Device Configurations

This section provides device configurations that are necessary for device onboarding and the supported deployment modes. For more information on adding devices, see the "Manage Inventory" chapter in the Cisco Crosswork Change Automation and Health Insights User Guide.

Prerequisites for Onboarding Devices

Before adding devices, you must ensure that the devices themselves are configured to collect and transmit telemetry data properly and communicate successfully with Cisco Crosswork Change Automation and Health Insights. The following sections provide sample configurations for a variety of communications options. Use them as a guide to configuring the devices you plan to manage using Cisco Crosswork Change Automation and Health Insights.

Note Only users configured with privilege level 15 can use the NETCONF APIs. Privilege level 15 can be used to configure the "enable" password option in XE devices. In such cases, NETCONF should not be included as one of the protocols to verify reachability and operational state for the onboarded devices.

Note Only SNMPv2 and SNMPv3 (NoAuth/NoPriv) traps are supported.

Pre-Onboarding SNMP v2 Device Configuration

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 (XR 6.5.3/6.6.3 or higher).

```
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
line default
 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>
!
service cli history size 5000
service cli interactive disable
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
grpc
 port 57400
!
netconf agent tty
!
netconf-yang agent
 ssh
!
```

Pre-Onboarding SNMPv3 Device Configuration

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

Pre-Onboarding SNMPv2 and SNMPv3 Trap Configuration

If you want the device to send SNMP traps to Cisco Crosswork Change Automation and Health Insights, use the following commands to perform a pre-onboarding device configuration and test for the trap version you want.

For SNMP v2 traps:

```
snmp-server trap link ietf

snmp-server host <CrossworkDataGatewaysouthboundIPAddress> traps version 2c cisco123 udp-port
 1062

snmp-server community cisco123

snmp-server traps snmp linkup

snmp-server traps snmp linkdown
```

For SNMP v3 traps:

```
snmp-server trap link ietf

snmp-server host < CrossworkDataGatewaysouthboundIPAddress> traps version 3 cisco123 udp-port
 1062

snmp-server community cisco123

snmp-server traps snmp linkup
```

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

Please note that, for traps to be received, the node_ip field for the device as listed in the Cisco Crosswork Change Automation and Health Insights inventory must match the IP address of the device interface from which the traps are sent. If they do not, Cisco Crosswork Change Automation and Health Insights will reject the traps. Also, the device needs to be in ADMIN_UP state for traps to be received.

Supported TCP/IP Stack

Cisco Crosswork Change Automation and Health Insights version 3.2 supports only single stack deployments (IPv4 or IPv6).

Table 1: Single stack deployment modes

Stack/Deployment mode	IPv4 only	IPv6 only
Cisco Crosswork Change Automation and Health Insights interfaces (two interfaces)	• IPv4 (mandatory) • IPv6 (optional)	• IPv4 (optional) • IPv6 (mandatory)
Cisco Crosswork Data Gateway	• IPv4 (mandatory) • IPv6 (optional)	• IPv4 (optional) • IPv6 (mandatory)
Providers	• IPv4 (mandatory) • IPv6 (optional)	• IPv4 (optional) • IPv6 (mandatory)
External Destinations	• IPv4 (mandatory) • IPv6 (optional)	• IPv4 (optional) • IPv6 (mandatory)
Devices	• IPv4 (mandatory) Device can be onboarded to Device Management only with IPv4 address.	• IPv6 (mandatory) Device can be onboarded to Device Management only with IPv6 address.
Restrictions	• Provider/Destination configuration and CDG Enrollment is prevented if interface connectivity information does not include an IPv4 address. • Device onboarding is prevented if IPv6 address is included.	• Provider/Destination configuration and CDG Enrollment is prevented if interface connectivity information does not include an IPv6 address. • Device onboarding is prevented if IPv4 address is included.