Get Up and Running (Post-Installation)

This section contains the following topics:

Before You Begin

Before using the Cisco Crosswork Network Controller applications, it is recommended that you familiarize yourself with basic concepts and complete necessary planning and information-gathering steps.:

- **User Roles**: Cisco recommends using role-based access control to restrict users to only the software functions necessary for their job duties. By default, new users have full administrative privileges. To avoid extending these privileges to every user, you should plan a system of user roles, create these roles, and assign them to user profiles accordingly.

- **User Accounts**: Cisco recommends creating separate accounts for all users to maintain an audit record of user activity on the system. Prepare a list of users for the Crosswork Network Controller applications, decide on their usernames and preliminary passwords, and create user profiles for them. Crosswork Network Controller also supports integration with TACACS+ and LDAP servers for centralized management of user roles and accounts. For more details, see Set Up User Authentication (TACACS+, LDAP, and RADIUS).

- **Device-Access Groups**: Device-Access Groups (DAGs) are groups of devices that define device access for users. Users who are associated with DAGs can make configuration changes and provision services on the devices within those groups. When creating a user, you must assign them at least one DAG and a role. For more details, see Manage Device Access Groups.

- **Credential Profiles**: For the Crosswork Network Controller to access a device or interact with a provider, it must present credentials. Instead of entering credentials each time, you can create credential profiles to securely store this information. The platform supports unique credentials for each access protocol and allows bundling multiple protocols and their corresponding credentials into a single profile. Devices using the same credentials can share a credential profile. For example, if all routers in a particular building share a single SSH user ID and password, you can create one credential profile for Crosswork Network Controller to manage them.

  Before creating a credential profile, gather the access credentials and supported protocols needed to monitor and manage your devices. This includes user IDs, passwords, and additional data such as SNMPv2 read and write community strings, and SNMPv3 authentication and privilege types. For other providers

(NSO, SR-PCE, Storage, Alert, and WAE), this always includes user IDs, passwords, and connection protocols. Use this information to create credential profiles.

- **Tags**: Tags are simple text strings that you can attach to devices to help group them. The Crosswork Network Controller includes a short list of pre-made tags for grouping network devices. You can also create your own tags to identify, find, and group devices for various purposes.

  Plan a preliminary list of custom tags to create when setting up the system, so you can use them to group your devices when you first onboard them. You don't need a complete list of tags initially, as you can always add more later. However, ensure that all the tags you plan to use are in place before you need them. Otherwise, you must manually go back and add them where you wish to use them. For more details, see Create Tags.

- **Providers**: Crosswork Network Controller applications rely on external services like Cisco Crosswork Network Services Orchestrator (NSO) or SR-PCE for tasks such as configuration changes and segment routing path computation. To manage access and reuse information between Crosswork Network Controller applications, a provider (for example, NSO, SR-PCE) must be configured for each external service. The provider family determines the type of service supplied to Crosswork Network Controller and the unique parameters that must be configured. The parameters needed to configure a provider depend on the type of Crosswork Network Controller application used. It is important to review and gather each application's requirements before configuring a provider. For more information, see About Provider Families and Provider Dependency.

  - Cisco Crosswork Network Services Orchestrator (NSO) is used by many Crosswork Network Controller applications to make changes to device configurations and provision services on devices. To add NSO as a provider, you need the IP address and credentials used for communication. For more details, see Add Cisco NSO Providers.

Note Additional steps are required when using NSO in LSA mode. For more details on these steps, see Enable Layered Service Architecture (LSA).

  - If you plan to use Crosswork Optimization Engine, at least one Cisco SR-PCE provider must be defined to discover devices and distribute policy configurations to devices. Additional SR-PCEs can be used for more complex network topologies and redundancy. You can either manually add devices to the system (see Add Devices to the Inventory for more details) or auto-onboard them via 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 getting too far into the deployment and configuration of Crosswork Network Controller.

- **Devices**: You can onboard devices using the UI, a CSV file, an API, SR-PCE discovery, or zero touch provisioning. The method used to onboard a device determines the type of information needed to configure it in Crosswork Network Controller. Also, Crosswork Network Controller can forward device configuration to NSO, which may affect how you provision an NSO provider. For more information, see Add Devices to the Inventory.

Note For information on device configuration, device monitoring, and device management workflows, see the *Crosswork Network Controller 7.0 Device Lifecycle Management* guide.

- **External Data Destination(s)**: Crosswork Network Controller functions as the controller for the Crosswork Data Gateway. Operators planning to have Crosswork Data Gateway forward data to other data destinations must understand 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 can execute a playbook. For example, you may allow lower-level operators to run check playbooks but use labels to prevent them from running more complex or impactful playbooks that make changes to network device configurations.
- If you plan to use Crosswork Health Insights, **KPI (Key Performance Indicators) Profiles** are used to monitor the health of the network. You can establish unique performance criteria based on how a device or devices are used in the network. KPIs can be grouped to form a KPI Profile. It is helpful to have a clear idea of the data you plan to monitor and the performance targets you want to establish as you set up Health Insights.
- If you plan to install the Crosswork Service Health application, you should review the provided samples 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 Crosswork Network Controller application using 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 filename.

Setup Workflow

The first step in getting started with Crosswork Network Controller 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 Crosswork Network Controller Applications and Crosswork Data Gateway. For the installation instructions, please refer to the latest version of *Cisco Crosswork Network Controller 7.0 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 Crosswork Network Controller

Step	Action
1. Ensure that your devices are configured properly for communication and telemetry.	Refer to the guidelines and sample configurations in: Configuration Prerequisites for New Devices Sample Configuration for Cisco NSO Devices
2. Create user accounts and user roles.	Follow the steps in Manage Users and Create User Roles.
3. Create credential profiles.	Follow the steps in Create Credential Profiles

Step	Action
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
6. Import or create tags.	To import them: Import Tags To create them: Create Tags
7. Onboard your devices.	See Add Devices to the Inventory. For more information, see the *Cisco Crosswork Network Controller 7.0 Device Lifecycle Management* guide.
8. Setup Crosswork Data Gateway	Follow the steps in Set Up Crosswork Data Gateway To Collect Data.
9. Validate Crosswork Network Controller communications with devices.	Review the **Devices** window. All the devices you have onboarded should be reachable. Click ⓘ to investigate any device whose **Reachability State** is marked as ✖ (unreachable), 🟠 (degraded), or ❓ (unknown). For more information, see the *Cisco Crosswork Network Controller 7.0 Device Lifecycle Management* guide.
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 Health by Color.

Log In and Log Out

The Crosswork Network Controller user interface is browser-based. For the supported browser versions, see the *Compatibility Information* section in the *Cisco Crosswork Network Controller 7.0 Release Notes*. .

Attention

- Crosswork Network Controller 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 Network Controller 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 Crosswork Network Controller 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 Crosswork Network Controller server as a trusted site in all subsequent logins.

Step 2 The 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**.