Cisco Crosswork Hierarchical Controller 11.0.3

Release Notes

August 2026

Cisco Crosswork Hierarchical Controller version 11.0.3 release includes known limitation and bug fixes.

Install

You can install the Crosswork Hierarchical Controller version 11.0.3 in the same way you install the Crosswork Hierarchical Controller version 11.0.

For installation instructions, see the Cisco Crosswork Hierarchical Controller 11.0 Installation Guide.

Note- For the complete list of limitations and operational considerations in the 11.0 release, see the Cisco Crosswork Hierarchical Controller 11.0 Release notes.

Upgrade a standalone Crosswork Hierarchical Controller

Crosswork Hierarchical Controller 11.0.x can be upgraded to version 11.0.3

Patch installation procedure

Upgrading Crosswork Hierarchical Controller from 11.0.x to 11.0.3 version requires you to copy and upload the system pack to one of the nodes, pull it to the other instances, and then apply the upgrade on all nodes.

Note: Install the adapter service packs. The installation command MUST use the name that was in use prior to upgrading (if this is not the default adapter name, that is, if the **DYNAMIC_APP_GUID** param was used in the original installation to modify the name, install the new service pack with **DYNAMIC_APP_GUID=[adapter name as it was displayed in Device Manager on v11]**.

Before you begin:

1. Download the HCO v11.0.3 system pack from cisco.com.
2. Check if the system status is **Running**.

   ```
   sedo system status
   ```

To upgrade Crosswork Hierarchical Controller 11.0.x to 11.0.3:

1. Disable all the adapters. For each adapter:
   a. In the applications bar in Crosswork Hierarchical Controller, select **Device Manager** > **Adapters**.
   b. Select the required adapter in the **Adapters** list on the left.
   c. Select the **General** tab.
   d. Deselect the **Enabled** checkbox.
   e. Click **Save**.

2. Make a full backup of the system:

   ```
   sedo backup create full
   ```

3. Download the backup.

   ```
   sedo backup download -P <Add password> <add backup name>
   ```

   The backup file is available in the `/nxf` folder. Copy the backup file to an easily accessible and secure location on your system.

4. Copy the system pack provided to one of the instances (e.g. node1).
5. Upload the system pack (from the node it was copied to, e.g. node1):

   ```
   sudo sedo system upgrade upload <system-pack-name>
   ```

6. List the available upgrades:

   ```
   sudo sedo system upgrade list
   ```

7. (For HA) Pull the system pack on all other instances (there is no need to pull it to the instance on which it was uploaded):

   ```
   sudo sedo system upgrade pull <system-pack-name>
   ```

8. Apply the upgrade (on all nodes):

   ```
   sudo sedo system upgrade apply
   ```

9. Confirm that the upgrade was successfully applied to all nodes. If any node did not receive the upgrade, reapply it to that node.

   Note: The system will not reboot if the upgrade fails to apply on a node.

10. Check the system status and ensure that the HCO pods are not running.

    ```
    sedo system status
    ```

11. Reboot to complete (all nodes):

    ```
    sudo reboot
    ```

Post-upgrade tasks

1. Check:

   ```
   sedo version
   ```

   ```
   sedo system status
   ```

   Verify that the version is 11.0.3 and the system status is **Running**.

   Check the logs in the folder: `nxf-system/controller` to be sure there are no issues encountered during the upgrade.

2. Run the `sedo logs brain` command to verify that there are no unusual exceptions. If any are found, contact Cisco Customer Support.
3. Download the adapter service packs.

4. Install the adapter service packs. The installation command MUST use the name that was in use prior to upgrading (if this is not the default adapter name, that is, if the **DYNAMIC_APP_GUID** param was used in the original installation to modify the name, install the new service pack with **DYNAMIC_APP_GUID=[adapter name as it was displayed in Device Manager on v11.0]**.
5. Wait until the adapter pods are re-created using the newly installed service pack, and then validate that the adapter pods are restarted:

   ```
   sedo system status command
   ```

6. Reconfigure and enable the adapters in Device Manager.

Upgrade a Crosswork Hierarchical Controller Supercluster

This procedure describes how to upgrade a Crosswork Hierarchical Controller supercluster from version 11.0.x to version 11.0.3.

A supercluster in a 1+1+1 scenario includes:

- active single-node cluster
- standby single-node cluster
- single witness (arbitrator) node

This procedure describes how to upgrade:

1. Disable the adapters on the Active node.
2. Backup the Active node.
3. Replace NSO packages on both the Active and Standby nodes.
4. Upgrade the nodes separately in the following order:
   a. Active
   b. Standby
   c. Arbitrator
5. Upgrade the adapters on the Active node.

Disable adapters on active node

Disable all the adapters on the active node only.

Important: Ensure that you disable all the adapters, especially the CNC adapters if the PM is enabled and CDG enabled, before upgrading. If you do not, the default **DYNAMIC_APP_PORT=65001** will not be available after upgrade for the CNC adapters, and this will require additional configuration to use a different port.

1. Disable all the adapters. For each adapter:
   d. In the applications bar in Crosswork Hierarchical Controller, select **Device Manager > Adapters**.

e. Select the required adapter in the **Adapters** list on the left.

f. Select the **General** tab.

g. Deselect the **Enabled** checkbox.

h. Click **Save**.

2. Disable all the adapters. For each adapter:

```
sedo service disable <adapter_service_name>
```

3. Check that the adapter services are disabled:

```
sedo system status
```

Backup active node

Backup the active node only.

1. Make a full backup of the system:

```
sedo backup create full
```

2. Check the backup list:

```
sedo backup list
```

3. Download the backup file with a password:

```
sedo backup download -p <password> <backup file name>
```

Replace NSO packages

Replace the NSO packages on both the Active and Standby nodes:

1. Create an NSO backup before upgrading the NSO packages:

```
sedo nso backup create
```

2. Delete the old packages in the /nso/run/packages directory of the NSO Manager pod:

```
nso-pod$ cd /nso/run/packages
nso-pod$ rm -r *
nso-pod$ exit
```

3. Download new packages and place them in the /nso/run/packages directory:

```
kubectl cp [nso-package].tar.gz hco/nso-manager-srv-0:/usr/app
kubectl exec -it nso-manager-srv-0 -n hco -- /bin/bash
nso-pod$ cp /usr/app/[nso-package].tar.gz /nso/run/packages/
nso-pod$ cd /nso/run/packages/
nso-pod$ tar -zvxf [nso-package].tar.gz
nso-pod$ cp [nso-package]/packages/*.tar.gz /nso/run/packages/
```

Note: After the upgrade, the NSO package version will be 6.4.11.

Upgrade the nodes

Upgrade the nodes concurrently, starting the upgrades in the following order:

1. Active
2. Standby
3. Arbitrator

1. Copy the system pack to all instances.
2. Upload the system pack on all nodes:

   ```
   sudo sedo system upgrade upload <system-pack-name>
   ```

3. List the available upgrades on all nodes:

   ```
   sudo sedo system upgrade list
   ```

4. Apply the upgrade on all nodes:

   ```
   sudo sedo system upgrade apply
   ```

   Note: Wait for apply to be completed on all nodes before proceeding to the next step.

5. Wait for a minute and then reboot to complete (all nodes):

   ```
   sudo reboot
   ```

6. Check:

   ```
   sedo version

   sedo hco version

   sedo nso version

   sedo config list-keys
   ```

Upgrade adapters on active node

Upgrade and enable the adapters on the active node only.

Note: During the upgrade, if the Cisco CNC adapter is configured with the same destination name, old CDG adapter collection jobs are automatically removed from the Cisco CNC controller. If a different destination name is used, the old collection jobs must be manually deleted from the Cisco CNC controller.

1. Download the adapter service packs.
2. Install the adapter service packs. The installation command MUST use the name that was in use prior to upgrading (if this is not the default adapter name, that is, if the **DYNAMIC_APP_GUID** param was used in the original installation to modify the name, install the new service pack with **DYNAMIC_APP_GUID=[adapter name as it was displayed in Device Manager on v11] .**
3. Wait until the adapter pods are re-created using the newly installed service pack, and then validate that the adapter pods are restarted:

   ```
   sedo system status command
   ```

4. Re-enable the adapters in Device Manager.

Issues resolved

- CSCwt62908: CNC adapter incorrectly models Juniper device hierarchy by omitting FPC cards and mapping MIC and PIC components directly to the router.

- CSCwt63201: CNC adapter incorrectly identifies Nokia QSFP28 modules as non-pluggable, preventing them from appearing in the Transceivers tab.
- CSCwt91311: CNC adapter incorrectly models L2VPN signaling types as unknown instead of the reported BGP signaling.
- CSCwt96866: CNC adapter fails to remove links or adjacencies from HCO upon receiving DELETE notifications due to processing errors.
- CSCwu08118: CNC adapter now appends " TRA" to Nokia transceiver port names to differentiate them from physical ports in the inventory tree and resolve display confusion.
- CSCwu44856: CNC adapter fails to model all LAG links, causing some links to be missing from HCO.
- CSCwu63429: CNC adapter fails to persist LAG port status changes in HCO due to an unexpected value in the tp.layer-rate field.
- CSCwu72975: CNC adapter fails to create aggregate ports for certain devices, resulting in missing aggregate links in HCO.
- CSCwv09820: CNC adapter fails to return the archive path to NFDK, leaving topology files in the archive directory uncompressed.
- CSCwv07954: Optical ports are not created due to regex pattern mismatch.
- CSCwt64785: Network Explorer App does not clearly represent parent-child VPN relationships, preventing navigation from parent to child VPNs.
- CSCwq09417: Logical Link Persistor fails to discover or incorrectly marks LAG-based logical links as DOWN when all underlying R_PHY ports contain cross-links.
- CSCwt42683: Link Manager validation fails due to request timeouts during device adapter communication
- CSCwt76739: Service Assurance app omits Ingress and Egress QOS columns for L2 VPN services.
- CSCwv34641: RCA application fails to process and remains in 'Running/NODATA' state when a downlink path references itself.

Known limitations

Validation of Notification Flow for Specific Defects

Verification for the following defects was conducted using simulated topology files rather than physical hardware components. As a result, the end-to-end notification flow for these specific scenarios has not been validated in a live environment:

- CSCwt62908
- CSCwt63201
- CSCwu08118
- CSCwu44856

Application updates

There are no new features.

Release collaterals

All the Cisco Crosswork Hierarchical Controller 11.0 documents are relevant and can be used for 11.0.3 release.

This includes:

Documents
Cisco Crosswork Hierarchical Controller 11.0 Network Visualization Guide
Cisco Crosswork Hierarchical Controller 11.0 Administration Guide
Cisco Crosswork Hierarchical Controller 11.0 Assurance and Performance Guide
Cisco Crosswork Hierarchical Controller 11.0 Service Provisioning Guide
Cisco Crosswork Hierarchical Controller 11.0 Analytics Guide
Cisco Crosswork Hierarchical Controller 11.0 NBI and SHOL Reference Guide
Cisco Crosswork Hierarchical Controller 11.0 Installation Guide
Adapter documentation is released on www.cisco.com

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.