Unified CCX Upgrade

Unified CCX Upgrade Types

You can upgrade to Unified CCX version 12.5(1) SU2 only from Unified CCX versions 11.6(2), 12.0, 12.5(1), and 12.5(1) SU1. If you are using any prior release of Unified CCX, you have to upgrade to 11.6(2) or 12.0 and then upgrade to 12.5(1) SU2.

Note To upgrade to 12.5(1) SU2, apply the release-specific preupgrade COP file. For more information on release versions and their corresponding COP files, see Preupgrade Tasks, on page 5.

Table 1: Upgrade Details

Upgrade File Type	Upgrade Method	Apply Upgrade From
ISO Image	• Command Line Interface (CLI) • Cisco Unified OS Administration Web Interface	• Local ISO • FTP/SFTP server

Note

- There is service interruption during the upgrade and subsequent server restart.
- The new version installs on the inactive partition.
- For more information on supported component versions and browsers, see the Unified CCX Compatibility related information that is located at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-device-support-tables-list.html.

Note You can use the Cisco Prime Collaboration Deployment application also to upgrade your cluster. For more information, see *Cisco Prime Collaboration Deployment Administration Guide*.

Important Considerations for Upgrade

- To manage your license better, migrate to smart Licensing. For more information about Smart Licensing, see *Cisco Unified Contact Center Express Features Guide*.

  If you want to continue using Cisco WFO, you must remain on Classic Licensing as Cisco WFO does not support Smart Licensing.

- For systems upgrading from 12.5.1 SU1 or earlier to 12.5.1 SU2 or higher, you must update `AssertionConsumerService` URL manually on IDP, or as part of normal configuration process you must disable SSO, generate new Service Provider XML file, and reconfigure SSO.

  Upon upgrading from 12.5.1 SU1 to SU2, the SP XML File on UCCX changes as below:

  - For 12.5.1 SU1 or prior, `https://FQDN:8553/ids/saml/response`
  - For 12.5.1 SU2 or higher, `https://FQDN:8553/ids/saml/response?metaAlias=/sp`

- For a 100 agent profile, if you want to deploy Cloud Connect, you must configure 14GB of vRAM. For a 400 agent profile, you must configure 20GB of vRAM.

Note

- A 300 agent profile is not available. You cannot switch versions.
- For a 100 agent profile, if you do not want to deploy Cloud Connect, there is no change.
- Ensure that the reservation of CPU and memory adhere to the specifications mentioned in the Virtualization Wiki.

- Install Unified CCX only on virtual machines. Unified CCX will not run on bare metal.
- In the virtual machine, change the Guest OS version to match the OS version of Unified CCX.
- DNS is mandatory. Before you upgrade, configure the domain name and DNS server IPs and ensure the forward and reverse lookups on the DNS server are correct.
- Do not make any configuration changes during upgrade because changes are lost after upgrade.
- Always ensure to perform the backup on the first node before you start upgrading the second node.
- Upgrade Unified CCX during off-peak hours or during a maintenance window to avoid service interruptions.
- In an HA deployment of Unified CCX, you must switch both the Unified CCX nodes to the newer version during the same maintenance window.

  If the contact center is expected to function with only the first node that is switched to the new version, ensure that the following conditions are met until the switch version on the second node is complete:

  - No agents are logged in to the second node.
  - The services, **Cisco Finesse Tomcat**, **Cisco Unified CCX Engine**, and **Cisco Unified CCX Database** are in **Stopped** state on the second node.

- Upgrade Unified CCX and Cisco Customer Collaboration Platform in the same maintenance window and perform the upgrade on Cisco Customer Collaboration Platform first, followed by Unified CCX.
- After the upgrade of Cisco Customer Collaboration Platform, unread and unhandled emails are downloaded from the mail server and added to Unified CCX. However, the draft emails are not downloaded.
- Ensure that a valid Cisco Customer Collaboration Platform OVA is deployed for a successful install or upgrade. The upgrade stops if no Cisco Customer Collaboration Platform OVA is found in the deployment.
- Both the nodes in a cluster must run the same release of Unified CCX. The only exception is while you are upgrading the cluster software, during which a temporary mismatch is allowed.
- Upgrade VMware tools and change the NIC adapter type for Unified CCX after the refresh upgrade and before initiating the switch version.
- For more information on Certificates, see *Cisco Unified Contact Center Certificate Management Guide* available at: https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/118855-configure-uccx-00.html.
- Unified CCX 10.0(1) and later versions include a feature in the VMware Installation information line to indicate if the disk partitions are aligned. For aligned disk partitions, the VMware installation information line indicates "Partitions aligned". After upgrading, if the VMware installation information line indicates

"ERROR-UNSUPPORTED: Partitions unaligned.", it means that Cisco cannot provide support for any performance issues. To correct a virtual machine with unaligned partitions, you must perform the applicable restore (with rebuild) scenario procedure in Unified CCX Administration. For more information, see *Cisco Unified Contact Center Express Admin and Operations Guide*.

- After the upgrade, the OS Administration lists the manually uploaded third-party CA certificates but does not list the third-party CA certificates that are packaged with Unified CCX.
- If any Unified Intelligence Center user was made an Administrator using the **utils cuic user make-admin [user-name]** command before an upgrade of Unified CCX, the user loses the Cisco Cisco Unified Intelligence Center Administrator capabilities after the upgrade. Execute the CLI again, after the upgrade, to make the user a Cisco Unified Intelligence Center Administrator.
- In an HA setup, do not switch versions on both the first and second nodes at the same time.
- When you upgrade Unified CCX in an HA deployment, ensure that the following conditions are met before the switch version is initiated on Node 2:
  - If you have upgraded Node 1 to a new version and then reinstalled Node 2 with an older version, you must upgrade Node 1 and Node 2 again to the new version, before you start the switch version.
  - The switch version of Node 1 is complete and the node is successfully restarted. Otherwise, the upgrade might fail or there might be discrepancy in data.

Note The switch version of Node 1 automatically initiates a node restart and there is no need to manually restart Node 1.

  - Ensure that you are able to log in successfully to Cisco Unified Intelligence Center, on Node 1, using the Administrator or Reporting User credentials.

- You may experience a delay of approximately 30 minutes for the services to start during the first restart of the Unified CCX system after switching the version. This is due to the application of security policies after upgrade. This delay will not appear in subsequent restarts.
- Do not modify the Hostname or IP address of the Unified CCX server during the upgrade process.
- After the upgrade of Unified CCX, agents and supervisors must clear the browser cache and cookies before logging in to the Cisco Finesse Desktop and the Cisco Unified Intelligence Center.
- After a successful installation or upgrade, download and install the language pack COP to use the Cisco Unified Intelligence Center interface and the Cisco Finesse Desktop interface in a language other than English.
- After the upgrade, you must manually remove the Context Service gadget from the Cisco Finesse desktop (Desktop Layout and Team Desktop Layout).
- After the upgrade of Unified CCX, if necessary, the administrator can copy the sample configurations for customizing desktop properties from the **View Default Layout** (Cisco Finesse Administration console > **Desktop Layout**) and add to the respective custom layouts.

  For more information, see the *Upgrade* section in the *Cisco Finesse Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html.

- After the upgrade, you can move to Smart Licensing. For Smart Licensing details, see *Cisco Unified Contact Center Express Features Guide*.
- From Unified CCX Release 12.5(1) SU1, the connection between RmCm Subsystem and Unified CM can be secured by enabling Secure Real–Time Transport Protocol (SRTP) in AppAdmin. If you had enabled SRTP before upgrading to Unified CCX Release 12.5(1) SU1, disable and enable it again after upgrade. Otherwise, the connection between RmCm Subsystem and Unified CM will not be secure.
- When SRTP is enabled in Unified CCX release 12.5(1), after upgrading to Unified CCX release 12.5(1) SU1, the RmCm subsystem will be out of service on the subscriber node. Disable and enable SRTP again to operate Unified CCX in SRTP-enabled mode.
- When SRTP is enabled in Unified CCX release 12.5(1) SU1, if you switch back to Unified CCX release 12.5(1), the RmCm subsystem will be out of service on both the nodes. Disable and enable SRTP again to operate Unified CCX in SRTP-enabled mode.

Preupgrade Tasks

Note All the nodes in a cluster must be on the same version. However, if you have upgraded only some nodes and want **Intelligence Center Reporting Service** available on the upgradednodes, do one of the following:

- Stop the **Intelligence Center Reporting Service** on all the nodes that aren't upgraded and then restart the upgraded nodes.
- Before the upgrade, change the cluster mode to UDP on all the nodes using the utils cuic cluster mode CLI command. After upgrading all the nodes, set the cluster mode to TCP. For more information, see the section in the Administration Console User Guide Cluster Configuration for JVM Using Hazelcast for Cisco Unified Intelligence Center.

Step 1 Obtain the pre-upgrade COP from https://software.cisco.com/download/home/270569179.

The following table lists the release versions and their corresponding COP files to upgrade to Release 12.5(1) SU2:

Table 2: Release Versions and COP Files for Unified CCX

Version	Release 12.5(1) SU2 Pre-Upgrade COP Name
11.6(2)	ciscouccx.1162.1251SU2PREUPGRADE.41.cop.sgn ucos.keymanagement.v01.cop.sgn
12.0(1)	ciscouccx.1201.1251SU2PREUPGRADE.3.cop.sgn ucos.keymanagement.v01.cop.sgn
12.5(1)	ciscouccx.1251.1251SU2PREUPGRADE.3.cop.sgn ucos.keymanagement.v01.cop.sgn

Version	Release 12.5(1) SU2 Pre-Upgrade COP Name
12.5(1) SU1	ciscouccx.1251.SU1.1251SU2PREUPGRADE.37.cop.sgn ucos.keymanagement.v02.cop.sgn

Table 3: Release Versions and COP Files for Customer Collaboration Platform

Version	Release 12.5(1) SU2 Pre-Upgrade COP Name
11.6(2)	ciscosm.keymanagement.cop.sgn ciscocvos.enable-sha512sum-signing-key-v1.0.cop
12.0(1)	ciscosm.keymanagement.cop.sgn ciscocvos.enable-sha512sum-signing-key-v1.0.cop
12.5(1)	ciscoccp.keymanagement.cop.sgn ciscocvos.enable-sha512sum-signing-key-v1.0.cop
12.5(1) SU1	ciscoccp.keymanagement.cop.sgn ciscocvos.enable-sha512sum-signing-key-v1.0.cop
12.5(1) SU2	ciscoccp.keymanagement.cop.sgn ciscocvos.enable-sha512sum-signing-key-v1.0.cop

Note There is no specific order you must follow while installing the pre-upgrade COP files.

You must install the COP files on both the publisher and the subscriber nodes. The changes take effect immediately after you install the pre-upgrade COP files. Reboot is not needed.

For information on installing COP files, see Apply COP File, on page 10.

Step 2 Obtain the ISO file from https://software.cisco.com/download/home/270569179.

Step 3 Create an ISO image of the upgrade file and place the ISO image on an FTP/SFTP server to which your server has access.

Step 4 Obtain the license file.

Note You require the license file only if you continue to use Classic Licensing.

Step 5 Back up all the existing data. For more information, see the *Cisco Unified Contact Center Express Admin and Operations Guide*.

Step 6 In the Unified CCX Administration, navigate to **Tools** > **Password Management**. Ensure that the passwords are same in both the nodes.

Step 7 Upload the Customer Collaboration Platform certificate to the Unified CCX Tomcat trust store using the Cisco Unified OS Administration interface. You can also use the **set cert import trust tomcat** CLI.

Step 8 Perform one of the following:

a) If the Cisco Unified Communications Manager (CUCM) cluster is using the self-signed certificate, upload the Tomcat certificates from all the nodes of the cluster to the Unified CCX Tomcat trust store. To upload certificates, use the Cisco Unified OS Administration interface (for example, `https://<uccx-hostname>/cmplatform`) or the **set cert import trust tomcat** CLI.

b) If the Cisco Unified Communications Manager (CUCM) cluster is using a CA-signed certificate, upload the root and the intermediate CA certificates to the Unified CCX Tomcat trust store.

Note

- For adding the UCCX certificate to the CUCM Phone trust store, refer to Finesse IP Phone Agent Certificate Management section in the Cisco Unified Contact Center Express Admin and Operations Guide.
- For information on using secure ports, refer to Finesse Port Utilization section in the Port Utilization Guide for Cisco Unified Contact Center Express Solution.
- The single button FIPPA service must be added to CUCM.

Step 9 Install the COP files. Refer to Step 1, on page 5 for the list of Unified CCX and Customer Collaboration Platform COP files and the corresponding releases.

For information about installing the COP files, see COP File, on page 9.

Note If you do not install these COP files, the upgrade fails.

Unified CCX Upgrade Scenarios

The following table lists the required tasks to upgrade a Single Node and a High Availability (HA) setup for Refresh Upgrade and Linux to Linux Upgrade types.

Note During Refresh Upgrade to Release 12.5.1 SU2, the `system-history.log` file may contain the following information, which can be ignored:

```
Switch Version 12.5.1.11002-XYZ to 12.0.1.10000-24 Aborted
```

Table 4: Upgrade Scenarios

Upgrade Scenario	Tasks
11.6.x/12.0/12.5(1)/12.5(1) SU1/12.5(1) SU2 to 12.5(1) SU3	Preupgrade Task Obtain the required preupgrade COP file from https://software.cisco.com/download/home/270569179. To know more about the preupgrade files needed for your release version, see Preupgrade Tasks, on page 5. Single Node Setup: 1. Upgrade Unified CCX Using Web Interface, on page 10 Or Upgrade Unified CCX Using CLI, on page 11 2. Verify Version of Unified CCX, on page 14 3. Verify Status of Services, on page 14

Upgrade Scenario	Tasks
	HA Setup: 1. Upgrade Unified CCX Using Web Interface, on page 10 or Upgrade Unified CCX Using CLI, on page 11. a. Upgrade the first node. Check all the services in the first Node from CLI and GUI and ensure that all the services are in Good/In_Service state. b. Upgrade the second node. 2. **Check and Perform Switch Version**. **Note** Check all the services in the first Node from CLI and GUI and ensure that all the services are in Good/In_Service state. a. Perform switch version on the first node. b. Perform switch version on the second node. **Note** After the switch version is complete on the second node, open the **Unified CCX Administration** page of the first node to check if the page is requesting for a license. Provide the license on the first node. 3. Verify Version of Unified CCX, on page 14 4. Verify Status of Services, on page 14 5. Verify Unified CCX Database Replication, on page 15

COP File

The COP file is the Cisco Options Package file. It is a compressed TAR file or an RPM file that has a `cop.sgn` file extension, and is signed by Cisco. COP files are installed on the active partition. You can apply the COP file using the CLI. The COP files for a specific release version can be downloaded from the location, Download Software. (For example, browse to **Unified Contact Center Express Upgrade Utilities** for a specific release version from the following location, **Products** > **Customer Collaboration** > **Contact Center Solutions** > **Unified Contact Center Express**).

Apply COP File

Attention See the documentation that is provided with the COP file for additional instructions on how to apply the COP file.

Attention Contact Cisco if you want to roll back the COP file.

Note For an HA setup, repeat this procedure for node 2 only after restarting node 1 after successful COP installation.

Before you begin

1. Place the COP file on an FTP/STFP server to which your server has access.

Step 1 Follow Steps 1 to 8 from Upgrade Unified CCX Using CLI, on page 11.

Step 2 Enter the command **utils system restart** to restart the server.

Upgrade Unified CCX Using Web Interface

You can upgrade Unified CCX either from a local DVD or from a FTP/SFTP server.

Step 1 Log in to **Cisco Unified OS Administration** using administrator username and password.

Step 2 Choose **Software Upgrades** > **Install/Upgrade**.

Step 3 Choose source as either **DVD/CD** or **Remote Filesystem** from the **Source** list.

Step 4 Enter the path of the upgrade file in the **Directory** field. For **Remote Filesystem**, enter a forward slash (/) followed by the directory path.

Step 5 If you chose **Remote Filesystem**, follow the instructions on the screen; otherwise, skip to **Step 6**.

Step 6 Click **Next** to see the list of upgrades that are available.

Step 7 Choose the appropriate upgrade file, and click **Next**.

Step 8 Enter relevant information in the **Email Destination** and **SMTP server** fields to use the Email Notification feature.

Step 9 Click **Next** to initiate the upgrade process.

Note After upgrading Unified CCX, the CAs that are not approved by Cisco are removed from the platform trust store. However, you can add them back, if necessary.

- For information about the list of CAs that Cisco supports, see Cisco Trusted External Root Bundle in https://www.cisco.com/security/pki.
- For information about adding a certificate, follow the procedure mentioned from step 5 under *Obtain and Upload CA Certificate* section in *Cisco Unified Contact Center Express Admin and Operations Guide*.

Upgrade Unified CCX Using CLI

Step 1 Log in to Cisco Unified OS Platform CLI using administrator username and password.

Step 2 Enter the command **show version active** and check the current version.

Step 3 Enter the command **utils system upgrade status** and check that the node is ready for upgrade.

Step 4 Enter the command **utils system upgrade initiate** to initiate the upgrade process.

Step 5 Choose the source where the upgrade file is placed.

Step 6 Follow the instructions on the screen.

Your entries are validated and the available files list is displayed.

Step 7 After the installation is complete, enter the **show version inactive** command to check the upgraded version.

Note If you enter **show version active** command during the upgrade process (by using an ISO image), it displays the version that is being upgraded to.

After upgrading Unified CCX, the CAs that are not approved by Cisco are removed from the platform trust store. However, you can add them back, if necessary.

- For information about the list of CAs that Cisco supports, see Cisco Trusted External Root Bundle in https://www.cisco.com/security/pki.
- For information about adding a certificate, follow the procedure mentioned from step 5 under *Obtain and Upload CA Certificate* section in *Cisco Unified Contact Center Express Admin and Operations Guide*.

Upgrade VMware Tools

Perform the below procedures to install and upgrade VMware tools for Unified CCX post Refresh Upgrade and prior to initiating Switch Version.

Upgrade VMware Tools using vSphere Client for Unified CCX

Step 1 Ensure you have powered on the virtual machine.

Step 2 Right-click the VM menu bar, choose **Guest** > **Install/Upgrade VMware tools**.

Step 3 Select the automatic tools update and click **OK**. It takes few minutes to complete. Once the update is complete, the tools are listed as Running (Current) on the VM's **Summary** tab in vSphere.

Note For more information about VMware ESXi's that are supported, refer to the *Virtualization for Cisco Unified Contact Center Express*.

Upgrade VMware Tools using CLI for Unified CCX

Step 1 Ensure you have powered on the virtual machine.

Step 2 Right-click the VM menu bar, choose **Guest** > **Install/Upgrade VMware tools**.

Step 3 Select the interactive tools update and click **OK**.

Step 4 Open the console and login at the command prompt.

Step 5 Enter the command **utils vmtools refresh** and confirm.
The server automatically reboots twice.

Step 6 After reboot, check the **Summary** tab for the VM to verify that the VMware tools version is current. If it is not current, reboot the VM and check the version again. It takes few minutes to complete. Once the process is complete, the tools are listed as Running (Current) on the VM's **Summary** tab in vSphere.

Upgrade VMware Tools using Windows guest OS for Unified CCX

Step 1 Ensure you have powered on the virtual machine.

Step 2 Right-click the VM menu bar, choose **Guest** > **Install/Upgrade VMware tools**. Click **OK** on the popup window.

Step 3 Login to the VM as a user with Administrative privileges.

Step 4 Run VMware tools from the DVD drive. The installation wizard starts.

Step 5 Follow the prompts in the wizard to complete the VMware Tools installation. Choose the Typical installation option.

Step 6 When the VM Tools installation finishes, restart the virtual machine for the changes to take effect. After the process is complete , the tools are listed as Running (Current) on the VM's **Summary** tab in vSphere.

Change NIC Adapter Type

Perform the below procedure post Refresh Upgrade and prior to initiating Switch Version.

Step 1 From **VMware VSphere**, select the **virtual machine** > **Edit Settings**. The Virtual Machine Properties window appears.

Step 2 To add the new Network Adapter, on the **Hardware** tab, click **Add**. The **Add Hardware** window appears.

Step 3 Select **Device Type** and **Ethernet Adapter**. Click **Next**. Choose the adapter type as **VXMNET3**. Click **Next** and **Finish**.

Step 4 To remove the existing Network Adapter 1, under the **Hardware** tab, select **Network Adapter 1**, click **Remove**, and select **OK**.

Step 5 Power on the virtual machine.

Check and Perform Switch Version

Caution **Never initiate switch version from the recovery CD.**

Note

- Perform switch version in the same maintenance window to avoid additional downtime.
- The time taken for switch version depends on the size of records in the database.
- Always ensure that all the third-party Wallboard server and WFM servers that query the Unified CCX database externally are powered off prior to the switch version process. These servers may cause conflict in database operations.
- Update the Unified CCX VM to latest OVA for 100 and 400 Agent profile for the switch version to be successful. This is mandatory as the vRAM required has been changed. For more information, see the Unified CCX Virtualization related information located at: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-contact-center-express.html.
- Do not modify the Hostname or IP address of the Unified CCX server before performing switch version.

Step 1 To check and perform switch version using the web interface:

a) Log in to **Cisco Unified OS Administration** using administrator username and password.
b) Choose **Settings** > **Version** to check the versions.
c) Click **Switch Versions**, and click **OK** to initiate the switch version process.
d) Choose **Settings** > **Version** to check the active version.

Step 2 To check and perform switch version using the CLI:

a) Log in to Cisco Unified OS Platform CLI using administrator username and password.
b) Enter the command **show version active** to check the active version.
c) Enter the command **show version inactive** to check the inactive version.
d) Enter the command **utils system switch-version** to initiate the switch version process.
e) Enter the command **show version active** to check the active version.

Step 3 If switch version is unsuccessful:

a) Log in to Cisco Unified OS Platform CLI using administrator username and password.
b) Enter the command **utils uccx switch-version db-check** to check if the database is corrupt.
c) Enter the command **utils uccx switch-version db-recover** to restore the database.

Verify Version of Unified CCX

You can verify the current active and inactive versions of Unified CCX either by using the web interface or using CLI.

Note For an HA setup, verify the versions on both the nodes.

Step 1 To verify the active and inactive versions of Unified CCX using the web interface:
a) Log in to **Cisco Unified OS Administration** using administrator username and password.
b) Choose **Settings** > **Version** to check the current active and inactive versions.

Step 2 To verify the active and inactive versions of Unified CCX using the CLI:
a) Log in to Cisco Unified OS Platform CLI using administrator username and password.
b) Enter the command **show version active** to check the active version.
c) Enter the command **show version inactive** to check the inactive version.

Verify Status of Services

Note For HA setup, verify the services on both the nodes.

Step 1 To verify the status of Customer Collaboration Platform:
a) After Unified CCX upgrade, log in to **Cisco Unified CCX Administration** using administrator username and password.
b) Choose **Subsystems** > **Chat and Email CCP Configuration**.
c) Click **Save** and verify that the **CCP Status** displays green for all the components.

Step 2 To verify the status of services using the web interface:
a) Log in to **Cisco Unified CCX Serviceability** using administrator username and password.
b) Choose **Tools** > **Control Center - Network Services** and verify that all the services are running.

Step 3 To verify the status of services using the CLI:
a) Log in to Cisco Unified OS Platform CLI using administrator username and password.

b) Enter the command **utils service list** to verify that all the services are running.

Verify Unified CCX Database Replication

Note For Cisco Finesse Desktop Failover to succeed, ensure the status of Cisco Database Replication is 'Good replication'.

Step 1 Log in to **Cisco Unified CCX Serviceability** using administrator username and password.

Step 2 Choose **Tools** > **Datastore Control Center** > **Replication Servers**.

Step 3 Ensure the servers are in ACTIVE/CONNECTED state and database replication of the operating system is functioning between the first node and the second node.

Step 4 If there is a problem with the replication continue; otherwise, skip to **Step 5**.

a) Log in to Unified CCX CLI using Unified CCX username and password.
b) Enter the command **utils uccx dbreplication status** and determine the location and cause of failure.
c) Enter the command **utils uccx dbreplication repair {all|database_name}** on the node or nodes to remove data discrepancy between the nodes.
d) Enter the command **utils uccx dbreplication status** to ensure the status is 'Good replication'. If failure persists, continue; otherwise, skip to **Step 5**.
e) Enter the command **utils uccx dbreplication teardown** to remove database replication.
f) Enter the command **utils uccx dbreplication setup** to setup database replication.
g) Enter the command **utils uccx dbreplication status** to ensure the status is 'Good replication'.

Step 5 Log in to **Unified CCX Administration** using Unified CCX username and password.

Step 6 Verify that your configuration data exists on both the nodes.

Verify Cisco Database Replication

Step 1 Run the Cisco Unified Real-Time Monitoring Tool (RTMT).

Step 2 Choose **System** > **Performance** > **Open Performance Monitoring**.

Step 3 Click the **Node1** or **Node2** radio button as required.

Step 4 Click the **Number of Replicates Created and State of Replication** radio button.

Step 5 Double-click **Replicate_State**.

Step 6 Choose **ReplicateCount**, and click **Add**.

The “Performance Counter” graph is displayed in the right window.

Step 7 Use the following list to monitor the status of database replication.

- 0—Initializing
- 1—Replication setup script fired from this node
- 2—Good replication
- 3—Bad replication
- 4—Replication setup did not succeed

Step 8 If there is a problem with the replication:

a) Log in to Cisco Unified OS Platform CLI using administrator username and password.
b) Enter the command **utils dbreplication status{all|node|replicate}** and determine the location and cause of failure.
c) Enter the command **utils dbreplication repair{nodename|all}** on the node or nodes to remove data discrepancy between the nodes.
d) Enter the command **utils dbreplication status** to ensure the status is 'Good replication'.

Upgrade Unified CCX Editor

Step 1 Uninstall the Unified CCX Editor.
Step 2 Log in to **Cisco Unified CCX Administration** using Unified CCX username and password.
Step 3 Choose **Tools** > **Plug-ins**.
Step 4 Click the **Cisco Unified CCX Editor Web Launcher** hyperlink.
Step 5 Download the Unified CCX Editor (.jnlp) file.

Launch Unified CCX Editor

Step 1 Log in to **Cisco Unified CCX Administration** using Unified CCX username and password.
Step 2 Choose **Tools** > **Plug-ins**.
Step 3 Click the **Cisco Unified CCX Editor Web Launcher** hyperlink to download and launch the Unified CCX Editor (.jnlp) file.

Install Unified CCX Real-Time Monitoring Tool

Step 1 Uninstall the previous version of Unified CCX Real-Time Monitoring Tool.
Step 2 Log in to **Cisco Unified CCX Administration** using Unified CCX username and password.

Step 3 Choose **Tools** > **Plug-ins**.

Step 4 Click **Cisco Unified Real-Time Monitoring Tool for Windows** or **Cisco Unified Real-Time Monitoring Tool for Linux** to download and install Unified Real-time Monitoring Tool.

Note
- The current Unified RTMT requires JRE to run. Verify that the system has JRE installed (Java 1.8).
- On a Linux workstation, run RTMT with root access. Otherwise, when you initially install RTMT, the application will not start.

Launch Unified CCX Real-Time Reporting Tool

Step 1 Log in to **Cisco Unified CCX Administration** using Unified CCX username and password.

Step 2 Choose **Tools** > **Plug-ins**.

Step 3 Click the **Cisco Unified CCX Real-Time Reporting Tool** hyperlink to download and launch the RTR (.jnlp) file.