



Get Up and Running (Post-Installation)

This section contains the following topics:

- [Before You Begin, on page 1](#)
- [Setup Workflow, on page 3](#)
- [Log In and Log Out, on page 4](#)

Before You Begin

Before you begin using the Cisco Crosswork applications, you are recommended to be familiar with the following basic concepts and complete the planning and information-gathering steps:

- **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.
- **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 the Crosswork application. Decide on their user names and preliminary passwords, and create user profiles for them. Crosswork also supports integration with many TACACS+ and LDAP servers to allow you to centrally manage user roles and accounts. See [Set Up User Authentication \(TACACS+, LDAP, and RADIUS\)](#) for more details.
- **Device-Access Groups:** Device-access groups (DAGs) are groups of devices that are used to define device access for users. Users associated with the DAGs are allowed to make configuration changes and provision services on the devices that belong to those DAGs. When a user is created, they must be assigned both a DAG (at least one) and a role. See [Manage Device Access Groups](#) for more details.
- **Credential Profiles:** For Cisco Crosswork 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 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 to access and manage them.

Before creating a credential profile, you must gather access credentials and supported protocols that you will use to monitor and manage your devices. 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. For

other type of providers (NSO, SR-PCE, Storage, Alert, and WAE), this always includes user IDs, passwords, and connection protocols. You will use these to create credential profiles.

- **Tags:** Tags are simple text strings you can attach to devices to help group them. Cisco Crosswork 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.

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. 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. Otherwise, you will need to manually go back and add them where you wish to use them. See [Create Tags](#) for more details.

- **Providers:** Cisco Crosswork applications rely on external services such as Cisco Network Services Orchestrator (NSO) or SR-PCE for various tasks like configuration changes, segment routing path computation, and so on. In order to manage the access and reuse of information between Crosswork applications, a Provider (such as NSO and SR-PCE) needs to be configured for each external service. The provider family determines the type of service that provider supplies to Cisco Crosswork, and the parameters unique to that service, which must be configured. The parameters needed to configure a provider depend on the type of Crosswork application is used. It is important to review and gather each Crosswork application requirement, before configuring a Provider. For more information, see [About Provider Families](#) and [Provider Dependency](#).
 - Cisco Network Services Orchestrator (Cisco NSO) is used by many Crosswork Applications to make changes to device configurations and to provision services on devices. To add Cisco NSO as a provider you will need the IP address and credentials used to communicate. See [Add Cisco NSO Providers](#) for more details.



Note Additional steps are needed when using Cisco NSO in LSA mode. See [Enable Layered Service Architecture \(LSA\)](#) for more details.

- If you plan to use Crosswork Optimization Engine, at least one Cisco SR-PCE provider, at minimum, must be defined in order to discover devices and to distribute policy configuration to devices. Additional SR-PCEs can be used for more complex network topologies and redundancy. You can either add devices to the system yourself (see [Add Devices to the Inventory](#) for more details) or auto-onboard them via the SR-PCE discovery (see [Add Cisco SR-PCE Providers](#) for more details). While you can change the configuration at any time it is ideal to decide which process you will use before you get too far into the deployment and configuration of Crosswork.
- **Devices:** You can onboard devices using the UI, a CSV file, an API, SR-PCE discovery, or ZTP. The way a device is onboarded determines the type of information needed to configure a device in Crosswork. Also, Crosswork can forward device configuration to NSO which can change how you provision an NSO provider. For more information, see [Add Devices to the Inventory](#).
- **External Data Destination(s):** Cisco Crosswork functions as the controller for the Cisco Crosswork Data Gateway. Operators who plan to have Cisco Crosswork Data Gateway forward data to other data destinations, need to know about the format required by those destinations and other connection requirements. This is covered in detail in [Cisco Crosswork Data Gateway](#).
- **Labels:** Labels are used with Crosswork Change Automation to restrict which users are able to execute a playbook. For example, while you may want lower-level operators to be able to run check playbooks

you may use labels to prevent them from running more complex or impactful playbooks that make changes to network device configuration.

- If you plan to use Crosswork Health Insights, **KPI (Key Performance Indicators) Profile(s)** 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 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.
- If you plan to install the Crosswork Service Health application, you should review the samples provided to determine if they are adequate for monitoring devices in your network.

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 the Cisco Crosswork application that you are using with the help of the Import feature. 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.

Setup Workflow

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







Note This workflow assumes that you have already installed Cisco Crosswork Applications and Crosswork Data Gateway. For the installation instructions, please refer to the latest version of *Cisco Crosswork Network Controller 6.0 Installation Guide*.

If you were able to complete the recommended planning steps explained in "Before you begin", you should have all the information you need to finish each step in this workflow.

Table 1: Tasks to Complete to Get Started with Cisco Crosswork

Step	Action
1. Ensure that your devices are configured properly for communication and telemetry.	Refer to the guidelines and sample configurations in: Telemetry Prerequisites for New Devices Sample Configuration for Cisco NSO Devices
2. (Optional) If the set-up is a Cisco NSO LSA deployment, enable LSA.	Follow the steps in Enable Layered Service Architecture (LSA)
3. Create credential profiles.	Follow the steps in Create Credential Profiles
4. Add the provider(s).	Follow the steps in About Adding Providers
5. Validate communications with the provider(s).	Check on the provider's reachability using the steps in Get Provider Details

Step	Action
6. Import or create tags.	To import them: Import Tags To create them: Create Tags
7. Onboard devices using the method you prefer.	See Add Devices to the Inventory
8. Setup Crosswork Data Gateway	Follow the steps in Set Up Crosswork Data Gateway to Collect Data .
9. Validate Cisco Crosswork 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).
10. (Optional) Enable source IP for auditing.	If you want to log the user's IP address for auditing and accounting, see Configure AAA Settings .
11. (Optional) Create additional user accounts and user roles.	Follow the steps in Manage Users and Create User Roles .
12. (Optional) Import or create additional credential profiles and providers.	To import providers: Import Providers To create providers: Add Providers Through the UI
13. (Optional) Group your devices logically as per your requirement.	Follow the steps in Use Device Groups to Filter your Topology Map .
14. (Optional) Set display preferences for your topology.	Follow the steps in Use Internal Maps Offline for Geographical Map Display and Show Link Utilization by Color .

Log In and Log Out

The Cisco Crosswork user interface is browser-based. For the supported browser versions, see the *Cisco Crosswork Network Controller 6.0 Installation Guide*.

**Attention**

- Cisco Crosswork locks out users for a specified period of time after repeated unsuccessful login attempts. Users can attempt to log in with the correct credentials once the wait time is over. Users remain locked out until they enter the valid login credentials. The number of unsuccessful login attempts and the lockout time are configured by the administrators in the **Local Password Policy**. For more information, see [Configure AAA Settings](#).
- The Crosswork login page is not rendered when the CAS (Central Authentication Service) pod is restarting or not running.
- If a user has multiple sessions open from same client (via multiple tabs/windows) and logout/terminate session is performed for that session from one of the windows, the logout screen is displayed on that window while the following error message is displayed on all other tabs/windows: "Your session has ended. Log into the system again to continue".

Step 1

Open a web browser and enter:

```
https://<Crosswork Management Network Virtual IP (IPv4)>:30603/
```

or

```
https://[<Crosswork Management Network Virtual IP (IPv6)>]:30603/
```

Note

- The IPv6 address in the URL must be enclosed with brackets.
- When you access Cisco Crosswork from your browser for the first time, some browsers display a warning that the site is untrusted. When this happens, follow the prompts to add a security exception and download the self-signed certificate from the server. After you do this, the browser accepts the Cisco Crosswork server as a trusted site in all subsequent logins.


Step 2

The Cisco Crosswork browser-based user interface displays the login window. Enter your username and password. The default administrator user name and password is **admin**. This account is created automatically at installation (see [Administrative Users Created During Installation](#)). The initial password for this account must be changed during installation verification. Cisco strongly recommends that you keep the default administrator credential secure, and never use it for routine logins. Instead, create new user roles with appropriate privileges and assign new users to those roles. At least one of the users you create must be assigned the "admin" role.

Step 3

Click **Log In**.

Step 4

To log out, click  in the top right of the main window and choose **Log out**.

