Cisco Crosswork Network Controller 7.0 Closed-Loop Network Automation

First Published: 2024-08-28

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.

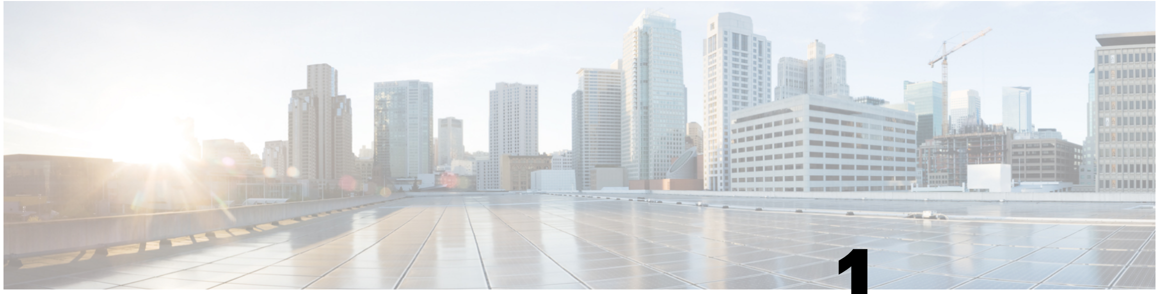
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY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

CONTENTS



CHAPTER 1

Overview

This section contains the following topics:

Audience

This guide is for experienced network administrators who want to use 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 Cisco Crosswork Infrastructure and how Crosswork applications are installed. For more information, see the Cisco Crosswork Network Controller Installation Guide.

Overview of Change Automation and Health Insights

Cisco Crosswork Health Insights and Cisco Crosswork Change Automation are components that can optionally be installed with Cisco Crosswork Network Controller (Crosswork Essentials or Crosswork Advantage).

The applications provide 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.

Change Automation

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

Health Insights

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 using the Cisco Crosswork APIs. For more details, see Cisco Crosswork Network Automation APIs.

Cisco Crosswork API

All the Cisco Crosswork Network Controller applications provide 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

Cisco Crosswork Health Insights and Cisco Crosswork Change Automation are components that can optionally be installed with Cisco Crosswork Network Controller. For more details on Crosswork Network Controller, see the Cisco Crosswork Network Controller Product page on Cisco.com.

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

- **Cisco Crosswork Planning**: Cisco Crosswork Planning provides traffic and topology analysis to Change Automation and Health Insights. It gives a cross-sectional view of traffic, topology, and equipment state. For more information, see Cisco Crosswork Planning.
- **Cisco Network Services Orchestrator (Cisco NSO)**: 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 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 Health Insights. For more information, see Cisco Crosswork Optimization Engine Data Sheet.
- **Non-Cisco Products**: Change Automation and Health Insights supports the loading of models for non-Cisco equipment which will enable the creation of KPIs and in some cases, the execution of plays. For more information on how to do these advanced integrations, see the Cisco Crosswork Network Controller Administration Guide and the Cisco Crosswork Network Controller API Documentation on Cisco DevNet. If you require assistance with these integration efforts, contact your account team.

CHAPTER 2

Get Started

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

Getting Started with Change Automation

This procedure covers the initial setup of the application post installation of the Change Automation and Health Insights applications. For more information, see the Cisco Crosswork Network Controller Installation Guide.

Change Automation can be used independently or as part of workflows that leverage Health Insights or other applications. In this procedure, we will present workflows that demonstrate some of these capabilities to illustrate the flexibility of the Crosswork solution. You can use these concepts and examples to build a virtually unlimited combination of tools to meet your operational needs.

Before you begin:

- Make sure to install the Change Automation and Health Insights applications. See the Cisco Crosswork Network Controller Installation Guide.
- Configure the Change Automation settings. See the Configure Change Automation Settings, on page 3.

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.

As you configure Change Automation settings, remember that Crosswork provides several ways to run Playbooks.

- Manually ("on demand") or via scheduled execution. These two methods are typically used for Playbooks that accomplish data collection, configuration changes, or SMU deployment independent of any KPI-related fault detected in the network.

- Manually or automatically when the Playbook is tied to a KPI. These methods are typically used when you want to run a Playbook intended to remediate a fault detected in the network. Key parameters needed to run the Playbook are populated when the alert tied to the KPI is triggered.

Note The Change Automation settings can only be configured once. If you want to modify the settings, Change Automation must be re-installed. Before re-installing, export any Plays or Playbooks you have created, and after re-installing, import them. For more information, see Export Plays, on page 21, Import Custom Plays, on page 22, Export Playbooks, on page 29, and Import Playbooks, on page 30.

System Settings

After you install Change Automation, check that you can access the Change Automation application from the main menu: Go to **Network Automation** > **Dashboard**. Crosswork displays the Change Automation window, prompting you to complete the Change Automation application's configuration.

Once initial setup is done, navigate to **Administration** > **Settings** > **System Settings** > **Network Automation** > **Device Override Credentials** to review the Change Automation settings:

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

  As you make these changes, please note the following special considerations:

  - If you want to enable automatic Playbook execution, you must ensure that **Playbook Job Scheduling** is **enabled** and that **Credential Prompt** is **disabled**. For more guidance, see Enable Automatic Playbook Execution, on page 4.
  - If **Credential Prompt** is **enabled**: 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 their accuracy.
  - If **Credential Prompt** is **disabled**: Only user IDs with write permissions for **Administration APIs** under **Change Automation** can complete the credential profile and provider setup tasks. If you are unsure if your user ID has the required privileges, you can check by selecting **Administration** > **Users and Roles** > **Roles** and inspecting the ID's privileges.
  - If **Playbook Job Scheduling** is **disabled**, the **Credential Prompt** is **enabled** by default. You cannot disable the credential prompt if you disable Playbook job scheduling.

- Click **Save** after you configure the above settings.

Enable Automatic Playbook Execution

In addition to running KPI-linked Playbooks manually, at the network operator's discretion, Change Automation and Health Insights permits you to run one or more of your KPI-linked Playbooks automatically whenever the KPI linked to that Playbook raises an alert of sufficient severity.

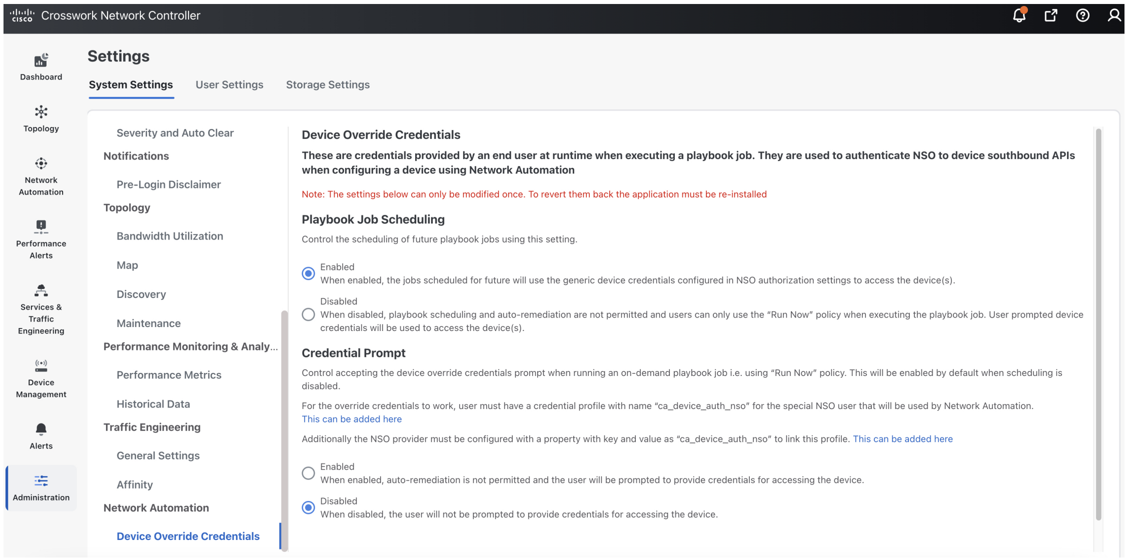
To enable this option, **Playbook Job Scheduling** must be **enabled**, and **Credential Prompt** must be **disabled**. As noted above, you must have Crosswork system administrator privileges to change these settings.

> **Warning** Once these settings are saved, changes cannot be made unless you first use the Crosswork Manager to uninstall and then reinstall both the Change Automation and Health Insights applications.

1. From the main menu, choose **Administration** > **Settings** > **System Settings** > **Network Automation** > **Device Override Credentials**. The **Device Override Credentials** page opens.
2. Under **Playbook Job Scheduling**, click the **Enabled** button. Under **Credential Prompt** click the **Disabled** radio button.

   When you are finished, the window should look like the illustration below.

   Figure 1: System Settings



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, playbook scheduling and auto-remediation are not permitted and 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, auto-remediation is not permitted and 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.

3. Click **Save** to commit to these settings.

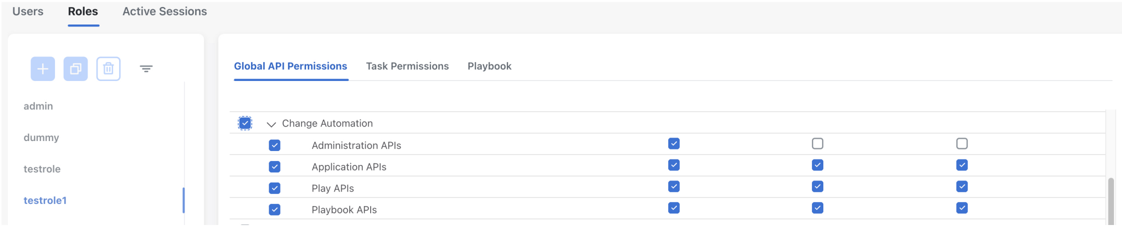
Assign Change Automation User Access Levels

Once the Change Automation system settings are completed, an admin user must review other user roles to ensure that all the users who need them have the proper level of access to run, import, and create Plays and Playbooks. Only users with write permissions for **Administration APIs** can disable or enable Playbook execution access and assign labels.

To provide this access, the admin user must:

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

Figure 2: Global API Permissions



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

Using Change Automation

The following table describes the steps to start using the Change Automation application once you have configured the Change Automation settings.

Table 1: Getting started with Change Automation

Workflow	Action
1. Run the Playbooks manually with the available Playbooks.	See About Running Playbooks
2. Schedule Playbooks to perform routine maintenance.	See Schedule Playbooks
3. If any existing Plays or Playbooks do not meet the requirements fully or partially, build new Plays or Playbooks with new or existing Plays, as necessary.	See Develop Custom Playbooks
4. Link a Playbook to a Health Insights triggered KPIs	See Closed-Loop Automation

Schedule Playbooks

The workflow below describes the steps to follow when using Change Automation to automate routine network tasks and verify that each routine change is 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 3.

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 Change Automation Playbooks.	See About Running Playbooks, on page 31 and View the Playbook List, on page 15.
2. Configure Playbooks to perform these tasks at the desired time.	See About Running Playbooks, on page 31 and Schedule Playbook Runs, on page 51.

Step	Action
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 54 and View or Abort Playbook Jobs, on page 53.

Develop Custom Playbooks

The following workflow describes the steps to follow when developing a Change Automation custom Play or Playbook.

Step	Action
1. Review the existing Plays and Playbooks to see if they fully or partially meet your needs.	From the main menu, choose **Network Automation** > **Play List** or **Playbook List**.
2. If required, build new plays and then a new Playbook with new or existing Plays, as necessary, to meet your requirements.	See About Custom Plays, on page 17 and About Customizing Playbooks, on page 23.
3. For a Playbook you have developed that meets your needs, you can optionally: • Link to a KPI for manual or automated execution. • Schedule the playbook to run automatically. • Manually run the playbook as needed.	See: • Link KPIs to Playbooks and Run Them Manually, on page 67 • Link KPIs to Playbooks and Run Them Automatically, on page 69 • About Running Playbooks, on page 31 • Schedule Playbook Runs, on page 51

Getting Started with Health Insights

Before you begin:

Make sure to confirm if the Yang modules we have provided include the data point you want to evaluate. If yes, then review whether the available KPI templates are adequate to evaluate the data point.

If the Yang module has the data you need and we have an existing KPI, you can create a new KPI profile.

If the Yang module has the data that you need and doesn't have an existing KPI, then you can build a new KPI.

Build a new KPI based on the below requirements:

- If the data you want to gather can be collected or evaluated using one of the four templates we provide, then build the KPI.

- If the data you want to gather can not be collected or evaluated using one of the four templates we provide, then build a new KPI with the tools available in the developer network (developer.cisco.com).

In the instance, if the module does not include the data point that you need, you have to get the new Yang module and load it on the data collection UI and then you can build KPI.

The following table describes the steps to get started with Health Insights application.

Table 2: Getting started with Health Insights

Workflow	Actions
1. Create KPI Profiles to monitor device Key Performance Indicators (KPIs) for issues and anomalies.	See Monitor Key Performance Indicators
2. Enable KPI profiles for the devices.	See Enable KPI Profiles on Devices
3. Make sure that the collections are provisioned on the device (MDT collections).	See Verify the Deployment Status of Enabled KPIs
4. Make sure collections are gathering data.	

Monitor Key Performance Indicators

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

Step	Action
1. (Optional) Tag all the devices whose KPIs you plan to monitor with a tag indicating the function they perform, per your plan.	See Manage Tags in the Cisco Crosswork Network Controller Administration Guide.
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.	See List of Health Insights KPIs, on page 58. To create a new KPI that fits your requirements, 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.	See Create a New KPI Profile, on page 72.
4. Enable the appropriate KPI Profiles on the devices you want to monitor.	See Enable KPI Profiles on Devices, on page 75.

Develop Custom KPIs

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

Step	Action
1. Review the existing KPIs to ensure the telemetry you want to monitor is not already available.	See List of Health Insights KPIs, on page 58.
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, we must load a new Yang module.	See Create a New KPI, on page 65.
3. Determine if the Yang module we have provided includes the data point you wish to evaluate. If it does, determine whether one of the available KPI templates can evaluate it. If it can, proceed with building a new KPI. If not, you must build the KPI with the tools available in the dev network (developer.cisco.com) and then import it into Crosswork. Once you import the KPI, you can add it to your profile. If the module does not include the data point you need, you have to get the new Yang module and load it on the data collection UI, and then you can build the KPI.	
4. 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 72.
5. Enable the new KPI Profile on a test device.	See Enable KPI Profiles on Devices, on page 75.
6. Confirm that collections are working.	
7. Confirm that the data reported matches your expectations and, if necessary, investigate the alarms raised by the new KPI. Be aware that KPIs that depend on data over time to establish baseline performance will need some time to establish a baseline before they provide meaningful data.	See View Alerts for Network Devices, on page 81.
8. If the KPI Profile meets expectations, enable it on all devices where applicable. **Warning** When enabling KPI profiles on many devices, ensure that sufficient capacity is available on Cisco Crosswork Data Gateway. If adequate capacity is not available and if you enable the KPI profiles on a 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 Profiles on Devices, on page 75.
9. Make sure the KPI Profile was deployed on the device (MDT only) and that the collection jobs are functioning.	See Verify the Deployment Status of Enabled KPIs, on page 77.

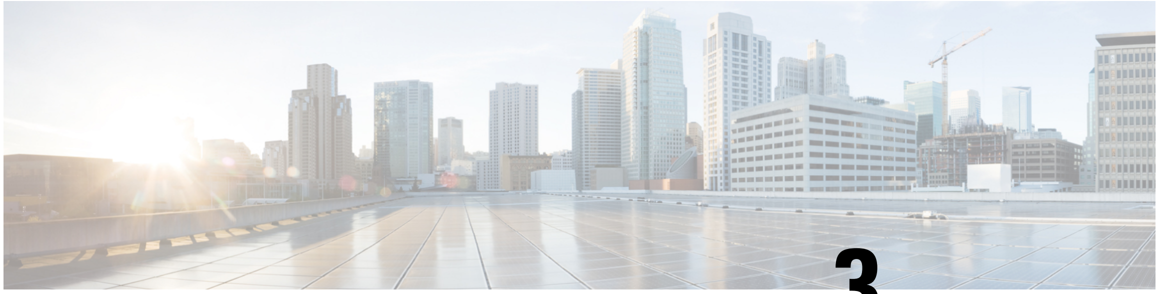
Closed-Loop Automation

The following workflow describes the steps to follow when using Health Insights to run a remediation Playbook from Change Automation in response to the performance challenges detected in the network by a KPI. A remediation Playbook can be:

- Linked to a KPI, alerting the operator to run the Playbook and make the remediation easier.
- Linked to a KPI and selected for automatic execution without operator intervention.

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 81 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 Play Using Templates, on page 17 and Create a Custom Playbook Through the UI, on page 23.
3. Try out the selected Playbooks and see if they are applicable to your purposes. As you experiment, adjust the Playbook parameters as needed.	See: Perform a Dry Run of a Playbook, on page 33 Run Playbooks In Single Stepping Mode, on page 39 Run Playbooks In Continuous Mode, on page 45
4. If required, build new plays and then build new playbooks with the combination of plays needed to make the desired change(s) to the network.	See Create a Custom Play Using Templates, on page 17 and Create a Custom Playbook Through the UI, on page 23.
5. (Optional) For frequently triggered KPIs with a known remediation Playbook, link the Playbook to the KPI to make executing the Playbook easier for the operator.	Follow the steps for linking and triggering Playbook runs under operator control in Link KPIs to Playbooks and Run Them Manually, on page 67. Use the Remediation icon shown in View Alerts for Network Devices, on page 81 to trigger a run of a linked Playbook from a device or KPI alert.

Step	Action
6. (Optional) For frequently triggered KPIs with a known remediation Playbook and no danger of runaway execution, link the Playbook to the KPI and set it to run automatically.	Follow the steps in Link KPIs to Playbooks and Run Them Automatically, on page 69 to trigger an automatic run of a linked Playbook upon receipt of a device or KPI alert.



CHAPTER 3

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 consist 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.

Change Automation, in conjunction with health insights, allows operators to build automation in 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 from 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 they fully or partially meet your needs.

> **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 some combination of existing Plays accomplishes the task, build a new Playbook using those 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 performs as expected.
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 17 and About Customizing Playbooks, on page 23.

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.

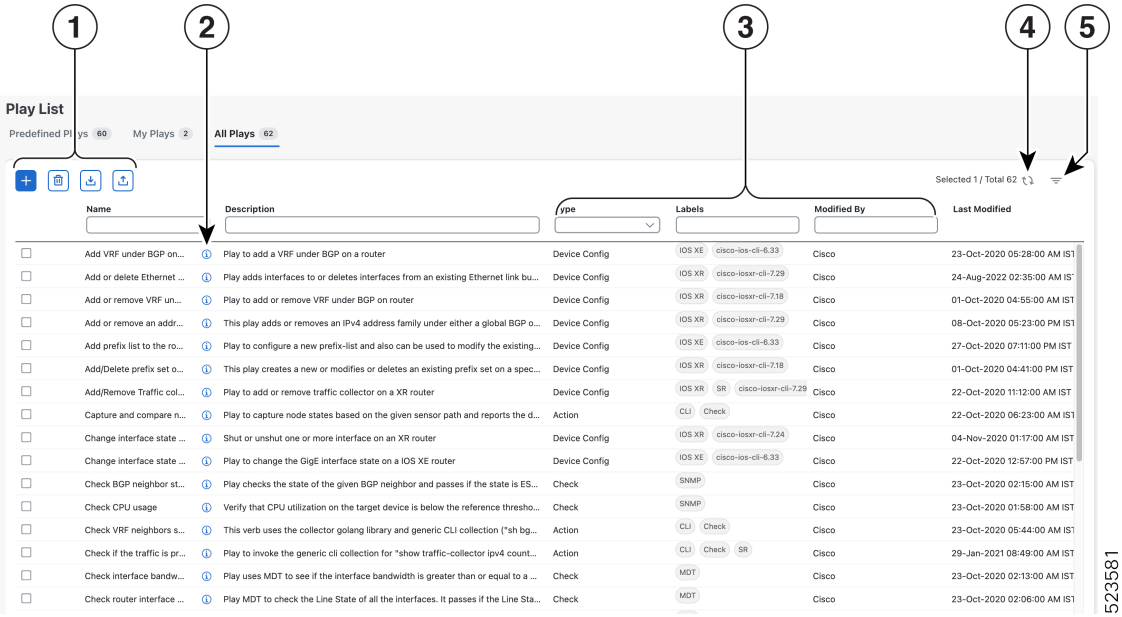
For more information, see Configure Change Automation Settings.

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.

Figure 3: Play List



Play List

Predefined Pl ys 60 | My Plays 2 | All Plays 62

Selected 1 / Total 62

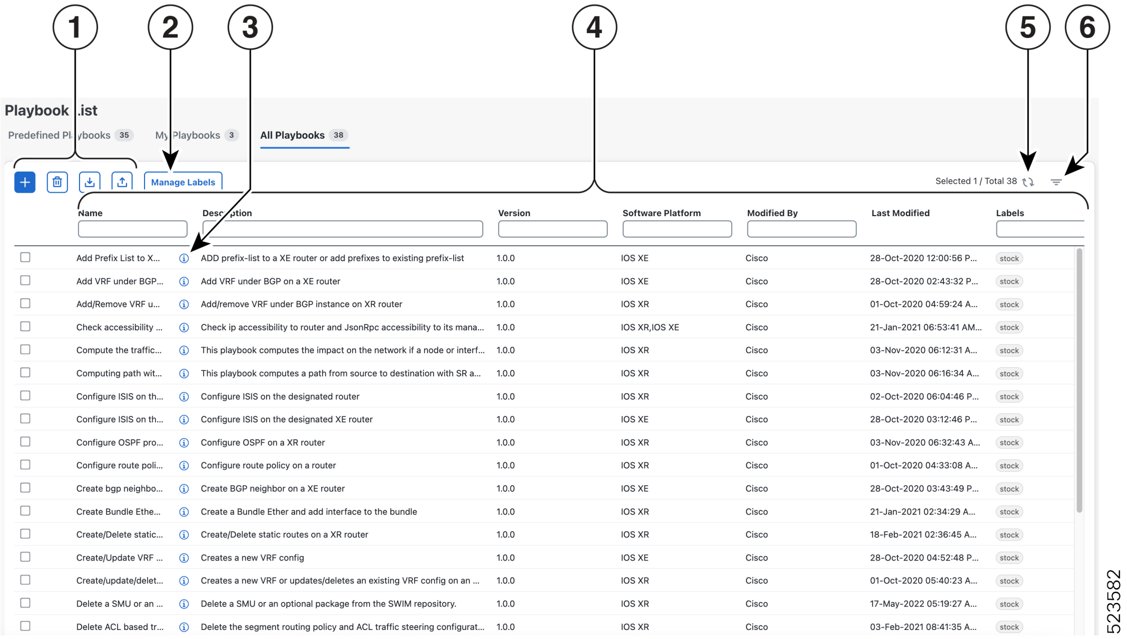
	Name		Description	ype	Labels	Modified By	Last Modified
☐	Add VRF under BGP on...	ⓘ	Play to add a VRF under BGP on a router	Device Config	IOS XE cisco-ios-cli-6.33	Cisco	23-Oct-2020 05:28:00 AM IST
☐	Add or delete Ethernet ...	ⓘ	Play adds interfaces to or deletes interfaces from an existing Ethernet link bu...	Device Config	IOS XR cisco-iosxr-cli-7.29	Cisco	24-Aug-2022 02:35:00 AM IST
☐	Add or remove VRF un...	ⓘ	Play to add or remove VRF under BGP on router	Device Config	IOS XR cisco-iosxr-cli-7.18	Cisco	01-Oct-2020 04:55:00 AM IST
☐	Add or remove an addr...	ⓘ	This play adds or removes an IPv4 address family under either a global BGP o...	Device Config	IOS XR cisco-iosxr-cli-7.29	Cisco	08-Oct-2020 05:23:00 PM IST
☐	Add prefix list to the ro...	ⓘ	Play to configure a new prefix-list and also can be used to modify the existing...	Device Config	IOS XE cisco-ios-cli-6.33	Cisco	27-Oct-2020 07:11:00 PM IST
☐	Add/Delete prefix set o...	ⓘ	This play creates a new or modifies or deletes an existing prefix set on a spec...	Device Config	IOS XR cisco-iosxr-cli-7.18	Cisco	01-Oct-2020 04:41:00 PM IST
☐	Add/Remove Traffic col...	ⓘ	Play to add or remove traffic collector on a XR router	Device Config	IOS XR SR cisco-iosxr-cli-7.29	Cisco	22-Oct-2020 11:12:00 AM IST
☐	Capture and compare n...	ⓘ	Play to capture node states based on the given sensor path and reports the d...	Action	CLI Check	Cisco	22-Oct-2020 06:23:00 AM IST
☐	Change interface state ...	ⓘ	Shut or unshut one or more interface on an XR router	Device Config	IOS XR cisco-iosxr-cli-7.24	Cisco	04-Nov-2020 01:17:00 AM IST
☐	Change interface state ...	ⓘ	Play to change the GigE interface state on a IOS XE router	Device Config	IOS XE cisco-ios-cli-6.33	Cisco	22-Oct-2020 12:57:00 PM IST
☐	Check BGP neighbor st...	ⓘ	Play checks the state of the given BGP neighbor and passes if the state is ES...	Check	SNMP	Cisco	23-Oct-2020 02:15:00 AM IST
☐	Check CPU usage	ⓘ	Verify that CPU utilization on the target device is below the reference thresho...	Check	SNMP	Cisco	23-Oct-2020 01:58:00 AM IST
☐	Check VRF neighbors s...	ⓘ	This verb uses the collector golang library and generic CLI collection ("sh bg...	Action	CLI Check	Cisco	23-Oct-2020 05:44:00 AM IST
☐	Check if the traffic is pr...	ⓘ	Play to invoke the generic cli collection for "show traffic-collector ipv4 count...	Action	CLI Check SR	Cisco	29-Jan-2021 08:49:00 AM IST
☐	Check interface bandw...	ⓘ	Play uses MDT to see if the interface bandwidth is greater than or equal to a ...	Check	MDT	Cisco	23-Oct-2020 02:13:00 AM IST
☐	Check router interface ...	ⓘ	Play MDT to check the Line State of all the interfaces. It passes if the Line Sta...	Check	MDT	Cisco	23-Oct-2020 02:06:00 AM IST

Item	Description
1	Click + to create a custom Play. See Create a Custom Play Using Templates, on page 17.
	Click 🗑 to delete a custom Play. See Delete Custom Plays, on page 22.
	Click ⤓ to import a custom Play from a gzipped TAR archive file. See Import Custom Plays, on page 22.
	Click ⤒ to export a custom Play as a gzipped TAR archive file. See Export Plays, on page 21.
2	Click ⓘto see a pop-up **Play Details** window showing the Play's description and schema. When you are finished viewing these details, click × or the **Close** button 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 using 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 ⊗ 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**.

Figure 4: Playbook List



	Name		Description	Version	Software Platform	Modified By	Last Modified	Labels
□	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	28-Oct-2020 12:00:56 P...	stock
□	Add VRF under BGP...	ⓘ	Add VRF under BGP on a XE router	1.0.0	IOS XE	Cisco	28-Oct-2020 02:43:32 P...	stock
□	Add/Remove VRF u...	ⓘ	Add/remove VRF under BGP instance on XR router	1.0.0	IOS XR	Cisco	01-Oct-2020 04:59:24 A...	stock
□	Check accessibility ...	ⓘ	Check ip accessibility to router and JsonRpc accessibility to its mana...	1.0.0	IOS XR,IOS XE	Cisco	21-Jan-2021 06:53:41 AM...	stock
□	Compute the traffic...	ⓘ	This playbook computes the impact on the network if a node or interf...	1.0.0	IOS XR	Cisco	03-Nov-2020 06:12:31 A...	stock
□	Computing path wit...	ⓘ	This playbook computes a path from source to destination with SR a...	1.0.0	IOS XR	Cisco	03-Nov-2020 06:16:34 A...	stock
□	Configure ISIS on th...	ⓘ	Configure ISIS on the designated router	1.0.0	IOS XR	Cisco	02-Oct-2020 06:04:46 P...	stock
□	Configure ISIS on th...	ⓘ	Configure ISIS on the designated XE router	1.0.0	IOS XE	Cisco	28-Oct-2020 03:12:46 P...	stock
□	Configure OSPF pro...	ⓘ	Configure OSPF on a XR router	1.0.0	IOS XR	Cisco	03-Nov-2020 06:32:43 A...	stock
□	Configure route poli...	ⓘ	Configure route policy on a router	1.0.0	IOS XR	Cisco	01-Oct-2020 04:33:08 A...	stock
□	Create bgp neighbo...	ⓘ	Create BGP neighbor on a XE router	1.0.0	IOS XE	Cisco	28-Oct-2020 03:43:49 P...	stock
□	Create Bundle Ethe...	ⓘ	Create a Bundle Ether and add interface to the bundle	1.0.0	IOS XR	Cisco	21-Jan-2021 02:34:29 A...	stock
□	Create/Delete static...	ⓘ	Create/Delete static routes on a XR router	1.0.0	IOS XR	Cisco	18-Feb-2021 02:36:45 A...	stock
□	Create/Update VRF ...	ⓘ	Creates a new VRF config	1.0.0	IOS XE	Cisco	28-Oct-2020 04:52:48 P...	stock
□	Create/update/delet...	ⓘ	Creates a new VRF or updates/deletes an existing VRF config on an ...	1.0.0	IOS XR	Cisco	01-Oct-2020 05:40:23 A...	stock
□	Delete a SMU or an ...	ⓘ	Delete a SMU or an optional package from the SWIM repository.	1.0.0	IOS XR	Cisco	17-May-2022 05:19:27 A...	stock
□	Delete ACL based tr...	ⓘ	Delete the segment routing policy and ACL traffic steering configurat...	1.0.0	IOS XR	Cisco	03-Feb-2021 08:41:35 A...	stock

Item	Description
1	Click + to create a custom Playbook. See Create a Custom Playbook Through the UI, on page 23.
	Click 🗑 to delete the currently selected custom Playbook. See Delete Custom Playbooks, on page 30.
	Click ⤓ to import Playbooks from a gzipped TAR archive file. See Import Playbooks, on page 30.
	Click ⤒ to export the currently selected Playbook(s) as a gzipped TAR archive file. See Export Playbooks, on page 29.
2	Click **Manage Labels** to assign a label(s) to the Playbook. Assigning label(s) to the Playbooks allows the system administrator 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 × or the **Close** button to close the pop-up window.
4	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 for any column.
5	Click ⟲ to refresh the Playbooks list.

Item	Description
6	Click ≡ to set filter criteria on one or more columns in the table.
	Click ⊗ to clear any filter criteria you may have set.

About Custom Plays

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

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

- **Check Play**: Verifies the data from your devices using a logical expression.
- **Data Collection Play**: Collects data from your devices.
- **Device Config Play**: Performs configuration changes on your device
- **Service Play**: 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 supports MDT and SNMP collection.

Create a Custom Play Using Templates

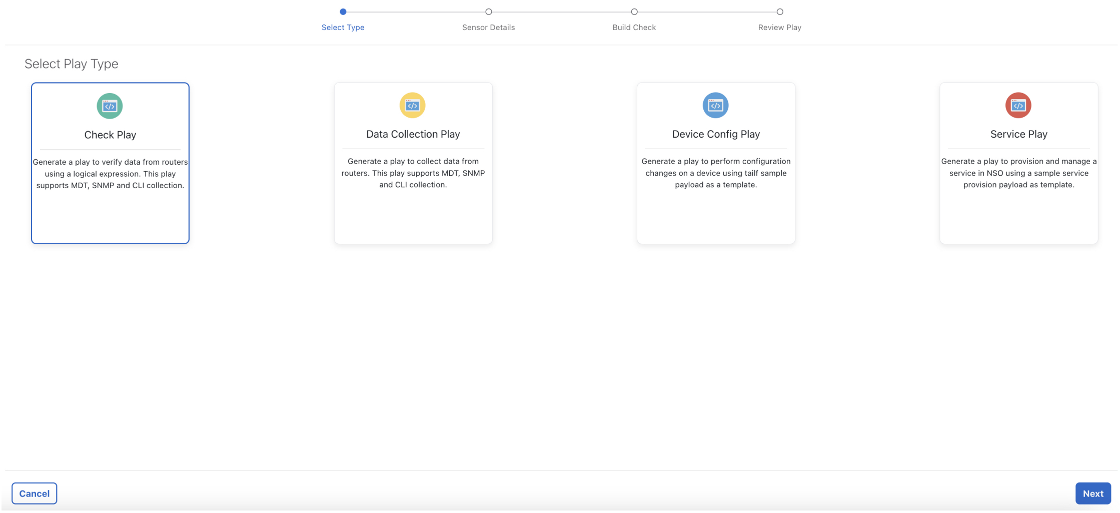
This section explains the procedure to create a custom Play. The stages of Play creation vary depending on the Play type you choose:

- **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.

Figure 5: Select Play Type



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.

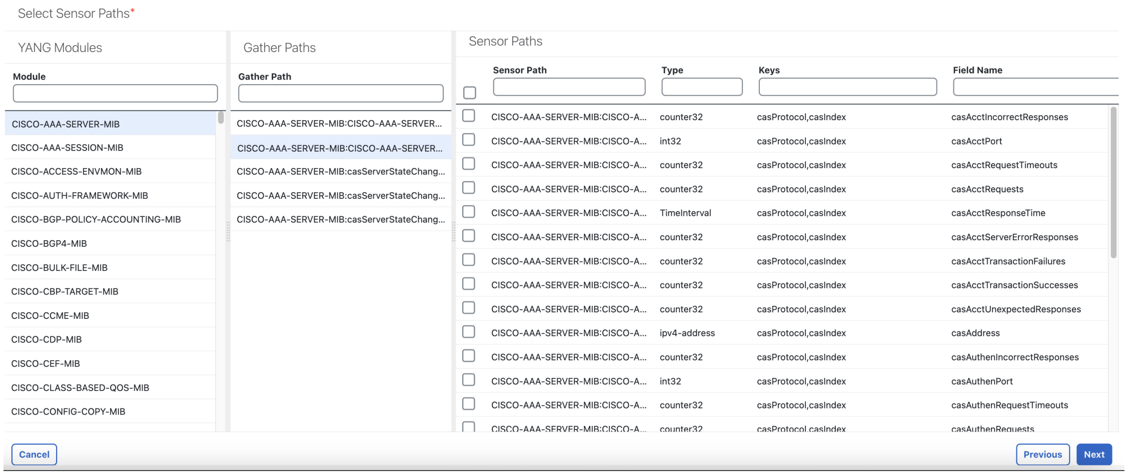
Select the Play type that you want to create and click **Next**.

Step 3 Creating a Check Play or Data Collection Play

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 the topic Manage Device Packages in the Cisco Crosswork Network Controller Administration Guide.

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

Figure 6: Select Sensor Paths



Select Sensor Paths*

YANG Modules

Module
CISCO-AAA-SERVER-MIB
CISCO-AAA-SESSION-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-CCME-MIB
CISCO-CDP-MIB
CISCO-CEF-MIB
CISCO-CLASS-BASED-QOS-MIB
CISCO-CONFIG-COPY-MIB

Gather Paths

Gather Path
CISCO-AAA-SERVER-MIB:CISCO-AAA-SERVER...
CISCO-AAA-SERVER-MIB:CISCO-AAA-SERVER...
CISCO-AAA-SERVER-MIB:casServerStateChang...
CISCO-AAA-SERVER-MIB:casServerStateChang...
CISCO-AAA-SERVER-MIB:casServerStateChang...

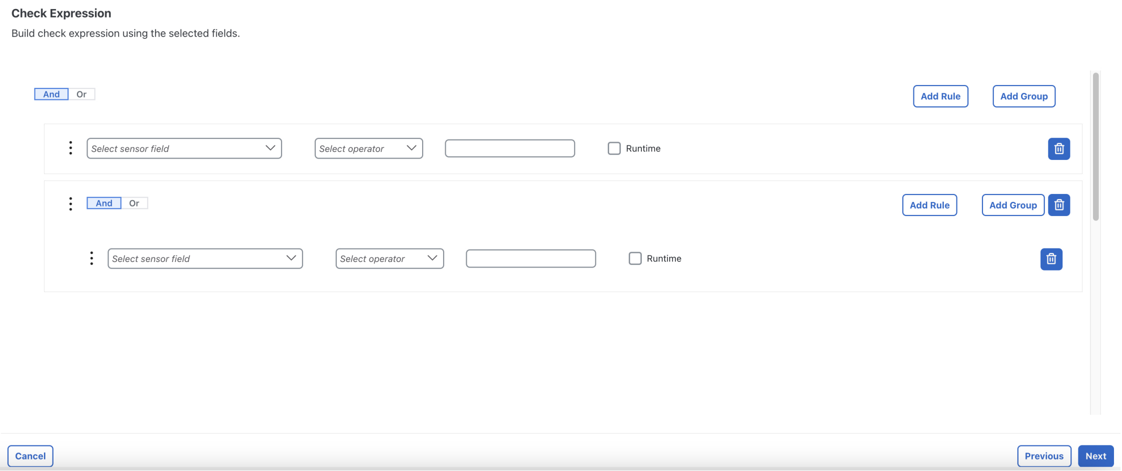
Sensor Paths

□	Sensor Path	Type	Keys	Field Name
□	CISCO-AAA-SERVER-MIB:CISCO-A...	counter32	casProtocol,casIndex	casAcctIncorrectResponses
□	CISCO-AAA-SERVER-MIB:CISCO-A...	int32	casProtocol,casIndex	casAcctPort
□	CISCO-AAA-SERVER-MIB:CISCO-A...	counter32	casProtocol,casIndex	casAcctRequestTimeouts
□	CISCO-AAA-SERVER-MIB:CISCO-A...	counter32	casProtocol,casIndex	casAcctRequests
□	CISCO-AAA-SERVER-MIB:CISCO-A...	TimeInterval	casProtocol,casIndex	casAcctResponseTime
□	CISCO-AAA-SERVER-MIB:CISCO-A...	counter32	casProtocol,casIndex	casAcctServerErrorResponses
□	CISCO-AAA-SERVER-MIB:CISCO-A...	counter32	casProtocol,casIndex	casAcctTransactionFailures
□	CISCO-AAA-SERVER-MIB:CISCO-A...	counter32	casProtocol,casIndex	casAcctTransactionSuccesses
□	CISCO-AAA-SERVER-MIB:CISCO-A...	counter32	casProtocol,casIndex	casAcctUnexpectedResponses
□	CISCO-AAA-SERVER-MIB:CISCO-A...	ipv4-address	casProtocol,casIndex	casAddress
□	CISCO-AAA-SERVER-MIB:CISCO-A...	counter32	casProtocol,casIndex	casAuthenIncorrectResponses
□	CISCO-AAA-SERVER-MIB:CISCO-A...	int32	casProtocol,casIndex	casAuthenPort
□	CISCO-AAA-SERVER-MIB:CISCO-A...	counter32	casProtocol,casIndex	casAuthenRequestTimeouts
□	CISCO-AAA-SERVER-MIB:CISCO-A...	counter32	casProtocol,casIndex	casAuthenRequests

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 the **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.

Figure 7: Check Expression



Check Expression

Build check expression using the selected fields.

Click **Next** to continue.

Step 4 Creating a Device Config Play or Service Play

Ensure that the configuration you are trying to create is available in NSO; otherwise, it will show an error.

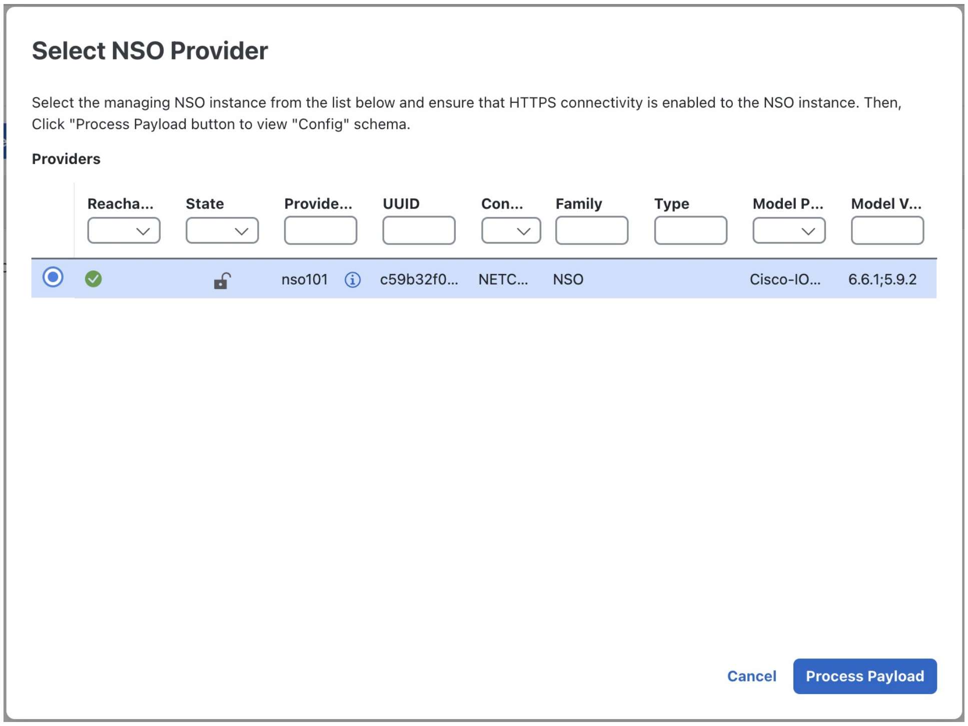
When creating a Service Play, you are not creating a new service for NSO but creating a Play to manage and provision an existing service in one or more NSO instances. For more information, see https://developer.cisco.com/docs/nso/.

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**.

Figure 8: Select NSO Provider



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.

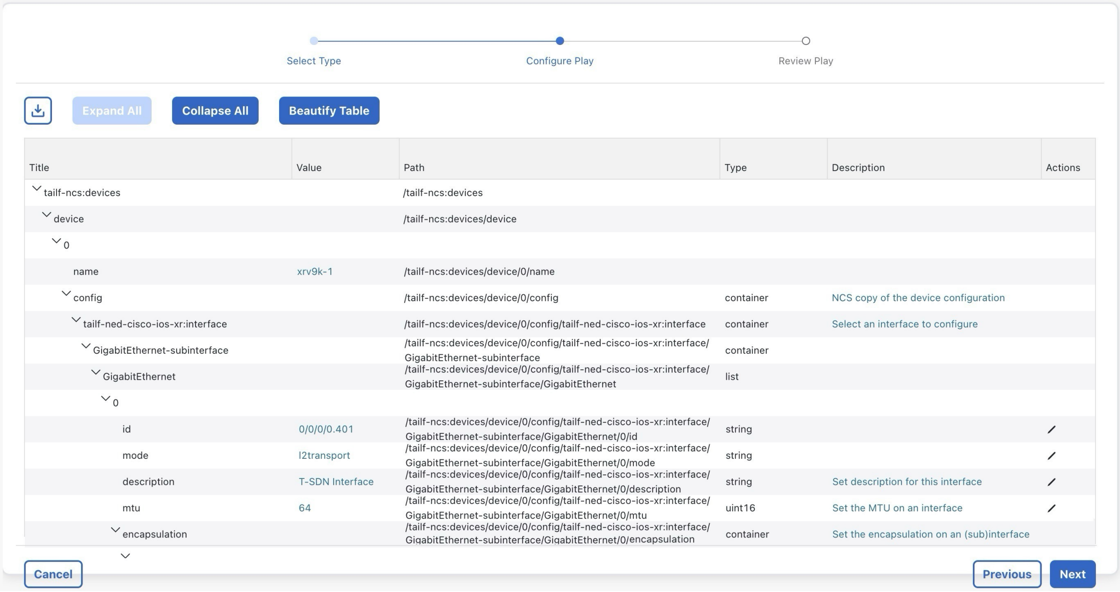
Providers

	Reacha...	State	Provide...	UUID	Con...	Family	Type	Model P...	Model V...
●	✓	🔓	nso101 ⓘ	c59b32f0...	NETC...	NSO		Cisco-IO...	6.6.1;5.9.2

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.

Figure 9: Configure Play



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-subinterface		/tailf-ncs:devices/device/0/config/tailf-ned-cisco-ios-xr:interface/GigabitEthernet-subinterface	container		
GigabitEthernet		/tailf-ncs:devices/device/0/config/tailf-ned-cisco-ios-xr:interface/GigabitEthernet-subinterface/GigabitEthernet	list		
0					
id	0/0/0/0.401	/tailf-ncs:devices/device/0/config/tailf-ned-cisco-ios-xr:interface/GigabitEthernet-subinterface/GigabitEthernet/0/id	string		✎
mode	l2transport	/tailf-ncs:devices/device/0/config/tailf-ned-cisco-ios-xr:interface/GigabitEthernet-subinterface/GigabitEthernet/0/mode	string		✎
description	T-SDN Interface	/tailf-ncs:devices/device/0/config/tailf-ned-cisco-ios-xr:interface/GigabitEthernet-subinterface/GigabitEthernet/0/description	string	Set description for this interface	✎
mtu	64	/tailf-ncs:devices/device/0/config/tailf-ned-cisco-ios-xr:interface/GigabitEthernet-subinterface/GigabitEthernet/0/mtu	uint16	Set the MTU on an interface	✎
encapsulation		/tailf-ncs:devices/device/0/config/tailf-ned-cisco-ios-xr:interface/GigabitEthernet-subinterface/GigabitEthernet/0/encapsulation	container	Set the encapsulation on an (sub)interface	

Click **Next** to continue.

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

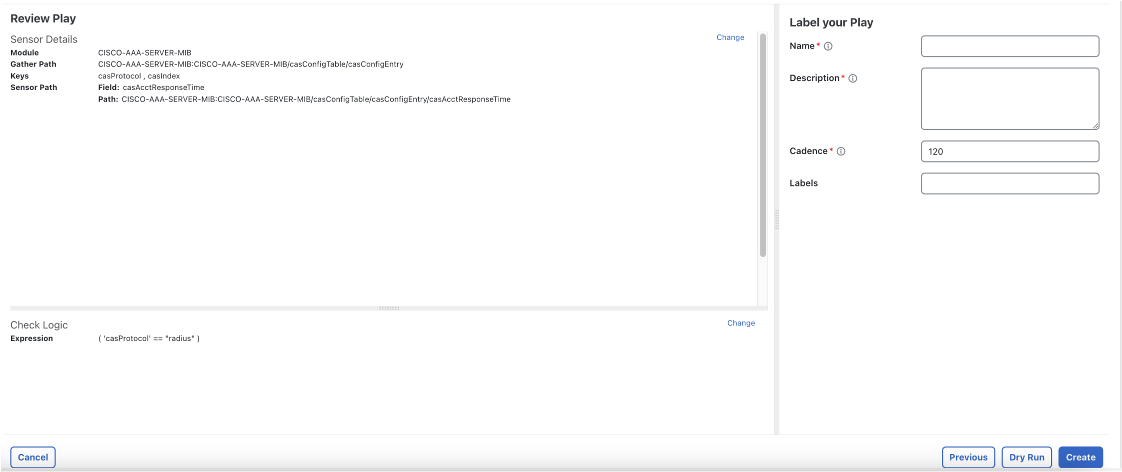
Label your Play with a unique **Name** and **Description**.

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 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 with which you can use the Play. 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) when you add them.

Figure 10: Review Play



Review Play

Sensor Details

Module CISCO-AAA-SERVER-MIB
Gather Path CISCO-AAA-SERVER-MIB:CISCO-AAA-SERVER-MIB/casConfigTable/casConfigEntry
Keys casProtocol , casIndex
Sensor Path **Field:** casAcctResponseTime
Path: CISCO-AAA-SERVER-MIB:CISCO-AAA-SERVER-MIB/casConfigTable/casConfigEntry/casAcctResponseTime

Check Logic

Expression ('casProtocol' == "radius")

Label your Play

Name *
Description *
Cadence * 120
Labels

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 authored or imported by you or another user into Change Automation.

The exported archive contains only the user-customizable files listed in Playbook Components and Files, on page 23. 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 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 you do not accidentally overwrite the custom Plays you created.

Before you begin

To import Plays, a user must have write access. For more information about granting a user read-write role access, see Configure Change Automation Settings, on page 3.

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 are 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 will fail.

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 you want to delete.

Step 3 Click the 🗑 icon.

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

About Customizing Playbooks

You can create your own Playbooks from scratch, based on details from Cisco-supplied Playbooks. You 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 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 the:

- "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 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

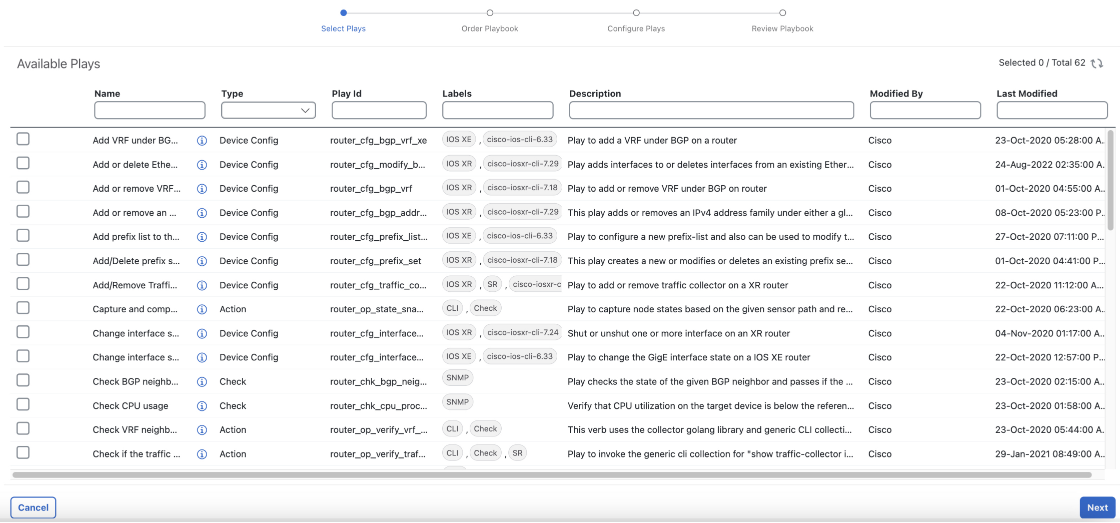
Change Automation allows users with admin and read/write roles to create custom Playbooks using the available Plays. For more information about granting read/write role access to a user, see the section "Assign Change Automation User Access Levels" in the topic Configure Change Automation Settings, on page 3.

Note You cannot edit a custom Playbook once it is created. We recommend that you perform a dry run of the Playbook *before completing the creation* to ensure that the Playbook's purpose 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.

Figure 11: Select plays



Available Plays

Selected 0 / Total 62

	Name		Type	Play Id	Labels	Description	Modified By	Last Modified
□	Add VRF under BG...	ⓘ	Device Config	router_cfg_bgp_vrf_xe	IOS XE , cisco-ios-cli-6.33	Play to add a VRF under BGP on a router	Cisco	23-Oct-2020 05:28:00 A...
□	Add or delete Ethe...	ⓘ	Device Config	router_cfg_modify_b...	IOS XR , cisco-iosxr-cli-7.29	Play adds interfaces to or deletes interfaces from an existing Ether...	Cisco	24-Aug-2022 02:35:00 A...
□	Add or remove VRF...	ⓘ	Device Config	router_cfg_bgp_vrf	IOS XR , cisco-iosxr-cli-7.18	Play to add or remove VRF under BGP on router	Cisco	01-Oct-2020 04:55:00 A...
□	Add or remove an ...	ⓘ	Device Config	router_cfg_bgp_addr...	IOS XR , cisco-iosxr-cli-7.29	This play adds or removes an IPv4 address family under either a gl...	Cisco	08-Oct-2020 05:23:00 P...
□	Add prefix list to th...	ⓘ	Device Config	router_cfg_prefix_list...	IOS XE , cisco-ios-cli-6.33	Play to configure a new prefix-list and also can be used to modify t...	Cisco	27-Oct-2020 07:11:00 P...
□	Add/Delete prefix s...	ⓘ	Device Config	router_cfg_prefix_set	IOS XR , cisco-iosxr-cli-7.18	This play creates a new or modifies or deletes an existing prefix se...	Cisco	01-Oct-2020 04:41:00 P...
□	Add/Remove Traffi...	ⓘ	Device Config	router_cfg_traffic_co...	IOS XR , SR , cisco-iosxr-c	Play to add or remove traffic collector on a XR router	Cisco	22-Oct-2020 11:12:00 A...
□	Capture and comp...	ⓘ	Action	router_op_state_sna...	CLI , Check	Play to capture node states based on the given sensor path and re...	Cisco	22-Oct-2020 06:23:00 A...
□	Change interface s...	ⓘ	Device Config	router_cfg_interface...	IOS XR , cisco-iosxr-cli-7.24	Shut or unshut one or more interface on an XR router	Cisco	04-Nov-2020 01:17:00 A...
□	Change interface s...	ⓘ	Device Config	router_cfg_interface...	IOS XE , cisco-ios-cli-6.33	Play to change the GigE interface state on a IOS XE router	Cisco	22-Oct-2020 12:57:00 P...
□	Check BGP neighb...	ⓘ	Check	router_chk_bgp_neig...	SNMP	Play checks the state of the given BGP neighbor and passes if the ...	Cisco	23-Oct-2020 02:15:00 A...
□	Check CPU usage	ⓘ	Check	router_chk_cpu_proc...	SNMP	Verify that CPU utilization on the target device is below the referen...	Cisco	23-Oct-2020 01:58:00 A...
□	Check VRF neighb...	ⓘ	Action	router_op_verify_vrf_...	CLI , Check	This verb uses the collector golang library and generic CLI collecti...	Cisco	23-Oct-2020 05:44:00 A...
□	Check if the traffic ...	ⓘ	Action	router_op_verify_traf...	CLI , Check , SR	Play to invoke the generic cli collection for "show traffic-collector i...	Cisco	29-Jan-2021 08:49:00 A...

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

Note The recommendation is to include the **Perform Check Sync on the device** and **Sync NSO from device** Plays as a pre-step to running other operations in the Playbook or as part of pre-maintenance.

The **Perform Check Sync on the device** Play checks the device sync status with NSO and performs sync only when needed, based on the Playbook's sync parameter value. It reduces the playbook execution time and ensures the NSO configuration matches the device configuration.

- If the Playbook's sync parameter is set to True and the device is not in sync, the **Perform Check Sync on the device** Play will sync the device with the NSO configuration.
- If the sync parameter is set to False and the device is not in sync, the Play will fail to execute with a commit message.
- If the device is already in sync, the Play will succeed.

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.

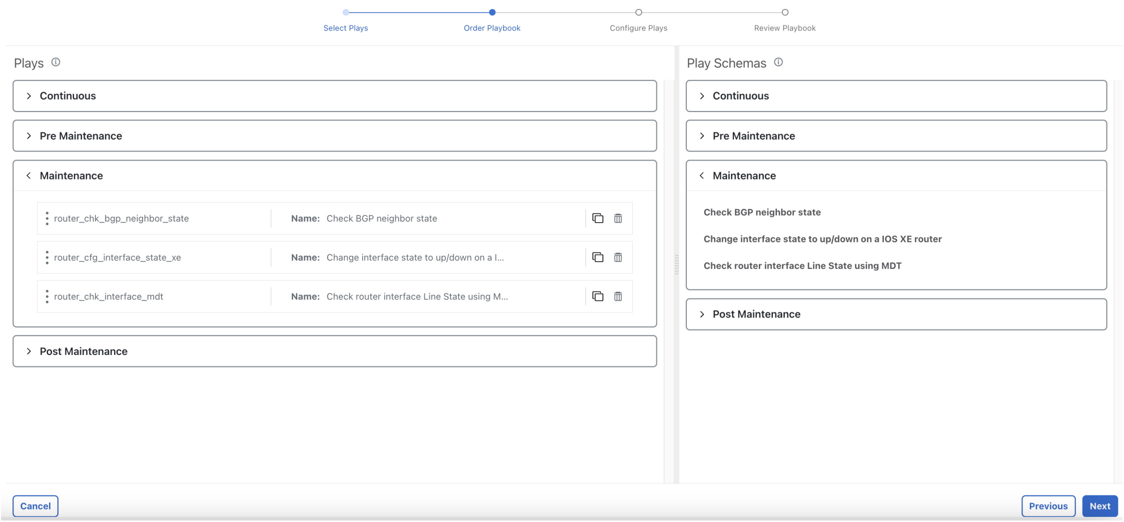
Depending on the type of Play you have selected, it may be restricted from being used in certain phases. For example, a configuration Play cannot be used outside of the Maintenance phase.

For more information on each execution phase, see Playbook Execution Order, on page 32.

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.

Figure 12: Order playbook



Plays ⓘ

› Continuous

› Pre Maintenance

‹ Maintenance

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

› Post Maintenance

Play Schemas ⓘ

› Continuous

› Pre Maintenance

‹ Maintenance

Check BGP neighbor state

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

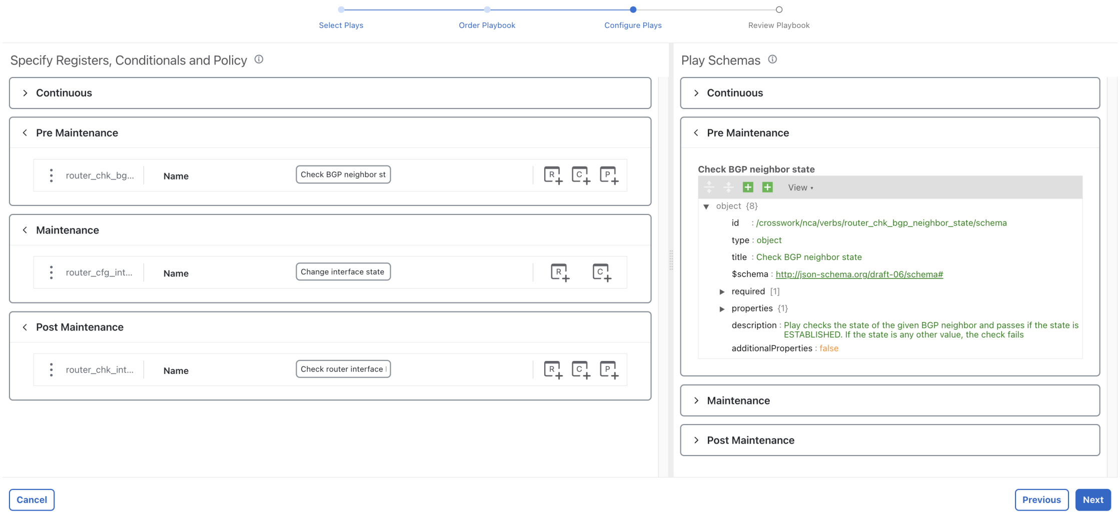
Check router interface Line State using MDT

› Post Maintenance

Click **Next**.

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

Figure 13: Configure plays



Specify Registers, Conditionals and Policy ⓘ

› Continuous

‹ Pre Maintenance

router_chk_bg...	Name	Check BGP neighbor st

‹ Maintenance

router_cfg_int...	Name	Change interface state

‹ Post Maintenance

router_chk_int...	Name	Check router interface l

Play Schemas ⓘ

› Continuous

‹ Pre Maintenance

Check BGP neighbor state

```
View ▾
▼ object {8}
      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#
   ▶ required  [1]
   ▶ properties  {1}
      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
```

› Maintenance

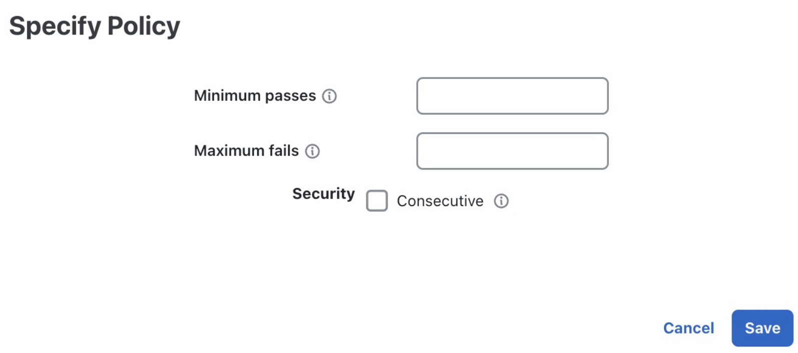
› Post Maintenance

You can perform the following:

- Click P+ to specify a 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 14: Specify Policy


Specify Policy

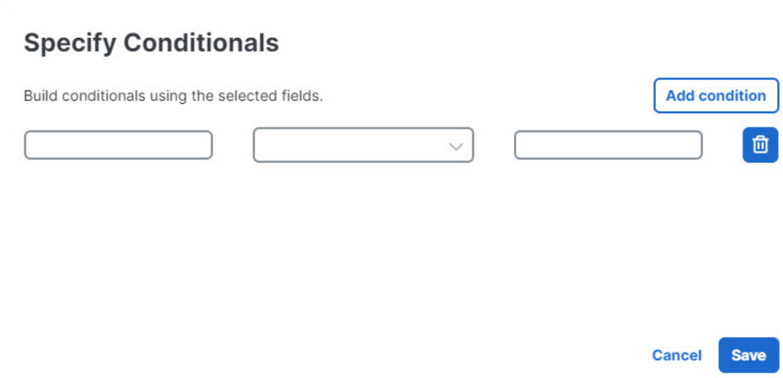
Minimum passes ⓘ

Maximum fails ⓘ

Security ☐ Consecutive ⓘ

- 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.

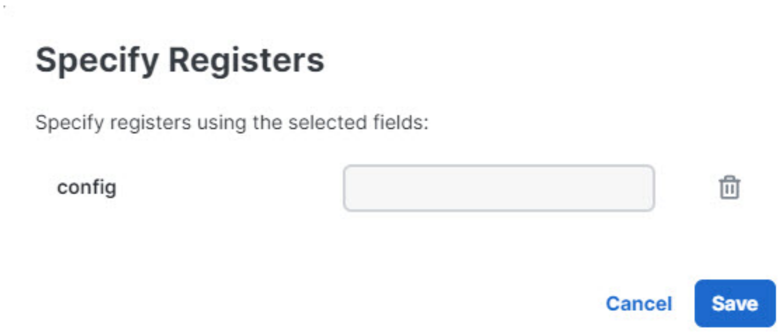
Figure 15: Specify Conditionals


Specify Conditionals

Build conditionals using the selected fields.

- 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.

Figure 16: Specify Registers


Specify Registers

Specify registers using the selected fields:

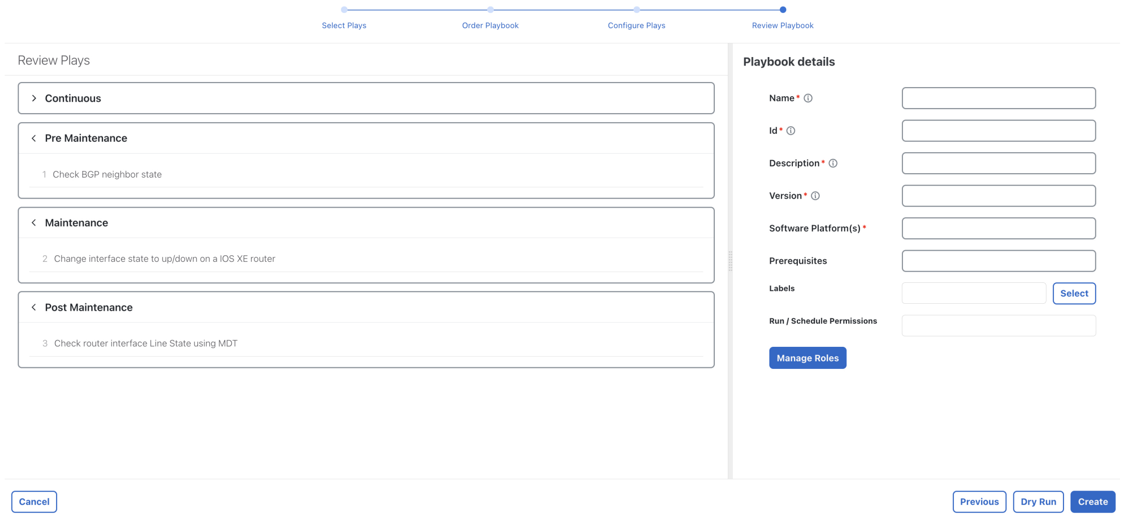
config

- (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.

Figure 17: Review Playbook



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

Playbook details

Name * ⓘ

Id * ⓘ

Description * ⓘ

Version * ⓘ

Software Platform(s) *

Prerequisites

Labels

Run / Schedule Permissions

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**:

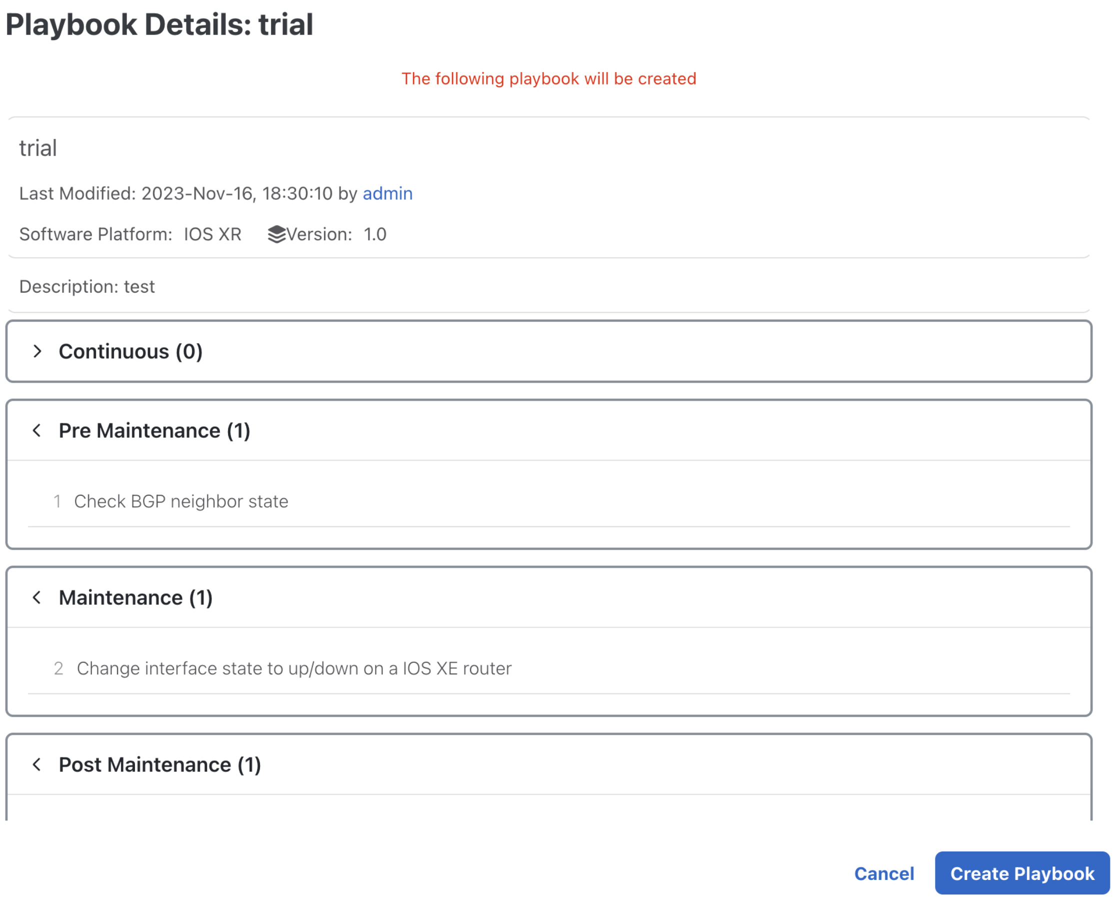
- Select the applicable label and click **Done**.
- Click **+ New label**, enter relevant values for **Label** and **Roles**, and click **Save**. Select the new label and click **Done**.

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 31.

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

Figure 18: Playbook Details



Playbook Details: trial

The following playbook will be created

trial

Last Modified: 2023-Nov-16, 18:30:10 by admin

Software Platform: IOS XR Version: 1.0

Description: test

Note Dry run does not commit the changes but 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 on the list.

Create a Custom Playbook Using APIs

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

Note A Playbook containing a custom Play can be created through the UI (see Create a Custom Playbook Through the UI, on page 23) or using APIs.

A Playbook consisting of one or more custom Plays is 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 17) 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 and custom Playbooks you or another party have authored and imported into Change Automation.

The exported archive contains only the user-customizable files listed in Playbook Components and Files, on page 23. It also 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. Then, you can import them as explained in Import Playbooks, on page 30.

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 Playbooks for export.

Step 4 Click ⇪. Your browser will prompt you to select a path and the file name 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

To import Playbooks, a user must have write access. For more information about granting a user read-writer role access, see Configure Change Automation Settings, on page 3.

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 you want to overwrite the existing Playbook.

If you are creating an improved version of a Playbook, it is recommended that you use a version number or other indicator to ensure 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 you want to delete.

Step 3 Click the 🗑 icon.

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

Assign Playbooks to Specific Roles

This section explains how to assign Playbook labels to specific roles so that they can 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

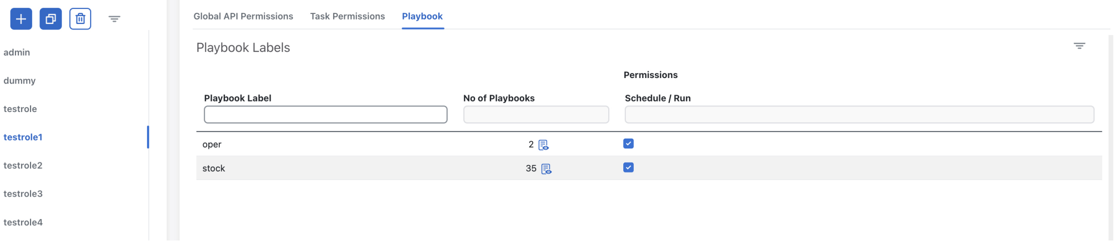
If required, create a new user to whom you would want to assign the Playbook. For more information, see the topic Create User Roles in the Cisco Crosswork Network Controller Administration Guide.

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

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

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

Figure 19: Playbook Labels



Playbook Labels

		Permissions
Playbook Label	No of Playbooks	Schedule / Run
oper	2	☑
stock	35	☑

About Running Playbooks

You must have 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 31.

Running any Playbook consists of five steps:

1. Select the **Playbook** you want to run (see View the Playbook List, on page 15).
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 33, where you can see what the Playbook does before make changes to the network.
   b. Run Playbooks In Single Stepping Mode, on page 39, so you can pause after each Playbook check or action, and roll back changes you did not intend.

c. Run Playbooks In Continuous Mode, on page 45 and apply the changes immediately.

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

- Schedule Playbook Runs, on page 51 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 if a failure occurs during the Playbook run.

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

Depending on their complexity and network factors, some Playbooks may take much time to run. You can view the run details and status at any time during and after the completion of a run. 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 23):

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 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.

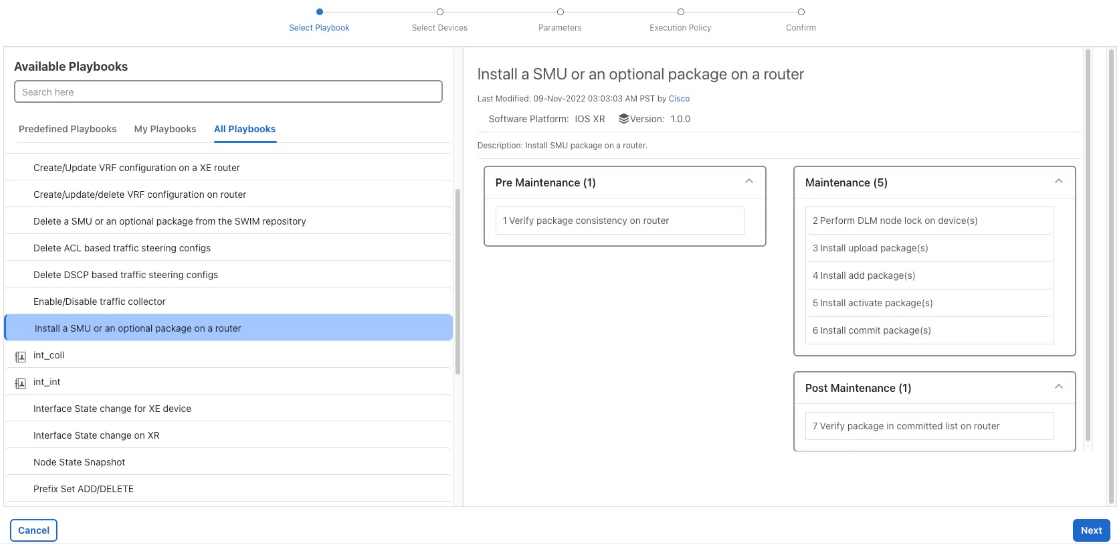
It is a best practice to perform a dry run and verify the configuration changes before you deploy those changes to the router. If the dry run fails, you may want to debug its parameter values using another dry run. You can also debug by performing a single-stepping run, which will allow you to abort 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 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 **Available Playbooks** 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.

Figure 20: Select Playbook



Available Playbooks

- Create/Update VRF configuration on a XE router
- Create/update/delete VRF configuration on router
- Delete a SMU or an optional package from the SWIM repository
- Delete ACL based traffic steering configs
- Delete DSCP based traffic steering configs
- Enable/Disable traffic collector
- Install a SMU or an optional package on a router
- int_coll
- int_int
- Interface State change for XE device
- Interface State change on XR
- Node State Snapshot
- Prefix Set ADD/DELETE

Install a SMU or an optional package on a router

Last Modified: 09-Nov-2022 03:03:03 AM PST by Cisco

Software Platform: IOS XR Version: 1.0.0

Description: Install SMU package on a router.

Pre Maintenance (1)

1 Verify package consistency on router

Maintenance (5)

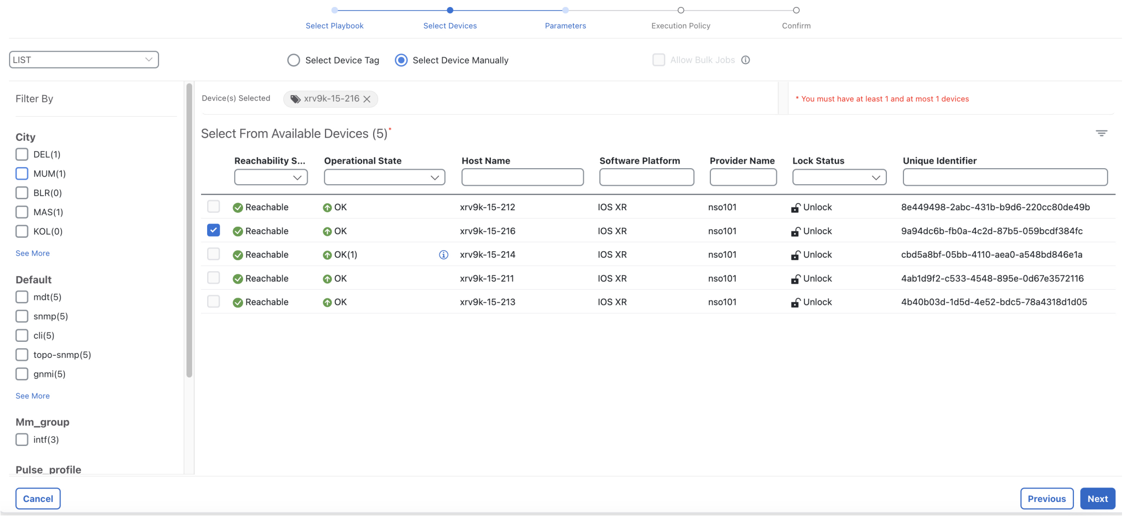
2 Perform DLM node lock on device(s)
3 Install upload package(s)
4 Install add package(s)
5 Install activate package(s)
6 Install commit package(s)

Post Maintenance (1)

7 Verify package in committed list on router

Step 3 Click **Next**. The **Select Devices** window appears.

Figure 21: Select Devices



Device(s) Selected xrv9k-15-216

* You must have at least 1 and at most 1 devices

Select From Available Devices (5)*

	Reachability S...	Operational State	Host Name	Software Platform	Provider Name	Lock Status	Unique Identifier
□	Reachable	OK	xrv9k-15-212	IOS XR	nso101	Unlock	8e449498-2abc-431b-b9d6-220cc80de49b
☑	Reachable	OK	xrv9k-15-216	IOS XR	nso101	Unlock	9a94dc6b-fb0a-4c2d-87b5-059bcdf384fc
□	Reachable	OK(1)	xrv9k-15-214	IOS XR	nso101	Unlock	cbd5a8bf-05bb-4110-aea0-a548bd846e1a
□	Reachable	OK	xrv9k-15-211	IOS XR	nso101	Unlock	4ab1d9f2-c533-4548-895e-0d67e3572116
□	Reachable	OK	xrv9k-15-213	IOS XR	nso101	Unlock	4b40b03d-1d5d-4e52-bdc5-78a4318d1d05

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 manually or using tags. The **Select Device Tag** option targets you to select the relevant tag instead of devices from the table and all devices associated with the relevant tag are selected. The **Select Device Manually** option allows you to select the devices from the list using quick and advanced filters and filter by tags on the left. Hover the mouse pointer over the ⓘ icon next to the options for more information. You can also view the selection criteria, such as the number of devices required for the selected playbook.

  Note If you are a non-admin user and selecting the devices manually, make a note of the following:

  - The devices on which you want to run the Playbook must belong to a Device Access Group, and you must have access to this Device Access Group. For more information on Device Access Groups and associating a user with a Device Access Group, see the Manage Device Access Groups section in the Cisco Crosswork Network Controller Administration Guide.

  - If your role is associated with an empty Device Access Group, then you will receive an error message.

  - If your role is associated with multiple Device Access Groups and the device belongs to any of these Device Access Groups, then you can run the Playbook on this device. If the device does not belong to any of your Device Access Groups, then the operation fails.

  - If you are selecting multiple devices (using **Allow Bulk Jobs** option or using tags) and if any of the devices does not have access, then an error message appears stating that this list of devices does not have access to run the Playbook.

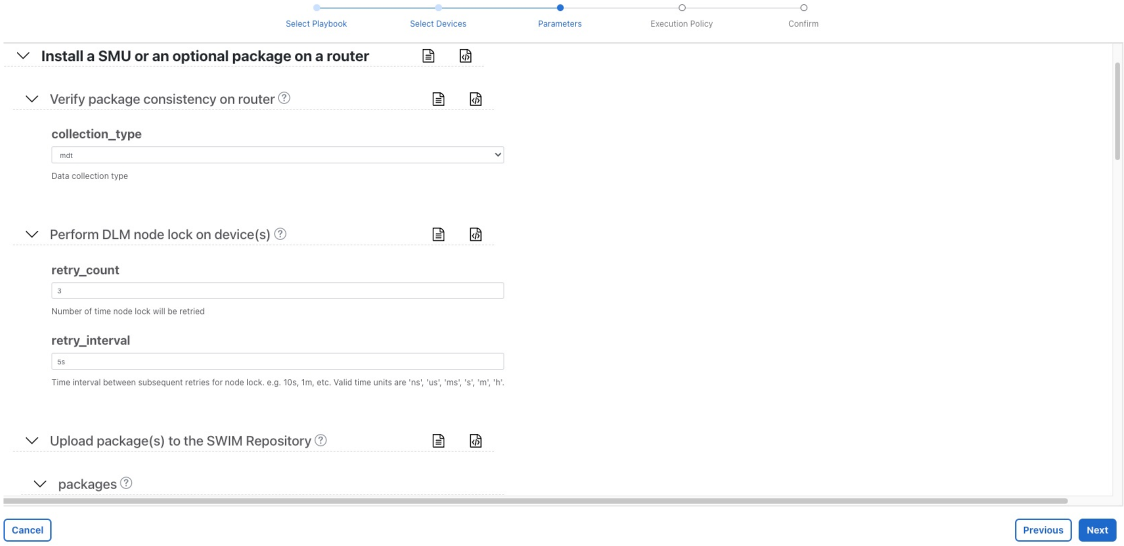
- In the **Select Device Manually** selection mode, you can check the **Allow Bulk Jobs** check box to select multiple devices and run the selected playbook on them simultaneously. Based on your selection, the system creates a static group of multiple jobs. Hover the mouse pointer over the ⓘ icon next to the check box for more information. There is no limit to 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 Click **Next**. The **Parameters** window appears.

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

Figure 22: Parameters



Install a SMU or an optional package on a router

Verify package consistency on router

collection_type: mdt

Data collection type

Perform DLM node lock on device(s)

retry_count: 3

Number of time node lock will be retried

retry_interval: 5s

Time interval between subsequent retries for node lock. e.g. 10s, 1m, etc. Valid time units are 'ns', 'us', 'ms', 's', 'm', 'h'.

Upload package(s) to the SWIM Repository

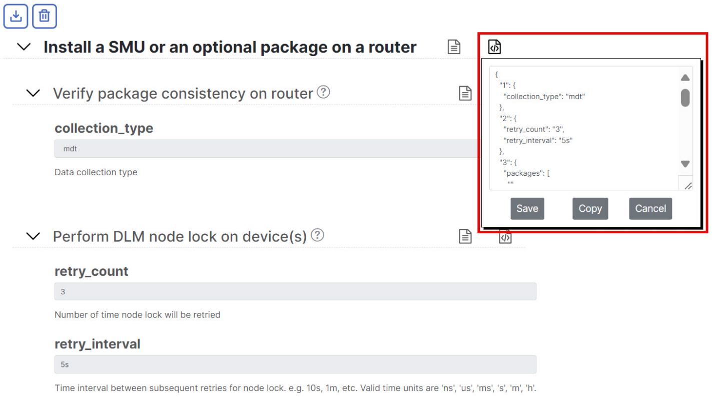
packages

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

- 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 </> 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**.

Figure 23: Edit JSON



Install a SMU or an optional package on a router

Verify package consistency on router

collection_type

mdt

Data collection type

```
{
  "1": {
    "collection_type": "mdt"
  },
  "2": {
    "retry_count": "3",
    "retry_interval": "5s"
  },
  "3": {
    "packages": [
      ""
```

Perform DLM node lock on device(s)

retry_count

3

Number of time node lock will be retried

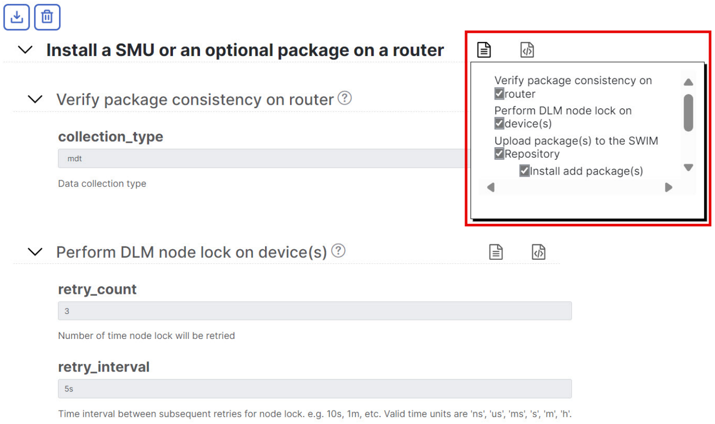
retry_interval

5s

Time interval between subsequent retries for node lock. e.g. 10s, 1m, etc. Valid time units are 'ns', 'us', 'ms', 's', 'm', 'h'.

- Click 🗎 to select the items you want to configure. A pop-up text window will appear, displaying the complete list of plays or parameters that can be configured. For the Playbook, it will show a list of Plays and, for each selected Play, it will display a list of parameters that can be configured for that Play. If you unselect any item, it will not appear for configuration. Uneditable options indicate mandatory items that cannot be deselected.

Figure 24: Object Properties for a Playbook



Install a SMU or an optional package on a router

Verify package consistency on router

collection_type

mdt

Data collection type

☑ Verify package consistency on router
☑ Perform DLM node lock on device(s)
☑ Upload package(s) to the SWIM Repository
☑ Install add package(s)

Perform DLM node lock on device(s)

retry_count

3

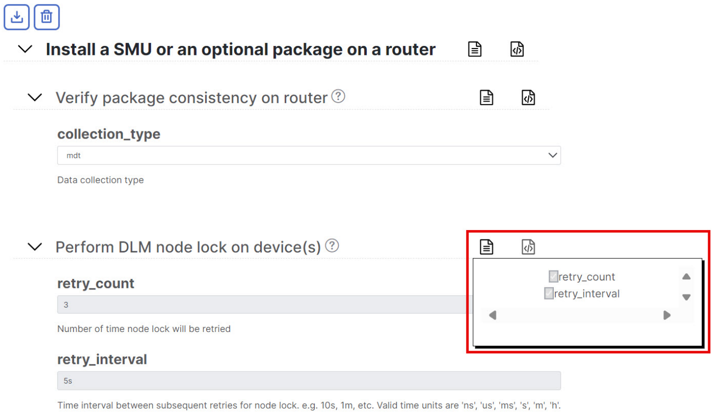
Number of time node lock will be retried

retry_interval

5s

Time interval between subsequent retries for node lock. e.g. 10s, 1m, etc. Valid time units are 'ns', 'us', 'ms', 's', 'm', 'h'.

Figure 25: Object Properties for a Play



Install a SMU or an optional package on a router

Verify package consistency on router

collection_type

mdt

Data collection type

Perform DLM node lock on device(s)

□retry_count
□retry_interval

retry_count

3

Number of time node lock will be retried

retry_interval

5s

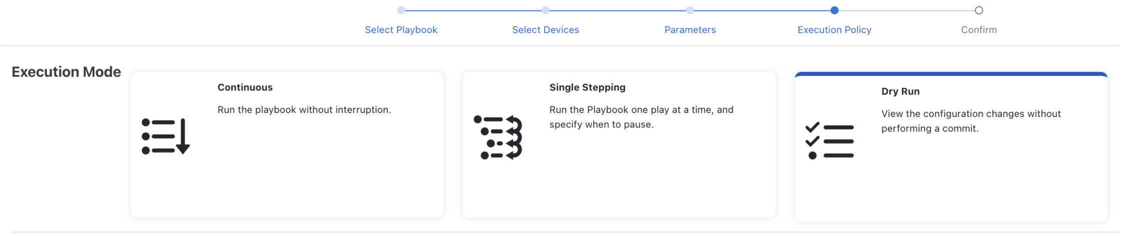
Time interval between subsequent retries for node lock. e.g. 10s, 1m, etc. Valid time units are 'ns', 'us', 'ms', 's', 'm', 'h'.

- Click ⊕ to add additional instances of a particular parameter, if required for the Playbook you are running. Click 🗑 to delete instances added in this way.
- Click 🗑 to clear all the parameter values entered so far.

a.

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

Figure 26: Execution Policy



Execution Mode

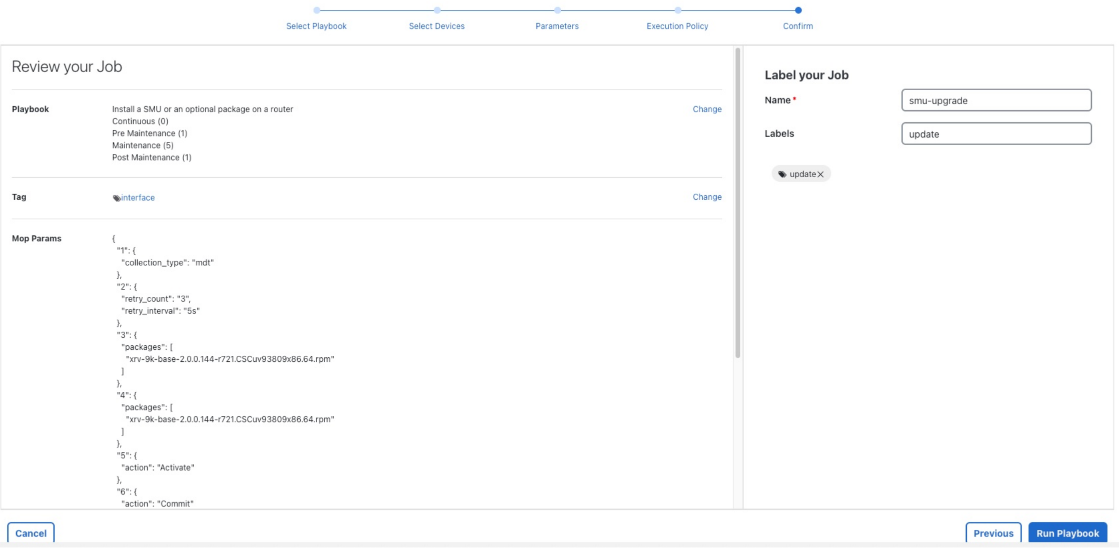
Continuous
Run the playbook without interruption.

Single Stepping
Run the Playbook one play at a time, and specify when to pause.

Dry Run
View the configuration changes without performing a commit.

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

Figure 27: Review your Job



Review your Job

Playbook: Install a SMU or an optional package on a router
Continuous (0)
Pre Maintenance (1)
Maintenance (5)
Post Maintenance (1)

Tag: interface

Mop Params:

```
{
 "1": {
  "collection_type": "mdt"
 },
 "2": {
  "retry_count": "3",
  "retry_interval": "5s"
 },
 "3": {
  "packages": [
   "xrv-9k-base-2.0.0.144-r721.CSCuv93809x86.64.rpm"
  ]
 },
 "4": {
  "packages": [
   "xrv-9k-base-2.0.0.144-r721.CSCuv93809x86.64.rpm"
  ]
 },
 "5": {
  "action": "Activate"
 },
 "6": {
  "action": "Commit"
```

Label your Job

Name *: smu-upgrade

Labels: update

In this window:

- You must provide a relevant **Name** for the job.
- You can enter labels for your job using the **Labels** field.
- You can click on any **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 3.

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 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` later, 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 56.
- 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 all of your parameter values from the dry run.

Run Playbooks In Single Stepping Mode

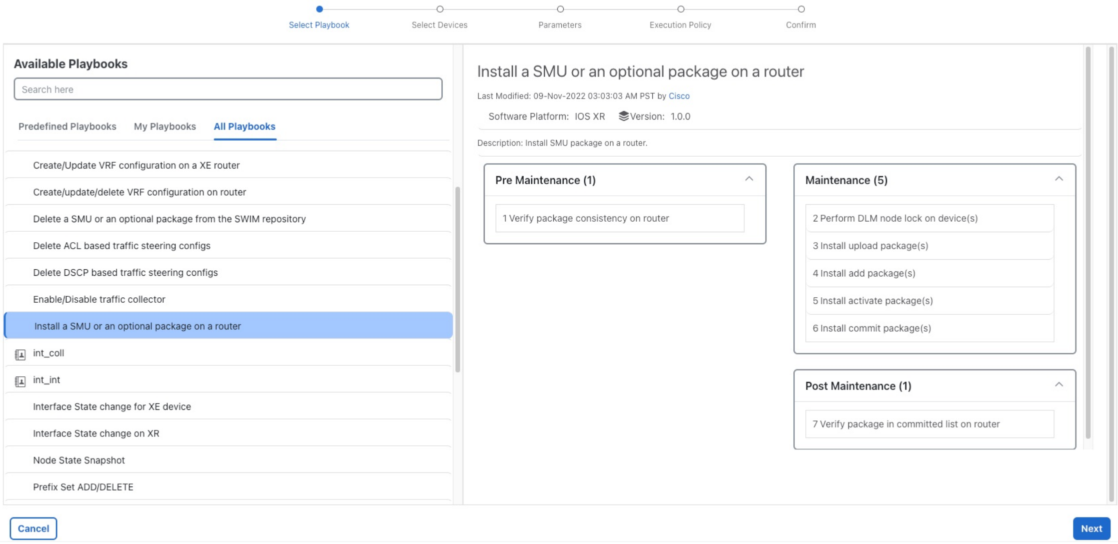
Single-stepping execution mode is a handy way to test a custom or modified Playbook or diagnose problems with a pre-packaged Playbook that does not give you the desired results. Unlike a dry run, a single-stepping execution commits configuration changes to the device as the Playbook runs. However, you can set breakpoints on or pauses after any Maintenance or Post-Maintenance action in the Playbook. 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 abort the entire run and roll back all changes made or roll back to any previous play.

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

Step 2 In the **Available Playbooks** 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.

Figure 28: Select Playbook



Create/Update VRF configuration on a XE router
Create/update/delete VRF configuration on router
Delete a SMU or an optional package from the SWIM repository
Delete ACL based traffic steering configs
Delete DSCP based traffic steering configs
Enable/Disable traffic collector
Install a SMU or an optional package on a router
int_coll
int_int
Interface State change for XE device
Interface State change on XR
Node State Snapshot
Prefix Set ADD/DELETE

Install a SMU or an optional package on a router

Last Modified: 09-Nov-2022 03:03:03 AM PST by Cisco

Software Platform: IOS XR Version: 1.0.0

Description: Install SMU package on a router.

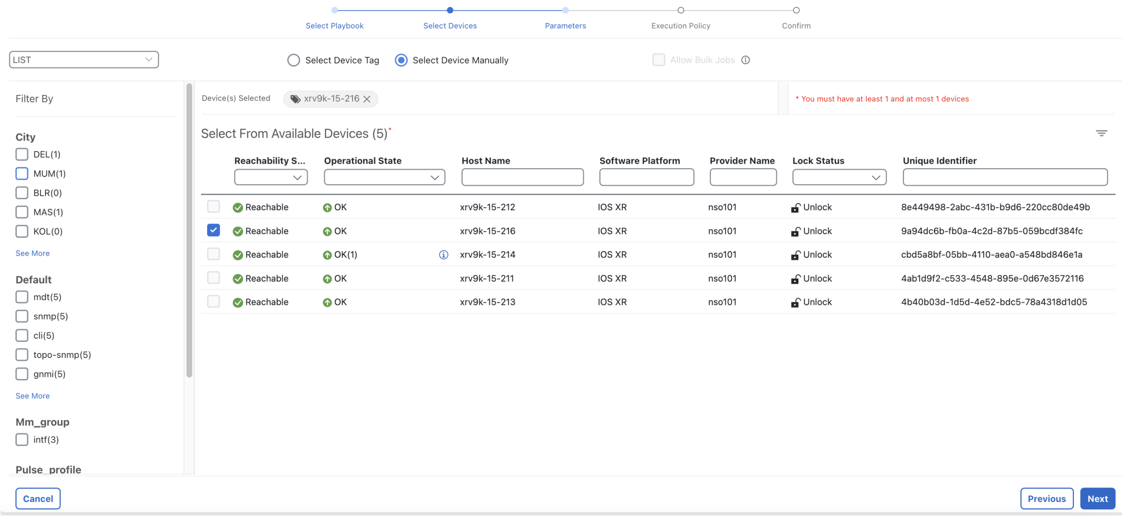
Pre Maintenance (1)
1 Verify package consistency on router

Maintenance (5)
2 Perform DLM node lock on device(s)
3 Install upload package(s)
4 Install add package(s)
5 Install activate package(s)
6 Install commit package(s)

Post Maintenance (1)
7 Verify package in committed list on router

Step 3 Click **Next**. The **Select Devices** window appears.

Figure 29: Select Devices



Device(s) Selected xrv9k-15-216

* You must have at least 1 and at most 1 devices

Select From Available Devices (5)*

	Reachability S...	Operational State	Host Name	Software Platform	Provider Name	Lock Status	Unique Identifier
□	Reachable	OK	xrv9k-15-212	IOS XR	nso101	Unlock	8e449498-2abc-431b-b9d6-220cc80de49b
☑	Reachable	OK	xrv9k-15-216	IOS XR	nso101	Unlock	9a94dc6b-fb0a-4c2d-87b5-059bcdf384fc
□	Reachable	OK(1) ⓘ	xrv9k-15-214	IOS XR	nso101	Unlock	cbd5a8bf-05bb-4110-aea0-a548bd846e1a
□	Reachable	OK	xrv9k-15-211	IOS XR	nso101	Unlock	4ab1d9f2-c533-4548-895e-0d67e3572116
□	Reachable	OK	xrv9k-15-213	IOS XR	nso101	Unlock	4b40b03d-1d5d-4e52-bdc5-78a4318d1d05

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 in 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 manually or using tags. The **Select Device Tag** option targets you to select the relevant tag instead of devices from the table and all devices associated with the relevant tag are selected. The **Select Device Manually** option allows you to select the devices from the list using quick and advanced filters and filter by tags on the left. Hover the mouse pointer over the ⓘ icon next to the options for more information. You can also view the selection criteria, such as the number of devices required for the selected playbook.

  Note If you are a non-admin user and selecting the devices manually, make a note of the following:

  - The devices on which you want to run the Playbook must belong to a Device Access Group, and you must have access to this Device Access Group. For more information on Device Access Groups and associating a user with a Device Access Group, see the Manage Device Access Groups section in the Cisco Crosswork Network Controller Administration Guide.

  - If your role is associated with an empty Device Access Group, you will receive an error message.

  - If your role is associated with multiple Device Access Groups and the device belongs to any of these Device Access Groups, then you can run the Playbook on this device. The operation fails if the device does not belong to any of your Device Access Groups.

  - If you select multiple devices (using the **Allow Bulk Jobs** option or using tags) and if any of them does not have access, an error message appears stating that this list of devices does not have access to run the Playbook.

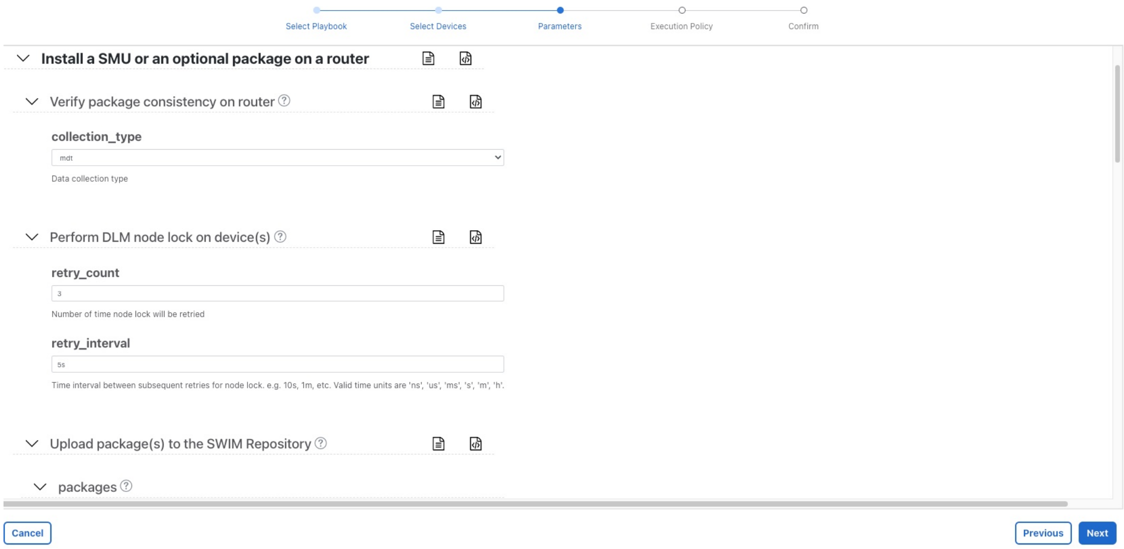
- In the **Select Device Manually** selection mode, you can check the **Allow Bulk Jobs** check box to select multiple devices and run the selected playbook on them simultaneously. Based on your selection, the system creates a static group of multiple jobs. Hover the mouse pointer over the ⓘ icon next to the check box for more information. There is no limit to 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 Click **Next**. The **Parameters** window appears.

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

Figure 30: Parameters


Select Playbook
Select Devices
Parameters
Execution Policy
Confirm
Install a SMU or an optional package on a router
Verify package consistency on router
Perform DLM node lock on device(s)
Upload package(s) to the SWIM Repository
packages
Cancel
Previous
Next

collection_type: mdt
Data collection type

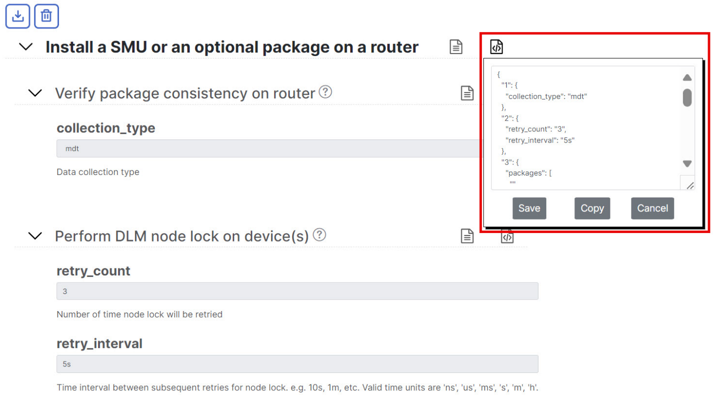
retry_count: 3
Number of time node lock will be retried

retry_interval: 5s
Time interval between subsequent retries for node lock. e.g. 10s, 1m, etc. Valid time units are 'ns', 'us', 'ms', 's', 'm', 'h'.

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

- 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 </> 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**.

Figure 31: Edit JSON



Install a SMU or an optional package on a router

Verify package consistency on router

collection_type

mdt

Data collection type

Perform DLM node lock on device(s)

retry_count

3

Number of time node lock will be retried

retry_interval

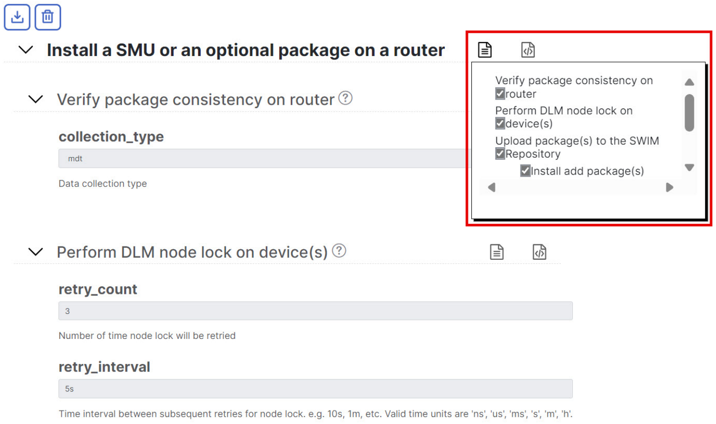
5s

Time interval between subsequent retries for node lock. e.g. 10s, 1m, etc. Valid time units are 'ns', 'us', 'ms', 's', 'm', 'h'.

```
{
 "1": {
  "collection_type": "mdt"
 },
 "2": {
  "retry_count": "3",
  "retry_interval": "5s"
 },
 "3": {
  "packages": [
   ""
```

- Click 🗎 to select the items you want to configure. A pop-up text window will appear, displaying the complete list of plays or parameters that can be configured. For the Playbook, it will show a list of Plays and, for each selected Play, it will display a list of parameters that can be configured for that Play. If you unselect any item, it will not appear for configuration. Uneditable options indicate mandatory items that cannot be deselected.

Figure 32: Object Properties for a Playbook



Install a SMU or an optional package on a router

Verify package consistency on router

collection_type

mdt

Data collection type

Perform DLM node lock on device(s)

retry_count

3

Number of time node lock will be retried

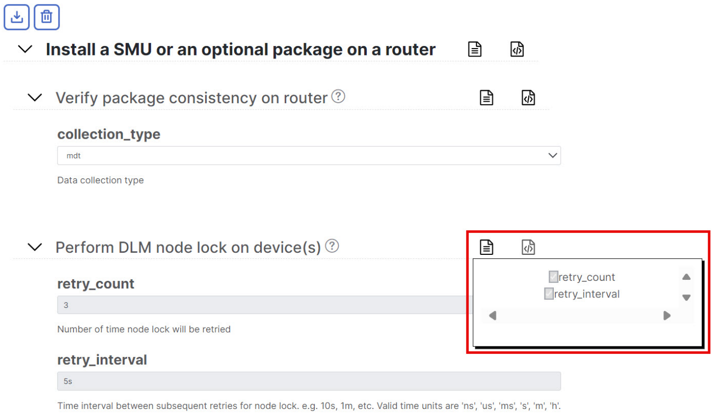
retry_interval

5s

Time interval between subsequent retries for node lock. e.g. 10s, 1m, etc. Valid time units are 'ns', 'us', 'ms', 's', 'm', 'h'.

Verify package consistency on ☑router
Perform DLM node lock on ☑device(s)
Upload package(s) to the SWIM ☑Repository
☑Install add package(s)

Figure 33: Object Properties for a Play



Install a SMU or an optional package on a router

Verify package consistency on router

collection_type: mdt

Data collection type

Perform DLM node lock on device(s)

retry_count: 3

Number of time node lock will be retried

retry_interval: 5s

Time interval between subsequent retries for node lock. e.g. 10s, 1m, etc. Valid time units are 'ns', 'us', 'ms', 's', 'm', 'h'.

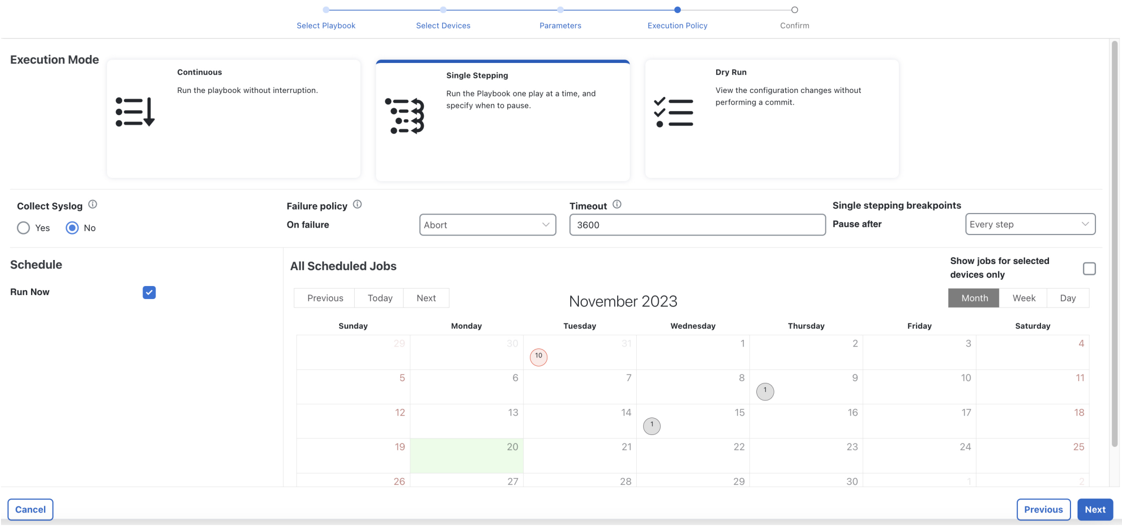
- Click ⊕ to add additional instances of a particular parameter, if required for the Playbook you are running. Click 🗑 to delete instances added in this way.

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

Figure 34: Execution Policy



Execution Mode

Continuous: Run the playbook without interruption.

Single Stepping: Run the Playbook one play at a time, and specify when to pause.

Dry Run: View the configuration changes without performing a commit.

Collect Syslog: ○ Yes ● No

Failure policy: On failure: Abort

Timeout: 3600

Single stepping breakpoints: Pause after: Every step

Schedule

Run Now ☑

All Scheduled Jobs

Show jobs for selected devices only □

November 2023

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
29	30	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

- Under **Collect Syslog**, click **Yes** if you want syslogs to be collected during and immediately after the run and **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 51 for help on using the **Schedule** area features.

Step 8 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 Check Point** pop-up 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 9 Click **Next**. The **Review your Job** window appears, displaying a summary of your choices: playbook, devices, parameters, and execution policy. In this window:

- You must provide a relevant **Name** for the job.
- You can enter labels for your job using the **Labels** field.
- You can click on any **Change** links in the **Review your Job** window summary to modify your choices.

Step 10 (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 3.

Step 11 When you are ready to continue, click **Run Playbook**.

Step 12 At the confirmation prompt, click **Confirm**. Click **View Job Set** to view the status of the current job. The job details include job status, job set tags, the title of the selected playbook, execution parameters and policy, last updated date, and updated comments (if any).

Step 13 While the run is executing, the **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 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 your selected step. All the previous steps will have a roll back point icon next to them. Click this icon 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 pop-up version of the **Parameters** window, just as you did in step 6. When resuming, the parameters exposed for editing are specific

to the task being resumed, meaning 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 14 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 **Playbook** and **Devices** tiles at the top of the window.
- See the current status of the run in the **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 appropriately 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 15 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 **Syslog** 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.
- An event is created in the audit log (**Administration** > **Audit Log**). The audit log includes details like the name of the Playbook, the user who ran the Playbook, and the commit label, if present.

Run Playbooks In Continuous Mode

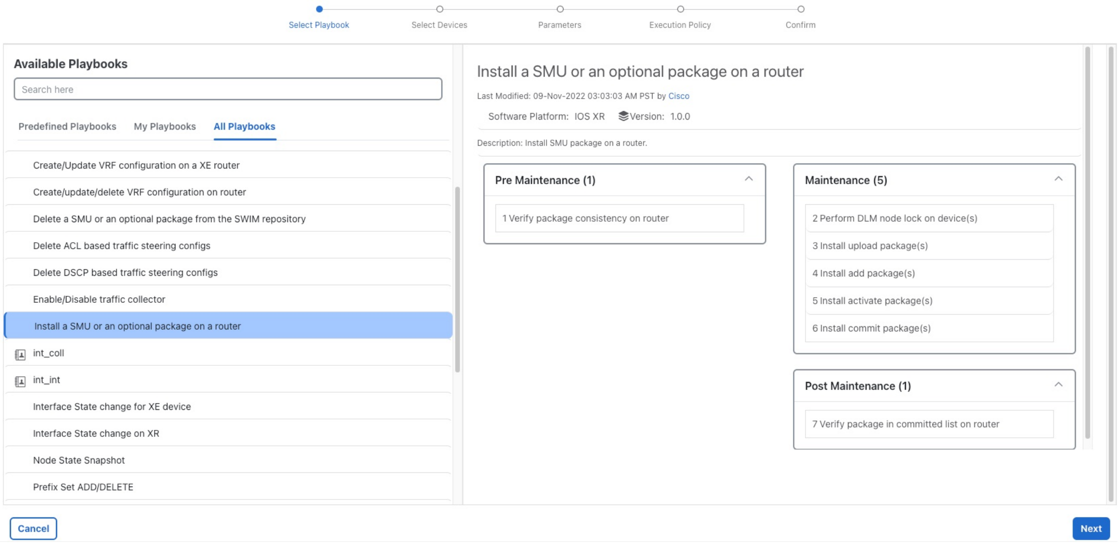
Continuous execution mode is the standard way to run Playbooks. Configuration changes are committed to the device during the run, with no checks or delays except those programmed for system resets or other purposes. The run continues until it succeeds or fails. If it fails, you can use the run's Failure 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 33). 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 39).

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

Step 2 In the **Available Playbooks** 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.

Figure 35: Select Playbook



Available Playbooks

- Create/Update VRF configuration on a XE router
- Create/update/delete VRF configuration on router
- Delete a SMU or an optional package from the SWIM repository
- Delete ACL based traffic steering configs
- Delete DSCP based traffic steering configs
- Enable/Disable traffic collector
- Install a SMU or an optional package on a router
- int_coll
- int_int
- Interface State change for XE device
- Interface State change on XR
- Node State Snapshot
- Prefix Set ADD/DELETE

Install a SMU or an optional package on a router

Last Modified: 09-Nov-2022 03:03:03 AM PST by Cisco

Software Platform: IOS XR Version: 1.0.0

Description: Install SMU package on a router.

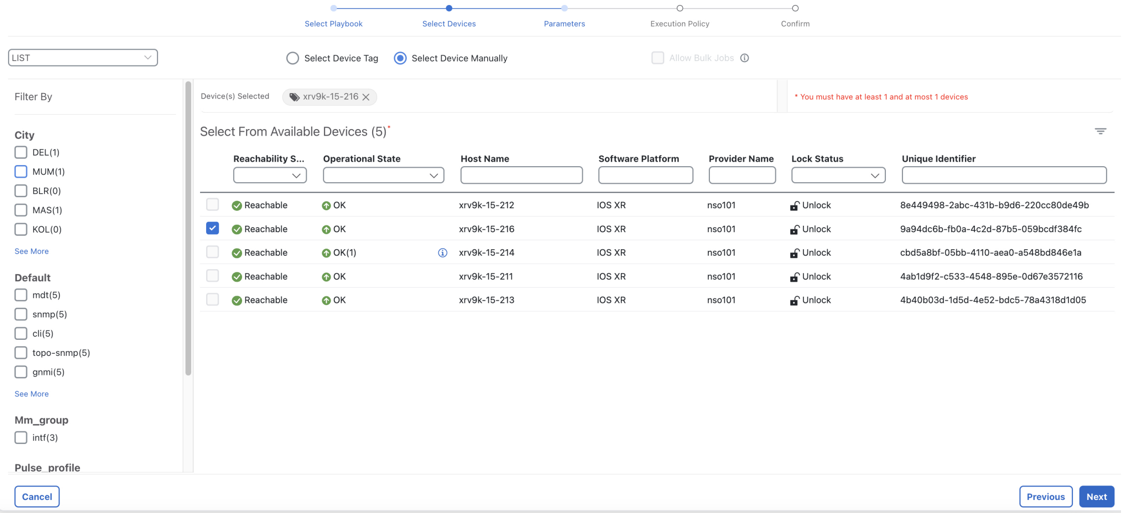
Pre Maintenance (1)
- 1 Verify package consistency on router

Maintenance (5)
- 2 Perform DLM node lock on device(s)
- 3 Install upload package(s)
- 4 Install add package(s)
- 5 Install activate package(s)
- 6 Install commit package(s)

Post Maintenance (1)
- 7 Verify package in committed list on router

Step 3 Click **Next**. The **Select Devices** window appears.

Figure 36: Select Devices



○ Select Device Tag ● Select Device Manually □ Allow Bulk Jobs

Device(s) Selected: xrv9k-15-216

* You must have at least 1 and at most 1 devices

City: □ DEL(1) □ MUM(1) □ BLR(0) □ MAS(1) □ KOL(0)

Default: □ mdt(5) □ snmp(5) □ cli(5) □ topo-snmp(5) □ gnmi(5)

Mm_group: □ intf(3)

Pulse_profile

Select From Available Devices (5)*

	Reachability S...	Operational State	Host Name	Software Platform	Provider Name	Lock Status	Unique Identifier
□	Reachable	OK	xrv9k-15-212	IOS XR	nso101	Unlock	8e449498-2abc-431b-b9d6-220cc80de49b
☑	Reachable	OK	xrv9k-15-216	IOS XR	nso101	Unlock	9a94dc6b-fb0a-4c2d-87b5-059bcdf384fc
□	Reachable	OK(1)	xrv9k-15-214	IOS XR	nso101	Unlock	cbd5a8bf-05bb-4110-aea0-a548bd846e1a
□	Reachable	OK	xrv9k-15-211	IOS XR	nso101	Unlock	4ab1d9f2-c533-4548-895e-0d67e3572116
□	Reachable	OK	xrv9k-15-213	IOS XR	nso101	Unlock	4b40b03d-1d5d-4e52-bdc5-78a4318d1d05

Using this window:

- You can toggle between the table view and topology map view by clicking and selecting the relevant option in 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 manually or using tags. The **Select Device Tag** option targets you to select the relevant tag instead of devices from the table and all devices associated with the relevant tag are selected. The **Select Device Manually** option allows you to select the devices from the list using quick and advanced filters and filter by tags on the left. 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.

  Note If you are a non-admin user and selecting the devices manually, make a note of the following:

  - The devices on which you want to run the Playbook must belong to a Device Access Group and you must have access to this Device Access Group. For more information on Device Access Groups and associating a user with a Device Access Group, see the Manage Device Access Groups section in the Cisco Crosswork Network Controller Administration Guide.

  - If your role is associated with an empty Device Access Group, you will receive an error message.

  - If your role is associated with multiple Device Access Groups and if the device belongs to any one of these Device Access Groups, then you can run the Playbook on this device. If the device does not belong to any of your Device Access Groups, the operation fails.

  - If you are selecting multiple devices (using **Allow Bulk Jobs** option or using tags) and if any devices does not have access, an error message appears stating that this list of devices does not have access to run the Playbook.

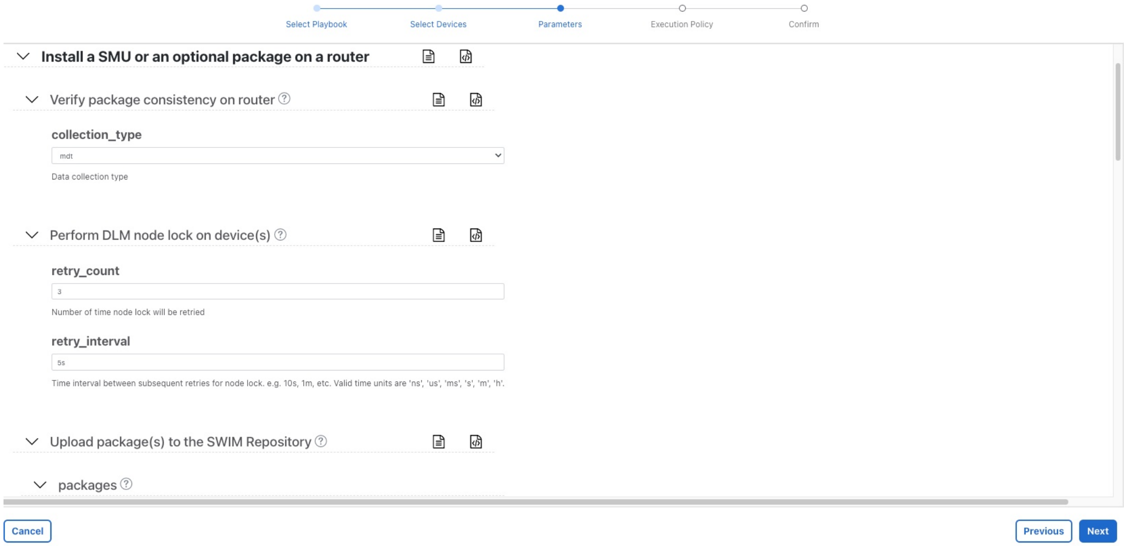
- In the **Select Device Manually** selection mode, you can check the **Allow Bulk Jobs** check box to select multiple devices and run the selected playbook simultaneously. Based on your selection, the system creates a static group of multiple jobs. Hover the mouse pointer over the ⓘ icon next to the check box for more information. There is no limit to 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 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 run.

Figure 37: Parameters



Install a SMU or an optional package on a router

Verify package consistency on router

collection_type: mdt

Data collection type

Perform DLM node lock on device(s)

retry_count: 3

Number of time node lock will be retried

retry_interval: 5s

Time interval between subsequent retries for node lock. e.g. 10s, 1m, etc. Valid time units are 'ns', 'us', 'ms', 's', 'm', 'h'.

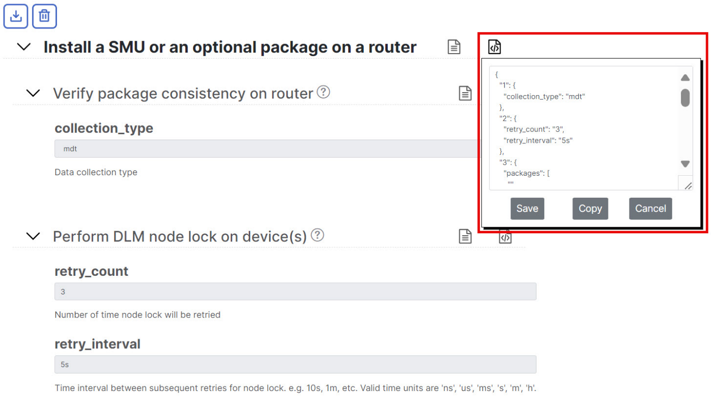
Upload package(s) to the SWIM Repository

packages

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

- 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 </> 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**.

Figure 38: Edit JSON



Install a SMU or an optional package on a router

Verify package consistency on router

collection_type: mdt

Data collection type

Perform DLM node lock on device(s)

retry_count: 3

Number of time node lock will be retried

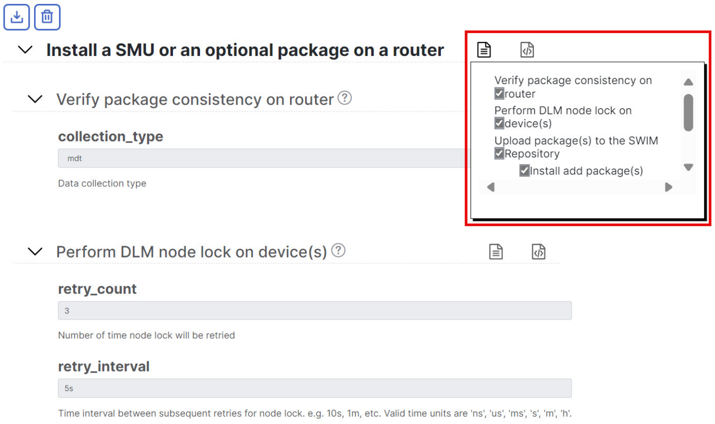
retry_interval: 5s

Time interval between subsequent retries for node lock. e.g. 10s, 1m, etc. Valid time units are 'ns', 'us', 'ms', 's', 'm', 'h'.

```
{
  "1": {
    "collection_type": "mdt"
  },
  "2": {
    "retry_count": "3",
    "retry_interval": "5s"
  },
  "3": {
    "packages": [
      ""
```

- Click 🗎 to select the items you want to configure. A pop-up text window will appear, displaying the complete list of plays or parameters that can be configured. For the Playbook, it will show a list of Plays and, for each selected Play, it will display a list of parameters that can be configured for that Play. If you unselect any item, it will not appear for configuration. Uneditable options indicate mandatory items that cannot be deselected.

Figure 39: Object Properties for a Playbook



Install a SMU or an optional package on a router

Verify package consistency on router

collection_type

mdt

Data collection type

Verify package consistency on
☑router
Perform DLM node lock on
☑device(s)
Upload package(s) to the SWIM
☑Repository
☑Install add package(s)

Perform DLM node lock on device(s)

retry_count

3

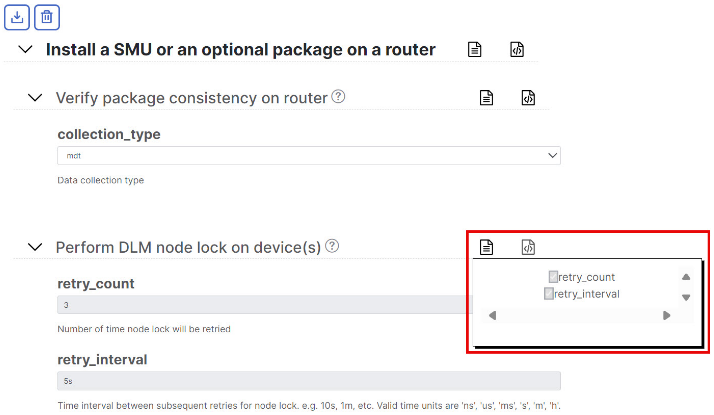
Number of time node lock will be retried

retry_interval

5s

Time interval between subsequent retries for node lock. e.g. 10s, 1m, etc. Valid time units are 'ns', 'us', 'ms', 's', 'm', 'h'.

Figure 40: Object Properties for a Play



Install a SMU or an optional package on a router

Verify package consistency on router

collection_type

mdt

Data collection type

Perform DLM node lock on device(s)

☐retry_count
☐retry_interval

retry_count

3

Number of time node lock will be retried

retry_interval

5s

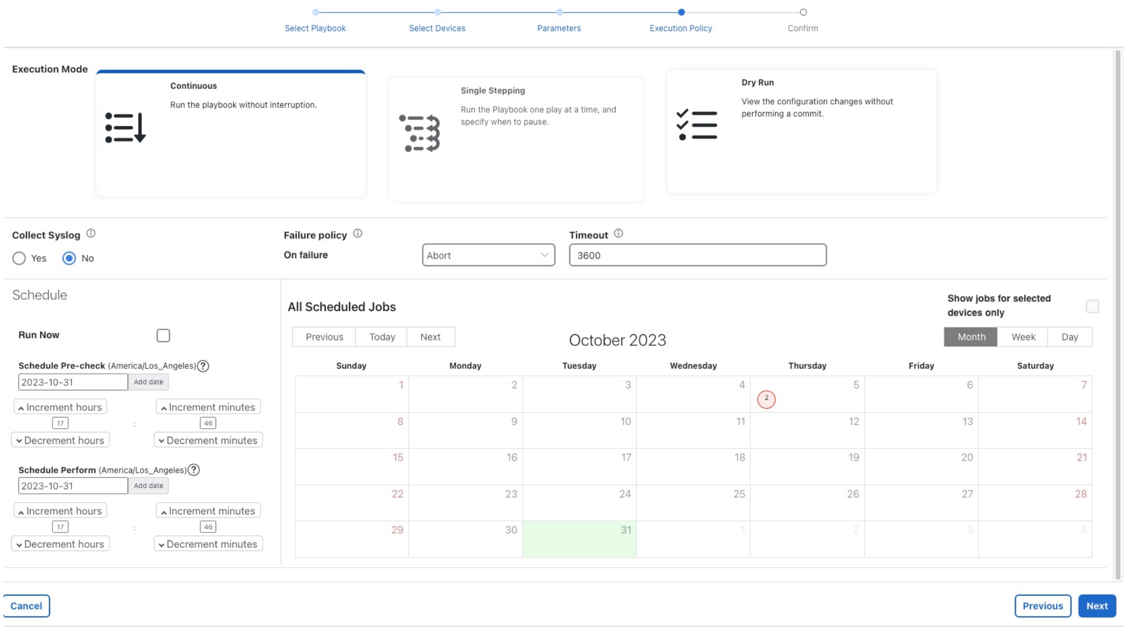
Time interval between subsequent retries for node lock. e.g. 10s, 1m, etc. Valid time units are 'ns', 'us', 'ms', 's', 'm', 'h'.

- Click ⊕ to add additional instances of a particular parameter, if required for the Playbook you are running. Click 🗑 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:

Figure 41: Execution Policy



Execution Mode

Continuous (selected): Run the playbook without interruption.

Single Stepping: Run the Playbook one play at a time, and specify when to pause.

Dry Run: View the configuration changes without performing a commit.

Collect Syslog: ○ Yes ● No

Failure policy: On failure: Abort

Timeout: 3600

Schedule

Run Now □

Schedule Pre-check (America/Los_Angeles): 2023-10-31, Add date; hours 17 : minutes 46

Schedule Perform (America/Los_Angeles): 2023-10-31, Add date; hours 17 : minutes 46

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
1	2	3	4	5 2	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	31	1	2	3	4

- Under **Collect Syslog**, click **Yes** if you want syslogs to be collected during and immediately after the run, and **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 51 for help on using the **Schedule** area features.

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

- You must provide a relevant **Name** for the job.
- You can enter labels for your job using the **Labels** field.
- You can click on 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 3.

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

Step 11 At the confirmation prompt, click **Confirm**. Click **View Job Set** to view the status of the current job. The job details include information such as job status, job set tags, the title of the selected playbook, execution parameters, and policy, last updated date, and update comments (if any).

Step 12 While the run is executing, the **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 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 **Playbook** and **Devices** tiles at the top of the window.
- See the current status of the run in the **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 **Syslog** 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.
- An event is created in the audit log (**Administration** > **Audit Log**). The audit log includes details like the name of the Playbook, the user who ran the Playbook, and the commit label, if present.

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 enabled when Change Automation was installed and initially configured. For more information, see Configure Change Automation Settings, on page 3. To change this setting, you must uninstall and then reinstall Change Automation.

Note If you are a non-admin user, ensure you have access to the Schedule Playbook task. You cannot schedule playbooks without this task.

Prerequisites:

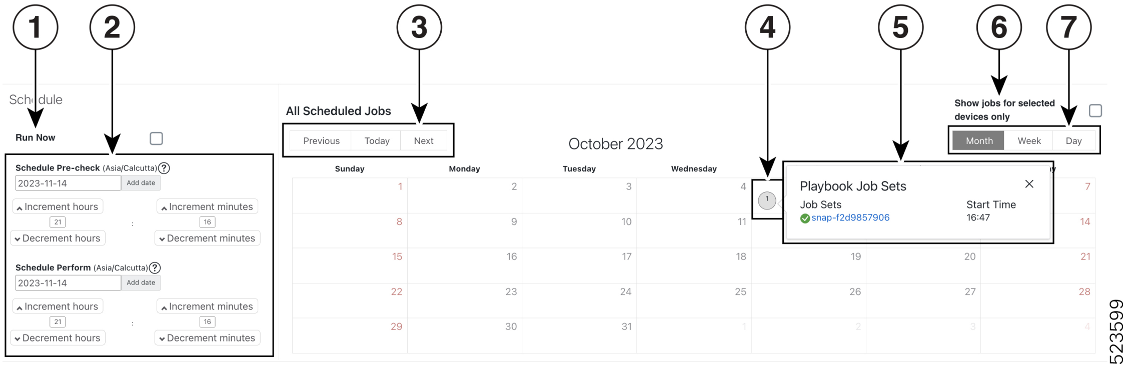
Ensure that **Playbook Job Scheduling** is enabled on the Device Override Credentials page. For more information, see Configure Change Automation Settings, on page 3.

To enable the task permission, do the following:

1. Go to **Administration** > **Users and Roles** > **Roles**.
2. Under the **Roles** pane, select the role for which you want to grant the access.
3. Under the **Task Permissions** tab, enable the **Schedule Playbook** check box and click **Save**.

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 42: Execution Mode Scheduling Features



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 simultaneously, 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.

Item	Description
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 jobs 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 Change Automation Playbooks have a **`mop_timeout`** parameter, which is a user-specified input 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 taken. Then, add a buffer time (for example, 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 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 incomplete (in between transitions) if the timeout gets triggered while rollback is in progress. If this happens, you have to revert the changes manually or create a Playbook with the changes 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. This panel displays the name of the Playbook, its plays, the devices it ran on, the parameters used, and all events, Syslog, console, and other messages. These details are helpful when diagnosing failures.

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

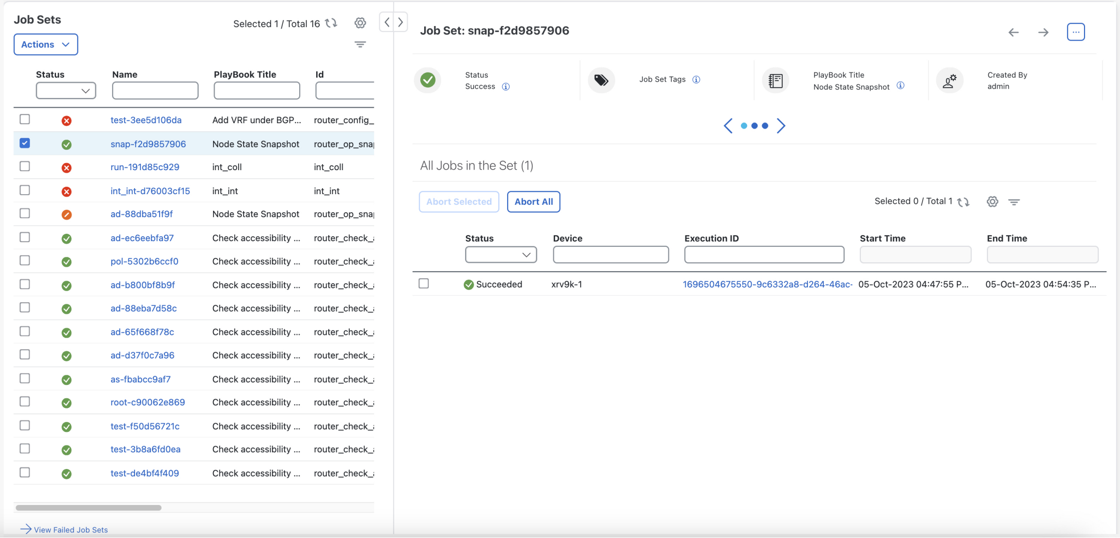
You can also navigate to **Automation Job History** window from the **Jobs** panel in the Change Automation **Dashboard**.

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 31.

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

Figure 43: Automation Job History



Job Sets

Selected 1 / Total 16

	Status	Name	PlayBook Title	Id
□	✗	test-3ee5d106da	Add VRF under BGP...	router_config_
☑	✓	snap-f2d9857906	Node State Snapshot	router_op_sna
□	✗	run-191d85c929	int_coll	int_coll
□	✗	int_int-d76003cf15	int_int	int_int
□	⊘	ad-88dba51f9f	Node State Snapshot	router_op_sna
□	✓	ad-ec6eebfa97	Check accessibility ...	router_check_
□	✓	pol-5302b6ccf0	Check accessibility ...	router_check_
□	✓	ad-b800bf8b9f	Check accessibility ...	router_check_
□	✓	ad-88eba7d58c	Check accessibility ...	router_check_
□	✓	ad-65f668f78c	Check accessibility ...	router_check_
□	✓	ad-d37f0c7a96	Check accessibility ...	router_check_
□	✓	as-fbabcc9af7	Check accessibility ...	router_check_
□	✓	root-c90062e869	Check accessibility ...	router_check_
□	✓	test-f50d56721c	Check accessibility ...	router_check_
□	✓	test-3b8a6fd0ea	Check accessibility ...	router_check_
□	✓	test-de4bf4f409	Check accessibility ...	router_check_

Job Set: snap-f2d9857906

Status: Success
Job Set Tags
PlayBook Title: Node State Snapshot
Created By: admin

All Jobs in the Set (1)

Selected 0 / Total 1

	Status	Device	Execution ID	Start Time	End Time
□	✓ Succeeded	xrv9k-1	1696504675550-9c6332a8-d264-46ac-	05-Oct-2023 04:47:55 P...	05-Oct-2023 04:54:35 P...

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 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 ⓘ 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**.

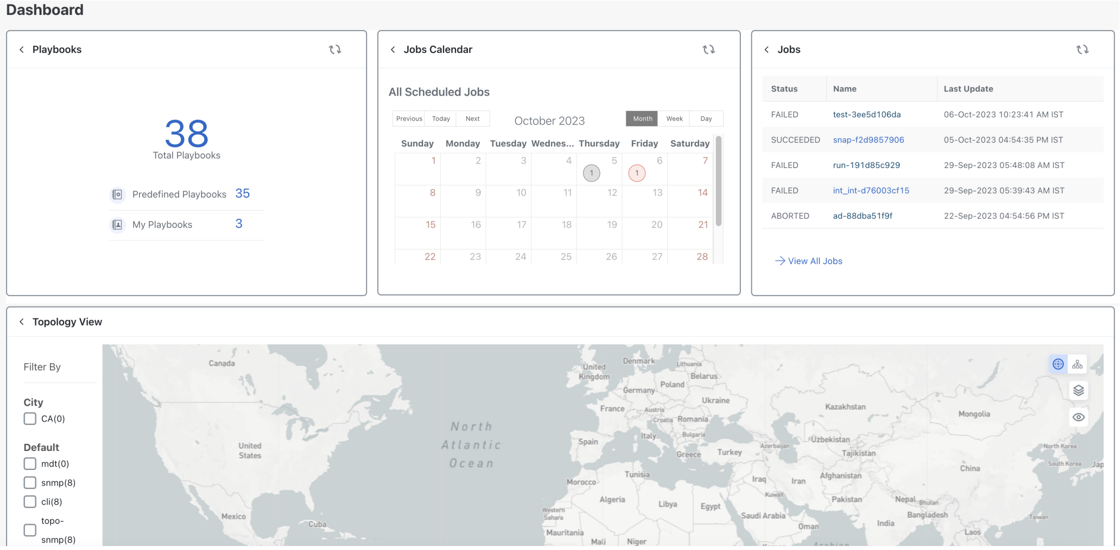
When prompted, click **Confirm**. Jobs currently running, paused, or scheduled will abort once the current task has been completed.

Use the Change Automation Dashboard

The Change Automation **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 44: Change Automation Dashboard Window



Dashboard

Playbooks

38
Total Playbooks

Predefined Playbooks 35

My Playbooks 3

Jobs Calendar

All Scheduled Jobs

Previous Today Next — October 2023 — Month Week Day

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

Jobs

Status	Name	Last Update
FAILED	test-3ee5d106da	06-Oct-2023 10:23:41 AM IST
SUCCEEDED	snap-f2d9857906	05-Oct-2023 04:54:35 PM IST
FAILED	run-191d85c929	29-Sep-2023 05:48:08 AM IST
FAILED	int_int-d76003cf15	29-Sep-2023 05:39:43 AM IST
ABORTED	ad-88dba51f9f	22-Sep-2023 04:54:56 PM IST

→ View All Jobs

Topology View

Filter By

City
□ CA(0)

Default
□ mdt(0)
□ snmp(8)
□ cli(8)
□ topo-snmp(8)

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:

- **Total Playbooks** indicate the total number of pre-defined and user-created Playbooks (My Playbooks) 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 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. 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 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.

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 **gray** circle indicates that all job sets are 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 gives you direct access to the Change Automation **Automation Job History** window.

Troubleshoot Change Automation

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

Table 3: 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 communication. Message text varies but may include "device out of sync," "NC client timeout," and other text indicating 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.
Playbook run fails with "access error" messages indicating failure "to set device override credentials in NSO".	Ensure that "admin" is a member of the **ncsadmin** user group in Cisco NSO.

"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 it 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.
SMU install fails at "Verify package in committed list on router".	Instead of using the tar.gz file in the packages field under Verify package in the committed list on router sub-option, use the committed package name to verify the package.

CHAPTER 4

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, and alerting and aids in 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 Telemetry (MDT), SNMP-based telemetry, or GNMI/Openconfig based telemetry collection. The Health Insights Recommendation Engine uses data mining to analyze your network and recommends which telemetry paths you should enable and monitor.

Note For MDT-based KPIs, crossword pushes the KPI configuration down to the device. For SNMP, CLI, and GNMI-based KPIs, the operator must have the device configured to respond to a request for telemetry data.

Important Due to the additional data collection tasks required, Health Insights requires the use of Extended Cisco Crosswork Data Gateways.

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.

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 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 maximize network performance.

List of Health Insights KPIs

This section lists the prebuilt Health Insights KPIs supplied with Health Insights application.

Supported Protocols

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.

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.

Health Insights uses either MDT or gNMI protocols but the device supports both. gNMI is a preferred default.

Table 4: Health Insights KPIs

Category	KPI Name	Description	Alerting	Protocol
Dataplane-Counters	CEF drops	Monitors CEF drop counters and baseline. Generates an alert for an unusual number of drops.	Rate Change	MDT, gNMI
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
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
Basics	Device uptime	Monitors device uptime.	Low Single Threshold	MDT, gNMI

Category	KPI Name	Description	Alerting	Protocol
Layer 1-Traffic	Ethernet port error counters	Monitors port transmit and receive error counters.	Rate Change	MDT, gNMI
Layer 1-Traffic	Ethernet port packet size distribution	Monitors port transmit and receive packet size distributions.	No Alert	MDT, gNMI
Layer 1-Traffic	Ethernet port packet statistics	Monitors port transmit and receive packet statistics.	Standard Deviation of Rate Change	MDT, gNMI
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
Layer 3-Traffic	Interface counters by protocol	Monitors interface statistics (such as incoming and outgoing packets or byte counters) organized by protocol.	No Alert	MDT, gNMI
Layer2-Interface	Interface flap detection	Monitors interface flaps and alerts when flap count reaches set threshold.	Two-Level Threshold	MDT, gNMI
Layer 2-Traffic	Interface packet counters	Monitors interface transmit and receive counters. Generates an alert when unusual traffic rates occur.	No Alert	MDT, gNMI
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
QOS	Interface QoS (egress)	Monitors interface QoS on the egress direction for queue statistics, queue depth, and so on.	No Alert	MDT, gNMI
QOS	Interface QoS (ingress)	Monitors interface QoS on the ingress direction for queue statistics, queue depth, and so on.	No Alert	MDT, gNMI
Layer 2-Traffic	Interface rate counters	Monitors interface statistics as rate counters. Generates an alert when unusual traffic rates occur.	Standard Deviation	MDT, gNMI
IPSLA	IP SLA UDP echo RTT	Monitors IP SLA UDP echo RTT. Generates an alert when unusual RTT values occur.	Standard Deviation	MDT, gNMI
IPSLA	IP SLA UDP jitter monitoring	Monitors IP SLA UDP jitter. Generates an alert when an abnormal UDP jitter occurs.	Standard Deviation	MDT, gNMI

Category	KPI Name	Description	Alerting	Protocol
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
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
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
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
Protocol-ISIS	ISIS neighbor summary	Monitors ISIS neighbor summaries for changes in neighbor status.	No Alert	MDT, gNMI
Layer 1-Optics	Layer 1 optical alarms	Monitors per-port optical alarms (current and past).	No Alert	MDT, gNMI
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
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
Layer 1-Optics	Layer 1 optical power	Monitors per-port optical power.	No Alert	MDT, gNMI
Layer 1-Optics	Layer 1 optical temperature	Monitors per-port optical temperature.	No Alert	MDT, gNMI
Layer 1-Optics	Layer 1 optical voltage	Monitors per-port optical voltage.	No Alert	MDT, gNMI
Layer 2-Interface	Line state	Monitors interface line states.	No Alert	MDT, gNMI
LLDP	LLDP neighbors	Monitors LLDP neighbors.	No Alert	MDT, gNMI

Category	KPI Name	Description	Alerting	Protocol
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
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
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
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
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
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
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
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
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

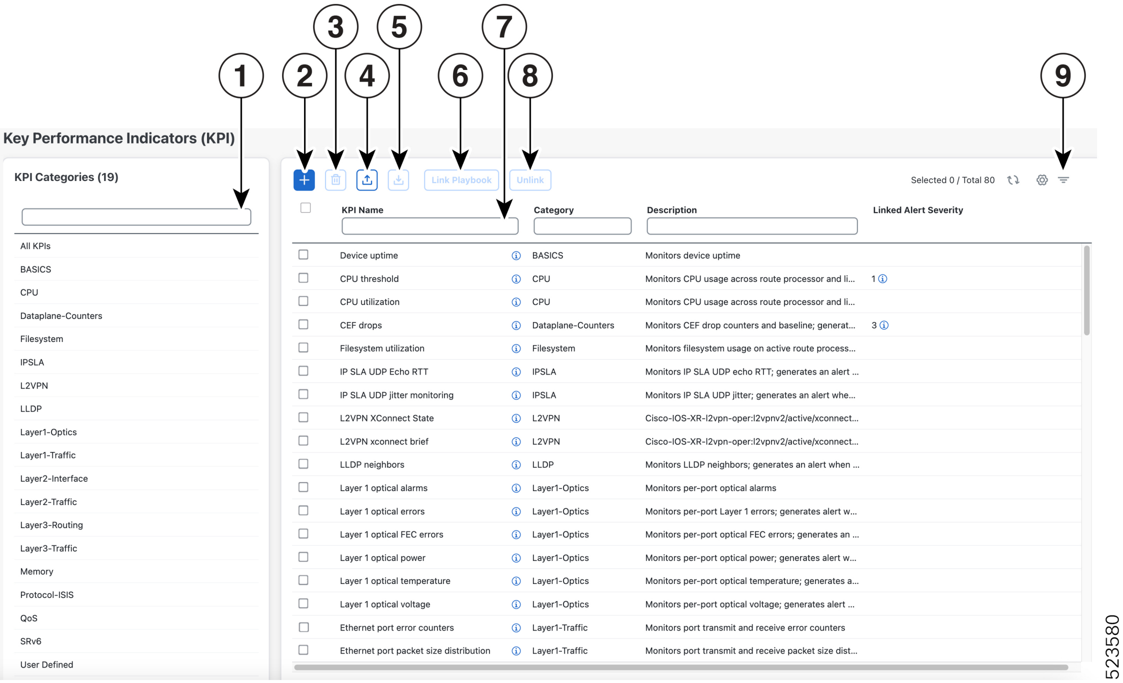
Category	KPI Name	Description	Alerting	Protocol
Layer 3-Routing	RIBv6 local route count	Monitors RIBv6 for route count and memory used by local. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, gNMI
Layer 3-Routing	RIBv6 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
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
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.	No Alert	SNMP
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	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

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.

Figure 45: Key Performance Indicators (KPI)



Key Performance Indicators (KPI)

KPI Categories (19)

- All KPIs
- BASICS
- CPU
- Dataplane-Counters
- Filesystem
- IPSLA
- L2VPN
- LLDP
- Layer1-Optics
- Layer1-Traffic
- Layer2-Interface
- Layer2-Traffic
- Layer3-Routing
- Layer3-Traffic
- Memory
- Protocol-ISIS
- QoS
- SRv6
- User Defined

+ 🗑 Link Playbook Unlink   Selected 0 / Total 80

□	KPI Name		Category	Description	Linked Alert Severity
□	Device uptime	ⓘ	BASICS	Monitors device uptime	
□	CPU threshold	ⓘ	CPU	Monitors CPU usage across route processor and li...	1 ⓘ
□	CPU utilization	ⓘ	CPU	Monitors CPU usage across route processor and li...	
□	CEF drops	ⓘ	Dataplane-Counters	Monitors CEF drop counters and baseline; generat...	3 ⓘ
□	Filesystem utilization	ⓘ	Filesystem	Monitors filesystem usage on active route process...	
□	IP SLA UDP Echo RTT	ⓘ	IPSLA	Monitors IP SLA UDP echo RTT; generates an alert ...	
□	IP SLA UDP jitter monitoring	ⓘ	IPSLA	Monitors IP SLA UDP jitter; generates an alert whe...	
□	L2VPN XConnect State	ⓘ	L2VPN	Cisco-IOS-XR-l2vpn-oper:l2vpnv2/active/xconnect...	
□	L2VPN xconnect brief	ⓘ	L2VPN	Cisco-IOS-XR-l2vpn-oper:l2vpnv2/active/xconnect...	
□	LLDP neighbors	ⓘ	LLDP	Monitors LLDP neighbors; generates an alert when ...	
□	Layer 1 optical alarms	ⓘ	Layer1-Optics	Monitors per-port optical alarms	
□	Layer 1 optical errors	ⓘ	Layer1-Optics	Monitors per-port Layer 1 errors; generates alert w...	
□	Layer 1 optical FEC errors	ⓘ	Layer1-Optics	Monitors per-port optical FEC errors; generates an ...	
□	Layer 1 optical power	ⓘ	Layer1-Optics	Monitors per-port optical power; generates alert w...	
□	Layer 1 optical temperature	ⓘ	Layer1-Optics	Monitors per-port optical temperature; generates a...	
□	Layer 1 optical voltage	ⓘ	Layer1-Optics	Monitors per-port optical voltage; generates alert ...	
□	Ethernet port error counters	ⓘ	Layer1-Traffic	Monitors port transmit and receive error counters	
□	Ethernet port packet size distribution	ⓘ	Layer1-Traffic	Monitors port transmit and receive packet size dist...	

Item	Description
1	**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.
2	**Add KPIs**: Click + to add a new, user-created KPI. For help with this task, see Create a New KPI, on page 65.
3	**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
4	**Import KPIs**: Click ⤓ to import new user-written or Cisco-supplied KPIs. **Note** When upgrading from an older version of CNC, it's important to consider the following: Before attempting to load a KPI, ensure that it complies with the requirements of the current release. If you try to load a KPI that was created for a previous release and is not compatible, you will receive an error message. 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 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.
5	**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.
6	**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. Filtering is case-sensitive. Click ⊗ to clear any filter criteria you may have set.
7	**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 and Run Them Manually, on page 67.
8	**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.
9	**Filter**: Click ≡ to set filter criteria on one or more columns in the table.

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 include 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 you want to monitor are available in Crosswork. If they are not available, perform the Add Custom Packages procedure given in the Cisco Crosswork Network Controller Administration Guide. Then continue with the steps below.

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. Perform the Add Custom Packages procedure given in the Cisco Crosswork Network Controller Administration Guide, then continue with the subsequent steps in this procedure.

Click **Next** to display the **Select Alert Templates** window. You can select from the following alerting types:

- **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.

You can also use the following additional alerting types when you export and modify a prebuilt KPI to create a KPI with custom parameters (see the Cisco Crosswork Network Automation Custom KPI Tutorial Documentation on Cisco DevNet):

- **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.

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 72.

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.

Link KPIs to Playbooks and Run Them Manually

The default option for KPI-linked Playbooks is for the network operator to run them manually, when an alert is displayed. Crosswork displays the linked Playbooks as options, and the operator can select which Playbooks to run. However, if Device Override Credentials are enabled properly, you have the option to run one or more KPI-linked Playbook automatically, whenever the linked KPI raises an alert, as explained in Link KPIs to Playbooks and Run Them Automatically, on page 69.

Note You can't use this function if you haven't installed the Change Automation Crosswork application. If that's the case, Crosswork will not display the UI features that link Health Insights KPIs and Change Automation Playbooks (for example, you won't see the Link Playbook icon).

You can specify the **Source** of the parameter values the linked Playbooks use when you run them. When linking a Playbook to a KPI alert, you can select these sources:

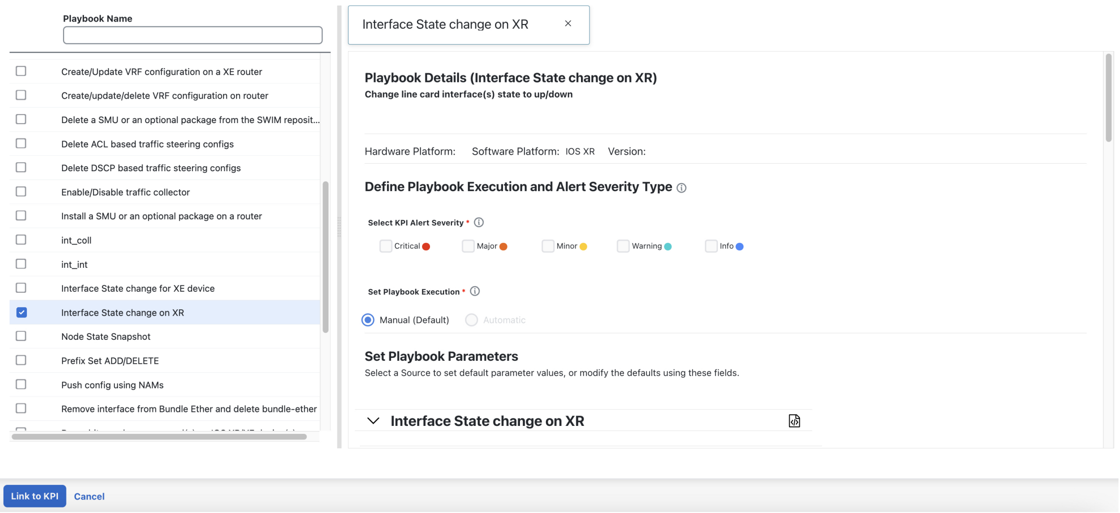
- **Playbook**: Use default values coded into the Playbook itself
- **KPI Alert**: Use values that are taken from the alert that is raised by the linked KPI.
- **Run-time Input**: Use values that you enter only at the moment you run the Playbook.

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 may 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 46: Example: Specifying Parameter Value Sources for a Linked Playbook



Playbook Name

- □ Create/Update VRF configuration on a XE router
- □ Create/update/delete VRF configuration on router
- □ Delete a SMU or an optional package from the SWIM reposit...
- □ Delete ACL based traffic steering configs
- □ Delete DSCP based traffic steering configs
- □ Enable/Disable traffic collector
- □ Install a SMU or an optional package on a router
- □ int_coll
- □ int_int
- □ Interface State change for XE device
- ☑ Interface State change on XR
- □ Node State Snapshot
- □ Prefix Set ADD/DELETE
- □ Push config using NAMs
- □ Remove interface from Bundle Ether and delete bundle-ether

Interface State change on XR ×

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

Hardware Platform: Software Platform: IOS XR Version:

Define Playbook Execution and Alert Severity Type ⓘ

Select KPI Alert Severity * ⓘ

□ Critical ● □ Major ● □ Minor ● □ Warning ● □ Info ●

Set Playbook Execution * ⓘ

● Manual (Default) ○ Automatic

Set Playbook Parameters
Select a Source to set default parameter values, or modify the defaults using these fields.

Interface State change on XR

Link to KPI Cancel

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 62.

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 to see.

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

- The **Hardware Platform** and **Software Platform** with which the Playbook is compatible.
- The minimum software **Version** required to execute the Playbook.
- The **KPI Alert Severity** level needed to trigger a run of this Playbook. Note that, if you will be choosing multiple Playbooks to run when a KPI alert is raised, be aware that Playbooks do not share severity levels. If you have selected a **Critical** severity level for one Playbook, you must select **Major**, **Minor**, **Warning** or **Info** severities for a second Playbook, and another still for a third Playbook.
- Choose the **Set Playbook Execution** function you want to use. **Manual** execution is the default and is recommended for most purposes. See Link KPIs to Playbooks and Run Them Automatically, on page 69 before selecting the **Automatic** execution option.
- Modify the **Set Playbook Parameters** default values to be used when the Playbook runs. In many cases, you can select from a range of default values. You can also enter your own. These values vary widely, depending on the Playbook and its purpose. For help, see the information offered on screen for the Playbook you have selected.

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 Playbooks shown next to the name of the KPI in the **Key Performance Indicators (KPIs)** list.

Step 8 If you want to run more Playbooks (up to three Playbooks total): Repeat steps 5 through 7 for each additional Playbook you want to run when an alert for this KPI is raised.

Step 9 To change the Playbook parameters linked to a given KPI, repeat steps 5 through 7 for that KPI, but this time choose the Playbook whose settings you want to modify. If you have chosen multiple KPIs, you can switch among them by clicking on the Playbook tiles at the top of the window. To unlink a Playbook entirely, select the KPI and click Unlink.

Link KPIs to Playbooks and Run Them Automatically

In addition to running KPI-linked Playbooks only at the network operator's discretion, you can choose to run one or more of your KPI-linked Playbooks automatically, whenever the KPI linked to that Playbook raises an alert of sufficient severity.

Note You can't use this function if you haven't installed the Change Automation application. If that's the case, Crosswork will not display the UI features that link Health Insights KPIs and Change Automation Playbooks (for example, you won't see the Link Playbook icon).

All of the same considerations in setting Playbook values described in Link KPIs to Playbooks and Run Them Manually, on page 67 apply to this automatic option. Note, however, that:

- You must ensure that none of the required linking parameters are left empty. The user interface indicates the required parameters.
- You must not set any of the form fields as "runtime" parameters. If you are running Playbooks automatically, you will not have the option to choose a value at runtime.
- If you are a non-admin user, ensure that you have access to the **Auto Remediation** task. Unless you have access to this task, you cannot unlink or link KPIs to Playbook with automatic remediation.

  Prerequisites:

  - Ensure that the Health Insights application is installed.
  - Ensure that **Playbook Job Scheduling** is enabled and **Credential Prompt** is disabled in the Device Override Credentials page. For more information, see Configure Change Automation Settings, on page 3.

  You must have Crosswork system administrator privileges to change these settings. Once these settings are saved, you cannot change them unless you first use the Crosswork Manager to uninstall, then reinstall both the Change Automation and Health Insights applications.

  To enable the task permission, do the following:

  1. Go to **Administration** > **Users and Roles** > **Roles**.
  2. Under the **Roles** pane, select the role for which you want to grant the access.
  3. Under the **Task Permissions** tab, enable the **Auto Remediation** check box and click **Save**.

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

Step 2 Select the KPI you want to link to one or more Playbooks. You can use filters to find the KPI you want, as explained in Manage KPIs, on page 62.

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 to see.

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

- The **Hardware Platform** and **Software Platform** with which the Playbook is compatible.
- The minimum software **Version** required to execute the Playbook.
- The **KPI Alert Severity** level needed to trigger a run of this Playbook. Note that, if you will be choosing multiple Playbooks to run when a KPI alert is raised, be aware that Playbooks do not share severity levels. If you have selected a **Critical** severity level for one Playbook, you must select **Major**, **Minor**, **Warning** or **Info** severities for a second Playbook, and another still for a third Playbook.
- Under the **Set Playbook Execution** field, select **Automatic**. Note that, if you or a Crosswork administrator have not already done so, Crosswork will prompt you to enable **Playbook Job Scheduling** (and disable **Credential Prompt** overrides) in order to enable automatic Playbook execution.
- Modify the **Set Playbook Parameters** default values to be used when the Playbook runs. In many cases, you can select from a range of default values. You can also enter your own. These values vary widely, depending on the Playbook and its purpose. For help, see the information offered on screen for the Playbook you have selected.

Step 6 Verify or modify the **Source** and other 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 Playbooks shown next to the name of the KPI in the **Key Performance Indicators (KPIs)** list.

Step 8 If you want to run more Playbooks (up to three Playbooks total): Repeat steps 5 through 7 for each additional Playbook you want to run when an alert for this KPI is raised.

Step 9 To change the Playbook parameters linked to a given KPI, repeat steps 5 through 7 for that KPI, but this time choose the Playbook whose settings you want to modify. If you have chosen multiple KPIs, you can switch among them by clicking on the Playbook tiles at the top of the window. To unlink a Playbook entirely, select the KPI and click Unlink.

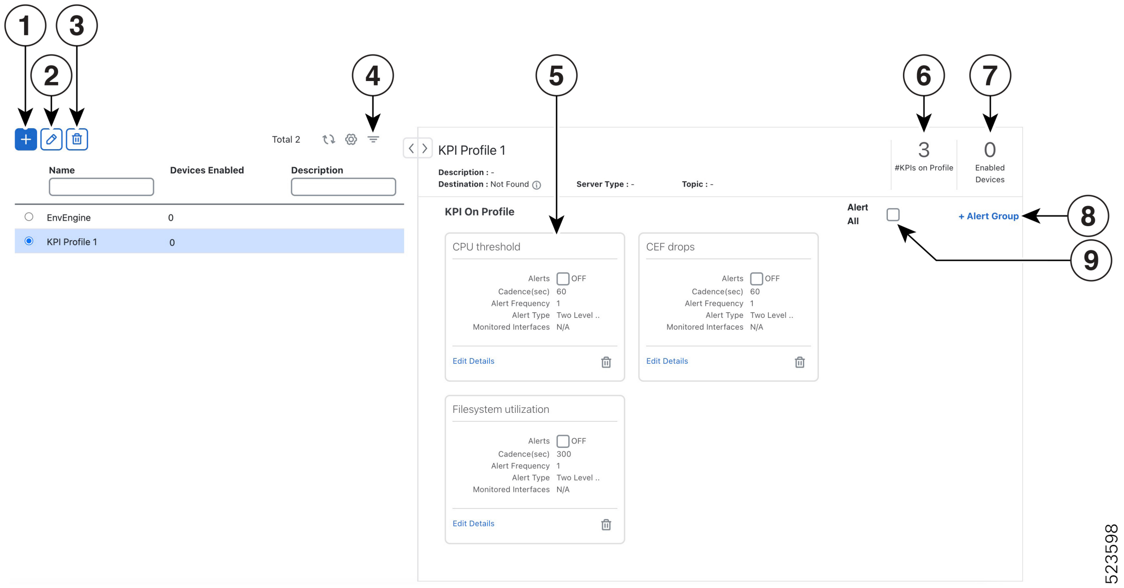
Manage KPI Profiles

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.

Figure 47: KPI Profiles



Total 2

Name	Devices Enabled	Description
○ EnvEngine	0	
● KPI Profile 1	0	

KPI Profile 1

Description : -
Destination : Not Found
Server Type : -
Topic : -

3 #KPIs on Profile
0 Enabled Devices

KPI On Profile

Alert All □

+ Alert Group

CPU threshold
Alerts □ OFF
Cadence(sec) 60
Alert Frequency 1
Alert Type Two Level ..
Monitored Interfaces N/A
Edit Details

CEF drops
Alerts □ OFF
Cadence(sec) 60
Alert Frequency 1
Alert Type Two Level ..
Monitored Interfaces N/A
Edit Details

Filesystem utilization
Alerts □ OFF
Cadence(sec) 300
Alert Frequency 1
Alert Type Two Level ..
Monitored Interfaces N/A
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 72.
2	**Edit KPI Profile**: Select a user-created KPI Profile in the list and then click ✎ to edit it.
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. Filtering is case-sensitive.
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. For KPI Profiles with custom KPI, the Alert checkbox will be disabled, and an alarm will be raised to inform users that alerting is disabled for the profile.
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 72
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.

To avoid problems with alerting, ensure that each KPI **Profile Name** you assign is unique and does not share sub strings with other KPI profiles. For example: In a set of three KPI profiles with the IDs "L2", "L2SNMP" and "L2GRPC", all three profiles IDs contain the sub string "L2".

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 the Cisco Crosswork Network Controller Administration Guide topic, Add or Edit a Data Destination.

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

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

b) **Recommended KPIs**: Use this option if you want the system to recommend KPIs for your devices. Clicking **Recommended KPIs** displays a list of your devices from the network. You can filter the device list by entering relevant values in the Name field, or by using tags. Select a device from the list to show recommended KPIs on the right side. Select the desired 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 Profiles on Devices, on page 75

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:

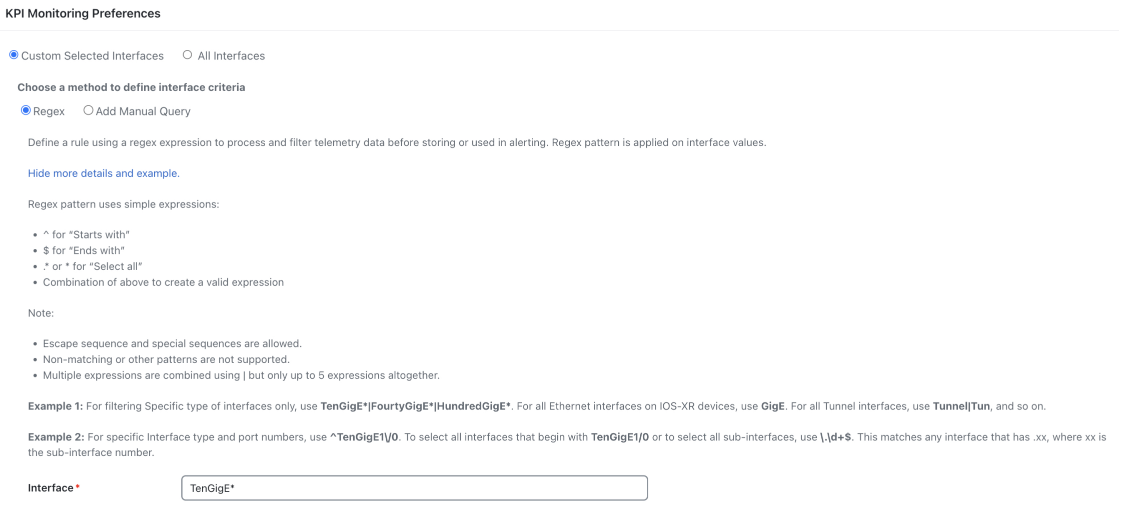
- **Common Parameters**
  - **Alert**: This is an on/off toggle switch for alerting. Based on the **Alert** parameter value, the corresponding alerting logic is deployed. Alerting can be enabled even after the KPI Profile has been applied to the devices.

    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.

Figure 48: KPI Monitoring Preferences



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.

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 * TenGigE*

  - **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 Profiles on Devices, on page 75.

See Disable KPI Profiles on Devices or Device Groups, on page 78 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.

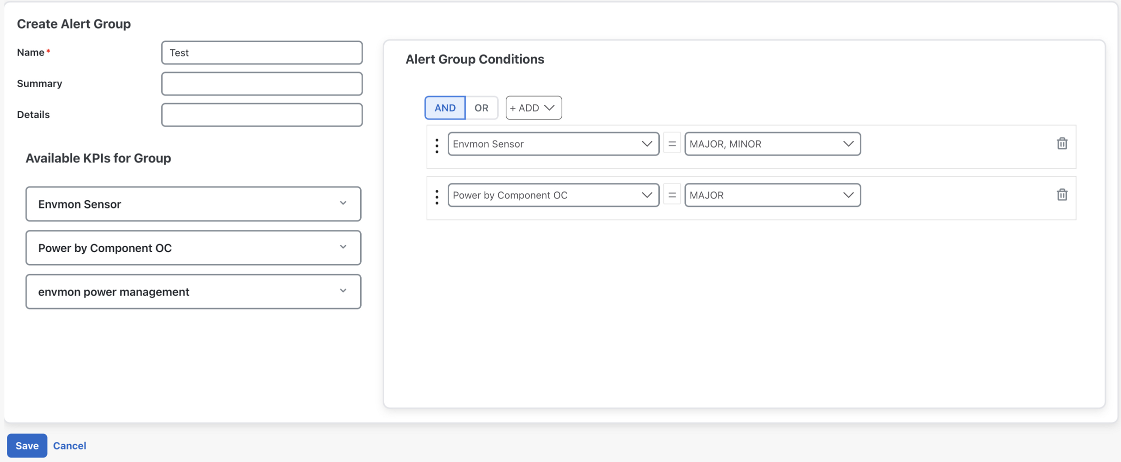
Step 12 Provide a relevant entry in the **Name** field. **Summary** and **Details** are optional fields.

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 multiple 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.

Figure 49: Create Alert Group



Create Alert Group

Name* Test

Summary

Details

Available KPIs for Group

- Envmon Sensor
- Power by Component OC
- envmon power management

Alert Group Conditions

AND OR + ADD

Envmon Sensor = MAJOR, MINOR

Power by Component OC = MAJOR

Save Cancel

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 Profiles 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

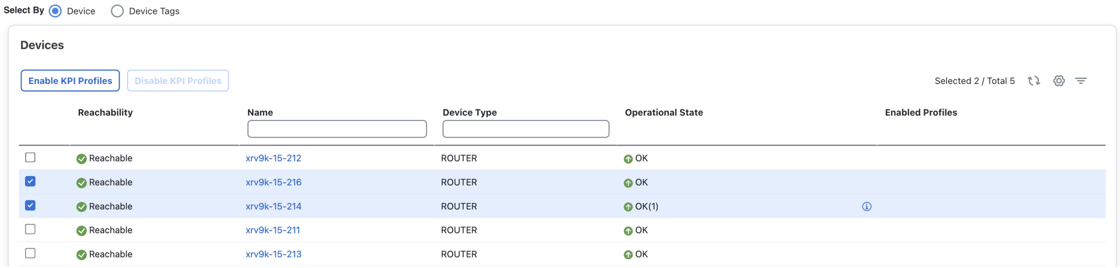
- You can only enable KPI Profiles with MDT-based KPIs on a device that has been mapped to a Cisco Network Services Orchestrator (Cisco NSO) provider and attached to a Crosswork Data Gateway.
- Do not enable KPI Profiles on devices that are not reachable.
- The load that is created on Cisco Crosswork 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 the topic Monitor Crosswork Data Gateway Health in the Cisco Crosswork Network Controller Administration Guide.

To enable KPI Profiles 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.

Figure 50: Devices Window



Select By ● Device ○ Device Tags

Devices

Enable KPI Profiles | Disable KPI Profiles

Selected 2 / Total 5

	Reachability	Name	Device Type	Operational State	Enabled Profiles
□	✓ Reachable	xrv9k-15-212	ROUTER	OK	
☑	✓ Reachable	xrv9k-15-216	ROUTER	OK	
☑	✓ Reachable	xrv9k-15-214	ROUTER	OK(1) ⓘ	
□	✓ Reachable	xrv9k-15-211	ROUTER	OK	
□	✓ Reachable	xrv9k-15-213	ROUTER	OK	

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.

Note You cannot enable a KPI on a device that is attached to a standard Crosswork Data Gateway. Also, you cannot move a KPI-enabled device from extended Crosswork Data Gateway to standard Crosswork Data Gateway. In both cases, Crosswork displays 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.

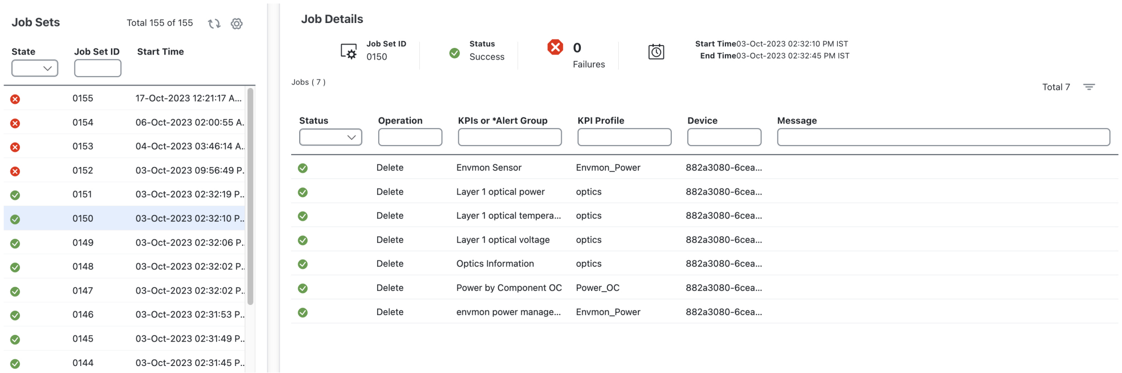
The **Alert** flag for the KPI profile (click **Edit Details** on the relevant KPI) must be turned **ON** in order to trigger an alert when the data is collected.

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.

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.

Figure 51: KPI Job History



Job Sets — Total 155 of 155

State	Job Set ID	Start Time
✗	0155	17-Oct-2023 12:21:17 A...
✗	0154	06-Oct-2023 02:00:55 A..
✗	0153	04-Oct-2023 03:46:14 A..
✗	0152	03-Oct-2023 09:56:49 P..
✓	0151	03-Oct-2023 02:32:19 P..
✓	0150	03-Oct-2023 02:32:10 P..
✓	0149	03-Oct-2023 02:32:06 P..
✓	0148	03-Oct-2023 02:32:02 P..
✓	0147	03-Oct-2023 02:32:02 P..
✓	0146	03-Oct-2023 02:31:53 P..
✓	0145	03-Oct-2023 02:31:49 P..
✓	0144	03-Oct-2023 02:31:45 P..

Job Details

Job Set ID 0150 | Status Success | 0 Failures | Start Time03-Oct-2023 02:32:10 PM IST End Time03-Oct-2023 02:32:45 PM IST

Jobs (7) — Total 7

Status	Operation	KPIs or *Alert Group	KPI Profile	Device	Message
✓	Delete	Envmon Sensor	Envmon_Power	882a3080-6cea...	
✓	Delete	Layer 1 optical power	optics	882a3080-6cea...	
✓	Delete	Layer 1 optical tempera...	optics	882a3080-6cea...	
✓	Delete	Layer 1 optical voltage	optics	882a3080-6cea...	
✓	Delete	Optics Information	optics	882a3080-6cea...	
✓	Delete	Power by Component OC	Power_OC	882a3080-6cea...	
✓	Delete	envmon power manage...	Envmon_Power	882a3080-6cea...	

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. For more information on monitoring the status of collection job, see the Monitor Collection Jobs section in the Cisco Crosswork Network Controller Administration Guide.

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

- 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 profiles 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.

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.

Any KPI job stuck in the processing state that does not complete within 60 minutes will be marked as "failed". After addressing any underlying issues (for example, device connectivity, credentials, NSO sync, and so on), the same job must be reactivated, as explained in Create a New KPI, on page 65.

Disable KPI Profiles 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.

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.

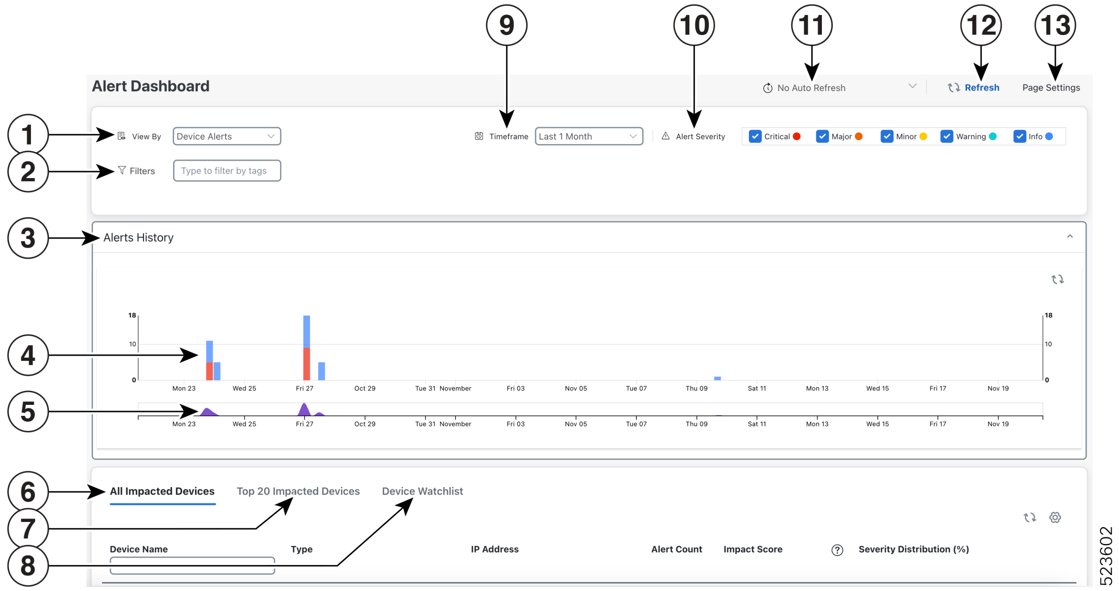


Figure 52: Health Insights Alert Dashboard

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

Item	Description
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 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.
5	**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**.
6	**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.
7	**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.

Item	Description
8	**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.
9	**Timeframe**: Specifies the time period for which the dashboard provides alert information: The last one hour, last day, last three days, last week, and last month. 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.

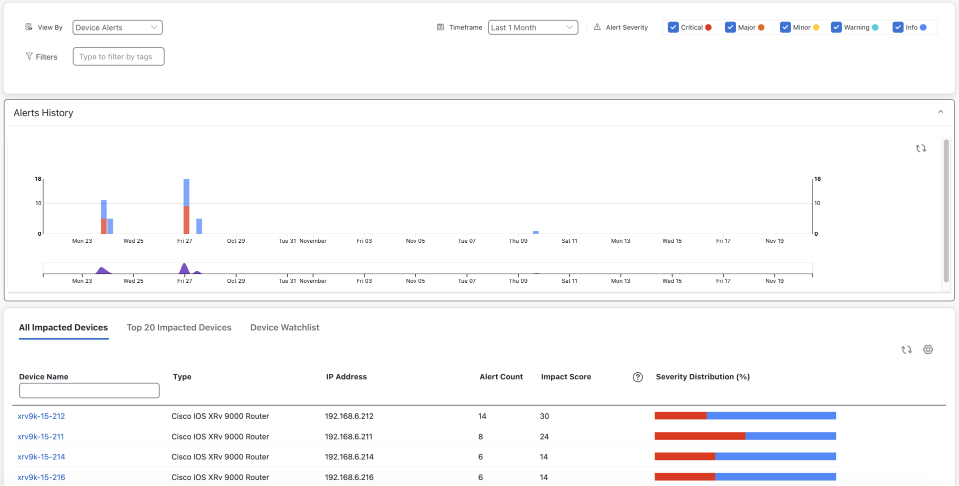
View Alerts for Network Devices

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 58.

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

Figure 53: Alert Dashboard



View By: Device Alerts
Filters: Type to filter by tags
Timeframe: Last 1 Month
Alert Severity: ☑ Critical ● ☑ Major ● ☑ Minor ● ☑ Warning ● ☑ Info ●

Alerts History

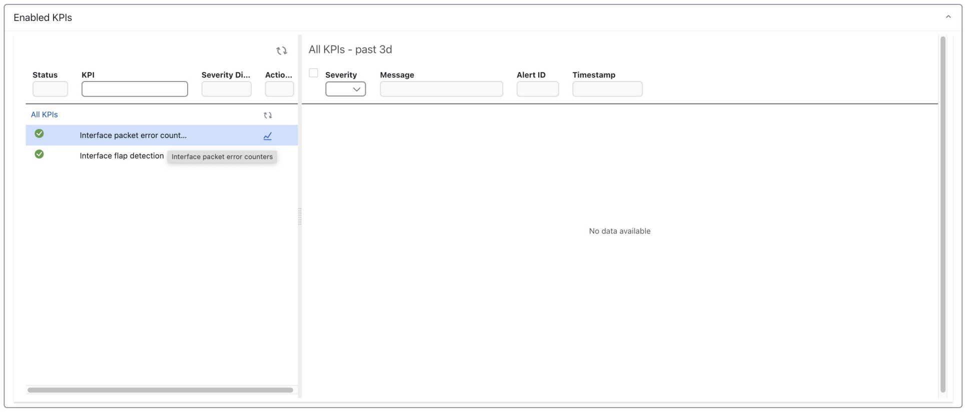
All Impacted Devices | Top 20 Impacted Devices | Device Watchlist

Device Name	Type	IP Address	Alert Count	Impact Score	Severity Distribution (%)
xrv9k-15-212	Cisco IOS XRv 9000 Router	192.168.6.212	14	30	🟥🟦
xrv9k-15-211	Cisco IOS XRv 9000 Router	192.168.6.211	8	24	🟥🟦
xrv9k-15-214	Cisco IOS XRv 9000 Router	192.168.6.214	6	14	🟥🟦
xrv9k-15-216	Cisco IOS XRv 9000 Router	192.168.6.216	6	14	🟥🟦

Step 2 Make sure that the **Device Alerts** view is displayed (select the **View By: 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**.

Figure 54: Device Alert Details



Enabled KPIs

Status	KPI	Severity Di...	Actio...
All KPIs			
✓	Interface packet error count...		
✓	Interface flap detection		

Interface packet error counters

All KPIs - past 3d

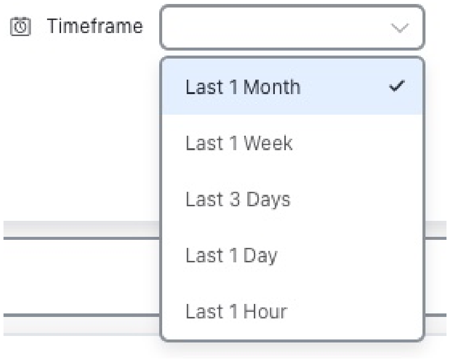
□	Severity	Message	Alert ID	Timestamp

No data available

The **Topology** map is a version of the map that you see when you select **Topology** from the main menu, but centered on the device for which you are viewing KPI alerts. The **Enabled KPIs** panel lists all the KPIs currently enabled on the selected device, plus a list of all the alerts for that device raised by any of the enabled KPIs during the past hour.

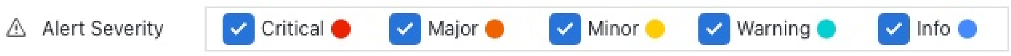
To see alerts for a different period, click the **Timeframe** dropdown (shown below) and select the time frame you want (up to `Last 1 Month`).

Figure 55: Timeframe Dropdown



To focus the display only on alerts of the severity you want, check or uncheck the boxes in the **Alert Severity** field, (shown below).

Figure 56: Alert Severity



Step 4 To view telemetry data received for any of the KPIs for this device: In the **Enabled KPIs** list on the left, click the 📈 icon next to the KPI whose telemetry data you want to see. Crosswork displays a popup telemetry data window like the one shown below. The popup window shows a timeline at the top, representing all the alert data received during the last 72 hours (with hourly slots), and relevant performance for the same period in a Grafana graph at the bottom.

Step 5 The timeline shows a blue box, with brushes on the sides, representing the limits of the time period shown in the graph at the bottom. Click on and move the blue box or the brushes on the timeline to select the desired time slot (up to 6 hours). Move the mouse cursor over any data point in the graph to view additional pop-up information for that data point.

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.

Graphical data is only visible for time slots for which alerts were triggered. Be default, the Grafana graph shows telemetry for the last six hours.

Step 6 To focus the Grafana view on a different timeframe, click the time period field (with the clock icon) shown at the top of the **Summary** tab. You can select time periods up to several years.

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 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 alerts' duration are displayed at the top of the Device/KPI view in the Alert dashboard. For more information, see View Alerts for Network Devices, on page 81. The alerts can also be queried using REST APIs. For more information, see the Cisco Crosswork Network Controller API Documentation on Cisco DevNet.

Troubleshoot Health Insights

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

Table 5: 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.
Operation timeouts can occur when adding a new KPI to an existing KPI Profile and then editing the newly added KPI.	Write times for KPI edits can take up to five minutes, so the edited KPI in the profile will be enabled eventually. If you find the timeout message a problem, you may want to disable the KPI profile for a short period until the write delay has passed.
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.