database.
- Existing device records (excluding system-generated UUIDs) are overwritten if the inventory key type matches a record in the CSV.
- Fields requiring unique values, such as VRF, router loopback, or loopback ID, must be explicitly set.
- Non-required fields can be left blank, set to a default value, or are auto-populated after device communication is established (e.g., model, type, software version).

### Handling non-required fields in the CSV file

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.

# Recommendations for CSV import

To prevent errors when importing CSV files, follow these recommendations:

- Export a backup copy of your existing device list before any CSV import, to prevent accidental data loss.
- Export the current device configuration to generate a CSV template tailored to your environment. Use this exported file as a baseline for further additions.
- Always make necessary edits to exported CSV files. Files exported directly from the UI cannot be re-imported without changes.
- Add a few devices using the Crosswork Network Controller UI and verify they are functioning before importing in bulk.
- Before importing, ensure the Crosswork Data Gateway and UUID columns in the CSV file are empty.
- If importing multiple CSV files, verify that there are no duplicate devices between them.
- 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. Address these errors sequentially as reported during import.
- The device import CSV format differs for cluster deployments versus single VM deployments. Use the correct template for your environment.

## Formatting guidelines

- CSV files from Windows machines must use ‘newline’ characters, not ‘carriage return,’ in order to process correctly.
- To enter multiple values in a field, use semicolons (e.g., SSH;SNMP;NETCONF). Use double semicolons ‘;;’ with no space for blank fields.
- 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

## Template usage

After downloading and editing the CSV template, delete all sample data rows before saving. Retain only the column header row for import.

## Special fields

Populate the TE router ID for each device to ensure unique identification within the topology.

### Device reachability

Devices may initially 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.

## Add devices from a CSV file

Add multiple network devices to Crosswork Network Controller by importing their details from a CSV file.

Use this task when you want to onboard several devices at once, rather than adding them individually.

**Procedure**

**Step 1** Choose **Device Management** > **Network Devices**. The **Network Devices** tab is displayed.

**Step 2** Open the **Import CSV File** dialog box.

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

a) Click the **Download sample 'Device Management template (*.csv)' file** 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.

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.

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

## Export device information to a CSV file

Keep a record of all devices in the system at one time by exporting the device information.

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 .

# Large Routers

A Large Router (LR) is a high-scale ASR 9000 router category that

- supports very large interface counts,
- requires a specialized inventory collection approach for reliable discovery, and
- is identified by Crosswork Network Controller to enable optimized inventory handling.

Some ASR 9000 router deployments operate at significantly higher interface scale than typical devices. At this scale, standard inventory collection approaches are not sufficient. Crosswork Network Controller introduces the LR classification to distinguish these high-scale ASR 9000 routers and apply an inventory strategy suited to large-scale deployments, without affecting inventory behavior for other devices.

## Requirements for LR inventory

This section describes the device-side requirements and inventory behavior that must be met before onboarding a LR in Crosswork Network Controller.

### Criteria for LR inventory support

Large router inventory support applies only to devices that meet all these conditions:

***Table 2: Criteria for LR inventory support***

| Attribute | Value |
|---|---|
| Platform | ASR 9000 (ASR 9K) |
| Minimum number of interfaces | 1000 |
| Software version | Special image- *Contact Cisco Customer Experience* |
| Supported scale | Up to 48K interfaces |
| GNMI encoding | JSON_IETF encoding |

Devices that do not meet these criteria are not supported for LR inventory handling.

### GNMI configuration requirements

Inventory collection for LR uses GNMI.

Ensure these configurations on the ASR 9K device:

- GNMI is enabled on the device
- GNMI access is available using the configured device credentials

- GNMI supports the OpenConfig interfaces model

GNMI-based inventory collection is triggered during device addition and inventory synchronization.

For GNMI configuration sample, see Configuration sample for gNMI and gRPC, on page 11.

### GNMI bundling requirements

GNMI bundling is **recommended** on ASR 9K devices used as LRs to improve inventory performance. Bundling groups multiple GNMI updates into a single update, reducing processing overhead.

For LR devices:

- Inventory relies on bundled GNMI responses to complete collection efficiently.
- If GNMI bundling is not enabled, inventory collection may fail.

### Inventory collection behavior

For devices that meet the LR criteria:

- Inventory uses GNMI with **JSON_IETF** encoding
- CLI- and SNMP-based interface collection is bypassed only for the inventory features that have been replaced by GNMI-based large routers collection.

# Onboard large ASR 9000 routers

Onboard an ASR 9000 Large Router device to enable large-scale inventory collection of interface data through GNMI.

Onboarding the ASR 9000 LR ensures that all interface and sub-interface information from the device is accessible in the inventory system. This is required for comprehensive monitoring and management of large wireless routers within your network, especially when using GNMI for scalable data retrieval.

**Note** GRE tunnel interfaces are not modeled in inventory for LR devices.

**Before you begin**

Ensure that the device meet the requirements mentioned in Requirements for LR inventory, on page 22.

Follow these steps to onboard an LR device:

**Procedure**

**Step 1** Create the LR identification tag (one-time setup).

For information on tag creation, see Create tags.

- **Category**: `DeviceClassification`
- **Tag name**: `large-interface-density`

**Note**
This tag is not created by default and must be manually created.

**Step 2** Create a credential profile that includes GNMI credentials, SNMP credentials, and CLI credentials.

For more information, see Create credential profiles.

**Step 3** Add a new ASR 9K device. For more information, see Add devices individually through the UI, on page 13 and Field descriptions for new device addition, on page 13.

- Set **Admin state** to **Up**.
- Enable **Reachability check** (recommended).
- Select **Tag** as `large-interface-density`.
- Select the credential profile created earlier.

**Note**
If the `large-interface-density` tag is applied to an unsupported device, inventory collection will not complete.

**Step 4** Add the newly added device to a Data Gateway.

For more information, see Attach devices to Data Gateway.

**Note**
Distribute LR devices evenly across available Data Gateways to avoid overloading a single gateway.

**Step 5** Trigger inventory synchronization.

a) On the **Network Devices** window, perform an inventory sync.
   - Select the ASR 9000 devices and click **Actions** > **Detailed sync selected devices**.
   - If you do not select any devices, click **Actions** > **Detailed sync all devices**.

b) Monitor the device status.
   - Status changes to **In progress**
   - On success, status changes to **Completed**

---

- The device reaches **Completed** state.
- All interfaces are visible under the **Interfaces** tab, which can be accessed by navigating to **Topology** > **Device details** or **Topology** > **Device details** > **Detailed inventory**.