



Get Started

This section contains the following topics:

- [Basic Concepts, on page 1](#)
- [Before You Begin, on page 2](#)
- [High-Level Workflow, on page 3](#)
- [Workflow 1: Setup, on page 4](#)
- [Workflow 2: Monitor Key Performance Indicators, on page 5](#)
- [Workflow 3: Respond to KPI Data, on page 6](#)
- [Workflow 4: Schedule Playbooks, on page 6](#)
- [Workflow 5: Develop Custom KPIs, on page 7](#)
- [Workflow 6: Develop Custom Playbooks, on page 8](#)
- [Workflow 7: Set Up Data Collection for External Data Destinations, on page 8](#)
- [Workflow 8: Add Additional Device Collection Support, on page 10](#)

Basic Concepts

Cisco Crosswork Change Automation and Health Insights makes extensive use of three basic concepts. It is helpful to be familiar with them before you get started.

- **Tags:** Tags will be familiar from other Web applications. They are simple text strings you can attach to objects to help group them. Cisco Crosswork Change Automation and Health Insights comes with a short list of ready-made tags used to group network devices. You can create your own tags and use them to identify, find, and group devices for a variety of purposes. For example, in addition to type and geolocation, which are already stored when you on-board devices, you may want to identify and group them by their location in your network topology (Spine vs. Leaf), or the function they serve on your network (Provider vs. ProviderEdge). Tags are especially useful when setting up KPI monitoring, as you can apply a KPI to every member of a tagged group. You will want to develop your own tags for your purposes, and rework them as needed to meet changing needs.
- **Providers:** Cisco Crosswork Change Automation and Health Insights does not perform network discovery, inventory collection, monitoring, or configuration changes directly. Instead, it relies on providers, such as Cisco Network Services Orchestrator and Cisco WAN Automation Engine, to deliver these special services. The provider family determines the type of service that provider supplies to Cisco Crosswork Change Automation and Health Insights, and the parameters unique to that service, which must be configured. Because these providers are separate applications, you will be asked to register them and provide values for their unique parameters when you set up Cisco Crosswork Change Automation and

Health Insights. This architecture permits Cisco Crosswork Change Automation and Health Insights to devote all of its resources to processing and interpreting network events and rolling out changes in response to these events.


- **Credential Profiles:** For Cisco Crosswork Change Automation and Health Insights to be able to access a device or to interact with a provider, it must be able to present credentials. Rather than entering credentials each time they are needed, you can instead create credential profiles to securely store this information. The platform supports unique credentials for each type of access protocol, and allows you to bundle multiple protocols and their corresponding credentials in a single profile. Devices that use the same credentials can share a credential profile. For example, if all of your routers in a particular building share a single SSH user ID and password, you can create a single credential profile to allow Cisco Crosswork Change Automation and Health Insights to access and manage them.

Before You Begin

Before you begin using Cisco Crosswork Change Automation and Health Insights, Cisco recommends that you complete the following planning and information-gathering steps:

- **User Accounts :** Cisco recommends as a best practice that you create separate accounts for all of your users, so that there is an audit record of user activity on the system. Prepare a list of the people who will use Cisco Crosswork Change Automation and Health Insights. Decide on their user names and preliminary passwords, and create user profiles for them (see [Manage Users](#)).
- **User Roles:** Cisco recommends that you use role-based access control to confine users to just the software functions needed to perform their job duties. By default, every new user you create has full administrative privileges. Unless you want to extend the same privileges to every user, you will need to plan a system of user roles, create them, and assign them to the user profiles you create (see [Create User Roles](#)).
- **Credentials:** Gather the access credentials for your providers and for each supported protocol that you will use to monitor and manage your devices. For providers, this always includes user IDs, passwords, and connection protocols. For devices, it includes user IDs, passwords, and additional data such as the SNMP v2 read and write community strings, and SNMPv3 auth and privilege types. You will use these to create credential profiles (see [Basic Concepts, on page 1](#) and [Manage Credential Profiles](#)).
- **Tags:** Plan a preliminary list of custom tags to create when setting up the system, so that you can use them to group your devices when you first onboard them. As explained in [Basic Concepts, on page 1](#), you will want to consider grouping devices by functionality, so that you can apply KPI monitoring to tagged groups easily. You need not have a complete list of tags at first, as you can always add more later, but please note that all the tags you do plan to use must be in place before you need them; you cannot create them "on the fly" (see [Manage Tags](#) and [Create Tags](#)).
- **Providers:** As explained in [Basic Concepts, on page 1](#), providers do the basic work of direct interaction with network devices, so that Cisco Crosswork Change Automation and Health Insights can automate monitoring and responses to network events. Cisco Network Services Orchestrator (Cisco NSO) is the default provider used in nearly every Cisco Crosswork Change Automation and Health Insights installation, so you will need to gather the Cisco NSO IP address or host name, port and protocol, and the credentials to be used to communicate with it (which you will need to add as a credential profile). You will need to do the same for any other providers you may plan to use, such as Cisco Software Manager or Cisco WAN Automation Engine (see [Manage Providers](#) and [Add Cisco NSO Providers](#)). This includes system service providers, such as an FTP server to store syslogs, or Cisco Crosswork Situation Manager for processing alerts.

- **Devices:** Decide how you are going to onboard your devices: manually, via the user interface, or automatically via synchronization or CSV import. This determines the amount of additional information you will need to onboard your devices, which is covered in [About Adding Devices to Inventory](#).
- **External Data Destination(s):** Decide which external data destination (Kafka or gRPC) you are going to use and ensure it is set up to receive input from Cisco Crosswork Data Gateway.
- **KPI Profile(s):** KPIs (Key Performance Indicators) are used to monitor the health of the network. You can establish unique performance criteria based on the way a device or devices are used in the network. KPIs can be grouped to form a KPI Profile. It is helpful if you to have a good idea of the data you plan to monitor and the performance targets that you want to establish as you setup Health Insights.

Note that you can capture the devices, credential profiles, tags, and providers lists in spreadsheet form, convert the spreadsheet to CSV format, and then upload them in bulk to Cisco Crosswork Change Automation and Health Insights. You do this using the Import feature (accessed using the Import icon, ).

You can access CSV templates for each of these lists by clicking the Import icon in the corresponding places in the user interface. Select the **Download template** link when prompted to choose an export destination path and file name.

High-Level Workflow

The following workflow describes the main steps to getting started with Cisco Crosswork Change Automation and Health Insights.

Step	For details, see...
1. Populate the Cisco Crosswork Change Automation and Health Insights environment and set up Cisco Crosswork Data Gateway.	Workflow 1: Setup
2. Create KPI Profiles to monitor device Key Performance Indicators (KPIs) for issues and anomalies.	Workflow 2: Monitor Key Performance Indicators, on page 5
3. Link KPIs to playbooks.	Workflow 3: Respond to KPI Data, on page 6
4. Schedule Playbooks to perform routine maintenance.	Workflow 4: Schedule Playbooks, on page 6
5. Expand telemetry insight with custom KPIs.	Workflow 5: Develop Custom KPIs, on page 7
6. Remediate common scenarios and automate routine tasks with custom playbooks.	Workflow 6: Develop Custom Playbooks, on page 8
7. Create collection jobs for external data destinations. Note This is applicable only if the add on entitlement license for Cisco Crosswork Data Gateway API access has been purchased.	Workflow 7: Set Up Data Collection for External Data Destinations, on page 8
8. Adding additional device collection support	Workflow 8: Add Additional Device Collection Support, on page 10

Workflow 1: Setup

The first step in getting started with Cisco Crosswork Change Automation and Health Insights is to prepare the system for use. The table below provides topics to refer to for help when executing each of the following tasks:





1. Create a credential profile for at least one provider
2. Gather the setup for the provider using that credential profile
3. Create credential profiles for the devices from that provider
4. Get the devices from that provider
5. Create tags.
6. Create any additional credential profiles for other providers you need, the setup for those providers, and credential profiles for the devices from those providers
7. Add devices to Cisco Crosswork Data Gateway.


Note

This workflow assumes that you have already installed and enrolled Cisco Crosswork Data Gateway as explained in *Cisco Crosswork Change Automation and Health Insights 3.2 Installation Guide*.

If you were able to complete the recommended planning steps explained in [Before You Begin, on page 2](#), you should have all the information you need to finish each step in this workflow.

Step	Action
1. Ensure that your devices are themselves configured properly for communication and telemetry.	Refer to the guidelines and sample configurations in: Prerequisites for Onboarding Devices Sample Configuration for Devices in Cisco NSO Prerequisites for Device Model Driven Telemetry
2. Create credential profiles for your device provider and for your devices.	Follow the steps in Create Credential Profiles
3. Add the provider (Cisco NSO).	Follow the steps in About Adding Providers
4. Validate communications with the provider.	Check on the provider's reachability using the steps in Get Provider Details
5. Import or create tags.	To import them: Import Tags To create them: Create Tags
6. Onboard devices using the method you prefer.	See About Adding Devices to Inventory

Step	Action
7. Attach devices to Cisco Crosswork Data Gateway.	Review the Data Gateways pane (see Manage Cisco Crosswork Data Gateway Instances). The operational state of the Cisco Crosswork Data Gateway instance to which you want to attach devices must be Up . Follow the steps in Attach a Device to a Cisco Crosswork Data Gateway Instance
8. Validate Cisco Crosswork Change Automation and Health Insights communications with devices.	Review the Devices window (see Manage Network Devices). All the devices you have onboarded should be reachable. Click  to investigate any device whose Reachability State is marked as  (unreachable),  (degraded), or  (unknown).
9. (Optional) Create additional user accounts.	Follow the steps in Add Users
10. (Optional) Import or create additional credential profiles and providers.	To import providers: Import Providers To create providers: Add Providers Through the UI

Workflow 2: Monitor Key Performance Indicators

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

Step	Action
1. (Optional) Tag all of the devices whose KPIs you plan to monitor with a tag indicating the function they perform, per your plan.	Follow the tasks in the Manage Tags section. You can add them in the UI , or import them via CSV , and then apply them to the devices you want to monitor.
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.	Review the Cisco-supplied KPIs documented in List of Health Insights KPIs .
3. Group the relevant KPIs to form KPI Profiles.	Follow the instructions in Create a New KPI Profile .
4. Enable the appropriate KPI Profiles on the devices you want to monitor.	Review and follow the instructions in Monitor Network Health and KPIs

Workflow 3: Respond to KPI Data

The following workflow describes the steps to follow when using Cisco Crosswork Change Automation and Health Insights Playbook to reconfigure the network in response to changes in performance detected by your selected KPIs (after associating the Playbooks to the KPIs):

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 , using the Alerts Dashboard to research the alerts and their possible causes.
2. Review the Cisco-supplied Playbooks and determine which ones will allow you to address the situation.	Review the list of Plays, Playbooks, and generic parameters in the "Playbooks" and "Verbs" references in the Change Automation Developer Guide on Cisco Devnet .
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 Run Playbooks In Single Stepping Mode Run Playbooks In Continuous Mode
4. If the Playbooks are appropriate for your purposes, and the situation occurs often, link the selected Playbooks and KPIs, so alerts triggered by a KPI will always display the linked Playbook for selection by operators. Once the KPI and Playbook are linked, operators can click on the Remediation icon, modify the Playbook parameters as needed, and execute the selected Playbook.	Follow the steps in Link KPIs to Playbooks . Use the Remediation icon shown in View Alerts for Network Devices to trigger a run of a linked Playbook from a device or KPI alert.

Workflow 4: Schedule Playbooks

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

Step	Action
1. Identify routine maintenance tasks (such as throughput checks, software upgrades, SMU installs, and so on) that you perform on a regular schedule and that may be suitable for automation using one or more Cisco Crosswork Change Automation and Health Insights Playbooks.	See About Running Playbooks and View the Playbook List
2. Configure Playbooks to perform these tasks at the desired time.	See About Running Playbooks and Schedule Playbook Runs

Step	Action
3. Review the Change Automation Job History to review the current status of the Playbook and confirm that it ran successfully.	See Use the Change Automation Dashboard and View or Abort Playbook Jobs
4. Use the APIs to perform routine maintenance tasks from your own scripts and applications.	See the Cisco Crosswork Network Automation API Documentation on Cisco DevNet .

Workflow 5: Develop Custom KPIs

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

Step	Action
1. Review the existing KPIs to make sure the telemetry you want to monitor is not already available.	Follow the instructions in Monitor Network Health and KPIs , using the Alerts Dashboard to research the alerts and their possible causes.
2. Review the data available from the devices you want to monitor to see if they can supply the needed information: <ul style="list-style-type: none"> • If they can, proceed with building a custom KPI. • If they cannot: Contact Cisco to see if we can include the required data in a future version of the device code. <p>The latest information on the data your devices can provide is always available at the Cisco Telemetry Data Mapper (https://tdm.cisco.com).</p>	Review the KPIs in List of Health Insights KPIs .
3. Build the custom KPI and add it to a KPI Profile.	See Create a New KPI and Create a New KPI Profile
4. Enable the new KPI Profile on a test device and confirm that the data reported matches your expectations. Be aware that KPIs that depend on data over time to establish baseline performance will need some time to "calibrate" before they provide meaningful data.	See Enable KPI Profile on Devices and View Alerts for Network Devices
5. If the KPI Profile is meeting expectations, enable it on all devices where you consider it applicable.	Follow the steps in Enable KPI Profile on Devices .
6. Review the Health Insights Job History to make sure the KPI Profile was deployed to all targeted devices	See Verify the Deployment Status of Enabled KPIs

Workflow 6: Develop Custom Playbooks

The following workflow describes the steps to follow when deciding to develop a Cisco Crosswork Change Automation and Health Insights custom Playbook.

Step	Action
1. Review the existing Playbook to see if any of them meet your needs fully or partially.	Review the Plays, Playbooks, and parameters in the "Playbooks" and "Verbs" references in the Change Automation Developer Guide on Cisco Devnet .
2. Find the Playbook that most closely matches your requirements and export that Playbook. Once you get good at modifying Playbook, you may choose to build them from scratch and skip this step.	See Export Playbooks
3. Modify the exported Playbook or create a new Playbook as necessary to meet your requirements.	Review the "Custom Playbooks" tutorial in the Change Automation Developer Guide on Cisco DevNet .
4. Import the new Playbook and then perform a dry run, or run it in single-stepping or continuous mode against a test device or devices, to confirm that it performs as expected.	First, follow the instructions in Import Playbooks . Then: Perform a Dry Run of a Playbook Run Playbooks In Single Stepping Mode Run Playbooks In Continuous Mode
5. For a Playbook you have developed that meets your needs: <ul style="list-style-type: none"> • In response to KPI alerts: If the Playbook is meeting expectations, link it to the KPI that indicates the need for the Playbook to be run, so that it is easy for operators to trigger the Playbook in response. • For planned maintenance or configuration changes: Schedule the Playbook to run, or run it, at the planned time. 	See: Link KPIs to Playbooks Schedule Playbook Runs

Workflow 7: Set Up Data Collection for External Data Destinations

Crosswork allows you to add two types of external data destinations:

- Kafka Server
- gRPC Server

The following workflow describes the steps to follow to add external destinations to Crosswork and create collection jobs to feed these external data destinations.

Step	Action
<p>1. Ensure that you have set up the external data destination servers that you want to use.</p> <p>Also, if you are using an external Kafka server, ensure that you have created Kafka topics prior to Crosswork using them.</p>	<p>The target destination installation and administration are left to the user and outside the scope of this document. Please refer your Kafka/gRPC administration and configuration guide.</p> <p>Refer to the guidelines and sample configurations in:</p> <ul style="list-style-type: none"> Prerequisites for Onboarding Devices Sample Configuration for Devices in Cisco NSO Prerequisites for Device Model Driven Telemetry
<p>2. Add a data destination to Crosswork.</p>	<p>Review the Data Destinations pane (see Manage Data Destinations).</p> <p>Follow the steps in Add a Data Destination.</p>
<p>3. Ensure that prerequisites for device telemetry are met.</p>	<p>Refer to the guidelines and sample configurations in:</p> <ul style="list-style-type: none"> Prerequisites for Device Model Driven Telemetry
<p>4. Create collection jobs</p>	<p>Refer to the following topics (in order of their listing) for guidelines and sample configurations:</p> <ol style="list-style-type: none"> 1. About Collection Jobs 2. Collection Job Payload Model 3. Collection Jobs 4. Best Practices and Limitations for Creating Collection Jobs <p>Then, follow the steps in Create Collection Jobs.</p>
<p>5. Monitor collection jobs for status updates, issues, and alerts.</p>	<p>See Monitoring Collection Jobs.</p>

Workflow 8: Add Additional Device Collection Support

Cisco Crosswork Data Gateway allows you to register and deploy three types of custom software packages to expand device coverage for external data collection:

1. CLI Device Package
2. Custom MIB Packages
3. SNMP Device Packages

The following workflow describes the steps to follow to add a custom package.

Step	Action
1. If you want to use a CLI Device Package, Custom MIB Package, or an SNMP Device Package, add them to Cisco Crosswork Data Gateway prior to creating collection jobs.	Review the Custom Software pane (see Manage Custom Software Packages). Follow the steps in Add a Custom Software Package