Cisco Crosswork Change Automation and Health Insights 4.4 User Guide

First Published: 2022-06-23

Last Modified: 2022-08-16

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

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

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

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

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

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

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

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

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

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

CONTENTS

CHAPTER 4

CHAPTER 5

CHAPTER 1

Overview

This section contains the following topics:

Audience

This guide is for experienced network administrators who want to use Cisco Crosswork Change Automation and Health Insights in their network. This guide assumes that you are familiar with the following topics:

- Networking technologies and protocols (IS-IS, BGP, and so on)
- Network monitoring and troubleshooting
- Familiarity with the Cisco Crosswork Infrastructure 4.3 and how the applications are installed. For more information, see *Cisco Crosswork Infrastructure 4.3 and Applications Installation Guide*.

Overview of Cisco Crosswork Change Automation and Health Insights

Cisco Crosswork Change Automation and Health Insights is part of the Cisco Crosswork Network Controller.

The application provides a ready-to-use solution supporting the following use cases:

- Monitor Key Performance Indicators (KPIs) and notify of any anomalies.
- Prepare network changes triggered by changes in KPIs and roll out these changes.
- Automate change and remediation.

Cisco Crosswork Change Automation

Cisco Crosswork Change Automation helps to codify workflows using parameterized Plays and stitches them into Playbooks for execution.

Cisco Crosswork Health Insights

Cisco Crosswork Health Insights offers real-time, telemetry-based Key Performance Indicator (KPI) monitoring and intelligent alerting. The alerts are based on predefined templates or user-defined logic. These alerts can be tied to the Playbooks to implement closed-loop automation workflows.

Health Insights configures KPIs based on telemetry using MDT, SNMP, or GNMI. The collected data is evaluated in one of the following four possible ways (using UI based tools):

- No alert
- Standard deviation
- Two-level threshold
- Rate change

Other configurations are also possible. For more details, see Cisco Crosswork Network Automation APIs.

This guide explains how to use Cisco Crosswork Change Automation and Health Insights.

For more information about Cisco Crosswork Network Controller, see the Cisco Crosswork Network Controller Product page on Cisco.com.

Cisco Crosswork API

All the Cisco Crosswork Network Controller applications provides a robust set of APIs that allow it to be integrated with other tools you use to manage and configure your network. For more details on the product APIs, see the Cisco Crosswork Network Controller API Documentation on Cisco DevNet.

Integration with other Cisco and non-Cisco products

Crosswork Change Automation and Health Insights is integrated as part of Cisco Crosswork Network Controller. For more details on Crosswork Network Controller, see Cisco Crosswork Network Controller Data Sheet.

Below are the other Cisco and non-Cisco products with which Crosswork Change Automation and Health Insights can be integrated:

- **Cisco WAN Automation Engine (Cisco WAE)**: Provides traffic and topology analysis to Crosswork Change Automation and Health Insights. The foundation software is Cisco WAE Planning, which provides a cross-sectional view of traffic, topology, and equipment state. For more information, see Cisco WAN Automation Engine (WAE).
- **Cisco Network Services Orchestrator**: Crosswork Change Automation and Health Insights uses Cisco Network Services Orchestrator as the default provider to configure the devices according to their expected functions, including configuring any required model-driven telemetry (MDT) sensor paths for data collection. Cisco Network Services Orchestrator is vital in supplying device management and configuration-maintenance services. For more information, see Cisco Network Services Orchestrator (NSO).
- **Cisco Crosswork Active Topology**: Crosswork Active Topology enables visualization of topology and services on logical and geographical maps.
- **Cisco Crosswork Optimization Engine**: Crosswork Optimization Engine provides real-time network optimization. Some Plays enable integration with Crosswork Optimization Engine so that the optimization

decision is based on the KPIs being tracked in Crosswork Health Insights. For more information, see Cisco Crosswork Optimization Engine Data Sheet.

- **Cisco Crosswork Zero Touch Provisioning**: Crosswork Zero Touch Provisioning is an optional package that can be installed on the Cisco Crosswork Infrastructure 4.3 to allow the users to bring up the devices quickly and easily using a Cisco-certified software image and a day-zero software configuration of the customer's choice. Once provisioned in this way, the new device is onboarded to the Crosswork device inventory. For more information, see Cisco Crosswork Zero - Touch Provisioning Data Sheet.

Licensing

Crosswork Change Automation and Health Insights 4.3 is now available as an add-on license in the purchase of Cisco Crosswork Network Controller 3.0 and is no longer separately orderable.

One Right-To-Manage (RTM) license is required for each managed physical device.

Also, licenses are required to use Crosswork Change Automation and Crosswork Health Insights. The licenses come in packs - KPI pack and Playgroup pack:

- KPI license packs cover all the KPIs you intend to deploy. One KPI pack includes a set of five KPIs.
- Playbook license packs cover all of the built-in and custom plays you plan to run. One Playgroup pack includes a set of five plays which can be combined in multiple Playbooks. The system only counts unique plays even if they are included in one or more Playbooks.

Crosswork Change Automation increments the license count for each play that is run (whether successful or not) including dry run. Creating new play without running it does not use license. Crosswork Health Insights licenses are based on the number of KPIs enabled through a KPI Profile and the license count increments for each enabled KPI.

If additional KPI packs or Playgroup packs are required, contact your Cisco account representative (sales) or the partner from whom the product was purchased.

Note For demonstrations and field trials, Crosswork Change Automation or Crosswork Health Insights can be used without license for up to 90 days. After 90 days of evaluation period, the product will be out of compliance. All the existing tasks will still continue as is but enabling new Plays or KPIs is not allowed. To find out the total and used number of licenses, check the Smart Licensing site. For more information, see Smart Software Manager Guide.

For more information about licensing, see the Cisco Crosswork Network Automation Product Data Sheet at Cisco.com.

CHAPTER 2

Get Started

This section contains the key workflows and an overview of Cisco Crosswork Change Automation and Health Insights dashboard:

Getting Started

Workflow	For details, see...
1. Install Cisco Crosswork Change Automation and Health Insights environment and set up Cisco Crosswork Data Gateway.	See *Cisco Crosswork Infrastructure 4.3 and Applications Administration Guide*
2. Do the basic reachability checks.	See Section: *Setup Workflow* in the *Cisco Crosswork Infrastructure 4.3 and Applications Administration Guide*
3. Configure the Change Automation settings.	Configure Change Automation Settings, on page 26
4. (Optional) Setup and configure your map settings.	Workflow 1: Configure Network View, on page 6
5. Create KPI Profiles to monitor device Key Performance Indicators (KPIs) for issues and anomalies.	Workflow 2: Monitor Key Performance Indicators, on page 6
6. (Optional) Link KPIs to playbooks.	Workflow 3: Closed-Loop Automation, on page 7
7. (Optional) Schedule Playbooks to perform routine maintenance.	Workflow 4: Schedule Playbooks, on page 8

Workflow	For details, see...
8. (Optional) Expand telemetry insight with custom KPIs.	Workflow 5: Develop Custom KPIs, on page 9
9. (Optional) Remediate common scenarios and automate routine tasks with custom playbooks.	Workflow 6: Develop Custom Playbooks, on page 10

Workflow 1: Configure Network View

The following workflow describes the steps to configure the map display settings in Cisco Crosswork Change Automation and Health Insights:

Step	Action
1. Group your devices logically as per your requirement.	Follow the instructions in Create and Modify Device Groups, on page 21 and Enable Dynamic Device Grouping, on page 22.
2. Set display preferences for your topology.	Follow the instructions in Customize Map Display Settings, on page 23.
3. Manage your custom topology views.	Follow the instructions in Save Topology Views for Easy Access, on page 23.

Workflow 2: Monitor Key Performance Indicators

Once you have completed initial setup, use Cisco Crosswork Health Insights to begin device performance monitoring using KPI Profiles.

Step	Action
1. (Optional) Tag all of the devices whose KPIs you plan to monitor with a tag indicating the function they perform, per your plan.	See *Cisco Crosswork Change Automation and Health Insights 4.3 Administration Guide* for the procedure.

Step	Action
2. Plan which Cisco-supplied KPIs you want to begin using, based on each device's function and the device performance characteristics you want to monitor. **Note** Health Insight can be used without a license for up to 90 days. After 90 days of evaluation period, the product will be out of compliance. All the existing tasks will still continue as is but enabling new KPIs is not allowed. Also, check the total number of KPIs and make sure that you have enough licenses. To check, visit the Smart Licensing site. For more information, see Smart Software Manager Guide.	Review the Cisco-supplied KPIs documented in List of Health Insights KPIs, on page 69. To create a new KPI that fits your requirement, see Create a New KPI, on page 65.
3. Based on your experience or by using the recommendation engine, group the KPIs to form KPI Profiles.	Follow the instructions in Create a New KPI Profile, on page 76.
4. Enable the appropriate KPI Profiles on the devices you want to monitor.	Review and follow the instructions in Monitor Network Health and KPIs, on page 57

Workflow 3: Closed-Loop Automation

The following workflow describes the steps to follow when using Cisco Crosswork Health Insights to alert the operator of the need to run a remediation Playbook from Cisco Crosswork Change Automation in response to the performance challenges detected in the network. A remediation Playbook can be linked to a KPI to make the remediation easier.

Step	Action
1. Research the KPIs that are triggering alerts, and determine the best corrective action to take for the situation your network has experienced.	Follow the instructions in Monitor Network Health and KPIs, on page 57, using the View Alerts for Network Devices, on page 61 to research the alerts and their possible causes.
2. Review the plays and Playbooks to determine which will best address the alerting KPI. For example: • Look for an existing Playbook that could resolve the issue. • Look for existing plays that could be combined to resolve the issue. Create a new Playbook with those plays.	Review the list of Plays, Playbooks, and generic parameters in the "Playbooks" and "Plays" references in the Change Automation Developer Guide on Cisco Devnet. See Create a Custom Playbook Through the UI, on page 37

Step	Action
3. Try out the selected Playbooks and see if they are applicable to your purposes. As you experiment, adjust the Playbook parameters as needed. **Note** Crosswork Change Automation increments the license count for each Playbook that is run (whether successful or not) including dry run. If a Playbook is run once, it can be used multiple times without increasing the license count.	See: Perform a Dry Run of a Playbook, on page 44 Run Playbooks In Single Stepping Mode, on page 46 Run Playbooks In Continuous Mode, on page 49
4. If required, build a new Playbook with new or existing plays, as necessary, to meet your requirements.	See Create a Custom Play using Templates, on page 31 See Create a Custom Playbook Through the UI, on page 37
5. (Optional) For frequently triggered KPIs with a known remediation Playbook, link the Playbook to the KPI to make executing the Playbook easier.	Follow the steps in Link KPIs to Playbooks, on page 67. Use the Remediation icon shown in View Alerts for Network Devices, on page 61 to trigger a run of a linked Playbook from a device or KPI alert.

Workflow 4: Schedule Playbooks

The workflow below describes the steps to follow when using Cisco Crosswork Change Automation to automate routine network upkeep, and to verify that each routine change completed correctly.

Note This workflow is applicable only if scheduling is enabled in the Change Automation settings. For more information, see Configure Change Automation Settings, on page 26.

Step	Action
1. Identify routine maintenance tasks (such as throughput checks, software upgrades, SMU installs, and so on) that you perform on a regular schedule and that may be suitable for automation using one or more Cisco Crosswork Change Automation Playbooks.	See About Running Playbooks, on page 43 and View the Playbook List, on page 30
2. Configure Playbooks to perform these tasks at the desired time.	See About Running Playbooks, on page 43 and Schedule Playbook Runs, on page 52
3. Review the Change Automation Job History to review the current status of the Playbook. If the job fails, the details will be available.	See Use the Change Automation Dashboard, on page 27 and View or Abort Playbook Jobs, on page 53

Workflow 5: Develop Custom KPIs

The following workflow describes the steps to follow when considering whether or not to develop Cisco Crosswork Health Insights custom KPIs for your special needs, and how to proceed if you decide you do.

Step	Action
1. Review the existing KPIs to make sure the telemetry (SNMP, CLI, Cisco IOS XR, or IOS-XE) you want to monitor is not already available.	Follow the instructions in Monitor Network Health and KPIs, on page 57, using the View Alerts for Network Devices, on page 61 to research the alerts and their possible causes.
2. Review the data available from the devices you want to monitor to see if they can supply the needed information: - If they can, proceed with building a custom KPI. - If they cannot, Contact Cisco. The latest information on the data your devices can provide is always available at the Cisco Telemetry Data Mapper (https://tdm.cisco.com).	Review the KPIs in List of Health Insights KPIs, on page 69.
3. Build the custom KPI and add it to a KPI Profile.	See Create a New KPI, on page 65 and Create a New KPI Profile, on page 76
4. Enable the new KPI Profile on a test device and confirm that the data reported matches your expectations. Be aware that KPIs that depend on data over time to establish baseline performance will need some time to "anneal" before they provide meaningful data.	See Enable KPI Profile on Devices, on page 79 and View Alerts for Network Devices, on page 61
5. Make sure it gets activated properly on the device (MDT only) and Crosswork Data Gateway.	See Verify the Deployment Status of Enabled KPIs, on page 69
6. If the KPI Profile is meeting expectations, enable it on all devices where you consider it applicable. **Warning** When you are enabling KPI profiles on large number of devices, ensure that sufficient capacity is available on Cisco Crosswork Data Gateway. If sufficient capacity is not available and if you enable the KPI profiles on large number of devices, it may cause overload and outage. To check Cisco Crosswork Data Gateway load, see *Health Insights CDG load calculator* at Cisco Crosswork Network Automation APIs.	Follow the steps in Enable KPI Profile on Devices, on page 79.
7. Make sure it got deployed on the device (MDT only) and Crosswork Data Gateway (all).	See Verify the Deployment Status of Enabled KPIs, on page 69

Workflow 6: Develop Custom Playbooks

The following workflow describes the steps to follow when deciding to develop a Change Automation custom Playbook.

Step	Action
1. Review the existing plays and Playbooks to see if any of them meet your needs fully or partially.	From the main menu, go to **Network Automation** > **Play List or Playbook List**.
2. If required, build a new Playbook with new or existing plays, as necessary, to meet your requirements.	See Create a Custom Play using Templates, on page 31 See Create a Custom Playbook Through the UI, on page 37
3. For a Playbook you have developed that meets your needs: • In response to KPI alerts: If the Playbook is meeting expectations, link it to the KPI that indicates the need for the Playbook to be run, so that it is easy for operators to trigger the Playbook. • For planned maintenance or configuration changes: Schedule the Playbook to run, or run it at the planned time.	See: Link KPIs to Playbooks, on page 67 Schedule Playbook Runs, on page 52

CHAPTER 3

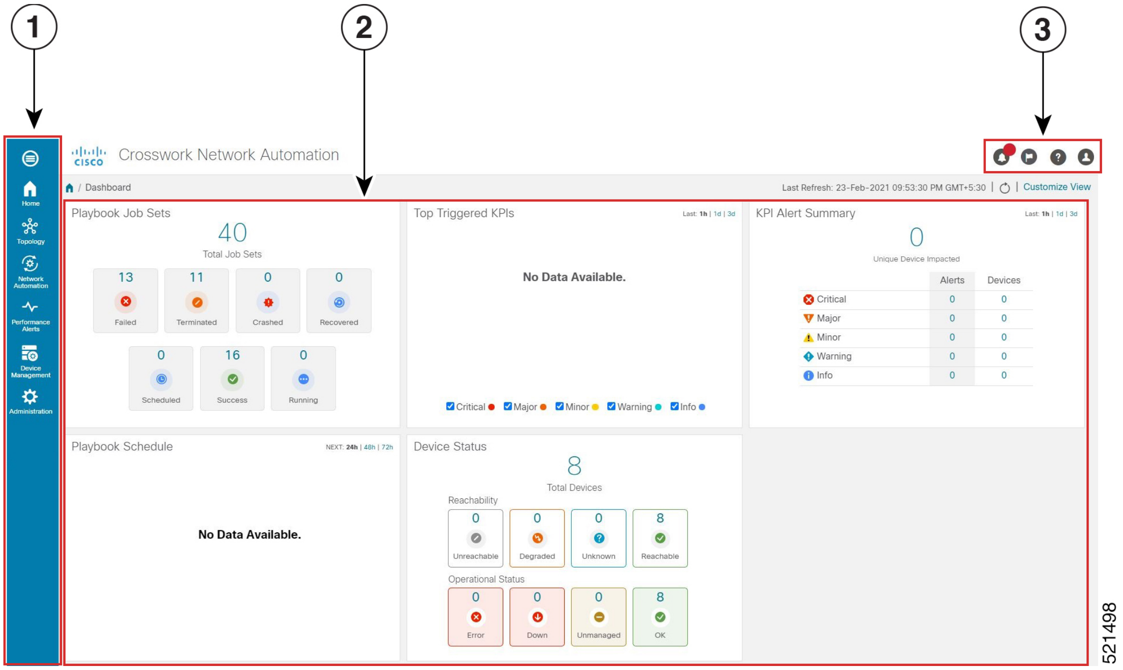
Set Up and Monitor Your Network View

Familiarize yourself with the UI and set up your network view. This section contains the following topics:

Get a Quick View in the Dashboard

The Home page displays a customizable collection of dashlets which provide an at-a-glance operational summary of the network being managed, including reachability and operational status of devices. The Dashboard is made of a series of dashlets, and each dashlet represents different types of data belonging to the same category.

Figure 1: Crosswork Home page



	Alerts	Devices
Critical	0	0
Major	0	0
Minor	0	0
Warning	0	0
Info	0	0

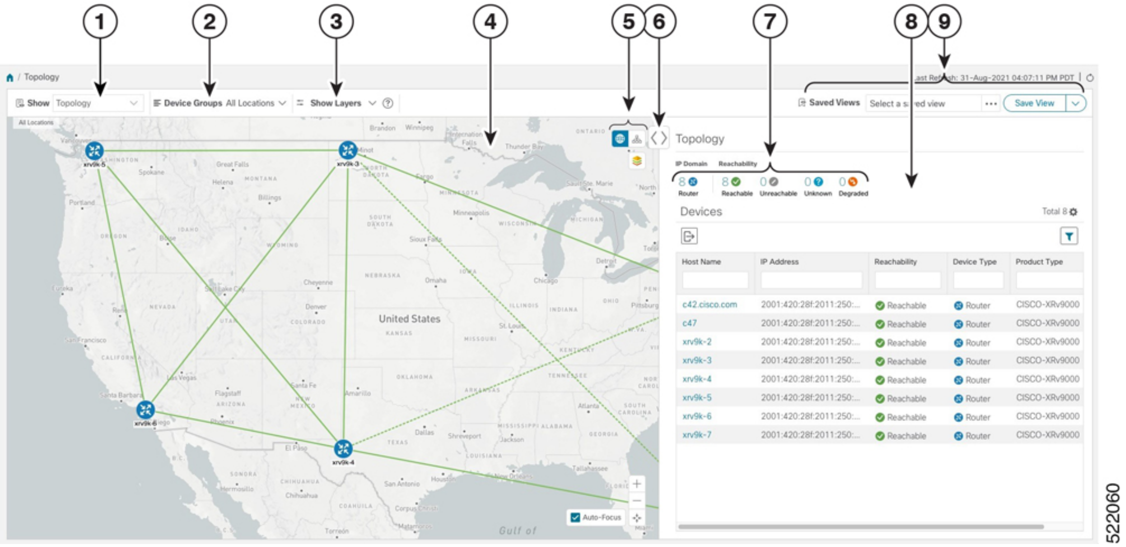
Callout No.	Description
1	**Main Menu**: The main menu allows you to navigate to installed Cisco Crosswork applications and device management and administrative tasks. Menu options may look slightly different depending on what Cisco Crosswork applications are installed.
2	**Dashlets**: Information varies depending on what Cisco Crosswork applications are installed. • To drill down for more information within a dashlet, click on a value. A window appears displaying only the filtered data you clicked on. • To add or change the layout of dashlets, click **Customize View**. Move the dashlets to your desired layout and click **Save**.
3	Settings icons: The **Alerts** icon notifies you of any current error conditions related to the system operations which require attention, and provides a link to detailed information about those conditions. The **Events** icon notifies you of new events related to system operation, and also provides access to the history of all system events. The **About** icon displays the current version of the Cisco Crosswork product. The **User Account** icon lets you view your username, change your password, and log out.

View Devices and Links on the Topology Map

To view the network topology map, from the main menu choose **Topology**.

For more information, see View Device and Link Details, on page 15.

Figure 2: Cisco Crosswork UI and Topology Map



Host Name	IP Address	Reachability	Device Type	Product Type
c42.cisco.com	2001:420:28f:2011:250:...	Reachable	Router	CISCO-XRv9000
c47	2001:420:28f:2011:250:...	Reachable	Router	CISCO-XRv9000
xrv9k-2	2001:420:28f:2011:250:...	Reachable	Router	CISCO-XRv9000
xrv9k-3	2001:420:28f:2011:250:...	Reachable	Router	CISCO-XRv9000
xrv9k-4	2001:420:28f:2011:250:...	Reachable	Router	CISCO-XRv9000
xrv9k-5	2001:420:28f:2011:250:...	Reachable	Router	CISCO-XRv9000
xrv9k-6	2001:420:28f:2011:250:...	Reachable	Router	CISCO-XRv9000
xrv9k-7	2001:420:28f:2011:250:...	Reachable	Router	CISCO-XRv9000

Callout No.	Description
1	**Topology Map View**: From the **Show** drop-down list, click the option that displays the data that you would like to see on the map. If **Topology** is selected, devices and links in the network are displayed.
2	**Device Groups**: From the drop-down list, click the group of devices you want displayed on the map. All other device groups will be hidden.
3	**Show Hide**: From the drop-down list, click the network layers you want displayed on the map. All devices and links that belong to the selected layers are then displayed. By default, all layers are displayed.

Callout No.	Description
4	**Topology Map**: The network topology can be displayed on a logical map or a geographical map, where the devices and links are shown in their geographic context. From the map, you can drill down to get detailed information about devices and links. **Devices:** • To view a device configuration summary, hover the mouse cursor over the device icon. A pop up window displaying the host name, state, node ID, and device type appears. • To view device details, click on the device icon. • If devices are in close physical proximity, the geographical map shows them as a cluster. The number in a blue circle (4) indicates the number of devices in the cluster. Displaying devices in this manner helps prevent overlap and clutter on the map. **Links:** • A solid line indicates a *single link* between two devices. If there is more than one link between two devices, or between a device and a cluster of devices, the line is shown dashed instead. A dashed line indicates an *aggregated* link that represents more than one link, or the use of multiple protocols (for example, IPv4 and IPv6) on the same physical link. • A and Z indicates headend and endpoint, respectively. • To view link information details, click on the link. **Note** Although aggregated, dual stack links show as one single line.
5	🖧: The logical map shows devices and their links, positioned according to an automatic layout algorithm, ignoring their geographical location. You can change the layout algorithm. 🌐: The geographical map shows single devices, device clusters, links, and tunnels, superimposed on a map of the world. Each device location on the map reflects the device's GPS coordinates (longitude and latitude) as defined in the device inventory. ≋: The Display Preferences window allows you to change display settings for devices, links, and utilization..
6	**Expand/Collapse/Hide Side Panel**: Expand or collapse the contents of the side panel. Close the side panel to get a larger view of the topology map.

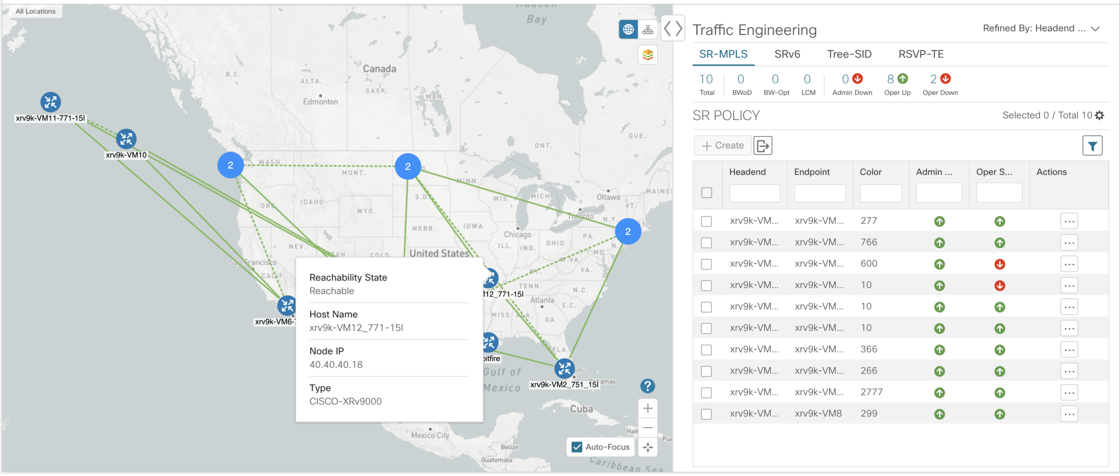
Callout No.	Description
7	The **Mini Dashboard** provides a summary of the IP Domain and device reachability status. If filters are applied, the **Mini Dashboard** is updated to reflect what is displayed in the Devices table. **Note** If the Alarm Status feature is enabled, you will also see Alarm information here. To view the Alarm Status, you must install the Common EMS Services application and configure host information for Syslog and SNMP traps on the devices you want to view alarms for. For more information, see the *Cisco Crosswork Infrastructure and Applications Installation Guide* and the *Cisco Crosswork Infrastructure and Applications Administration Guide*. The Alarm Status feature is available for select licensing packages.
8	The content of this window changes depending on what **Show** is set to for the Topology Map and if you have selected to view more information on a device or link.
9	**Saved Custom Map Views**: Lets you create a named custom view using the settings and layout for your current map, settings of the tables saved in the saved views, or display a custom view you have created previously.

View Device and Link Details

This example shows how you can view device and link details using the topology map.

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

Step 2 To quickly view the host name, reachability state, IP address and type of device, hover the mouse over the device icon.



Reachability State
Reachable

Host Name
xrv9k-VM12_771-15I

Node IP
40.40.40.18

Type
CISCO-XRv9000

Traffic Engineering

Refined By: Headend ...

SR-MPLS SRv6 Tree-SID RSVP-TE

10 Total | 0 BWoD | 0 BW-Opt | 0 LCM | 0 Admin Down | 8 Oper Up | 2 Oper Down

SR POLICY

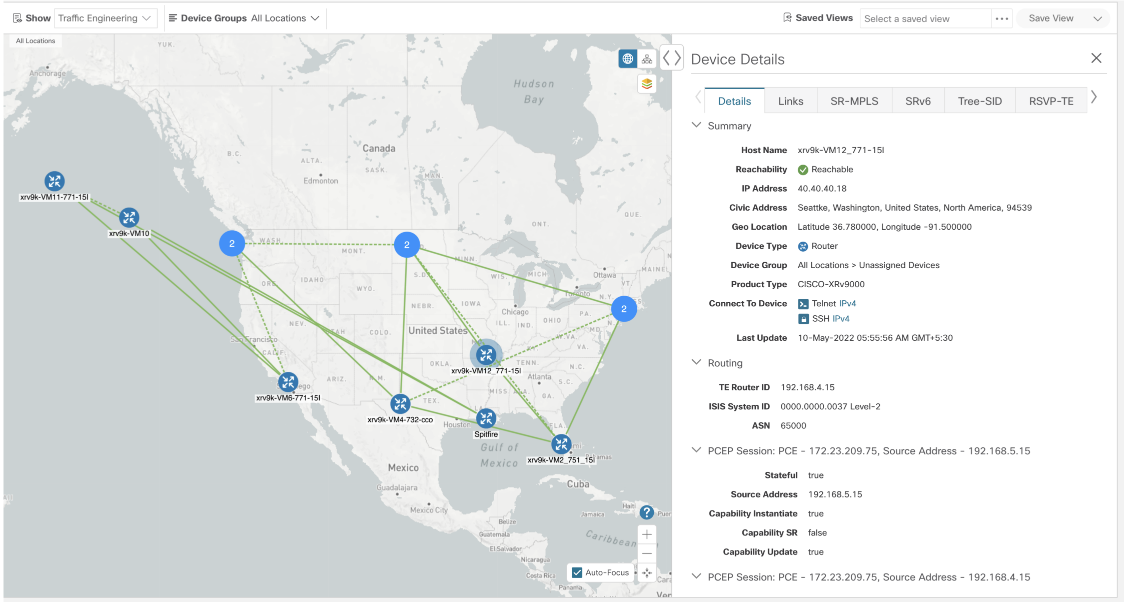
Selected 0 / Total 10

+ Create

□	Headend	Endpoint	Color	Admin ...	Oper S...	Actions
□	xrv9k-VM...	xrv9k-VM...	277	↑	↑	...
□	xrv9k-VM...	xrv9k-VM...	766	↑	↑	...
□	xrv9k-VM...	xrv9k-VM...	600	↑	↓	...
□	xrv9k-VM...	xrv9k-VM...	10	↑	↓	...
□	xrv9k-VM...	xrv9k-VM...	10	↑	↑	...
□	xrv9k-VM...	xrv9k-VM...	10	↑	↑	...
□	xrv9k-VM...	xrv9k-VM...	366	↑	↑	...
□	xrv9k-VM...	xrv9k-VM...	266	↑	↑	...
□	xrv9k-VM...	xrv9k-VM...	2777	↑	↑	...
□	xrv9k-VM...	xrv9k-VM8	299	↑	↑	...

Step 3 To view more device details, click on the device icon.

a) The following examples show the Device details from the Topology map.



Device Details

Details | Links | SR-MPLS | SRv6 | Tree-SID | RSVP-TE

Summary

Host Name	xrv9k-VM12_771-15I
Reachability	✓ Reachable
IP Address	40.40.40.18
Civic Address	Seattke, Washington, United States, North America, 94539
Geo Location	Latitude 36.780000, Longitude -91.500000
Device Type	Router
Device Group	All Locations > Unassigned Devices
Product Type	CISCO-XRv9000
Connect To Device	Telnet IPv4 SSH IPv4
Last Update	10-May-2022 05:55:56 AM GMT+5:30

Routing

TE Router ID	192.168.4.15
ISIS System ID	0000.0000.0037 Level-2
ASN	65000

PCEP Session: PCE - 172.23.209.75, Source Address - 192.168.5.15

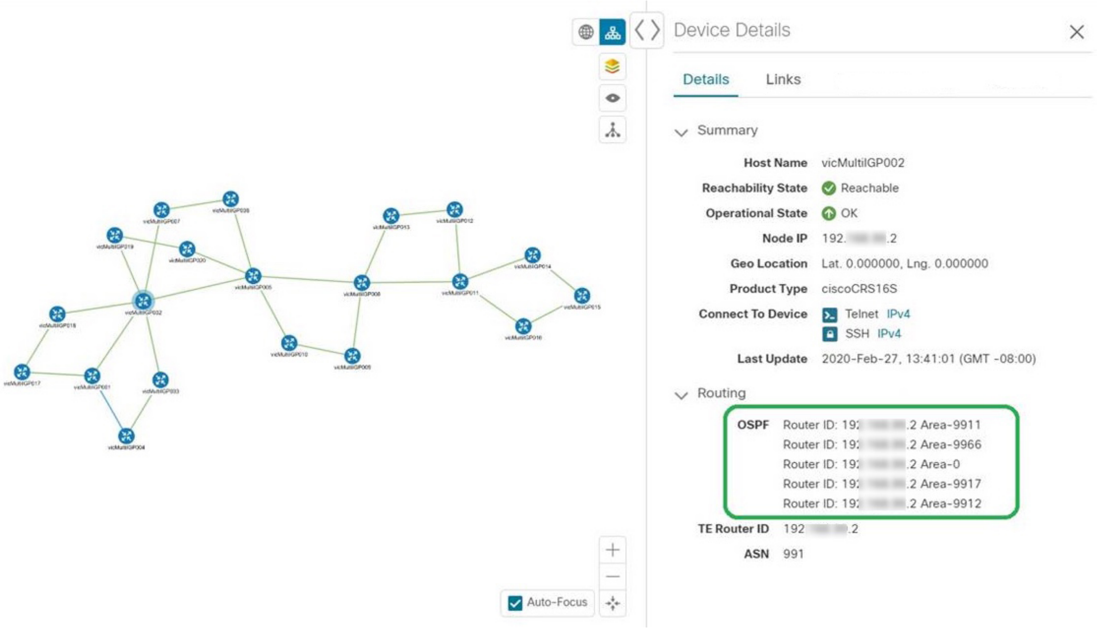
Stateful	true
Source Address	192.168.5.15
Capability Instantiate	true
Capability SR	false
Capability Update	true

PCEP Session: PCE - 172.23.209.75, Source Address - 192.168.4.15

Note If the Alarm Status feature is enabled, you will also see Alarm information here. To view the Alarm Status, you must install the Common EMS Services application and configure host information for Syslog and SNMP traps on the devices you want to view alarms for. For more information, see the *Cisco Crosswork Infrastructure and Applications Installation Guide* and the *Cisco Crosswork Infrastructure and Applications Administration Guide*. The Alarm Status feature is available for select licensing packages.

In a multiple IGP setup, you can also view all the IGP, IS-IS, and OSPF processes in the Routing details. See the following examples:

Figure 3: Multiple IGP: OSPF Processes



Device Details

Details | Links

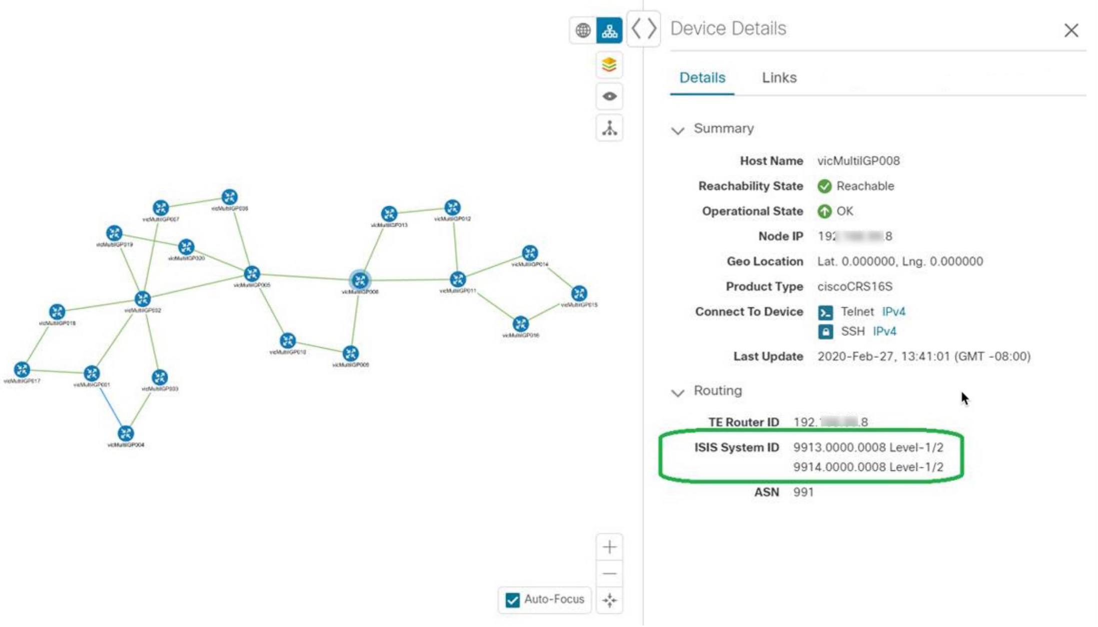
Summary

Host Name	vicMultiIGP002
Reachability State	✓ Reachable
Operational State	OK
Node IP	192.[redacted].2
Geo Location	Lat. 0.000000, Lng. 0.000000
Product Type	ciscoCRS16S
Connect To Device	Telnet IPv4 SSH IPv4
Last Update	2020-Feb-27, 13:41:01 (GMT -08:00)

Routing

OSPF	Router ID: 19[redacted].2 Area-9911 Router ID: 19[redacted].2 Area-9966 Router ID: 19[redacted].2 Area-0 Router ID: 19[redacted].2 Area-9917 Router ID: 19[redacted].2 Area-9912
TE Router ID	192[redacted].2
ASN	991

Figure 4: Multiple IGP: ISIS Processes



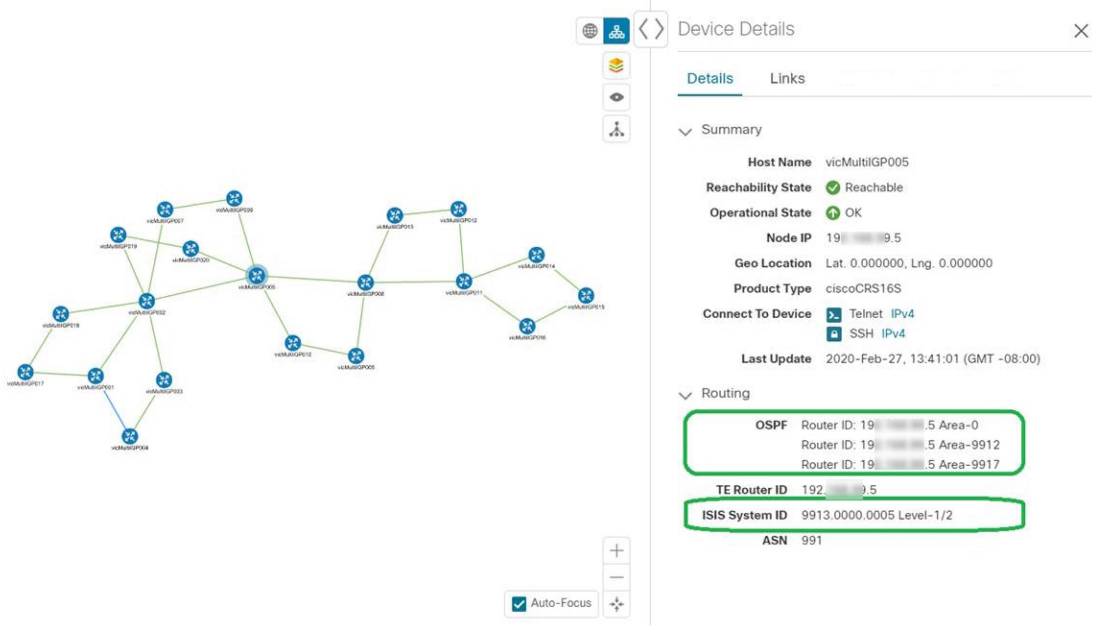
Summary

Host Name	vicMultiIGP008
Reachability State	✓ Reachable
Operational State	OK
Node IP	192[redacted].8
Geo Location	Lat. 0.000000, Lng. 0.000000
Product Type	ciscoCRS16S
Connect To Device	Telnet IPv4 SSH IPv4
Last Update	2020-Feb-27, 13:41:01 (GMT -08:00)

Routing

TE Router ID	192.[redacted].8
ISIS System ID	9913.0000.0008 Level-1/2 9914.0000.0008 Level-1/2
ASN	991

Figure 5: Multiple IGP: OSPF and ISIS Processes



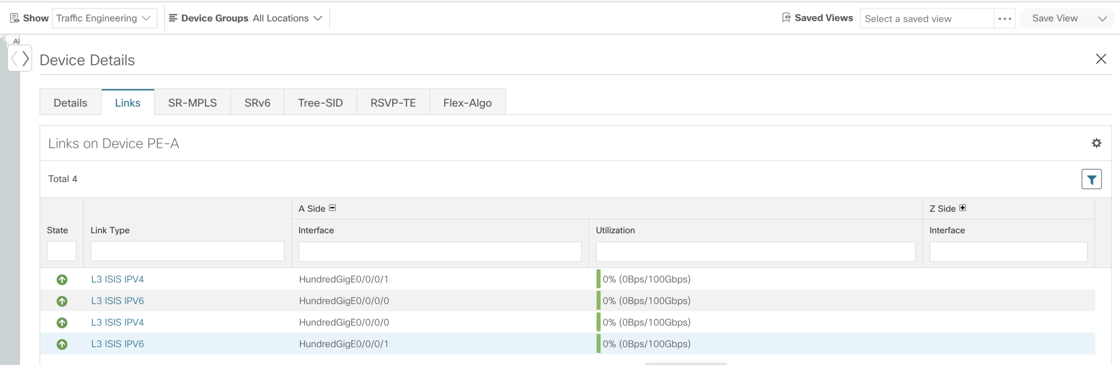
Summary

Host Name	vicMultiIGP005
Reachability State	✓ Reachable
Operational State	OK
Node IP	19[redacted]9.5
Geo Location	Lat. 0.000000, Lng. 0.000000
Product Type	ciscoCRS16S
Connect To Device	Telnet IPv4 SSH IPv4
Last Update	2020-Feb-27, 13:41:01 (GMT -08:00)

Routing

OSPF	Router ID: 19[redacted].5 Area-0 Router ID: 19[redacted].5 Area-9912 Router ID: 19[redacted].5 Area-9917
TE Router ID	192.[redacted].5
ISIS System ID	9913.0000.0005 Level-1/2
ASN	991

Step 4 To view links on the device, click the **Links** tab and expand the right panel to see all the link details.



Links on Device PE-A

Total 4

		A Side ⊟		Z Side ⊞
State	Link Type	Interface	Utilization	Interface
⬆	L3 ISIS IPV4	HundredGigE0/0/0/1	0% (0Bps/100Gbps)	
⬆	L3 ISIS IPV6	HundredGigE0/0/0/0	0% (0Bps/100Gbps)	
⬆	L3 ISIS IPV4	HundredGigE0/0/0/0	0% (0Bps/100Gbps)	
⬆	L3 ISIS IPV6	HundredGigE0/0/0/1	0% (0Bps/100Gbps)	

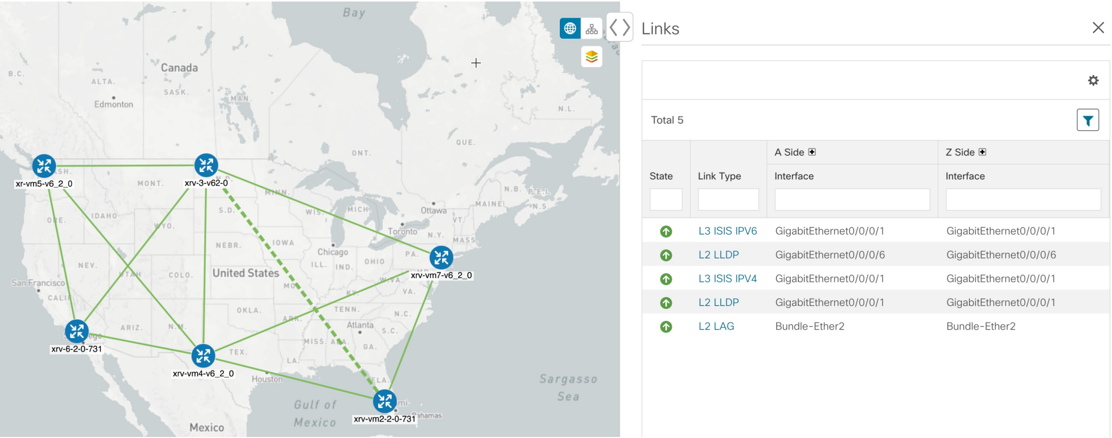
Step 5 To view the utilization, expand **A side**or **Z side**.

The utilization shown on ipv4 and ipv6 links represents the aggregate traffic on the interface or sub-interface, not specific to each address family.The utilization shown on sub-interface links represents the bandwidth utilization on the main interface of the sub-interface’s traffic.

Step 6 Collapse the side panel and close the **Device Details** window.

Step 7 Click on a dashed line. A dashed line indicates an aggregated link that represents more than one link.

Note Dual stack links (although aggregate) are shown as one single line.



Total 5

		A Side ⊞	Z Side ⊞
State	Link Type	Interface	Interface
⬆	L3 ISIS IPV6	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/1
⬆	L2 LLDP	GigabitEthernet0/0/0/6	GigabitEthernet0/0/0/6
⬆	L3 ISIS IPV4	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/1
⬆	L2 LLDP	GigabitEthernet0/0/0/1	GigabitEthernet0/0/0/1
⬆	L2 LAG	Bundle-Ether2	Bundle-Ether2

Use Device Groups to Filter Your Topology View

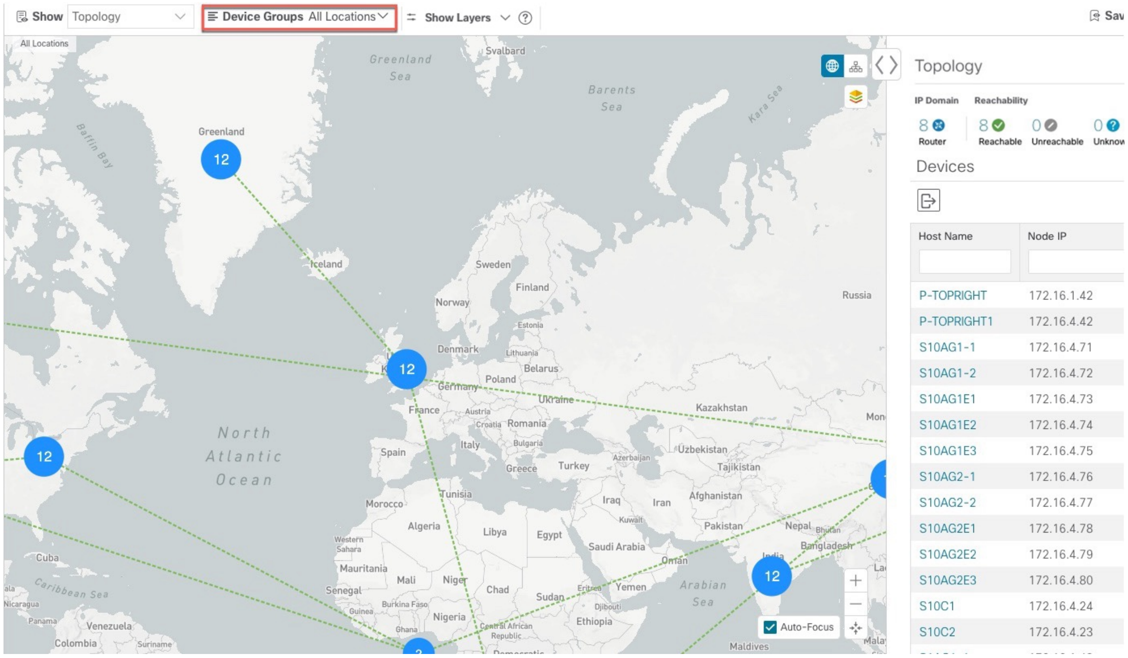
To help you identify, find, and group devices for a variety of purposes, you can create Device Groups. The Device Group window (**Device Management** > **Groups**) displays all devices and the device groups to which they belong. By default, all devices initially appear in the **Unassigned Devices** group.

To demonstrate the grouping and filtering functions, we have built an environment with devices distributed globally. You can sub-group the devices based on regions. For this example, we have a sub-group called **US West**.

Step 1 View devices on the geographical map:

a) From the main menu, choose **Topology**.

Note Devices without a geo-location appear in the **Devices** table only. To display these devices on the map, provide their geographical coordinates in the **Geo Location** column.



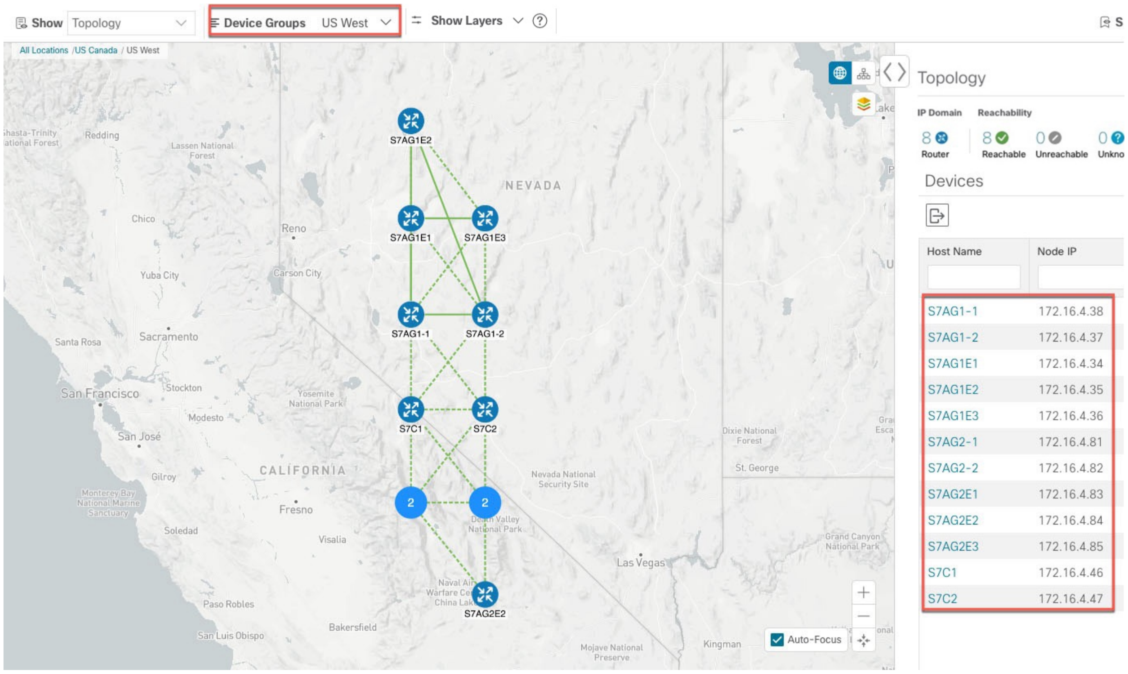
Topology

IP Domain	Reachability		
8 Router	8 Reachable	0 Unreachable	0 Unknow

Devices

Host Name	Node IP
P-TOPRIGHT	172.16.1.42
P-TOPRIGHT1	172.16.4.42
S10AG1-1	172.16.4.71
S10AG1-2	172.16.4.72
S10AG1E1	172.16.4.73
S10AG1E2	172.16.4.74
S10AG1E3	172.16.4.75
S10AG2-1	172.16.4.76
S10AG2-2	172.16.4.77
S10AG2E1	172.16.4.78
S10AG2E2	172.16.4.79
S10AG2E3	172.16.4.80
S10C1	172.16.4.24
S10C2	172.16.4.23

b) From the **Device Group** drop-down list, select a group (US West). Only the devices in that group and related links are displayed on the geographical map. The Devices table has also been filtered to list only those devices in the group.



Topology

IP Domain	Reachability		
8 Router	8 Reachable	0 Unreachable	0 Unkno

Devices

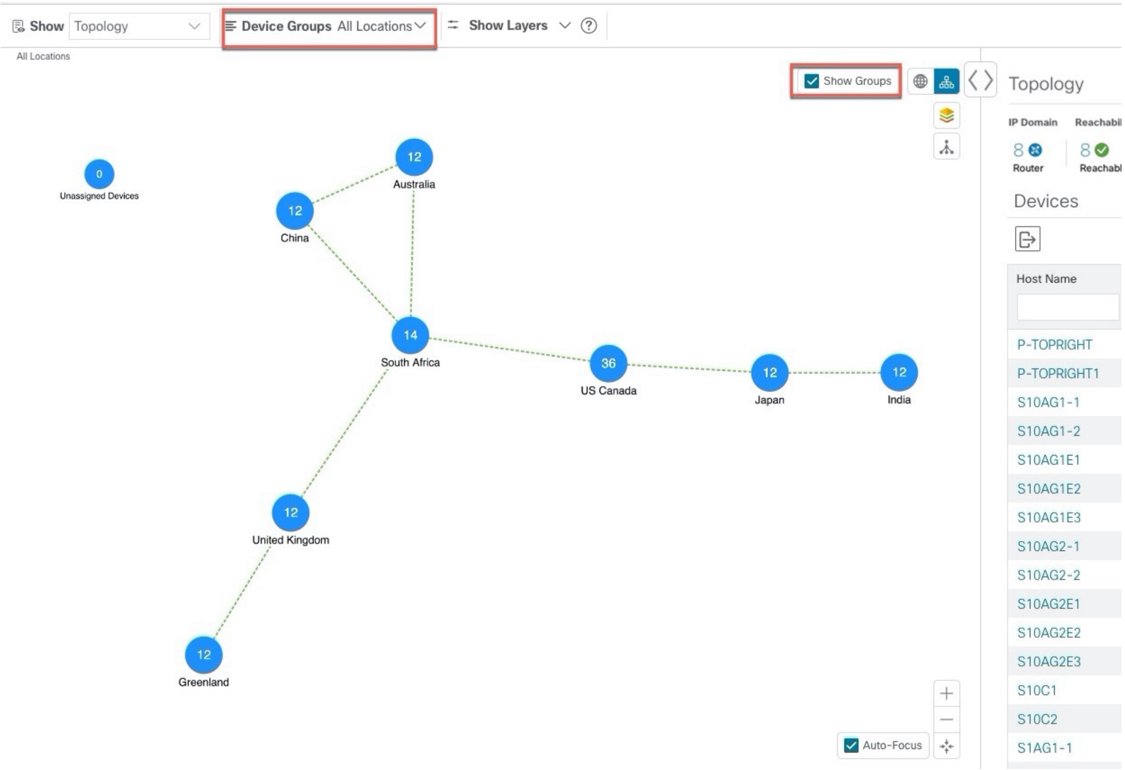
Host Name	Node IP
S7AG1-1	172.16.4.38
S7AG1-2	172.16.4.37
S7AG1E1	172.16.4.34
S7AG1E2	172.16.4.35
S7AG1E3	172.16.4.36
S7AG2-1	172.16.4.81
S7AG2-2	172.16.4.82
S7AG2E1	172.16.4.83
S7AG2E2	172.16.4.84
S7AG2E3	172.16.4.85
S7C1	172.16.4.46
S7C2	172.16.4.47

Step 2 View devices on the logical map:

a) From the main menu, choose **Topology**.

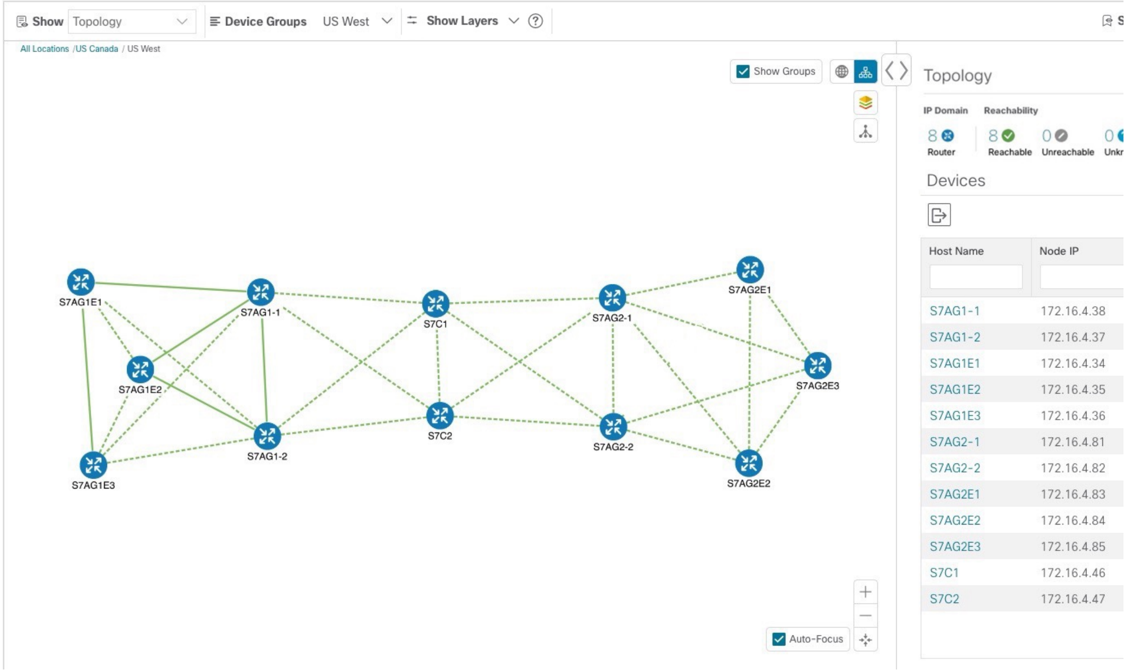
b) Click 🖧.

c) From the **Device Group** drop-down list, select **All Locations** and check **Show Groups** if it is not already checked. You can see all device groups in this view. Device groups can be seen in this way only within the logical map.



Host Name
P-TOPRIGHT
P-TOPRIGHT1
S10AG1-1
S10AG1-2
S10AG1E1
S10AG1E2
S10AG1E3
S10AG2-1
S10AG2-2
S10AG2E1
S10AG2E2
S10AG2E3
S10C1
S10C2
S1AG1-1

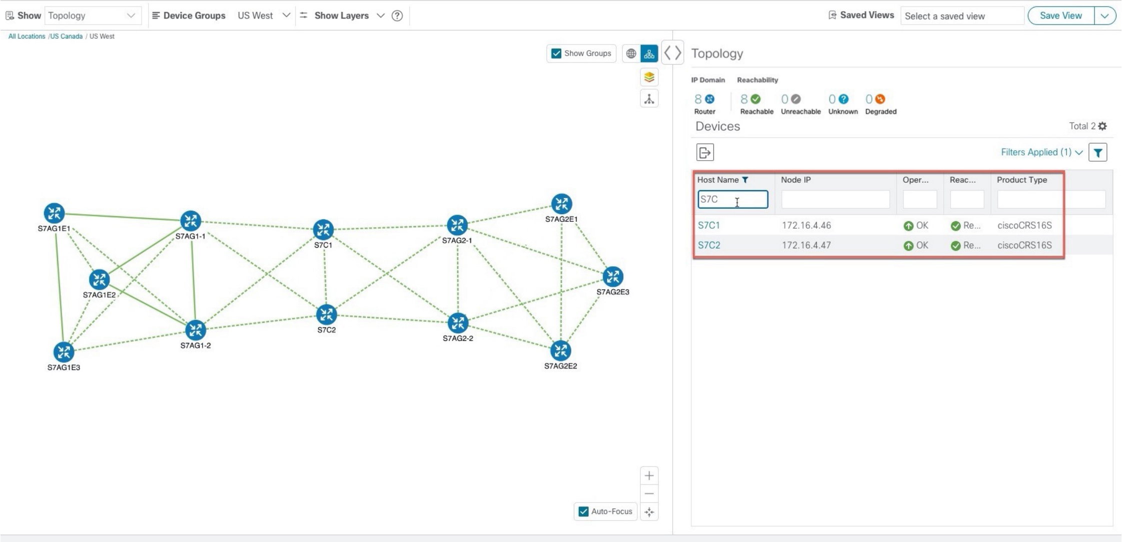
d) From the **Device Group** drop-down list, select a group (US West). Devices that belong to this group are shown in the topology map and the **Devices** table.



Host Name	Node IP
S7AG1-1	172.16.4.38
S7AG1-2	172.16.4.37
S7AG1E1	172.16.4.34
S7AG1E2	172.16.4.35
S7AG1E3	172.16.4.36
S7AG2-1	172.16.4.81
S7AG2-2	172.16.4.82
S7AG2E1	172.16.4.83
S7AG2E2	172.16.4.84
S7AG2E3	172.16.4.85
S7C1	172.16.4.46
S7C2	172.16.4.47

e) Filter devices in the Device table by entering the partial host name or IP address in the text box (for example, **S7C** is entered in the **Host Name** text box for the current configuration). The Device table displays only devices that match the filtering criteria. However, filtering the Device table does not filter the devices visually on the topology map. To visually filter devices on the geographical or logical maps is to use device groups.

Note You can also double click on the device in the list to recenter the selected device on the geographical or logical maps.



Host Name	Node IP	Oper...	Reac...	Product Type
S7C				
S7C1	172.16.4.46	OK	Re...	ciscoCRS16S
S7C2	172.16.4.47	OK	Re...	ciscoCRS16S

Create and Modify Device Groups

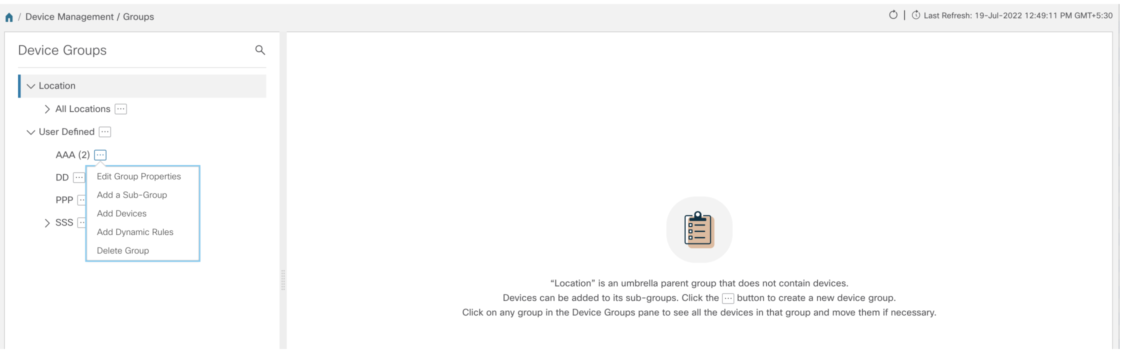
Device groups and assignment of devices to the groups can be done either manually (as described in this section) or automatically (as described in the next section).

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

Step 2 To add a new sub-group, click next to **All Locations**.
A new sub-group gets added under **All Locations**.

Step 3 To add a device to a group, from the right-pane, under **Unassigned Devices**, select a device and then from the **Move to Group**drop-down, select the appropriate group.

Step 4 To edit, delete, or add a sub-group under an existing group, from the Device Groups tree, click next to a group.



"Location" is an umbrella parent group that does not contain devices.
Devices can be added to its sub-groups. Click the ⋯ button to create a new device group.
Click on any group in the Device Groups pane to see all the devices in that group and move them if necessary.

Step 5 Choose to add, delete, or edit (rename or move) a group. If you delete a group, all devices that belong to that group are moved to the Unassigned Devices group. Also, deleting a group deletes all the sub-groups under it.

Note Devices can belong to only one device group.

Step 6 Click **Save**.

Enable 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 hostname. Any newly added or discovered devices that match the rule will be placed in the appropriate group.

Note 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.

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

Step 2 Click ⋯ next to **All Locations > Manage Dynamic Grouping Rule**.

Step 3 Click **Show more details and examples** to help you fill out the required Host Name and Group Name fields.

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.

Step 8 To move newly created Unassigned groups to the correct group, do the following:

a) Click ⋯ next to All Locations and click **Add a Sub-Group**.
b) Enter the New Group details and click **Create**.
c) Click on the unassigned devices from the left pane.
d) From the right pane, select the devices you want to move and click **Move to Group** to move to an appropriate group.

Customize Map Display Settings

You can configure visual settings on the topology map based on your needs and preferences. You can do the following:

- Customize the Display of Links and Devices, on page 23

Customize the Display of Links and Devices

To set device and link map display preferences, choose **Topology** and click ≋ on the topology map.

- Click **Links** to show aggregated links and how links should be colored so that you can easily see their state and utilization status. By default, aggregated links will be differentiated from single links on the map and links will be colored based on link utilization thresholds. Administrators can change the utilization thresholds and their corresponding colors.
- Click **Devices** to show the device state and how the devices should be labeled. By default, the device state is shown on the map and the host name is used to label devices.

Save Topology Views for Easy Access

When you rearrange the devices and links on a map, your changes are not normally saved. To easily access a useful map layout, you can save it as a named custom view and quickly retrieve it, without having to rearrange the map each time. This is especially useful when managing large networks with many devices.

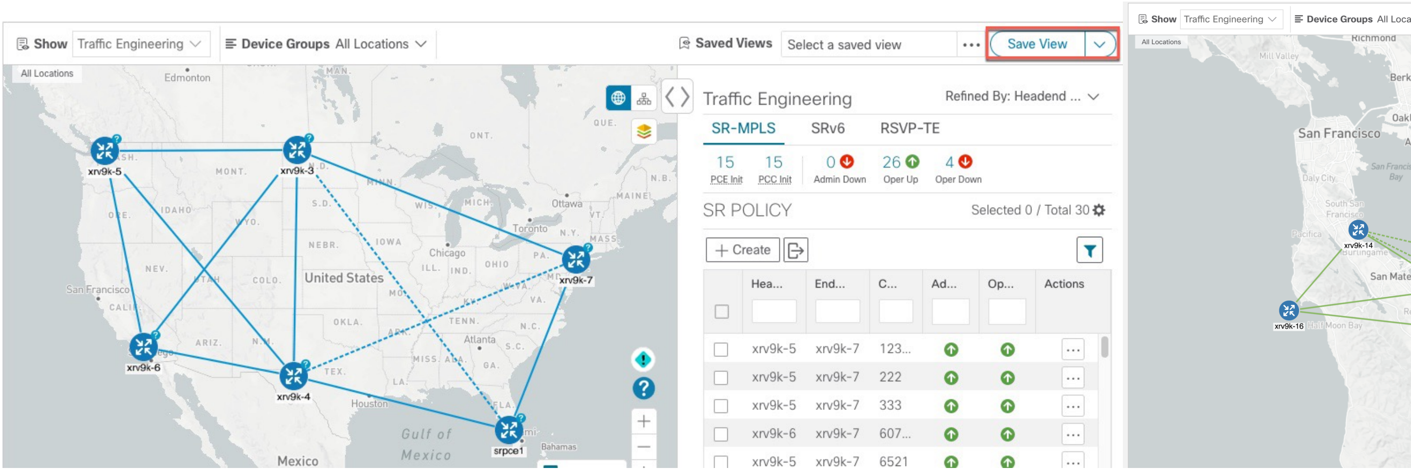
When you save a custom view, the following settings will be saved:

- Whether it is a geographical or logical map.
- Device positions in the logical map layout.
- Device and link display settings

Note All custom views can be seen by all users. However, only users with the admin role or users that created the custom view can modify the view.

Step 1 Customize the current map view until it contains only the information you want and until the layout meets your needs.

Step 2 When you have the view the way you want it, click **Save View**.



Traffic Engineering — Refined By: Headend ...

SR-MPLS | SRv6 | RSVP-TE

15 PCE Init · 15 PCC Init · 0 Admin Down · 26 Oper Up · 4 Oper Down

SR POLICY — Selected 0 / Total 30

+ Create

□	Hea...	End...	C...	Ad...	Op...	Actions
□	xrv9k-5	xrv9k-7	123...	↑	↑	...
□	xrv9k-5	xrv9k-7	222	↑	↑	...
□	xrv9k-5	xrv9k-7	333	↑	↑	...
□	xrv9k-6	xrv9k-7	607...	↑	↑	...
□	xrv9k-5	xrv9k-7	6521	↑	↑	...

Step 3 Enter a unique name for the new custom view and click **Save**. You can later modify the view (click **Select a saved view**) and choose to edit the topology, rename, or delete the view.

CHAPTER 4

Automate Network Changes

This section contains the following topics:

Change Automation Overview

The Change Automation application automates the process of deploying changes to the network. You can define automation tasks to achieve the intended network states in Change Automation using Playbooks that consists of plays written using YAML. You can then push configuration changes to Cisco Network Service Orchestrator (NSO), which deploys these changes to the network devices.

The difference between Change Automation and other existing scripted automation frameworks is that Change Automation is a *closed-loop framework*. Changes are deployed to the router or other device using programmable APIs, and the intent of the change is verified using telemetry that comes back in the router. Change Automation relies on telemetry to verify the intent of the change, avoiding the need to frequently poll the device for updates.

The following is a high level Change Automation workflow:

1. Review the existing plays and Playbooks to see if any of them meet your needs fully or partially.

Note Change Automation comes with a robust library of Playbooks, each with its own collection of configuration and check plays.

2. Build Playbook as required:
   - If the required Playbook is available, use it.
   - If the required Playbook is not available, build a new Playbook using the existing plays.
   - If some of the required plays are not available, create new plays and build a new Playbook using the new and existing plays.
3. Dry run the Playbook to test if it accomplishes the desired changes in the network.

4. Deploy the Playbook.

Change Automation allows you to customize and generate plays and Playbooks using its API interface. For more information, see About Custom Plays, on page 31 and About Customizing Playbooks, on page 36.

Configure Change Automation Settings

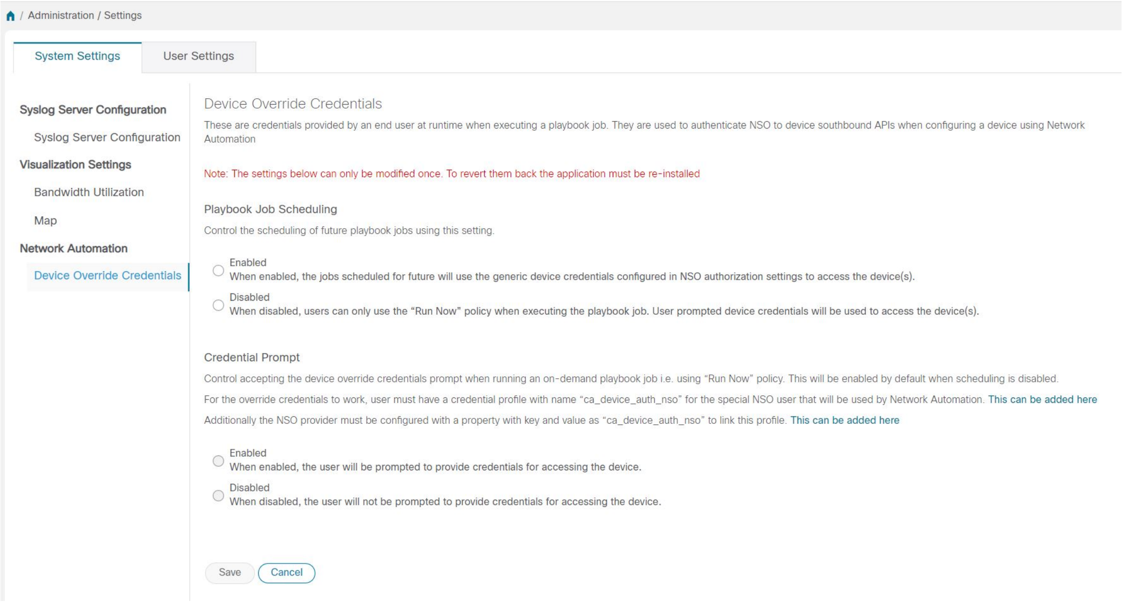
Configuring Change Automation settings is a post-installation activity and is the first task to be performed after installing Change Automation. This section explains the initial settings that must be configured before you can start using Change Automation.

Note The Change Automation settings can only be configured once. If you want to modify the settings, Change Automation must be re-installed. Before reinstalling, make sure to export the Playbooks, and after reinstalling, import the Playbooks. For more information, see Export Playbooks, on page 41 and Import Playbooks, on page 41.

System settings

After Change Automation is installed in your Crosswork platform, you can access Change Automation in the main menu (go to **Network Automation** > **Dashboard**). The Change Automation window is displayed prompting you to complete the configuration. Click **Start Configuration** to review the change Automation settings. Alternatively, you can navigate to **Administration** > **Settings** > **Device Override Credentials** to view the settings.

Figure 6: Change Automation settings


/ Administration / Settings
System Settings
User Settings
Syslog Server Configuration
Syslog Server Configuration
Visualization Settings
Bandwidth Utilization
Map
Network Automation
Device Override Credentials
Save
Cancel

Device Override Credentials

These are credentials provided by an end user at runtime when executing a playbook job. They are used to authenticate NSO to device southbound APIs when configuring a device using Network Automation

Note: The settings below can only be modified once. To revert them back the application must be re-installed

Playbook Job Scheduling

Control the scheduling of future playbook jobs using this setting.

○ Enabled
When enabled, the jobs scheduled for future will use the generic device credentials configured in NSO authorization settings to access the device(s).

○ Disabled
When disabled, users can only use the "Run Now" policy when executing the playbook job. User prompted device credentials will be used to access the device(s).

Credential Prompt

Control accepting the device override credentials prompt when running an on-demand playbook job i.e. using "Run Now" policy. This will be enabled by default when scheduling is disabled.

For the override credentials to work, user must have a credential profile with name "ca_device_auth_nso" for the special NSO user that will be used by Network Automation. This can be added here

Additionally the NSO provider must be configured with a property with key and value as "ca_device_auth_nso" to link this profile. This can be added here

○ Enabled
When enabled, the user will be prompted to provide credentials for accessing the device.

○ Disabled
When disabled, the user will not be prompted to provide credentials for accessing the device.

Click **Save** after you configure the following settings:

- **Playbook Job Scheduling**: Enable or disable the ability the schedule the Playbook jobs.

- **Credential Prompt**: Device override credentials are an additional level of authentication that can improve change auditing. If enabled, users will be prompted to enter the credentials (device override credentials) before each Playbook execution. If disabled, you must create the relevant credential profile and provider settings for the override credentials to work. Follow the prompts on the window to meet each requirement.

Note If **Playbook Job Scheduling** is **disabled**, then the **Credential Prompt** is **enabled**, by default. You cannot disable the credential prompt in this case.

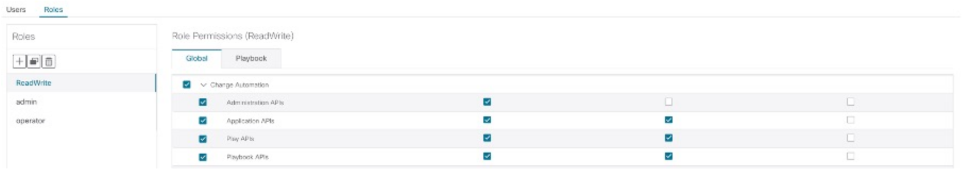
Note While executing Device Config plays, entering incorrect device override credentials will cause the playbook execution to fail. However, for a Check play or Data Collection play, the device override credentials are not validated and the Playbook will execute successfully irrespective of the accuracy of the override credentials. Device override credentials are only validated while pushing configuration changes.

Note Also, users with write permissions for the **Administration APIs** under **Change Automation** (Go to **Administration** > **Users and Roles** > **Roles**) can only perform this task.

Assign proper level of access to other users

Once the system settings are completed, the admin user must review the user roles to make sure that all the users they have are configured with the proper level of access to run, import, and create Plays and Playbooks. To provide the access, the admin user must:

1. Go to **Administration** > **Users and Roles** > **Roles**.
2. Under **Roles** pane, select the role for which you want to grant the access.
3. Under the **Role Permissions** > **Global**, enable **Read** and **Write** check boxes (as necessary) for **Play APIs** and **Playbook APIs** under **Change Automation**.



☑ Change Automation			
☑ Administration APIs	☑	□	□
☑ Application APIs	☑	☑	□
☑ Play APIs	☑	☑	□
☑ Playbook APIs	☑	☑	□

Note Also, the user with write permissions for **Administration APIs** can only disable or enable run Playbook access and assign labels.

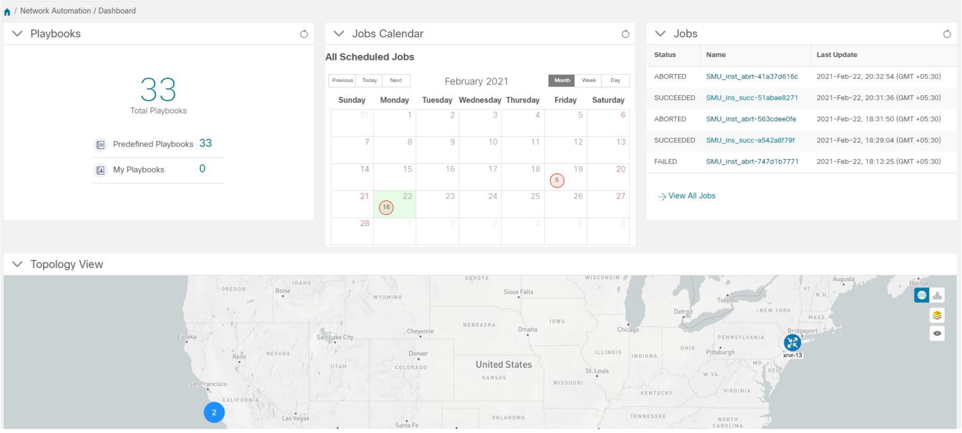
Use the Change Automation Dashboard

The Change Automation application's **Dashboard** window (shown in the figure below) lets you view all Playbook-related activity and initiate Playbook runs. It displays the total number of Playbooks, the Playbook

Jobs Calendar, the most recently run Playbook jobs, and the same network topology map you see when you select **Topology** from the main menu.

To view the Change Automation **Dashboard** window, select **Network Automation** > **Dashboard**.

Figure 7: Change Automation Dashboard Window



/ Network Automation / Dashboard

Playbooks

33

Total Playbooks

Predefined Playbooks 33

My Playbooks 0

Jobs Calendar

All Scheduled Jobs

Previous Today Next — February 2021 — Month Week Day

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19 5	20
21	22 16	23	24	25	26	27
28	1	2	3	4	5	6

Jobs

Status	Name	Last Update
ABORTED	SMU_inst_abrt-41a37d616c	2021-Feb-22, 20:32:54 (GMT +05:30)
SUCCEEDED	SMU_ins_succ-51abae8271	2021-Feb-22, 20:31:36 (GMT +05:30)
ABORTED	SMU_inst_abrt-563cdee0fe	2021-Feb-22, 18:31:50 (GMT +05:30)
SUCCEEDED	SMU_ins_succ-a542a8f79f	2021-Feb-22, 18:29:04 (GMT +05:30)
FAILED	SMU_inst_abrt-747d1b7771	2021-Feb-22, 18:13:25 (GMT +05:30)

→ View All Jobs

Topology View

The **Playbooks** tile displays the total number of Playbooks (pre-defined and custom). Clicking on a specific number displays all the Playbooks that correspond to the selected category.

Note **Total Playbooks** indicate the total number of pre-defined and user created. Playbooks (My Playbooks) that exist in the system.

Predefined Playbooks indicate the number of pre-defined Playbooks that exist in the system.

My Playbooks indicate the number of custom Playbooks that are created by the current user.

Creating Playbooks does not use a license. The license count is incremented only upon the first execution of a Playbook (pre-defined or user created), irrespective of whether the Playbook runs successfully or not. Subsequent execution of the Playbook does not increment the license count.

The **Jobs Calendar** tile displays a calendar (month, week, day) with the number of job sets executed on a given day that is marked in a circle against the corresponding date. Clicking on the number displays a dialog box with the names of the Playbook job sets and their execution time. Click the desired job set to view the execution details.

Note The color of the circle indicates the overall status of the job sets.

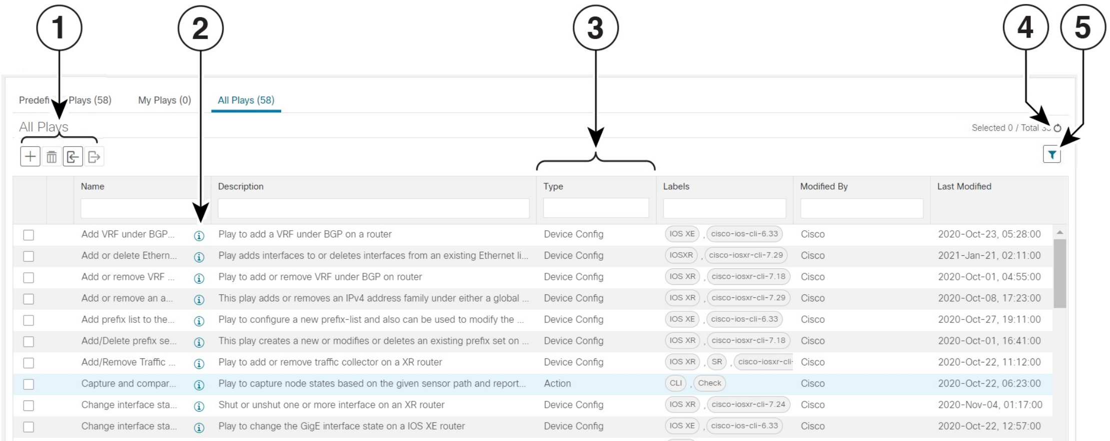
- A **red** circle indicates at least one job set with **Failed** status among the day's overall job sets.
- A **grey** circle indicates that all job sets are either in **Scheduled** or **Running** status.
- A **blue** circle indicates at least one critical job set in **Recovered** status among the day's overall job sets.
- A **green** circle indicates most of the Playbooks are in success state. Clicking on it displays all the jobs that are **Recovered**, **Scheduled**, or **Running**.

The **View All Jobs** link on the **Jobs** tile give you direct access to the Change Automation **Automation Job History** window.

View the Play list

The **Play List** window of the Change Automation application gives you a consolidated list of all the Plays in the system.

From the main menu, select **Network Automation** > **Play List** to view the **Play List** window.



Predefi Plays (58)   My Plays (0)   All Plays (58)

All Plays

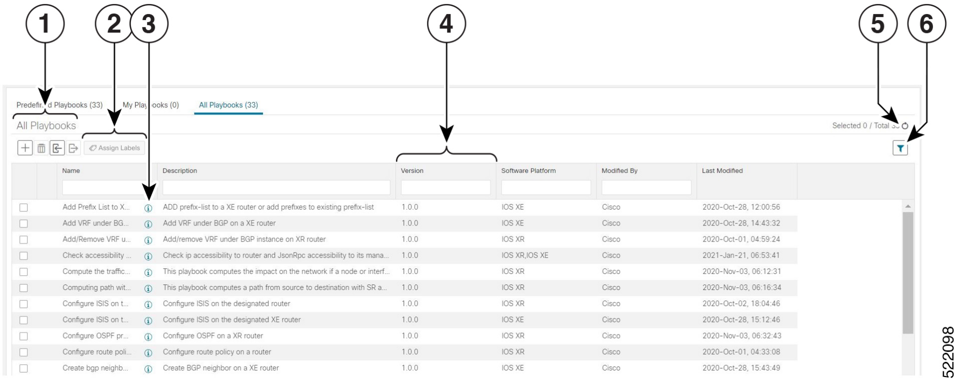
Selected 0 / Total

	Name		Description	Type	Labels	Modified By	Last Modified
□	Add VRF under BGP...	ℹ	Play to add a VRF under BGP on a router	Device Config	IOS XE , cisco-ios-cli-6.33	Cisco	2020-Oct-23, 05:28:00
□	Add or delete Ethern...	ℹ	Play adds interfaces to or deletes interfaces from an existing Ethernet li...	Device Config	IOSXR , cisco-iosxr-cli-7.29	Cisco	2021-Jan-21, 02:11:00
□	Add or remove VRF ...	ℹ	Play to add or remove VRF under BGP on router	Device Config	IOS XR , cisco-iosxr-cli-7.18	Cisco	2020-Oct-01, 04:55:00
□	Add or remove an a...	ℹ	This play adds or removes an IPv4 address family under either a global ...	Device Config	IOS XR , cisco-iosxr-cli-7.29	Cisco	2020-Oct-08, 17:23:00
□	Add prefix list to the...	ℹ	Play to configure a new prefix-list and also can be used to modify the ...	Device Config	IOS XE , cisco-ios-cli-6.33	Cisco	2020-Oct-27, 19:11:00
□	Add/Delete prefix se...	ℹ	This play creates a new or modifies or deletes an existing prefix set on ...	Device Config	IOS XR , cisco-iosxr-cli-7.18	Cisco	2020-Oct-01, 16:41:00
□	Add/Remove Traffic ...	ℹ	Play to add or remove traffic collector on a XR router	Device Config	IOS XR , SR , cisco-iosxr-cli-	Cisco	2020-Oct-22, 11:12:00
□	Capture and compar...	ℹ	Play to capture node states based on the given sensor path and report...	Action	CLI , Check	Cisco	2020-Oct-22, 06:23:00
□	Change interface sta...	ℹ	Shut or unshut one or more interface on an XR router	Device Config	IOS XR , cisco-iosxr-cli-7.24	Cisco	2020-Nov-04, 01:17:00
□	Change interface sta...	ℹ	Play to change the GigE interface state on a IOS XE router	Device Config	IOS XE , cisco-ios-cli-6.33	Cisco	2020-Oct-22, 12:57:00

Item	Description
1	Click + to create a custom Play. See Create a Custom Play using Templates, on page 31.
	Click 🗑 to delete a custom Play. See Delete Custom Plays, on page 36.
	Click ⇦ to import custom Play from a gzipped TAR archive file. See Import Custom Plays, on page 35.
	Click ⇨ to export a custom Play as a gzipped TAR archive file. See Export Plays, on page 35.
2	Click ℹ to see a pop-up **Play Details** window showing the Play's description and schema. When you are finished viewing these details, click ✕ to close the pop-up window.
3	The **Type** column indicates the type of the Play. You can click the column headings (Name, Description, Type, Labels, and Modified by) to sort the table by that column's data.
4	Click ↻ to refresh the Plays list.
5	Click ▼ to set filter criteria on one or more columns in the table.
	Click the **Clear Filter** link to clear any filter criteria you may have set.

View the Playbook List

The Change Automation application's **Playbook List** window (in the following figure) gives you a consolidated list of all the Playbooks in the system. To view the **Playbook List** window, select **Network Automation** > **Playbook List**.



Predefined Playbooks (33) | My Playbooks (0) | All Playbooks (33)

All Playbooks

Selected 0 / Total 33

＋ 🗑 ⇦ ⇨ Assign Labels

□	Name		Description	Version	Software Platform	Modified By	Last Modified
□	Add Prefix List to X...	ⓘ	ADD prefix-list to a XE router or add prefixes to existing prefix-list	1.0.0	IOS XE	Cisco	2020-Oct-28, 12:00:56
□	Add VRF under BG...	ⓘ	Add VRF under BGP on a XE router	1.0.0	IOS XE	Cisco	2020-Oct-28, 14:43:32
□	Add/Remove VRF u...	ⓘ	Add/remove VRF under BGP instance on XR router	1.0.0	IOS XR	Cisco	2020-Oct-01, 04:59:24
□	Check accessibility ...	ⓘ	Check ip accessibility to router and JsonRpc accessibility to its mana...	1.0.0	IOS XR,IOS XE	Cisco	2021-Jan-21, 06:53:41
□	Compute the traffic...	ⓘ	This playbook computes the impact on the network if a node or interf...	1.0.0	IOS XR	Cisco	2020-Nov-03, 06:12:31
□	Computing path wit...	ⓘ	This playbook computes a path from source to destination with SR a...	1.0.0	IOS XR	Cisco	2020-Nov-03, 06:16:34
□	Configure ISIS on t...	ⓘ	Configure ISIS on the designated router	1.0.0	IOS XR	Cisco	2020-Oct-02, 18:04:46
□	Configure ISIS on t...	ⓘ	Configure ISIS on the designated XE router	1.0.0	IOS XE	Cisco	2020-Oct-28, 15:12:46
□	Configure OSPF pr...	ⓘ	Configure OSPF on a XR router	1.0.0	IOS XR	Cisco	2020-Nov-03, 06:32:43
□	Configure route poli...	ⓘ	Configure route policy on a router	1.0.0	IOS XR	Cisco	2020-Oct-01, 04:33:08
□	Create bgp neighb...	ⓘ	Create BGP neighbor on a XE router	1.0.0	IOS XE	Cisco	2020-Oct-28, 15:43:49

Item	Description
1	Click ＋ to create a custom Playbook. See Create a Custom Playbook Through the UI, on page 37.
	Click 🗑 to delete the currently selected custom Playbook. See Delete Custom Playbooks, on page 42.
	Click ⇦ to import Playbooks from a gzipped TAR archive file. See Import Playbooks, on page 41.
	Click ⇨ to export the currently selected Playbook(s) as a gzipped TAR archive file. See Export Playbooks, on page 41.
2	Click **Assign Labels** to assign lable(s) to the Playbook. Assigning label(s) to the Playbooks gives the system administrator the ability to control which Playbooks each user role is allowed to run.
3	Click ⓘ to see a pop-up **Playbook Details** window showing the Playbook's description, software compatibility, version number, and its plays. When you are finished viewing these details, click ✕ to close the pop-up window.
3	click the **Name**, **Description**, **Version**, **Software Platform**, and **Last Modified** column headings in the table to sort the table by that column's data. You can also choose which columns are shown, and set quick or advanced filters on any column.
4	Click ↻ to refresh the Playbooks list.
5	Click ▼ to set filter criteria on one or more columns in the table.
	Click the **Clear Filter** link to clear any filter criteria you may have set.

About Custom Plays

Change Automation allows you to create their own custom Plays, either based on Cisco models or from scratch. You can also import, export, and delete their custom Plays.

You can create custom Plays in any of the following types:

- **Check Plays**: Verifies the data from your devices using a logical expression.
- **Data Collection Plays**: Collects data from your devices.
- **Device Config Plays**: Performs configuration changes on your device
- **Service Plays**: Provisions and manages a service that is deployed.

Note You cannot edit, export, or delete, Cisco-supplied Plays.

Note Check Play and Data Collection Play support MDT and SNMP collection.

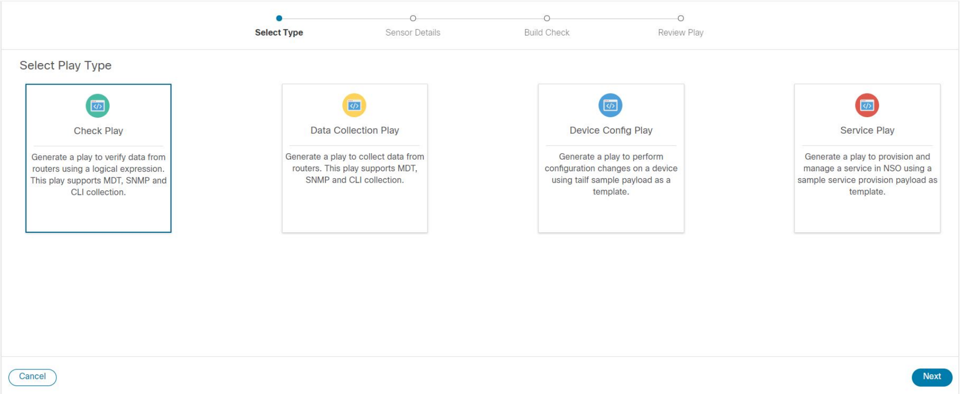
Create a Custom Play using Templates

This section explains the procedure to create a custom Play. The stages of Play creation varies depending on the Play type you choose:

- **Check Play**: *Select Play Type > Select Sensor Path > Build Check Expression > Review Play*
- **Data Collection Play**: *Select Play Type > Select Sensor Path > Build Filter Expression > Review Play*
- **Device Config Play** or **Service Play**: *Select Play Type > Configure Play (using sample payload in JSON format) > Review Play*

Step 1 From the main menu, choose **Network Automation** > **Play List**. The **Play List** window is displayed.

Step 2 Click ⊞ to create a custom Play. The **Select Play Type** window opens displaying the types of Plays supported and a description for each. The stages of creation are also displayed, and it varies depending on the Play type you select.



Select Type · Sensor Details · Build Check · Review Play

Select Play Type

Check Play
Generate a play to verify data from routers using a logical expression. This play supports MDT, SNMP and CLI collection.

Data Collection Play
Generate a play to collect data from routers. This play supports MDT, SNMP and CLI collection.

Device Config Play
Generate a play to perform configuration changes on a device using tailf sample payload as a template.

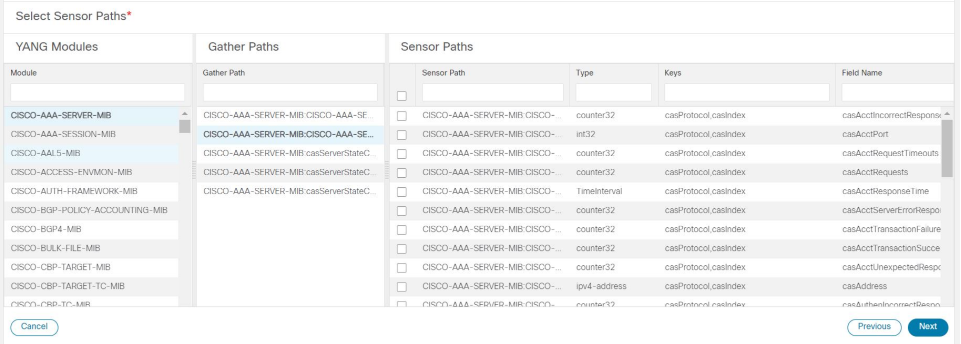
Service Play
Generate a play to provision and manage a service in NSO using a sample service provision payload as template.

Select the Play type that you want to create and click **Next**.

Step 3 Creating a Check Play or Data Collection Play

Note When creating Check or Data collection plays, Cisco provides YANG modules for Cisco products. The process that is described in this section assumes that the sensor that you want to use or the field that you want to modify is included in the modules that are provided by Cisco. If the sensor or field is not listed in the default YANG modules, Cisco allows you to expand the device coverage. For information on loading a new or modified module, see *Section: Manage Custom Software Packages* in the *Cisco Crosswork Infrastructure 4.3 and Applications Administration Guide*.

a) In the **Select Sensor Paths** window, select the required YANG module, Gather Path, and Sensor Paths. Click **Next** to continue.



Select Sensor Paths*

YANG Modules

Module
CISCO-AAA-SERVER-MIB
CISCO-AAA-SESSION-MIB
CISCO-AAL5-MIB
CISCO-ACCESS-ENVMON-MIB
CISCO-AUTH-FRAMEWORK-MIB
CISCO-BGP-POLICY-ACCOUNTING-MIB
CISCO-BGP4-MIB
CISCO-BULK-FILE-MIB
CISCO-CBP-TARGET-MIB
CISCO-CBP-TARGET-TC-MIB
CISCO-CBP-TC-MIB

Gather Paths

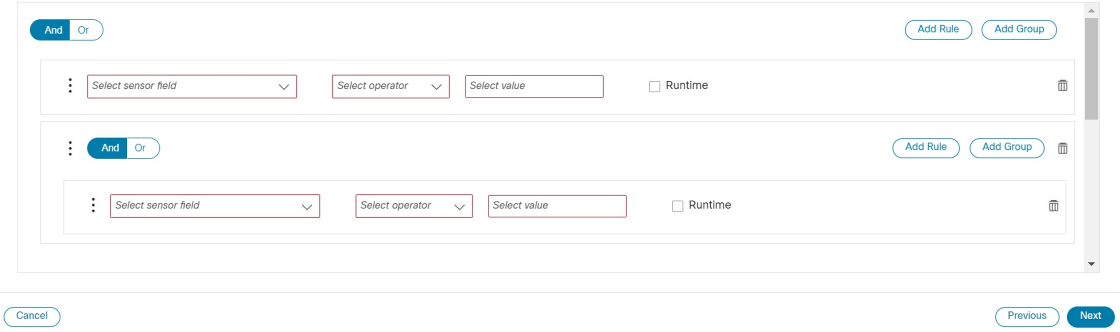
Gather Path
CISCO-AAA-SERVER-MIB:CISCO-AAA-SE...
CISCO-AAA-SERVER-MIB:CISCO-AAA-SE...
CISCO-AAA-SERVER-MIB:casServerStateC...
CISCO-AAA-SERVER-MIB:casServerStateC...
CISCO-AAA-SERVER-MIB:casServerStateC...

Sensor Paths

□	Sensor Path	Type	Keys	Field Name
□	CISCO-AAA-SERVER-MIB:CISCO-...	counter32	casProtocol,casIndex	casAcctIncorrectRespons
□	CISCO-AAA-SERVER-MIB:CISCO-...	int32	casProtocol,casIndex	casAcctPort
□	CISCO-AAA-SERVER-MIB:CISCO-...	counter32	casProtocol,casIndex	casAcctRequestTimeouts
□	CISCO-AAA-SERVER-MIB:CISCO-...	counter32	casProtocol,casIndex	casAcctRequests
□	CISCO-AAA-SERVER-MIB:CISCO-...	TimeInterval	casProtocol,casIndex	casAcctResponseTime
□	CISCO-AAA-SERVER-MIB:CISCO-...	counter32	casProtocol,casIndex	casAcctServerErrorRespo
□	CISCO-AAA-SERVER-MIB:CISCO-...	counter32	casProtocol,casIndex	casAcctTransactionFailure
□	CISCO-AAA-SERVER-MIB:CISCO-...	counter32	casProtocol,casIndex	casAcctTransactionSucce
□	CISCO-AAA-SERVER-MIB:CISCO-...	counter32	casProtocol,casIndex	casAcctUnexpectedResp
□	CISCO-AAA-SERVER-MIB:CISCO-...	ipv4-address	casProtocol,casIndex	casAddress
□	CISCO-AAA-SERVER-MIB:CISCO-	counter32	casProtocol,casIndex	casAuthenIncorrectRespo

b) Depending on the Play type you have selected, you must **Build Check** (for Check Play) or **Build Filter** (for Data Collection Play) to apply in your Play. Click **Add Rule** to add a logic expression using the keys and fields of the selected sensor path(s). Click **Add Group** to add a new logic group. Select the sensor field, operator, and value from the drop-down lists. Select the desired logic operation (AND/OR) between each rule or group.

Click **Runtime** check box if you prefer to enter the value of the sensor field dynamically during run time. If you select this check box, the *value* field is disabled, and you will be prompted to enter the input parameter when this Play is executed (as part of a Playbook) during run time.



Click **Next** to continue.

Step 4 **Creating a Device Config Play or Service Play**

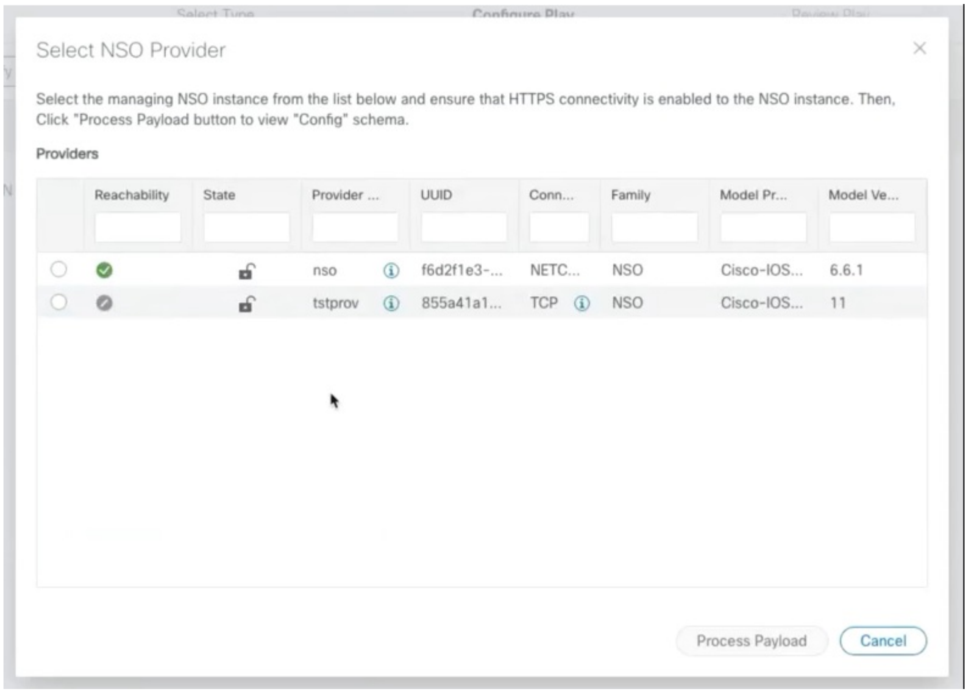
Note Ensure that the configuration that you are trying to create is available in the NSO, or else it shows an error.

When creating a Service Play, you are not creating a new service for NSO, but creating a Play to manage and provision an existing service in one or more NSO instances. For more information, see https://developer.cisco.com/docs/nso/.

a) In the **Configure Play** window, click or the **Import** link to import your device config (.JSON) file. You can download and use the sample configuration template. Browse and select your .JSON file, and click **Import**.

b) In the acknowledgment prompt, click **Continue** to select the NSO instance for the config you have imported.

c) Select the NSO provider instance from the dialog box, and click **Process Payload**.



Select NSO Provider

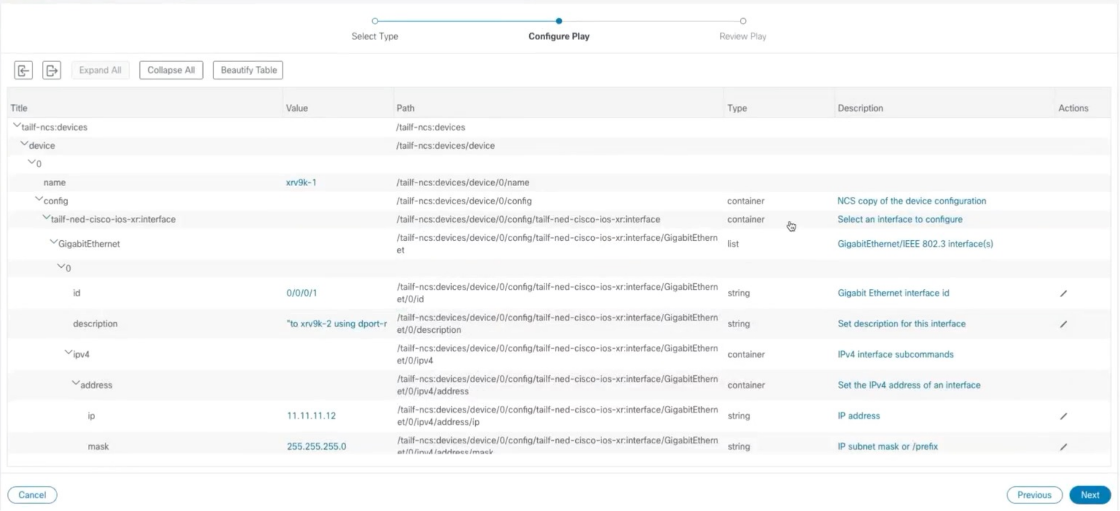
Select the managing NSO instance from the list below and ensure that HTTPS connectivity is enabled to the NSO instance. Then, Click "Process Payload button to view "Config" schema.

Providers

	Reachability	State	Provider ...	UUID	Conn...	Family	Model Pr...	Model Ve...
○	✓	🔓	nso ⓘ	f6d2f1e3-...	NETC...	NSO	Cisco-IOS...	6.6.1
○	●	🔓	tstprov ⓘ	855a41a1...	TCP ⓘ	NSO	Cisco-IOS...	11

Note The creation workflow of a Service Play is similar to the Device Config Play, except in the template of the payload file used.

d) The **Configure Play** window opens displaying information from the payload file. You can edit the *value* or *description* columns with the values that you want to see during a Playbook execution.



Title	Value	Path	Type	Description	Actions
tailf-ncs:devices		/tailf-ncs:devices			
device		/tailf-ncs:devices/device			
0					
name	xrv9k-1	/tailf-ncs:devices/device/0/name			
config		/tailf-ncs:devices/device/0/config	container	NCS copy of the device configuration	
tailf-ned-cisco-ios-xr:interface		/tailf-ncs:devices/device/0/config/tailf-ned-cisco-ios-xr:interface	container	Select an interface to configure	
GigabitEthernet		/tailf-ncs:devices/device/0/config/tailf-ned-cisco-ios-xr:interface/GigabitEthernet	list	GigabitEthernet/IEEE 802.3 interface(s)	
0					
id	0/0/0/1	/tailf-ncs:devices/device/0/config/tailf-ned-cisco-ios-xr:interface/GigabitEthernet/0/id	string	Gigabit Ethernet interface id	✎
description	"to xrv9k-2 using dport-r	/tailf-ncs:devices/device/0/config/tailf-ned-cisco-ios-xr:interface/GigabitEthernet/0/description	string	Set description for this interface	✎
ipv4		/tailf-ncs:devices/device/0/config/tailf-ned-cisco-ios-xr:interface/GigabitEthernet/0/ipv4	container	IPv4 interface subcommands	
address		/tailf-ncs:devices/device/0/config/tailf-ned-cisco-ios-xr:interface/GigabitEthernet/0/ipv4/address	container	Set the IPv4 address of an interface	
ip	11.11.11.12	/tailf-ncs:devices/device/0/config/tailf-ned-cisco-ios-xr:interface/GigabitEthernet/0/ipv4/address/ip	string	IP address	✎
mask	255.255.255.0	/tailf-ncs:devices/device/0/config/tailf-ned-cisco-ios-xr:interface/GigabitEthernet/0/ipv4/address/mask	string	IP subnet mask or /prefix	✎

Click **Next** to continue.

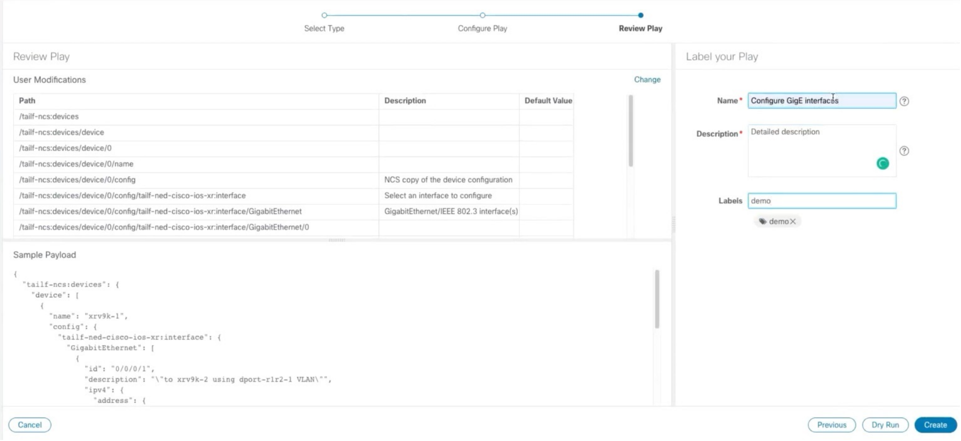
Step 5 In the **Review Play** window, review the parameters of your Play. Click **Dry Run** to validate your parameters.

Label your Play with a unique **Name** and **Description**.

Note Cisco also formats the play names with indicators such as cfg for configuration, chk for check, and so on, in the name to help you organize the plays properly. You can also use a similar tagging for the plays you create.

You can also add labels to your Play to group it in the future (optional).

Note The labels determine the type of devices that you can use the play with. For example, an IOS XR Play cannot run on IOS XE devices. Be sure to review the labels (IOS XR, IOS XE, and so on) that exist when you add them.



Path	Description	Default Value
/tailf-ncs:devices		
/tailf-ncs:devices/device		
/tailf-ncs:devices/device/0		
/tailf-ncs:devices/device/0/name		
/tailf-ncs:devices/device/0/config	NCS copy of the device configuration	
/tailf-ncs:devices/device/0/config/tailf-ned-cisco-ios-xr:interface	Select an interface to configure	
/tailf-ncs:devices/device/0/config/tailf-ned-cisco-ios-xr:interface/GigabitEthernet	GigabitEthernet/IEEE 802.3 interface(s)	
/tailf-ncs:devices/device/0/config/tailf-ned-cisco-ios-xr:interface/GigabitEthernet/0		

Name* Configure GigE interfaces

Description* Detailed description

Labels demo

demo ✕

```
{
  "tailf-ncs:devices": {
    "device": [
      {
        "name": "xrv9k-1",
        "config": {
          "tailf-ned-cisco-ios-xr:interface": {
            "GigabitEthernet": [
              {
                "id": "0/0/0/1",
                "description": "\"to xrv9k-2 using dport-r1r2-1 VLAN\"",
                "ipv4": {
                  "address": {
```

Step 6 If you are satisfied with your changes, click **Create**.

The **Play List** window opens displaying your new custom Play in the Play list.

Export Plays

A user must have Change Automation read permission to export any custom Play that is authored or imported by you or another user into Cisco Crosswork Change Automation.

The exported archive contains only the user-customizable files that are listed in Playbook Components and Files, on page 36. Once you extract them from the archive, you can identify the Play components by their file names and filename extensions.

Step 1 From the main menu, choose **Network Automation** > **Play List**.

Step 2 Check the check boxes for the custom Plays you want to export.

Step 3 Click ⎘. Your browser will prompt you to select a path and the file name to use when saving the gzipped tar archive. Follow the prompts to save the file.

Import Custom Plays

You can import any custom Play that meets the following requirements:

- The Play files must be packaged as a gzipped tar archive.
- The archive must contain a `.play` file (a data spec file for the play), at minimum.
- The archive file must have a unique name.

Note For more details about editing and importing, see Cisco Crosswork Change Automation Developer Guide.

You *can* overwrite a custom Play. The system will warn you when you are about to overwrite a custom Play, but will not prevent you from doing so.

Warning Take precautions to ensure that you do not accidentally overwrite the custom Plays that you had created.

Before you begin

A user must have the write access to import Plays. For more information about granting read-writer role access to a user, see *Assign proper level of access to other users* in Configure Change Automation Settings, on page 26.

Step 1 From the main menu, choose **Network Automation** > **Play List**.

Step 2 Click ⇤. Your browser will prompt you to browse to and select the gzipped archive file containing the Plays you want to import.

Make sure that there is no Cisco-supplied Plays with the same name as the Play you intend to import. If you import a Play with the same name, it fails.

Step 3 Follow the prompts to import the archive file.

Delete Custom Plays

You can delete custom Plays only. You cannot delete a Cisco-supplied Play.

Your user ID must have Change Automation delete permission to delete Plays.

Step 1 From the main menu, choose **Network Automation** > **Play List**.

Step 2 In the **Play List** window, select the custom Plays that you want to delete.

Step 3 Click 🗑 icon.

Step 4 When prompted, click **Delete** again to confirm.

About Customizing Playbooks

You can create their own Playbooks from scratch that are based on the details from Cisco-supplied Playbooks. They can also create custom Playbooks using the available Plays.

Creating and modifying Cisco-supplied Playbooks are engineering tasks that take place outside of the user interface for Cisco Crosswork Change Automation. As such, they are outside the scope of this User Guide.

Cisco supplies developer-level documentation for Cisco-supplied Playbooks. For more information on how to create custom plays and Playbooks, see:

- "Playbooks" and "Plays" references in the Change Automation Developer Guide on Cisco Devnet
- "Custom Playbooks" tutorial in the Change Automation Developer Guide on Cisco DevNet

Playbook Components and Files

Change Automation Playbooks contain various components, referred to using specialized names. The components are implemented in the Playbook as files. Some of these components' names are borrowed from the Ansible specification, but all have their own definitions, and not all the corresponding files can be customized by users. Some components are Cisco proprietary intellectual property; while you can use them in custom Plays and Playbooks, you cannot customize them directly. For more information, see Section: Writing Custom Playbooks at Cisco Crosswork Change Automation Developer Guide.

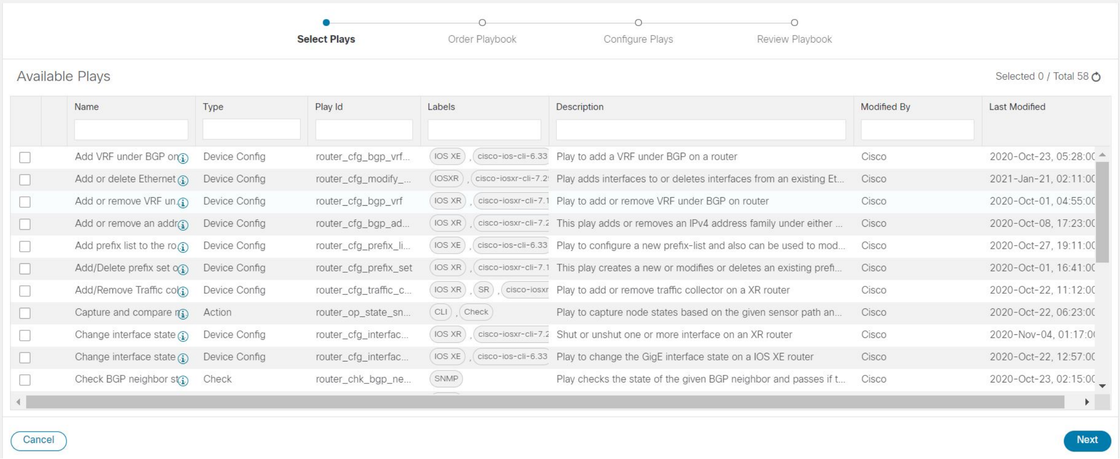
Create a Custom Playbook Through the UI

Change Automation allow users with admin and read/write roles to create custom Playbooks using the available Plays. For more information about granting read/write role access to a user, see *Assign proper level of access to other users* in Configure Change Automation Settings, on page 26.

Note You cannot edit a custom Playbook after it is created. It is recommended to Dry Run the Playbook before completing the creation to make sure that the purpose of the Playbook is met. Once created, if you must make changes to the custom Playbook, you have to recreate your Playbook with the relevant changes.

Step 1 From the main menu, choose **Network Automation** > **Playbook List**. The **Playbook List** window is displayed.

Step 2 Click ⊞ to create a custom Playbook. The **Select Plays** window opens displaying the available Plays. The stages of creation are also displayed.



Available Plays

Selected 0 / Total 58

	Name	Type	Play Id	Labels	Description	Modified By	Last Modified
□	Add VRF under BGP on	Device Config	router_cfg_bgp_vrf...	IOS XE, cisco-ios-cli-6.33	Play to add a VRF under BGP on a router	Cisco	2020-Oct-23, 05:28:0(
□	Add or delete Ethernet	Device Config	router_cfg_modify_...	IOSXR, cisco-iosxr-cli-7.2	Play adds interfaces to or deletes interfaces from an existing Et...	Cisco	2021-Jan-21, 02:11:0(
□	Add or remove VRF un	Device Config	router_cfg_bgp_vrf	IOS XR, cisco-iosxr-cli-7.1	Play to add or remove VRF under BGP on router	Cisco	2020-Oct-01, 04:55:0(
□	Add or remove an addr	Device Config	router_cfg_bgp_ad...	IOS XR, cisco-iosxr-cli-7.2	This play adds or removes an IPv4 address family under either ...	Cisco	2020-Oct-08, 17:23:0(
□	Add prefix list to the ro	Device Config	router_cfg_prefix_li...	IOS XE, cisco-ios-cli-6.33	Play to configure a new prefix-list and also can be used to mod...	Cisco	2020-Oct-27, 19:11:0(
□	Add/Delete prefix set o	Device Config	router_cfg_prefix_set	IOS XR, cisco-iosxr-cli-7.1	This play creates a new or modifies or deletes an existing prefi...	Cisco	2020-Oct-01, 16:41:0(
□	Add/Remove Traffic col	Device Config	router_cfg_traffic_c...	IOS XR, SR, cisco-iosxr	Play to add or remove traffic collector on a XR router	Cisco	2020-Oct-22, 11:12:0(
□	Capture and compare n	Action	router_op_state_sn...	CLI, Check	Play to capture node states based on the given sensor path an...	Cisco	2020-Oct-22, 06:23:0(
□	Change interface state	Device Config	router_cfg_interfac...	IOS XR, cisco-iosxr-cli-7.2	Shut or unshut one or more interface on an XR router	Cisco	2020-Nov-04, 01:17:0(
□	Change interface state	Device Config	router_cfg_interfac...	IOS XE, cisco-ios-cli-6.33	Play to change the GigE interface state on a IOS XE router	Cisco	2020-Oct-22, 12:57:0(
□	Check BGP neighbor st	Check	router_chk_bgp_ne...	SNMP	Play checks the state of the given BGP neighbor and passes if t...	Cisco	2020-Oct-23, 02:15:0(

Select all the Plays you want in your Playbook, and click **Next**.

Note It is recommended to include **Sync NSO from device** Play. This Play performs the NSO sync from device to get the configuration in NSO to match the device.

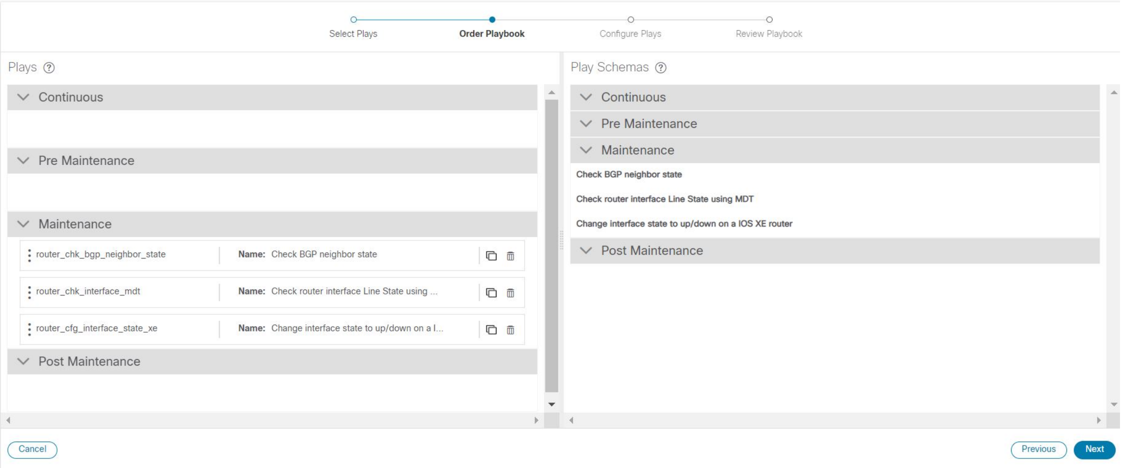
Step 3 In the **Order Playbook** window, arrange the order of the Plays in the Playbook as per the execution phase (Continuous, Pre-maintenance, Maintenance, Post Maintenance). By default, all the selected Plays are displayed within the Maintenance phase. You can click and drag the Plays to rearrange them to the appropriate phase.

Depending on the type of Play you have selected, it may be restricted from being used in certain phases. For example, a configuration Play cannot be used outside of the Maintenance phase.

For more information on each execution phase, see Playbook Execution Order, on page 44.

Crosswork Change Automation also formats the Play names with indicators such as cfg for configuration, chk for check, and so on, in the name to help you organize the plays properly. You can use similar tagging for the Plays you create.

You can also duplicate or delete a Play by clicking on the icons provided.



Maintenance:

- router_chk_bgp_neighbor_state — Name: Check BGP neighbor state
- router_chk_interface_mdt — Name: Check router interface Line State using ...
- router_cfg_interface_state_xe — Name: Change interface state to up/down on a I...

Play Schemas, Maintenance:

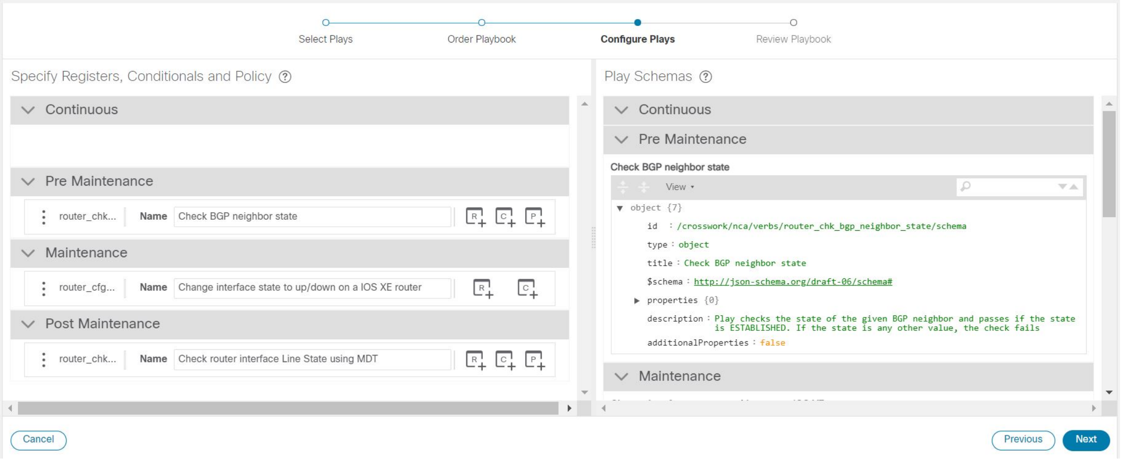
Check BGP neighbor state

Check router interface Line State using MDT

Change interface state to up/down on a IOS XE router

Click **Next**.

Step 4 The **Configure Plays** window opens displaying the Plays in each execution phase, and the Play schemas.



Pre Maintenance: router_chk... Name: Check BGP neighbor state

Maintenance: router_cfg... Name: Change interface state to up/down on a IOS XE router

Post Maintenance: router_chk... Name: Check router interface Line State using MDT

Check BGP neighbor state

```
▼ object {7}
    id  : /crosswork/nca/verbs/router_chk_bgp_neighbor_state/schema
    type : object
    title : Check BGP neighbor state
    $schema : http://json-schema.org/draft-06/schema#
  ▶ properties {0}
    description : Play checks the state of the given BGP neighbor and passes if the state
                  is ESTABLISHED. If the state is any other value, the check fails
    additionalProperties : false
```

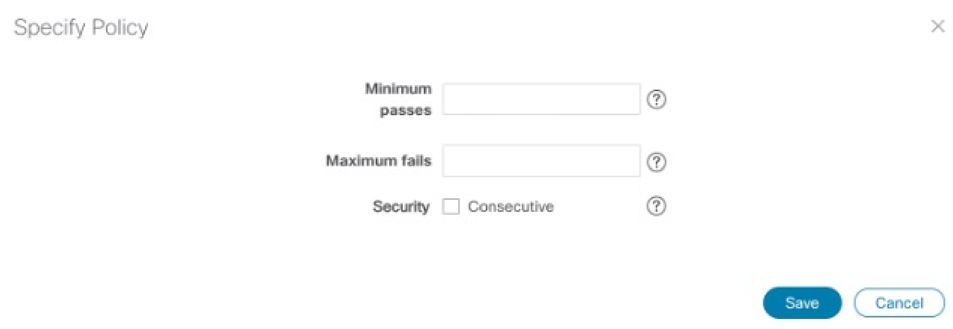
You can perform the following:

- Click P+ to specify policy for a Play. In the **Specify Policy** dialog box, specify relevant values for the fields provided.

  Click ? for more information about each field. Click **Save** to save your policy values.

Note Policies are applicable to Check Plays.

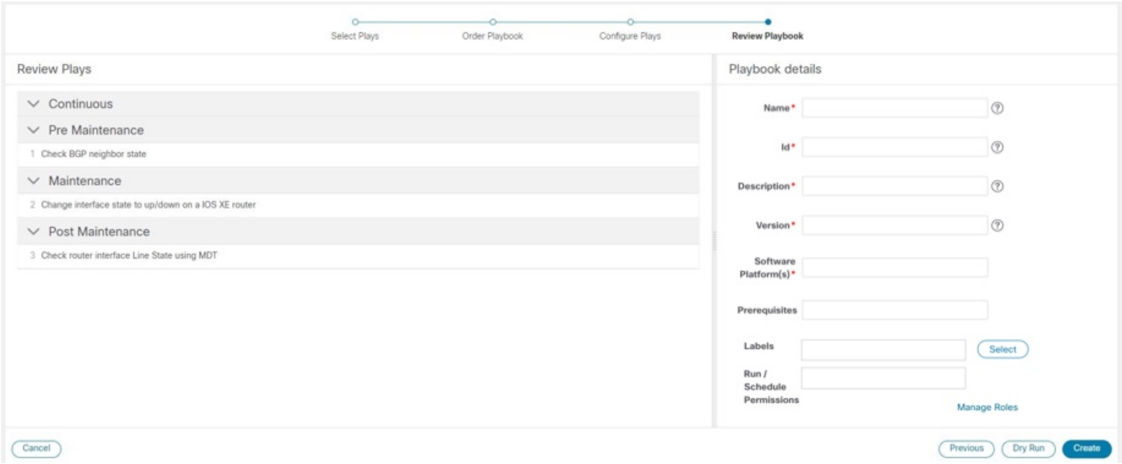
Figure 8: Specify Policy for Check Play



- Click C+ to apply a condition to a Play. Execution of the play proceeds only if the condition is met. In the **Specify Conditionals** dialog box, click **Add Condition** to add a condition. Click **Save** to save your conditional values.
- Click R+ to specify a register for a Play. Specifying registers allows you to use the output of a previous Play as the input for another Play. Click **Save** to save your registers.
- (Optional) Rename the Plays if you want them to be displayed with different names during the Playbook execution.

Click **Next** to continue.

Step 5 In the **Review Playbook** window, review the Plays in your Playbook. Enter relevant values for the **Playbook details** fields. You can click ? for more information about each field.



Review Plays

- Continuous
- Pre Maintenance
  1 Check BGP neighbor state
- Maintenance
  2 Change interface state to up/down on a IOS XE router
- Post Maintenance
  3 Check router interface Line State using MDT

Note For the **Software Platform(s)** field, make sure to use the exact software type name as it is mentioned in **Device Management** > **Network Devices** > **Software Type** column.

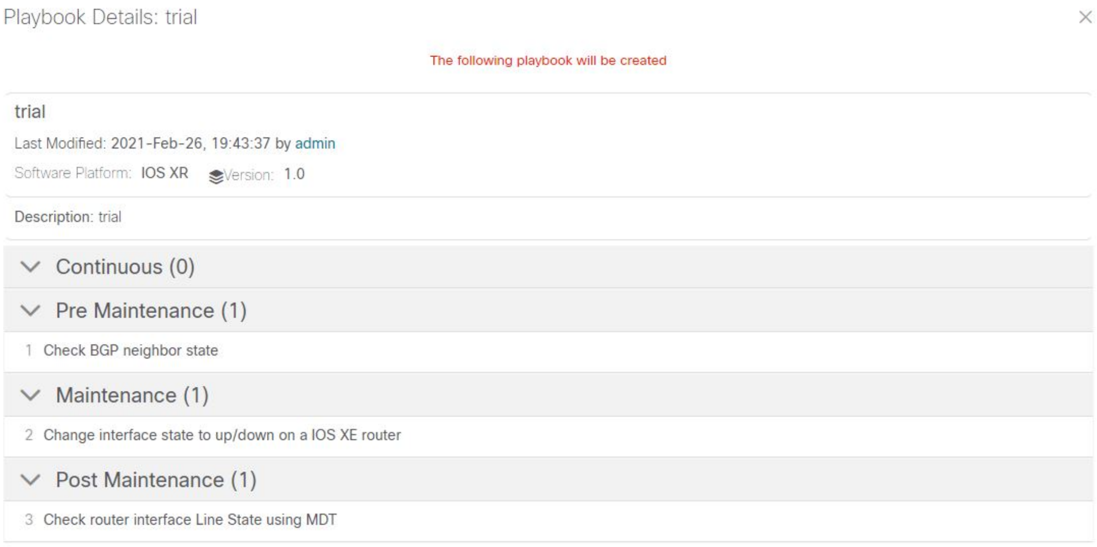
Step 6 (Optional) Click **Select** and perform one of the following, as applicable, to set the **Labels**:

- Select the applicable label and click **Done**.
- Click **Create**, enter relevant values for **Label** and **Roles**, and click **Save**. Select the new label and click **Done**.

Note The labels determine which user or roles can run which Playbooks.

For more information on assigning Playbooks to specific roles, see Assign Playbooks to Specific Roles, on page 42.

Step 7 (Optional) After you enter the relevant details, click **Dry Run** to validate the parameters. A dialog box opens displaying the Playbook Details.



Playbook Details: trial

The following playbook will be created

trial

Last Modified: 2021-Feb-26, 19:43:37 by admin

Software Platform: IOS XR Version: 1.0

Description: trial

Continuous (0)

Pre Maintenance (1)

1 Check BGP neighbor state

Maintenance (1)

2 Change interface state to up/down on a IOS XE router

Post Maintenance (1)

3 Check router interface Line State using MDT

Note Dry run does not commit the changes but just provides a platform to validate whether the Playbook would work with the parameters you entered.

Step 8 Click **Previous** to navigate back to a step to make changes as necessary to get the Playbook to function properly.

Step 9 Click **Create** to create the Playbook.

The **Playbook List** window opens displaying your new custom Playbook in the list.

Create a Custom Playbook using API

This section explains the steps to create a custom playbook using APIs. For more information, see "Custom Playbooks" tutorial in the Change Automation Developer Guide on Cisco DevNet.

Note A playbook containing a custom play can be created either through the UI (see Create a Custom Playbook Through the UI, on page 37) or using the API.

A playbook consisting of one or more custom plays are expected to have a *dataspec* value for the custom play in the playbook file. The *dataspec* value is generated when the custom playbook is created using the API in this procedure. You cannot create the same custom playbook using the import option (API: **/v1/mops/import**), as it does not add the *dataspec* value for the custom play.

Step 1 Ensure that the plays (stock or custom) you need for the playbook are created beforehand.

You can create a custom play either through the UI (see Create a Custom Play using Templates, on page 31) or using API (use the API call **//crosswork_ip:30603/crosswork/nca/v1/plays/device/config**).

Note If you are importing plays that share the same name with existing plays, then the error "`play validation failed, custom play already present`" will be displayed, to prevent the existing plays being overwritten.

Step 2 Create the playbook using the following API:

API call: **//crosswork_ip:30603/crosswork/nca/v1/mops**

Export Playbooks

You can export any Playbook as a gzipped tar archive. This includes any Cisco-supplied Playbook, as well as custom Playbooks that you or another party have authored and have imported into Cisco Crosswork Change Automation.

The exported archive contains only the user-customizable files that are listed in Playbook Components and Files, on page 36. The archive contains one or more `.pb` files (for example: `router_config_bgp_rd.pb` for the Playbook code), which are parsed and processed at the back end.

You can edit the exported files as needed, following the guidelines in the "Custom Playbooks" tutorial in the Change Automation Developer Guide on Cisco DevNet. You can then import them as explained in Import Playbooks, on page 41.

Your user ID must have Change Automation read permission to export Playbooks, and write permissions to import new or modified playbooks..

Step 1 From the main menu, choose **Network Automation** > **Playbook List**.

Step 2 (Optional) In the **Playbook List** window, filter the table as needed.

Step 3 Check the check boxes for the Playbooks you want to export. Check the check box at the top of the column to select all of the Playbooks for export.

Step 4 Click ⇨. Your browser will prompt you to select a path and the file name to use when saving the gzipped tar archive. Follow the prompts to save the file.

Import Playbooks

You can import any custom Playbook, provided it meets the following requirements:

- The Playbook files must be packaged as a gzipped tar archive.
- The archive must contain a `.pb` file, at minimum.
- The archive file must have a unique name.

The individual files included in the archive must meet the additional validation requirements described in the "Custom Playbooks" tutorial in the Change Automation Developer Guide on Cisco DevNet.

Note While you cannot overwrite a Cisco-supplied Playbook, you *can* overwrite a custom Playbook. The system will warn you when you are about to overwrite a custom Playbook, but will not prevent you from doing so. Take precautions to ensure that you do not overwrite your custom Playbooks accidentally.

You cannot re-import an exported Cisco-supplied Playbook with the same name as the original.

Before you begin

A user must have the write access to import Playbooks. For more information about granting read-writer role access to a user, see *Assign proper level of access to other users* in Configure Change Automation Settings, on page 26.

Step 1 From the main menu, choose **Network Automation** > **Playbook List**.

Step 2 Click ⇦. Your browser will prompt you to browse to and select the gzipped archive file containing the Playbooks you want to import.

Make sure there is no existing Playbook with the same name as the Playbook you intend to import, unless it is your intent to overwrite the existing Playbook.

If you are creating an improved version of a Playbook, it is recommend to use a version number or other indicator to make sure that the name is unique and does not overwrite the original Playbook until the replacement is completely tested.

Step 3 Follow the prompts to import the archive file.

Delete Custom Playbooks

You can delete user-defined Playbooks only. You cannot delete a Cisco-supplied Playbook.

Your user ID must have Change Automation delete permission to delete Playbooks.

Step 1 From the main menu, choose **Network Automation** > **Playbooks List**.

Step 2 In the **Playbooks List** window, select the custom Playbook that you want to delete.

Step 3 Click 🗑 icon.

Step 4 When prompted, click **Delete** again to confirm.

Assign Playbooks to Specific Roles

This section gives the procedure to assign Playbook labels to specific roles for them to run and import the Playbooks with that particular label. Admin users can enable other users to run Playbooks with a specific label.

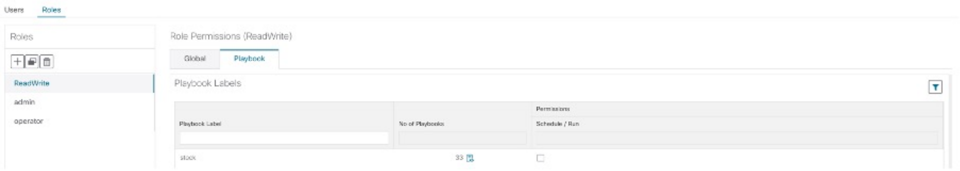
Before you begin

If required, create a new user to whom you would want to assign the Playbook. For more information, see Section: *Create User Roles* in the *Cisco Crosswork Infrastructure 4.3 and Applications Administration Guide*.

Step 1 Go to **Administration** > **Users and Roles** > **Roles** > **Playbook**.

Step 2 Under **Roles** pane, select the role to whom you would want to assign the Playbook labels.

Step 3 Enable **Permissions** check boxes for the **Playbook Label**(s) you would want to assign.



Playbook Label	No of Playbooks	Permissions
		Schedule / Run
stock	33	□

About Running Playbooks

You must have the permission to run the Playbooks with a particular Playbook label. For more information on assigning Playbooks to specific roles, see Assign Playbooks to Specific Roles, on page 42.

Running any Playbook consists of five steps:

1. Select the **Playbook** you want to run (see View the Playbook List, on page 30).

2. Select the **device or devices** that you want to run it on.

3. Enter the appropriate run-time **parameters** that you want the Playbook to apply.

4. Select the **execution mode** that you want to use:

   a. Perform a Dry Run of a Playbook, on page 44, where you can see what the Playbook does before you commit to make changes to the network.

   b. Run Playbooks In Single Stepping Mode, on page 46, so you have a chance to pause after each Playbook check or action, and roll back changes you did not intend.

   c. Run Playbooks In Continuous Mode, on page 49 and apply the changes immediately.

   While selecting the execution mode, you can also choose to:

   - Schedule Playbook Runs, on page 52 for another calendar date or time.

   - **Collect syslogs** during and after the run. Syslog collection is available only when running the Playbook in single-stepping or continuous execution mode, and only if you have already configured a syslog storage provider.

   - Specify a **Failure Policy**, where you decide what the system should do in case a failure occurs at any time during the Playbook run.

5. **Confirm** your settings and run the Playbook in the execution mode you selected.

Depending on their complexity and on network factors, some Playbooks may take a lot of time to run. At any time during and after completion of a run, you can view the run details and status. If the Playbook is still running, you can also choose to cancel it. For details, see View or Abort Playbook Jobs, on page 53.

Playbook Execution Order

When it is running, every Playbook conducts checks and configuration changes in four phases, which correspond to sections of the Playbook code (identified using the tags discussed in Playbook Components and Files, on page 36):

1. **Pre-Maintenance**—This phase of the Playbook includes non-disruptive checks and any other operations on the device that prepare it for potentially traffic-impacting changes. For example:
    - Take snapshots of various routing protocol states.
    - Take snapshots of memory, CPU, and system health parameters.
    - Validate the capacity (storage, memory) on active and standby routers for the new software patch upgrade.
2. **Maintenance**—This phase of the Playbook includes any task that may disrupt traffic flowing through the router or impact neighboring routers. For example:
    - Cost out the router and wait until traffic drains out completely.
    - Verify that the redundant router is healthy and carrying traffic.
    - Perform the upgrade procedure on the device.
    - Reconfigure the device(s) to support a new configuration or feature.
3. **Post-Maintenance**—This phase of the Playbook includes verification tasks to perform on the router after any disruptive operation. For example:
    - Verify that the current state matches the desired state.
    - Cost in the router and wait for traffic to return to normal levels.
4. **Continuous**—In addition to the three serial phases already described, Change Automation can also run check tasks that span the entire duration of Playbook execution. These tasks check the state of the router while the Playbook is being deployed, and cancel the Playbook execution if any catastrophic or undesirable state change occurs. The checks in the Playbook may also monitor a neighboring router to guarantee that there are no second-order failures in the network while the changes are being deployed.

Perform a Dry Run of a Playbook

A dry run lets you view configuration changes that the Playbook will send to the device, without performing the actual commit of the changes, as you would with a run in the single-stepping or continuous execution modes.

It is a best practice to perform a dry run and verify the configuration changes before you deploy those changes to the router. If the dry run fails, you may want to debug its parameter values using another dry run. You can also debug by performing a single-stepping run, which will allow you to abort and rollback changes after one or more of the plays, instead of only at the end, as part of a continuous run's Failure Policy.

Note that dry run mode is intended for use only with Playbooks that perform actual device configuration changes via Cisco NSO. See the "Playbooks" and "Plays" references in the Change Automation Developer Guide on Cisco Devnet for details on Playbooks that do not support dry run mode. These will include, for example, Node state snapshot, Install optional package or SMU, and Uninstall optional package or SMU.

Step 1 From the main menu, choose **Network Automation** > **Run Playbook**.

Step 2 In the **Select Playbook** list on the left, click on the Playbook you want to dry run. On the right, the window displays the Playbook name, hardware and software compatibility information, and descriptions for all the plays in the selected Playbook.

Step 3 Click **Next**. The **Select Devices** window appears. Using this window:

- You can toggle between the table view and topology map view by clicking and selecting the relevant option on the drop-down button on the upper left corner of the window. Choose **Select Devices From List** or **Select Devices From Map** to select the table view or topology map view respectively. By default, the table view is displayed.

- With the topology map view displayed, you can toggle between the map's geographical and logical views by clicking on the 🌐 or the 🖧. You can also zoom, display bandwidth utilization, and change logical view layouts as you do with the topology map you see when you select **Topology** from the main menu.

- You can select the devices using **Static** or **Dynamic using Tags** device selection options. **Static** selection allows you to select devices from the list using quick and advanced filters and filter by tags on the left. **Dynamic using Tags** selection targets you to select the relevant tag intead of devices from the table on the left side, and all devices associated with the relevant tag are selected. Hover the mouse pointer over the ? icon next to the options for more information. You can also view the selection criteria such as number of devices required for the selected playbook.

- In **Static** selection mode, you can check the **Allow Bulk Jobs** check box to select multple devices and run the selected playbook on them at the simultaneously. Based on your selection, the system creates a static group of multiple jobs. Hover the mouse pointer over the ? icon next to the check box for more information. There is no limitation on the number of devices you can select for a bulk job.

  Note **Allow Bulk Jobs** option is enabled for playbooks that can be executed on a single device.

Step 4 The **Select Devices** window will prompt you to select one or more of the devices shown (depending on the Playbook). Click on the devices you want to select, then click **Next**. The **Parameters** window appears.

Step 5 In the fields provided in the **Parameters** window, enter the Playbook parameter values to use for this dry run.

With the **Parameters** window displayed, you can also:

- Click **JSON** to enter the parameter values in JSON format. A popup text window displays the full list of JSON parameters, with empty values in quotes. Edit the values and, when you are finished, click **Save**.

- Click ⭱ to upload a JSON file with the parameter values you want. You will be prompted to navigate to the JSON parameters file you have previously prepared (or downloaded from a previous Playbook run) and then upload it as appropriate for your browser and operating system.

- Click **+ Add** to add additional instances of a particular parameter, if required for the Playbook you are running. Click **X Remove** to delete instances added in this way.

- Click ⌫ to clear all the parameter values entered so far.

Step 6 With the parameter values set, click **Next**. The **Execution Policy** window appears.

Step 7 Choose **Dry Run** and click **Next**. The **Review your Job** window appears, displaying a summary of all of your choices: playbook, devices, parameters, and execution policy. In this window:

- You must provide a relevant **Name** for the job.
- You can assign tags to your job. Click **New Job Tag**, provide a name and color and save your settings to create your own tag. You can also select from the list of existing job tags by clicking the corresponding checkboxes. Click **Manage Job Tags** to create, edit or delete job tags.
- You can click on any of the **Change** links in the **Review your Job** window summary to modify your choices.

Step 8 (Optional) Enter the device credentials (name and password).

Note This step is applicable only if **Credential Prompt** is enabled in the Change Automation settings. For more information, see Configure Change Automation Settings, on page 26.

Step 9 When you are ready to continue, click **Run Playbook**.

Step 10 At the confirmation prompt, click **Confirm**. The **Execution Mode** window is displayed.

Step 11 After the dry run is complete:

- Click the **Dry Run** tab and verify the configuration changes that would be pushed to the device had this not been a dry run. This tab will display a `no config change` message if no changes would have been made. Please note that this tab shows only cumulative configuration changes, not each individual change made. For example, if a Playbook configures `set-overload-bit` in one step and then unconfigures it using `no set-overload-bit` in a later step, the tab will show `no config change`.
- Click the **Events** tab to see success and failure messages for each step of the Playbook. This can help you diagnose and correct problems with individual plays and the run as a whole. For troubleshooting information, see Troubleshoot Change Automation, on page 55.
- Click the **Console** tab to see messages that are generated during the run.

As syslog collection is disabled for dry run, the **Syslog** tab will contain only a message stating that.

Step 12 (Optional) If you want to perform a single-step debugging run, or are ready to commit the changes to the device, click **Execute Now**. The **Execution Policy** window will display, with all of your parameter values from the dry run pre-filled.

Run Playbooks In Single Stepping Mode

Single-stepping execution mode is a handy way to test a custom or modified Playbook, or diagnose problems with a pre-packaged Playbook that is not giving you the results you want. Unlike a dry run, a single-stepping execution commits configuration changes to the device as the Playbook runs. However, you can set breakpoints on or pauses after any Maintenance or Post-Maintenance action in the Playbook. Please note that, while you can set breakpoints on Pre-Maintenance actions, doing so will have no effect, and these actions will not pause.

Whenever the Playbook hits a breakpoint, it will stop, and will not continue until you issue the command to proceed. At each pause, you can also choose to abort the entire run and roll back all changes made, or rollback to any previous play.

Step 1 From the main menu, choose **Network Automation** > **Run Playbook**.

Step 2 In the **Select Playbook** list on the left, click on the Playbook you want to run. On the right, the window displays the Playbook name, hardware and software compatibility information, and descriptions for all the plays in the selected Playbook.

Step 3 Click **Next**. The **Select Devices** window appears. Using this window:

- You can toggle between the table view and topology map view by clicking and selecting the relevant option on the drop-down button on the upper left corner of the window. Choose **Select Devices From List** or **Select Devices From Map** to select the table view or topology map view respectively. By default, the table view is displayed.
- With the topology map view displayed, you can toggle between the map's geographical and logical views by clicking on the 🌐 or the 品. You can also zoom, display bandwidth utilization, and change logical view layouts as you do with the topology map you see when you select **Topology** from the main menu.
- You can select the devices using **Static** or **Dynamic using Tags** device selection options. **Static** selection allows you to select devices from the list using quick and advanced filters and filter by tags on the left. **Dynamic using Tags** selection allows you to select the relevant tag from the table on the left side, and all devices associated with the relevant tag are selected. Hover the mouse pointer over the ? icon next to the options for more information. You can also view the selection criteria such as number of devices required for the selected playbook.
- In **Static** selection mode, you can check the **Allow Bulk Jobs** check box to select multple devices and run the selected playbook on them at the simultaneously. Based on your selection, the system creates a static group of multiple jobs. Hover the mouse pointer over the ? icon next to the check box for more information. There is no limitation on the number of devices you can select for a bulk job.

  Note **Allow Bulk Jobs** option is enabled for playbooks that can be executed on a single device.

Step 4 The **Select Devices** window will prompt you to select one or more of the devices shown (depending on the Playbook). Click on the devices you want. Click **Next**.

Step 5 Click **Next**. The **Parameters** window appears.

Step 6 In the fields provided in the **Parameters** window, enter the Playbook parameter values to use for this run.

With the **Parameters** window displayed, you can also:

- Click **JSON** to enter the parameter values in JSON format. A popup text window displays the full list of JSON parameters, with empty values in quotes. Edit the values and, when you are finished, click **Save**.
- Click ⤒ to upload a JSON file with the parameter values you want. You will be prompted to navigate to the JSON parameters file you have previously prepared (or downloaded from a previous Playbook run) and then upload it as appropriate for your browser and operating system.
- Click **+ Add** to add additional instances of a particular parameter, if required for the Playbook you are running. Click **X Remove** to delete instances added in this way.
- Click ◈ to clear all the parameter values entered so far.

Step 7 With the parameter values set, click **Next**. The **Execution Policy** window appears.

Step 8 Choose **Single Stepping**. The **Execution Policy** window displays additional features to customize the job:

- Under **Collect Syslogs**, click **Yes** if you want syslogs to be collected during and immediately after the run, **No** if you do not. **Yes** is the default selection only if you have a syslog provider configured.
- From the **Failure Policy** dropdown, select:

    - **Abort** to abort the entire run, without rolling back any changes, if a failure occurs at any point. This is the default. Any configuration changes made up to the point of failure will not be rolled back.
    - **Pause** to pause the run and allow you to decide how to handle the failure. This pause will be in addition to any breakpoints you set using the **Single stepping breakpoints** dropdown.
    - **Complete Roll Back** to abort the entire run and roll back all configuration changes made.
- In the **Schedule** area, uncheck the default **Run Now** selection to schedule the job for a later time. See Schedule Playbook Runs, on page 52 for help on using the **Schedule** area features

Step 9 From the **Single stepping breakpoints** dropdown, select either

- **Every step** to pause automatically after every step in the Playbook.
- **Customize** to select the steps where you want the Playbook to pause.

If you select **Customize**, the **Customize Breakpoints** popup displays a list of all the plays in the Playbook, with a ⏸at the step between each play. Click the ⏸ at each step where you want to set a breakpoint. When you are finished, click **Done**.

Step 10 Click **Next**. The **Review your Job** window appears, displaying a summary of all of your choices: playbook, devices, parameters, and execution policy. In this window:

- You must provide a relevant **Name** for the job.
- You can assign tags to your job. Click **New Job Tag**, provide a name and color and save your settings to create your own tag. You can also select from the list of existing job tags by clicking the corresponding checkboxes. Click **Manage Job Tags** to create, edit or delete job tags.
- You can click on any of the **Change** links in the **Review your Job** window summary to modify your choices.

Step 11 (Optional) Enter the device credentials (name and password).

Note This step is applicable only if **Credential Prompt** is enabled in the Change Automation settings. For more information, see Configure Change Automation Settings, on page 26.

Step 12 When you are ready to continue, click **Run Playbook**.

Step 13 At the confirmation prompt, click **Confirm**. The **Automation Job History** window is displayed, with the details of the current job displayed on the right side. The job details include information such as job status, job set tags, title of selected playbook, execution parameters and policy, last updated date and update comments (if any). Click the ℹ icon next to the detail to view more information.

Step 14 While the run is executing, the blue **Running** tile at the top of the window will change to **Paused** for each step at which you have set a breakpoint. Your choices at each pause will be displayed as buttons below the blue tiles:

- Click **Resume** to resume running from this point, with no changes. The **Resume** request includes the runtime parameters from the previous step; you can edit these, as needed, later.
- Click **Roll Back** to roll back any changes made so far. You can choose how far to rollback:
    - Click **Complete Roll Back** to roll back all changes to the start of the Playbook run. Once you have rolled back to the start, you can choose to **Resume** from that point, **Abort** the run entirely, or **Edit runtime parameters** of the run.
    - Click **Select Roll Back Point** to roll back changes to the step you select. All the previous steps will then have a roll back point icon displayed next to them: ↶. Click the ↶ for the step to which you want to roll back.

Once you have selected the step, you can choose to **Resume** from that step, **Roll Back** further, **Abort** the run entirely, or **Edit runtime parameters**.

- Click **Abort** to abort the run entirely. No changes made will be rolled back.
- Click **Edit runtime parameters** to edit the parameters the run is using. You edit using a popup version of the **Parameters** window, just as you did in step 6. The parameters exposed for editing when resuming are specific to the task being resumed, which means that they are not the same global parameters you defined in step 6. Most of the time, they are a subset of the global parameters. When you are finished, click **Apply**. You can then choose to **Resume** execution with the changed parameters.

Step 15 While the run is executing, you can also use the following features of the progress window:

- View the execution status of each play in the Playbook in the **Maintenance** play list at the left side of the window. Plays that fail are indicated with a red icon; plays that succeed are indicated with a green icon.
- See reminders of your choices in the blue **Playbook** and **Devices** tiles at the top of the window.
- See the current status of the run in the blue **Running** tile at the top of the window.
- Click **View** in the **Parameters** tile to view the run's parameters. While viewing the parameters, you can click **Download Parameters** to save them in a JSON file. You will be prompted to name and save the file as appropriate for your browser and operating system.
- Use the network topology in the map at the right side of the window to view the device and its connections to the rest of your network.

Step 16 After the run is complete:

- Click the **Events** tab to see success and failure messages for each step of the Playbook. This can help you diagnose and correct problems with individual plays and the run as a whole.
- Click the **Syslogs** tab to access syslog messages collected during and immediately after the run. If syslog collection is enabled, the tab will provide a pointer to the path on the syslog storage provider where collected syslogs are stored. If you chose not to collect syslogs, or no syslog storage provider has been configured, this tab will display a message indicating that syslog collection is disabled.
- Click the **Console** tab to see relevant commands and responses from the device consoles that took place during the run. These messages can also help with diagnostics.

Run Playbooks In Continuous Mode

Continuous execution mode is the standard way to run Playbooks. Configuration changes are committed to the device during the run, with no checks or delays except those programmed into it for system resets or other purposes. The run continues until it succeeds or fails. If it fails, you can use the run's Failure Policy to abort, rollback all changes made to the device, or pause execution at the failure point.

It is always good practice to perform a dry run and verify the configuration changes before committing to a continuous run (see Perform a Dry Run of a Playbook, on page 44). You can also run the Playbook in single-stepping mode, which will allow you to pause execution after any play you select, abort and rollback changes as needed, and even change runtime parameters in the middle of the run (see Run Playbooks In Single Stepping Mode, on page 46).

Step 1 From the main menu, choose **Network Automation** > **Run Playbook**.

Step 2 In the **Select Playbook** list on the left, click on the Playbook you want to run. On the right, the window displays the Playbook name, hardware and software compatibility information, and descriptions for all the plays in the selected Playbook.

Step 3 Click **Next**. The **Select Devices** window appears. Using this window:

- You can toggle between the table view and topology map view by clicking and selecting the relevant option on the drop-down button on the upper left corner of the window. Choose **Select Devices From List** or **Select Devices From Map** to select the table view or topology map view respectively. By default, the table view is displayed.
- With the topology map view displayed, you can toggle between the map's geographical and logical views by clicking on the 🌐 or the 🖧. You can also zoom, display bandwidth utilization, and change logical view layouts as you do with the topology map you see when you select **Topology** from the main menu.
- You can select the devices using **Static** or **Dynamic using Tags** device selection options. **Static** selection allows you to select devices from the list using quick and advanced filters and filter by tags on the left. **Dynamic using Tags** selection allows you to select the relevant tag from the table on the left side, and all devices associated with the relevant tag are selected. Hover the mouse pointer over the ? icon next to the options for more information. You can also view the selection criteria such as number of devices required for the selected playbook.
- In **Static** selection mode, you can check the **Allow Bulk Jobs** check box to select multple devices and run the selected playbook on them at the simultaneously. Based on your selection, the system creates a static group of multiple jobs. Hover the mouse pointer over the ? icon next to the check box for more information. There is no limitation on the number of devices you can select for a bulk job.

  Note **Allow Bulk Jobs** option is enabled for playbooks that can be executed on a single device.

Step 4 The **Select Devices** window will prompt you to select one or more of the devices shown (depending on the Playbook). Click on the devices you want to select them, then click **Next**. The **Parameters** window appears.

Step 5 In the fields provided in the **Parameters** window, enter the Playbook parameter values to use for this dry run.

With the **Parameters** window displayed, you can also:

- Click **JSON** to enter the parameter values in JSON format. A popup text window displays the full list of JSON parameters, with empty values in quotes. Edit the values and, when you are finished, click **Save**.
- Click ⇡ to upload a JSON file with the parameter values you want. You will be prompted to navigate to the JSON parameters file you have previously prepared (or downloaded from a previous Playbook run) and then upload it as appropriate for your browser and operating system.
- Click **+ Add** to add additional instances of a particular parameter, if required for the Playbook you are running. Click **X Remove** to delete instances added in this way.
- Click ◆ to clear all the parameter values entered so far.

Step 6 With the parameter values set, click **Next**. The **Execution Policy** window appears.

Step 7 Choose **Continuous**. The **Execution Policy** window displays additional features to customize the job:

- Under **Collect Syslogs**, click **Yes** if you want syslogs to be collected during and immediately after the run, **No** if you do not. **Yes** is the default selection only if you have a syslog provider configured.

- From the **Failure Policy** dropdown, select:
  - **Abort** to abort the entire run, without rolling back any changes, if a failure occurs at any point. This is the default. Any configuration changes made up to the point of failure will not be rolled back.
  - **Pause** to pause the run and allow you to decide how to handle the failure.
  - **Complete Roll Back** to abort the entire run and roll back all configuration changes made.
- In the **Schedule** area, uncheck the default **Run Now** selection to schedule the job for a later time. See Schedule Playbook Runs, on page 52 for help on using the **Schedule** area features

Step 8 Click **Next**. The **Review your Job** window appears, displaying a summary of all of your choices: playbook, devices, parameters, and execution policy. In this window:

- You must provide a relevant **Name** for the job.
- You can assign tags to your job. Click **New Job Tag**, provide a name and color and save your settings to create your own tag. You can also select from the list of existing job tags by clicking the corresponding checkboxes. Click **Manage Job Tags** to create, edit or delete job tags.
- You can click on any of the **Change** links in the **Review your Job** window summary to modify your choices.

Step 9 (Optional) Enter the device credentials (name and password).

Note This step is applicable only if **Credential Prompt** is enabled in the Change Automation settings. For more information, see Configure Change Automation Settings, on page 26.

Step 10 When you are ready to continue, click **Run Playbook**.

Step 11 At the confirmation prompt, click **Confirm**. The **Automation Job History** window is displayed, with the details of the current job displayed on the right side. The job details include information such as job status, job set tags, title of selected playbook, execution parameters and policy, last updated date and update comments (if any). Click the ℹ icon next to the detail to view more information.

Step 12 While the run is executing, the blue **Running** tile at the top of the window will change to **Paused** if you chose a **Failure Policy** of **Pause**. Your choices will be displayed as buttons below the blue tiles:

- Click **Resume** to resume running from this point, with no changes.
- Click **Roll Back** to roll back any changes made so far.
- Click **Abort** to abort the run entirely. No changes made will be rolled back.

Step 13 While the run is executing, you can also use the following features of the progress window:

- View the execution status of each play in the Playbook in the **Maintenance** play list at the left side of the window. Plays that fail are indicated with a red icon; plays that succeed are indicated with a green icon.
- See reminders of your choices in the blue **Playbook** and **Devices** tiles at the top of the window.
- See the current status of the run in the blue **Running** tile at the top of the window.
- Click **View** in the **Parameters** tile to view the run's parameters. While viewing the parameters, you can click **Download Parameters** to save them in a JSON file. You will be prompted to name and save the file as appropriate for your browser and operating system.
- Use the network topology in the map at the right side of the window to view the device and its connections to the rest of your network.

Step 14 After the run is complete:

- Click the **Events** tab to see success and failure messages for each step of the Playbook. This can help you diagnose and correct problems with individual plays and the run as a whole.
- Click the **Syslogs** tab to access syslog messages collected during and immediately after the run. If syslog collection is enabled, the tab will provide a pointer to the path on the syslog storage provider where collected syslogs are stored. If you chose not to collect syslogs, or no syslog storage provider has been configured, this tab will display a message indicating that syslog collection is disabled.
- Click the **Console** tab to see relevant commands and responses from the device consoles that took place during the run. These messages can also help with diagnostics.

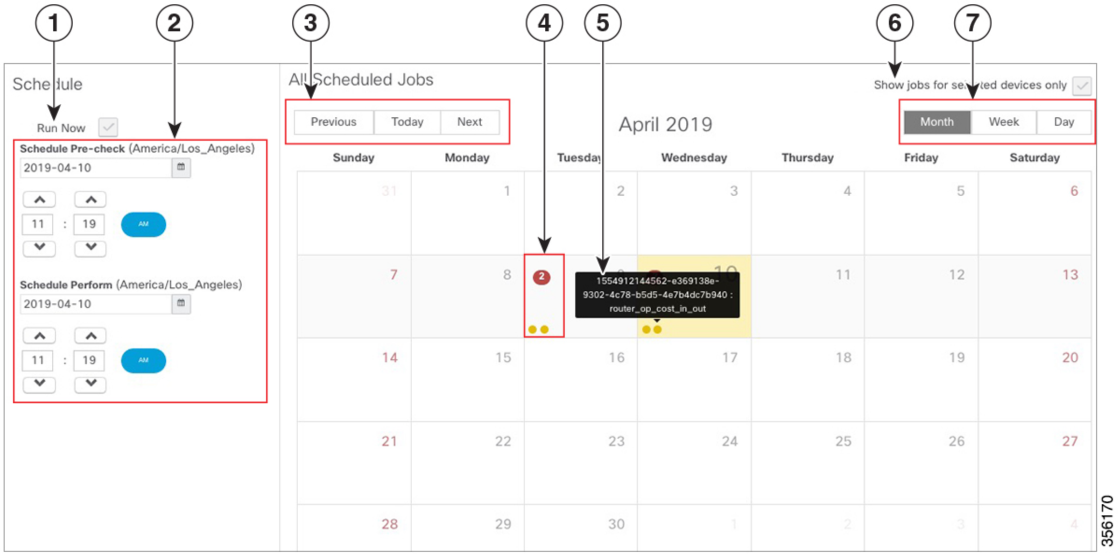
Schedule Playbook Runs

The Change Automation application's **Execution Mode** window allows you to schedule future Playbook runs as jobs, and view all the jobs that have been scheduled. Use the **Schedule** area on the left to schedule a job. Use the **All Scheduled Jobs** area on the right to view scheduled jobs on the calendar.

Note **Playbook Job Scheduling** is only available if it was enabled when Change Automation was installed and initially configured. For more information, see Configure Change Automation Settings, on page 26. To change this setting, you must uninstall and then reinstall Change Automation.

The **Execution Mode** window's scheduling features are only displayed when you have chosen to run a Playbook in continuous or single-stepping mode. You cannot schedule a dry run of a Playbook.

Figure 9: Execution Mode Scheduling Features



Run Now ☑

Schedule Pre-check (America/Los_Angeles) 2019-04-10 11 : 19 AM

Schedule Perform (America/Los_Angeles) 2019-04-10 11 : 19 AM

Show jobs for selected devices only ☑

April 2019

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4

1554912144562-e369138e-9302-4c78-b5d5-4e7b4dc7b940 : router_op_cost_in_out

Item	Description
1	**Run Now**: Running Playbooks immediately is the default for continuous and single-stepping execution modes. To schedule a run for a future time and date, you must uncheck this box.
2	**Schedule Selectors**: Use these fields to select the future time and date when the Playbook runs. Although it is the default for the Pre-Maintenance and Maintenance phases of a scheduled Playbook to start at the same time, you can use the upper **Schedule Pre-check** and lower **Schedule Perform** fields to schedule the start of Pre-Maintenance and the start of Maintenance independently. The **Schedule Perform** time must always be greater than or equal to the **Schedule Pre-check** time.
3	**Previous/Today/Next Selectors**: Use these three selectors with the **Month/Week/Day** selectors to focus the calendar's display of scheduled jobs on the time range in which you are interested. For example: To show only those jobs scheduled for next week, click **Next** and **Week**.
4	**Job Icons**: Red, numbered icons in the squares representing each calendar date show how many jobs are scheduled for that date. Yellow circle icons represent each scheduled job.
5	**Job Details pop-up**: Hover your mouse cursor over a yellow circle icon to see the details for the scheduled job represented by that icon. The pop-up shows the execution ID of the job and the name of the Playbook to be run.
6	**Show jobs for selected devices only**: Check this box to restrict the calendar display to only those jobs that are scheduled to run on the devices you have already selected. This is a handy way to see if the schedule you plan for your Playbook run conflicts with other scheduled jobs on the same devices.
7	**Month/Week/Day Selectors**: Use these three selectors with the **Previous/Today/Next** selectors to focus the calendar's display of scheduled jobs on the time range in which you are interested. For example: To show only those jobs scheduled for last month, click **Last** and **Month**.

Note Crosswork Change Automation Playbooks have a **`mop_timeout`** parameter, which is a user specified input that is needed to schedule any Playbook.

If you are scheduling a Playbook with **Failure Policy** set to **`Complete Roll Back`**, first dry run the Play and note the time that is taken. Then add a buffer time (for example, say 10 minutes) to the time taken during the dry run. After that, double the time value and enter it to the **`mop_timeout`** parameter as it can possibly take as much time to roll back the Playbook as it takes to run it until the last step. Without sufficient **`mop_timeout`**, the Playbook can end up in an incomplete state (in between transitions) if the timeout gets triggered while rollback is in progress. If this happens, you have to manually revert the changes done or you have to create a Playbook with the changes that you want to revert.

View or Abort Playbook Jobs

The **Automation Job History** window lets you click on any individual job in the list to see that job's detailed execution progress panel, which displays the name of the Playbook, its plays, the devices it ran on, the parameters used, and all event, syslog, console and other messages. These details are useful when diagnosing failures.

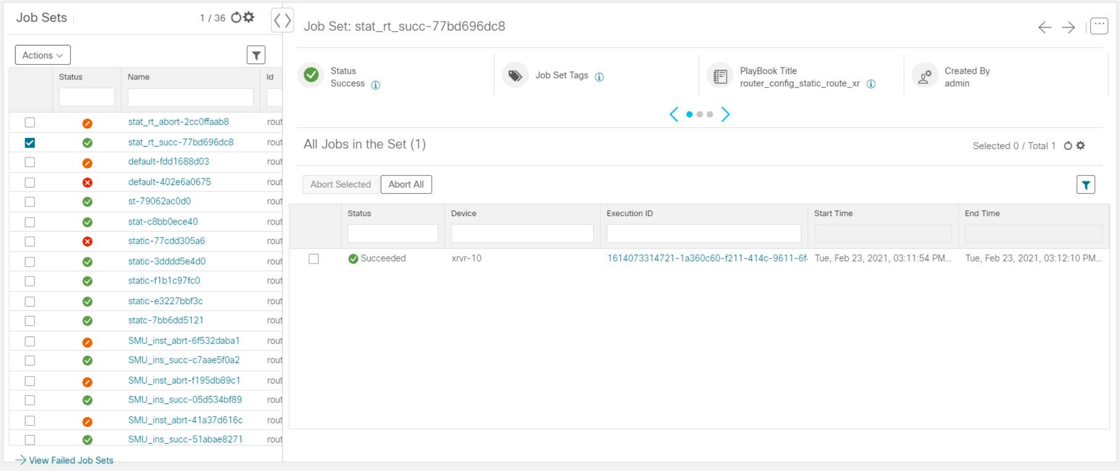
The **Automation Job History** window also allows you to abort *running* jobs.

Note You can also navigate to **Automation Job History** window from the**Jobs** panel in the Change Automation **Dashboard**.

Before you begin

A user must have the permission for specific Playbook label to run or abort a Playbook. For more information on assigning Playbooks to specific roles, see Assign Playbooks to Specific Roles, on page 42.

Step 1 From the main menu, select **Network Automation** > **Automation Job History**. The **Automation Job History** window is displayed with a list of Job Sets.



Job Sets 1 / 36

Actions

	Status	Name	Id
□	⊘	stat_rt_abort-2cc0ffaab8	rout
☑	✓	stat_rt_succ-77bd696dc8	rout
□	⊘	default-fdd1688d03	rout
□	✗	default-402e6a0675	rout
□	✓	st-79062ac0d0	rout
□	✓	stat-c8bb0ece40	rout
□	✗	static-77cdd305a6	rout
□	✓	static-3dddd5e4d0	rout
□	✓	static-f1b1c97fc0	rout
□	✓	static-e3227bbf3c	rout
□	✓	statc-7bb6dd5121	rout
□	⊘	SMU_inst_abrt-6f532daba1	rout
□	✓	SMU_ins_succ-c7aae5f0a2	rout
□	⊘	SMU_inst_abrt-f195db89c1	rout
□	✓	SMU_ins_succ-05d534bf89	rout
□	⊘	SMU_inst_abrt-41a37d616c	rout
□	✓	SMU_ins_succ-51abae8271	rout

→ View Failed Job Sets

Job Set: stat_rt_succ-77bd696dc8

Status Success

Job Set Tags

PlayBook Title router_config_static_route_xr

Created By admin

All Jobs in the Set (1) Selected 0 / Total 1

Abort Selected Abort All

	Status	Device	Execution ID	Start Time	End Time
□	✓ Succeeded	xrvr-10	1614073314721-1a360c60-f211-414c-9611-6f	Tue, Feb 23, 2021, 03:11:54 PM...	Tue, Feb 23, 2021, 03:12:10 PM...

The list in **Automation Job History** window is sorted by the last update time, with running or most recently executed jobs at the top. You can apply quick or advanced filters to the table as you would with columns in other table windows.

Step 2 To view information about a specific Playbook job, click the relevant job ID checkbox on the left. The job's status and execution details are displayed on the right side. Click on the ℹ icon next to each detail to get more information about the selected job set.

Step 3 You can abort a job set in running, paused or scheduled status, as follows:

- To abort a specific job, click the check box next to it and then click **Abort Selected**.
- To abort all jobs immediately, click **Abort All**.

When prompted, click **Confirm**. Jobs that are currently running, paused, or scheduled will abort once the current task has run to completion.

Troubleshoot Change Automation

The following table describes issues that you may encounter when using the Change Automation application, and their solutions or workarounds.

Table 1: Change Automation Troubleshooting

Issue	Solution
Playbook run fails with messages indicating that Cisco Network Services Orchestrator (Cisco NSO) and the target device are out of sync or otherwise out of communication. Message text varies, but may include "device out of sync", "NC client timeout", and other text indicating that there are connectivity or sync issues between Cisco NSO and the device.	Ensure that the Playbook does not include a sync operation. Get the device and Cisco NSO back in sync and then re-run the Playbook. Alternatively, you can create a new Playbook that includes a sync operation to avoid future problems.

"Failed to end NSO transaction, 500:fatal:YClientError: Failed to send RPC:" error is displayed while running the playbook.	Include the below settings in the Cisco NSO configuration file (`ncs.conf`):
	`<ssh>`
	`<client-alive-interval>infinity</client-alive-interval>`
	`<client-alive-count-max>5</client-alive-count-max>`
	`</ssh>`
	Note This configuration could increase the load on Cisco NSO. So, it is better to do this only when necessary.

Playbook aborted due to failure in locking the device nodes.	In the Devices window, select the relevant devices and clear the lock by moving the device to DOWN and then UP. Go to **Administration** > **Crosswork Manager**, click the **Change Automation** tile and restart the robot-nca process. Once the protocols are reachable, you can schedule to run a new playbook.

CHAPTER 5

Monitor Network Health and KPIs

This section contains the following topics:

Health Insights Overview

Health Insights is a network health application that performs real-time key performance indicator (KPI) monitoring, analytics, alerting, and troubleshooting.

It builds dynamic detection and analytics modules that allow operators to monitor and alert network events with user-defined logic.

It also provides prebuilt KPIs that are based on model-driven and SNMP-based telemetry. The Health Insights Recommendation Engine uses data mining to analyze your network and then recommends which telemetry paths you should enable and monitor.

Important There must be an extended Cisco Crosswork Data Gateway that is configured if you plan to gather telemetry using KPIs and Health Insights.

Note For the recommendation engine to work in Health Insights, you must ensure that connectivity is established between Cisco Crosswork Health Insights and the device. Enable the NETCONF protocol on the device itself, in the device configuration in Crosswork and in the credential profile for the device in Crosswork.

Health Insights is configured to gather the link bandwidth usage data for device links. After a time period, it establishes a performance baseline for each link. If a link deviates from its baseline causing an alert to be generated, Health Insights detects it and you can then go and run the Playbook to reconfigure the network to resolve the issue.

The following high-level example gives a basic view of how Health Insights interacts with the other Cisco Crosswork Network Controller components:

1. Health Insights detects an anomaly: The optical bit error rate that you are monitoring on each of the links in your network suddenly increases.
2. Change Automation Playbooks automate remediation: Switch to the backup link immediately. Restore service. Open a ticket (manually initiated by the user). Alert the network engineer.

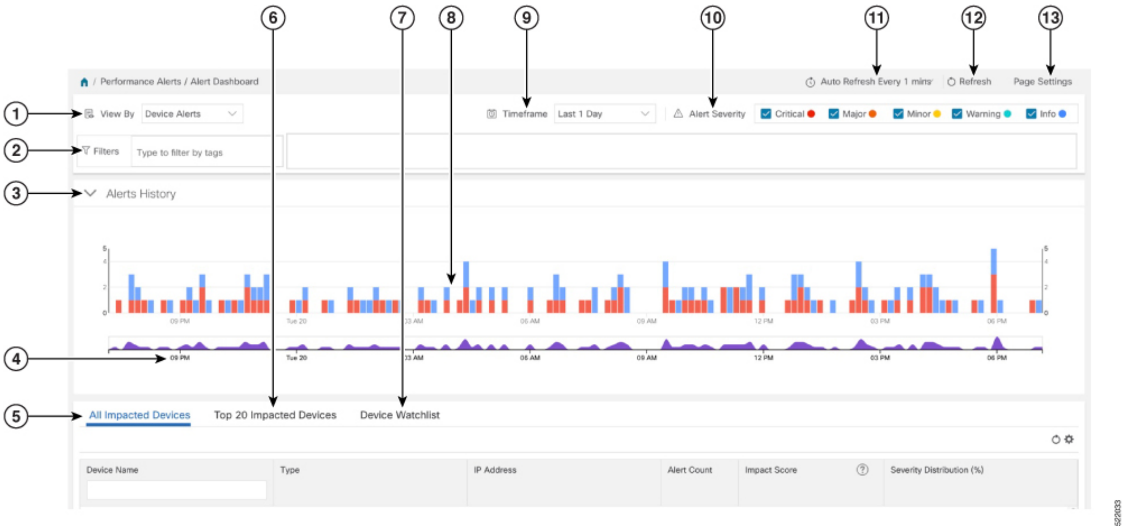
The complexity of the interaction will depend on the type of anomaly, how it is detected, and the Playbooks you choose to use to remediate it. You can orchestrate any form of network remediation using Change Automation Playbooks, helping you to close the loop on problem resolution and minimize network downtime.

Health Insights Alert Dashboard

The Health Insights alert dashboard provides device health summary information that is based on real-time network state events. The dashboard displays a network view of KPI sensors that are paired to specific device groups. Health Insights raises customizable events and alerts that are based on user-defined logic.

Note Alert dashboard displays individual KPI alerts, although the mechanism of enabling KPI on a device is done through a KPI profile.

To display the Health Insights dashboard, choose **Performance Alerts** > **Alert Dashboard** from the main menu.



View By: Device Alerts

Timeframe: Last 1 Day

Alert Severity: ☑ Critical ● ☑ Major ● ☑ Minor ● ☑ Warning ● ☑ Info ●

Auto Refresh Every 1 mins

Item	Description
1	**Device/KPI Alert Selector**: Click here to toggle between device alert and KPI alert information.

Item	Description
2	**Filters**: This field lets you filter the alert dashboard information by associated tag names. To select a tag, do one of the following: • If you know the tag that you want to use, enter it in the **Type to filter by Tags** field and then check its check box. Repeat this step to select more tags. • If you want to select a tag from the tags that are currently available: **1.** In the **Type to filter by Tags** field, type any character to open the results list. **2.** Click the **View All Tags** link at the bottom of the list. **3.** Check the check box for each tag that you want to use and then click **Apply Filters**. **4.** Delete the character that you typed in Step 1 to clear the results list. Tag filters you create are not saved. If you open another window and then return to the alert dashboard, you need to re-create tag filters.
3	**Alerts History**: This dashlet shows the total number of device alerts or KPI alerts that have been raised during the chosen time period, with detailed time lines showing both individual sets of alerts and the overall alert trend.
4	**Alerts Trend Line**: This line shows the overall trend in alerts for the chosen time period. You can use the **Alerts Trend Line** to select and zoom in on a specific time period within the **Alerts History Line**, as follows: **1.** Click the time-period starting point in the **Alerts Trend Line** and hold down the mouse. **2.** Drag the cursor to the endpoint and then release the mouse. To restore the full view of the **Alerts History Line**, click on any point outside of the light gray shading on the **Alerts Trend Line**.

Item	Description
5	**All Impacted Devices/All Impacted KPIs**: When selected, this dashlet provides a complete list of all devices or KPIs affected by alerts. The information for each affected device or KPI includes: • Device Name or KPI Name • Device or KPI Type • IP address: The IP address of the impacted device. This column is only displayed for devices. • Alert count: The total number of alerts for that device or KPI during the selected period. • Impact score—This value is determined using the following formula: (5 x number of critical alerts) + (4 x number of major alerts) + (3 x number of minor alerts) + (2 x number of warning alerts) + (1 x number of info). These are the default values. You can change the weightage in the **Page Settings** option. When monitoring the health of your network, focus on devices or KPIs with a higher impact score. • Severity distribution—Provides a visual breakdown of the severity that is associated with a device or KPI's alerts. To view a tooltip that indicates the number of raised alarms (by severity and in total), place your cursor over the appropriate bar segment.
6	**Top 20 Impacted Devices/ Top 20 Impacted KPIs**: When selected, this dashlet displays a map of tiles, each tile representing one of the 20 devices or KPIs with the most alerts during the selected time period. The amount of space that each tile occupies in the map corresponds to the number of alerts raised: the more alerts, the bigger the tile. Also, the tiles are color coded. The colors correspond to the **Alert Severity**. To view more detailed information for a particular device or KPI, click the device or KPI name link in the center of the tile.
7	**Device/KPI Watchlist**: When selected, this dashlet provides a list of all devices or KPIs, that you had selected from **+ Manage Deveice/KPI Watchlist**, which are affected by alerts. The information for each affected device or KPI includes: • Device Name or KPI Name • Device or KPI Type • IP address: The IP address of the impacted device. This column is only displayed for devices. • Alert count: The total number of alerts for that device or KPI during the selected period. • Impact score—This value is determined using the following formula: (4 x number of critical alerts) + (3 x number of major alerts) + (2 x number of minor alerts) + number of warning alerts. When monitoring the health of your network, focus on devices or KPIs with a higher impact score. • Severity distribution—Provides a visual breakdown of the severity that is associated with a device or KPI's alerts. To view a tooltip that indicates the number of raised alarms (by severity and in total), place your cursor over the appropriate bar segment.

Item	Description
8	**Alerts History**: The **Alerts History** line shows alerts as discrete bar indicators whose height represents the total number of alerts gathered at each point in time. To see the total for each type of alert, hover your mouse cursor over the bar indicator. You can also use the **Alerts Trend** line to zoom in on particular portions of the alert history.
9	**Timeframe**: Specifies the time period for which the dashboard provides alert information: The past one hour, past day, past week, and so on. Please note that the dashboard provides alert information only, not telemetry information.
10	**Alert Severity**: Maps the bar indicator colors that are used in the **Alert History** dashlet to the corresponding alert severity. To display or hide the alerts for a particular severity, click the check box for that severity. An enabled check box indicates that alerts of that severity have been raised and are being displayed. A clear check box indicates that the alerts of that severity are either not being displayed or have not been raised during the displayed time period.
11	**Auto Refresh**: Specifies how often the dashboard is automatically refreshed.
12	**Refresh Icon**: Refreshes the dashboard.
13	**Page Settings**: Provides the default page settings for that particular session. You can customize the page display based on Alert Type, Timeframe, Auto Refresh, Detail Display, and Alert Severity. You can also change the weightage here for the impact score calculation.

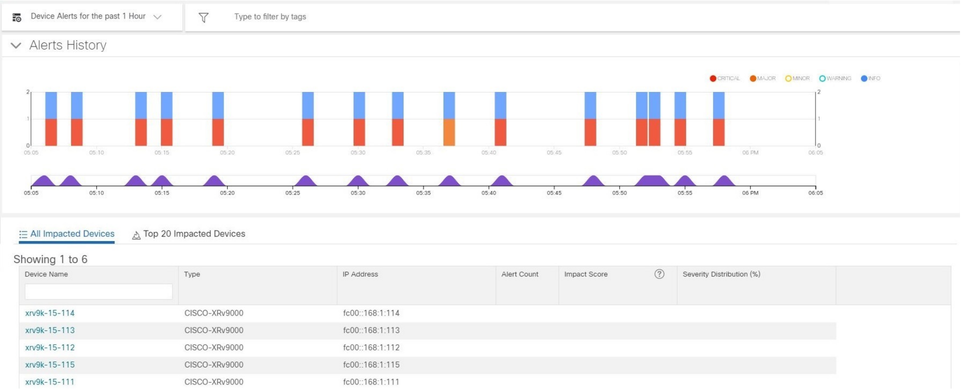
Note The individual alerts for any specific KPI are shown in the dashboard. Alerts resulting from the alert group logic are not shown in the dashboard. Only the API shows the impacted results.

View Alerts for Network Devices

After enabling KPIs on a device, you can view alerts for that device and get data for each performance indicator being monitored.

Note The KPIs shown in the following steps are examples. There are many more KPIs available in Health Insights. For the complete list, see List of Health Insights KPIs, on page 69.

Step 1 From the main menu, choose **Performance Alerts** > **Alert Dashboard**. The Health Insights Alert dashboard is displayed.

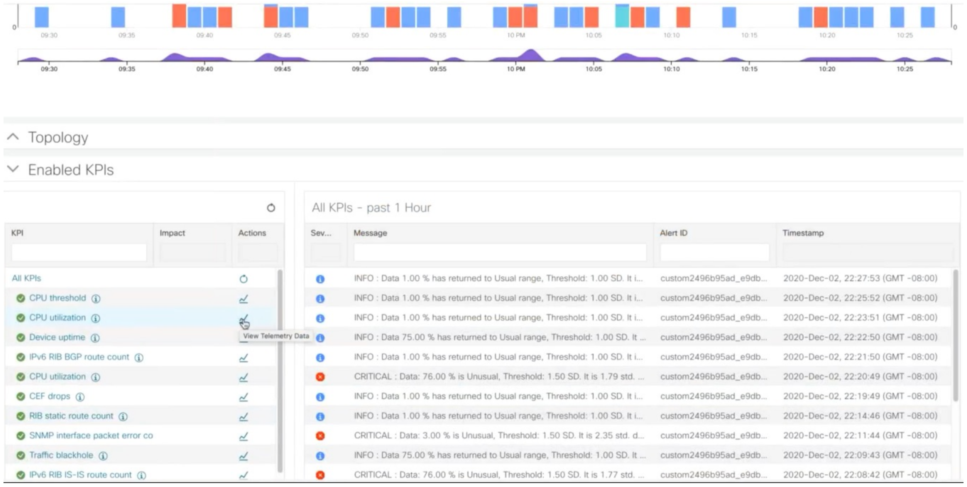


Showing 1 to 6

Device Name	Type	IP Address	Alert Count	Impact Score	Severity Distribution (%)
xrv9k-15-114	CISCO-XRv9000	fc00::168:1:114			
xrv9k-15-113	CISCO-XRv9000	fc00::168:1:113			
xrv9k-15-112	CISCO-XRv9000	fc00::168:1:112			
xrv9k-15-115	CISCO-XRv9000	fc00::168:1:115			
xrv9k-15-111	CISCO-XRv9000	fc00::168:1:111			

Step 2 Make sure that the **Device Alerts** view is displayed (select the **Device Alerts** toggle, if needed). Then scroll down below the **Alert History** panel and click the **All Impacted Devices** tab. The dashboard displays a list of devices with alerts.

Step 3 Click the **Device Name** for the device whose details that you want to view. Health Insights displays the device's basic **Overview** information, **Alert History**, a **Topology** map, and the list of the device's currently **Enabled KPIs**.



KPI	Impact	Actions
All KPIs		
CPU threshold		
CPU utilization		
Device uptime		
IPv6 RIB BGP route count		
CPU utilization		
CEF drops		
RIB static route count		
SNMP interface packet error co		
Traffic blackhole		
IPv6 RIB IS-IS route count		

All KPIs - past 1 Hour

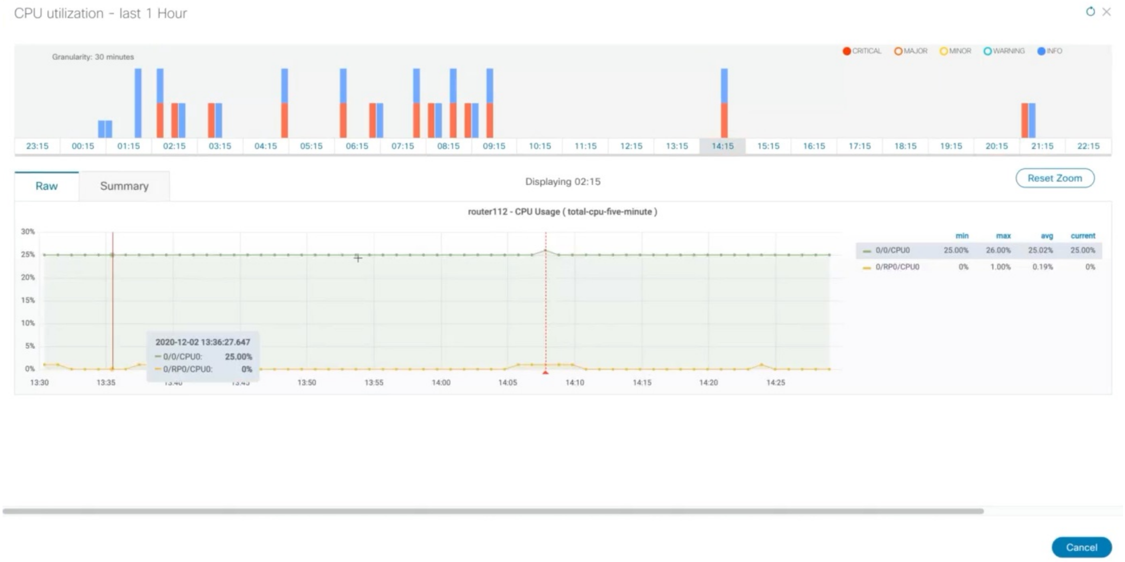
Sev...	Message	Alert ID	Timestamp
ℹ	INFO : Data 1.00 % has returned to Usual range, Threshold: 1.00 SD. It i...	custom2496b95ad_e9db...	2020-Dec-02, 22:27:53 (GMT -08:00)
ℹ	INFO : Data 1.00 % has returned to Usual range, Threshold: 1.00 SD. It i...	custom2496b95ad_e9db...	2020-Dec-02, 22:25:52 (GMT -08:00)
ℹ	INFO : Data 1.00 % has returned to Usual range, Threshold: 1.00 SD. It i...	custom2496b95ad_e9db...	2020-Dec-02, 22:23:51 (GMT -08:00)
ℹ	INFO : Data 75.00 % has returned to Usual range, Threshold: 1.00 SD. It ...	custom2496b95ad_e9db...	2020-Dec-02, 22:22:50 (GMT -08:00)
ℹ	INFO : Data 1.00 % has returned to Usual range, Threshold: 1.00 SD. It i...	custom2496b95ad_e9db...	2020-Dec-02, 22:21:50 (GMT -08:00)
✖	CRITICAL : Data: 76.00 % is Unusual, Threshold: 1.50 SD. It is 1.79 std. ...	custom2496b95ad_e9db...	2020-Dec-02, 22:20:49 (GMT -08:00)
ℹ	INFO : Data 1.00 % has returned to Usual range, Threshold: 1.00 SD. It i...	custom2496b95ad_e9db...	2020-Dec-02, 22:19:49 (GMT -08:00)
ℹ	INFO : Data 1.00 % has returned to Usual range, Threshold: 1.00 SD. It i...	custom2496b95ad_e9db...	2020-Dec-02, 22:14:46 (GMT -08:00)
✖	CRITICAL : Data: 3.00 % is Unusual, Threshold: 1.50 SD. It is 2.35 std. d...	custom2496b95ad_e9db...	2020-Dec-02, 22:11:44 (GMT -08:00)
ℹ	INFO : Data 75.00 % has returned to Usual range, Threshold: 1.00 SD. It ...	custom2496b95ad_e9db...	2020-Dec-02, 22:09:43 (GMT -08:00)
✖	CRITICAL : Data: 76.00 % is Unusual, Threshold: 1.50 SD. It is 1.77 std. ...	custom2496b95ad_e9db...	2020-Dec-02, 22:08:42 (GMT -08:00)

The **Topology** map is a version of the map that you see when you select **Topology** from the main menu.

Step 4 Under **Enabled KPIs**, click 📈 on the desired KPI to view the detailed KPI information. A graphical representation of that KPIs data, along with a list of alert messages and other information, is displayed on the right.

A graphical time-series representation of the selected KPI is displayed for a 72-hour window with hourly slots.

Step 5 Click and move the brush on the timeline to select the desired time slot (selects up to 6 hours) to view the corresponding **Raw** or **Summary** graphical data. Move the mouse cursor over any data point in the graph to view additional pop-up information for that data point.

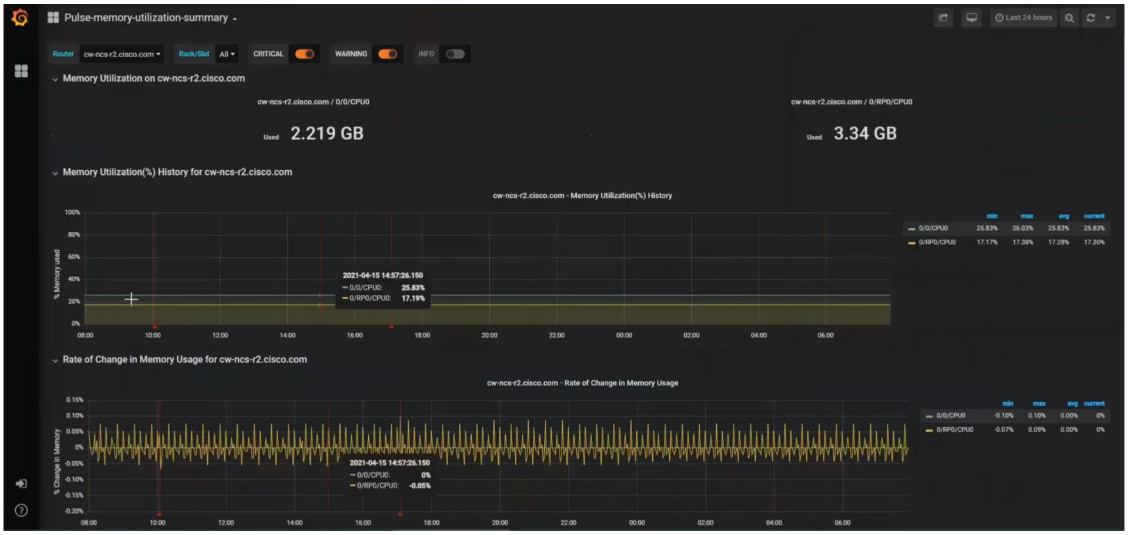


2020-12-02 13:36:27.647
— 0/0/CPU0: 25.00%
— 0/RP0/CPU0: 0%

	min	max	avg	current
— 0/0/CPU0	25.00%	26.00%	25.02%	25.00%
— 0/RP0/CPU0	0%	1.00%	0.19%	0%

A red line or tag represents a point at which the KPI was triggered. This can occur on any subscribed statistic the KPI is monitoring. Health Insights collects and identifies the time points and frequency, which help determine when these events become an operational concern.

Note Graphical data is only visible for time slots that have alerts that are triggered. To view the alerts for the last 72 hours, go to the grafana dashboard (*https://<IPaddress:port>/robot-grafana/*), and select the desired KPI from the dashboard or from the drop-down list. By default, the KPI display is set for last 1 hour. You can change the duration (maximum up to last 72 hours) by selecting the desired option from the drop-down.



Pulse-memory-utilization-summary
Last 24 hours
Router
cw-ncs-r2.cisco.com
Rack/Slot
All
CRITICAL
WARNING
INFO
Memory Utilization on cw-ncs-r2.cisco.com
cw-ncs-r2.cisco.com / 0/0/CPU0
Used
2.219 GB
cw-ncs-r2.cisco.com / 0/RP0/CPU0
Used
3.34 GB
Memory Utilization(%) History for cw-ncs-r2.cisco.com
cw-ncs-r2.cisco.com - Memory Utilization(%) History
% Memory used
100%
80%
60%
40%
20%
0%
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00
Rate of Change in Memory Usage for cw-ncs-r2.cisco.com
cw-ncs-r2.cisco.com - Rate of Change in Memory Usage
% Change in Memory
0.15%
0.10%
0.05%
0%
-0.05%
-0.10%
-0.15%
-0.20%
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00

2021-04-15 14:57:26.150
— 0/0/CPU0: 25.83%
— 0/RP0/CPU0: 17.19%

	min	max	avg	current
— 0/0/CPU0	25.83%	26.03%	25.83%	25.83%
— 0/RP0/CPU0	17.17%	17.38%	17.28%	17.30%

2021-04-15 14:57:26.150
— 0/0/CPU0: 0%
— 0/RP0/CPU0: -0.05%

	min	max	avg	current
— 0/0/CPU0	-0.10%	0.10%	0.00%	0%
— 0/RP0/CPU0	-0.07%	0.09%	0.00%	0%

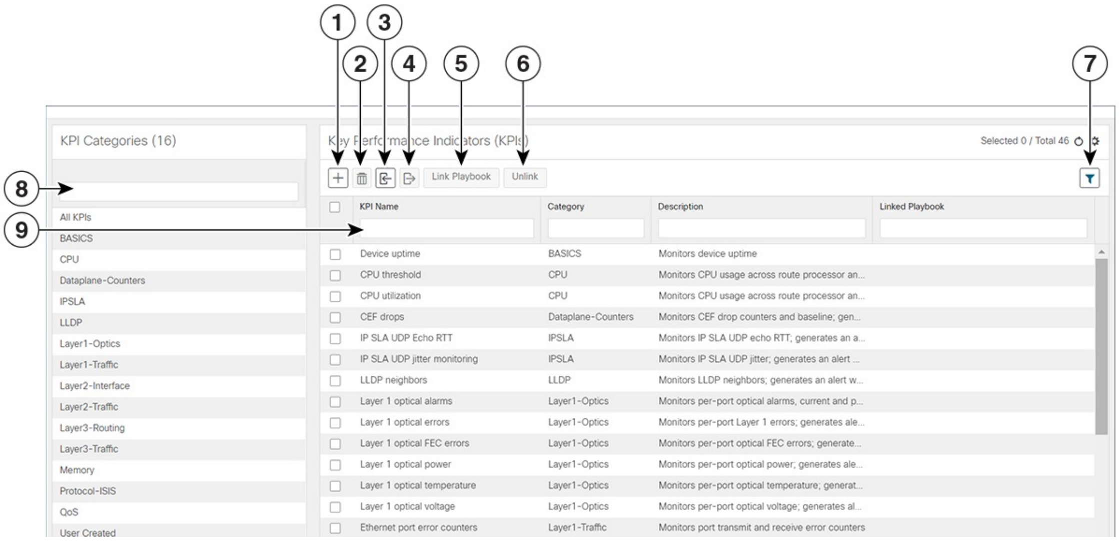
Telemetry Data Retention

Telemetry data is collected from devices and stored in the time-series database. This data is retained for the last 72 hours, and is used in the Health Insights Alert dashboard to identify alerts using a process that is known as stream based alerting. The resulting 'alerts'; if any, are stored in the same time-series database. The alerts are retained for 30 days, and the messages showing the duration of alerts are displayed in the top-right corner of the Device/KPI view in the Alert dashboard. For more information, see View Alerts for Network Devices, on page 61. The alerts can also be queried using REST APIs.

Manage KPIs

The Health Insights Key Performance Indicators (KPI) window gives you complete access to Cisco-supplied and user-created KPIs. You can add, edit, delete, import, and export your KPIs. You can also link your KPIs to the Change Automation application's Playbooks.

To display the Health Insights Manage KPIs window, choose **Performance Alerts** > **Key Performance Indicators (KPI)** from the main menu.



KPI Categories (16)

- All KPIs
- BASICS
- CPU
- Dataplane-Counters
- IPSLA
- LLDP
- Layer1-Optics
- Layer1-Traffic
- Layer2-Interface
- Layer2-Traffic
- Layer3-Routing
- Layer3-Traffic
- Memory
- Protocol-ISIS
- QoS
- User Created

Key Performance Indicators (KPIs)

Selected 0 / Total 46

□	KPI Name	Category	Description	Linked Playbook
□	Device uptime	BASICS	Monitors device uptime	
□	CPU threshold	CPU	Monitors CPU usage across route processor an...	
□	CPU utilization	CPU	Monitors CPU usage across route processor an...	
□	CEF drops	Dataplane-Counters	Monitors CEF drop counters and baseline; gen...	
□	IP SLA UDP Echo RTT	IPSLA	Monitors IP SLA UDP echo RTT; generates an a...	
□	IP SLA UDP jitter monitoring	IPSLA	Monitors IP SLA UDP jitter; generates an alert ...	
□	LLDP neighbors	LLDP	Monitors LLDP neighbors; generates an alert w...	
□	Layer 1 optical alarms	Layer1-Optics	Monitors per-port optical alarms, current and p...	
□	Layer 1 optical errors	Layer1-Optics	Monitors per-port Layer 1 errors; generates ale...	
□	Layer 1 optical FEC errors	Layer1-Optics	Monitors per-port optical FEC errors; generate...	
□	Layer 1 optical power	Layer1-Optics	Monitors per-port optical power; generates ale...	
□	Layer 1 optical temperature	Layer1-Optics	Monitors per-port optical temperature; generat...	
□	Layer 1 optical voltage	Layer1-Optics	Monitors per-port optical voltage; generates al...	
□	Ethernet port error counters	Layer1-Traffic	Monitors port transmit and receive error counters	

Item	Description
1	**Add KPIs**: Click + to add a new, user-created KPI. For help with this task, see Create a New KPI, on page 65.
2	**Delete KPIs**: Select one or more existing user-created KPIs in the list and then click 🗑. You will be prompted to confirm that you want to delete the KPIs. Click **Delete** to confirm. **Note** You can delete user-created KPIs only. You cannot delete Cisco-supplied KPIs.

Item	Description
3	**Import KPIs**: Click ⇤ to import new user-written or Cisco-supplied KPIs. You will be prompted to browse to the gzipped tar archive containing the KPIs to be imported. When you have selected the archive, click **OK** to begin importing it. Once imported, the new KPIs appear in the list of KPIs, with each KPI name and category assigned based on the definition in the KPI itself. In order for Cisco Crosswork Health Insights to import them, KPI files must: • Be packaged as a gzip tar archive. You can include more than one KPI in a single archive; each will be imported as a separate KPI. • Have unique names and descriptions. These must not match the name or description of any Cisco-supplied KPI. If the name or description of the KPI matches an existing user-created KPI, the import will overwrite the existing KPI. • Meet other minimum requirements for Health Insights KPIs, as explained in the Cisco Crosswork Network Automation Custom KPI Tutorial Documentation on Cisco DevNet.
4	**Export KPIs**: Select one or more existing KPIs in the list and then click ⇥ to export them. Health Insights will package the exported KPIs as a single TGZ archive with a unique name. Your browser will then prompt you to save the archive to a name and location in your local file system that you select.
5	**Link Playbooks**: Select a KPI and then click Link Playbook to link it to a Playbook. Linking a Playbook streamlines the remediation process by importing data from the alert and using it to pre-populate the parameters the Playbooks needs (such as device, interface names, and so on) to run in order when you attempt to remediate the issue. For help with this task, see Link KPIs to Playbooks, on page 67.
6	**Unlink Playbooks**: Select a KPI with a linked Playbook and then click Unlink to unlink the Playbook. You will be prompted to confirm that you want to unlink the Playbook. Click **Unlink** to confirm.
7	**Clear Filters**: Click **Clear All Filters** to clear any filters you have set.
8	**Filter KPI Categories**: To find a KPI category, enter all or part of the KPI Category name in this field. Then click ▼ to filter the list below.
9	**Filter KPIs**: To find a KPI, enter all or part of the **KPI Name**, **Category**, **Description**, or **Linked Playbook** in the fields provided. The list below is automatically filtered to match your typed entry.

Create a New KPI

You can create a custom KPI and enable it on the desired devices. The workflow is as follows:

1. Supply basic information, such as the KPI name and a summary description.
2. Set the KPI cadence.

3. Select a YANG module and choose sensor paths.
4. Select an alert template and set its parameters.
5. Enable the KPI on the devices.

Note Health Insights supports creating and using KPIs that use GNMI as the transport and use sensors that are based on Open Config (OC) YANG modules for collecting telemetry data (with GNMI transport). The requirements for this feature are:

- GRPC must be configured in your device.
- The device properties, while onboarding, must mention GNMI under the **Capability** field, and the GNMI protocol details must be provided under the **Connectivity Details** field.
- While creating a KPI, choosing an OC YANG module supports the KPI affinity for GNMI transport, while choosing Cisco-provided YANG models provides the KPI affinity for both MDT and GNMI transports.

The GNMI transport capability is determined at runtime which is based on the following factors such as GNMI capability of the device, GNMI affinity of the KPI, and the combined capability as a set of devices in a KPI Profile.

The following steps explain how to create a KPI:

Before you begin

Make sure that the device packages for the devices are available in Crosswork. If they are not available, perform *Add a Custom Software Package* procedure from *Cisco Crosswork Infrastructure 4.3 and Applications Administration Guide* and then continue with the steps in this procedure.

Step 1 From the main menu, choose **Performance Alerts** > **Key Performance Indicators (KPI)**. The **Key Performance Indicators (KPI)** window is displayed.

Step 2 Click the ⊞. The **Create KPI** window opens.

Step 3 In the text fields provided, enter a unique **KPI Name**, a short **KPI Summary** description, and **KPI details**. The **KPI Group** is preset to `User Created`.

Step 4 The **Cadence** field sets the number of seconds between data collections . Leave it at the default or use the numerical selector to choose a different value.

Step 5 In the **YANG Modules** area, choose one module and one or more sensor paths from which to stream data:

a) Use the **Module** field to filter and choose the desired Cisco IOS XR YANG module.

b) Use the table fields to filter and choose the desired sensor path. When you choose a path, the leaf node gets resolved to the base encoding path. If the YANG module is hierarchical, the field names are concatenated down from the base path. Only one gather path is supported for user-created KPIs.

Note If the devices are not listed in the default YANG modules, you can expand the device coverage. For more information, see the section *Manage Custom Software Packages and Add a Custom Software Package* in the *Cisco Crosswork Infrastructure 4.3 and Applications Administration Guide* and then continue with the subsequent steps in this procedure.

Click **Next** to display the **Select Alert Templates** window.

Note To build a KPI that uses data from more than one module, you can do this with KPI profiles and alert groups. For more information, see Create a New KPI Profile, on page 76.

Step 6 Choose the alert template that you want to use with your new KPI: **No Alert**, **Standard Deviation**, **Two-Level Threshold** or **Rate Change**. Then click **Next** to display the **Alert Parameters** window appropriate for the type of alert template you chose.

Step 7 Edit the alert template parameter values as appropriate for the template and the purpose of your KPI, as follows:

- Use the **Basic** and **Advanced Parameters** dropdowns to view and edit the parameter sets you need.
- Change alert parameter numerical values using the selectors or by editing the field contents
- Change alert parameters with discrete choices using parameter field dropdowns and select each choice as needed.
- Learn more about an alert parameter: Hover your mouse cursor over the ? shown next to the parameter name.
- Click the **View Tick Script** link to view the tick script code you are generating with your changes. The tick script code updates as you make your edits. At any time, click the **Hide Tick Script** to close the tick script code window.

Step 8 When you are finished making changes, click **Finish** to save the new KPI and display the **Key Performance Indicators (KPI)** window.

Link KPIs to Playbooks

You can link any Health Insights KPI to one Change Automation Playbook of your choice. You can run the linked Playbook whenever the linked KPI raises an alert in response to the event associated with the performance indicator the KPI is monitoring. The KPI alert can be raised in response to a threshold crossing, topology changes, flapping conditions, and other parameters. These parameters vary, as appropriate, for each KPI.

Note This procedure is not applicable if the Change Automation application is not installed in your device. In this case, the UI features that link Health Insights and Change Automation (For example, Link Playbook) are not displayed in the UI.

You can specify the **Source** of the parameter values the linked Playbook uses when you run it. You can select these sources:

- **Playbook**: Use default values coded into the Playbook itself
- **KPI Alert**: Use values that are taken from the alert that is raised by the linked KPI.
- **Run-time Input**: Use values that you enter only at the moment you run the Playbook.

The ability to set the source of these Playbook parameter values gives you flexibility in how you use the linked Playbook. For example: Link the KPI **Interface flap detection**, which detects interface flapping, to the Playbook **Interface state change on XR**, which can be used to set the interface up or down. Depending on circumstances, you can want to set the Playbook parameters as follows:

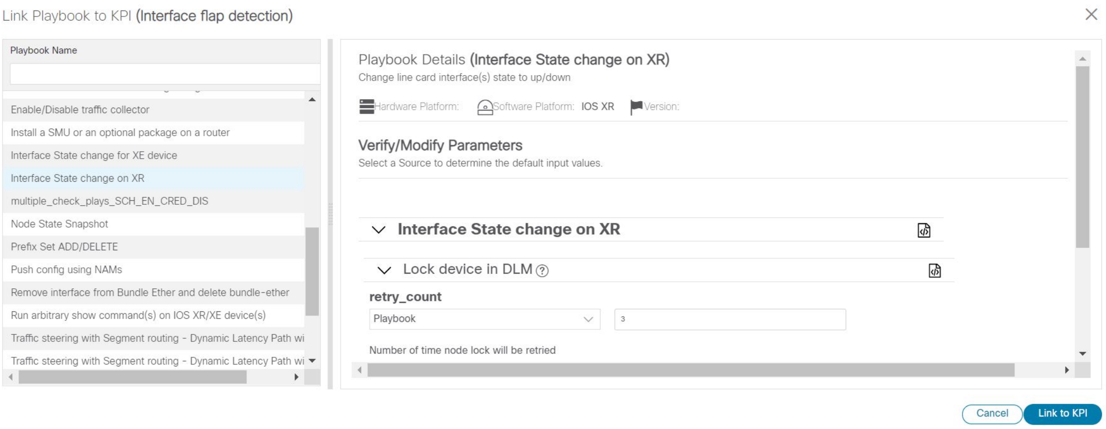
- **Playbook**: You want to run the Playbook as it normally does, so you would set the **Source** as **`Playbook`** for the *provider*, *collection_type* and *mop_timeout* parameters. In the case of the *collection_type*, you can still choose between **`telemetry`** and **`snmp`**, depending on whether you want to use MDT or SNMP to gather device data.

- **KPI Alert**: You want the Playbook to run only on the host device and interface affected by the flapping, which are identified in the flap-detection Alert. So set the **Source** of the Playbook's *hosts* and *if_names* parameters to **`KPI Alert`**. You can then use the alert's data about the **`Producer`** device and the **`interface_name`** of the flapping interface on that device.

- **Run-time Input**: You want the freedom to decide at runtime whether to bring the flapping interface up or down. So set the **Source** of the Playbook parameter *admin_state* to **`Runtime Input`**. The Playbook will prompt you for an **`up`** or **`down`** choice when you initiate the run.

The following figure shows what this set of choices will look like:

Figure 10: Example: Specifying Parameter Value Sources for a Linked Playbook



Link Playbook to KPI (Interface flap detection)

Playbook Name

Enable/Disable traffic collector
Install a SMU or an optional package on a router
Interface State change for XE device
Interface State change on XR
multiple_check_plays_SCH_EN_CRED_DIS
Node State Snapshot
Prefix Set ADD/DELETE
Push config using NAMs
Remove interface from Bundle Ether and delete bundle-ether
Run arbitrary show command(s) on IOS XR/XE device(s)
Traffic steering with Segment routing - Dynamic Latency Path wi
Traffic steering with Segment routing - Dynamic Latency Path wi

Playbook Details (Interface State change on XR)
Change line card interface(s) state to up/down

Hardware Platform: Software Platform: IOS XR Version:

Verify/Modify Parameters
Select a Source to determine the default input values.

Interface State change on XR

Lock device in DLM

retry_count
Playbook 3
Number of time node lock will be retried

Step 1 From the main menu, choose **Performance Alerts** > **Key Performance Indicators (KPI)**. The **Key Performance Indicators (KPI)** window opens, displaying lists of the KPI categories and the KPIs available in each category.

Step 2 Select the KPI you want to link to a Playbook. You can use filters to find the KPI you want, as explained in Manage KPIs, on page 64.

Step 3 Click Link Playbook. The **Link Playbook to KPI** window opens.

Step 4 The left side of the window lists the name of the selected KPI and the Playbooks appropriate for linking to it. Scroll through the list, or use the **Playbook Name** field to restrict the list to just the Playbooks you want.

Step 5 When you have found the Playbook that you want to link, click the name. The right side of the window will then list the **Playbook Details** for the selected Playbook, including:

- The hardware and software platforms with which it is compatible.
- The minimum software version requirement
- The **Source** and default values that will be used when the Playbook runs. In many cases, you can select from a range of default values, or enter your own.

Step 6 Verify or modify the **Source** and parameter values as needed.

Step 7 When you are finished making changes, click **`Link to KPI`**. The **Key Performance Indicators (KPI)** window is displayed again, this time with the linked Playbook shown next to name of the KPI in the **Key Performance Indicators (KPIs)** list.

Step 8 To change the Playbook linked to a given KPI, repeat steps 3 through 7 for that KPI, this time choosing the Playbook that you want. To unlink a Playbook entirely, select the KPI and click Unlink.

Verify the Deployment Status of Enabled KPIs

After you enable a KPI Profile, you can verify the deployment status.

Step 1 From the main menu, choose **Performance Alerts** > **KPI Job History** The **KPI Job History** window lists the jobs that have been run most recently, indicating whether they succeeded or failed, when they ran, and on what devices.

Step 2 Click the transaction ID in the job listing to view detailed KPI job information, including the device on which the KPI Profile was enabled and the KPI ID.

List of Health Insights KPIs

The following table lists the prebuilt Health Insights KPIs supplied with Cisco Crosswork Health Insights.

Alerting types in the table that you can select when you create a new KPI through the UI. See Create a New KPI, on page 65:

- **No Alert**: The KPI gathers, tracks, and reports performance data without triggering alerts.
- **Standard Deviation**: The KPI detects spikes or drops in measured values and alerts when these values deviate some number of standard deviations away from their normal values.
- **Two-Level Threshold**: The KPI detects abnormal measured values using two custom thresholds and the ability to provide dampening intervals on the thresholds.
- **Rate Change**: The KPI detects abnormal rates of change in measured values to detect rising or falling values.

Additional alerting types that you can use when you export and modify a prebuilt KPI to create KPI with custom parameters are:

- **Standard Deviation of Rate Change**: The KPI alerts on standard deviations of the rate of change.
- **Low Single Threshold**: The KPI alerts on a single threshold when the value falls below that threshold.
- **Direct Alarm Forwarding**: The KPI uses the alarm from the device directly, as a Health Insights KPI alert.
- **Major/Minor/Low/High Thresholds**: The KPI alerts on Major high, Minor high, Minor low, and Major low values.
- **Line State Changes**: The KPI alerts on shutdowns and flapping in line states.

For more on creating KPIs with custom parameters from exported KPIs, see the Cisco Crosswork Network Automation Custom KPI Tutorial Documentation on Cisco DevNet.

Table 2: Health Insights KPIs

Category	KPI Name	Description	Alerting	Protocol[1]
Dataplane-Counters	CEF drops	Monitors CEF drop counters and baseline. Generates an alert for an unusual number of drops.	Rate Change	MDT, gNMI[2]
CPU	CPU threshold	Monitors CPU usage across route policies and line cards on routers. Generates an alert when CPU utilization exceeds the configured threshold	Two-Level Threshold	MDT, gNMI[2]
CPU	CPU utilization	Monitors CPU usage across route policies and line cards on routers. Generates an alert when CPU utilization is unusual.	Standard Deviation	MDT, gNMI[2]
Basics	Device uptime	Monitors device uptime.	Low Single Threshold	MDT, gNMI[2]
Layer 1-Traffic	Ethernet port error counters	Monitors port transmit and receive error counters.	Rate Change	MDT, gNMI[2]
Layer 1-Traffic	Ethernet port packet size distribution	Monitors port transmit and receive packet size distributions.	No Alert	MDT, gNMI[2]
Layer 1-Traffic	Ethernet port packet statistics	Monitors port transmit and receive packet statistics.	Standard Deviation of Rate Change	MDT, gNMI[2]
Layer 2-Traffic	Interface bandwidth monitor	Monitors bandwidth utilization across all interfaces on a router. Generates an alert when bandwidth exceeds the configured threshold.	Two-Level Threshold	MDT, gNMI[2]
Layer 3-Traffic	Interface counters by protocol	Monitors interface statistics (such as incoming and outgoing packets or byte counters) organized by protocol.	Standard Deviation	MDT, gNMI[2]
Layer2-Interface	Interface flap detection	Monitors interface flaps and alerts when flap count reaches set threshold.	Two-Level Threshold	MDT, gNMI[2]
Layer 2-Traffic	Interface packet counters	Monitors interface transmit and receive counters. Generates an alert when unusual traffic rates occur.	No Alert	MDT, gNMI[2]
Layer 2-Traffic	Interface packet error counters	Monitors interface transmit and receive error counters. Generates an alert when unusual error rates occur.	Rate Change	MDT, gNMI[2]
QOS	Interface QoS (egress)	Monitors interface QoS on the egress direction for queue statistics, queue depth, and so on.	No Alert	MDT, gNMI[2]

Category	KPI Name	Description	Alerting	Protocol[1]
QOS	Interface QoS (ingress)	Monitors interface QoS on the ingress direction for queue statistics, queue depth, and so on.	No Alert	MDT, gNMI[2]
Layer 2-Traffic	Interface rate counters	Monitors interface statistics as rate counters. Generates an alert when unusual traffic rates occur.	Standard Deviation	MDT, gNMI[2]
IPSLA	IP SLA UDP echo RTT	Monitors IP SLA UDP echo RTT. Generates an alert when unusual RTT values occur.	Standard Deviation	MDT, gNMI[2]
IPSLA	IP SLA UDP jitter monitoring	Monitors IP SLA UDP jitter. Generates an alert when an abnormal UDP jitter occurs.	Standard Deviation	MDT, gNMI[2]
Layer 3-Routing	IPv6 RIB BGP route count	Monitors IPv6 RIB for route count and memory used by BGP. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, gNMI[2]
Layer 3-Routing	RIB IS-IS route count	Monitors RIB for route count and memory used by IS-IS. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, gNMI[2]
Layer 3-Routing	IPv6 RIB IS-IS route count	Monitors IPv6 RIB for route count and memory used by IS-IS. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, gNMI[2]
Layer 3-Routing	IPv6 RIB OSPF route count	Monitors IPv6 RIB for route count and memory used by OSPF. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, gNMI[2]
Protocol-ISIS	ISIS neighbor summary	Monitors ISIS neighbor summaries for changes in neighbor status. Generates an alert when an anomaly is detected (such as neighbors down or flapping).	Standard Deviation	MDT, gNMI[2]
Layer 1-Optics	Layer 1 optical alarms	Monitors per-port optical alarms (current and past).	Direct Alarm Forwarding	MDT, gNMI[2]
Layer 1-Optics	Layer 1 optical errors	Monitors per-port Layer 1 errors. Generates an alert when error rates exceed the configured threshold.	Rate Change	MDT, gNMI[2]

Category	KPI Name	Description	Alerting	Protocol[1]
Layer 1-Optics	Layer 1 optical FEC errors	Monitors per-port optical FEC errors. Generates an alert when FEC errors exceed the configured threshold.	Rate Change	MDT, gNMI[2]
Layer 1-Optics	Layer 1 optical power	Monitors per-port optical power. Generates an alert when power levels exceed the configured threshold.	Major/Minor/Low/High Thresholds	MDT, gNMI[2]
Layer 1-Optics	Layer 1 optical temperature	Monitors per-port optical temperature. Generates an alert when temperature exceeds the configured threshold.	Major/Minor/Low/High Thresholds	MDT, gNMI[2]
Layer 1-Optics	Layer 1 optical voltage	Monitors per-port optical voltage. Generates an alert when voltages exceed the configured threshold.	Major/Minor/Low/High Thresholds	MDT, gNMI[2]
Layer 2-Interface	Line state	Monitors interface line states. Generates an alert when link states change.	Line State Changes	MDT, gNMI[2]
LLDP	LLDP neighbors	Monitors LLDP neighbors. Generates an alert when any sudden changes are detected.	Standard Deviation	MDT, gNMI[2]
Memory	Memory utilization	Monitors memory usage across route processor and line cards on routers. Generates an alert when memory utilization is unusual.	Standard Deviation	MDT, gNMI[2]
Memory	Memory utilization (cXR)	Monitors memory usage across route processor and line cards on classic XR devices. Generates an alert when memory utilization is unusual.	Standard Deviation	MDT, gNMI[2]
Layer 3-Routing	RIB BGP route count	Monitors RIB for route count and memory used by BGP. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, gNMI[2]
Layer 3-Routing	RIB connected route count	Monitors RIB for route count and memory used by connected. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, gNMI[2]
Layer 3-Routing	RIB IS-IS route count	Monitors RIB for route count and memory used by IS-IS. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts)	Standard Deviation	MDT, gNMI[2]

Category	KPI Name	Description	Alerting	Protocol[1]
Layer 3-Routing	RIB local route count	Monitors RIB for route count and memory used by local. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, gNMI[2]
Layer 3-Routing	RIB OSPF route count	Monitors RIB for route count and memory used by OSPF. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, gNMI[2]
Layer 3-Routing	RIB static route count	Monitors RIB for route count and memory used by static. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, gNMI[2]
Layer 3-Routing	RIBv6 connected route count	Monitors RIBv6 for route count and memory used by connected. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, gNMI[2]
Layer 3-Routing	RIBv6 local route count	Monitors RIBv6 for route count and memory used by local. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, gNMI[2]
Layer 3-Routing	RIBv6 static route count	Monitors RIBv6 for route count and memory used by static. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, gNMI[2]
Layer 3-Routing	RIBv6 subscriber route count	Monitors RIBv6 for route count and memory used by subscriber. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, gNMI[2]
Layer 2-Traffic	SNMP interface packet error counters	Monitors interface transmit and receive error counters. Generates an alert when unusual error rates occur.	No Alert	SNMP
Layer 2-Traffic	SNMP interface packet counters	Monitors interface transmit and receive counters. Generates an alert when unusual traffic rates occur.	Rate Change	SNMP

Category	KPI Name	Description	Alerting	Protocol[1]
Layer 2-Traffic	SNMP interface rate counters	Monitors interface statistics as rate counters. Generates an alert when unusual traffic rates occur.	Standard Deviation Rate of Change	SNMP
Layer 2-Traffic	SNMP traffic black hole	Monitors input and output data rates for black hole behavior. Checks the ratio of output data rate to input data rate and verifies that the ratio is within acceptable ranges, otherwise a black hole is occurring.	Two-Level Threshold	SNMP
Layer 2-Traffic	Traffic black hole	Monitors input and output data rates for black hole behavior. Checks the ratio of output data rate to input data rate and verifies that the ratio is within acceptable ranges, otherwise black hole.	Two-Level Threshold	MDT, gNMI[2]
Layer 2-Traffic	Interface packet error counters (Openconfig)	Monitors interface error counters; generates an alert when unusual error rates occur. This KPI uses openconfig-interfaces YANG model.	Rate Change	gNMI
Layer 2-Traffic	Interface rate counters (Openconfig)	Monitors interface statistics (such as rate counters), and generates an alert when unusual traffic rates occur.	Rate Change	gNMI
File System	Filesystem Utilization	Monitors filesystem usage on active route processor and generates an alert when filesystem utilization exceeds the configured threshold.	Two-Level Threshold	CLI

Note The target device(s) must support the form of telemetry used by the KPI either SNMP, GNMI, or MDT. The application validates for a match between KPI and device telemetry capabilities.

[1]: Definition of the protocols:

- Model-Driven Telemetry (MDT): Model-driven telemetry provides a mechanism to stream operational data from device as defined in the YANG model(s) to a data collector.
- gRPC Network Management Interface (gNMI): gNMI provides the mechanism to install, manipulate, and delete the configuration of network devices, and also to view operational data.
- Simple Network Management Protocol (SNMP): SNMP is an IP protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.
- Command Line Interface (CLI): CLI is used in network device management.

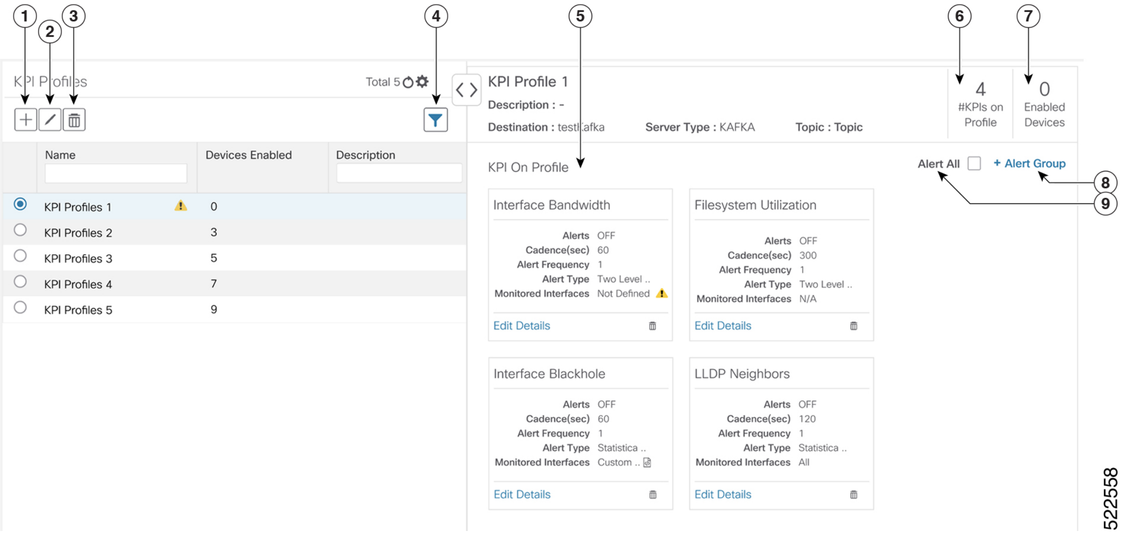
[2]: Health Insights uses either MDT or gNMI protocols but the device supports both. gNMI is a preferred default. Selection of the protocol also depends on the capability of the other device, part of the KPI enable operation or job.

Manage KPI Profiles

The Health Insights KPI Profiles window allows you to create, edit, and delete KPI Profiles.

A KPI Profile is a collection of KPIs and their corresponding parameters such as alert frequency, alert type, cadence, and more. You can group relevant KPIs into a KPI Profile, give it meaningful name that is based on the purpose (for example, environmental or health check), and configure parameters that are relevant to monitoring a specific type of devices (for example, edge routers). Once the KPI profiles are created and validated by the system, they are ready to be used. You can select the device(s) in Health Insights, select appropriate KPI Profiles, and enable them. This action enables all the KPIs in the selected KPI Profile. Similarly, you can select the device(s) and choose to disable the KPI Profiles. This removes all the collection jobs on the Crosswork Data Gateway for all the KPIs and for MDT-based KPIs, this removes the configuration in the device(s).

To display the Health Insights KPI Profiles window, choose **Performance Alerts** > **KPI Profiles** from the main menu.



KPI Profiles Total 5

Name	Devices Enabled	Description
● KPI Profiles 1 ⚠	0	
○ KPI Profiles 2	3	
○ KPI Profiles 3	5	
○ KPI Profiles 4	7	
○ KPI Profiles 5	9	

KPI Profile 1
Description : -
Destination : testKafka Server Type : KAFKA Topic : Topic

4 #KPIs on Profile
0 Enabled Devices

KPI On Profile
Alert All □ + Alert Group

Interface Bandwidth
Alerts OFF
Cadence(sec) 60
Alert Frequency 1
Alert Type Two Level ..
Monitored Interfaces Not Defined ⚠
Edit Details

Filesystem Utilization
Alerts OFF
Cadence(sec) 300
Alert Frequency 1
Alert Type Two Level ..
Monitored Interfaces N/A
Edit Details

Interface Blackhole
Alerts OFF
Cadence(sec) 60
Alert Frequency 1
Alert Type Statistica ..
Monitored Interfaces Custom ..
Edit Details

LLDP Neighbors
Alerts OFF
Cadence(sec) 120
Alert Frequency 1
Alert Type Statistica ..
Monitored Interfaces All
Edit Details

Item	Description
1	**Create KPI Profile**: Click ⊞ to create a new, user-created KPI Profile. For help with this task, see Create a New KPI Profile, on page 76.
2	**Edit KPI Profile**: Select a user-created KPI Profile in the list and then click ✎ to edit it. For help with this task, see Create a New KPI Profile, on page 76.
3	**Delete KPI Profile**: Select a user-created KPI Profile in the list and then click 🗑 to delete it. You cannot delete a KPI Profile that has been enabled on any device(s).
4	**Filter KPI Profile**: To find a KPI category, enter all or part of the KPI Profile name in this field, and the list is automatically filtered based on your input. Click ⏷ to clear any filters you have set.
5	**KPI On Profile**: The KPI(s) added on the selected KPI Profile and the associated parameters are displayed here. You can edit the KPI parameters, or remove a KPI from the selected KPI Profile using the appropriate options here.
6	**#KPIs on Profile**: This is the number of KPIs added on the selected KPI Profile.
7	**Enabled Devices**: This is the number of devices on which the selected KPI Profile is enabled.
8	**+Alert Group**: Click this option to create Alert Group for the selected KPI Profile. For help with this task, see Create a New KPI Profile, on page 76
9	**Alert All**: Click this option to turn off or turn on the alerts for all KPIs in the profile.

Create a New KPI Profile

You can create a KPI Profile and enable it on the desired devices. The workflow is as follows:

1. Supply basic information, such as the Profile name and a description.
2. Add KPI(s) and save the profile.

3. Edit KPI parameters and create alert groups.
4. Enable the KPI Profile on the devices.

The following steps explain how to perform these tasks.

Step 1 From the main menu, choose **Performance Alerts** > **KPI Profiles**. The **KPI Profiles** window is displayed.

Step 2 Click the ⊞. The **Create New Profile** window is displayed.

Step 3 In the text fields provided, enter a unique **Profile Name**, a short **Description**. The **Profile Name** can contain a maximum of 32 alphanumeric characters, plus underscores ("_"). No other special characters are allowed.

Step 4 (Optional) You can specify an external destination to send the data collected by KPIs. To create an external data destination, go to **Administration** > **Data Gateway Global Settings** Provide relevant values for the following fields:

- **Server Type**: Select either KAFKA or GRPC.
- **Name**: Select the name of the external destination.
- **Topic**: Enter a topic to provide context for the data being sent. This field is applicable only for KAFKA.

Note You need to create a new data destination to export the KPI data. The predefined data destinations cannot be used for this activity. For more information about creating a data destination, see *Cisco Crosswork Infrastructure 4.3 and Applications Administration Guide*.

Step 5 Add KPI to the profile, using the following filter options:

a) **All KPIs**: By default, this option is selected and the list of all KPIs are displayed in the list. You can select the required KPI by checking the relevant check box.

b) **Recommended KPIs**: You can select KPIs based on the KPIs recommended for a specific device. Click **Recommended KPIs** and the device list is displayed. You can filter the device list by entering relevant values in the Name field, or by using tags. Select a device from the list and the recommended KPI list is displayed on the right side. Select the required KPI by checking the relevant check box.

Note Selecting KPIs from the recommended KPI list of a selected device does not automatically enable the KPI Profile in the selected device. The KPI Profile can be enabled after it is created. For more information, see Enable KPI Profile on Devices, on page 79

Step 6 Click **Save** save the new KPI Profile and display the **KPI Profiles** window.

Step 7 In the **KPI Profiles** area on the left side, choose the KPI Profile that you created, and the individual KPI details are displayed on the right side.

Note For the Interface KPIs, you can gather the data for **all** the interfaces or **selected** interfaces. If you opt to gather the information for **all** the interfaces, a warning symbol appears on the KPI Profile name on the left side and on the individual KPI details on the right side, indicating that the monitoring interfaces are not customized.

Important Gathering telemetry data for all the interfaces can be resource-intensive and may require additional worker nodes and/or CDG resources to be deployed.

Step 8 You can leave the KPI parameters at the default or choose a different value. To edit the KPI parameters and preferences, click **Edit Details**, and the **KPI Details** window is displayed. Edit the values as appropriate for the purpose of your KPI. The details are:

- **Common Parameters**

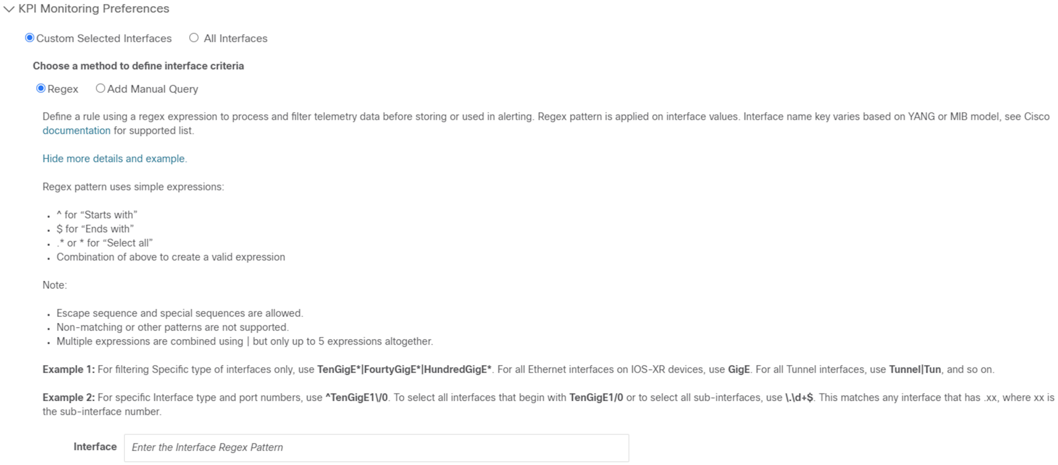
- **Alert**: This is an on/off toggle switch for alerting. Based on the **Alert** parameter value, the corresponding alerting logic is deployed. Alerting can be enabled even after the KPI Profile has been applied to the devices.

  Note Any KPI using the group alerting logic need to have the alerting flag set to ON.

- **Cadence (sec)**: Set the frequency of sensor data. Set the frequency (in seconds) in which the KPI will gather sensor data from the devices on which the KPI Profile is enabled.

- **Alerting Down Sample Rate**: Alert frequency rate. It determines how often KPI data will be evaluated for any alert conditions, and is relative to the Cadence. For example, if Cadence is 60 seconds and you want to do an alerting evaluation every 300 sec, then specify Alerting Down Sample Rate as "5".

- **KPI Monitoring Preferences**: Applicable only for Interface KPIs.



KPI Monitoring Preferences

● Custom Selected Interfaces ○ All Interfaces

Choose a method to define interface criteria

● Regex ○ Add Manual Query

Define a rule using a regex expression to process and filter telemetry data before storing or used in alerting. Regex pattern is applied on interface values. Interface name key varies based on YANG or MIB model, see Cisco documentation for supported list.

Hide more details and example.

Regex pattern uses simple expressions:

- ^ for “Starts with”
- $ for “Ends with”
- .* or * for “Select all”
- Combination of above to create a valid expression

Note:

- Escape sequence and special sequences are allowed.
- Non-matching or other patterns are not supported.
- Multiple expressions are combined using | but only up to 5 expressions altogether.

Example 1: For filtering Specific type of interfaces only, use **TenGigE*|FourtyGigE*|HundredGigE***. For all Ethernet interfaces on IOS-XR devices, use **GigE**. For all Tunnel interfaces, use **Tunnel|Tun**, and so on.

Example 2: For specific Interface type and port numbers, use **^TenGigE1\/0**. To select all interfaces that begin with **TenGigE1/0** or to select all sub-interfaces, use **\.\d+$**. This matches any interface that has .xx, where xx is the sub-interface number.

Interface *Enter the Interface Regex Pattern*

  - **Customer Selected Interfaces**: You can define the interface criteria.

    - **Regex**: You can define a rule using regex expression.

    - **Add Manual Query**: You can add different sets of rules.

  - **All Interfaces**: The selected KPI is applied to all the interfaces.

Step 9 You can also edit the alert logic parameters of the selected KPI. To learn more about a parameter, hover your mouse cursor over the ? shown next to the parameter name.

Note When different thresholds are desired for different types of devices in the network, it is advisable to create multiple profiles and split the KPIs across them to meet the needs of different device types.

Step 10 When you are finished making changes, click **Save** to save the new KPI Profile. Health Insights validates your input parameters and displays the **KPI Profiles** window.

Note You can create up to 50 KPI profiles, and an individual KPI Profile can consist up to 50 KPIs. KPI profile creation can fail if the total number is exceeded, or if Health Insights could not create the required tags in Inventory manager. This status is reflected in the profile state. Once profile is ready, it can be applied on devices.

With the **KPI Profiles** window displayed, you can enable the new KPI Profiles on one or more devices immediately, following the steps given in Enable KPI Profile on Devices, on page 79.

See Disable KPI Profile on Devices or Device Groups, on page 82 for instructions to disable KPI Profiles.

Step 11 (Optional) You can also create alert groups for a KPI Profile. Alert groups use boolean logic (cascaded OR and AND) to combine alert outputs from primary KPIs in your KPI profile and create a group logic query. To create an alert group, click **+ Alert Group**. The **Create Alert Group** window is displayed.

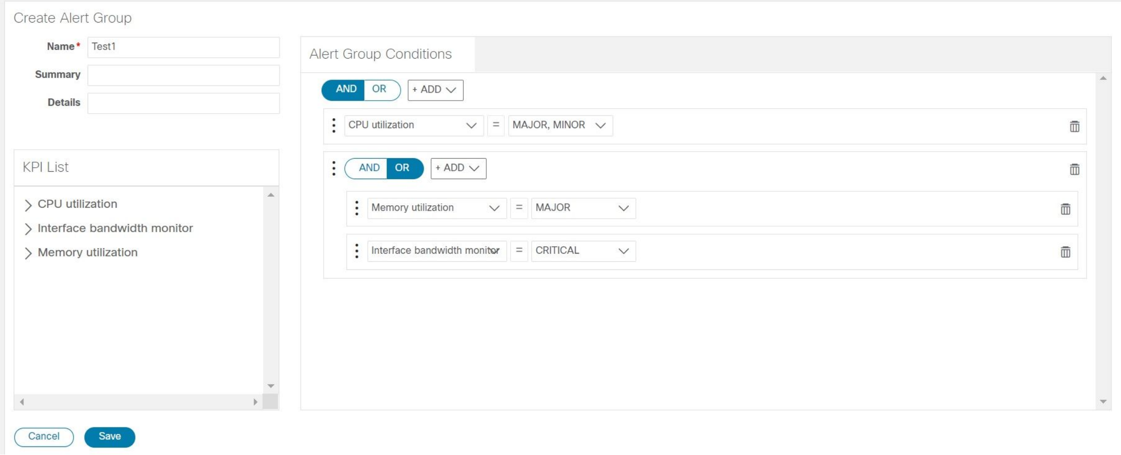
Note Configuring an alert provider enables the alerts from the group alert to be sent to a REST endpoint using Webhook registered in the alert provider.

Step 12 Provide a relevant entry in the **Name** field. **Summary** and **Details** are optional fields.

Step 13 The **Alert Group Conditions** area on the right side lets you select a logic gate (AND/OR) and add a KPI on which the logic is applied. Your alert group can be based on the alert criteria of a single KPI, or it can be a combination of mutliple KPI outputs. Click the desired logic (**AND** gate is selected by default), and click the **+ ADD** dropdown list to add an **Item** or a **Group**.

Item allows you to add individual KPI items and set the corresponding alert level, and **Group** allows you to add a nested alert group.

Step 14 Choose the desired KPI from the **Select KPI** dropdown, and select the desired level(s) for which the alerts need to be set for the chosen KPI. The alert levels are CRITICAL, MAJOR, MINOR, WARNING and INFO. Based on the logic gate and alert criteria you select, the output of the KPIs are evaluated and the alert is generated.


Create Alert Group

Name* Test1
Summary
Details

KPI List
- CPU utilization
- Interface bandwidth monitor
- Memory utilization

Alert Group Conditions

AND | OR | + ADD
- CPU utilization = MAJOR, MINOR
- AND | OR | + ADD
  - Memory utilization = MAJOR
  - Interface bandwidth monitor = CRITICAL

In the example shown above, the alert is set based on the output of two logic gates. The first logic gate is the output of an **OR** operation between the **Memory Utilization** and **Interface Bandwidth monitor** KPIs. If the set alert levels are met for either of the KPIs, the output of the first logic gate is set as true. This output is considered as the input for the second logic gate, which is an **AND** operation with the **CPU Utilization** KPI. If the alert levels of both the KPIs are met, the output of the second logic gate is set as true.

Step 15 Click **Save** to save the new alert group and display the **KPI Profiles** window. Click **Edit Details** or 🗑 to edit or delete an existing alert group respectively.

Enable KPI Profile on Devices

With Health Insights, you can enable and monitor the KPI Profiles in which you are interested. Instead of sifting through all the data that a given device can supply, you choose to monitor only the information relevant to the role the device plays in your network. Your network devices operate most efficiently when configured to only report data that specifically relates to the performance of its role in the network.

Some KPIs trigger alerts based on deviation from an established level of performance. For these types of KPIs, it is necessary to allow the system some annealing time in order to establish normal performance levels.

Important You can only enable KPI Profiles with MDT-based KPIs on a device that has been mapped to a Cisco Network Services Orchestrator (Cisco NSO) provider and attached to a Crosswork Data Gateway.

Note Do not enable KPI Profiles on devices that are not reachable.

Warning The load that is created on Cisco Crosswork Data Gateway and Crosswork Infrastructure caused by enabling KPI profiles on many devices or KPI profiles that gather a lot of data is hard to estimate. Crosswork provides a UI and API that allows you to see the current load and provides general guidelines for determining when you must refrain from enabling more collections until either other collections are disabled or more resources (CDG or worker nodes) are added. To check Cisco Crosswork Data Gateway load, see *Monitor Crosswork Data Gateway Health* at *Cisco Crosswork Infrastructure 4.3 and Applications Administration Guide*.

To enable KPI Profile on devices:

Step 1 From the main menu, choose **Performance Alerts** > **Enable/Disable KPI Profiles**. The **Devices** window is displayed.

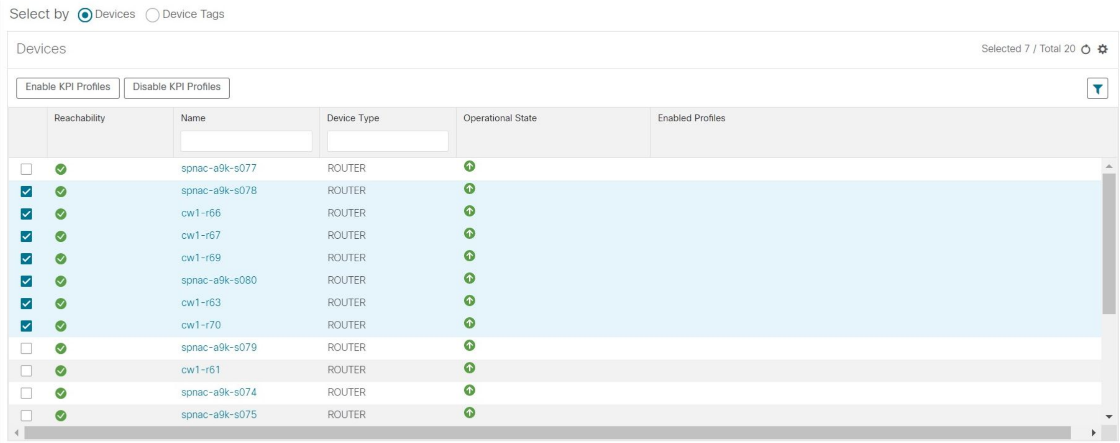
Step 2 Select the devices for which you want to enable KPI Profiles. You can click the **Device** or **Device Tags** buttons above the table on the left to toggle between selecting the devices by name or by tagged device group membership. Depending on your selection, the device list or the device tag list is displayed on the left.

If you choose to select by **Device**:

- Click ▼ in the table on the right. Type a **Name** or **Device Type** in the filter fields. As you type, the table displays only the devices whose name or type match the text that you typed.
- Click the check box next to the device(s) you want. You can select multiple devices at the same time.

If you choose to select by **Device Tags**:

- Type a tag name in the **Name** field to find a Device Group in the table. As you type, the table displays only the tag names that match the text you typed.
- Click the check box next to the group that you want. The names of all the devices in that group appear in the devices table on the right.



Select by ● Devices ○ Device Tags

Devices — Selected 7 / Total 20

	Reachability	Name	Device Type	Operational State	Enabled Profiles
□	✓	spnac-a9k-s077	ROUTER	↑	
☑	✓	spnac-a9k-s078	ROUTER	↑	
☑	✓	cw1-r66	ROUTER	↑	
☑	✓	cw1-r67	ROUTER	↑	
☑	✓	cw1-r69	ROUTER	↑	
☑	✓	spnac-a9k-s080	ROUTER	↑	
☑	✓	cw1-r63	ROUTER	↑	
☑	✓	cw1-r70	ROUTER	↑	
□	✓	spnac-a9k-s079	ROUTER	↑	
□	✓	cw1-r61	ROUTER	↑	
□	✓	spnac-a9k-s074	ROUTER	↑	
□	✓	spnac-a9k-s075	ROUTER	↑	

Note You cannot enable a KPI on the device that is attached to a standard Crosswork Data Gateway. It will show an error pop-up. Also, you cannot move a KPI-enabled device from extended Crosswork Data Gateway to standard Crosswork Data Gateway. It shows an error pop-up.

Step 3 Click **Enable KPI Profiles** to continue. Health Insights detects the selected devices, their types and models, and retrieves and analyzes their running configurations. The **KPI Profiles** window presents the KPI Profiles available for your selected devices.

Step 4 Choose the KPI Profiles that you want to enable by clicking the check box next to the KPI Profile name, and click **Next**.

The **Verify Details** window appears, listing all the KPI Profiles you have chosen to be enabled on the selected devices.

Step 5 (Optional) To get information about the KPIs included in the KPI Profile. Click the KPI Profile in the **Selected Profile(s)** table, and the content of the selected KPI Profile is displayed on the right side. Click **View More Details** to view the parameters of a specific KPI. A pop-up window provides the details of the KPI. Click the ✕ to close the pop-up window.

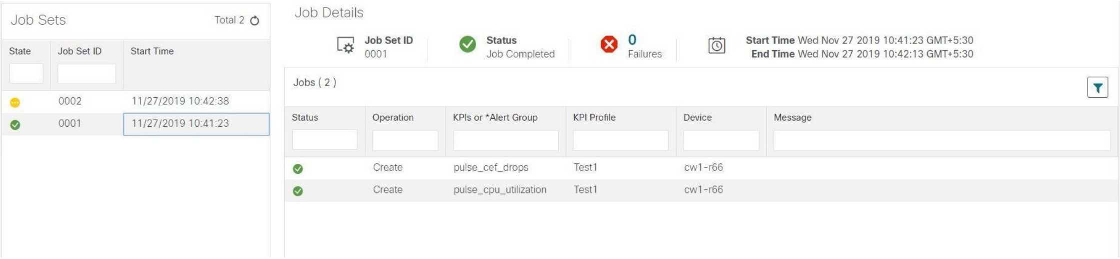
Step 6 To enable the selected KPI Profiles on the selected devices, click **Enable**. Health Insights schedules the KPI Profile(s) as a series of job sets.

Note The **Alert** flag for the KPI profile (click **Edit Details** on the relevant KPI) must be turned **ON** in order to trigger an alert when the data is collected.

Note Enabling a KPI results in configuring a collection job on the Crosswork Data Gateway. For GNMI-based and SNMP-based KPIs, the Crosswork Data Gateway polls the desired data and forwards it to Health Insights for processing and evaluation. For MDT-based KPIs, the devices (through NSO) are configured to push the data to the Crosswork Data Gateway which then forwards it to Health Insights for processing and evaluation.

Note In the **Device** table, in the **Enabled Profiles** column, you can click the number to see the status of the KPI collection job (for example to see if the KPI Profile ID is active or not).

Step 7 From the main menu, choose **Performance Alerts** > **KPI Job History** to watch the progress of each job set, as shown below. You should see job sets completing with a status of "Success". If job sets complete with a "Partial" or "Failed" status, be sure to read the job completion messages, and check that the selected devices are still reachable.



Job Sets — Total 2

State	Job Set ID	Start Time
●	0002	11/27/2019 10:42:38
✓	0001	11/27/2019 10:41:23

Job Details

Job Set ID 0001 | **Status** Job Completed | 0 Failures | **Start Time** Wed Nov 27 2019 10:41:23 GMT+5:30 **End Time** Wed Nov 27 2019 10:42:13 GMT+5:30

Jobs (2)

Status	Operation	KPIs or *Alert Group	KPI Profile	Device	Message
✓	Create	pulse_cef_drops	Test1	cw1-r66	
✓	Create	pulse_cpu_utilization	Test1	cw1-r66	

When the job sets complete successfully, the KPIs are now associated to the devices and the platform begins the process of enabling the relevant collection procedures for those network elements. In making these changes, you are automating the configuration of both the platform and the devices themselves to collect only the information required.

Step 8 From the main menu, choose **Administration** > **Collection Jobs** to look at the collection jobs and to make sure that they are created and the incoming data is collected.

Step 9 From the main menu, choose **Performance Alerts** > **Alert Dashboard**. The dashboard shows the alert status for the devices on which you have enabled KPI monitoring.

Note

- SNMP/MDT jobs may take more time than expected to reach the completed state when there is an increase in the number of devices, interfaces and KPIs.
- Enabling KPI profile per device takes around 3-5 seconds (but the time varies based on the number of KPIs being enabled). If the device is not reachable, it keeps trying until it is timed out. This may result in the job taking more time to reach the completed state.

Disable KPI Profile on Devices or Device Groups

You can use the **Enable/Disable KPI Profiles** window to disable the KPI Profiles running on device(s) or device groups.

Step 1 From the main menu, choose **Performance Alerts** > **Enable/Disable KPI Profiles**. The **Enable/Disable KPI Profiles** window is displayed.

Step 2 To disable KPIs enabled on one or more devices:

a) Click the **Device** button above the table on the left. The **Devices** table displays all the devices, with the total number of KPIs enabled on each device.

b) Click the check box next to the devices on which you want to disable KPIs.

If you select one device, you can disable all KPI Profiles for the device or just some of the KPI Profiles. If you select more than one device, you can only disable all KPIs for them.

c) Click **Disable KPI Profiles**. You will be prompted to confirm that you want to disable the KPIs running on all the selected devices. If you selected only one device, click the checkboxes next to the KPI Profiles you want to disable on that device, or click the checkbox at the top of the column to disable all the KPI Profiles running on that device. Click **Disable** to confirm.

Step 3 To disable all KPI Profiles enabled on all the devices within a device group:

a) Click the **Device Tags** button above the table on the left. The table displays the list of device tags.

b) Click the checkbox next to the device tag(s) used on the devices from which you no longer want to collect the KPI data.

When you select a device tag, the **Devices** table on the right shows all the devices that are associated with that tag. All of the devices are preselected.

c) Click **Disable KPI Profiles**. You will be prompted to confirm that you want to disable all the KPIs running on all the devices in the group. Click **Disable** to confirm.

Troubleshoot Health Insights

The following table describes issues that you may encounter when using the Health Insights application, and their solutions or workarounds.

Table 3: Health Insights Troubleshooting

Issue	Solution
Apply a KPI to a device fails with messages indicating that Cisco Network Services Orchestrator (Cisco NSO) and the target device are out of sync or otherwise out of communication. Message text will vary, but may include "device out of sync," "NC client timeout," and other text indicating that there are connectivity or sync issues between NSO and the device.	**1.** Go to **Performance Alerts** > **KPI Job History** and check the **Message** column for an error message. **2.** Go to **Device Management** > **Network Devices**. **3.** For the failed device, in the **NSO state** column, click ⓘ. **4.** From the **Check Sync** drop-down list, click **Sync From**. **5.** Confirm that the device is in sync now.
Health Insights not receiving data.	**1.** Confirm that the KPI configuration job completed without error: Go to **Performance Alerts** > **KPI Job History** **2.** Check the Collection/distribution status: Go to **Administration** > **Collection Jobs**. **3.** Check for the collection job to see if the table (accessed by clicking the graph icon for the job) indicates that data collections are processing.