Perform Administrative Tasks

This section contains the following topics:

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 Optimization Engine 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 Optimization Engine creates two special administrative IDs:

1. The **virtual machine administrator**, with the username **`cw-admin`**, and the default password**`cw-admin`**. Data center administrators use this ID to log in to and troubleshoot the VM hosting the Cisco Crosswork Optimization Engine 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 Optimization Engine 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 2.
- 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 Optimization Engine) 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 1).

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 1).

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.

Create User Roles

Local users with administrator privileges can create new users as needed (see Add Users, on page 2).

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 2).

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 3), 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 2). 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.

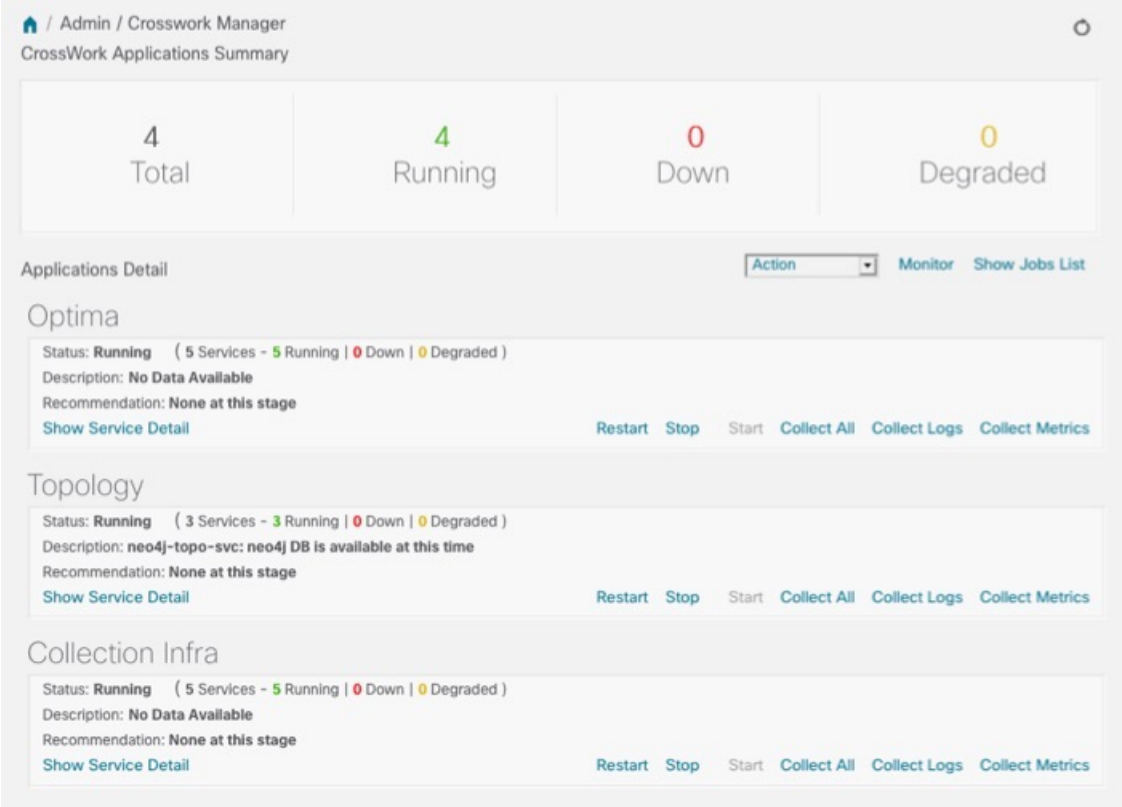
Step 4 Click **Delete** to confirm that you want to delete the user role.

Manage Cisco Crosswork Network Automation

The **Crosswork Manager** window gives you consolidated information about the current status of each installed Cisco Crosswork Optimization Engine 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 Optimization Engine.

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

Figure 1: Crosswork Manager Window



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 Optimization Engine 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 2: Applications Detail View

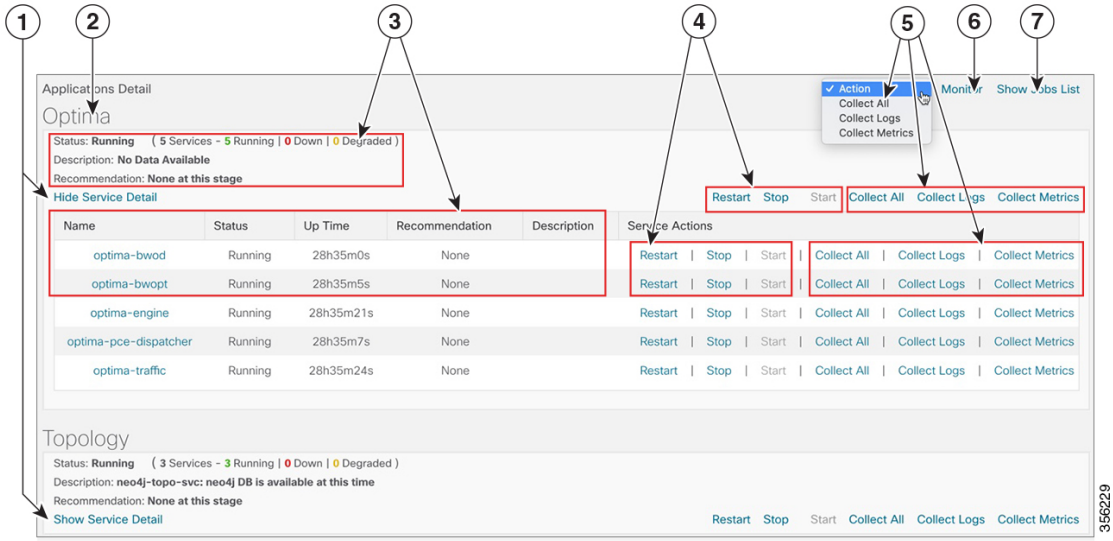


Figure 3: Applications Detail View

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: • **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 15.

Item	Description
5	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: • **Collect All** to collect both logs and metrics. • **Collect Logs** to collect only logs. • **Collect Metrics** to collect only metrics. See Collect and Share Cisco Crosswork Network Automation Logs and Metrics, on page 12.
6	Click the **Monitor** link to monitor individual Cisco Crosswork Optimization Engine functions and features, using analytical dashboards and data gathered over the last 24 hours of run time. See Monitor Cisco Crosswork Network Automation Functions in Real Time, on page 8.
7	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.

Monitor Cisco Crosswork Network Automation Functions in Real Time

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

Cisco Crosswork Optimization Engine 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 Optimization Engine 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...
Optima	Cisco Crosswork Optimization Engine function pack, traffic, and SR-PCE dispatcher functions.
Topology	Topology service and database functions.
Collection Infra	Device-data collection functions. Metrics include telemetry collection latencies, total collection operations, memory and database activity related to telemetry, delayed collections, and so on.
Core Infra	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 Optimization Engine maintains a maximum of 24 hours of collected metric data.

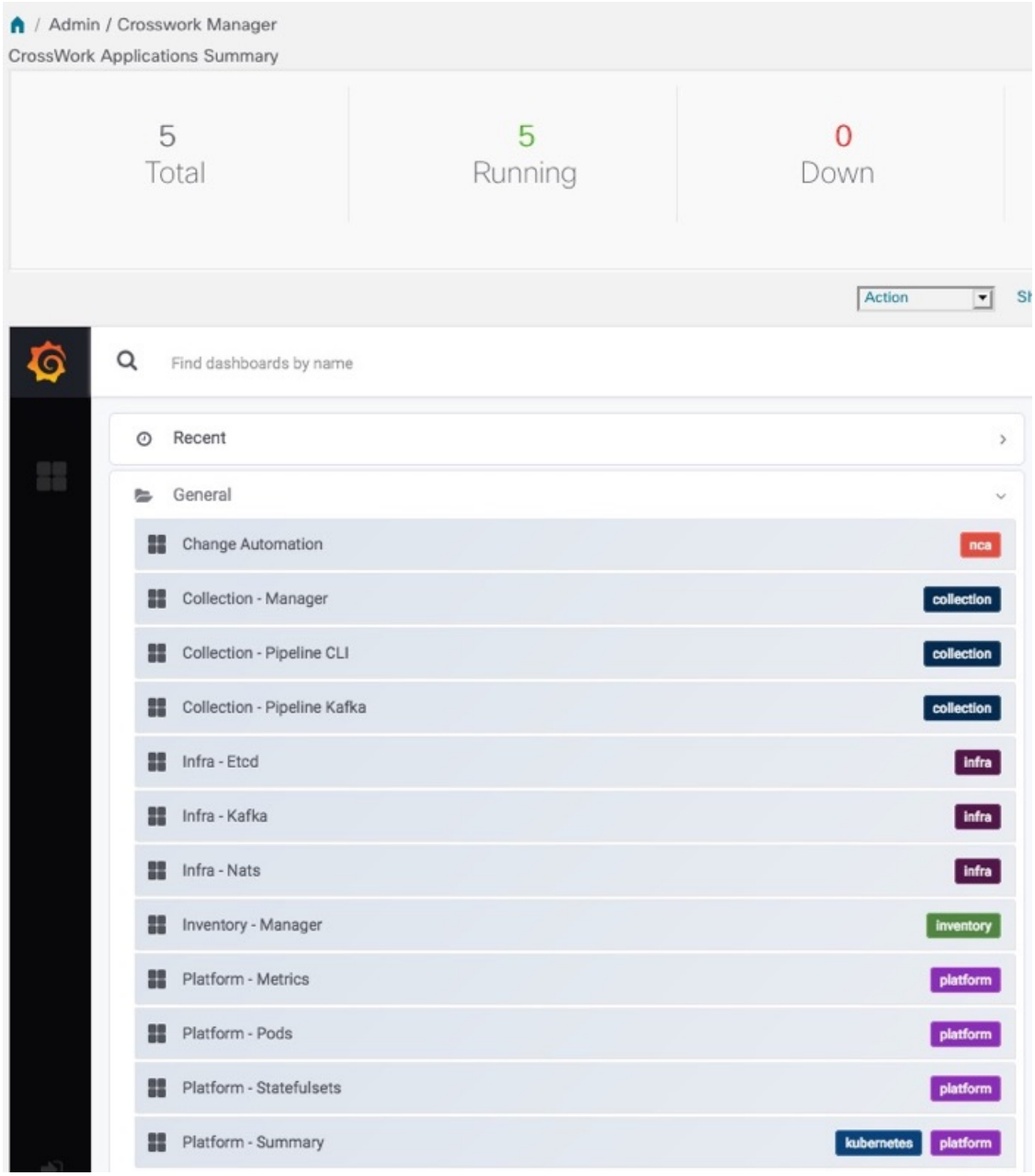
Grafana is an open-source visualization tool. The following provides general information about how to use the Cisco Crosswork Optimization Engine implementation of Grafana. For more information about Grafana itself, see https://grafana.com and http://docs.grafana.org

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

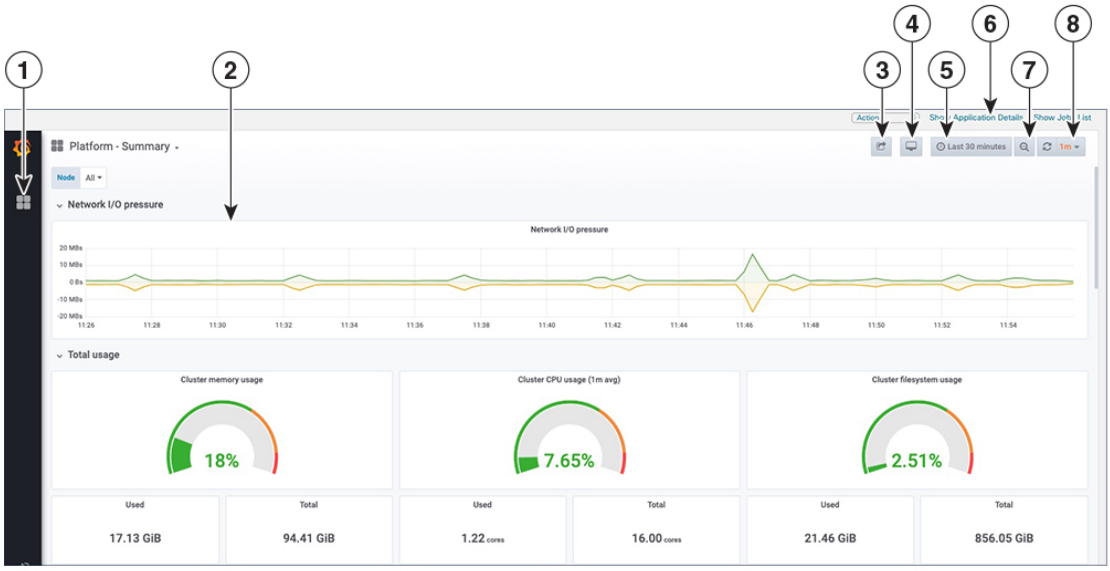
Step 2 At the right, just below the **Crosswork Applications Summary** view, click the **Monitor** link, highlighted below.

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.



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 htttps://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	**Time Series Graph Zoom**: You can zoom in on a specific time period within the graph of any time series data, as follows: **a.** Click a time-period starting point in the graph line and hold down the mouse. **b.** 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. To reset a zoomed time series graph to the default, click the **Zoom Out icon**.
3	**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: • **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 templatize 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.

Item	Description
4	**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.
5	**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. 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**. You can choose predefined refresh rates from **Off** to **2 Days**. When you have finished making changes, click **Apply**. When making selections, remember that Cisco Crosswork Optimization Engine keeps only 24 hours of data. If you select time ranges or refresh rates beyond that limit, the dashboard may be blank.
6	**Show Application Details**: Click this link to re-display the **Crosswork Manager** window's **Applications Detail** view.
7	**Zoom Out icon**: Click this icon to reset a zoomed time series graph back to the unzoomed state.
8	**Refresh icon**: Immediately refresh the data shown.

Collect and Share Cisco Crosswork Network Automation Logs and Metrics

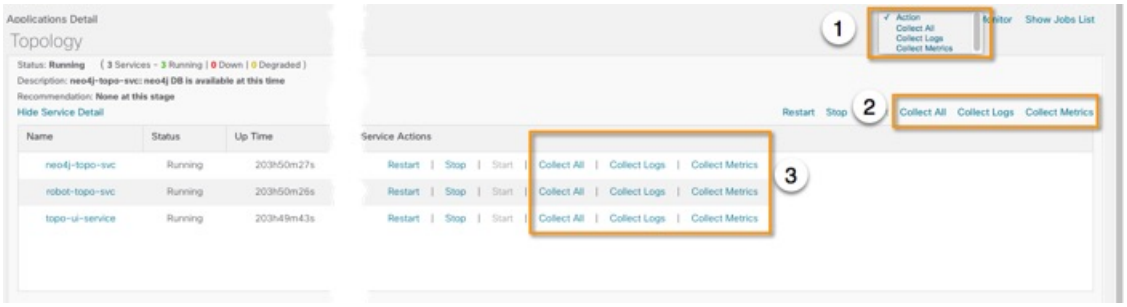
You can collect logs and metrics on multiple levels of Cisco Crosswork Optimization Engine. You can collect logs and metrics for the entire system, for any of its installed application, or for any service supporting an application. You can also choose to collect only logs, only the additional metrics,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

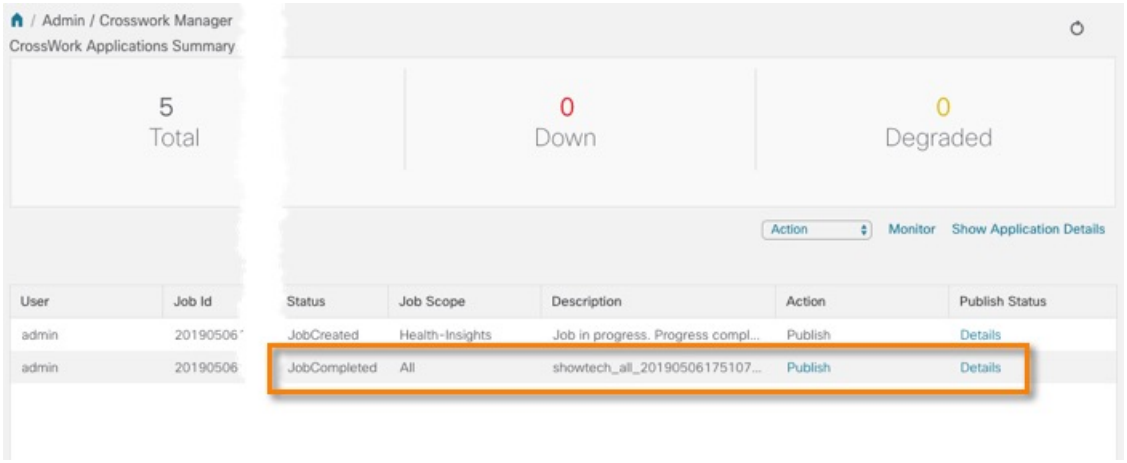
Step 2 Click the option for the collection level and target information you want, as follows:

- 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.

Audit Log

Audit logs map the user information in Cisco Crosswork Optimization Engine with all the critical user actions performed in the system.

User actions related to the following operations are included in the audit log:

- Device onboarding
- User creation, deletion, and configuration updates

- Cisco Crosswork Data Gateway management operations
- Collection job creation
- Administrative tasks (show-tech execution, topology updates, NSO-related actions)
- SR policy and RSVP TE tunnel creation, deletion, and configuration updates
- Affinity mapping configuration
- Bandwidth on Demand and Bandwidth Optimization function pack threshold and configuration updates
- RESTCONF API creation, deletion, and configuration updates

Sample Audit Log Entry

Cisco Crosswork Optimization Engine UI Audit Log Entry Example

```
2020-06-12 02:48:07,990 INFO c.c.s.o.e.AuditLogger [http-nio-8080-exec-3] time=2020-06-12
02:48:07.000990 message=SR Policy created successfully. user=admin policyId=admin
backend=local loginTime=1591929794
{data={"headEnd":"192.168.0.2","endPoint":"192.168.0.6","color":"999","description":"","profileId":"","bindingSid":"333",
 "path":{"type":"dynamic","pathName":"Automation_validating_sr","metric":"IGP",
"affinity":[{"constraintType":"EXCLUDE_ANY","affinity":[31]}],"disjointness":{"disjointType":"",
 "associationGroup":"","subId":""}, "protectedSegment":"SEG_PROTECTED"}}}
```

Cisco Crosswork Optimization Engine RESTCONF API Audit Log Entry Example

```
time="2020-06-06 13:49:06,308"
message="action=/operations/cisco-crosswork-optimization-engine-sr-policy-operations:sr-policy-delete,
 input={\"input\": {\"sr-policies\": [{\"head-end\": \"192.168.0.2\", \"end-point\":
\"192.168.0.3\", \"color\": 301}]}},
output={\"cisco-crosswork-optimization-engine-sr-policy-operations:output\":{\"results\":
[{\"head-end\":\"192.168.0.2\",\"end-point\":\"192.168.0.3\",\"color\":301, \"message\":\"SR
 policy  not found in Config DB\",\"state\":\"failure\"}]}}" user=admin policyId=admin
backend=local loginTime=1591451346 method=POST
url=/operations/cisco-crosswork-optimization-engine-sr-policy-operations:sr-policy-delete
```

Table 2: Common Audit Log entry fields

Field	Description
time	Time when the audit log is printed.
message	Message sent between applications.
user	Name of the user.
policyId	Role or permission of user (taken from local database, TACACS, or LDAP server).
backend	Server (local database, TACACS, or LDAP) against which user is authenticated.
loginTime	The epoch time when the user has logged in. Epoch time is intentionally selected, as it shorter and independent of time zones.
Other fields	Individual applications use additional fields specific to that application. For example: In the UI audit log entry above, **data** is a field that refers to the creation details of an SR policy and its attributes.

Audit Log location

Logs are placed in `/var/log/robot/audit/audit.log` under the respective application pods. For example: The Cisco Crosswork Optimization Engine UI audit log is under the **optima-uiservice** pod and the RESTCONF API audit log is under the **optima-restconf** pod.

In addition to the individual application audit logs, all audit log files are collected every hour as separate gzipped tar files in the following data directory:
`/mnt/robot_datafs/<app-name>/<instance>/auditlogs/auditlogs.tar.gz`

The audit log files are collected and circulated based on the maximum size and maximum number of backups on Cisco Crosswork Optimization Engine. For example: **`MaxSize:20 megabytes`** and **`MaxBackups: 5`**.

Control Cisco Crosswork Network Automation Applications and Services

Users with administrator privileges can control the runtime status of any Cisco Crosswork Optimization Engine 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

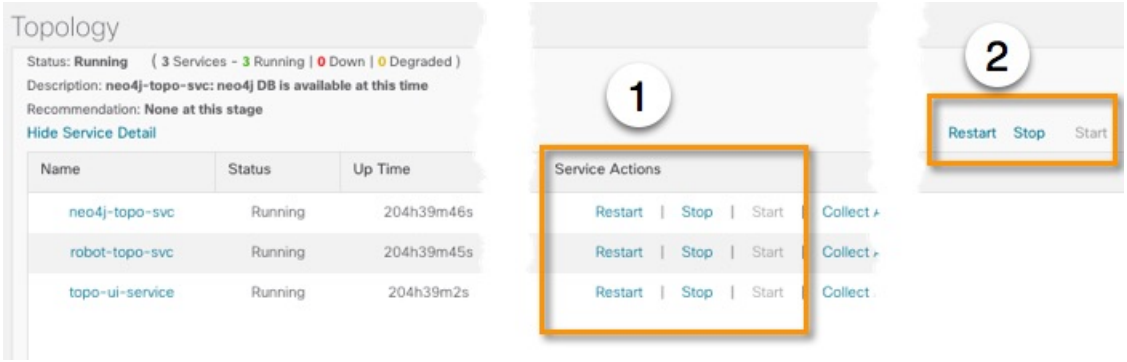
Please note that stopping, starting and restarting Cisco Crosswork Optimization Engine applications and services can result in anomalous system behavior and possible data loss. Use these functions only with the supervision of Cisco TAC staff.

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.



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 VM.

Follow the steps below to create a backup for the Cisco Crosswork Optimization Engine 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 Optimization Engine 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 Optimization Engine 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** and a prompt is displayed that suggests doing the backup or restore during maintenance window owing to 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 a job progress:**

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 ℹ 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 Cisco Crosswork Optimization Engine 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.
- If you find that there are missing SR policies or RSVP-TE tunnels in your topology, use the Configuration Database CLI tool (see Configuration Database CLI Tool, on page 18).

Configuration Database CLI Tool

The Configuration Database contains all SR policies and RSVP-TE tunnels that Cisco Crosswork Optimization Engine is aware of. The Configuration Database is updated whenever an SR policy or RSVP-TE tunnel is provisioned, modified, or deleted. The Configuration Database CLI tool is a utility that can do the following:

- Reads/writes CSV files to the Configuration Database
- Populates SR policy and RSVP-TE tunnel information from the Configuration Database to create a CSV file

The Configuration Database CLI tool is especially useful when trying to recover missing SR policies and RSVP-TE tunnels after a Restore operation. For example, the `--dump-missing` option produces a CSV file which lists missing SR policies and RSVP-TE tunnels. After reviewing this CSV file, you determine which SR policies and RSVP-TE tunnels were provisioned by Cisco Crosswork Optimization Engine and load them back into the topology using the `--load` option. See the CLI tool help for more information.

Step 1 Enter the **optima-pce-dispatcher** container:

```
kubectl exec -it optima-pce-dispatcher-XXXXXXX-XXXX bash
```

Step 2 You can run the following commands:

a) Show CLI tool help text.

```
python3 /opt/optima/pce_dispatcher/config_db/csv_util.py --help
```

b) Save all SR policies and RSVP-TE tunnels that are in the Configuration Database to a CSV file.

```
python3 /opt/optima/pce_dispatcher/config_db/csv_util.py --dump=/path/to/file/dump_file.csv
```

c) Load the contents from the provided CSV file and write policies to the Configuration Database.

```
python3 /opt/optima/pce_dispatcher/config_db/csv_util.py --load=/path/to/file/load_file.csv
```

Note If any duplicate SR policies (combination of headend, endpoint, and color) or RSVP-TE tunnels (combination of headend and tunnel name) are found, they will be overwritten. Only valid TE tunnels will be added to the Configuration Database.

d) Compare SR policies and RSVP-TE tunnels that are currently in the topology with what is saved in the Configuration Database and save the missing SR policies and RSVP-TE tunnels to a CSV file. This CSV file can then be used to load the missing policies into the Configuration Database.

```
python3 /opt/optima/pce_dispatcher/config_db/csv_util.py -dump-missing=/path/to/file/dump_file.cs
```

Manage TACACS+ Servers

In addition to local database authentication, Cisco Crosswork Optimization Engine 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. Priority field value is unique across TACACS+ and LDAP servers. Providing a duplicate value will result in an error.

Note

- Please note that any operation you do following the instructions in this section will affect all new logins to the Cisco Crosswork Optimization Engine 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 Optimization Engine supports the use of LDAPv3 servers with OpenLDAP 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 a unique 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 Optimization Engine user interface. To minimize session interruption, Cisco recommends that you perform all your TACACS+ 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.

Before you begin

Note the following:

- Cisco Crosswork Optimization Engine supports the use of LDAPv3 servers with OpenLDAP to authenticate users
- Roles needs to be mapped exactly to the same LDAP CrossworkPolicyId. See the example figure below.
- The user name in Crosswork and LDAP cannot be the same. If they are, the Crosswork user is prioritized.
- LDAP users cannot create Roles/Users even if it has an admin role.
- There are no errors that will indicate a misconfiguration when adding an LDAP server.

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

The **AAA** window opens. Click on the **LDAP Servers** tab.

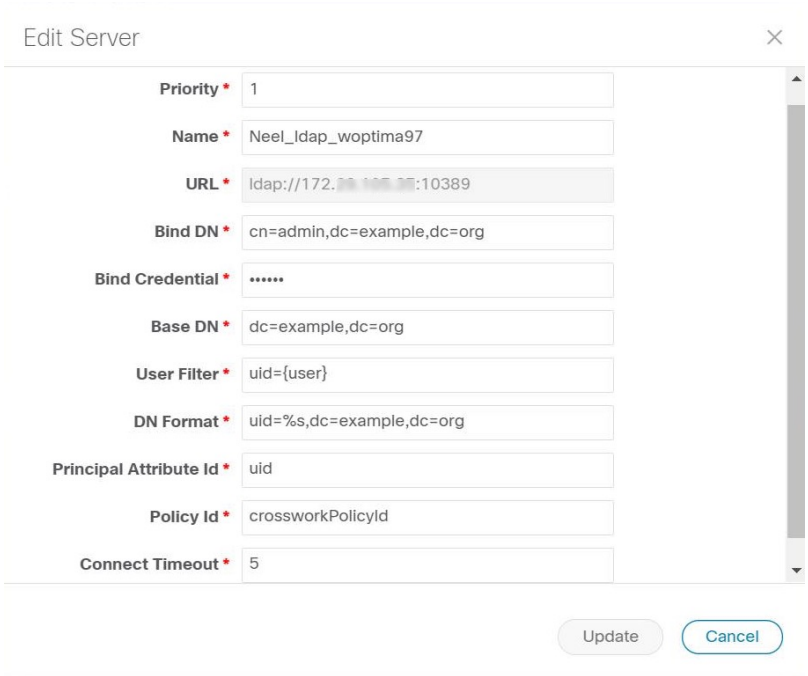
Step 2 Click ⊞ to open the **Add Server** dialog box.

Step 3 Enter the LDAP server settings, then click **Add**.

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.

The following figure shows a sample OpenLDAP configuration:

Figure 4: Adding an LDAP Server (OpenLDAP Configuration)



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 Topology Display Settings

Cisco Crosswork Optimization Engine administrator privileges are required to configure the display settings that are used by the Network Topology 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 Optimization Engine 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 31 and HTTPS, on page 31

When installed, Cisco Crosswork Optimization Engine 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 24

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 Optimization Engine 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 Optimization Engine.
- 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**
<COMMON NAME>	Common Name (CN=)	The IP address of the Cisco Crosswork Optimization Engine 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:

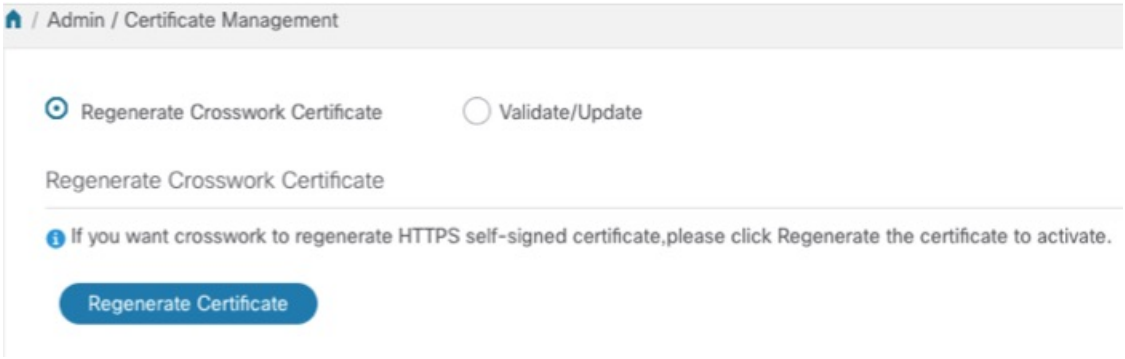
```
/usr/bin/openssl req \
                  -x509 \
                  -nodes \
                  -days 730 \
                  -newkey rsa:4096 \
                  -keyout "filename.key" \
                  -out "filename.crt" \
                  -subj "/C=US/ST=CALIFORNIA/L=SAN JOSE/O=CISCO SYSTEMS
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.



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

When Cisco Crosswork Optimization Engine 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 Optimization Engine.

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.

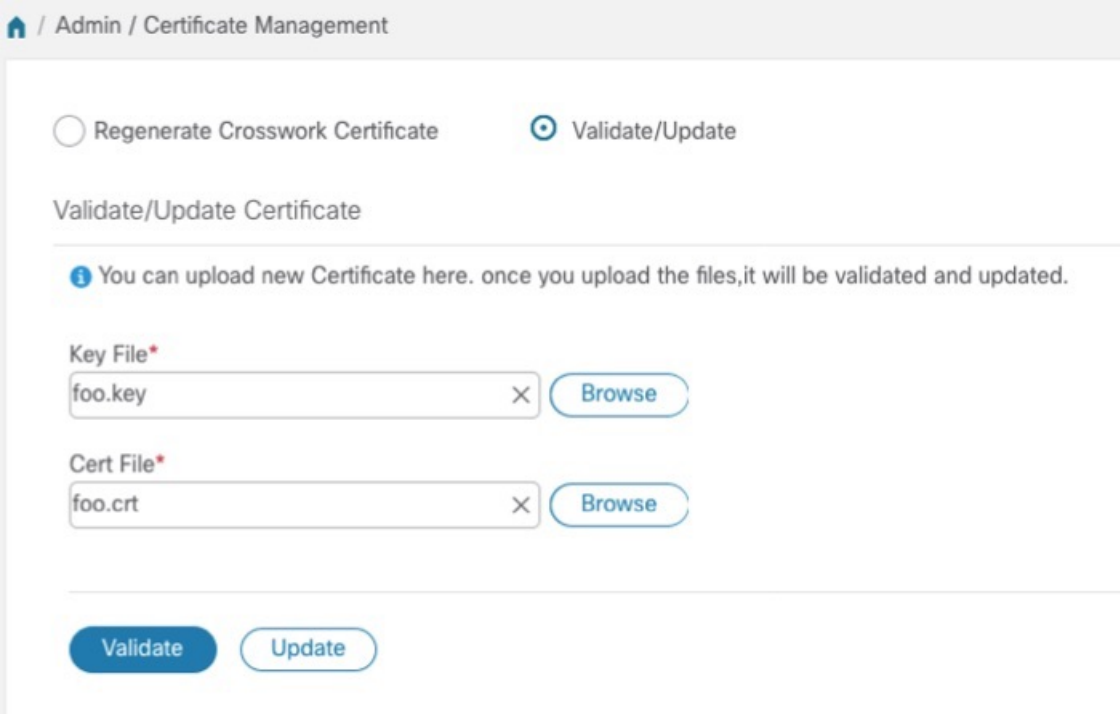
Before you begin

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.



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 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 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 Optimization Engine application.

Configure Transport Settings

You can configure the transport settings to decide how 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.

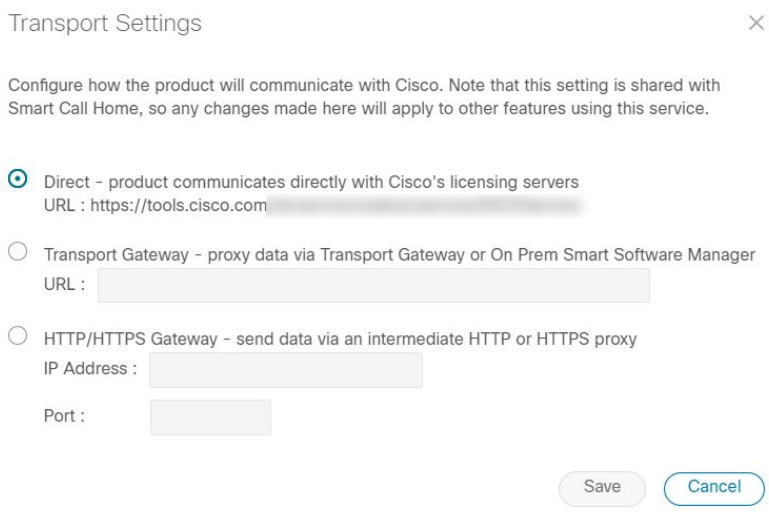
  Note For more information on the CSSM on-prem option, see the Smart Software Manager guide.

- **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 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.



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

Step 3 Click **Save**.

Register

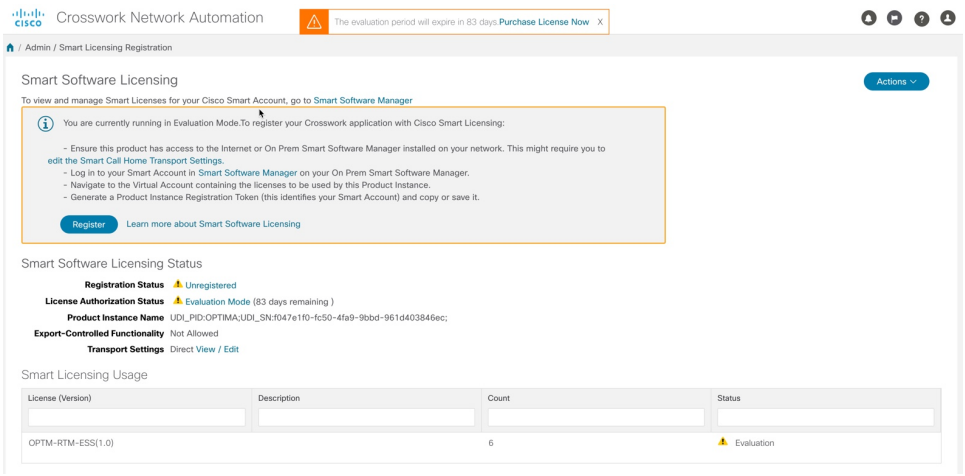
To enable licensed features, must be registered to CSSM using a registration ID token. Once registered, an Identity Certificate is saved securely in the Smart Account and used for all ongoing communications. The certificate is valid for one year and will be renewed automatically after six months to ensure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

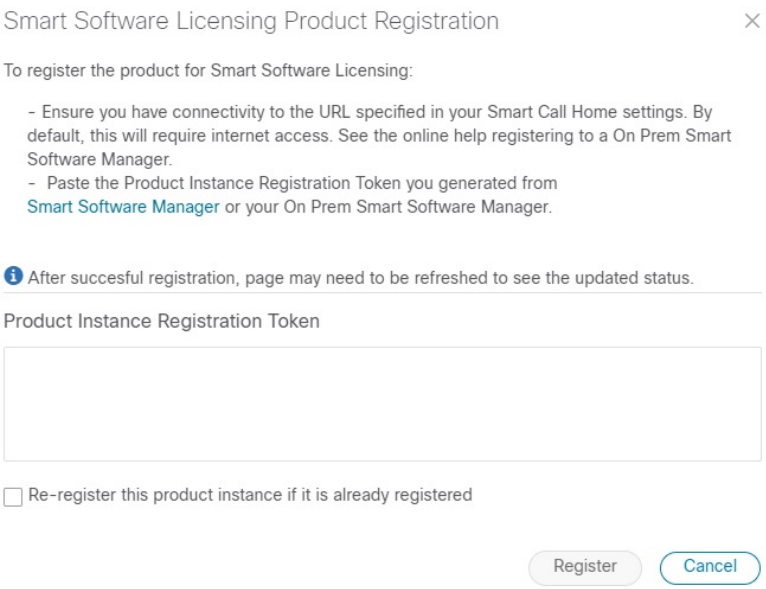
The registration status and license authorization status will be **Unregistered** and **Evaluation mode** respectively.

Figure 5: Smart Software Licensing Unregistered



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

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



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.

Note After a backup restore or disaster restore operation, you must manually re-register the VM to CSSM. This is applicable in case of a VM that has been already registered while taking the backup which is used in the restore operations.

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

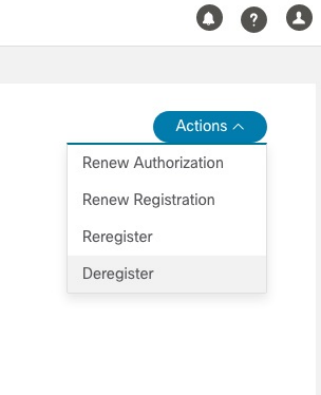
The registration status and license authorization status will be updated as **Registered** and **Authorized** respectively.

Note
- If you encounter a communication timeout error during registration, click **OK** in the error dialog box and the application will reattempt the registration.
- In some cases, after succesful registration, the page may need to be refreshed manually to see the updated status.

Manual Actions

The renewal of registration and authorization are automatically enabled for , 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.



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

Note Once de-registered, the 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 30

Step 2 The selected action is executed successfully.

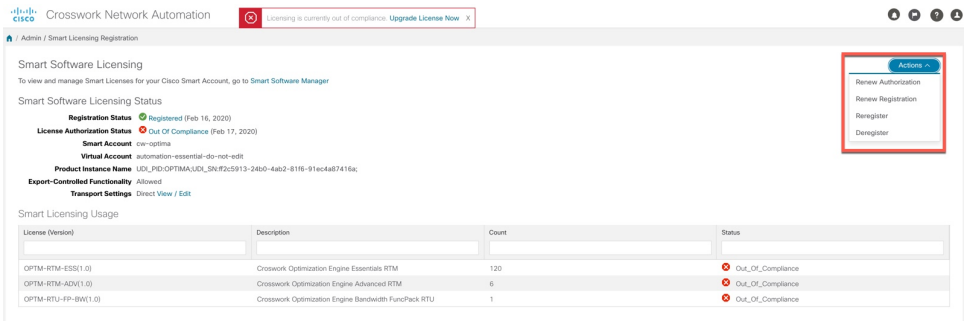
License Authorization Statuses

Based on the registration status of your 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. See figure below.
	Authorization Expired	The application is unable to communicate with the CSSM for 90 days or more, and the authorization has expired.

Figure 6: Registered and Out of Compliance Sample



Security Hardening Overview

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

- infrastructure
- storage system (local or external)

Hardening security requires completion of the following tasks:

- Shutting down insecure and unused ports
- Configuring network firewalls
- Hardening the 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 .

Core Security Concepts

If you are an administrator and are looking to optimize the security of your 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 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 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 . You can do this by listing the ports that are open and comparing it with a list of ports needed for .

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 Optimization Engine Installation Guide* for the table of ports used by Cisco Crosswork Optimization Engine, 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 Optimization Engine to operate.

Harden Your Storage

We recommend that you secure all storage elements that will participate in your 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 , 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.