Upgrade

Overview of the Upgrade Workflow

The upgrade process is evaluated by the HCS for CC deployment type you plan to upgrade. Follow the section in the table to plan for your upgrade from 11.0 or earlier to 11.6.

Current Deployment Type	Target Deployment Type	Upgrade Process
HCS for CC 500	HCS for CC 2000	Migration CC Upgrade
HCS for CC 1000	HCS for CC 2000	Migration CC Upgrade
HCS for CC 4000	HCS for CC 4000	Standard CC Upgrade
HCS for CC 12000	HCS for CC 12000	Standard CC Upgrade

Note

- All upgrades from 11.5 to 11.6 are Standard CC upgrades. However if you are upgrading from the 500 Agent deployment type (deprecated in 11.5(1) and removed and unsupported from 11.6(1)), use the Migration CC Upgrade procedure.
- The Small Contact Center (SCC) deployment uses the HCS for CC 4000 deployment type and follows same upgrade process.

Perform the Cisco HCS for Contact Center upgrade in the same sequence as the upgrade and validation steps are described in this document.

For more information, see *Cisco Hosted Collaboration Solution Documentation, Version 10.6 and 11.0*, https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html

The following upgrade paths are supported:

- Unified CCE 11.0 to 11.6
- Unified CCE 11.5 to 11.6
- Unified CCE 10.0 to 11.0 to 11.6
- Unified CCE 9.0 to 10.5 to 11.0 to 11.6.
- Unified CCE 9.0 to 10.0 to 11.0 to 11.6.

Upgrading Management Components

Upgrade HCM-F

Before you begin

Before upgrading a Cisco HCM-F application node, perform the following tasks.

- Create a valid DRF backup of your HCM-F.
- From the command-line interface on the application node, run **show hcs cluster nodes** to verify that the node is at the pre-upgrade version.
- Obtain the upgrade media for upgrading the HCM-F platform: upgrade disk or a downloaded executable file.

Procedure

Step 1 If you downloaded the executable file from Cisco.com, perform one of the following steps.

- Prepare to upgrade from a local folder.
  a. Copy the upgrade file to a temporary folder on a local hard drive.
  b. Open an SFTP client and connect to the HCM-F server using your adminsftp user ID and password.
  c. Run the **cd upgrade** command to navigate to the upgrade folder.
  d. Run the **put [upgrade file name]** command to transfer the file.
- Prepare to load an ISO file.
  a. Copy the upgrade ISO to a data store that is accessible by your virtual machine.
  b. Attach the ISO image to the CD/DVD drive of the virtual machine.
- Put the upgrade file on an FTP or SFTP server that is accessible by the virtual machine that you are upgrading.

Step 2 Copy the contents of the upgrade disk or downloaded files to the virtual machine that you are upgrading. Ensure that the upgrade filename begins with 'HCS.'

Step 3 On the virtual machine that you are upgrading, log in to the HCM-F command-line interface and run the **utils system upgrade initiate** command.

Step 4 Choose the source from which you want to upgrade.

- Remote file system via SFTP
- Remote file system via FTP
- Local DVD/CD
- Local Upload Directory

Step 5 Follow system prompts for the upgrade option you chose.
The system prompts you when the upgrade is complete.

Step 6 If you did not choose to automatically switch versions, run the **utils system switch-version** command. Enter **`yes`** to reboot the server and switch to the new software version.

Step 7 From the HCM-F command-line interface, run the **show version active** command to verify that the software version is the upgraded version.

Step 8 If you performed step 6, run the **utils service list** command to view services. Then run **utils service start [service name]** to restart any services that were stopped before the upgrade.

Validate the HCM-F Upgrade

Perform the following steps to validate the upgrade of Cisco HCM-F.

Procedure

Step 1 Verify that no error logs were created during or after the upgrade.

Step 2 Run the **show version active** command to verify that the active version is the upgraded version.

Step 3 Run the **utils service list** command to verify that all services are running as they were before the upgrade.

Step 4 Sign in to the administration interface and click the **About** link to verify that the interface displays the upgraded version.

Step 5 Verify that all synchronization is successful for Service Provider, Data Center, vCenter, Customer, and UCS Manager.

Step 6 Verify that Hosted License Manager does not contain post-upgrade errors. Also verify that licenses are assigned to the proper customers.

Step 7 Depending on which you used for the upgrade, ensure that Platform Manager or Prime Collaboration Deployment is running.

Step 8 Verify that Service Inventory is running.

Upgrade UCDM

Procedure

Step 1 Create a backup using the platform command-line interface. You can back up the cluster or back up each node individually.

Step 2 Turn off any scheduled imports.

Step 3 Check for running imports. Either wait for them to complete or cancel them.

Step 4 Upgrade multinode environment. See, *Upgrade a Multinode Environment* section in *Cisco Hosted Collaboration Solution Upgrade and Migration Guide* https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html

The *Cisco Unified Communications Domain Manager Planning and Install Guide* also contains installation instructions for multinode environments. You can find the guide on the **Component Documentation** tab here: https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-version-10-6-1/model.html.

Validate the Unified CDM Upgrade

Take the following steps to validate the upgrade of Unified CDM in a multinode or standalone environment.

Procedure

Step 1 Sign in to the user interface as hcsadmin, and click **About** > **Extended Version** to verify the upgrade.

Step 2 Reactivate the scheduled imports that you turned off before upgrading.

Step 3 Use the command-line interface on the primary node to run the **cluster status** command.
The command returns a list of clusters and their status.

Step 4 Attempt to associate a phone with a user:

a) In Unified CDM, navigate to **Subscriber Management** > **Phone** and add a phone.
b) Add a line to the phone.
c) Navigate to **Subscriber Management** > **Agent Line** and identify the new phone as an agent line.
d) In Unified CM, navigate to **User Management** > **Application User** and verify that the new phone is associated with pguser.

Upgrade Prime Collaboration Assurance

Cisco supports the upgrade to Cisco Prime Collaboration Assurance 11.6 or later version.

To upgrade Prime Collaboration Assurance, follow the steps in the "Overview of Data Migration Assistant" topic in the *Cisco Prime Collaboration Assurance and Analytics Install and Upgrade Guide* : https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-collaboration/products-installation-guides-list.html.

Note For downloading the Prime Collaboration patch, refer to the Dowload Software page. Navigate to **Products > Cloud and System Management > Collaboration and Unified Communications Management > Prime Collaboration**.

Validate the Upgrade of Prime Collaboration Assurance

Take the following steps to validate the upgrade of Prime Collaboration Assurance.

Validation consists of adding a Contact Center customer component and verifying that the component is in Managed state. In this example, we add the Customer Voice Portal component.

Procedure

Step 1 Sign in to HCM-F as an administrator.

Step 2 Add a cluster.

a) Navigate to **Cluster Management** > **Cluster** and click **Add New**.
b) Enter the cluster name.
c) Select the customer associated with the cluster.
d) Select **CC** as the cluster type.
e) Select the cluster application version.
f) In the **Application Monitoring the Cluster** field, select the hostname of the Prime Collaboration Assurance instance.
g) Click **Save**.

Step 3 Add the Customer Voice Portal component.

a) Navigate to **Application Management** > **Cluster Application**.
b) In the General Information section, complete the following steps:

- Click **Add New**.
- In the **Application Type** field, select **CVP**.
- Provide the hostname for the Customer Voice Portal component.
- Select the appropriate cluster.
- Click **Save**.

c) In the Credentials section, complete the following steps:

- Click **Add New**.
- In the **Credential Type** field, select **SNMP_V2**.
- Provide the community string for the Customer Voice Portal component.
- Select the **Read Only** access type.
- Click **Save**.

- Click **Add New**.
- In the **Credential Type** field, select **ADMIN**.
- Provide the administrator credentials. For Customer Voice Portal, the User ID is wsmadmin. Use the password that is configured for the OAMP web interface.
- Select the **Read Only** access type.
- Click **Save**.

d) In the Network Addresses section, complete the following steps:

- Click **Add New**.
- In the **Network Space** field, select **Application Space**.
- Provide the IPv4 address and the hostname.
- Click **Save**.
- Click **Add New**.
- In the **Network Space** field, select **Service Provider Space**.
- Provide the NAT IPv4 address and the hostname.
- Click **Save**.

Step 4 Navigate to the **Current Inventory** (Inventory > Inventory Management) page.
The **State** column shows the Customer Voice Portal as **Managed**.

Upgrade Unified CCDM

To upgrade Cisco Unified Contact Center Domain Manager, follow the installation steps in the *Installation and Configuration Guide for Cisco Unified Contact Center Domain Manager*: https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html.

Validate the Unified CCDM Upgrade

Take the following steps to verify the upgrade of Unified CCDM.

Verification Task	Success Criteria
Provisioning Tests for Unified CCE	
Log in to the side A web server (portal). Create a Skill Group to test the provisioning from the side A web server. Run this test for each configured Unified CCE instance.	You can successfully create the Skill Group, and it is visible on side A, and on side B if applicable.

Verification Task	Success Criteria
Log in to the side A web server (Portal). Create an Agent to test the provisioning from the side A web server. Run this test for each configured Unified CCE instance.	You can successfully create an Agent, and it is visible on side A, and on side B if applicable.
Create a Skill Group on the Administrative Workstation using the Cisco Skill Group Explorer tool. After a few minutes, verify that the Skill Group was imported into Unified CCDM.	The Skill Group is visible on side A, and on side B if applicable.
Replication Tests for Dual-Sided Deployments	
Log in to the side B web server (Portal). Create a Skill Group to test Unified CCE provisioning from the side B web server. Run this test for each configured Unified CCE instance.	You can successfully create the Skill Group, and it is visible on side A.
Create a Skill Group on the Administrative Workstation using the Cisco Skill Group Explorer tool. After a few minutes, verify that the Skill Group was imported into Unified CCDM.	The Skill Group is visible on side A and on side B.
Log in to the side B web server (Portal). Create an IP phone to test Unified CM provisioning from the side B web server.	The IP phone is visible on side A and on side B.

Standard CC Upgrade

Upgrading Unified Customer Voice Portal Components

Upgrade the Unified Customer Voice Portal

Follow these steps to upgrade Cisco Unified Customer Voice Portal.

Procedure

Step 1 Back up the Unified CVP Operations Console configuration.

Step 2 Install the upgrade software.
For more information, see the "Unified CVP Upgrade" chapter in the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html.

Validate the Customer Voice Portal Upgrade

Follow these steps to validate the upgrade of Cisco Unified Customer Voice Portal.

Procedure

Step 1 Log in to the Operations Console.
Step 2 Validate the version of each component.
Step 3 Verify that all services are running.
Step 4 Make a test inbound PSTN call to an agent.

Upgrading Gateway Components

Upgrade Gateway Components

Follow the steps to upgrade Cisco Unified Border Element (SP Edition), Cisco Unified Border Element (Enterprise Edition), or a virtual peripheral gateway (vPGW). For more information, see the following topics and guides:

- For upgrading Cisco Unified Border Element Enterprise see *Common Upgrade Tasks* section in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html
- Upgrade the IOS on the Cisco ASR 1006 for Cisco Unified Border Element (SP Edition), on page 9
- Upgrading the Cisco ASR 1000 Series Router for Cisco Unified Border Element (SP Edition), on page 8
- The *vPGW Documentation* guides on the **Component Documentation** tab: https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-version-10-6-1/model.html

Procedure

Step 1 Back up all the gateways.
Step 2 Use the gateway consoles to back up component configurations.
Step 3 Upgrade the gateways.

Upgrading the Cisco ASR 1000 Series Router for Cisco Unified Border Element (SP Edition)

Cisco Unified Border Element (SP Edition) is used as a demarcation between the Cisco HCS network and an outside network, such as IMS, PSTN, or other SIP network. The ASR 1000 Series router is connected to the aggregation switches at the aggregation layer.

To upgrade this component, follow the procedures in the *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*: https://www.cisco.com/c/en/us/support/routers/asr-1000-series-aggregation-services-routers/products-installation-and-configuration-guides-list.html.

When you have a redundant Cisco Unified Border Element (SP Edition) deployed, upgrade the component using the procedures in *Cisco Unified Border Element (SP Edition) Configuration Guide: Unified Model* :

https://www.cisco.com/c/en/us/support/routers/asr-1000-series-aggregation-services-routers/products-installation-and-configuration-guides-list.html.

To upgrade the ROMmon image on a Cisco ASR 1000 Series router, see the *Cisco ASR 1000 Series Routers ROMmon Upgrade Guide*: https://www.cisco.com/c/en/us/support/routers/asr-1000-series-aggregation-services-routers/products-maintenance-guides-list.html.

Upgrade the IOS on the Cisco ASR 1006 for Cisco Unified Border Element (SP Edition)

Use this procedure to upgrade Cisco Unified Border Element (SP Edition) ASR 1006 from version IOS 15.3(3)S to IOS 15.3(3)S4.

Before you begin

1. Ensure Cisco Unified Border Element (SP Edition) is configured for inter-chassis redundancy, with one Cisco ASR 1006 Aggregation Service Router in the Active state and the other in the Standby state.
2. Save the current configuration and download the software image to the boot flash of both of the ASR 1006 devices. It takes about 15 minutes.

Procedure

Step 1 Enter the CLI command **show redundancy application group <RG Group Id>** to determine which Session Border Controller (SBC) is Active. The Primary SBC is the Active chassis and the Secondary SBC is the Standby chassis.

Step 2 Download the new software version to the Primary and Secondary SBCs.

Step 3 On the Secondary SBC, enter the CLI command **boot system bootflash: <new image>** to change the boot variable to point to the new image.

Step 4 On the Primary SBC, perform an SBC sync from configuration mode. Enter the sbc configuration by executing CLI command **sbc <name of SBC>** and execute the CLI command **sync**.

Step 5 On the Secondary SBC, enter the CLI command **write memory** to save the running configuration.

Step 6 On the Primary SBC, enter the CLI command **redundancy > application redundancy > group # > shutdown** to shut down the redundancy group.
The Secondary SBC immediately becomes the Active Cisco Unified Border Element and all active calls are preserved. There is no service outage when the switchover of the Active SBC takes place.

Step 7 On the Primary SBC, change the boot variable to point to new software image and save the running configuration.

Step 8 Reload the Primary chassis for upgrade and wait for this SBC to come up with upgraded version.
It can take 10 to 12 minutes after the box is reloaded before the SBC reinitializes with the upgraded version.

Step 9 On the Secondary SBC, shut down the redundancy and immediately execute CLI command **no shutdown** of the redundancy group on the Primary SBC. Keep the duration between shutting down the redundancy group in the Secondary SBC and the **no shutdown** command in the Primary box as minimal as possible.
This step causes a service outage of approximately 4 minutes. The Primary box becomes the Active Cisco Unified Border Element (SP Edition) with upgraded software and starts servicing the calls.

Step 10 Save the running configuration in the Primary SBC.

Step 11 Reload the Secondary chassis for upgrade. When prompted to save the configuration before proceeding with the reload, enter “No” so that after the upgrade the Secondary SBC comes up in Standby mode.

Validate the Upgrade of Gateway Components

This section describes the steps to verify the upgrade of Cisco Unified Border Element (SP Edition), Metaswitch Perimeta Session Border Controller, Cisco Unified Border Element (Enterprise Edition), or a virtual peripheral gateway (vPGW).

Procedure

Step 1 Use Telnet or SSH to access the gateways and verify the version you upgraded to.

Step 2 Make an inbound call to an agent and verify the prompts. You can run the **debug voip dial peer** command to ensure that the inbound call uses the correct dial peer.

Upgrading the Unified Component

Upgrading the Unified Component

Follow the steps to upgrade the Cisco Unified Contact Center Enterprise Central Controller.

Unless otherwise indicated, the following steps reference topics in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Procedure

Step 1 Upgrade the Administration and Data server that is connected to Side A.
For more information, see the "Migrate HDS Database and Upgrade the Unified CCE Administration & Data Server" topic.

Step 2 Perform Enhancement of TempDB.

For more information, see the **Performance Enhancement of TempDB** section in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Step 3 Reduce the reserved unused space for HDS

For more information, see the **Reduce Reserved Unused Space for HDS** section in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Step 4 Bring the Side A logger and call router into service.
For more information, see the "Bring Upgraded Side A into Service" topic.

Step 5 Upgrade Cisco Unified Intelligence Center reporting templates.
For more information, see the *Installation and Upgrade Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html.

Step 6 Upgrade the Unified CCE Administration Client.
For more information, see the "Upgrade Unified CCE Administration Client" topic.

Step 7 Upgrade the gateways.
For more information, see the "Upgrade Peripheral Gateways" section in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Step 8 Upgrade the Outbound Option Dialer.
For more information, see the "Upgrade Outbound Option Dialer" section in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Step 9 Upgrade the CTI server.
For more information, see the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html

Upgrading Peripheral Gateways and Components

Upgrading Peripheral Gateways and Components

Follow the steps to upgrade Unified CCE peripheral gateways, such as agent or VRU peripheral gateways, and the associated components.

Procedure

Step 1 Upgrade the gateways.
For more information, see the "Upgrade Peripheral Gateways" section in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Step 2 Upgrade the Outbound Option Dialer.
For more information, see the "Upgrade Outbound Option Dialer" section in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Step 3 Upgrade the CTI server.
For more information, see the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Validate the Upgrade of Peripheral Gateways and Components

Take the following steps to validate the upgrade of your peripheral gateways and their components.

Procedure

Step 1 Validate Unified CCE processes.

a) Ensure that each software process is running according to specifications.
b) Verify that each NIC has the proper connection to the network carrier.

c) Stop and then restart each process.

Step 2 Launch queries against the upgraded Loggers to ensure the presence and integrity of historical call detail.

Step 3 Examine the reporting data from Cisco Unified Intelligent Contact Management.

Step 4 Use the Internet Script Editor to open and examine the most commonly monitored Unified ICM scripts.

Step 5 Set all Unified UCM services to start automatically.

a) On each Unified ICM component, double-click the local **Unified CCE Service Control** icon.
b) Set each ICM service to **Automatic Start**.

Step 6 In the Internet Script Editor, navigate to **Script** > **Validate All** to ensure that all scripts are running properly.

Upgrading Reporting Components

Upgrade Cisco Unified Intelligence Center

To upgrade Cisco Unified Intelligence Center, see the *Installation and Upgrade Guide for Cisco Unified Intelligence Center*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html.

Validate the Upgrade of Unified Intelligence Center

Take the following steps to validate the upgrade of Cisco Unified Intelligence Center.

Procedure

Step 1 Open the Unified OS Administration web page at the following URL, where [server-name] is the hostname or IP address of the node: `https://[server-name]/cmplatform`.

Step 2 Sign in with administrator credentials.

Step 3 Navigate to **Settings** > **Version** and verify the software version on the active and inactive partitions.

Upgrading Desktop Components

Upgrade Finesse

To upgrade Cisco Finesse, see the *Cisco Finesse Installation and Upgrade Guide*: https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html.

Note ES65 provides the ability to connect a maximum of two versions of Finesse to the same PG during the upgrade or migration process to facilitate the migration of agentsand supervisors to the new Finesse version. However, this mode of operation isnot supported for production use beyond the upgrade or migration phase.

Validate the Finesse Upgrade

Take the following steps to validate the upgrade of Cisco Finesse.

Procedure

Step 1 Ensure that the version of Finesse is the version you upgraded to. From the command line interface, you can run the **show status** command to verify the version.

Step 2 In the Finesse console, verify that all services are up.

Step 3 Log in to an agent and run desktop-initiated tests such as Call Hold, Transfer, and Conference.

Upgrade Desktop Clients

(Optional). To upgrade CTI OS Agent and Supervisor desktops, see the *CTI OS System Manager Guide for Cisco Unified ICM/Contact Center Enterprise*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Validate the Upgrade of Desktop Clients

Take the following steps to validate the upgrade of CTI OS Agent and Supervisor desktops.

Procedure

Step 1 Validate the version of each desktop.

Step 2 Sign in to an agent and run desktop-initiated tests such as Call Hold, Transfer, and Conference.

Upgrading Recording Components

Upgrade MediaSense

To upgrade MediaSense, see the *Installation and Administration Guide for Cisco MediaSense*: https://www.cisco.com/c/en/us/support/customer-collaboration/mediasense/products-installation-guides-list.html.

Upgrading Call-Processing Components

Upgrading Cisco Virtualized Voice Browser Components

Upgrade Cisco Virtualized Voice Browser

To upgrade the Cisco Virtualized Voice Browser, follow the steps in the "Cisco Virtualized Voice Browser Upgrade" chapter in the *Installation and Upgrade Guide for Cisco Virtualized Voice Browser Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/products-installation-guides-list.html

Validate the Cisco Virtualized Voice Browser Upgrade

Follow these steps to validate the upgrade of Cisco Virtualized Voice Browser portal.

Procedure

Step 1 Log into Cisco Virtualized Voice Browser portal.

Step 2 Check the existing configuration.

Upgrade Cisco Unified Communications Manager

Take the following steps to upgrade Cisco Unified Communications Manager.

Procedure

Step 1 Upgrade Cisco Unified CM.
For more information, see the *Upgrade Guide for Cisco Unified Communications Manager*: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.

Step 2 Uninstall and then reinstall the JTAPI client on the Cisco Unified CM peripheral gateway.
For more information, see the "Upgrade Cisco JTAPI Client on the Unified Communications Manager PG" topic in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*: https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Validate the Upgrade of Cisco Unified Communications Manager

Take the following steps to validate the upgrade of Cisco Unified Communications Manager.

Procedure

Step 1 In Cisco Unified CDM, add an IP phone. For more information, see the *Cisco Hosted Collaboration Solution End-User Provisioning Guide*: https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-hcs/tsd-products-support-series-home.html.

Step 2 In Cisco Unified CM, verify that the phone was added.

Migration CC Upgrade

Migration to 2000 Agents Deployment Model

Common Ground Migration Process

The migration process for HCS for CC 500 and 1000 to 2000 agents deployment is designed for minimal Contact Center downtime. While you are upgrading Side A, Side B remains operational. After you upgrade Side A, contact center activity resumes on Side A while you upgrade Side B.

In Release 11.0(1), CS for CC 500 and 1000 agents deployment is moving to a new deployment model (HCS for CC: 2000 Agents). In release 11.5(1), HCS for CC 500 (deprecated in 11.5 and removed and unsupported from 11.6) is moving to a new deployment model (HCS for CC: 2000 Agents).The upgrade process also includes steps to migrate to this new model.

The layout of the VMs on the hardware changes as shown in the following diagram.

Things to note include the following:

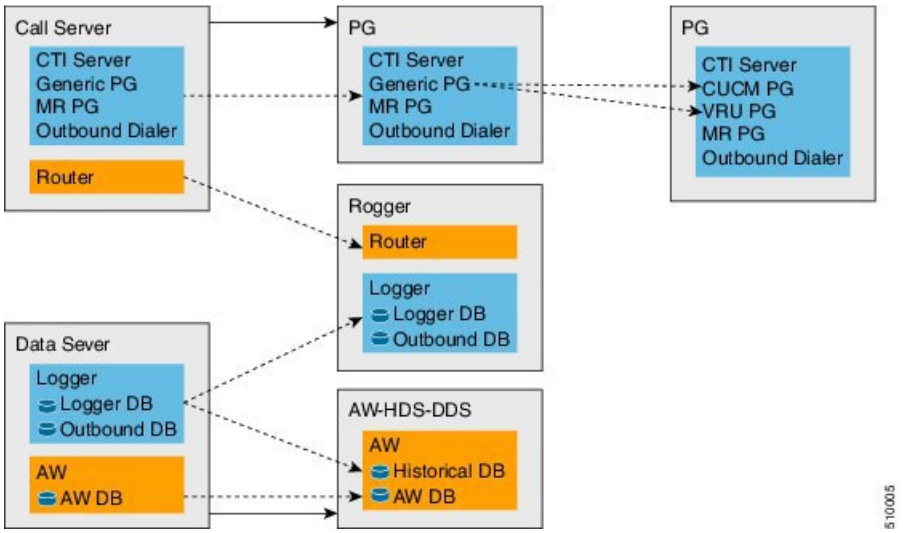
- The on-box Unified CCE Call Server and Data Server VMs change to on-box Unified CCE Rogger, PG, and AW-HDS-DDS.
- Two Unified CVP Servers are replaced with one Unified CVP Server that can support up to 3000 ports.
- Enterprise Chat and Email (ECE) can be coresident on box or deployed off box.

Note

- On-box ECE is supported on the B200 M4 and C240 M4 hardware only.
- On-box ECE is not supported in 2000 agent deployment model for two 500 agent instances in single pair of server

When you migrate to the HCS for CC 2000 Agent model, the Unified CCE Call Server and Data Server are migrated as shown in the following diagram.

Figure 1: HCS for CC Migration



Important The upgrade requires four maintenance windows:

- One maintenance window to shut down services on Side A to prepare for upgrade.
- A second maintenance window in the middle of the upgrade to cut over from Side B to Side A. You must bring down Side B before you bring up Side A.
- A third maintenance window after you upgrade Side B to synchronize Side A to Side B.
- A fourth maintenance window to finish migrating the Unified CCE Call Server to a Unified CCE PG.

This guide steps you through the upgrade and migration process for HCS for CC 2000 agents deployment, which includes the following major tasks:

- Meeting the system requirements for upgrade.
- Performing preupgrade tasks.
- Installing the Unified CCE Rogger.
- Migrating the Unified CCE Data Server to a Unified CCE AW-HDS-DDS.
- Migrating the Unified CCE Call Server to a Unified CCE PG.
- Upgrading all components on Side A.
- Cutting over from Side A to Side B, during which you bring Side B down and then bring Side A up.
- Migrating and upgrading all components on Side B.
- Synchronizing Side A and Side B.
- Performing postupgrade procedures.

Prerequisites and Important Considerations

- If your deployment includes Cisco Unified WIM and EIM, you must shut it down during the upgrade. Enterprise Chat and Email replaces Unified WIM and EIM in Release 11.6(1). Unified WIM and EIM is not supported from HCS for CC 11.5(1) onwards. After the upgrade is complete, you can install Enterprise Chat and Email.
- Live Data does not work during the migration and upgrade.
- Make sure that you have backups of Side A and Side B Call Servers, Data Servers, and Unified CVP Servers before you begin your upgrade.
- Use the Disaster Recover System (DRS) application to back up Finesse and Unified Intelligence Center system data.
  - Finesse: To access the DRS application, direct your browser to `https://FQDN of Finesse server:8443/drf/`. For more information, see the online help provided with the DRS application.
  - Unified Intelligence Center: To access the DRS application, direct your browser to `https://IP address of Unified Intelligence Center:8443/drf`. For more information, see the online help provided with the DRS application.
- After you begin the migration and upgrade process, you cannot back out of it. If you want to go back to the previous release, you must restore your VMs from your backup.
- Optionally, you can stage the Unified CCE Rogger off box before you begin the migration and upgrade to lessen your downtime.
- Plan out your hostnames. You may want to change the hostnames of the migrated Unified CCE components (Unified CCE Call Server, which becomes the Unified CCE PG, and Unified CCE Data Server, which becomes the Unified AW-HDS-DDS). If you change these hostnames, you must update them in other places (such as Finesse, PG Setup, and private network DNS entries).
- Make sure that you are running the minimum supported version of ESXi. For information about supported ESXi versions, see the *Virtualization for Cisco HCS for Contact Center* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/hcs_cc_virt.html.

Supported Upgrade

You can upgrade to this HCS for CC release from any version of HCS for CC Release 11.0(x).

Before you upgrade HCS for CC, you must upgrade on-box or off-box Unified Communication Manager Publisher and Subscribers to a version supported by this release of HCS for CC.

For information about supported versions, see the *HCS for CC Compatibility Information* at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-device-support-tables-list.html.

Note HCS for Contact Center 11.6(1) release, supports CUCM 11.5(1).

Hardware Refresh with Common Ground Upgrade

If you are performing a hardware refresh as part of the upgrade process, you must first prepare the target servers:

- Prepare Customer Site Servers
- *Virtualization for Cisco HCS for Contact Center* at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/hcs_cc_virt.html

After you configure the servers, you can move the VMs to the servers and complete the common ground upgrade process.

NTP Configuration Requirements

HCS for Contact Center relies on time synchronization. Properly configuring NTP is critical for reliability of reporting data and cross-component communication. It's important to implement the requirements outlined in NTP and Time Synchronization.

Preupgrade Tasks

Perform the tasks in the following table in the order that they are listed.

Important You must perform the tasks **in the order that they are listed in this table**. Some tasks link to procedures in other parts of the guide. When you reach the end of a procedure, refer back to this table to determine what you must do next. **Failure to perform upgrade tasks in the order listed in this table can cause the upgrade to fail**.

Step	Task
1.	In the Unified CCE Administration **System Inventory** tool, check the status of the alerts for the hosts and for each virtual machine (VM). Resolve any issues. Make sure that inventory alerts are at 0 before you continue.
2.	Shut down Enterprise Chat and Email (ECE).
Reduce the impact of Side A services shutdown. Stopping Side A services to upgrade the components may force agents to sign out of their desktops and cause IP phones to rehome. If customers require agents to be active during the upgrade, you can reduce the impact of Side A shutdown by completing these preupgrade tasks.	

Step	Task
3.	Force phones to rehome to the Side B Unified Communications Manager Subscriber. Perform this step if the device pool for the agent phones contains only the Side A Unified Communications Manager Subscriber 1. In Unified Communications Manager Administration, add the Side B Unified Communications Manager Subscriber 2 as preferred and change the Subscriber 1 to secondary. Reset the phones after you change the device pool. You can skip this step if the device pool for the agent phones is configured with the Side A Unified Communications Manager Subscriber 1 as preferred and the Side B Unified Communications Manager Subscriber 2 as secondary. When you shut down Side A, Unified Communications Manager forces logout for agents using phones logged in to Subscriber 1 and rehomes their phones to Subscriber 2.
4.	Direct agents to sign in to the Side B Finesse Secondary node.
5.	Configure the Cisco IOS Enterprise Ingress Voice Gateway dial-peer priority so that calls are sent to the Side B Unified CVP Servers first, and then to the Side A Unified CVP Servers.
6.	To maintain reporting capabilities during the Side A upgrade, configure Unified Intelligence Center historical and real-time data sources to one of the following: • Side B Unified CCE Data Server • External HDS with Side B as the Central Controller preferred side See Configure Unified Intelligence Center Data Sources for External AW-HDS-DDSHDS, on page 20 for steps to configure Unified Intelligence Center data sources. For the **Datasource Host** and **Database Name** fields, enter values for the Side B Unified CCE Data Server with Side B as the Central Controller preferred side.
Complete Finesse preupgrade tasks	
7.	Save your current desktop layout configuration. Sign in to Finesse Administration on the primary Finesse node (`https://FQDN of primary Finesse server/cfadmin`). Copy the layout XML file from the Manage Desktop Layout gadget on the **Desktop Settings** tab. Save it as a text file on your local system. **Note** If you are currently running the default layout, the layout automatically upgrades to the new layout. To use the layout from the previous version, copy and paste the layout XML to the Manage Desktop Layout gadget after the upgrade is complete.
Complete Unified CVP preupgrade tasks	
8.	Complete the pre-upgrade tasks on Side A and Side B Unified CVP Servers and Operations Console Server. See Unified CVP Preupgrade Tasks, on page 21.
Complete Unified Communications Manager preupgrade tasks	
9.	Complete Unified Communications Manager preupgrade tasks. See Unified Communications Manager Preupgrade Tasks, on page 21.

Configure Unified Intelligence Center Data Sources for External AW-HDS-DDSHDS

Perform this procedure only if your deployment includes an external AW-HDS-DDS.

Before you begin

Configure the Unified Intelligence Center SQL user for the External AW-HDS-DDSHDS databases before configuring the data sources (applicable for 4000 Agents and 12000 Agents). For more information, see Configure Unified Intelligence Center SQL User Account on the External AW-HDS-DDS, on page 20

Procedure

Step 1 Sign in to Unified Intelligence Center with your Cisco Intelligence Center administrator account (https://<hostname/ IP address of CUIC Publisher>:8444/cuicui).

Step 2 Click **Data Sources** in the left panel.

Step 3 Select the **UCCE Historical** data source. Click **Edit**.

a) In the **Datasource Host** field, enter the IP Address of the external AW-HDS-DDS server.
b) In the **Port** field, enter **`1433`**.
c) In the **Database Name** field, enter **`{instance}_hds`**.
d) Leave the **Instance** field blank.
e) Select the **Timezone**.
f) In the **Database User ID**, enter the user name that you configured for the Cisco Unified Intelligence Center SQL Server user account.
g) Enter and confirm the SQL Server User **password**.
h) Select the **Charset** based on the collation of SQL Server installation.
i) Click **Test Connection**.
j) Click **Save**.

Step 4 Click the **Secondary** tab to configure Unified CCE Historical Data Source.

a) Check the **Failover Enabled** checkbox.
b) In the **Datasource Host** field, enter the IP address of the second external AW-HDS-DDS server.
c) In the **Port** field, enter **`1433`**.
d) In the **Database Name** field, enter **`{instance}_hds`**.
e) Complete other fields as in the Primary tab.
f) Click **Test Connection**.
g) Click **Save**.

Step 5 Repeat this procedure for the **UCCE Realtime** datasource .

The **Database Name** for the Realtime Data Source is **`{instance}_hds`** .

Configure Unified Intelligence Center SQL User Account on the External AW-HDS-DDS

Procedure

Step 1 Launch Microsoft SQL Server Management Studio .

Step 2 Navigate to **Security** >**Logins**, right-click **Logins** and select **New Login**.

This login is used when you configure the data sources for Cisco Unified Intelligence Center reporting.

Step 3 On the General Screen:

a) Enter the Login Name.
b) Select **SQL Server authentication**.
c) Enter and confirm the Password.
d) Uncheck **Enforce password policy**.

Step 4 Click **User Mapping**.

a) Check the databases associated with the AWdb.
b) Choose each database and associate it with the **db_datareader** and **public** role, and click **OK**.

Step 5 Click **OK**.

Unified CVP Preupgrade Tasks

Unified CVP Server and Unified CVP OAMP Server Preupgrade Tasks

Procedure

Step 1 Close all programs.

Step 2 Stop any third-party services and applications that are running on the server.

Step 3 Back up the `C:\Cisco\CVP` folder for all Unified CVP Servers.

Step 4 Back up the Operations Console as follows:

a) Log in to Operations Console.
b) On the Operations Console page, click **System** > **Export System Configuration** > **Export**, and save the CVP-OpsConsole-Backup.zip file.
c) Manually copy the sip.properties file from the directory `<CVP_HOME>\conf`. (Unified CVP Operations Console cannot export the sip.properties file.)
d) Copy the exported configuration and custom files onto network storage media or a portable storage media.

Unified Communications Manager Preupgrade Tasks

Procedure

Step 1 Ensure that you have the necessary license files for the new release.

Step 2 Back up your system. For more information, see the *Administration Guide for Cisco Unified Communications Manager* at this address: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Step 3 Obtain the upgrade file from Cisco.com and save it to an FTP or SFTP server. Folder names and filenames that you enter to access the upgrade file are case-sensitive. For more information, see the *Release Notes for*

Cisco Unified Communications Manager at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html

Prepare Side A for Upgrade

Before you begin, complete all tasks listed in Preupgrade Tasks, on page 18.

The user account that performs the upgrade must have access to PG Explorer and Network Trunk Group Explorer in Configuration Manager. Use the User List tool in Configuration Manager to provide access. For more information, see the Configuration Guide for Cisco Unified ICM/Contact Center Enterprise at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Perform the tasks in the following table during a maintenance window and in the order they are listed.

Important Make sure that you have backups of all components before you proceed.

Step	Task
1.	Sign in to Unified CCE Administration on the Side A Unified CCE Data Server. Select **System** > **Deployment**. **Note** When you sign in to Unified CCE Administration, a screen appears that contains warnings about virtual machine mismatches. You can ignore these warnings and close the screen. Switch out of the HCS for Contact Center 500 or HCS for Contact Center 1000 deployment model and into **UCCE 4000 Agents Rogger**.
2.	Disable configuration changes. Set the following registry key to **1** on the Side A Unified CCE Call Server: `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\RouterA\Router\CurrentVersion\Configuration\Global\DBMaintenance` The change is replicated to the other side automatically.
3.	On each of the following VMs, select **Unified CCE Service Control** on the desktop. Stop the Unified CCE services and change **Startup** to **Manual**: • Side A Unified CCE Call Server • Side A Unified CCE Data Server • External HDS associated with Side A (if used)
4.	If Outbound Option is used, on the Side B Unified CCE Call Server, select **Unified CCE Service Control** on the desktop. Stop the Dialer service and change **Startup** to **Manual**.

Migrate and Upgrade Side A

Before you begin, check the following to confirm that call activity has ended on Side A:

- In Unified CVP Diagnostic Portal, check that no Side A ports are in use.
- In the Unified Communications Manager RTMT tool, check that phones have migrated to Side B.

Important You must perform the tasks **in the order that they are listed in this table**. Some tasks link to procedures in other parts of the guide. When you reach the end of a procedure, refer back to this table to determine what you must do next. **Failure to perform upgrade tasks in the order listed in this table can cause the upgrade to fail**.

For best results, place upgrade media ISOs on local data stores. Make sure to remove them when the upgrade is complete.

Step	Task
Upgrade the Side A Unified CVP VMs	
1.	Remove the Unified CVP Server 2A VM.
2.	Update the Cisco IOS Enterprise Ingress Voice Gateway dial-peer configuration to remove Unified CVP Server 2A.
3.	Upgrade Unified CVP Server 1A. See Upgrade the Unified Customer Voice Portal, on page 7.
4.	Validate the Unified CVP upgrade. See Validate the Customer Voice Portal Upgrade, on page 7
Upgrade Side A Cisco Voice Gateway IOS Version if needed	
5.	Upgrade the Side A Cisco Voice Gateway IOS version to the minimum required by the upgraded HCS for CC release (or later). See Upgrade Cisco Voice Gateway IOS Version, on page 27. See the *HCS for CC Compatibility Information* at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-device-support-tables-list.html.
Upgrade the Side A Finesse and Unified Intelligence Center VMs	
6.	Upgrade the VMware version on the Finesse Primary VM. See Upgrade the Virtual Machine Hardware Version, on page 28.
7.	Update the settings on the Finesse Primary VM. See Update VMware Settings for Cisco Finesse, on page 28.
8.	Upgrade the Finesse Primary node. See Upgrade Finesse, on page 12

Step	Task
9.	Upgrade the VMware version on the Unified Intelligence Center Publisher VM. See Upgrade the Virtual Machine Hardware Version, on page 28.
10.	Update the settings on the Unified Intelligence Center Publisher VM. See Update VMware Settings for Cisco Unified Intelligence Center, on page 28.
11.	Upgrade the Unified Intelligence Center Publisher node. See Upgrade Cisco Unified Intelligence Center, on page 12
Prepare for Side A Migration to HCS for CC 2000 Agent Rogger Deployment	
12.	Back up and export the Logger database and the Outbound Option (if used). See Back Up Database, on page 30.
13.	Back up and export your network configuration. See Back Up Network Configuration, on page 30.
Install the Side A Unified CCE Rogger (if not previously staged off box)	
14.	Create a VM for the Side A Unified CCE Rogger. Select **Rogger** from the drop-down list.
15.	Install Microsoft Windows Server on the Side A Unified CCE Rogger VM.
16.	Install VMware tools on the Side A Unified CCE Rogger VM.
17.	Configure the network adapters for the Side A Unified CCE Rogger. See Configure Network Adapters for Unified CCE Call Server and Unified CCE Data Server, on page 42 .
18.	Install antivirus software on the Side A Unified CCE Rogger.
19.	Configure the database drive for the Side A Unified CCE Rogger. See Configure Database Drive, on page 43.
20.	Set persistent static routes. See Set Persistent Static Routes, on page 44.
21.	Run Windows updates. See Run Windows Updates, on page 44.
22.	Add the Unified CCE Rogger to the domain.
23.	Install Microsoft SQL Server.
24.	Install Cisco Unified Contact Center Enterprise.
Configure the Side A Unified CCE Rogger	

Step	Task
25.	Add a UCCE Instance in Web Setup. See Add a UCCE Instance, on page 31.
26.	Configure SQL Server for the Logger database on the Unified CCE Rogger. See Configure SQL Server for CCE Components, on page 45.
27.	Configure the Logger database and log. See Configure the Logger Database and Log, on page 31.
28.	Import the Logger and Outbound Option databases that you backed up and exported in step 24. See Import the Logger and Outbound Databases, on page 32.
29.	Setup two-way replication between the Outbound Option database on Logger Side A and the Outbound Option database on Logger Side B. See Two-Way Outbound Option Database Replication, on page 34
30.	Add a Unified CCE Router component in Web Setup. See Add a Unified CCE Router Component, on page 35.
31.	Add a Unified CCE Logger component in Web Setup. See Add a Unified CCE Logger Component, on page 35.
Convert the Side A Unified CCE Data Server and Unified CCE Call Server	
32.	Upgrade the VMware version on the Side A Data Server VM. See Upgrade the Virtual Machine Hardware Version, on page 28.
33.	Update the settings on the Side A Data Server VM. See Update VMware Settings on the Unified CCE Data Server, on page 36.
34.	Convert the Side A Unified CCE Data Server to a Unified CCE AW-HDS-DDS. See Convert Unified CCE Data Server to Unified CCE AW-HDS-DDS, on page 37.
35.	Update the real-time and historical data sources for Unified Intelligence Center to point to the Unified CCE AW-HDS-DDS. You must update the historical data source database name from <*instancename*>_sideA to <*instancename*>_awdb.
36.	Upgrade the VMware version on the Side A Call Server VM. See Upgrade the Virtual Machine Hardware Version, on page 28.
37.	Update the settings on the Side A Call Server VM. See Update VMware Settings on the Unified CCE Call Server, on page 38.

Step	Task
38.	Remove the Router from the Side A Unified CCE Call Server. See Remove the Router from the Unified CCE Call Server, on page 39. **Note** If CTI OS Server is present, use `\icm\CTIOS_bin\SETUP.exe` to remove it also. CTI OS is no longer supported. The Call Server is now a PG.
40.	Disable configuration changes on the Unified CCE Rogger. Change the following registry key to 1: `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\RouterA\Router\CurrentVersion\Configuration\Global\DBMaintenance`
41.	Run the Unified CCE Release 11.6(1) installer on the Side A Unified CCE AW-HDS-DDS (former Data Server). See Upgrade to Release 11.6(1), on page 45.
43.	Modify the Side A PG to point to the Unified CCE Rogger. See Modify the PG, on page 39.
44.	Modify the dialer to point to the Unified CCE Rogger (if using Outbound Option). See Modify the Dialer, on page 39.
Optional: Upgrade the External HDS associated with Side A (if used)	
45.	Upgrade the VMware version on the External HDS associated with Side A. See Upgrade the Virtual Machine Hardware Version, on page 28.
46.	Run the Unified CCE Release 11.6(1) installer the External HDS associated with Side A. See Upgrade to Release 11.6(1), on page 45.
47.	Update the Central Controller connectivity to point to the Unified CCE Rogger. See Update the Central Controller Connectivity, on page 40.
Optional: Install language pack	
48.	Install the language pack on the Side A Unified CCE Rogger, AW-HDS-DDS (former Data Server), PG (former Call Server), and External HDS associated with Side A (if used). See Install the Language Pack, on page 40.
Upgrade the Side A Unified Communications Manager Publisher and Subscriber 1	
49.	Upgrade the Side A Unified Communications Manager Publisher. See Upgrade Cisco Unified Communications Manager, on page 14
Optional: Change hostnames of the Unified CCE components	

Step	Task
50.	Optional: Change the hostnames of the Unified CCE components (AW-HDS-DDS and PG). **Note** You can perform this task when you reboot each component as part of the upgrade. If you do change the hostnames, also change them in the following places: • Cisco Finesse • PG Setup • Unified Intelligence Center - Historical and real-time • Private network DNS entries • Live Data—If you change the hostname of the AW-HDS-DDS (former Data Server), Live Data no longer connects to the AW-HDS-DDS after the Data Server hostname is removed from DNS. To fix this, do the following: 1. Run the following CLI command on the CUIC-LD-IdS Publisher: **unset live-data aw-access primary** 2. Restart Cisco Tomcat on the Side A AW-HDS-DDS.

Cisco Enterprise Voice Gateway Upgrade Procedures

Upgrade Cisco Voice Gateway IOS Version

Perform this procedure for each gateway.

For more information, see https://www.cisco.com/c/en/us/td/docs/routers/access/1900/software/configuration/guide/Software_Configuration/upgrade.pdf.

Upgrade the Cisco Voice Gateway IOS version to the minimum version required by HCS for CC (or later). See the *HCS for CC Compatibility Information* at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-device-support-tables-list.html.

Procedure

Step 1 Copy the new image from the remote TFTP server into flash memory, making sure that you specify your own TFTP server's IP address and Cisco IOS filename.

Step 2 Verify that the new image was downloaded.

Step 3 Boot using the new image. Update the gateway config to boot using the new version.

Step 4 Reload the gateway to use the new image.

Common Software Upgrade Procedures

Upgrade the Virtual Machine Hardware Version

Perform the following procedure on the VSphere Web Client on the Finesse and Unified Intelligence Center VMs.

Procedure

Step 1 Shut down the virtual machine.

Step 2 Right-click the virtual machine and choose **Compatibility > Upgrade VM Compatibility**.

Step 3 Click **Yes** to confirm upgrade.

Step 4 From the **Compatible with (*)** drop-down list, choose **ESXi 5.1 and later**.

Step 5 Click **OK** to save the settings.

Step 6 Power on the virtual machine.

Update VMware Settings for Cisco Finesse

Update the virtual machine settings for the Finesse Primary and Finesse Secondary VMs to match the OVA file.

Procedure

Step 1 Use the following CLI command to shut down the virtual machine: **utils system shutdown**

Step 2 Right-click the virtual machine and choose **Edit Settings**.

Step 3 Click the **Hardware** tab.

a) Click **Memory** and update the **Memory Size** to 10 GB.

Step 4 Click the **Resources** tab.

a) Click **CPU** and update the **Reservation** field to 5000 MHz.

b) Click **Memory** and update the **Reservation** field to 10240 MB.

Step 5 Click **OK**.

Step 6 Power on the virtual machine.

Update VMware Settings for Cisco Unified Intelligence Center

Update the settings on the Unified Intelligence Center Publisher and Subscriber to match the 11.5(1) OVA file.

Update the settings on the Unified Intelligence Center Publisher and Subscriber to match the OVA file.

Procedure

Step 1 Use the following CLI command to shut down the virtual machine: **utils system shutdown**

Step 2 Right-click the virtual machine and choose **Edit Settings**.

Step 3 Click the **Hardware** tab.

a) Select the hard disk to modify. In the **Disk Provisioning** pane, change the **Provisioned Size** to 200 GB.
b) Click **Memory** and update the **Memory Size** to 16 GB.

Note If you deploy two 500 agent instances in single pair of blade then update the **Memory Size** to 10GB

Step 4 Click the **Resources** tab.

a) Click **CPU** and update the **Reservation** field to 5500 MHz.
b) Click **Memory** and update the **Reservation** field to 16384 MB.

Step 5 Click **OK** to save your changes.

Step 6 Power on the virtual machine.

Upgrade VOS-Based Contact Center Applications from a Remote File System

Finesse and Unified Intelligence Center 11.0 support aligned partitions, but only with a fresh installation. When you upgrade from a previous release, the platform detects the unaligned partitions and displays the following error: `ERROR-UNSUPPORTED: Partitions unaligned`.

You can run Finesse and Unified Intelligence Center with the unaligned partitions without functional impact. To experience the benefits of aligned partitions, you must you perform a fresh installation after upgrade.

Procedure

Step 1 Upgrade VMware Settings

Before you perform an upgrade to 11.x, modify the following virtual machine settings (Red Hat Enterprise Linux version, Network Adapter, Memory and Video Card) as follows:

a) Power down the virtual machine.
b) From **VMWare VSphere**, select the virtual machine > **Edit Settings**. The Virtual Machine Properties window appears.
c) In the **Options** tab, select **General Options** and update the **Guest Operating System** from Red Hat Enterprise Linux 4(32-bit) to Red Hat Enterprise Linux 6(64-bit). Click **OK**.
d) Again select the virtual machine > **Edit Settings**.
e) In the **Hardware** tab, update the following parameters:

Memory > **Memory Size** > **10GB**.

Video Card > **Total Video Memory** > **8MB**.

f) Power on the virtual machine and continue with the upgrade.

Step 2 SSH to your Finesse, Unified Intelligence Center, or Unified Communications Manager system, or open it in the VM console in VSphere.

Step 3 Log in with the platform administration account.

Step 4 From the CLI, run the command **utils system upgrade initiate**.

Step 5 Choose **SFTP** or **FTP**.

Step 6 Follow the instructions provided by the `utils system upgrade initiate` command.

Step 7 Provide the location and credentials for the remote site.

Step 8 Enter SMTP server information when prompted. If you do not have an SMTP server, skip this step.

Step 9 At the Automatically switch versions if the upgrade is successful prompt, type **yes**.

Step 10 Verify that the upgrade was successful, as follows:

- **Finesse:** Sign in to the Finesse Agent Desktop (`https://<FQDN of Finesse server>/desktop`).

  Note After Finesse restarts, wait approximately 20 minutes before signing in to the desktop.

- **Unified Intelligence Center:** Sign in to Unified Intelligence Center (`https://<hostname>:8444/cuic`).
- **Unified Communications Manager:** Verify on the sign-in screen in the console.

Migration Procedures

Back Up Database

You must perform both a SQL backup of the Logger database and an ICMDBA backup of the configuration from the Logger database on the Data Server. Later in the migration process, the configuration backup will be imported into the Unified CCE Rogger. The SQL backup, which contains the historical data, will be imported into the Unified CCE AW-HDS-DDS.

Back up the databases on to a network share.

Procedure

Step 1 Use Microsoft SQL Server Backup and Restore utilities to back up and export the Logger and Outbound Option (if used) databases.

You can then use the backup to restore the historical data to the Unified CCE AW-HDS-DDS.

Step 2 On Side A, use ICMDBA to export the Logger database.

Note When upgrading side B, ensure ICMDBA export is performed from the Side B Logger database.

Step 3 Note the HDS customizable values.

Step 4 Copy the backup files to a shared location.

Back Up Network Configuration

Back up your network configuration to use when setting persistent static routes on the Unified CCE Rogger.

Procedure

Make note of the local static route configuration on the Unified CCE Call Server.

When you install and configure the Unified CCE Rogger, configure the local static routes to match this configuration.

Note This procedure assumes that the private network will be the same.

Configure Unified CCE Rogger

Add a UCCE Instance

Procedure

Step 1 Launch **Web Setup** in the VM you want installed or upgraded.

Step 2 Sign in as a domain user with local administrator permission.

Step 3 Click **Instance Management** and then click **Add**.

Step 4 In the **Add Instance** dialog box, choose the customer facility and instance.

Step 5 In the **Instance Number** field, enter 0.

Step 6 Click **Save**.

Configure the Logger Database and Log

Procedure

Step 1 Launch **ICMdba**.

Step 2 Navigate to **Server** > **Instance**.

Step 3 Right-click the instance name and choose **Create**.

Step 4 In the **Select Component** dialog box, choose the logger you are working on (Logger A or Logger B). Click **OK**.

Step 5 At the prompt "SQL Server is not configured properly. Do you want to configure it now?", click **Yes**.

Step 6 On the **Configure** page, in the **SQL Server Configurations** pane, check the defaults for Memory (MB) and Recovery Interval. Click **OK**.

Step 7 On the **Stop Server** page, click **Yes** to stop the services.

Step 8 In the **Select Logger Type** dialog box, choose **Enterprise**. Click **OK** to open the **Create Database** dialog box.

Step 9 Create the Logger database and log as follows:

a) In the **DB Type** field, choose the side (A or B).

b) In the **Storage** pane, click **Add**.

c) Click **Data**.

d) Choose the E drive.
e) Enter 130000 MB in the **Size** field.
f) Click **OK** to return to the **Create Database** dialog box.
g) Click **Add** again.
h) Choose the E drive.
i) Enter 3072 MB in the **Size** field.
j) Click **OK** to return to the **Create Database** dialog box.

Step 10 In the **Create Database** dialog box, click **Create**. Then click **Start**.

When you see the successful creation message, click **OK** and then **Close**.

Import the Logger and Outbound Databases

Import the Logger and Outbound Option (if used) databases that you previously exported to a network share.

Note Do not import the SQL backup of the Logger database into the Unified CCE Rogger. The SQL backup contains the historical data from the Data Server. Depending on the amount of data, it may be larger than the allocated disk size on the Rogger VM.

Procedure

Step 1 Launch **ICMdba**.

Step 2 Select the Unified CCE Rogger VM under Servers and expand the tree to <*instance name*>_sideA.

Step 3 Choose **Data** > **Import**.

Step 4 Browse to the location where you stored the backup of the Logger database and click **Open**.

Step 5 Click **OK** and then click **Import**.

Step 6 Click **Start** and then click **OK** on all messages that appear.

Step 7 Repeat the above steps for Side B.

Step 8 If you use Outbound Option and want to keep your Outbound Option customer database, restore the database with the Microsoft SQL Server Backup and Restore utilities. Repeat to set up Outbound Option database for Side B.

For more information see the *Outbound Option Guide for Unified Contact Center Enterprise* guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html

Note Size of the Outbound Option database should not exceed 10 GB.

During the Technology Refresh upgrade, run the EDMT tool for each of the Logger and HDS databases to migrate data to the new version.

For detailed information on running the EDMT tool to migrate the data, see *Synchronizing or Updating Data from Logger or HDS Production Server to Staged 12.0(1) Server During Cut-over* in the at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

For detailed information on running the EDMT tool to migrate the data, see *Synchronizing or Updating Data from Logger or HDS Production Server to Staged 12.5(1) Server During Cut-over* in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide, Release 12.5(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Related Topics

Two-Way Outbound Option Database Replication, on page 34

Outbound Option for High Availability: Preliminary Two-Way Replication Requirements

If you plan to set up Outbound Option for High Availability two-way replication, there are several preliminary requirements.

Assign Privileges to Select Users

You must:

- Create a Microsoft SQL Server user and assign that user the sysadmin privilege. The username and password must be the same on Logger Side A and Logger Side B. (You use this username and password when you run Web Setup to configure Outbound Option and enable Outbound Option High Availability).
- Assign the sysadmin privilege to the NT authority/System user.

Verify Replication Feature Selected During Microsoft SQL Server Installation

If you intend to use Outbound Option High Availability Replication, you must select Replication as a feature when you install Microsoft SQL Server. To confirm the selection of the Replication feature:

1. From the Microsoft SQL Server installation disk, run `setup.exe`.
2. Select **Tools**, and click **Installed SQL Server Discovery Report**.
3. Confirm that the Replication feature is listed. If the feature is not listed, run the following command:

   ```
   setup.exe /q /Features=Replication /InstanceName=<instancename> /ACTION=INSTALL
   /IAcceptSQLServerLicenseTerms
   ```

   in which you enter the applicable instance name for your Microsoft SQL Server installation as the `<Instance Name>`.

Create an Outbound Option Database on Logger Side A and Side B

If you have enabled Outbound Option on Logger Side A in a previous release, you must:

- Stop all Logger services on Logger Side A.

- Perform a full database backup for the Outbound Option database on Logger Side A and restore it to Logger Side B. Use SQL Server Management Studio (SSMS) to complete this task.

If you have not enabled Outbound Option in a previous release, you must create an Outbound Option database on Logger Side A and Logger Side B. Use the ICMDBA utility to complete this task.

Note If the database replication fails and it is resolved, the Outbound Option HA must be enabled again. In such a case, you must again synchronize the databases on the Active and Standby sides. Perform a full database backup for the Outbound Option database on Active side and restore it to the Standby side.

Define Logger Public Interface Hostname on Logger Side A and Logger Side B

As you configure Outbound Option for High Availability, you must define the Logger Public Interface Hostname on both sides of the Logger. IP addresses are not allowed.

Make Campaign Manager and Dialer Registry Setting Customizations on Both Side A and Side B

If you customize any Campaign Manager and Dialer registry settings on one side, you must make the same updates for the registry settings on the other side.

Stop the Logger Service Before Enabling or Disabling Outbound Option High Availability

Before you enable or disable Outbound Option High Availability, stop the Logger service on the applicable side or sides.

Two-Way Outbound Option Database Replication

If you choose to enable Outbound Option, you can also enable Outbound Option High Availability. Outbound Option High Availability supports two-way replication between the Outbound Option database on Logger Side A and the Outbound Option database on Logger Side B.

You create an Outbound Option database on Side A and Side B either by:

- Using the ICMDBA tool (if you haven't set up Outbound Option at all).
- Backing up the Outbound Option database on Logger Side A and restoring it to Logger Side B (if you have already set up Outbound Option on Side A).

Also, create a Microsoft SQL Server user and assign that user the sysadmin privilege. The username and password must be the same on Logger Side A and Logger Side B. (You use this username and password when you run Web Setup to configure Outbound Option and enable Outbound Option High Availability.)

You then use Web Setup to configure the Loggers to support Outbound Option and Outbound Option High Availability.

Related Topics

Configure SQL Server for CCE Components, on page 45
Import the Logger and Outbound Databases, on page 32

Add a Unified CCE Router Component

Procedure

Step 1 Launch **Web Setup**.

Step 2 Choose **Component Management** > **Routers**.

Step 3 Click **Add**.

Step 4 On the **Deployment** page:

a) Select the appropriate side (Side A or Side B).
b) Select **Duplexed**.
c) Click **Next**.

Step 5 On the **Router Connectivity** page:

a) Configure the Private Interfaces and Public (Visible) Interfaces. Use the same hostname for Side A Normal and High Priority and the same hostname for Side B Normal and High Priority.
b) Click **Next**.

Step 6 On the **Enable Peripheral Gateways** page:

a) In the **Enable Peripheral Gateways** field, enter 1-3.
b) Click **Next**.

Step 7 On the **Router Options** page:

a) Check the **Enable Quality of Service (QoS)** check box.
b) Check the **Enable Application Gateway** check box.
c) Click **Next**.

Note This step applies to Side A only.

Step 8 On the **Router Quality of Service** page, accept the default values and click **Next**.

Step 9 On the **Summary** page, confirm the Router Summary is correct and then click **Finish**.

Add a Unified CCE Logger Component

You can (optionally) configure the Logger to enable Outbound Option and Outbound Option High Availability. Outbound Option High Availability facilitates two-way replication between the Outbound Option database on Logger Side A and the Outbound Option database on Logger Side B. Use the ICMDBA tool to create an outbound database on Side A and Side B; then set up the replication by using Web Setup.

Note Before you configure the Logger for Outbound Option High Availability:

- Create a Microsoft SQL Server user and assign that user the sysadmin privilege. You must use the same username and password on Logger Side A and Logger Side B. (You use this username and password in the following procedure to configure Outbound Option and enable Outbound Option High Availability.)
- Assign the sysadmin privilege to the NT authority/System user.

Procedure

Step 1 Launch **Web Setup**.

Step 2 Choose **Component Management** > **Loggers**.

Step 3 Click **Add**. Choose the Instance.

Step 4 On the **Deployment** page:

a) Select the appropriate side (Side A or Side B).
b) Select **Duplexed**.
c) Click **Next**.

Step 5 On the **Central Controller Connectivity** page:

a) Enter the hostnames for Side A and Side B for the Router Private Interface and Logger Private Interface.
b) Click **Next**.

Step 6 On the **Additional Options** page, click the **Enable Outbound Option** check box.

Step 7 Click the **Enable High Availability** check box to enable Outbound Option High Availability on the Logger.Checking this check box enables Outbound Option High Availability two-way replication between the Outbound Option database on Logger Side A and the Outbound Option database on Logger Side B. Two-way replication requires that you check this check box on the Additional Options page for both Logger Side A and Side B. If you disable two-way replication on one side, you must also disable it on the other side. You must enable Outbound Option in order to enable Outbound Option High Availability. Similarly, if you want to disable Outbound Option and you have enabled Outbound Option High Availability, you must disable High Availability (uncheck the **Enable High Availability** check box) before you can disable Outbound Option (uncheck the **Enable Outbound Option** check box).

Step 8 If you enable High Availability, enter a valid public server hostname address for **Logger Side A** and **Logger Side B**. Entering a server IP address instead of a server name is not allowed.

Step 9 If you enable High Availability, enter the **SQL Server Admin Credentials (Username and Password)**, which are required to establish two-way replication. The username and password must be the same on Logger Side A and Logger Side B, and the user must have the SQL Server System Admin privilege. SQL replication requires that the correct SQL system admin username and password be in place when setting up Outbound Option High Availability. Changing the password for the SQL user used to set up SQL replication in Outbound Option High Availability causes replication to fail until you disable High Availability and re-enable it with the new username and password. Because of this requirement, be careful about how andwhen you change the password for this user.

Step 10 Click **Next**.

Step 11 Review the **Summary** page, and click **Finish**.

Update VMware Settings on the Unified CCE Data Server

Update the virtual machine settings on the Side A and Side B Unified CCE Data Servers to match the OVA for the Unified CCE AW-HDS-DDS.

Procedure

Step 1 Shut down the virtual machine from the operating system (or right-click the VM and choose **Power** > **Shut Down Guest**).

Step 2 Select the virtual machine and choose **Edit Settings**.

Step 3 Click the **Hardware** tab.

a) Click **Memory** and update the **Memory Size** to 16 GB.
b) Click **Video Card** and update the **Total video memory** to 8 MB.

Step 4 Click the **Resources** tab.

a) Click **CPU** and update the **Reservation** field to 5000 MHz.
b) Click **Memory** and update the **Reservation** to 16384 MB.

Step 5 Click **OK** to save your changes.

Step 6 Power on the virtual machine.

Convert Unified CCE Data Server to Unified CCE AW-HDS-DDS

Before you begin

Make sure that you can restore from the network share to which you backed up the databases.

Stop the SQL Server service. Then, delete the SQL server data and log files to ensure that you have enough space to perform this procedure.

Procedure

Step 1 Rename the database.

a) Ensure that the SQL backup of the Side A Logger is copied to the AW-HDS-DDS network shared folder.
b) Restart the SQL Server service.
c) Open MS SQL Management Studio and run the following queries under the master database:

- `RESTORE FILELISTONLY from Disk='Path of the backup\<instancename>_sideA.bak'`

  Identify the logical filenames.

- ```
  Restore database <instance name>_hds
  from disk='Path of the backup\<instance name>_sideA.bak'
  with
  Move '<instancename>_sideA_data0' to
  'E:\MSSQL\DATA\<instancename>_hds_data0.mdf',
  Move '<instancename>_sideA_log0' to
  'E:\MSSQL\DATA\<instancename>_hds_log0.ldf',Stats=5
  ```

  Note Use the drive letter that the database is installed on.

  <instance name>_hds is the new database instance and <instance name>_sideA_data0 and log0 filenames are the results from the previous query.

d) In the **SQL Management Studio** window, select the <instance name>_hds database. Click **Properties**, and then select the **Files** pane. Change the logical filenames according to the HDS database:

- `<instance name>_sideA-log0` to `<instance name>_hds_log0`
- `<instance name>_sideA_data0` to `<instancename>_hds_data0`
  ```

e) Open a new query tab for the `<instance name>_hds` database and run the following query:

- Truncate table Logger_Type
- Truncate table Recovery
- Truncate table Logger_Admin

Step 2 Edit the Distributor.

a) Open Web Setup.
b) Select **Component Management** > **Administration and Data server component**.
c) Edit the Administration and Data server component to convert it to AW-HDS-DDS, as follows:

- Change the **Server Role** from **AW** to **AW-HDS-DDS**.
- Change the **Central Controller Connectivity** for the Router and Logger to use the hostnames for the side A and B Unified CCE Rogger VMs.

Step 3 Remove the Logger.

a) Open Web Setup.
b) Select **Component Management** > **Logger component**.
c) Select **Logger** and then click **Delete**.

Step 4 Remove the network adapter previously used for the private network.

a) In vSphere Client, right-click the virtual machine and choose **Edit Settings**.
b) Click the **Hardware** tab.
c) Remove the network adapter associated with the private network.

Update VMware Settings on the Unified CCE Call Server

Update the virtual machine settings on the Side A and Side B Unified CCE Call Servers to match the OVA for the Unified CCE PG.

Procedure

Step 1 Shut down the virtual machine from the operating system (or right-click the VM and choose **Power** > **Shut Down Guest**).

Step 2 Select the virtual machine and choose **Edit Settings**.

Step 3 Click the **Hardware** tab.

a) Click **CPUs**. Update the **Number of Virtual Sockets** to 2 and the **Cores per socket** to 1.
b) Click **Memory** and update the **Memory Size** to 6 GB.
c) Click **Video Card** and update the **Total video memory** to 8 MB.

Step 4 Click the **Resources** tab.

a) Click **CPU** and update the **Reservation** field to 4000 MHz.
b) Click **Memory** and update the **Reservation** to 6144 MB.

Step 5 Click **OK** to save your changes.

Step 6 Power on the virtual machine.

Remove the Router from the Unified CCE Call Server

Procedure

Step 1 On the Unified CCE Call Server, open Web Setup.
Step 2 Select **Component Management** > **Router component**.
Step 3 Select **Router** and then click **Delete**.

Modify the PG

Procedure

Step 1 Open Peripheral Gateway Setup.
Step 2 Select **PG1**.
Step 3 Click **Edit**.
Step 4 Click **Next** until you reach the **Peripheral Gateway Network Interfaces** dialog box.
Step 5 Update the Side A and Side B Router visible interfaces to point to the Unified CCE Rogger VMs.
Step 6 Click **Finish**.
Step 7 Repeat Step 2 through Step 6 for PG2.

Modify the Dialer

Perform this procedure if you use Outbound Option.

Procedure

Step 1 Launch the **Peripheral Gateway Setup**.
Step 2 In the **Instance Component** section, select **Dialer**.
Step 3 Click **Edit** and then click **Next**.
Step 4 In the **Outbound Option Dialer Properties** dialog box,
a. Enter the IP address for the Unified CCE Rogger in Side A in the **Campaign Manager server A** field.
b. Enter the IP address for the Unified CCE Rogger in Side B in the **Campaign Manager server B** field.
Step 5 Click **Next**.
Step 6 In the **Check Setup Information** dialog box, verify that the information is correct and then click **Next**.

Step 7 Check the **Yes, start the Unified ICM/CC Node Manager** check box and then click **Finish**.

Update the Central Controller Connectivity

Procedure

Step 1 Launch **Web Setup**.

Step 2 Choose **Component Management** > **Administration & Data Servers**.

Step 3 Check the **Administration & Data Server** check box and then click **Edit**.

Step 4 Click **Next** until you reach the Central Controller Connectivity page.

Step 5 On the Central Controller Connectivity page:

a) In the **Router Side A** and **Logger Side A** fields, enter the hostname of the Side A Rogger.

b) In the **Router Side B** and **Logger Side B** fields, enter the hostname of the Side B Rogger.

c) Click **Next**.

Step 6 Click **Finish**.

Install the Language Pack

If a customer requires a language other than the default (English), download the HCS for CC Language Pack executable from the Unified Contact Center Download Software page.

Install Language Pack

Install the Language Pack on the Unified CCE Data Servers and on any External AW-HDS-DDS servers after upgrading them.

After you install the Language Pack, the Unified CCE Administration Sign In page has a language drop-down menu that lists all available languages. Select a language to display the user interface and the online help in that language.

Uninstall Language Pack

You can uninstall the Language Pack from Windows **Control Panel > Programs and Features > Uninstall or change a program**.

Unified Communications Manager Upgrade Procedures

Upgrade JTAPI on the Call Server

If you upgrade Unified Communications Manager, you must also upgrade the JTAPI client that resides on the Side A and Side B Unified CCE Call Servers.

You must install the new JTAPI client using the Unified Communications Manager Administration application. For more information, see the *Install Cisco JTAPI Client on Unified Communications Manager PG* section in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* available here https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Procedure

Step 1 Uninstall the old JTAPI client from each Call Server:
a) Stop PG1A/PG1B.
b) Go to **Control Panel** > **Programs and Features**.
c) Uninstall the Cisco Unified Communications Manager JTAPI Client , following all prompts.

Step 2 To launch the Unified Communications Manager Administration application, enter the following URL in a Web browser on each Unified CCE Call Server: `https://<IP address of Unified Communications Manager Publisher>/ccmadmin`.

Step 3 Enter the username and password that you created when you installed and configured Unified Communications Manager.

Step 4 Select **Application** > **Plug-ins**.

Step 5 Click **Find** to see the list of applications.

Step 6 Click the download link next to **Cisco JTAPI 32-bit Client for Windows**.

Step 7 Choose **Run this program from its current location**. Click **OK**.

Step 8 If a Security Warning box appears, click **Yes** to install.

Step 9 When asked for the Cisco TFTP Server IP Address, enter the IP address of the Unified Communications Manager Publisher. Click **Next**.

Step 10 Choose **Next** or **Continue** through the remaining setup windows. Accept the default installation path.

Step 11 Click **Finish**.

Step 12 Start the PGs.

Transfer Unified CVP Scripts and Media Files

Create the notification destination and deploy to all of the Unified CVP devices.

Procedure

Step 1 Log in to the Operations Console and select **Bulk Administration** > **File Transfer** > **Scripts and Media**.

Step 2 In the **Select device type** field, select the Gateway.

Step 3 Move all Gateways to **Selected**.

Step 4 Select **Default Gateway files**.

Step 5 Select **Transfer**, and then select **OK** on the popup window.

If you have separate Ingress and VXML gateways, you must select the appropriate files and script for each component.

Step 6 Click **File Transfer Status** to monitor transfer progress.

Step 7 After configuring the application services in the gateways, log in to the gateway and use the Cisco IOS CLI command **call application voice load <service_Name>** to load the gateway download transferred files into the Cisco IOS memory for each Unified CVP service.

Configure Network Adapters for Unified CCE Call Server and Unified CCE Data Server

The Unified CCE Call Server and the Unified CCE Data Server each have two network adapters. You must identify them by MAC address and Network Label, rename them, configure them, and set the interface metric value.

Procedure

Step 1 Identify the MAC addresses and labels for the network adapters as follows:

a) From vSphere, select and right-click the VM.
b) Select **Edit Settings**. In the **Hardware** tab, click **Network adapter 1**. In the right panel, write down the last few digits of MAC addresses and note whether the label is PCCE Public or PCCE Private. For example, Network adapter 1 may have a MAC address that ends in 08:3b and the network label PCCE Public.
c) Repeat for Network adapter 2, noting its MAC address and label.
d) From the VM console, type **ipconfig /all** from the command line. This displays the adapter names and physical addresses.
e) Note the adapter names and physical addresses and match them with the MAC addresses and labels that you noted in VMware. For example, in ipconfig/all, Local Area Connection 2 may have a physical address that ends in 08-3b.
f) Match the MAC address of the network adapter that VMware identified as PCCE Public with the corresponding physical address of Local Area Connector. In this example, the physical address of Local Area Connection 2 (08-3b) matches the MAC address (08-3b) of Network adapter 1. This means that Local Area Connection 2 is PCCE Public.

Step 2 Locate and rename the network adapters in Windows as follows:

a) In Windows, open the **Control Panel** > **Network and Sharing Center** and click **Change adapter settings**.
b) Right-click **Local Area Connection** and select **Rename**. Rename it to **PCCE Public** or **PCCE Private**, based on the matching you did above.
c) Right-click **Local Area Connection 2** and select **Rename**. Rename it to **PCCE Public** or **PCCE Private**, based on the matching you did above. In the example above, **Local Area Connection 2** is renamed to PCCE Public.

Step 3 Set the Properties for PCCE Public as follows:

a) Right-click **PCCE Public** and select **Properties**.
b) In the **Networking** tab, uncheck **Internet Protocol Version 6 (TCP/IPv6)**.
c) Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
d) In the **General** tab for Internet Protocol Version 4, select **Use the following IP address** and enter **IP address**, **Subnet mask**, **Default gateway**, and DNS servers.
e) Click **OK** and **Close** to exit.

Step 4 Set the Properties for PCCE Private as follows:

a) Right-click **PCCE Private** and select **Properties**.
b) In the **Networking** tab, uncheck **Internet Protocol Version 6 (TCP/IPv6)**.
c) Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
d) In the **General** tab for Internet Protocol Version 4, select **Use the following IP address** and enter **IP address** and **Subnet mask**.
e) Click **Advanced**.
f) Click the **DNS** tab and uncheck *Register this connection's addresses in DNS*.

g) In the DNS Server, add an entry for the private IP address. Append a suffix such as *p* to the hostname for this IP, to identify it as a private.
h) Click **OK** to exit.

Configure Database Drive

Note Complete this procedure to create a virtual drive, if the virtual drive was not automatically created in the VM.

Procedure

Step 1 Add a virtual drive as follows:

Using Vsphere client:

a) Right-click the virtual machine and click **Edit Settings**.
b) In the **Hardware** tab, click on **Add**.

The **Add Hardware** window appears.

c) You can select the type of device you wish to add. Select **Hard Disk**, and then click **Next**.
d) Select the **Create a new virtual disk** option, and then click **Next**.
e) In the **Capacity** section, use the **Disk Size** box to assign the desired disk space, and then click **Next**.

Note Virtual machine templates for Logger, Rogger, AW, and HDS servers do not have a SQL database drive preprovisioned. The following reference table must be used to assign disk space to the virtual machine based on the type of validation errors will occur:

You can custom size the SQL database disk space to meet the data retention requirements on an external AW-HDS-DDS server only, as calculated by the Database Estimator tool.

f) On the **Disk Provisioning** section choose **Thick provision Lazy Zeroed format**. Click **Next**.
g) In the **Advanced Options** section, retain the default options and then click **Next**.
h) In the **Ready to Complete** section, click **Finish** to create the hard disk.
i) Click **OK** to confirm the changes.

The Recent Tasks window at the bottom of the screen displays the progress.

Step 2 In Windows, navigate to **Disk Management**.

Step 3 Right-click on the **Disk 1** box and select **Online**.

Step 4 Initialize Disk 1 as follows:

a) Right-click on the **Disk 1** box and select **Initialize Disk**.
b) Check the **Disk 1** checkbox.
c) Select the **MBR (Master Boot Record)** radio button.
d) Click **OK**.

Step 5 Create a new disk partition as follows:

a) Right-click the graphic display of **Disk 1** and select **New Simple Volume**.

b) Click **Next** on the first page of the **New Simple Volume Wizard**.
c) On the **Specify Volume Size** page, retain the default volume size. Click **Next**.
d) On the **Assign Drive Letter or Path** page, assign drive letter (E). Click **Next**.
e) On the **Format Partition** page, format the partition as follows:

1. Select the **Format this volume with the following settings** radio button.
2. Click **Format Disk**.
3. Select File System as **NTFS** and click **Start**.
4. Select **Default** from the **Allocation unit size** drop-down menu.
5. Enter a value in the **Volume label** field.
6. Check the **Perform a quick format** checkbox.
7. Click **Next**.

f) Click **Finish**.

The format is complete when the status changes to Healthy.

Set Persistent Static Routes

To create a persistent static route with the **route add** command, you need the destination subnet, the subnet mask, the local gateway IP, and the interface number of the local Private Network interface:

`route add <destination subnet> mask <subnet mask> <gateway IP> IF <interface number> -p`

You must launch the DOS prompt as an administrator to run the commands in this procedure.

Procedure

Step 1 On each , or PG VM, run `ipconfig /all`.
Record the `IPv4 Address`, `Subnet Mask`, and `Physical Address` (MAC address) for the Private Network interface.

Step 2 On each of these VMs, run `route print -4`.
Record the `Interface` for the Private Network. You can identify the correct interface by looking for its `Physical Address` (MAC address).

Step 3 On each of these VMs, run `route add <destination subnet> mask <subnet mask> <gateway IP> IF <interface number> -p` to add a persistent static route for the remote Private Network.

Run Windows Updates

Procedure

Go to **Settings** > **Update & Security** and run Microsoft Windows Update.

After the update is complete, click **Do not enable automatic updates**.

Configure SQL Server for CCE Components

Procedure

Step 1 Click the **Windows Start** icon, and then select the Downward Arrow icon to display all applications.

Step 2 Open **Microsoft SQL Server Management Studio**.

Step 3 Log in.

Step 4 Expand **Security** and then **Logins**.

Step 5 If the BUILTIN\Administrators group is not listed:

a) Right-click **Logins** and select **New Login**.
b) Click **Search** and then **Locations** to locate BUILTIN in the domain tree.
c) Type **Administrators** and click **Check Name** and then **OK**.
d) Double-click **BUILTIN\Administrators**.
e) Choose **Server Roles**.
f) Ensure that **public** and **sysadmin** are both checked.

Upgrade to Release 11.6(1)

Before you begin

- An upgrade to Release 11.6(1) requires Windows Update KB2919355 (Hotfix). If you applied a Windows update since March 2014, this update is already installed. To determine if this Windows Hotfix is installed, from your Control Panel go to **Programs** > **Programs and Features**. Click **View installed updates**.

  Make sure that the Windows update is not running in parallel when you install the release 11.6(1) patch.

- The minimum disk space required to perform the upgrade is 1500 MB.
- During the upgrade process, the installer takes a backup of the existing configuration database. This backup is available in `drive\temp\<instance name_logger side><schema version>`.

  For example: `C:\Temp\Inst_sideA181`

Procedure

Step 1 Log in to your system as a user with administrative privileges.

Step 2 After either downloading the installer or placing the media in the drive, start the Cisco ICM Minor Release ICM Installer.

Step 3 Follow the on-screen instructions to install Unified CCE Release.

Cut Over from Side B to Side A

Perform the following tasks during a maintenance window, in the order that they are listed.

Important You must perform the tasks **in the order that they are listed in this table**. Some tasks link to procedures in other parts of the guide. When you reach the end of a procedure, refer back to this table to determine what you must do next. **Failure to perform upgrade tasks in the order listed in this table can cause the upgrade to fail**.

Step	Task
Configure the Cisco Voice Gateway dial-peer priority	
1.	Reverse the Cisco IOS Enterprise Ingress Voice Gateway dial-peer priority configuration so that calls are sent to the Side A Unified CVP server first and then to Side B.
2.	Change the Unified CVP scripts as required so they do not point to DNs and labels on Unified CVP Server 2B.
Bring down Side B	
3.	On each of the following VMs, select **Unified CCE Service Control** on the desktop. Stop the Unified CCE services and change **Startup** to **Manual**: • Side B Unified CCE Call Server • Side B Unified CCE Data Server • External HDS with Side B as the Central Controller preferred side (if used)
4.	Power off the Finesse Secondary node VM in the vSphere client.
5.	Power off the Unified Intelligence Center Subscriber VM in the vSphere client.
6.	Transfer the Unified CVP scripts and media files to the gateways that are not currently in use on Side A. See Transfer Unified CVP Scripts and Media Files, on page 41.
7.	Shut down the following Unified CVP VMs from their Windows OS in the following order: **1.** Unified CVP Server 1B **2.** Unified CVP Server 2B **3.** Unified CVP Reporting Server **Important** At this point, Courtesy Callback no longer works. Unified CVP Reporting does not work unless you have an external Unified CVP Reporting Server.
8.	Power off the Unified Communications Manager Subscriber 2 VM in the vSphere client.
Bring up Side A	

Step	Task
9.	On each of the following VMs, select **Unified CCE Service Control** on the desktop. Start the Unified CCE services and change **Startup** to **Automatic**: • Side A Unified CCE Rogger • Side A Unified CCE AW-HDS-DDS (former Data Server) • Side A PG (former Call Server) • External HDS with Side A as the Central Controller (if used) Verify that services are started.
10.	If you changed the Unified Communications Manager device pool settings as part of the preupgrade, restore the original settings.
11.	Direct agents to sign in to the Side A Finesse Primary node.
12.	Change Unified Intelligence Center historical and real-time data sources to point to the Side A Unified CCE AW-HDS-DDS. See Configure Unified Intelligence Center Data Sources for External AW-HDS-DDSHDS, on page 20 for steps on how to configure Unified Intelligence Center data sources. Use the IP address of the Unified CCE AW-HDS-DDS.

Migrate and Upgrade Side B

Important You must perform the tasks **in the order that they are listed in this table**. Some tasks link to procedures in other parts of the guide. When you reach the end of a procedure, refer back to this table to determine what you must do next. **Failure to perform upgrade tasks in the order listed in this table can cause the upgrade to fail**.

For best results, place the upgrade media ISOs on local data stores. Make sure to remove them when the upgrade is complete.

Step	Task
Start the Side B Unified CVP components	
1.	Start Unified CVP Server 1B and then start the Unified CVP Reporting Server. **Note** You do not need to start Unified CVP Server 2B as it is removed during the migration.
Upgrade the Side B Unified CVP Servers	
2.	Remove the Unified CVP Server 2B VM.
3.	Update the Cisco IOS Enterprise Ingress Voice Gateway dial-peer configuration to remove Unified CVP Server 2B.

Step	Task
4.	Upgrade Unified CVP Server 1B. See Upgrade the Unified Customer Voice Portal, on page 7.
Upgrade Side B Cisco Voice Gateway IOS Version if needed	
5.	Upgrade the Side B Cisco Voice Gateway IOS version to the minimum required by the upgraded HCS for CC release (or later). See Upgrade Cisco Voice Gateway IOS Version, on page 27. See the *HCS for CC Compatibility Information* at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-device-support-tables-list.htmlfor IOS support information.
Upgrade the Side B Finesse and Unified Intelligence Center VMs	
6.	Power on the Finesse Secondary node VM in the vSphere client.
7.	Upgrade the VMware version on the Finesse Secondary VM. See Upgrade the Virtual Machine Hardware Version, on page 28.
8.	Update the settings on the Finesse Secondary VM. See Update VMware Settings for Cisco Finesse, on page 28.
9.	Upgrade the Finesse Secondary node. See Upgrade Finesse, on page 12
10.	Power on the Unified Intelligence Center Subscriber VM in the vSphere client.
11.	Upgrade the VMware version on the Unified Intelligence Center Subscriber VM. See Upgrade the Virtual Machine Hardware Version, on page 28.
12.	Update the settings on the Unified Intelligence Center Subscriber VM. See Update VMware Settings for Cisco Unified Intelligence Center, on page 28.
13.	Upgrade the Unified Intelligence Center Subscriber. See Upgrade Cisco Unified Intelligence Center, on page 12 **Note** Your configuration information migrates automatically to the upgraded version in the active partition.
Prepare for Side B Migration to HCS for CC 2000 Agent Rogger Deployment	
14.	Back up and export the Side B SQL database. See Back Up Database, on page 30.
Install the Side B Unified CCE Rogger	

Step	Task
15.	Create a VM for the Side B Unified CCE Rogger. Select **CCE Rogger** from the drop-down list.
16.	Install Microsoft Windows Server on the Side B Unified CCE Rogger VM.
17.	Install VMware tools on the Side B Unified CCE Rogger VM.
18.	Configure the network adaptors for the Side B Unified CCE Rogger. See Configure Network Adapters for Unified CCE Call Server and Unified CCE Data Server, on page 42 .
19.	Install antivirus software on the Side B Unified CCE Rogger.
20.	Configure the database drive for the Side B Unified CCE Rogger. See Configure Database Drive, on page 43.
21.	Set persistent static routes. See Set Persistent Static Routes, on page 44.
22.	Run Windows updates. See Run Windows Updates, on page 44.
23.	Add the Unified CCE Rogger to the domain.
24.	Install Microsoft SQL Server.
25.	Install Cisco Unified Contact Center Enterprise.
Configure the Side B Unified CCE Rogger	
26.	Add a UCCE Instance in Web Setup. See Add a UCCE Instance, on page 31.
27.	Configure SQL Server for the Logger database. See Configure SQL Server for CCE Components, on page 45.
28.	Configure the Logger database and log. See Configure the Logger Database and Log, on page 31.
29.	Import the Side B SQL database that you previously backed up in step 24. See Outbound Option for High Availability: Preliminary Two-Way Replication Requirements, on page 33
30.	Add a Unified CCE Router component in Web Setup. See Add a Unified CCE Router Component, on page 35.

Step	Task
31.	Add a Unified CCE Logger component in Web Setup. See Add a Unified CCE Logger Component, on page 35.
Convert the Side B Unified CCE Data Server and Unified CCE Call Server	
32.	Upgrade the VMware version on the Side B Data Server VM. See Upgrade the Virtual Machine Hardware Version, on page 28.
33.	Update the settings on the Side B Data Server VM. See Update VMware Settings on the Unified CCE Data Server, on page 36.
34.	Convert the Side B Unified CCE Data Server to a Unified CCE AW-HDS-DDS. See Convert Unified CCE Data Server to Unified CCE AW-HDS-DDS, on page 37.
35.	Update the real-time and historical data sources for Unified Intelligence Center to point to the Unified CCE AW-HDS-DDS. You must update the historical data source database name to <*instancename*>_awdb.
36.	Upgrade the VMware version on the Side B Call Server VM. See Upgrade the Virtual Machine Hardware Version, on page 28.
37.	Update the settings on the Side B Call Server VM. See Update VMware Settings on the Unified CCE Call Server, on page 38.
38.	Remove the Router from the Side B Unified CCE Call Server. See Remove the Router from the Unified CCE Call Server, on page 39. **Note** If CTI OS Server is present, remove it as well. CTI OS is no longer supported. The Call Server is now a PG.
39.	Run the Unified CCE 11.6(1) installer on the Side B Unified CCE Rogger to upgrade to Release 11.6(1). See Upgrade to Release 11.6(1), on page 45.
40.	Disable configuration changes on the Side B Unified CCE Rogger. Change the following registry key to 1: `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\RouterB\Router\CurrentVersion\Configuration\Global\DBMaintenance`
41.	Run the Unified CCE 11.6(1) installer on the Side B Unified CCE AW-HDS-DDS (former Data Server) to upgrade to Release 11.6(1). See Upgrade to Release 11.6(1), on page 45.

Step	Task
42.	Run the Unified CCE 11.6(1) installer on the Side B PG (former Call Server) to upgrade to Release 11.6(1). See Upgrade to Release 11.6(1), on page 45.
43.	Modify the Side B PG to point to the Unified CCE Rogger. See Modify the PG, on page 39.
44.	Modify the dialer to point to the Unified CCE Rogger (if using Outbound Option). See Modify the Dialer, on page 39.
Optional: Upgrade the External HDS associated with Side B (if used)	
45.	Upgrade the VMware version on the External HDS associated with Side B. See Upgrade the Virtual Machine Hardware Version, on page 28.
46.	Run the Unified CCE 11.6(1) installer on the External HDS associated with Side B to upgrade to Release 11.6(1). See Upgrade to Release 11.6(1), on page 45.
47.	Update the Central Controller connectivity to point to the Unified CCE Rogger. See Update the Central Controller Connectivity, on page 40.
Optional: Install language pack	
48.	Install the language pack on the Side B Unified CCE Rogger, AW-HDS-DDS, PG (formerly Call Server), and External HDS (if used). See Install the Language Pack, on page 40.
Upgrade Side B Unified Communications Manager Subscriber 2	
49.	Power on the Unified Communications Manager Subscriber 2 VM in the vSphere client.
50.	Upgrade the Side B Unified Communications Manager Subscriber 2. See Upgrade Cisco Unified Communications Manager, on page 14
51.	Upgrade JTAPI on the Side B PG (formerly Call Server). See Upgrade JTAPI on the Call Server, on page 40.
Optional: Change hostnames of the Unified CCE components	

Step	Task
52.	Optional: Change the hostnames of the Unified CCE components (AW-HDS-DDS and PG). **Note** You can perform this task when you reboot each component as part of the upgrade. If you do change the hostnames, you must also change them in the following places: • Finesse • PG Setup • Unified Intelligence Center - Historical and real-time • Private network DNS entries • Live Data—If you change the hostname of the AW-HDS-DDS (former Data Server), Live Data no longer connects to the AW-HDS-DDS after the Data Server hostname is removed from DNS. To fix this, do the following: **1.** Run the following CLI command on the CUIC-LD-IdS Publisher: **unset live-data aw-access secondary** **2.** Restart Cisco Tomcat on the Side B AW-HDS-DDS.

Sync Side A to Side B

Perform these tasks during the third maintenance window to sync Side A and Side B.

Step	Task
1	Set the following registry key to 0 on either the Side B Unified CCE Rogger: `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\Router B\Router\CurrentVersion\Configuration\Global\DBMaintenance`
2	On each of the following VMs, select **Unified CCE Service Control** on the desktop. Start the Unified CCE services and change Startup to Automatic, in this order: **1.** Side B Unified CCE Rogger **2.** Side B Unified CCE AW-HDS-DDS **3.** Side B PG **4.** External HDS with Side B as the Central Controller preferred side (if used) Verify that the services are started.

Migrate Call Server to Unified CCE PG

Perform these tasks in a maintenance window. Perform these tasks on the Side A PG (former Call Server) and then on the Side B PG and in the order they are listed.

Important You must perform the tasks **in the order that they are listed in this table**. Some tasks link to procedures in other parts of the guide. When you reach the end of a procedure, refer back to this table to determine what you must do next. **Failure to perform upgrade tasks in the order listed in this table can cause the upgrade to fail**.

Note You can continue the maintenance window that you used to sync Side A and Side B or you perform them in a later maintenance window.

Step	Task
For the Side A PG (formerly Call Server):	
1.	Add a new CUCM PG. See Add a New CUCM PG, on page 54.
2.	Remove the Dialed Number configuration. See Remove Dialed Number Configuration, on page 54.
3.	Remove the Agent Targeting Rule configuration. See Remove Agent Targeting Rule Configuration, on page 55.
4.	Remove the Network Trunk configuration. See Remove Network Trunk Configuration, on page 55.
5.	Remove the Label configuration. See Remove Label Configuration, on page 56.
6.	Remove the Unified CVP PIMs from PG Explorer. See Remove Unified CVP PIMs, on page 56.
7.	Install CUCM PG3. See Install the CUCM PG, on page 56.
8.	Install CG3. See Install CG3, on page 58.
9.	Modify PG1 to VRU PG. See Modify PG1 to VRU PG , on page 58.
10.	Uninstall CG1. See Uninstall CG1, on page 59.
11.	In Finesse Administration, configure the CTI port information in CTI Server Settings for Side A. Restart the Cisco Tomcat service and the Cisco Finesse Tomcat service.

Step	Task
For the Side B PG (formerly Call Server):	
12.	Repeat Step 7 through Step 10 for the Side B PG.
13.	In Finesse Administration, configure the CTI port information in CTI Server Settings for Side B. Restart the Cisco Tomcat service and the Cisco Finesse Tomcat Service.
Redo Dialed Number, Agent Targeting Rule, and Network Trunk Group configuration as required	

Add a New CUCM PG

Procedure

Step 1 In the **Configuration Manager** window, expand **Tools** > **Explorer Tools**.

Step 2 Open **PG Explorer**.

Step 3 Click **Add PG** and then enter the following values in the **Logical Controller** pane:

- In the **Name** field, enter **`CUCM_PG`**.
- For **Client type**, choose **CUCM**.
- Enter **Primary CTI Address** and **Secondary CTI Address** as mentioned in the generic PG.

Step 4 Delete the peripheral that was automatically created in the previous step.

Step 5 Click **Save**.

Step 6 Drag the CUCM peripheral from the Generic PG to the CUCM PG.

A message appears asking if you are sure you want to move the peripheral to a different PG. Click **Yes** to confirm.

Step 7 Rename the Generic PG to VRU PG and change the Client type to **VRU**.

Step 8 Click **Save**.

Note Make sure to record the Logical Controller ID of the new CUCM PG. You need to enter it when you install the PG.

Remove Dialed Number Configuration

Before you begin

Dialed numbers that are mentioned in any scripts must be removed from the scripts before you perform this procedure. Make sure that they are removed from all versions (not just the active scripts).

Procedure

Step 1 On the Unified CCE Admin Workstation server, select **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.

Step 2 In Configuration Manager, expand **Tools** > **List Tools**.

Step 3 Open **Dialed Number / Script Selector List**.

Step 4 Select **Routing Client** as the existing VRU for Unified CVP 2A / Unified CVP 2B and then click **Retrieve**.

Step 5 Select each dialed number associated to the routing client and then click **Delete**.

Step 6 Click **Save**.

Remove Agent Targeting Rule Configuration

Procedure

Step 1 On the Unified CCE Admin Workstation server, select **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.

Step 2 Expand **List Tools**.

Step 3 Select **Agent Targeting Rule**.

Step 4 Remove the Routing Client for Unified CVP 2A and Unified CVP 2B.

Step 5 Click **Save**.

Remove Network Trunk Configuration

Procedure

Step 1 On the Unified CCE Admin Workstation server, select **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.

Step 2 Expand **Explorer Tools**.

Step 3 Select **Network Trunk Group Explorer**.

Step 4 From the **PG** list, select **VRU_PG** and then click **Retrieve**.

Step 5 Expand **GENERIC** and click any trunk group that appears beneath it.

Step 6 Click **Multiple**.

Step 7 In the **Delete Multiple** dialog box, select all of the CVP 2A and CVP 2B trunk groups and then click **Delete**.

Step 8 Click **OK**.

Step 9 Click **Save**.

Remove Label Configuration

Procedure

Step 1 On the Unified CCE Admin Workstation server, select **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.

Step 2 Expand **List Tools**.

Step 3 Select **Label List**.

Step 4 Remove the labels associated with Unified CVP 2A and Unified CVP 2B.

Remove Unified CVP PIMs

Procedure

Step 1 On the Unified CCE Admin Workstation server, select **Start** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.

Step 2 Expand **Tools** > **Explorer Tools**.

Step 3 Open **PG Explorer**.

Step 4 Select **VRU PG**.

Step 5 Delete the PIMs for Unified CVP 2A and Unified CVP 2B.

Step 6 Click **Save**.

Install the CUCM PG

Procedure

Step 1

Step 2 On the PG (former Call Server), choose **Start** > **All Programs** > **Unified CCE Tools** > **Peripheral Gateway Setup**.

Step 3 In the **Instance Component** section, click **Add**.

Step 4 Click **Peripheral Gateway**.

Step 5 In the **Peripheral Gateways Properties** dialog, do the following:

a) Check the **Production Mode** check box.
b) Check the **Auto start at system start up** check box.
c) Check the **Duplexed Peripheral Gateway** check box.
d) From the **PG Node Properties ID** drop-down list, select **PG3**.
e) Select the appropriate side (Side A or Side B).
f) In the **Client Type Selection** section, add **CUCM** to the Selected Types.
g) Click **Next**.

Step 6 In the **Peripheral Gateway Managers** section of the **Peripheral Gateway Component Properties** dialog box, click **Add**.

Step 7 Select **CUCM** and **PIM1** and click **OK**.

Step 8 Check the **Enabled** check box.

Step 9 In the **Peripheral Name** field, enter CM.

Step 10 In the **Peripheral ID** field, enter the Peripheral ID that the system generated in Step 8 after the CUCM PG was added.

Step 11 In the **Agent Extension Length** field, enter the extension length for this deployment.

Step 12 In the **CUCM Parameters** section, do the following:

a) In the **Service** field, enter the hostname of the Unified Communications Manager Subscriber.
b) In the **User ID** field, enter pguser.
c) In the **User Password** field, enter the password of the user that will be created on Unified Communications Manager.
d) In the **Mobile Agent Codec** field, choose either **G711 ULAW/ALAW** or **G.729**.

Step 13 Click **OK**.

Step 14 In the **Logical controller ID** field, enter the Logical controller ID of the CUCM PG that you created previously in PG Explorer.

Step 15 In the **CTI Call Wrapup Data delay** field, enter 0. Click **Next**.

Step 16 In the **Device Management Protocols Properties** dialog box, do the following:

a) For Side A PG:
   - Select **Side A preferred**.
   - For Side A properties, select **CallRouter is local**.
   - For Side B properties, select **CallRouter is remote (WAN)**.

b) For Side B PG:
   - Select **Side B preferred**.
   - For Side A properties, select **CallRouter is remote (WAN)**.
   - For Side B properties, select **CallRouter is local**.

c) For both sides:
   - Accept the default in the Usable Bandwidth (kbps) field.
   - Accept the default in the Heartbeat Interval (100ms) field.

d) Click **Next**.

Step 17 In the **Peripheral Gateway Network Interfaces** dialog box, complete the interface fields:

a) Enter the Private and Visible network interface hostnames. For the PG, use the same hostnames for private and private high. For the Router, enter the hostname of the Unified CCE Rogger Side A for the Router visible A and Router visible A high interfaces. Enter the hostname of the Unified CCE Rogger Side B for the Router visible B and Router visible B high interfaces.
b) For the Side A PG, in the **Private Interfaces** section, click **QoS**. Check **Enable QoS** and click **OK**.
c) For both the Side A and Side B PGs, in the **Visible Interfaces** section, click **QoS**. Check **Enable QoS** and click **OK**.

d) Click **Next**.

Step 18 In the **Check Setup Information** dialog box, click **Next**.

Step 19 In the **Setup Complete** dialog box, click **Finish**.

Install CG3

Procedure

Step 1 Launch **Peripheral Gateway Setup**.

Step 2 In the **Instance Components** section, click **Add**.

Step 3 In the Component Selection dialog box, click **CTI Server**.

a) Check **Production mode**.
b) Check **Auto start at system startup**.
c) Check **Duplexed CTI Server**.
d) From the CG node properties pane ID list, choose **CG3**.
e) Enter 3 in the CG node properties ICM system ID field.
f) Click the appropriate side.
g) Click **Next**.

Step 4 In the CTI Server Component Properties dialog box, do the following:

a) For Side A, enter 42027 in the Client Connection Port Number field.
b) For Side B, enter 43027 in the Client Connection Port Number field.

Step 5 Click **Next**.

Step 6 In the CTI Server Network Interface Properties dialog box, fill in all interface fields and then click **Next**.

Step 7 Check your setup information and then click **Next**.

Step 8 Click **Finish**.

Modify PG1 to VRU PG

Procedure

Step 1 Open Peripheral Gateway Setup.

Step 2 Select **PG1**.

Step 3 Click **Edit**.

Step 4 In the **Client Type Selection** section, remove **CUCM**.

Step 5 Click **Next**.

Step 6 In the **Peripheral Gateway Component Properties** dialog box, remove the CUCM PIMs that were used for connecting to CUCM and click **Next**.

Step 7 In the **Device Management Protocol Properties** dialog box, click **Next**.

Step 8 In the **Peripheral Gateway Network Interfaces** dialog box, enter the hostname or IP address of the Unified CCE Rogger Side A for the Router visible A and Router visible A high interfaces. Enter the hostname or IP address of the Unified CCE Rogger Side B for the Router visible B and Router visible B high interfaces.

Step 9 Click **Next**.

Step 10 In the **Check Setup Information** dialog box, click **Next**.

Step 11 Check the **Yes, start the Unified ICM/CC Node Manager** check box and click **Finish**.

Uninstall CG1

Procedure

Step 1 Open Peripheral Gateway Setup.

Step 2 Select **CG1**.

Step 3 Click **Delete**.

Step 4 Click **OK**.

Switch into HCS for Contact Center Deployment

Step	Task
1.	In **Unified CCE Administration** > **Deployment**, switch into the HCS for Contact Center: 2000 Agents deployment type.
2.	Validate the HCS for Contact Center deployment in Unified CCE Administration. See Validate HCS for Contact Center Deployment and Build System Inventory, on page 59.
3.	Direct agents to sign in to the correct Finesse node.

Validate HCS for Contact Center Deployment and Build System Inventory

Validate the HCS for Contact Center deployment using the Unified CCE Administration Deployment tool.

As you complete the procedure, you are prompted only for missing information; you may not need to perform each step.

Postupgrade Tasks

You can perform these postupgrade tasks in any order.

Component	Task
Finesse	Complete postupgrade tasks for the Finesse desktop layout. See Finesse Desktop Layout Postupgrade Tasks, on page 60. Finesse server need a restart after the upgrade of peripheral gateways (PG).

Component	Task
Unified CVP	Upgrade Call Studio. Upgrade Unified Call Studio, on page 60
	Optional: Synchronize the metadata files for the Unified CVP REST API using the sync-up tool. See Initiate Metadata Synchronization for Unified CVP Rest API, on page 61.
All	Optional: Upgrade ESXi. See Upgrade VMware vSphere ESXi, on page 62.

Finesse Desktop Layout Postupgrade Tasks

If you do not use a custom desktop layout, do the following after upgrading Cisco Finesse:

1. Click **Restore Default Layout** on the Manage Desktop Layout gadget to add all updates from the new default desktop layout.
2. Disable the Agent Queue Statistics gadget from the default desktop layout for the Agent role. This gadget is not supported for the Agent role in HCS for CC deployments.
3. **Optional:** Enable Live Data Report gadgets for the Agent role.

If you use a custom desktop layout, do the following after upgrading Finesse:

1. Add optional Live Data Report gadgets for the Agent role after upgrading Cisco Finesse.
2. If you want to restore a previous layout for the desktop, sign in to the Administration Console on the primary Finesse node. Copy and paste your saved layout XML into the Manage Desktop Layout gadget.

Upgrade Unified Call Studio

Before you begin

Obtain a new license for Unified Call Studio because licenses for earlier versions are invalid with the latest version.

Note Upgrade of Call Studio is supported through the migration process.

Procedure

Step 1 Open Call Studio, right-click any existing project in the Navigator view, choose **Export**.

The **Export** wizard opens.

Step 2 Navigate to **General** > **File System**, and click **Next**.

Note From the list displayed by the Export wizard, select multiple projects to export them simultaneously.

Step 3 Browse to the directory where the projects will be exported and click **OK** and then click **Finish**.

Step 4 Uninstall the Call Studio software.

For more information, see the Unified CVP/Call Studio Uninstallation section.

Step 5 Install the Call Studio software.

For more information, see the Install Unified Call Studio section.

Install Unified Call Studio

Procedure

Step 1 Mount the Unified CVP software (including CVP Studio) installer ISO image, and run setup.exe.

Step 2 On the **Welcome** screen, click **Next**.

Note If you click **Cancel** here or on the dialog screens that follow before the **Ready to Install the Program** screen, the installation is canceled. The **Exit Setup** dialog box appears.

Step 3 Review **Copyrights to Products** used by Call Studio and click **Next**.

Step 4 Review and accept the license agreement, and click **Next**.

Step 5 On the Choose Destination Location screen, select the folder where setup will install files. By default, it is `C:\Cisco\CallStudio`.

Step 6 On the **InstallShield Wizard Complete** screen, click **Install**.

Step 7 Click **Finish** to exit the wizard.

The Call Studio software is installed on your computer.

Initiate Metadata Synchronization for Unified CVP Rest API

In the CVP REST API architecture, information of media files on Media Server and VXML applications on a VXML server is saved on a WSM Server as metadata in Derby database. This metadata information is created, updated, and deleted by the REST API calls. There may be situations where the metadata may go out of sync with files on VXML Servers and Media Servers. Examples are addition and deletion of CVP Servers, deployment of apps and media files by a tool other than the REST API, and CVP Media Server or the VXML server upgraded from a version where the REST API was not supported.

A command line tool "metasynch.cmd" is available at `C:\Cisco\CVP\wsm\CLI` to enable synchronization of metadata with the files on VXML Servers and Media Servers. The tool internally uses the Synch up API to perform the synchronization. It takes three arguments- WSM user name, WSM user password, and server type (MEDIA, VXML or VXML_ STANDALONE). Based on the server type information, all servers of the respective server type are synchronized. If the server type argument is not provided, metadata is synchronized with all media servers and VXML servers configured in OAMP.

In case of an upgrade, the media files and VXML applications are present in the Media Servers and VXML Servers but corresponding metadata information is not present in the WSM Server. The absence of metadata information limits a user from using the REST API to access, update, and delete existing media files and VXML applications on the Media Server and the VXML Server.

Synchronize Metadata Files Using Sync-Up Tool

To invoke **metasynch.cmd**, complete the following steps.

Procedure

Step 1 On the Unified CVP OAMP Server, navigate to the `C:\Cisco\CVP\wsm\`CLI location.

Step 2 Run the **metasynch.cmd** file with following arguments:

- **wsm username**
- **wsm password**

Example:

```
metasynch.cmd wsmusername wsmpassword MEDIA
```

Usage : metasynch [options] username password [servertype]

servertype : MEDIA/VXML

options : -help -? print this help message

Note The server type argument should be MEDIA, VXML type. If the server type argument is not provided, the metadata is synched with all the VXML applications on VXML servers and all media files on Media servers. Logs for synch command tool can be found at the following location:

`C:\Cisco\CVP\wsm\CLI\log\SyncTool.log`

Upgrade VMware vSphere ESXi

If you use VMware vCenter Server in your deployment, upgrade VMware vCenter Server before upgrading VMware vSphere ESXi.

Upgrade VMWare vSphere ESXi on Side A and Side B servers to the latest version supported with this release of HCS for CC. HCS for CC uses standard upgrade procedures, which you can find using VMware documentation (https://www.vmware.com/support/pubs/).