Upgrade Cisco Crosswork

This chapter contains the following topics:

Upgrade Overview

This section provides the high-level overview for upgrading Cisco Crosswork Network Controller to the latest version. This includes upgrading Cisco Crosswork cluster, Cisco Crosswork Data Gateway and Crosswork Applications within a single maintenance window.

You can upgrade Cisco Crosswork in the following methods:

1. Upgrade Using Existing Hardware, on page 4
2. Upgrade Using Parallel Hardware, on page 14

The time taken for the entire upgrade window can vary based on size of your deployment profile and the performance characteristics of your hardware.

Warning Migration of Cisco Crosswork from an earlier version has the following limitations:

- License tags are not auto-registered as part of the upgrade operation. You must register them manually after the upgrade.
- Third-party device configuration in Device Lifecycle Management (DLM) and Cisco NSO is not migrated, and needs to be re-applied on the new Cisco Crosswork version post migration.
- Custom user roles (Read-Write/Read) created in earlier version of Cisco Crosswork are not migrated, and need to be updated manually on the new version post migration.
- Any user roles with administrative privileges in the earlier version of Cisco Crosswork must be assigned new permissions after the upgrade to continue being administrative users.
- Crosswork Health Insights KPI alert history is not retrieved as part of the migration.
- After a successful migration, you must perform a hard refresh or browser cache deletion before proceeding to use the system. Failing to do this step can result in data discrepency.
- Any LDAP users in 5.0 will not be allowed to log in to Crosswork 6.0 as a mandatory Device Access Group Attribute is not migrated in the upgrade from Crosswork 5.0 to 6.0. This occurs because Crosswork is unable to identify the correct DAG attribute available in the LDAP server after the upgrade. To resolve this, post upgrade you must set the mandatory DAG attribute in the Crosswork 6.0 LDAP server settings and create the corresponding DAGs for the users. After this, the remote login will work.

Crosswork applications can be independently updated from the Cisco Crosswork UI in case of minor updates or patch releases. For more information, see Update a Crosswork Application (standalone activity) , on page 21.

Upgrade Requirements

This section explains the requirements for upgrading the Cisco Crosswork if you are using the Crosswork Optimization Engine.

If you have enabled feature packs (Local Congestion Mitigation, SR Circuit Style Manager, or Bandwidth on Demand) in an earlier version of Crosswork and want to upgrade to the latest version, you must perform the following tasks prior to upgrading:

LCM

- From the LCM **Configuration** page:
  1. Set the **Delete Tactical SR Policies when Disabled** option to **False**. This task must be done prior to disabling LCM so that tactical polices deployed by LCM remain in the network after the upgrade.
  2. Set the **Enable** option to **False**. If LCM remains enabled, there is a chance that tactical policies may be deleted after the upgrade.
  3. Note all options (Basic and Advanced) in the LCM **Configuration** page so that you can confirm the same configuration has been migrated after the upgrade.

- Export the current list of interfaces managed by LCM (**Traffic Engineering** > **Local Congestion Mitigation** > **Export** icon). Confirm the interfaces are valid by reimporting the CSV file without errors. For more information, see "Add Individual Interface Thresholds".
- After the upgrade, wait until the **Traffic Engineering** page shows all the nodes and links before enabling LCM

Note:

After the system is stable and before enabling domains for LCM, confirm that the migration of previously monitored interfaces has completed and that each domain has the expected configuration options.

1. Navigate to **Administration** > **Alarms** > **All** > **Events** and enter **LCM** to filter the **Source** column.
2. Look for the following event: "Migration complete. All migrated LCM interfaces and policies are mapped to their IGP domains". If this message does not appear wait for the **Congestion Check Interval** period (set in the LCM **Configuration** page), then restart LCM (**Administration** > **Crosswork Manager** > **Optimization Engine** > **optima-lcm** > **...** > **Restart**).
3. Wait until the optima-lcm service changes from Degraded to Healthy state.
4. For each domain, navigate to the **Configuration** page and verify the options have been migrated successfully. If the domain configurations are incorrect, restart LCM (**Administration** > **Crosswork Manager** > **Optimization Engine** > **optima-lcm** > **...** > **Restart**).
5. Check the **Events** page for the event mentioned above and the **Configuration** page to verify the options.

Note

- If the confirmation message does not appear or domain configuration options are incorrect, then contact Cisco Technical support and provide them with showtech information and the exported Link Management CSV file.
- You can also manually add missing interfaces that were previously monitored or update domain configuration options *after* the system is stable.

CSM

- Set the **Enable** option to **False**.
- Note all options (Basic and Advanced) in the CSM **Configuration** page so that you can confirm the same configuration has been migrated after the upgrade.
- After the upgrade, wait until the **Traffic Engineering** page shows all the nodes and links before enabling CSM.
- Circuit Style SR-TE policies will go to operation down (Oper Down) state if CSM is not enabled within 8 hours after disabling.

BWoD

- Set the **Enable** option to **False**. If BWoD remains enabled, there is a chance that tactical policies may be deleted after the upgrade

- Note all options (Basic and Advanced) in the BWoD **Configuration** page so that you can confirm the same configuration has been migrated after the upgrade.
- After the upgrade, wait until the **Traffic Engineering** page shows all the nodes and links before enabling BWoD.

Upgrade Using Existing Hardware

This section explains how to migrate to the latest version of Crosswork Network Controller using the existing cluster.

Each stage in this upgrade workflow must be executed in sequence, and is explained in detail in later sections of this chapter. The stages are:

1. Shut Down Cisco Crosswork Data Gateway VMs, on page 4
2. Create Backup and Shut Down Cisco Crosswork, on page 5
3. Install the latest version of the Cisco Crosswork Cluster, on page 7

Note While the cluster installation is in progress, you must upgrade NSO to version 6.1.4. The process to upgrade NSO is not covered in this document. For more information, see the relevant Cisco NSO documentation. You must also upgrade your SR-PCE to version 7.11.1. For install instructions, see the Cisco IOS XRv 9000 Router Installation Guide..

4. Install the Cisco Crosswork Applications, on page 8

Note You are recommended to download and validate the application CAPP files before starting the actual upgrade process. This will reduce your system downtime as opposed to downloading the CAPP files midway through the upgrade process.

5. Migrate Cisco Crosswork Backup, on page 8
6. Upgrade Crosswork Data Gateway, on page 9
7. Post-upgrade Checklist, on page 12

Shut Down Cisco Crosswork Data Gateway VMs

This is the first stage of the upgrade workflow.

Note When Crosswork Data Gateway VMs are shut down, data will not be forwarded to data destinations. Check with the application providers to determine if any steps are needed to avoid alarms or other problems.

Before you begin

Take screenshots of all the tabs in the **Data Gateway Management** page to keep a record of the list of Crosswork Data Gateways, **Attached Device Count** in the Cisco Crosswork UI. In the **Pools** tab, for each pool listed here, take a screenshot to make a note of the active, spare, and unassigned VMs in the pool. This information is useful during Upgrade Crosswork Data Gateway, on page 9.

Step 1 Check and confirm that all the VMs are healthy and running in your cluster.

Step 2 Shut down the Crosswork Data Gateway VMs.

a) Log in to the Crosswork Data Gateway VM. See Access Crosswork Data Gateway VM from SSH.

Crosswork Data Gateway launches an Interactive Console after you log in successfully.

b) Choose **5 Troubleshooting**.

c) From the **Troubleshooting** menu, choose **5 Shutdown VM** to shut down the VM.

Create Backup and Shut Down Cisco Crosswork

This is the second stage of the upgrade workflow. Creating a backup is a prerequisite when upgrading your current version of Cisco Crosswork to a new version.

Note We recommend that you create a backup only during a scheduled upgrade window. Users should not attempt to access Cisco Crosswork while the backup operation is running.

Before you begin

Follow these guidelines whenever you create a backup:

- Cisco Crosswork will back up the configuration of the system to an external server using SCP. Before you begin you need to have the following configuration in place and information about the SCP server available:
  - The hostname or IP address and the port number of a secure SCP server.
  - A preconfigured path on the SCP server where the backup will be stored.
  - User credentials with file read and write permissions to the directory.
  - The SCP server storage requirements will vary slightly but you must have at least 25 GB of storage.
- Ensure that you have configured a destination SCP server to store the backup files. This configuration is a one-time activity.
- After the backup operation is completed, navigate to the destination SCP server directory and ensure that the backup file is created. You will require this backup file in the later stages of the upgrade process.
- Both the Cisco Crosswork cluster and the SCP server must be in the same IP environment. For example: If Cisco Crosswork is communicating over IPv6, so must the backup server.

- Keep a record of the list of Crosswork applications you have installed in the current version of Cisco Crosswork, as you can only install those applications after migrating to the new version of Cisco Crosswork.
- If you have onboarded a custom MIB package in the current version of Cisco Crosswork, download a copy of the package to your system. You will need to upload the package after you complete migrating to new version of Cisco Crosswork. See Post-upgrade Checklist, on page 12 for more infomation.
- If you have modified the current version of Cisco Crosswork to include third-party device types, you must download the third-party device configuration file, and re-apply it to the new version of Cisco Crosswork. The device configuration file is located on the cluster node (at `/mnt/cw_glusterfs/bricks/brick3/sys-oids.yaml`) and on the pod (at `/mnt/backup/sys-oids.yaml`).
- If Local Congestion Mitigation (LCM), SR Circuit Style Manager (CSM), and Bandwidth on Demand (BWoD) are enabled, you must disable them before proceeding. You must also, if available, export the current list of interfaces managed by LCM (**Traffic Engineering > Local Congestion Mitigation > Domain Identifier <domain_id> > Interface Thresholds > Export**). Follow the steps documented in Upgrade Requirements, on page 2.

Step 1 Check and confirm that all the VMs are healthy and running in your cluster.

Step 2 **Configure an SCP backup server:**

a) From the Cisco Crosswork main menu, choose **Administration** > **Backup and Restore**.
b) Click **Destination** to display the **Edit Destination** dialog box. Make the relevant entries in the fields provided.
c) Click **Save** to confirm the backup server details.

Step 3 **Create a backup:**

a) From the Cisco Crosswork main menu, choose **Administration** > **Backup and Restore**.
b) Click **Actions** > **Data Backup** to display the **Data Backup** dialog box with the destination server details prefilled.
c) Provide a relevant name for the backup in the **Job Name** field.
d) If any of the VMs or applications are not in **Healthy** state, but you want to create the backup, check the **Force** check box.

Note The **Force** option must be used only after consultation with the Cisco Customer Experience team.

e) Uncheck the **Backup NSO** checkbox if you don't want to include Cisco NSO data in the backup.

If you do want to include Cisco NSO data in the Cisco Crosswork backup process, follow the instructions given in **Backup Cisco Crosswork with Cisco NSO** section in the *Cisco Crosswork Network Controller 6.0 Administration Guide* instead of the instructions here.

f) Complete the remaining fields as needed.

If you want to specify a different remote server upload destination: Edit the pre-filled **Host Name**, **Port**, **Username**, **Password** and **Remote Path** fields to specify a different destination.

g) (Optional) Click **Verify Backup Readiness** to verify that Cisco Crosswork has enough free resources to complete the backup. If the verifications are successful, Cisco Crosswork displays a warning about the time-consuming nature of the operation. Click **OK**.

If the verification is unsuccessful, please contact the Cisco Customer Experience team for assistance.

h) Click **Start Backup** to start the backup operation. Cisco Crosswork creates the corresponding backup job set and adds it to the job list. The Job Details panel reports the status of each backup step as it is completed.

i) To view the progress of a backup job: Enter the job details (such as Status or Job Type) in the search fields in the **Backup and Restore Job Sets** table. Then click on the job set you want.

The **Job Details** panel displays information about the selected job set, such as the job Status, Job Type, and Start Time. If there's a failed job, hover the mouse pointer over the icon near the **Status** column to view the error details.

Note After the backup operation is completed, navigate to the destination SCP server directory and ensure that the backup file is created. You will require this backup file in the later stages of the upgrade process.

Note If you do not see your backup job in the list, refresh the **Backup and Restore Job Sets** table.

j) If the backup fails during upload to the remote server: In the **Job Details** panel, just under the Status icon, click the **Upload backup** button to retry the upload.

Note Upload can fail due to connectivity problems with the SCP backup server (for example, incorrect credentials, missing directory or directory permissions, missing path and so on). This is indicated by failure of the task **`uploadBackupToRemote`**). If this happens, check the SCP server details, correct any mistakes and try again. Alternatively, you can use the **Destination** button to specify a different SCP server and path before clicking **Upload backup**.

Step 4 After a successful backup, shut down the Cisco Crosswork cluster by powering down the VMs hosting each node (start with the Hybrid VMs):

a) Log into the VMware vSphere Web Client.
b) In the **Navigator** pane, right-click the VM that you want to shut down.
c) Choose **Power** > **Power Off**.
d) Wait for the VM status to change to **Off**.
e) Wait for 30 seconds and repeat steps 4a to 4d for each of the remaining VMs.

Step 5 Move Cisco NSO into read-only mode to avoid any unintended updates to Cisco NSO during the upgrade.

Use the following command to move NSO to read-only mode:

```
ncs_cmd -c maapi_read_only
```

Install the latest version of the Cisco Crosswork Cluster

After the successful backup of the old version of Cisco Crosswork, proceed to install the latest version of the Cisco Crosswork cluster.

Note The number of VM nodes installed in the new version of Cisco Crosswork must be equal or more than the number of VM nodes in the old version of Cisco Crosswork.

Before you begin

- Make sure that your environment meets all the installation prerequisites (see Installation Prerequisites for VMware vCenter for VMware and Installation Prerequisites for AWS EC2 for AWS).

Step 1 Install Cisco Crosswork cluster on your preferred platform (see Install Crosswork Cluster on VMware vCenter for VMware and Install Cisco Crosswork Network Controller on AWS EC2 for AWS).

Note During installation, Cisco Crosswork will create a special administrative ID (**virtual machine (VM) administrator**, with the username *cw-admin*, and the default password *cw-admin*). The administrative username is reserved and cannot be changed. The first time you log in using this administrative ID, you will be prompted to change the password. Data center administrators use this ID to log into and troubleshoot the Crosswork application VM. You will use it to verify that the VM has been properly set up.

Step 2 After the installation is completed, log into the Cisco Crosswork UI and check if all the nodes are up and running in the cluster.

a) From the Cisco Crosswork main menu, choose **Administration** > **Crosswork Manager** > **Crosswork Summary**.

b) Click **Crosswork Cluster** tile to view the details of the cluster such as resource utilization by node, the IP addresses in use, whether each node is a Hybrid or Worker, and so on.

Install the Cisco Crosswork Applications

After successfully installing the new version of the Cisco Crosswork cluster, proceed to install the latest version of the Cisco Crosswork applications.

Note The Cisco Crosswork applications that you install must be the same ones that were backed up during Create Backup and Shut Down Cisco Crosswork, on page 5.

Step 1 Install the Cisco Crosswork applications using the steps described in Install Crosswork Applications.

Step 2 After the applications are successfully installed, check the health of the new Cisco Crosswork cluster.

a) From the Cisco Crosswork main menu, choose **Administration** > **Crosswork Manager** > **Crosswork Summary**.

b) Click **Crosswork Cluster** tile to view the health details of the cluster.

Migrate Cisco Crosswork Backup

After successfully installing the new versions of the Cisco Crosswork applications, proceed to migrate the Cisco Crosswork backup taken earlier to the new Cisco Crosswork cluster.

Before you begin

Before you begin, ensure that you have:

- The hostname or IP address and the port number of a secure destination SCP server used in Create Backup and Shut Down Cisco Crosswork, on page 5.
- The name and path of the backup file created in Create Backup and Shut Down Cisco Crosswork, on page 5.

- User credentials with file read and write permissions to the directory.

Step 1 Check and confirm that all the VMs are healthy and running in your cluster.

Step 2 **Configure an SCP backup server:**

a) From the main menu, choose **Administration** > **Backup and Restore**.
b) Click **Destination** to display the **Edit Destination** dialog box.
c) Make the relevant entries in the fields provided.

Note In the **Remote Path** field, please provide the location of the backup created in Create Backup and Shut Down Cisco Crosswork, on page 5.

d) Click **Save** to confirm the backup server details.

Step 3 **Migrate the previous Cisco Crosswork backup on the new Cisco Crosswork cluster:**

a) From the Cisco Crosswork main menu, choose **Administration** > **Backup and Restore**.
b) Click **Actions** > **Data Migration** to display the **Data Migration** dialog box with the destination server details prefilled.
c) Provide the name of the data migration backup (created in Create Backup and Shut Down Cisco Crosswork, on page 5) in the **Backup File Name** field.
d) If you want to perform the data migration backup despite any Cisco Crosswork application or microservice issues, check the **Force** check box.
e) Click **Start Migration** to start the data migration operation. Cisco Crosswork creates the corresponding data migration job set and adds it to the **Backup and Restore Job Sets** table. The Job Details panel reports the status of each backup step as it is completed.

Note If you do not see your job in the list, please wait for a few minutes and refresh the **Backup and Restore Job Sets** table.

f) To view the progress of a data migration job: Enter the job details (such as Status or Job Type) in the search fields in the **Backup and Restore Job Sets** table. Then click on the job set you want.

The **Job Details** panel displays information about the selected job set, such as the job Status, Job Type, and Start Time. If there's a failed job, hover the mouse pointer over the icon near the **Status** column to view the error details.

Note Crosswork UI might become temporarily unavailable during the data migration operation. When the Crosswork UI is down, you can view the job status in the Grafana dashboard. The Grafana link is available as *View Data Migration Process Dashboard* option on the right side of the Job Details window.

g) If the data migration fails in between, you need to restart the procedure from step 1.

Step 4 After the data migration is successfully completed, check the health of the new Cisco Crosswork cluster.

a) From the Cisco Crosswork main menu, choose **Administration** > **Crosswork Manager** > **Crosswork Summary**.
b) Click **Crosswork Cluster** tile to view the health details of the cluster.

Upgrade Crosswork Data Gateway

This is the final stage of the upgrade work flow. Ensure that the migration is complete and the new Cisco Crosswork UI is available before you proceed with installing the latest version of Crosswork Data Gateway.

Note This procedure is required only for a Cisco Crosswork Data Gateway Base VM upgrade. Upgrade of other components, such as collectors, is performed by Cisco Crosswork.

Crosswork Data Gateway functions as a passive device in the network. The Crosswork Data Gateway upgrade process consists of the following steps replacing all the old Crosswork Data Gateway VMs with Crosswork Data Gateway VMs in the network.

Important Step 8 in this procedure requires you log out of Cisco Crosswork and log in again after verifying the deployment and enrollment of the latest Crosswork Data Gateway VMs with Cisco Crosswork. After you log in, an **Action to be taken** window appears prompting you to confirm that the upgrade is complete. Do not click **Acknowledge** unless you have completed all the verification steps mentioned in Step 3, Step 4, and Step 5 in the procedure.

Step 1 Log out of Cisco Crosswork and log in again.

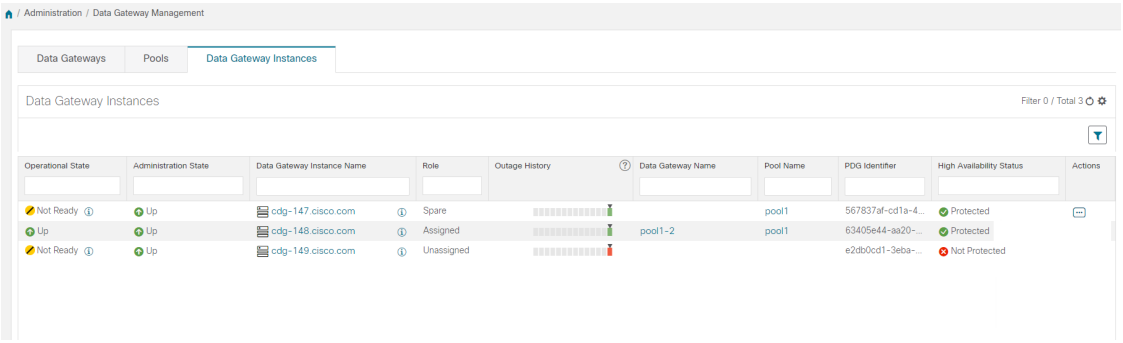
Step 2 After you log in, an **Action to be taken** window appears. Close this window and do not click **Acknowledge**.

Step 3 Install new Cisco Crosswork Data Gateway VMs with the same number and the same information (management interface importantly) as the old Crosswork Data Gateway VMs. Follow the steps in the Cisco Crosswork Data Gateway Installation Workflow.

Step 4 Wait for about 5 minutes and navigate to **Administration** > **Data Gateway Management**.

Step 5 Check the **Data Gateway Instances** tab to verify that the new Crosswork Data Gateway VMs are enrolled with Cisco Crosswork and have the **Admin State** as **Up** and **Operational State** as **Not Ready**.

Figure 1: Data Gateway Instances Window



Step 6 After the **Operational State** of the VMs changes to **Ready**, navigate to the **Pools** tab and verify that all the Crosswork Data Gateway pools from the previous version of Cisco Crosswork, are listed here. Edit each Crosswork Data Gateway pool to verify that the active Crosswork Data Gateway is same as one that you noted in the previous version of Cisco Crosswork.

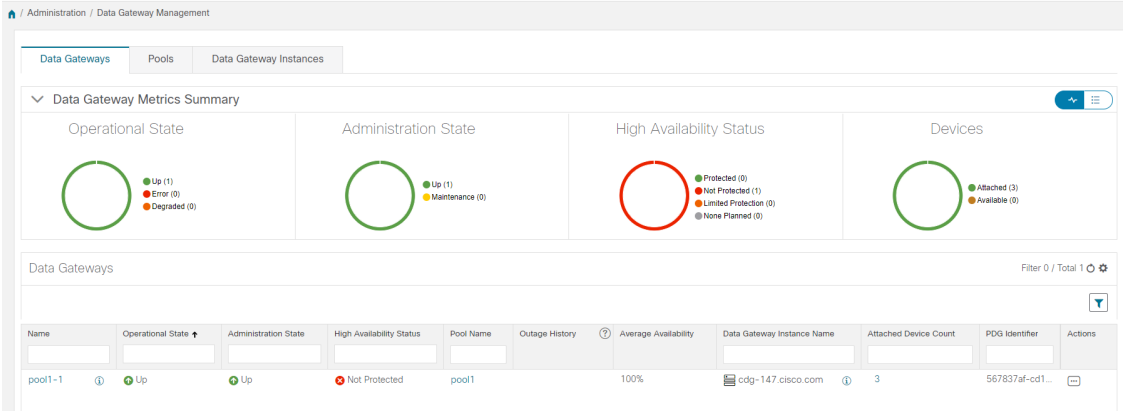
Note You can also verify the pool details by clicking on the pool name.

Step 7 **Verify that devices are attached to the Crosswork Data Gateways in the Cisco Crosswork UI.**

a) Navigate to the **Administration** > **Data Gateway Management** page.

b) Check the **Attached Device Count** of the Crosswork Data Gateway.

Figure 2: Data Gateway Window



Step 8 Log out of Cisco Crosswork.

After the upgrade is complete:

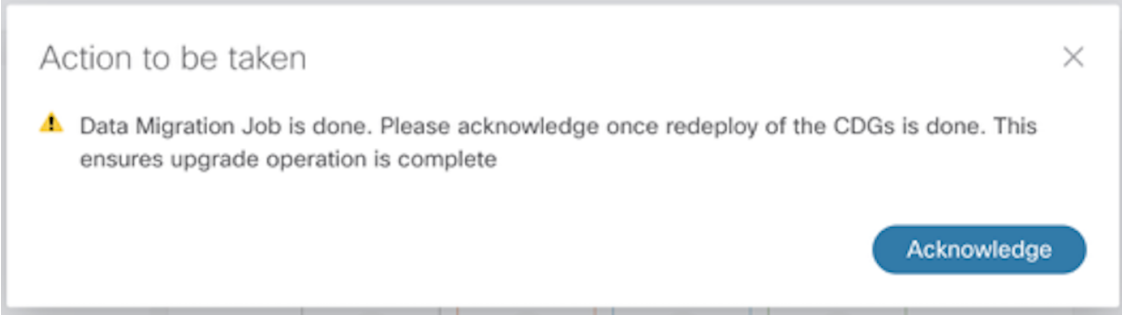
- Crosswork Data Gateway VMs are enrolled with Cisco Crosswork.
- All destinations, Crosswork Data Gateway pools, device-mapping information can be viewed on the Cisco Crosswork UI with the upgraded Crosswork Data Gateway VMs.
- Collection jobs start again automatically with the new Cisco Crosswork Data Gateway VMs.
- After upgrading the Crosswork Data Gateway VM, you must reconfigure the collector resources and the disabled containers. Global Parameter resources that were configured prior to the upgrade are not retained. To configure the resource parameters, on the Crosswork UI, navigate to **Administration** > **Data Gateway Global Settings** > **Data Gateway** > **Resource**. For more information on the resources, see *Cisco Crosswork Network Controller 6.0 Administration Guide*.

What to do next

After you log in to Crosswork Network Collection UI, the following window prompting for confirmation is displayed. Click **Acknowledge** in the pop-up that appears.

Important Do not click **Acknowledge** unless you have verified that the VMs are in the **Up**/**Not Ready** state. Doing so results in VMs having the state as **Error**. See Troubleshoot Crosswork Data Gateway Upgrade Issues.

Figure 3: Acknowledgment Window



(Optional) Move Cisco NSO out of maintenance or read-only mode.

```
ncs_cmd -c maapi_read_write
```

Troubleshoot Crosswork Data Gateway Upgrade Issues

The following table lists common problems that might be experienced when upgrading the Crosswork Data Gateway, and provides approaches to identifying the source of the problem and solving it.

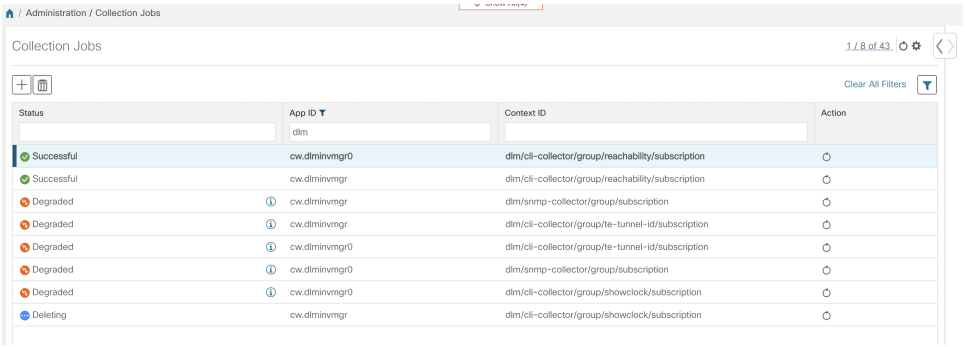
Issue	Recommended Action
Some of the Crosswork Data Gateway VMs are in **Error** or **Degraded** state because you clicked **Acknowledge** before the VMs came to the **Up**/**Not Ready** state	1. Wait for the Crosswork Data Gateway VMs to have the state as **Up** or **Not Ready** state. 2. Once the VMs have the state as **Up** or **Not Ready**, delete all Crosswork Data Gateway pools and create them again.
Some of the Crosswork Data Gateway VMs are in **Error** or **Degraded** state because you clicked **Acknowledge** before the VMs came to the **Up**/**Not Ready** state. The state of the VMs did not change to **Up**/ **Ready** and they are still in **Error**.	1. Delete all Crosswork Data Gateway pools. 2. Check if the VMs now have the state as **Up** or **Not Ready**. 3. If the VMs are still in a state of **Error**, manually re-enroll the VMs with the new version of Cisco Crosswork. See Re-enroll Crosswork Data Gateway for more information.
Crosswork Data Gateways VMs are stuck in the **Degraded** state with Image manager being in exited state. The list of components for the Crosswork Data Gateway either do not show Image manager or show it in an exited state.	1. In the Cisco Crosswork UI, navigate to **Data Gateway Management** > **Virtual Machines**. 2. Click the Crosswork Data Gateway that is degraded. 3. Click **Actions** and click **Reboot**.

Post-upgrade Checklist

After you upgrade Cisco Crosswork to the latest version, check the health of the new cluster. If your cluster is healthy, perform the following activities:

- Perform a hard refresh or browser cache deletion before proceeding to use the system. Failing to do this step can result in data discrepancy.
- Navigate to **Administration** > **Collection Jobs** in Cisco Crosswork UI and delete the duplicate system jobs.

Figure 4: Collection Jobs Window



- Verify that the collection jobs are running on the Crosswork Data Gateway VMs in the **Administration** > **Collection Jobs** page.
- Verify the restored AAA data by logging in using default credentials, and configure custom user roles (Read-Write/Read) in the upgraded Cisco Crosswork.
- (Optional) Based on your network requirements, download the relevant map files from cisco.com and re-upload them to the upgraded Cisco Crosswork.
- (Optional) If any NSO device onboarding policy was set in the previous version of Cisco Crosswork, you must update the policy with new Network Element Drivers (NED) on the NSO.
- (Optional) Re-apply any third-party device configurations (used in the previous version of Cisco Crosswork) to the new version of Cisco Crosswork.
- If you are using Crosswork Change Automation, verify that all the stock and custom playbooks are migrated successfully.
- If you are using Crosswork Health Insights, verify that the the collection to the external destination is working. Also, check if the alert dashboard is displaying the correct data.
- For Traffic Engineering, perform the following actions:
  - Upgrade the software versions in your devices as per the supported Cisco IOS XE/XR versions documented in the Traffic Engineering Compatibility Information.
  - Verify feature packs (Local Congestion Mitigation (LCM), Bandwidth Optimization (BWOpt), and Bandwidth on Demand (BWoD)) using the instructions in Upgrade Requirements, on page 2.

If you encounter errors in any of the above activities, please contact the Cisco Customer Experience team.

Upgrade Using Parallel Hardware

This section explains how to migrate to the latest version of Crosswork Network Controller using new hardware. This method relies on installing the new Cisco Crosswork cluster on new hardware in parallel while the data from the old Cisco Crosswork cluster is being backed up. This method is faster but requires twice the amount of resources for creating the new cluster in parallel.

The stages of the parallel upgrade workflow are:

1. Deploy a new Cisco Crosswork Cluster, on page 14

Note While the cluster installation is in progress, you must upgrade NSO to version 6.1.4. The process to upgrade NSO is not covered in this document. For more information, see the relevant Cisco NSO documentation. You must also upgrade your SR-PCE to version 7.11.1. For install instructions, see the Cisco IOS XRv 9000 Router Installation Guide..

2. Backup Cisco Crosswork Cluster, on page 15
3. Update DNS Server and Run Migration , on page 17
4. Add Crosswork Data Gateway to Cisco Crosswork, on page 18
5. Shut Down the old Cisco Crosswork Cluster, on page 20

Deploy a new Cisco Crosswork Cluster

Install the latest version of Cisco Crosswork cluster and applications on a new set of VMs in parallel.

Note The new Cisco Crosswork cluster must be installed with the same FQDN and same number of nodes as in the old version of Cisco Crosswork.

Before you begin

- Make sure that your environment meets all the installation prerequisites (see Installation Prerequisites for VMware vCenter for VMware and Installation Prerequisites for AWS EC2 for AWS).

Step 1 Install the new Cisco Crosswork cluster on your preferred platform (see Install Crosswork Cluster on VMware vCenter for VMware and Install Cisco Crosswork Network Controller on AWS EC2 for AWS).

Note During installation, Cisco Crosswork will create a special administrative ID (**virtual machine (VM) administrator**, with the username *cw-admin*, and the default password *cw-admin*). The administrative username is reserved and cannot be changed. The first time you log in using this administrative ID, you will be prompted to change the password. Data center administrators use this ID to log into and troubleshoot the Crosswork application VM. You will use it to verify that the VM has been properly set up.

Step 2 After the installation is completed, log into the Cisco Crosswork UI by navigating to https://<NEW_VIP>:30603.

Step 3 Check if all the nodes are up and running in the cluster.

a) From the Cisco Crosswork main menu, choose **Administration** > **Crosswork Manager** > **Crosswork Summary**.

b) Click **Crosswork Cluster** tile to view the details of the cluster such as resource utilization by node, the IP addresses in use, whether each node is a Hybrid or Worker, and so on.

Step 4 Install the applications which were part of the old version of Cisco Crosswork. For more information, see Install Crosswork Applications.

Step 5 After the applications are successfully installed, check the health of the new Cisco Crosswork cluster.

Backup Cisco Crosswork Cluster

Before you begin

Follow these guidelines whenever you create a backup:

- Cisco Crosswork will back up the configuration of the system to an external server using SCP. Before you begin you need to have the following configuration in place and information about the SCP server available:
  - The hostname or IP address and the port number of a secure SCP server.
  - A preconfigured path on the SCP server where the backup will be stored.
  - User credentials with file read and write permissions to the directory.
  - The SCP server storage requirements will vary slightly but you must have at least 25 GB of storage.
- Ensure that you have configured a destination SCP server to store the backup files. This configuration is a one-time activity.
- Both the Cisco Crosswork cluster and the SCP server must be in the same IP environment. For example: If Cisco Crosswork is communicating over IPv6, so must the backup server.
- Keep a record of the list of Crosswork applications you have installed in the current version of Cisco Crosswork, as you can only install those applications after migrating to the new version of Cisco Crosswork.
- If you have onboarded a custom MIB package in the previous version of Cisco Crosswork, download a copy of the package to your system. You will need to upload the package after you complete upgrading Cisco Crosswork. See Post-upgrade Checklist, on page 12 for more information.
- If you have modified the previous version of Cisco Crosswork to include third-party device types, you must download the third-party device configuration file, and re-apply it to the upgraded Cisco Crosswork. The device configuration file is located on the cluster node (at `/mnt/cw_glusterfs/bricks/brick3/sys-oids.yaml`) and on the pod (at `/mnt/backup/sys-oids.yaml`).
- If Cisco Crosswork Optimization Engine has feature packs (Local Congestion Mitigation (LCM), Bandwidth Optimization (BWOpt), and Bandwidth on Demand (BWoD)) that are enabled, you must disable them before proceeding. You must also, if available, export the current list of interfaces managed by LCM or BWOpt (**Traffic Engineering > Local Congestion Mitigation > Domain Identifier**

<domain_id> > Interface Thresholds > Export OR **Traffic Engineering > Bandwidth Optimization > Interface Thresholds > Export** icon). Follow the steps documented in Upgrade Requirements, on page 2.

Note We recommend that you create a backup only during a scheduled upgrade window. Users should not attempt to access Cisco Crosswork while the backup operation is running.

Step 1 Launch the Cisco Crosswork UI by using a browser and navigating to https://<FQDN>:30603

Step 2 Check and confirm that all the VMs are healthy and running in your cluster.

Step 3 **Configure an SCP backup server:**

a) From the Cisco Crosswork main menu, choose **Administration** > **Backup and Restore**.
b) Click **Destination** to display the **Edit Destination** dialog box. Make the relevant entries in the fields provided.
c) Click **Save** to confirm the backup server details.

Step 4 **Create a backup:**

a) From the Cisco Crosswork main menu, choose **Administration** > **Backup and Restore**.
b) Click **Actions** > **Backup** to display the **Backup** dialog box with the destination server details prefilled.
c) Provide a relevant name for the backup in the **Job Name** field.
d) If any of the VMs or applications are not in **Healthy** state, but you want to create the backup, check the **Force** check box.

Note The **Force** option must be used only after consultation with the Cisco Customer Experience team.

e) Uncheck the **Backup NSO** check box if you don't want to include Cisco NSO data in the backup.

If you want to include Cisco NSO data in the Cisco Crosswork backup process, follow the instructions given in **Backup Cisco Crosswork with Cisco NSO** section in the *Cisco Crosswork Network Controller 6.0 Administration Guide* instead of the instructions here.

f) Complete the remaining fields as needed.

If you want to specify a different remote server upload destination: Edit the pre-filled **Host Name**, **Port**, **Username**, **Password** and **Remote Path** fields to specify a different destination.

g) (Optional) Click **Verify Backup Readiness** to verify that Cisco Crosswork has enough free resources to complete the backup. Cisco Crosswork will also confirm that none of the applications are being updated, if the remote destination is correctly defined and if the applications are healthy. If the verifications are successful, Cisco Crosswork displays a warning about the time-consuming nature of the operation. Click **OK**.

If the verification is unsuccessful, please contact the Cisco Customer Experience team for assistance.

h) Click **Start Backup** to start the backup operation. Cisco Crosswork creates the corresponding backup job set and adds it to the job list. The Job Details panel reports the status of each backup step as it is completed.
i) To view the progress of a backup job: Enter the job details (such as Status or Job Type) in the search fields in the **Backup and Restore Job Sets** table. Then click on the job set you want.

The **Job Details** panel displays information about the selected job set, such as the job Status, Job Type, and Start Time. If there's a failed job, hover the mouse pointer over the icon near the **Status** column to view the error details.

Note If you do not see your backup job in the list, refresh the **Backup and Restore Job Sets** table.

j) If the backup fails during upload to the remote server: In the **Job Details** panel, just under the Status icon, click the **Upload backup** button to retry the upload.

Note Upload can fail due to connectivity problems with the SCP backup server (for example, incorrect credentials, missing directory or directory permissions, missing path and so on). This is indicated by failure of the task **`uploadBackupToRemote`**). If this happens, check the SCP server details, correct any mistakes and try again. Alternatively, you can use the **Destination** button to specify a different SCP server and path before clicking **Upload backup**.

Update DNS Server and Run Migration

Before you begin

Before you begin, ensure that you have:

- The hostname or IP address and the port number of a secure SCP server.
- The name and path of the backup file created in .
- User credentials with file read and write permissions to the directory.

Step 1 Update the DNS server to point the FQDN of the previous version of Cisco Crosswork cluster to the <VIP> of the new Cisco Crosswork cluster.

Step 2 Navigate to the upgraded Cisco Crosswork UI using https://<new_VIP>:30603.

Step 3 **Configure an SCP backup server:**

a) From the main menu, choose **Administration** > **Backup and Restore**.
b) Click **Destination** to display the **Edit Destination** dialog box.
c) Make the relevant entries in the fields provided.

Note In the **Remote Path** field, please provide the location of the backup created in Backup Cisco Crosswork Cluster, on page 15.

d) Click **Save** to confirm the backup server details.

Step 4 **Migrate the old Cisco Crosswork backup:**

a) From the Cisco Crosswork main menu, choose **Administration** > **Backup and Restore**.
b) Click **Actions** > **Data Migration** to display the **Data Migration** dialog box with the destination server details prefilled.
c) Provide the name of the data migration backup (created in Backup Cisco Crosswork Cluster, on page 15) in the **Backup File Name** field.
d) If you want to perform the data migration backup despite any Cisco Crosswork application or microservice issues, check the **Force** check box.
e) Click **Start Migration** to start the data migration operation. Cisco Crosswork creates the corresponding data migration job set and adds it to the **Backup and Restore Job Sets** table. The Job Details panel reports the status of each backup step as it is completed.

Note If you do not see your job in the list, refresh the **Backup and Restore Job Sets** table.

f) To view the progress of a data migration job: Enter the job details (such as Status or Job Type) in the search fields in the **Backup and Restore Job Sets** table. Then click on the job set you want.

The **Job Details** panel displays information about the selected job set, such as the job Status, Job Type, and Start Time. If there's a failed job, hover the mouse pointer over the icon near the **Status** column to view the error details.

Note Crosswork UI and Grafana monitoring might become temporarily unavailable during the data migration operation.

g) If the data migration fails in between, you need to restart the procedure from step 1.

Step 5 After the data migration is successfully completed, check the health of the new Cisco Crosswork cluster.

a) From the Cisco Crosswork main menu, choose **Administration** > **Crosswork Manager** > **Crosswork Summary**.

b) Click **Crosswork Cluster** tile to view the health details of the cluster.

Note After a successful migration, please perform a hard refresh or browser cache deletion before proceeding to use the system. Failing to do this step can result in data discrepency.

Add Crosswork Data Gateway to Cisco Crosswork

Ensure that the migration is complete and the new Cisco Crosswork UI is available before you proceed with installing the new version of Crosswork Data Gateway.

Note This procedure is required only for a Cisco Crosswork Data Gateway Base VM upgrade. Upgrade of other components, such as collectors, is performed by Cisco Crosswork.

Crosswork Data Gateway functions as a passive device in the network. The Crosswork Data Gateway upgrade process consists of replacing all old Crosswork Data Gateway VMs with new Crosswork Data Gateway VMs (latest version) in the network.

Important Step 6 in this procedure requires you to log out of Cisco Crosswork and log in again after verifying the deployment and enrollment of the new CDG VMs with Cisco Crosswork. After you log in, an **Action to be taken** window appears prompting you to confirm that the upgrade is complete. Do not click **Acknowledge** unless you have completed all the verification steps mentioned in Step 3, Step 4 and Step 5 in the procedure.

Step 1 Log out of the upgraded Cisco Crosswork and log in again.

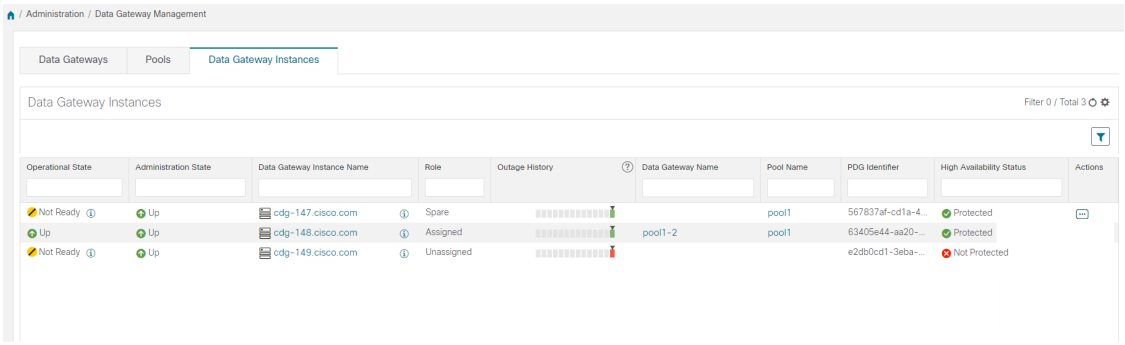
Step 2 After you log in, an **Action to be taken** window appears. Close this window and do not click **Acknowledge**.

Step 3 Install new Cisco Crosswork Data Gateway VMs (latest version) with the same number and the same information (management interface importantly) as the old Crosswork Data Gateway VMs. Follow the steps in the Cisco Crosswork Data Gateway Installation Workflow.

Step 4 Wait for about 5 minutes and navigate to **Administration** > **Data Gateway Management**.

Step 5 Check the **Data Gateway Instances** tab to verify that the new Crosswork Data Gateway VMs are enrolled with the new Cisco Crosswork, and have the **Admin State** as **Up** and **Operational State** as **Not Ready**.

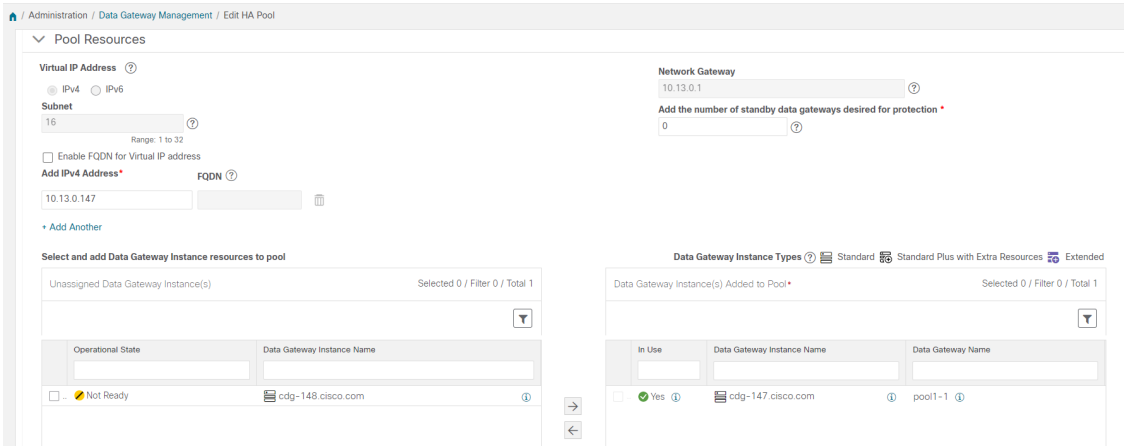
Figure 5: Data Gateway Instances Window



Step 6 After the **Operational State** of the VMs changes to **Ready**, navigate to the **Pools** tab and verify that all the Crosswork Data Gateway pools from the old Cisco Crosswork, are listed here. Edit each Crosswork Data Gateway pool to verify that the active Crosswork Data Gateway is same as one that you noted in the older version of Cisco Crosswork.

For example, the Crosswork Data Gateway pool in the following image contains two VMs, where the active VM is 172.23.247.78

Figure 6: Edit HA Pool Window



Step 7 **Verify that devices are attached to the new Crosswork Data Gateways in the upgraded Cisco Crosswork UI.**

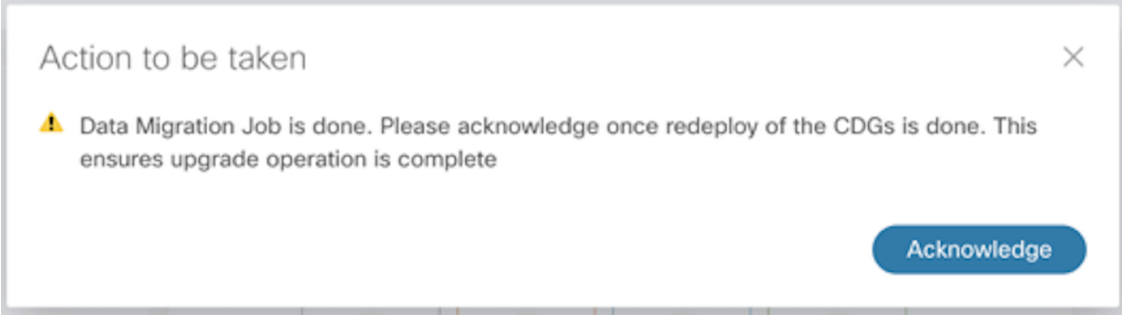
a) Navigate to the **Administration** > **Data Gateway Management** page.

b) Check the **Attached Device Count** of the Crosswork Data Gateway.

Step 8 Log out of Cisco Crosswork and log in again.

Step 9 After you log in, Cisco Crosswork presents you with the following window prompting for confirmation that the VMs. Click **Acknowledge** in the pop up that appears.

Figure 7: Acknowledgment Window



Important Do not click **Acknowledge** unless you have verified that the VMs are in the **Up**/**Not Ready** state. Doing so will result in VMs having the state as **Error**. See Troubleshoot Crosswork Data Gateway Upgrade Issues.

Step 10 (Optional) Move Cisco NSO out of maintenance or read-only mode.

```
ncs_cmd -c maapi_read_write
```

After the upgrade is complete:

- The new Crosswork Data Gateway VMs are enrolled with upgraded Cisco Crosswork.
- All destinations, HA Pools, device mapping information can be viewed on the Cisco Crosswork UI with the upgraded Crosswork Data Gateway VMs.
- Jobs start again automatically with the new Cisco Crosswork Data Gateway VMs.

Shut Down the old Cisco Crosswork Cluster

Before you begin

Gather the following information before shutting down the older version of Cisco Crosswork:

- All the IP addresses in the cluster.
- All the IP addresses of the CDGs.

Step 1 After a successful backup, shut down the Cisco Crosswork cluster by powering down the VMs hosting each node (start with the Hybrid VMs):

a) Log into the VMware vSphere Web Client.
b) In the **Navigator** pane, right-click the VM that you want to shut down.
c) Choose **Power** > **Power Off**.
d) Wait for the VM status to change to **Off**.
e) Wait for 30 seconds and repeat steps 1a to 1d for each of the remaining VMs.

Step 2 Shut down the Crosswork Data Gateway VMs.

a) Log in to the previous version of Crosswork Data Gateway VM. See Access Crosswork Data Gateway VM from SSH.

Crosswork Data Gateway launches an Interactive Console after you login successfully.

b) Choose **5 Troubleshooting**.
c) From the **Troubleshooting** menu, choose **5 Shutdown VM** to shut down the VM.

Step 3 (Optional) Move Cisco NSO into read-only mode to avoid any unintended updates to Cisco NSO during the upgrade.

Use the following command to move NSO to read-only mode:

```
ncs_cmd -c maapi_read_only
```

For more information, please refer to the relevant Cisco NSO documentation.

Update a Crosswork Application (standalone activity)

This section explains how to independently update a Crosswork application from the Cisco Crosswork UI in case of minor updates or patch releases. This procedure is not part of the upgrade workflow discussed in the earlier sections.

Before you begin, ensure that you:

- Take a backup of your data (using the backup/restore functionality) before any critical upgrade.
- Download the latest version of the Crosswork APPlication file (CAPP) from cisco.com to your local machine.

Note Crosswork does not support the downgrade operation of a CAPP file. However, if you want to go back to an older application version, you can uninstall the application and install the older version of the application. In case of a downgrade, you are advised to take a backup of your data prior to the operation.

Step 1 **Download and validate the CAPP files:**

a) Navigate to cisco.com and locate the CAPP files (.tar.gz) that you require.
b) Hover over the file and copy the MD5 or SHA512 checksum to your clip board.
c) Download the CAPP files to a server that can be reached from the Crosswork server.
d) Run a tool of your choice to calculate the checksum, and compare the checksum value in your downloaded file with the value you copied in the clip board.

For example, on a MAC you can use the **md5** command to calculate the MD5 sum on a file:

```
md5 cw-na-ztp-4.0.3-3-release-220614.tar.gz

ff47a72ed7dc4fc4be388db3a43fa13f
```

Verify that the result value matches with the posted value on cisco.com.

Step 2 Click on **Administration** > **Crosswork Manager**, and select the **Application Management** tab.

The Crosswork Platform Infrastructure and any applications that are added are displayed here as tiles.

Step 3 Click on the **Add File (.tar.gz)** option to add the application CAPP file that you had downloaded.

Step 4 In the Add File dialog box, enter the relevant information and click **Add**.

Once the CAPP file is added, you can observe the existing application tile (in this example, Zero Touch Provisioning) displaying an upgrade prompt.

Figure 8: Applications Window - Upgrade Prompt

Step 5 To upgrade, click the Upgrade prompt and the new version of the application is installed.

Figure 9: Applications Window - Update Progress

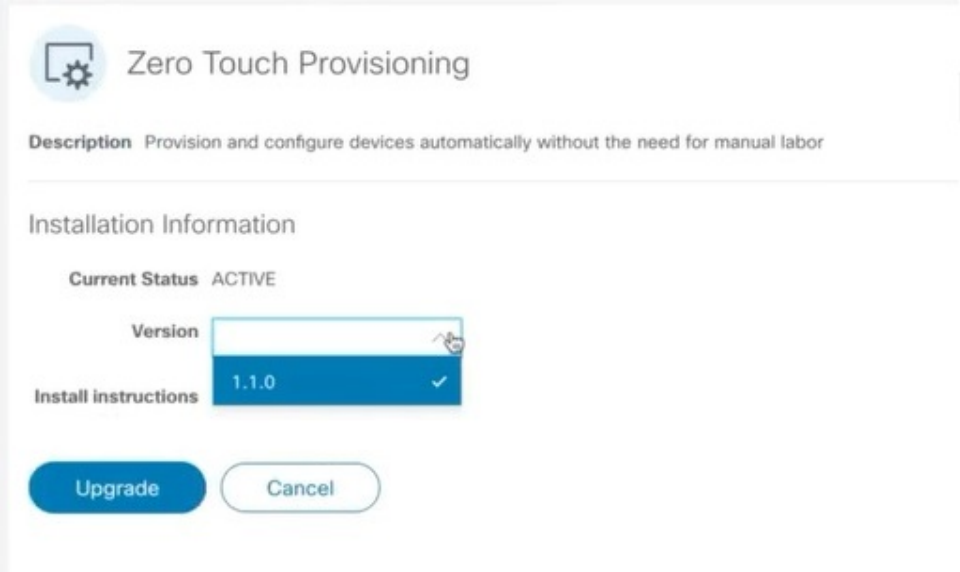
The upgrade progress is displayed on the application tile.

Step 6 Alternately, click ··· on the tile, and select the **Upgrade** option from the drop down list.

Figure 10: Applications Window - Upgrade Option

In the Upgrade screen, select the new version that you want to upgrade to, and click **Upgrade**.

Figure 11: Upgrade Window



Step 7 (Optional) Click on **Job History** to see the progress of the upgrade operation.

Note During an upgrade operation, typically only the components that have changed between the existing CAPP file and the new CAPP file are installed, as the new version may continue to use the most of the resources of the older version. This ensures a quick operation that happens without disruption to the current system and session.

Note During an upgrade, the application that is being updated will be unavailable until the update is completed. During this time, any other users using the application will be notified via an alarm about the upgrade.