



Perform Administrative Tasks

This section contains the following topics:

- [Manage Cisco Crosswork Network Automation, on page 1](#)
- [Manage Backup and Restore, on page 11](#)
- [Manage Users, on page 13](#)
- [Manage TACACS+ Servers, on page 19](#)
- [Manage LDAP Servers, on page 20](#)
- [Define Network Visualization Display Settings, on page 22](#)
- [Manage Certificates, on page 22](#)
- [Smart Licensing Registration, on page 24](#)
- [Security Hardening Overview, on page 29](#)

Manage Cisco Crosswork Network Automation

The **Crosswork Manager** window gives you consolidated information about the current status of each installed Cisco Crosswork Change Automation and Health Insights application and its supporting services. It also supplies tools and information that, with support and guidance from your Cisco Customer Experience account team, you can use to identify, diagnose and fix issues with Cisco Crosswork Change Automation and Health Insights.

Select **Admin > Crosswork Manager** to display a **Crosswork Manager** window, with information like the window shown in the following example.

The screenshot displays the Cisco Crosswork Network Automation Admin interface. The main dashboard, titled "CrossWork Applications Summary", shows the following statistics:

Category	Count
Total	5
Running	5
Down	0
Degraded	0

Below the summary, the interface lists several application categories with their status and actions:

- Application Details:** Status: Running (2 Services - 2 Running | 0 Down | 0 Degraded). Description: No Data Available. Recommendation: None at this stage.
- Change Automation:** Status: Running (2 Services - 2 Running | 0 Down | 0 Degraded). Description: robot-nca: All dependencies are reachable. Recommendation: None at this stage.
- Topology:** Status: Running (3 Services - 3 Running | 0 Down | 0 Degraded). Description: nca4-topo-svc: nca4 DB is available at this time. Recommendation: None at this stage.
- Collection Infra:** Status: Running (9 Services - 9 Running | 0 Down | 0 Degraded). Description: dg-manager: Data Gateway Manager Service started. State: Running| magellan: magellan started up robot-dimnvmgr: Inventory Manager Service is running.
- Core Infra:** Status: Running (11 Services - 11 Running | 0 Down | 0 Degraded). Description: csw-clms: **

Each application entry includes a "Show Service Details" link and a set of action buttons: Restart, Stop, Start, Collect All, Collect Logs, and Collect Metrics.

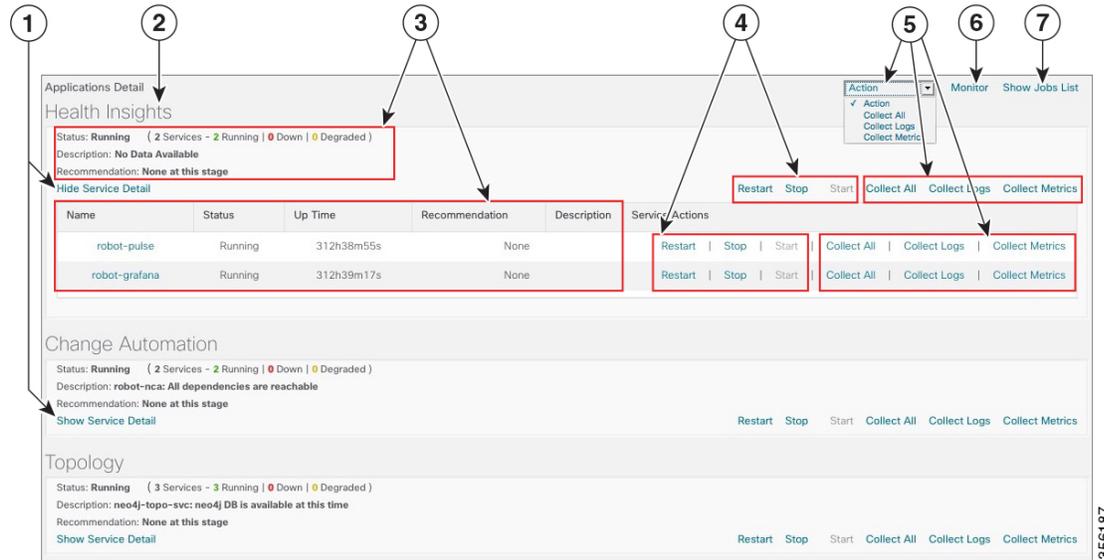
The **Crosswork Manager** window has two main views. The **Crosswork Applications Summary** view, at the top of the window, is a dashboard giving you a quick look at the overall health of the system. It displays the total number of Cisco Crosswork Change Automation and Health Insights applications currently installed in the system, and how many of that total are **Running**, **Down**, or **Degraded**.

The **Applications Detail** view, below the **Crosswork Applications Summary** view, allows you to:

- View the name and current runtime status of each installed application and its supporting services.
- Get advice about what to do when an application or one of its services has issues.
- Collect logs and metrics on any application or service, or for the system as a whole.
- Stop, start, or restart any application or service.

The **Applications Detail** view, shown in the following figure, is the best way to investigate any system health issues indicated in the **Crosswork Applications Summary**.

Figure 1: Applications Detail View



366187

Item	Description
1	Click the Show/Hide Service Detail link in each application tile to view the detailed status of the underlying services for that application.
2	An application tile like this shows the current status of the named application and a summary of the status of that application's services. This includes the total number of services, and how many of those services are Running, Down, or Degraded.
3	Both the application tile and its Service Detail table provide the name, status, description and recommendation for the respective application or service. The Service Detail table also provides service uptime, and you can click on the link in the Name column to see more details about the service, such as its process ID and pod identifier.
4	To control an application or service, click on any of the links in this section of the application tile or Service Detail table. You can click: <ul style="list-style-type: none"> • Restart to restart the application or service. • Stop to stop the application or service. • Start to start the application or service. See Control Cisco Crosswork Network Automation Applications and Services , on page 10.

Item	Description
5	<p>To gather logs and metrics for the entire system, or for any application or service, click on any of the "collect" links at the system (in the dropdown menu), application, or service level. You can choose:</p> <ul style="list-style-type: none"> • Collect All to collect both logs and metrics. • Collect Logs to collect only logs. • Collect Metrics to collect only metrics. <p>See Collect and Share Cisco Crosswork Network Automation Logs and Metrics, on page 8.</p>
6	<p>Click the Monitor link to monitor individual Cisco Crosswork Change Automation and Health Insights functions and features, using analytical dashboards and data gathered over the last 24 hours of run time.</p> <p>See Monitor Cisco Crosswork Network Automation Functions in Real Time, on page 4.</p>
7	<p>Choosing any of the control or collect actions at the system, application or service level will initiate a job. You can view each job's progress by clicking the Show Jobs List link at the top right corner of the window. You can also use the Show Jobs List to publish collected logs and metrics files, and check on the status of publish jobs you initiate.</p>

Monitor Cisco Crosswork Network Automation Functions in Real Time

You can monitor the health of Cisco Crosswork Change Automation and Health Insights and any of its functions in real time, using a set of monitoring dashboards you can access from the **Crosswork Manager** window.

Cisco Crosswork Change Automation and Health Insights uses Grafana to create these dashboards. They give you a graphical view of the product's infrastructure, using metrics collected in its database. You can use these dashboards to diagnose problems you may encounter with individual Cisco Crosswork Change Automation and Health Insights applications or their underlying services.

There are multiple monitor dashboards, categorized by the type of functionality they monitor and the metrics they provide, as shown in the following table.

Table 1: Monitoring Dashboard Categories

This dashboard category...	Monitors...
Change Automation	Playbook functions. Metrics include the number of MOP jobs executed, response latency, API calls, database activity, and so on.
Collection - Manager	Device-data collection functions. Metrics include telemetry collection latencies, total collection operations, memory and database activity related to telemetry, delayed collections, and so on.
Health Insights	Key Performance Indicator functions. Metrics include the number of KPI alerts, API calls, and so on.
Infra	System infrastructure messaging and database activity.

This dashboard category...	Monitors...
Inventory	Inventory manager functions. These metrics include total numbers of inventory change activities.
Platform	System hardware and communications usage and performance. Metrics include disk and CPU usage, database size, network and disk operations, and client/server communications.

To conserve disk space, Cisco Crosswork Change Automation and Health Insights maintains a maximum of 24 hours of collected metric data.

Grafana is an open-source visualization tool. The following provides general information about how to use the Cisco Crosswork Change Automation and Health Insights implementation of Grafana. For more information about Grafana itself, see <https://grafana.com> and <http://docs.grafana.org>

Step 1 From the main menu, choose **Admin > Crosswork Manager**.

Step 2 At the right, just below the **Crosswork Applications Summary** view, click the **Monitor** link, highlighted below.



The Grafana user interface appears within the **Crosswork Manager** window, replacing the **Applications Detail** view.

Step 3 In the Grafana user interface, click **Home**. Grafana displays the list of monitoring dashboards and their categories, as shown in the following example.

Home / Admin / Crosswork Manager

CrossWork Applications Summary

5 Total	5 Running	0 Down
------------	--------------	-----------

Action [v] St

Find dashboards by name

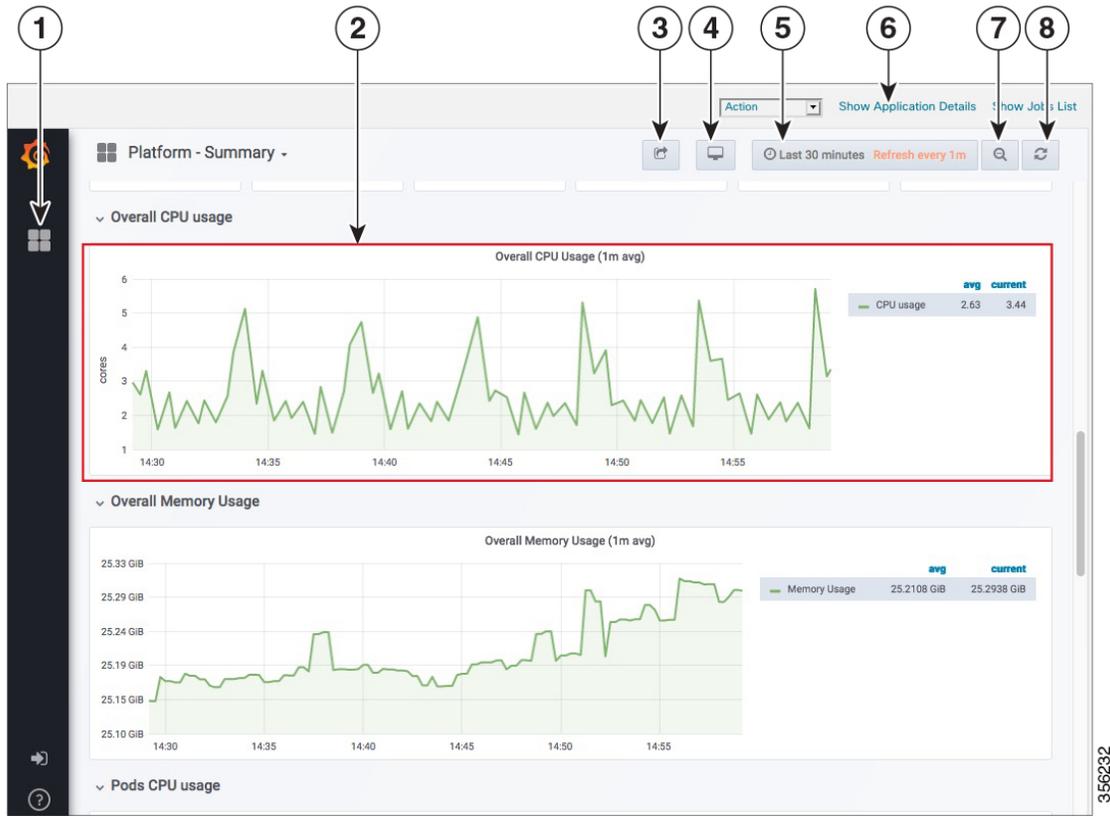
Recent

General

- Change Automation nca
- Collection - Manager collection
- Collection - Pipeline CLI collection
- Collection - Pipeline Kafka collection
- Infra - Etcd infra
- Infra - Kafka infra
- Infra - Nats infra
- Inventory - Manager inventory
- Platform - Metrics platform
- Platform - Pods platform
- Platform - Statefulsets platform
- Platform - Summary kubernetes platform

Step 4

Click the  icon next to the dashboard you want to view. For example: Clicking on the **Platform - Summary** dashboard displays a view like the one shown in the following figure. For more information on how to use Grafana go to <https://grafana.com>.



Step 5 Scroll the dashboard as needed to display all of the metrics it provides, or select any of the functions described in the following table.

Item	Description
1	Dashboard Icon: Click the icon to re-display the dashboard list and select a different dashboard.
2	<p>Time Series Graph Zoom: You can zoom in on a specific time period within the graph of any time series data, as follows:</p> <ol style="list-style-type: none"> Click a time-period starting point in the graph line and hold down the mouse. Drag the cursor to the endpoint. Light gray shading will appear in the block you are selecting. When you reach the endpoint, release the mouse. <p>To reset a zoomed time series graph to the default, click the Zoom Out icon.</p>

Item	Description
3	<p>Share Dashboard icon: Click the icon to make the dashboard you are viewing shareable with other users. Clicking this icon displays a popup window with tabs and options to share the dashboard in your choice of these forms:</p> <ul style="list-style-type: none"> • URL Link: Click the Link tab and then click Copy to copy the dashboard's URL to your clipboard. You can also choose whether to retain the current time and template settings with the URL. • Local Snapshot File: Click the Snapshot tab and then click Local Snapshot. Grafana creates a local snapshot of the dashboard on the server. When the snapshot is ready, click Copy Link to copy the URL of the snapshot to your clipboard. • Export to JSON File: Click the Export tab and then click Save to file. You will be prompted to save or open the exported JSON file. You can also choose to turn data source names in the file into templates by selecting the Export for sharing externally checkbox before clicking Save to file. • View JSON File and Copy to Clipboard: Click the Export tab and then click View JSON (you can choose to templatzize data source names by selecting the Export for sharing externally checkbox before clicking View JSON). Grafana displays the exported JSON code in a popup window. Click Copy to Clipboard to copy the file to your clipboard.
4	<p>Cycle View Mode icon: Click this icon to toggle between the default Grafana TV view mode and the Kiosk mode. The Kiosk view hides most of the Grafana menu. Press Esc to exit the Kiosk view.</p>
5	<p>Time/Refresh Selector: Indicates the time period for the metrics displayed in the dashboard and how often the metrics are refreshed. Click the selector to choose a different time range and refresh rate.</p> <p>You can specify a custom pair of time-range start and end points, or choose from one of several predefined ranges, such as Today so far or Last three hours.</p> <p>You can choose predefined refresh rates from Off to 2 Days.</p> <p>When you have finished making changes, click Apply.</p> <p>When making selections, remember that Cisco Crosswork Change Automation and Health Insights keeps only 24 hours of data. If you select time ranges or refresh rates beyond that limit, the dashboard may be blank.</p>
6	<p>Show Application Details: Click this link to re-display the Crosswork Manager window's Applications Detail view.</p>
7	<p>Zoom Out icon: Click this icon to reset a zoomed time series graph back to the unzoomed state.</p>
8	<p>Refresh icon: Immediately refresh the data shown.</p>

Collect and Share Cisco Crosswork Network Automation Logs and Metrics

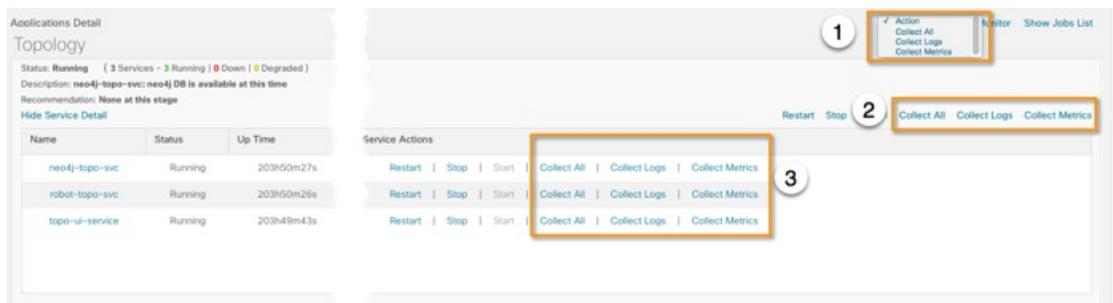
You can collect logs and metrics on multiple levels of Cisco Crosswork Change Automation and Health Insights. You can collect logs and metrics for the entire system, for any of its installed application, or for any service supporting an application. You can also choose to collect only logs, only the additional metrics, or both.

Collected logs and metrics are stored in gzipped tar archive files. You can publish these archives to an HTTP or HTTPS server of your choice.

Step 1 From the main menu, choose **Admin > Crosswork Manager**. The **Crosswork Manager** window displays, with the **Application Detail** section listing all the applications.

Step 2 Click the option for the collection level and target information you want, as follows:

- To collect for the entire system: From the **Action** drop down on the right, opposite the **Applications Detail** section title, choose **Collect All**, **Collect Logs**, or **Collect Metrics**. See item 1 in the following figure.
- To collect for an application: Scroll to the **Application Detail** tile for the application you want. Then click the **Collect All**, **Collect Logs**, or **Collect Metrics** link on the right, opposite the application's name. See item 2 in the following figure.
- To collect for a service: Scroll to the **Application Detail** tile for the application whose service you want to collect. Click the **Show Service Detail** link for that application. Then click the **Collect All**, **Collect Logs**, or **Collect Metrics** link on the right, opposite the service's name. See item 3 in the following figure.



Step 3 When you click on the collection option you want, the **Crosswork Manager** window displays a popup message indicating that a job was successfully created and giving the job ID. Click on the **Show Jobs List** link at the right to view the job's progress in the **Crosswork Manager** window's **Jobs List** view, which replaces the **Applications Detail** view.

Step 4 Wait for the job to complete. When the **Jobs List** view's **Status** column for your job has changed to **JobCompleted**, the **Action** column for the job will show an enabled **Publish** link for the completed job, and the **Description** column will show the file name of the gzipped tar archive file containing the collected information.



Step 5 (Optional) Click on the **Publish** link to publish the collected information to an HTTP or HTTPS server, as follows:

- a) A popup window will prompt you for the destination server host name, the storage path on the server, the port number, and the login user name and password for the server (if required). Enter the server information and click **Publish**.

- b) The **Job List** view's **Publish Status** column for the job shows an enabled **Details** link. Click the **Details** link to view a popup window showing the status of the publish job.

Step 6 When you are finished, click the **Show Application Details** link to re-display the **Applications Detail** view.

Control Cisco Crosswork Network Automation Applications and Services

Users with administrator privileges can control the runtime status of any Cisco Crosswork Change Automation and Health Insights application or service. This can include:

- Stopping a running application or service
- Starting a stopped application or service
- Restarting a running or stopped application or service

Please note that stopping, starting and restarting Cisco Crosswork Change Automation and Health Insights applications and services can result in anomalous system behavior and possible data loss. Use these functions only with the supervision of Cisco TAC staff.

Step 1 From the main menu, choose **Admin > Crosswork Manager**. The **Crosswork Manager** window displays, with the **Application Detail** view listing all the applications.

Step 2 Display the application or service whose runtime status you want to control:

- To control an application: Scroll to the **Application Detail** tile for the application you want.
- To control a service: Scroll to the **Application Detail** tile for the application whose service you want to control, then click the **Show Service Detail** link for that application to show its services.

Step 3 Click on the **Start**, **Stop**, or **Restart** link shown next to the service (item 1 in the following figure) or the application whose runtime status you want to control.

The screenshot shows the 'Topology' view in the Crosswork Manager. It displays a table of services with columns for Name, Status, and Up Time. The services listed are neo4j-topo-svc, robot-topo-svc, and topo-ui-service, all with a status of 'Running'. To the right of the table, there are two callouts: '1' points to the 'Service Actions' for the first service, which includes 'Restart', 'Stop', and 'Start' buttons; '2' points to the 'Restart', 'Stop', and 'Start' buttons for the application itself.

Name	Status	Up Time
neo4j-topo-svc	Running	204h39m46s
robot-topo-svc	Running	204h39m45s
topo-ui-service	Running	204h39m2s

Step 4 Click the **Show Jobs List** link at upper right to view the runtime control job's progress in the **Crosswork Manager** window's **Jobs List** view.

Step 5 When you are finished, click the **Show Application Details** link to re-display the **Applications Detail** view.

Manage Backup and Restore

The Backup Restore functionality is critical to prevent data loss in your Cisco Crosswork Change Automation and Health Insights VM.

Follow the steps below to create a backup for the Cisco Crosswork Change Automation and Health Insights VM and to restore a backup.



Important

- Cisco recommends that you perform the backup or restore operation only during a scheduled maintenance window when admin users should not access the UI. Both operations are time-consuming and stops all other applications running in the system.
- The same Cisco Crosswork Change Automation and Health Insights software image that was used to backup must also be used when doing a restore operation.
- Stay on the **Backup Restore** window until the backup/restore process completes. Otherwise, you may see incorrect content or UI errors since various services are rebooting frequently.
- Only one backup or restore operation can be running at any given time.

Before you begin, ensure that:

- You have the Host Name, Port number, and Remote path to a Secure FTP server to use as the destination for backup files.
- You have the user credentials to an account with write permissions to create files and directories in the destination server remote path.

Step 1 From the main menu, choose **Admin > Backup Restore**. The **Backup Restore** window is displayed.

Step 2 During your first login, you should configure a destination server to store the backup file. This is a one-time activity and has to be completed before taking the backup. Click **Destination** to display the **Edit Destination** dialog box. Make relevant entries in the fields provided.

Click **Save** to confirm the server details.

Step 3 To create a backup:

- a) Click **Backup**. The **Backup** dialog box is displayed with destination server details pre-filled.
- b) Provide a relevant name in the **Job Name** field.
- c) (Optional) Click **Verify Backup** to check if Cisco Crosswork Change Automation and Health Insights has enough resources to complete the operation. If the check is successful, a warning message is displayed about the time-consuming nature of the operation. Click **OK**.
- d) Click **Start Backup** to start the backup operation. The corresponding backup job set is created and added to the job list. See Step 5 to view Backup progress.

Step 4 To restore a backup file:

- a) Select the required backup file from the **Backup Restore Job Sets** table, and the job details are displayed on the right side.
- b) Click the **Restore** button to display the **Restore** dialog box with destination server details pre-filled.

- c) Provide a relevant name in the **Job Name** field.
- d) (Optional) Click **Verify Restore** to check if Cisco Crosswork Change Automation and Health Insights has enough resources to complete the operation. If the check is successful, a warning message is displayed about the time-consuming nature of the operation. Click **OK**.
- e) Click **Start Restore** to start the restore operation. The corresponding restore job set is created and added to the job list.

Step 5 To view the progress of a backup or restore job:

- a) Enter the job details (such as Status, Job Name, or Job Type) in the search fields in **Backup Restore Job Sets** table on the left side. Click  to select which columns to display in the Job set list. The list is automatically filtered based on your search string. Click the required job set from the search results.
- b) Alternately, you can manually scroll the list and click the required job set.
- c) The **Job Details** table on the right side displays information about the selected job set such as Status, Job Type and Start time. In case of a failed job, hover the mouse pointer over the  icon near **Status** to view the error details.

Disaster Restore

Disaster Restore is a restore operation, appropriately named to be used in case of a disaster, such as VM crash. The **Disaster Restore** option is displayed if no backup jobs have been initiated in the system. After the completion of the first backup job, this button is disabled.



Note While using disaster recovery operation, please note the following:

- The new VM that you use needs to have the same IP address as the one where backup was performed. This is important as internal certificates are tied to the IP address.
- The same software image that was used to backup must also be used when doing a restore operation.
- The VM which is brought up should have same services running when the backup was performed. If the previous VM was patched/upgraded then the new VM also needs to be patched/upgraded before disaster restore is performed.
- The disaster restore operation trusts the backup file which is provided. Caution is advised while selecting the appropriate backup file.

To perform a disaster restore:

- Step 1** From the main menu, choose **Admin > Backup Restore**. The **Backup Restore** window is displayed.
- Step 2** Click **Destination** to display the **Edit Destination** dialog box. Enter the details of the remote destination server where the backup file is uploaded.
- Step 3** Click **Disaster Restore** to display the **Disaster Restore** dialog box with destination server detailed pre-filled.
- Step 4** Make relevant entry in the **Backup File Name** field.
- Step 5** Click **Start Restore** to start the disaster restore operation.

Note If disaster restore operation fails, you are recommended to bring up a new VM to retry the disaster restore operation.

Manage Users

From the main menu, select **Admin > Users** to display the **Users** window. Using this window, you can add a new user, edit the settings for an existing user, delete a user from the network, and create user roles.



Note Before you can create a new user that does *not* have admin-level access to Cisco Crosswork Change Automation and Health Insights functionality, you must first create a new role that limits the features they can access. See [Create User Roles](#) for more information.

Only a local admin user can add, update, and delete other local user accounts. A TACACS+ user, regardless of role assigned, will not be able to manage local users.

Administrative Users Created During Installation

During installation, Cisco Crosswork Change Automation and Health Insights creates two special administrative IDs:

1. The **virtual machine administrator**, with the username **cw-admin**, and the default password **admin**. Data center administrators use this ID to log in to and troubleshoot the VM hosting the Cisco Crosswork Change Automation and Health Insights server.
2. The **Crosswork administrator**, with the username **admin** and the default password **admin**. Product administrators use this ID to log in to and configure the Cisco Crosswork Change Automation and Health Insights user interface, and to perform special operations, such as creating new user IDs.

The default password for both administrative user IDs must be changed the first time they are used. You can also change the Crosswork administrator password using the following methods:

- Log in as the admin user and edit the admin user password, as explained in [Edit Users, on page 14](#).
- Enter the following command: `admin(config)# username admin <password>`

Add Users

Follow the steps below to create a new user ID.

The user ID's user name must be unique. You cannot create a new user ID with the same user name as an existing user ID.

The special administrative user names **admin** (for administering Cisco Crosswork Change Automation and Health Insights) and **cw-admin** (for administering the virtual machine hosting the product) are created during installation and are reserved for those purposes (see [Administrative Users Created During Installation, on page 13](#)).

Step 1 From the main menu, choose **Admin > Users**.

The **Users** window opens.

If it is not already displayed, click the **Users** tab.

Step 2 Click  to open the **Add New User** dialog box.

Step 3 Enter the following information for the user you are adding:

- **User Name:** Enter a unique name for the user ID. User names cannot contain spaces or special characters.
- **First Name** and **Last Name:** Enter the first and last name of the person assigned to this user ID.
- From the **Role** drop-down at the bottom of the dialog box, choose the role that you want to assign to the user. See [Create User Roles](#) for more information.
- **Password** and **Confirm Password:** Enter the default password for this user ID. The user will be required to change the default password the first time they attempt to log on using it.

Note The user password must be string of minimum 8 characters without spaces and should include letters, numbers, upper-case and lower-case characters, and one of the allowed special characters ("@!\$%*?&").

Step 4 Click **Save**.

Edit Users

Users with administrator privileges can edit any user ID's User Name, First Name, Last Name, and Role.

Administrators cannot change a user's password by editing the user ID. Users can change their passwords by logging in, clicking , and selecting **Change Password**.

Step 1 From the main menu, choose **Admin > Users**.

The **Users** window opens.

If it is not already displayed, click the **Users** tab.

Step 2 Click on the check box of the user whose settings you want to update, then click  to open the **Edit User** dialog box.

Step 3 Make the necessary updates to the user ID.

Note First Name, Last Name and Role can be edited for user accounts with administrative privileges.

Step 4 Click **Update** to save your changes.

Delete Users

Follow the steps below to delete an existing user ID.

The administrative user IDs **admin** and **cw-admin** created during installation cannot be deleted (see [Administrative Users Created During Installation, on page 13](#)).

-
- Step 1** From the main menu, choose **Admin > Users**.
The **Users** window opens.
If it is not already displayed, click the **Users** tab.
- Step 2** Click on the check box of the user you want to delete, then click . The **Delete Username User** dialog displays.
- Step 3** Click **Delete** to confirm deletion.
-

User Roles, Functional Categories and Permissions

The **Roles** window lets users with the appropriate privileges define custom user roles. As with the default *admin* role, a custom user role consists of:

- A unique name, such as “Operator” or “admin”.
- One or more selected, named functional categories, which control whether or not a user with that role has access to the APIs needed to perform specific Crosswork functions controlled by that API. For example: The “Health Insights” category provides access to all of the “Health Insights API” functions, such as selecting and running KPI Profiles, importing custom user-defined KPIs, deleting custom KPIs, and so on.
- One or more selected permissions, which control the scope of what a user with that role can do in the functional category.

For a user role to have access to a functional category, that category and its underlying API must show as selected on the **Roles** page for that role. If the user role shows a functional category as unselected, then users with this role assigned will have no access to that functional area at all.

Some functional categories group multiple APIs under one category name. For example: The “AAA” category controls access to the Password Change, Remote Authentication Servers Integration, and Users and Role Management APIs. With this type of category, you can deny access to some of the APIs by leaving them unselected, while providing access to other APIs under the category by selecting them. For example: If you want to create an “Operator” role who is able to change his own password, but not see or change the settings for your installation’s integration with remote AAA servers, or create new users and roles, you would select the “AAA” category name, but uncheck the “Remote Authentication Server Integration API” and “Users and Role Management API” checkboxes.

For each role with a selected category, the **Roles** page also lets you define permissions to each underlying functional API:

- **Read** permission lets the user see and interact with the objects controlled by that API, but not change or delete them.
- **Write** permission lets the user see and change the objects controlled by that API, but not delete them.
- **Delete** permission gives the user role delete privileges over the objects controlled by that API. It is useful to remember that delete permission does not override basic limitations set by the Crosswork platform and its applications.

Although you can mix permissions as you wish:

- If you select an API for user access, you must provide at least “Read” permission to that API.
- When you select an API for user access, Cisco Crosswork Change Automation and Health Insights will assume that you want the user to have all permissions on that API, and will select all three permissions for you, automatically.
- If you uncheck all of the permissions, including “Read”, Cisco Crosswork Change Automation and Health Insights will assume that you want to deny access to the API, and unselect it for you.

Best Practices:

Cisco recommends that you follow these best practices when creating custom user roles:

- Restrict **Delete** permissions in roles for *admin* users with explicit administrative responsibility for maintenance and management of the Crosswork deployment as a whole.
- Roles for developers working with all the Crosswork APIs will need the same permissions as *admin* users.
- Apply at least **Read** and **Write** permissions in roles for users who are actively engaged in managing the network using Cisco Crosswork Change Automation and Health Insights.
- Give read-only access to roles for users who only need to see Cisco Crosswork Change Automation and Health Insights data to help their work as system architects or planners.

The following table describes some sample custom user roles you should consider creating:

Table 2: Sample custom user roles

Role	Description	Categories/API	Privileges
Operator	Active network manager, triggers Playbooks in response to KPI alerts	All	Read, Write
Monitor	Monitors alerts only	Health Insights, Inventory, Topology	Read only
KPI Developer	Develops custom KPIs for others to use	Core Infra, Health Insights, Inventory/All	All
API Integrator	All	All	All



Note Admin role needs to include permissions for Read, Write, and Delete, while read-write roles need to include both Read and Write permissions.

Create User Roles

Local users with administrator privileges can create new users as needed (see [Add Users, on page 13](#)).

Users created in this way can perform only the functions or tasks that are associated with the user role they are assigned.

The local **admin** role enables access to all functionality. It is created during installation and cannot be changed or deleted. However, its privileges can be assigned to new local users. Only local users can create or update user roles; TACACS users cannot.

Follow the steps below to create a new user role.

Step 1 From the main menu, choose **Admin > Users**.

The **Users** window opens.

If it is not already displayed, click the **Roles** tab. The **Roles** window has a **Roles** table on the left side and a corresponding **admin** table on the right side which shows the grouping of user permissions for the selected role.

Step 2 On the **Roles** table, click  to display a new role entry in the table.

Step 3 Enter a unique name for the new role.

Step 4 Define the user role's privilege settings:

- a) Check the check box for every API that users with this role can access. The APIs are grouped logically based their corresponding application.
- b) For each API, define whether the user role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box. You can also select an entire API group (such as AAA), and all the APIs under the group will be selected with **Read**, **Write** and **Delete** permissions pre-selected.

Step 5 Click **Save** to create the new role.

To assign the new user role to one or more user IDs, edit the **Role** setting for the user IDs (see [Edit Users, on page 14](#)).

Edit User Roles

Users with administrator privileges can quickly change the privileges of any user role other than the default **admin** role.

Step 1 From the main menu, choose **Admin > Users**.

The **Users** window opens.

If it is not already displayed, click the **Roles** tab.

Step 2 In the **Roles** table, click on an existing role to select it. The **Admin** table on the right side displays the permission settings for the selected role.

Step 3 Define the role's settings:

- a) Check the check box for every API that the role can access.
- b) For each API, define whether the role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box. You can also select an entire API group (such as AAA), and all the APIs under the group will be selected with **Read**, **Write** and **Delete** permissions pre-selected.

Step 4 When you are finished, click **Save** to save your changes.

Clone User Roles

Cloning an existing user role is the same as creating a new user role (see [Create User Roles, on page 16](#)), except that you need not set privileges for it. If you like, you can let the cloned user role inherit all the privileges of the original user role.

Cloning user roles is a handy way to create and assign many new user roles quickly. Following the steps below, you can clone an existing role multiple times. Defining the cloned user role's privileges is an optional step; you are only required to give the cloned role a new name. If you like, you can assign it a name that indicates the role you want a group of users to perform. You can then edit the user IDs of that group of users to assign them their new role (see [Edit Users, on page 14](#)). Later, you can edit the roles themselves to give users the privileges you want (see [Edit User Roles](#)).

Step 1 From the main menu, choose **Admin > Users**.

The **Users** window opens.

If it is not already displayed, click the **Roles** tab.

Step 2 Click on an existing role to select it.

Step 3 Click  to create a new duplicate entry in the **Roles** table with all the permissions of the original role.

Step 4 Enter a unique name for the cloned role.

Step 5 (Optional) Define the role's settings:

- a) Check the check box for every API that the cloned role can access.
- b) For each API, define whether the clone role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box. You can also select an entire API group (such as AAA), and all the APIs under the group will be selected with **Read**, **Write** and **Delete** permissions pre-selected.

Step 6 Click **Save** to create the newly cloned role.

Delete User Roles

Users with administrator privileges can delete any user role that is not the default **admin** user role or that is not currently assigned to a user ID. If you want to delete a role that is currently assigned to one or more user IDs, you must first edit those user IDs to assign them to a different user role.

Step 1 From the main menu, choose **Admin > Users**.

The **Users** window opens.

If it is not already displayed, click the **Roles** tab.

Step 2 Click on the role you want to delete, to select it.

- Step 3** Click  to display the **Delete Role** dialog box.
- Step 4** Click **Delete** to confirm that you want to delete the user role.
-

Manage TACACS+ Servers

In addition to local database authentication, Cisco Crosswork Change Automation and Health Insights can use TACACS+ servers to authenticate users. TACACS+ is a security protocol that provides centralized validation of users attempting to access your network. It allows for a single access control server (the TACACS+ daemon) to provide authentication, authorization, and accounting (AAA) services independently of one another.

Local database authorization takes precedence over authorization by TACACS+ server. When adding the TACACS+ server, you can specify the priority value for each instance.



Note Please note that any operation you do following the instructions in this section will affect all new logins to the Cisco Crosswork Change Automation and Health Insights user interface. To minimize session interruption, Cisco recommends that you perform all your TACACS+ changes and submit them in a single session.

Add a TACACS+ Server

Before adding a TACACS+ server, you will need to know the server's IP address, port number, shared secret, and service name.

- Step 1** From the main menu, choose **Admin > AAA**.
- The **AAA** window opens. If it is not already displayed, click the **TACACS+ Servers** tab.
- Step 2** Click  to open the **Add Server** dialog box.
- Step 3** Enter the TACACS+ server's settings, then click **Add**.
- Note** Only the server's IP address, port number, shared secret, and service name are required. You can leave the other values blank, as needed.
- Step 4** Click **Save Server Changes** to submit the changes. You will be prompted with a warning message about restarting the server to update the changes. Click **Save Changes** to confirm.
-

Edit a TACACS+ Server

- Step 1** From the main menu, choose **Admin > AAA**.
- The **AAA** window opens. If it is not already displayed, click the **TACACS+ Servers** tab.

Step 2 Click the check box next to the TACACS+ server whose settings you want to update, then click . The **Edit Server** dialog box opens.

Step 3 Make the necessary changes, then click **Update**.

Note You cannot change the value for the **Shared Secret** parameter.

Step 4 Click **Save Server Changes** to submit the changes. You will be prompted with a warning message about restarting the server to update the changes. Click **Save Changes** to confirm.

Delete a TACACS+ Server

Step 1 From the main menu, choose **Admin > AAA**.

The **AAA** window opens. If it is not already displayed, click the **TACACS+ Servers** tab.

Step 2 Click the check box next to the TACACS+ server you want to delete.

Note You can delete only one TACACS+ server at a time.

Step 3 Click . The **Delete server-IP-address** dialog box opens.

Step 4 Click **Delete** to confirm.

Manage LDAP Servers

Cisco Crosswork Change Automation and Health Insights supports the use of LDAP servers to authenticate users. Lightweight Directory Access Protocol (LDAP) is a server protocol used to access and manage directory information. It manages directories over IP networks and runs directly over TCP/IP using simple string formats for data transfer.

Like TACACS+ server, you can specify the priority value to assign precedence in the authentication request.



Note Please note that any operation you do following the instructions in this section will affect all new logins to the Cisco Crosswork Change Automation and Health Insights user interface. To minimize session interruption, Cisco recommends that you perform all your LDAP changes and submit them in a single session.

Add a LDAP Server

Before adding a LDAP server, you will need to know the Server name and URL, Bind DN and credential, Base DN, user filter, DN format, Principal Attribute ID, Policy ID, and connection timeout value.

-
- Step 1** From the main menu, choose **Admin > AAA**.
The **AAA** window opens. Click on the **LDAP Servers** tab.
- Step 2** Click  to open the **Add Server** dialog box.
- Step 3** Enter the LDAP server settings, then click **Add**.
- Note** Priority field value is unique across TACACS+ and LDAP servers. Providing a duplicate value will result in an error.
- Step 4** Click **Save Server Changes** to submit the changes. You will be prompted with a warning message about restarting the server to update the changes. Click **Save Changes** to confirm.
-

Edit a LDAP Server

-
- Step 1** From the main menu, choose **Admin > AAA**.
The **AAA** window opens. Click on the **LDAP Servers** tab.
- Step 2** Click the check box next to the LDAP server whose settings you want to update, then click .
The **Edit Server** dialog box opens.
- Step 3** Make the necessary changes, then click **Update**.
- Step 4** Click **Save Server Changes** to submit the changes. You will be prompted with a warning message about restarting the server to update the changes. Click **Save Changes** to confirm.
-

Delete a LDAP Server

-
- Step 1** From the main menu, choose **Admin > AAA**.
The **AAA** window opens. Click on the **LDAP Servers** tab.
- Step 2** Click the check box next to the LDAP server you want to delete.
Note You can delete only one LDAP server at a time.
- Step 3** Click . The **Delete** *server-IP-address* dialog box opens.
- Step 4** Click **Delete** to confirm.
-

Define Network Visualization Display Settings

Cisco Crosswork Change Automation and Health Insights administrator privileges are required to configure the display settings that are used by the Network Visualization application.

For a description of how to configure these settings, see the following topics:

- [Define Color Thresholds for Link Bandwidth Utilization](#)
- [Configure Geographical Map Settings](#)

Manage Certificates

The Cisco Crosswork Change Automation and Health Insights VM-hosted server and its browser-based user interface communicate with each other using SSL certificates exchanged over HTTPS. For details about these protocols, see [SSL Certificates, on page 30](#) and [HTTPS, on page 30](#)

When installed, Cisco Crosswork Change Automation and Health Insights secures these interactions using a self-signed TLS certificate. This certificate has a two-year lifespan, after which it expires. If you want to continue using the expired self-signed certificate to secure server/client communications, you will need to regenerate it by following the steps in [Extend Self-Signed Certificate Expiration, on page 23](#)

If you prefer to secure these communications with a user-provided certificate, either purchased from a Certificate Authority (CA) or self-signed by your organization, you can validate and upload it by following the steps in [Substitute a User-Provided Certificate, on page 24](#).

The user-provided certificate must meet the following requirements:

- Cisco Crosswork Change Automation and Health Insights supports IP Subject Alternative Name (SAN) server certificates only. The IP address is the primary means to reach the user interface.
- The server will present your user-provided certificates to the browser, so the certificates you supply must be valid both for Cisco and for Cisco Crosswork Change Automation and Health Insights.
- It must also include the required fields and field values shown in the following table.

Table 3: Required User-Provided Certificate Fields and Values

Field	Description	Value
<NUMBER OF DAYS>	Number of days the certificate will be valid.	Must be greater than 30 days and less than 730 days (or two years)
<COUNTRY>	Country (C=)	US
<STATE>	State (ST=)	CALIFORNIA
<LOCATION>	Location (L=)	SAN JOSE
<ORGANIZATION>	Organization (O=)	CISCO SYSTEMS INC
<ORGANIZATIONAL UNIT NAME>	Organizational Unit (OU=)	CROSSWORK

Field	Description	Value
<COMMON NAME>	Common Name (CN=)	The IP address of the Cisco Crosswork Change Automation and Health Insights server VM.

- The certificate must also have the SAN extension set, with both DNS and IP address keys. The following provides an example of how to generate a self-signed certificate using OpenSSL:

```

/usr/bin/openssl req \
    -x509 \
    -nodes \
    -days 730 \
    -newkey rsa:4096 \
    -keyout "filename.key" \
    -out "filename.crt" \
    -subj "/C=US/ST=CALIFORNIA/L=SAN JOSE/O=CISCO SYSTEMS
INC/OU=CROSSWORK/CN=1.1.1.1" \
    -extensions SAN \
    -config <(cat /etc/ssl/openssl.cnf \
    <(printf "\n[SAN]\nsubjectAltName=DNS:0.0.0.0,IP:1.1.1.1")

```

Extend Self-Signed Certificate Expiration

Follow these steps to regenerate the self-signed certificate and extend its lifetime by two years.

Step 1 From the main menu, select **Admin > Certificate Management**. The **Certificate Management** window appears.

Step 2 Select the **Regenerate Crosswork Certificate** radio button.

The screenshot shows the 'Admin / Certificate Management' page. At the top, there is a breadcrumb trail. Below it, there are two radio buttons: 'Regenerate Crosswork Certificate' (which is selected) and 'Validate/Update'. Underneath, the text 'Regenerate Crosswork Certificate' is displayed. A blue information icon is followed by the text: 'If you want crosswork to regenerate HTTPS self-signed certificate, please click Regenerate the certificate to activate.' At the bottom, there is a blue button labeled 'Regenerate Certificate'.

Step 3 When you are ready, click **Regenerate Certificate**.

When Cisco Crosswork Change Automation and Health Insights has finished regenerating the certificate, it displays an alert message indicating that the regeneration operation is successful and you will be logged out. You must log in again to continue using Cisco Crosswork Change Automation and Health Insights.

Substitute a User-Provided Certificate

Follow the steps below to validate and upload a user-provided certificate. The certificate must meet the requirements explained in [Manage Certificates, on page 22](#).

Before you begin

You must know the names of the user-provided certificate and key files and their locations in your local storage.

- Step 1** From the main menu, select **Admin > Certificate Management**. The **Certificate Management** window appears.
- Step 2** Select the **Validate/Update** radio button.
- Step 3** Use the **Browse** button next to each field to browse to and select the key and certificate files you want to validate and use.

The screenshot shows the 'Admin / Certificate Management' interface. At the top, there are two radio buttons: 'Regenerate Crosswork Certificate' (unselected) and 'Validate/Update' (selected). Below this is the section 'Validate/Update Certificate'. A blue information icon is followed by the text: 'You can upload new Certificate here. once you upload the files,it will be validated and updated.' There are two input fields: 'Key File*' with the value 'foo.key' and a 'Browse' button; and 'Cert File*' with the value 'foo.crt' and a 'Browse' button. At the bottom of the section, there are two buttons: 'Validate' (solid blue) and 'Update' (outlined blue).

- Step 4** Click **Validate** to validate the certificate and key files.
- Step 5** Click **Update** to replace the existing certificate with the user-provided certificate you have validated.

Smart Licensing Registration

This section provides an overview of the Cisco Smart Licensing feature integrated with the Cisco Crosswork Change Automation and Health Insights and describes the instructions to complete the product registration.

Overview

Smart Licensing is a software based end-to-end license platform that comprises several tools and processes that authorizes customers to use Cisco products. Smart Licensing provides a software inventory management system that provides Customers, Cisco, and selected Partners with information about Software Ownership and Software Utilization.

A **Cisco Smart Account** provides the repository for Smart enabled products and enables you to activate Cisco licenses, monitor license usage and track Cisco purchases. The **Cisco Smart Software Manager (CSSM)** enables you to manage all your Cisco Smart software licenses from one centralized website. With Cisco Smart Software Manager, you may create and manage multiple virtual accounts within your Smart Account to manage licenses. For more information, see <https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html>

From the main menu, select **Admin > Smart Licensing Registration** to display the **Smart Software Licensing** window. Using this window, you can register your Cisco Crosswork Change Automation and Health Insights application, edit the transport settings, renew the license, and de-register your application.

Prerequisites for Smart Licensing Registration

You should have:

- A Cisco Smart Account.
- Purchased licenses for the Cisco Crosswork Change Automation and Health Insights application.

Configure Transport Settings

You can configure the transport settings to decide how Cisco Crosswork Change Automation and Health Insights communicates with the Cisco servers.

- **Direct:** The application directly connects with Cisco Smart Software Manager (CSSM).
- **Transport Gateway:** The application communicates via a Transport Gateway or CSSM on-prem, which replicates the cloud-based user experience but keeps all communication on premises.



Note For more information on the CSSM on-prem option, see the [Smart Software Manager guide](#).

- **HTTP/HTTPS Gateway:** The application connects via an intermediate proxy server. This is applicable only for Direct mode.



Note Transport Settings cannot be changed while the Cisco Crosswork Change Automation and Health Insights is in Registered mode. You have to de-register to change them.

Step 1

In the **Smart Software Licensing** window, the Transport Settings display the current transport mode selected. To modify, click **View/Edit**.

The **Transport Settings** dialog box is displayed.

Transport Settings
×

Configure how the product will communicate with Cisco. Note that this setting is shared with Smart Call Home, so any changes made here will apply to other features using this service.

Direct - product communicates directly with Cisco's licensing servers
URL :

Transport Gateway - proxy data via Transport Gateway or On Prem Smart Software Manager
URL :

HTTP/HTTPS Gateway - send data via an intermediate HTTP or HTTPS proxy
IP Address :
Port :

Step 2 Select the relevant transport mode and make relevant entries in the fields provided.

Step 3 Click **Save**.

Register Cisco Crosswork Change Automation and Health Insights

To enable licensed features, Cisco Crosswork Change Automation and Health Insights must be registered to CSSM using a registration ID token. Once registered, an Identity Certificate is saved securely in the Smart Account and used for all ongoing communications. The certificate is valid for one year and will be renewed automatically after six months to ensure continuous operation.



Note For information on generating the registration token, please refer to the support resources provided in the [Smart Software Manager](#) webpage.

Step 1 From the main menu, select **Admin > Smart Licensing Registration** to display the **Smart Software Licensing** window. The registration status

The registration status and license authorization status will be **Unregistered** and **Evaluation mode** respectively.

Figure 2: Smart Software Licensing Unregistered

Crosswork Network Automation

The evaluation period will expire in 85 days. [Purchase License Now](#)

Admin / Smart Licensing Registration

Smart Software Licensing

To view and manage Smart Licenses for your Cisco Smart Account, go to [Smart Software Manager](#)

You are currently running in Evaluation Mode. To register your Crosswork application with Cisco Smart Licensing:

- Ensure this product has access to the Internet or On Prem Smart Software Manager installed on your network. This might require you to edit the Smart Call Home Transport Settings.
- Log in to your Smart Account in [Smart Software Manager](#) on your On Prem Smart Software Manager.
- Navigate to the Virtual Account containing the licenses to be used by this Product Instance.
- Generate a Product Instance Registration Token (this identifies your Smart Account) and copy or save it.

[Register](#) [Learn more about Smart Software Licensing](#)

Smart Software Licensing Status

Registration Status ▲ Unregistered

License Authorization Status ▲ Evaluation Mode (85 days remaining)

Product Instance Name UDI_...

Export-Controlled Functionality Not Allowed

Transport Settings [Direct View / Edit](#)

Smart Licensing Usage

License (Version)	Description	Count	Status
NTWAUTO_RTM(1.0)		4	▲ Evaluation
HL_SW(1.0)		12	▲ Evaluation
CA_SW(1.0)		1	▲ Evaluation

Step 2 In the **Smart Software Licensing** window, click **Register**.

The **Smart Software Licensing Product Registration** dialog box is displayed.

Smart Software Licensing Product Registration

To register the product for Smart Software Licensing:

- Ensure you have connectivity to the URL specified in your Smart Call Home settings. By default, this will require internet access. See the online help registering to a On Prem Smart Software Manager.
- Paste the Product Instance Registration Token you generated from [Smart Software Manager](#) or your On Prem Smart Software Manager.

Product Instance Registration Token

Re-register this product instance if it is already registered

[Register](#) [Cancel](#)

Step 3 In the **Product Instance Registration Token** field, enter the registration token generated from your Smart Account. Make sure the token ID is accurate and within validity period. For more information, see https://www.cisco.com/c/en_in/products/software/smart-accounts/software-licensing.html.

Step 4 (Optional) If you are re-registering the application, check the **Re-register this product registration if it is already registered** checkbox.

Step 5 Click **Register**. It may take a few minutes to process the registration. If successful, the 'Product Registration completed successfully' message is displayed.

The registration status and license authorization status will be updated as **Registered** and **Authorized** respectively.

Smart Software Licensing Registration

Smart Software Licensing

To view and manage Smart Licenses for your Cisco Smart Account, go to Smart Software Manager

Smart Software Licensing Status

Registration Status ✔ Registered (Dec 17, 2019)

License Authorization Status ✔ Authorized (Dec 18, 2019)

Smart Account InternalTest1

Virtual Account Crosswork

Product Instance Name

Export-Controlled Functionality Allowed

Transport Settings Direct View / Edit

Smart Licensing Usage

License (Version)	Description	Count	Status
Network Auto RTM(1.0)	Network Automation Right To Manage	20	✔ In_Compliance
Health Insights(1.0)	Telemetry driven KPI monitoring	45	✔ In_Compliance
Change Automation(1.0)	Playbook driven closed loop remediation	1	✔ In_Compliance

Note If you encounter a communication timeout error during registration, click **OK** in the error dialog box and the application will reattempt the registration.

Manual Actions

The renewal of registration and authorization are automatically enabled for Cisco Crosswork Change Automation and Health Insights, by default. However, in the event of a communication failure between the application and the Cisco server, these actions can be manually initiated. You can use the **Actions** drop-down button to manually renew, re-register and de-register the application.

Step 1 In the **Smart Software Licensing** window, click **Actions** drop-down button and select the relevant option for the following quick actions.

Actions ^

- Renew Authorization
- Renew Registration
- Reregister
- Deregister

- Actions > Renew Authorization:** To renew the authorization manually if the automatic renewal service fails at the end of 30 days.
- Actions > Renew Registration:** To renew the registration manually if the automatic renewal service fails at the end of 6 months.
- Actions > Re-register:** Re-register the application, for example, on account of the expiry of registration tokens.
- Actions > De-register:** De-register the application, for example, when the transport settings need to be changed.

Note Once de-registered, the Cisco Crosswork Change Automation and Health Insights application will be moved to **Evaluation** mode (if evaluation period is available), or **Evaluation Expired** mode. For more information, see [License Authorization Statuses, on page 29](#)

Step 2 The selected action is executed successfully.

License Authorization Statuses

Based on the registration status of your Cisco Crosswork Change Automation and Health Insights application, you can see the following License Authorization Statuses.

Table 4: License Authorization Statuses

Registration Status	License Authorization Status	Description
Unregistered	Evaluation mode	A 90-day evaluation period during which the licensed features of the application can be freely used. This state is initiated when you use the application for the first time.
	Evaluation Expired	The application has not been successfully registered at the end of the evaluation period. During this state, the application features are disabled, and you must register to continue using the application.
	Registered Expired	The application is unable to contact the CSSM before the expiration of Identity Certificates and has returned to the unregistered state. The application resumes the remaining evaluation period, if available. At this stage, new registration ID token is required to reregister the application.
Registered	Authorized (In Compliance)	The application has been fully authorized to use the reserved licensed features. The authorization is automatically renewed every 30 days.
	Out of Compliance	The associated Virtual Account does not have enough licenses to reserve for the application's current feature use. You must renew the entitlement/usage limit registered with the token to continue using the application.
	Authorization Expired	The application is unable to communicate with the CSSM for 90 days or more, and the authorization has expired.

Security Hardening Overview

Security hardening entails making adjustments to ensure that the following components optimize their security mechanisms:

- Cisco Crosswork Change Automation and Health Insights infrastructure

- Cisco Crosswork Change Automation and Health Insights storage system (local or external)

Hardening Cisco Crosswork Change Automation and Health Insights security requires completion of the following tasks:

- Shutting down insecure and unused ports
- Configuring network firewalls
- Hardening the Cisco Crosswork Change Automation and Health Insights infrastructure, as needed

Although your primary source of information is your Cisco representative, who can provide server hardening guidance specific to your deployment, you can also follow the steps in this section to secure Cisco Crosswork Change Automation and Health Insights.

Authentication Throttling

Cisco Crosswork Change Automation and Health Insights throttles the login attempts after a failed login attempt to avoid password guessing and other related abuse scenarios. After a failed login attempt for a username, all authentication attempts for that username would be blocked for 3 seconds. The throttling is applicable to all supported authentication schemes such as TACACS, LDAP and the default local authentication.

Core Security Concepts

If you are an administrator and are looking to optimize the security of your Cisco Crosswork Change Automation and Health Insights product, you should have a good understanding of the following security concepts.

HTTPS

Hypertext Transfer Protocol Secure (HTTPS) uses Secure Sockets Layer (SSL) or its subsequent standardization, Transport Layer Security (TLS), to encrypt the data transmitted over a channel. Several vulnerabilities have been found in SSL, so Cisco Crosswork Change Automation and Health Insights now supports TLS only.



Note TLS is loosely referred to as SSL often, so we will also follow this convention.

SSL employs a mix of privacy, authentication, and data integrity to secure the transmission of data between a client and a server. To enable these security mechanisms, SSL relies upon certificates, private-public key exchange pairs, and Diffie-Hellman key agreement parameters.

SSL Certificates

SSL certificates and private-public key pairs are a form of digital identification for user authentication and the verification of a communication partner's identity. Certificate Authorities (CAs), such as VeriSign and Thawte, issue certificates to identify an entity (either a server or a client). A client or server certificate includes the name of the issuing authority and digital signature, the serial number, the name of the client or server that the certificate was issued for, the public key, and the certificate's expiration date. A CA uses one or more signing certificates to create SSL certificates. Each signing certificate has a matching private key that is used to create the CA signature. The CA makes signed certificates (with the public key embedded) readily available, enabling anyone to use them to verify that an SSL certificate was actually signed by a specific CA.

In general, setting up certificates in both High Availability (HA) and non-HA environments involves the following steps:

1. Generating an identity certificate for a server.
2. Installing the identity certificate on the server.
3. Installing the corresponding root certificate on your client or browser.

The specific tasks you need to complete will vary depending on your environment.

Note the following:

- The start-stop sequencing of servers needs to be done carefully in HA environments.
- Non-HA environments, where a virtual IP address is configured, require the completion of a more complicated certificate request process.

1-Way SSL Authentication

This authentication method is used when a client needs assurance that it is connecting to the right server (and not an intermediary server), making it suitable for public resources like online banking websites. Authentication begins when a client requests access to a resource on a server. The server on which the resource resides then sends its server certificate (also known as an SSL certificate) to the client in order to verify its identity. The client then verifies the server certificate against another trusted object: a server root certificate, which must be installed on the client or browser. After the server has been verified, an encrypted (and therefore secure) communication channel is established. At this point, the Cisco Crosswork Change Automation and Health Insights server prompts for the entry of a valid username and password in an HTML form. Entering user credentials after an SSL connection is established protects them from being intercepted by an unauthorized party. Finally, after the username and password have been accepted, access is granted to the resource residing on the server.



Note A client might need to store multiple server certificates to enable interaction with multiple servers.



To determine whether you need to install a root certificate on your client, look for a lock icon in your browser's URL field. If you see this icon, this generally indicates that the necessary root certificate has already been installed. This is usually the case for server certificates signed by one of the bigger Certifying Authorities (CAs), because root certificates from these CAs are included with popular browsers.

If your client does not recognize the CA that signed a server certificate, it will indicate that the connection is not secure. This is not necessarily a bad thing. It just indicates that the identity of the server you want to connect has not been verified. At this point, you can do one of two things: First, you can install the necessary root certificate on your client or browser. A lock icon in your browser's URL field will indicate the certificate was installed successfully. And second, you can install a self-signed certificate on your client. Unlike a root certificate, which is signed by a trusted CA, a self-signed certificate is signed by the person or entity that created it. While you can use a self-signed certificate to create an encrypted channel, understand that it carries an inherent amount of risk because the identity of the server you are connected with has not been verified.

Disable Insecure Ports and Services

As a general policy, any ports that are not needed should be disabled. You need to first know which ports are enabled, and then decide which of these ports can be safely disabled without disrupting the normal functioning of Cisco Crosswork Change Automation and Health Insights. You can do this by listing the ports that are open and comparing it with a list of ports needed for Cisco Crosswork Change Automation and Health Insights.

To view a list of all open listening ports:

Step 1 Log in as a Linux CLI admin user and enter the `netstat -aln` command. The `netstat -aln` command displays the server's currently open (enabled) TCP/UDP ports, the status of other services the system is using, and other security-related configuration information. The command returns output similar to the following:

```
[root@vm ~]# netstat -aln
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp    0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp    0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN
tcp    0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp    0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
tcp    0      0 127.0.0.1:10248         0.0.0.0:*               LISTEN
tcp    0      0 127.0.0.1:10249         0.0.0.0:*               LISTEN
tcp    0      0 192.168.125.114:40764   192.168.125.114:2379    ESTABLISHED
tcp    0      0 192.168.125.114:48714   192.168.125.114:10250   CLOSE_WAIT
tcp    0      0 192.168.125.114:40798   192.168.125.114:2379    ESTABLISHED
tcp    0      0 127.0.0.1:33392         127.0.0.1:8080          TIME_WAIT
tcp    0      0 192.168.125.114:40814   192.168.125.114:2379    ESTABLISHED
tcp    0      0 192.168.125.114:40780   192.168.125.114:2379    ESTABLISHED
tcp    0      0 127.0.0.1:8080          127.0.0.1:44276         ESTABLISHED
tcp    0      0 192.168.125.114:40836   192.168.125.114:2379    ESTABLISHED
tcp    0      0 192.168.125.114:40768   192.168.125.114:2379    ESTABLISHED
tcp    0      0 127.0.0.1:59434         127.0.0.1:8080          ESTABLISHED
tcp    0      0 192.168.125.114:40818   192.168.125.114:2379    ESTABLISHED
tcp    0      0 192.168.125.114:22     192.168.125.1:45837     ESTABLISHED
tcp    0      0 127.0.0.1:8080          127.0.0.1:48174         ESTABLISHED
tcp    0      0 127.0.0.1:49150         127.0.0.1:8080          ESTABLISHED
tcp    0      0 192.168.125.114:40816   192.168.125.114:2379    ESTABLISHED
tcp    0      0 192.168.125.114:55444   192.168.125.114:2379    ESTABLISHED
```

Step 2 Check the *Cisco Crosswork Change Automation and Health Insights Installation Guide* for the table of ports used by Cisco Crosswork Change Automation and Health Insights, and see if your ports are listed in that table. That table will help you understand which services are using the ports, and which services you do not need—and thus can be safely disabled. In this case, *safe* means you can *safely disable the port without any adverse effects to the product*.

Note If you are not sure whether you should disable a port or service, contact your Cisco representative.

- Step 3** If you have firewalls in your network, configure the firewalls to only allow traffic that is needed for Cisco Crosswork Change Automation and Health Insights to operate.
-

Harden Your Storage

We recommend that you secure all storage elements that will participate in your Cisco Crosswork Change Automation and Health Insights installation, such as the database, backup servers, and so on.

- If you are using external storage, contact your storage vendor and your Cisco representative.
- If you are using internal storage, contact your Cisco representative.
- If you ever uninstall or remove Cisco Crosswork Change Automation and Health Insights, make sure that all VM-related files that might contain sensitive data are digitally shredded (as opposed to simply deleted). Contact your Cisco representative for more information.

