Phase 4-Unified Communications Applications Upgrade

- Workflow for Upgrading UC Applications, on page 1
- Plan - Pre Upgrade Checks, on page 3
- Plan - Unified CM and Unified CM IM and Presence, on page 5
- Plan - Cisco Unity Connection, on page 8
- Plan - Cisco Emergency Responder , on page 10
- Prepare - Pre Upgrade Actions, on page 10
- Prepare - Unified CM and Unified CM IM and Presence , on page 10
- Prepare - Cisco Unity Connection, on page 13
- Upgrade UC Application, on page 14
- Restore UC Application, on page 18
- Validate UC Application, on page 21
- Upgrade Toolkit Overview, on page 22
- Upgrade Requirements for Push Notifications, on page 46

Workflow for Upgrading UC Applications

The strategy for upgrading and migrating UC Applications involves these procedure and characteristics:

- Comprises one or more Cisco UC applications, management, and data center components.
- Completes the phase in a single or multiple maintenance windows.
- Completes the different phases in an order.
- Includes pre upgrade and post upgrade phase conditions and activities.
- Includes the upgrade maintenance window conditions and activities.

You can operate your Cisco HCS deployment between upgrade phases because the application and component groups of any phase are compatible with the subsequent upgrade phases. However, before you upgrade to the next phase, ensure to upgrade the previous phases to the minimum version. You can upgrade the required Service Provider Cisco HCS Data Center components (based on the minimum versioning analysis) significantly before upgrading the subsequent phases.

Step 1 Plan - Pre Upgrade Checks, on page 3

Perform the pre upgrade checks that before upgrading Cisco UC applications, management, and data center components in the following sequence:

a. Compatibility and Documentation References

b. Plan - Unified CM and Unified CM IM and Presence, on page 5

c. Plan-Cisco Unity Connection

d. Plan - Cisco Emergency Responder , on page 10

Note To perform pre-upgrade checks on Unified CM, Unified CM IM and Presence, and Cisco Unity Connection, use the HCM-F Release 11.5(4)SU1 interface. To understand the supported checks and their results, see Upgrade Checks, on page 26. For executing the checks, see Perform Upgrade Checks, on page 25.

Step 2 Prepare - Pre Upgrade Actions, on page 10

Perform these pre-upgrade actions or tasks before you upgrade Cisco UC applications in the following sequence:

a. Prepare - Unified CM and Unified CM IM and Presence , on page 10

b. Prepare - Cisco Unity Connection, on page 13

Step 3 Upgrade UC Application

Perform the upgrade tasks on Cisco UC applications (refresh and standard upgrade), management, and data center components:

- Upgrade UC Applications using Refresh Upgrade, on page 14
- Upgrade UC Applications using Standard Upgrade, on page 15

Step 4 Restore UC Application, on page 18

Perform these post upgrade actions or tasks after upgrade for restoring the UC applications.

- Restore Unified CM and IM and Presence, on page 18
- Restore Cisco Emergency Responder, on page 21

Step 5 Validate UC Application, on page 21

Perform these post upgrade checks after upgrade for validating the applications.

- Validate Unified CM and IM and Presence, on page 21
- Validate Unity Connection, on page 22

Note Use the HCM-F Release 11.5(4) SU1 interface, to perform validation by executing the upgrade checks before and after upgrade. Use the results for post upgrade validation. The post upgrade validation is supported on Unified CM, Unified CM IM and Presence, and Cisco Unity Connection. To understand the checks that are used for comparison, see Upgrade Comparison, on page 44. For executing the comparison, see Post Upgrade Comparison, on page 43.

Plan - Pre Upgrade Checks

This section helps you to:

- Determine the scope of your upgrade.
- Understand the hardware, software and component compatibility.

Note Upgrades can take a long time, depending on the number of customers to be migrated, or the size of individual customers.

Upgrading single customer's UC Application cluster (such as Cisco Unified Communications Manager, Cisco Unity Connection, or Cisco Emergency Responder) may require more than one maintenance window for larger customers.

The following table provides approximate time that is required for upgrade:

Table 1: Time Estimate for Upgrade

	Components considered	Approximate time taken	
		Refresh	Standard (includes upgrade and switch version time)
DC Component	ESXi	ESXi	Approximately 30 minutes per blade depending on the Data Center environment.
Management Applications	Unified CDM	-	4 hrs (standalone)
	HCM-F	-	1 hr
	PLM	-	30 min
	PCD	-	1 hr 50 min

	Components considered	Approximate time taken	
		Refresh	Standard (includes upgrade and switch version time)
Unified Communications Applications	Unified CM PUB	3 hrs	4 hrs per node (through PCD)
	Unified CM SUB	3 hrs	4 hrs per node (through PCD)
	Unity Connection PUB	3 hrs	4 hrs per node (through PCD)
	Unity Connection SUB	3 hrs	4 hrs per node (through PCD)
	IM and Presence PUB	3 hrs	4 hrs per node (through PCD)
	IM and Presence SUB	3 hrs	4 hrs per node (through PCD)
	CER PUB	3 hrs	4 hrs per node (through PCD)
	CER SUB	3 hrs	4 hrs per node (through PCD)

For information about Refresh and Standard upgrade, see *Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.

Prime Collaboration Deployment for UC Applications

Cisco Prime Collaboration Deployment helps you to manage Unified Communications (UC) applications. Its functions are to:

- Migrate a cluster of UC servers to a new cluster (such as MCS to virtual, or virtual to virtual).

Tip Cisco Prime Collaboration Deployment does not delete the source cluster VMs after migration is complete. You can fail over to the source VMs if there is a problem with the new VMs. When you are satisfied with the migration, you can manually delete the source VMs.

- Perform operations on clusters, such as:
  - Upgrade
  - Switch version

- Restart

- Fresh install a new release UC cluster
- Change IP addresses or hostnames in clusters (for a network migration).

  Cisco Prime Collaboration Deployment supports simple migration and network migration. Changing IP addresses or hostnames is not required for a simple migration. For more information, see the Prime Collaboration Deployment Guide.

The functions that are supported by the Cisco Prime Collaboration Deployment can be found in the Prime Collaboration Deployment Administration Guide.

Use the **Cluster Discovery** feature to find application clusters on which to perform fresh installs, migration, and upgrade functions. Perform this discovery on a blade-by-blade basis.

For more information about features, installation, configuration and administration, best practices, and troubleshooting, see the following documents:

- Prime Collaboration Deployment Administration Guide
- Release Notes for Cisco Prime Collaboration Deployment

Maintenance Windows and Time Estimates

Customer upgrades can take a long time, depending on the number of customers you upgrade or the size of individual customers. Upgrading an entire customer (including Cisco Unified Communications Manager, IM and Presence, Cisco Unity Connection, Cisco Emergency Responder, Attendant Console, and customer premises equipment) may require more than one maintenance window. Therefore, you can break Phase 4 into multiple maintenance windows while still following the overall upgrade order described in this guide.

At a minimum, perform customer upgrades in a separate maintenance window from any previous upgrade phases involving Cisco HCS management applications and telephony aggregation components.

For virtual machine upgrades to support newer VMware hardware and tools for UC applications, the following link describes the supported upgrade processes: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-software-requirements.html. Each VM must be running on a blade that has been upgraded to the latest version before the VM may be upgraded. For more information, see VMware Knowledge Base article 1010675, *Upgrading a virtual machine to the latest hardware version*: http://kb.vmware.com/selfservice/microsites/microsite.do.

Plan - Unified CM and Unified CM IM and Presence

Perform the following checks. You can use UI or CLI to complete the tasks or checks provided in the Command or Action column. To complete the check using UI, use the reference or use the command in CLI.

Procedure

	Command or Action	Purpose
Step 1	Check the network health (Network and Database) by performing these checks:	• Factors that Affect Upgrade Time Requirements • Generate a Database Status Report

	Command or Action	Purpose
		• Check Database Replication • Check Performance Reports • Run CLI Diagnostics • Check Network Connectivity, on page 8 The health of your system affects the amount of time that an upgrade requires. You can reduce the amount of time needed for an upgrade by ensuring that your system meets the conditions. Complete and repeat the steps for all upgrade and migration methods.
Step 2	Check device name. In Cisco Unified Communications Manager Administration, use the **Device** > **Phone** menu path to check **Device Name**.	Device name for the Cisco Unified Mobile Communicator device should be less than 15 characters.
Step 3	Ensure that there are no expired certificates on the partition, including any trust certificates in the certificate chain. To verify if certificates are valid, use the following commands in CLI: **show cert list own** and **show cert own** certificate**.pem**. If there are expired certificates, perform one or more of the following procedures: • Delete a Trust Certificate • Regenerate a Certificate if an identify certificate is expired. To check expired certificates in HCM-F 11.5(4), go to **Infrastructure Manager** > **Service Provider Toolkit** > **Certificate Monitoring** > **UC Applications** and select Collect Certificates.	**Note** Display fails if there are errors or certificate expires. Perform this step for refresh upgrades on Cisco Unified Communications Manager and IM and Presence Service nodes only. Expired certificates are not imported during a refresh upgrade. As a result, a new certificate is generated during upgrade process and can cause errors.
Step 4	Do any one of the following: • Check Connectivity between IM and Presence and Cisco Unified Communications Manager • To find PUB on IM and P, use the following commands in CLI: **utils network ping** <ip CUCM pub> and **utils dbreplication status**.	Verify that the IM and Presence Service node has connectivity with Cisco Unified Communications Manager. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade. See Upgrade section in Migration to Cisco Unified Communications Manager Using Prime Collaboration Deployment document.
Step 5	Do any one of the following: • Collect Configuration and Login Information • To record the current configuration and login information, use the following commands in CLI: **show network eth0** and **utils service list**	Record the current configuration and login information for your Unified Communications Manager nodes in case any issues are encountered during the upgrade process.
Step 6	Do any one of the following: • Record the Registered Device Count	Use the Real Time Monitoring Tool (RTMT) to capture the device count so that you can verify your endpoints and

	Command or Action	Purpose
	• To compare the output, use the following command in CLI: **show risdb query phone**	resources after the upgrade is complete. You can also use this information to verify that you have not exceeded the capacity of the virtual machine (VM) that you are deploying. Do this step for all upgrade and migration methods.
Step 7	Record the Number of Assigned Users	Record the number of assigned users on IM and Presence Service nodes so that you can verify this information after the upgrade is complete. Do this step for all upgrade and migration methods.
Step 8	Record TFTP Parameters	The upgrade process changes a TFTP parameter. Record the current setting so that you can reset the parameter after the upgrade is complete.
Step 9	Do any one of the following: • Record Enterprise Parameters • To record the enterprise parameters, use the following command in CLI: **show tech params enterprise**	Record the settings for Enterprise Parameters on both Unified Communications Manager nodes and IM and Presence Service nodes. Some Enterprise Parameters exist on both types of nodes and the settings that are configured on Unified Communications Manager nodes may overwrite the settings configured on IM and Presence Service nodes during an upgrade. Record the settings so that you can restore them as needed after the upgrade is complete. Do this step for all upgrade and migration methods.
Step 10	Check the Available Common Partition Space	Verify that you have enough common partition space for the upgrade. Typically, you need at least 25G of common partition space; however, your deployment may require more space if you have a lot of TFTP data (device firmware loads), music-on-hold (MOH) files, or if you have many locale files installed. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 11	If you do not have enough common partition space, perform one or more of the following procedures: • Adjust High and Low Watermarks • Maximize Usable Disk Space	Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade. **Note** Performing an upgrade without sufficient disk space can cause the upgrade to fail.
Step 12	Ensure that you have the necessary license files for the new release. You must migrate from PLM to Smart licensing for HCS UC Applications, see the Upgrade to Smart Licensing topic in the https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/hcs/12_5/HCS_Solution/Smart_Licensing/chcs_b_hcs-smart-licensing-guide/chcs_b_	

	Command or Action	Purpose
	hcs-smart-licensing-guide_chapter_011.html#task_BFE71556B8258D5C5249399937AC44F2 for details.	
Step 13	Verify Critical Services	Verify that all critical services are activated.

What to do next

See Plan - Cisco Unity Connection, on page 8.

Check Network Connectivity

Use this procedure to verify connectivity between all nodes and services in your network.

Step 1 Start a CLI session using one of the following methods:

- From a remote system, use SSH to connect securely to the Cisco Unified Operating System. In your SSH client, enter your **ssh *adminname@hostname*** and enter your password.
- From a direct connection to the serial port, enter your credentials at the prompt that displays automatically.

Step 2 Execute the **show network cluster** command on each node in your network to verify communication between servers in the cluster.

Step 3 If you have an NTP server, execute the **utils ntp status** command to verify connectivity to the NTP server.

Step 4 If you have an SMTP server, ping the server to verify connectivity.

Step 5 If you are using DNS, execute the **show network eth0** command on each node in your network to verify that the DNS and domain are configured.

Step 6 Check that DNS name resolution is working correctly:

a) Ping the FQDN of each node to ensure that it resolves to the IP address.

b) Ping the IP address of each to ensure that it resolves to the FQDN.

Plan - Cisco Unity Connection

Perform the following steps:

SUMMARY STEPS

1. Ensure that you have a good network connection to avoid service interruptions during upgrade.
2. Check the network reachability to FTP or SFTP server.
3. Check the server status in a cluster and confirm the running state of database replication. Publisher and subscriber servers must be active for answering the calls. This check can be done through CUC Servicebility UI or Publisher CLI.
4. Before upgrading to the release 11.x, rename the notification templates if created. To check the notification templates, login to CUC Publisher and navigate to Cisco Unity Connection Administration Page. Then, navigate to **Templates** > **Notification Templates** > **Notification Templates**.

DETAILED STEPS

Step 1 Ensure that you have a good network connection to avoid service interruptions during upgrade.

To check the network reachability to subscribers, DNS and default gateway, login to Publisher admin CLI and use the following commands:

a. # **utils network ping** <CUC_Subscriber_IP>

b. # **utils network ping** <Default_Gateway_IP>

c. # **utils network ping** <DNS_IP>

Step 2 Check the network reachability to FTP or SFTP server.

To check the network reachability to FTP or SFTP server, login to Publisher admin CLI and use the following command in CLI:

#**utils network ping** <SFTP_Server_IP>

Step 3 Check the server status in a cluster and confirm the running state of database replication. Publisher and subscriber servers must be active for answering the calls. This check can be done through CUC Servicebility UI or Publisher CLI.

To confirm if the server in a cluster is active, do any one of the following:

- Perform the following steps through CUC Serviceability UI:
  a. Sign in to CUC Serviceability UI.
  b. Expand **Tools** and select **Cluster Management**.
- Use the following commands on Publisher CLI:
  a. #**utils service list**
  b. # **show cuc cluster status**
  c. # **utils dbreplication runtimestate**

Step 4 Before upgrading to the release 11.x, rename the notification templates if created. To check the notification templates, login to CUC Publisher and navigate to Cisco Unity Connection Administration Page. Then, navigate to **Templates** > **Notification Templates** > **Notification Templates**.

Rename the notification templates if created with the below mentioned names:

- Default_Missed_Call_With_Summary
- Default_Scheduled_Summary
- Default_Voice_Message_With_Summary
- Default_Dynamic_Icons
- Default_Actionable_Links_Only

What to do next

See Plan - Cisco Emergency Responder , on page 10.

Plan - Cisco Emergency Responder

Perform the following steps as part of planning phase for Cisco Emergency Responder.

Step 1 Ensure to migrate from PLM to Smart licensing.

Request for hosted license for CER from License tool. For information about license, see *Cisco Emergency Responder Administration Guide* at https://www.cisco.com/c/en/us/support/unified-communications/emergency-responder/products-maintenance-guides-list.html.

Step 2 Unassign the UC clusters from PLM.

Select the PLM under **License Management** > **License Management Summary**. Unassign the clusters which you plan to upgrade to 12.5 from cluster management section.

Step 3 In the HCM-F, sync the version of the UC applications from the Smart account. See Upgrade to Smart Licensing topic in the Cisco Hosted Collaboration Solution Smart Licensing Guide, Release 12.5(1) SU1 guide for details.

What to do next

See Prepare - Pre Upgrade Actions, on page 10.

Prepare - Pre Upgrade Actions

This section helps you to complete the pre-upgrade tasks for the following Collaboration Applications and prepare for upgrade. Perform the following procedures to complete the pre-upgrade actions:

Step 1 Prepare - Unified CM and Unified CM IM and Presence , on page 10

Provides steps to follow before upgrading CUCM.

Step 2 Prepare - Cisco Unity Connection, on page 13

Provides steps to follow before upgrading CUC.

Prepare - Unified CM and Unified CM IM and Presence

Perform the following steps. You can use UI or CLI to complete the tasks or checks provided in the Command or Action column. To complete the check using UI, use the reference or use the command in CLI.

Procedure

	Command or Action	Purpose
Step 1	Take a Fresh Backup, see Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service for detailed procedure.	You must create a fresh backup file. Do this step for all upgrade and migration methods. **Note** You may lose data or you may be unable to restore your system if your backup is outdated. If you have custom ringtones or background images in the TFTP directory, you need to create a separate backup for these files. They are not included in the Disaster Recovery System (DRS) backup file. See Back Up Custom Ringtones and Background Images topic in the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service.
Step 2	Export User records, follow steps in the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service.	Export user records using the Bulk Administration Tool (BAT). Do this step for all upgrade and migration methods.
Step 3	Upgrade IP Phone Firmware, follow steps in the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service.	You can upgrade your IP phones to the firmware that corresponds to the new release as a pre-upgrade task. Although IP phones automatically download their new firmware after an upgrade, you can choose to apply new firmware files to the endpoints in a controlled manner prior to the upgrade in order to minimize phone downtime after an upgrade. Do this step for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 4	Do any one of the following: • Deactivate Cisco Extension Mobility, use steps mentioned in the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service. • To deactivate the service, use the following CLI command: **utils service stop** service name.	Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade. **Note** EM users who are already logged in can make calls normally and will remain logged in. Only, logout of existing EM users and login of fresh EM users will not work.
Step 5	Do any one of the following: • Deactivate TFTP services, use steps mentioned in the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service. • To deactivate the service, use the following CLI command: **utils service stop** service name.	Stop TFTP services on CUCM nodes before you begin an upgrade.

	Command or Action	Purpose
Step 6	Do any one of the following: • Stop the IM and Presence Sync Agent, use steps mentioned in Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service. • To deactivate the service, use the following CLI command: **utils service stop** service name.	If you need to upgrade CUCM as part of your IM and Presence upgrade, you need to stop the IM and Presence Sync Agent service before you begin the upgrade process. Do this step for only for direct upgrades, which use either the CUCM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 7	Do any one of the following: • For more information, see the "Pre-Upgrade Task Flow" and "Post-upgrade Task Flow" sections in the Upgrade and Migration Guide for Cisco Unified Communications Manager and IM and Presence Service. • To check if the COP file is available, use the following commands in CLI: **sh version active** and **sh version inactive**	Download the upgrade files for the CUCM and the IM and Presence Service. **Note** For refresh upgrades, you must also download the upgrade COP files. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 8	Increase the Data Replication Timeout, follow steps mentioned in the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service.	Optional. This procedure applies to the CUCM publisher node only. Use this procedure when you upgrade large clusters. If you increase the database replication timeout, you need to restore the timeout to the default value after the entire cluster upgrades and the CUCM subscriber nodes have successfully set up replication. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 9	Disable High Availablility on Presence Redundancy Groups, follow steps mentioned in the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service.	This procedure applies to IM and Presence Service nodes only. If you have configured presence redundancy groups for high availability, you need to disable it during the upgrade process. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 10	Add a Serial Port to the Virtual Machine, follow steps mentioned in the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service.	Add a serial port to the virtual machine so that you can dump logs in the event of an upgrade failure. Perform this procedure for all nodes. **Note** Shut down and power on the VMs in the following order: **a.** Unified CM PUB **b.** Unified CM SUB **c.** IM and Presence PUB **d.** IM and Presence SUB

	Command or Action	Purpose
		Do this step for all upgrade and migration methods.
Step 11	Subnet mask correction. To verify the subnet mask, use the following command in CLI: **set network ip eth0** server_ip_address **255.255.255.0**.	

Prepare - Cisco Unity Connection

Perform the following steps as part of prepare phase for CUC.

Step 1 Determine if you need COP files depending on the upgrade process.

Use the https://software.cisco.com/download/home/280082558 link and select the Unity Connection Release for downloading the COP files.

Step 2 Backing Up and Restoring Cisco Unity Connection Components

Backup all the existing data.

To backup existing data, use the following command in CLI: **utils disaster_recovery history backup**.

Step 3 Confirm the status of publisher and subscriber servers. Both the servers must be active and answer calls.

Perform the following steps to confirm the server status in a cluster:

a. Sign in to Cisco Unity Connection Serviceability.

b. Expand Tools and select **Cluster Management**.

c. Check the server status in a cluster.

d. Confirm the running state of database replication.

To confirm the status of Publisher and Subscriber, use the following commands on Publisher CLI:

a. **# utils service list**

b. **# show cuc cluster status**

c. **# utils dbreplication status**

d. **# utils dbreplication runtimestate**

Step 4 Initiate a pre-upgrade test before starting the upgrade process.

On the CUC Publisher Admin CLI, enter the following command to initiate a pre-upgrade test:

run cuc preupgrade test

Note The Refresh Upgrade of CUC node automatically switches version after upgrade, and do not require a separate switch command from UaaS service to the nodes.

Back Up and Restore Cisco Unity Connection Components

Upgrade UC Application

This section lists the upgrade tasks for Unified CM, Unified CM IM and Presence, Cisco Emergency Responder, and Cisco Unity Connection through Refresh or Standard upgrade.

Initiate Refresh or Standard upgrade depending on the upgrade method followed to upgrade ESXi, VMware, VMs, and Management Components.

Upgrade UC Applications using Refresh Upgrade

Perform the following tasks for upgrading UC Applications using Refresh Upgrade. Ensure to complete the following steps in sequence for Refresh Upgrade:

1. Compatibility and Documentation References
2. Upgrade ESXi,VMware,and VM, see https://www.vmware.com/support/pubs/ for details.

Follow the upgrade steps described in the following table in sequence for the refresh upgrade:

Table 2: Upgrade Tasks for Refresh Upgrade

Upgrade Step	Action
UC Applications	
1	**Order of upgrade** **a.** Unified CM PUB and switch version are set to No. **b.** Unified CM SUB and switch version are set to No. **c.** IM and Presence PUB and switch version are set to No. **d.** Upgrade Unified CM PUB version. **e.** Upgrade CM SUB version. **f.** Upgrade IM and Presence PUB version. **g.** Switch Unified CM PUB and SUB version. **h.** Switch IM and Presence PUB version. **Note** IM and Presence Subscriber node switch version is paused until the Publisher switch version is complete. You must manually verify the publisher switch version, and manage the upgrade to proceed further. **i.** By default, Unity Connection PUB and switch version are set to Yes. The switch version happens automatically once upgrade is triggered. **j.** By default, Unity Connection SUB and switch version are set to Yes.

Upgrade Step	Action
Unified CM	
2	Delete the product instances in the co-resident ELM.
PLM	
4	**Unassign the UC clusters from PLM** Select the PLM under ***License Management > License Management Summary***. Unassign the clusters which you plan to upgrade to 12.5 from cluster management section.
HCM-F	
5	In the HCM-F, sync the version of the UC applications from the Smart account. See Upgrade to Smart Licensing topic in the Cisco Hosted Collaboration Solution Smart Licensing Guide, Release 12.5(1) SU1 guide for details.

Upgrade UC Applications using Standard Upgrade

Perform the following tasks for upgrading UC Applications using Standard Upgrade. Ensure to complete the following steps in sequence for Standard Upgrade:

1. Compatibility and Documentation References
2. Upgrade ESXi,VMware,and VM, see https://www.vmware.com/support/pubs/ for details.
3. Upgrade Management Components

Follow the upgrade steps described in the following table in sequence for the standard upgrade:

Table 3: Upgrade Tasks for Standard Upgrade

Upgrade Step	Action	Approximate time taken
1	**Order of upgrade** **a.** Unified CM PUB and switch version are set to No. **b.** Unified CM SUB and switch version are set to No. **c.** IM and P PUB and switch version are set to No. **d.** Upgrade Unified CM SUB version. **e.** Upgrade Unified CM PUB version. **f.** Upgrade IM and P PUB version. **g.** Switch version for Unified CM SUB and PUB version. **h.** Switch version for IM and P PUB. **i.** By default, Unity Connection PUB and switch version are set to Yes. **j.** By default, Unity Connection SUB and switch version are set to Yes	
Unified CM		
2	**Upgrade Unified CM cluster from PCD** Unified CM PUB and Unity Connection PUB upgrade starts at the same time when the PCD and CER PUB starts manually. As part of Unified CM cluster, the following applications are upgraded: • Unified CM PUB • Unified CM SUB • IM and Presence PUB • IM and Presence SUB For detailed procedure, see the chapter *Upgrade, Migration, and Configuration* in Migration to Cisco Unified Communications Manager Release Using Prime Collaboration Deployment.	(Day 3) 3 to 3.5 hrs per node

Upgrade Step	Action	Approximate time taken
3	**Upgrade the Unity Connection cluster from PCD** Unified CM PUB and Unity Connection PUB upgrade starts at the same time when the PCD and CER PUB starts manually. As part of Unity Connection cluster, the following applications are upgraded: • Unity Connection PUB • Unity Connection SUB See *Upgrade CUCM/CUC/CUCM IM &P with Prime Collaboration Deployment* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-configuration-examples-list.html.	(Day 3) 3 to 3.5 hrs per node
Cisco Emergency Responder		
4	**Upgrade the CER cluster manually** Unified CM PUB and Unity Connection PUB upgrade can be started at the same time when the PCD and CER PUB starts manually. For information about the upgrade procedure, see section Software Upgrades in Cisco Emergency Responder Administration Guide.	(Day 3) 3 to 3.5 hrs per node
UC Applications Switch Version		
5	**Initiate switch version of Unified CM cluster from PCD** For detailed procedure, see the chapter *Upgrade, Migration, and Configuration* in Migration to Cisco Unified Communications Manager Release Using Prime Collaboration Deployment.	(Day 3) 30 min per node
6	**Initiate switch version of Unity Connection cluster from PCD** See *Upgrade CUCM/CUC/CUCM IM &P with Prime Collaboration Deployment* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/pcdadmin/12_5_1/cucm_b_pcd-admin-guide_126.html.	(Day 3) 30 min per node
CER Switch Version		
7	**Switch version CER PUB and SUB 12.5** For information about the upgrade procedure, see section Software Upgrades in Cisco Emergency Responder Administration Guide.	(Day 3) 30 min per node
Unified CDM		
8	**Change the version of UC applications in Unified CDM** See Set Up Cisco Unified Communications Manager Servers procedure in *Cisco Hosted Collaboration Solution Customer Onboarding Guide*.	(Day 3) 5 min
PLM		

Upgrade Step	Action	Approximate time taken
9	**Unassign the UC clusters from PLM** Select the PLM under ***License Management > License Management Summary***. Unassign the clusters which you plan to upgrade to 12.5 from cluster management section.	
HCM-F 11.5(x)		
10	**Sync HCM-F to Smart Account** In the HCM-F, sync the version of the UC applications from the Smart account. See Upgrade to Smart Licensing topic in the Cisco Hosted Collaboration Solution Smart Licensing Guide, Release 12.5(1) SU1 guide for details.	

Upgrading UC Applications for IP Telephony Customers

Upgrade all of the UC applications and components for one customer before you upgrade the UC applications and components for another customer.

The following upgrade strategies are for IP telephony components, based on the size of the deployment.

- Single-window upgrade: Recommended for small single-site or multi-site installations. For more information, see Single Maintenance Window Procedures and Sequence.
- Multi-window system upgrade: Recommended for medium or large single-site and medium multi-site installations. For more information, see Multiple Maintenance Windows Upgrade Sequence.

Note For Contact Center deployments, see "Appendix A: Upgrading Cisco HCS for Contact Center.

Restore UC Application

This section describes the procedures for restoring the services after the UC app upgrade.

Restore Unified CM and IM and Presence

Procedure

	Command or Action	Purpose
Step 1	Switch the software version, see the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service guide for details.	If you did not switch versions immediately after completing the upgrade, do so now. You must switch versions so that the upgrade is complete and all nodes in the cluster are updated. Do not perform a backup until you have switched to the new software version.

	Command or Action	Purpose
		Perform this procedure for all nodes.
Step 2	Remove the Serial Port, see the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service guide for details.	During the preupgrade tasks, you added a serial port to the virtual machine to capture the upgrade logs. After you have successfully upgraded the system, you must remove the serial port so that it does not impact the performance of the virtual machine. Perform this procedure for all nodes.
Step 3	Restart Extension Mobility, see the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service guide for details.	If you deactivated Cisco extension mobility as part of your preupgrade tasks, use this procedure to restart the service after the upgrade is complete.
Step 4	Restart TFTP Services, see the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service guide for details.	Use this procedure to restart TFTP services on Cisco Unified Communications Manager nodes after you complete an upgrade.
Step 5	Reset TFTP Parameters, see the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service guide for details.	Reset TFTP parameters that are changed during the upgrade process.
Step 6	Restore Enterprise Parameters, see the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service guide for details.	Use this procedure to restore Enterprise Parameters on IM and Presence Service nodes that may have been overwritten during the upgrade process.
Step 7	Reset High and Low Watermarks, see the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service guide for details.	Use this procedure to restore the high and low watermarks to their original values in order to avoid premature purging of traces. Do this step for only for direct upgrades, which use either the Unified CM OS Admin interface or the PCD Upgrade task to perform the upgrade.
Step 8	Updating VMware Tools, see the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service guide for details.	Update the VMWare Tools after you complete the upgrade. Perform this procedure for all nodes.
Step 9	Install Locales, see the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service guide for details.	Use this procedure to install locales. After an upgrade, you must reinstall any locales that you are using, with the exception of US-English, which is installed by default. Perform this procedure for all nodes.
Step 10	Restore the Database Replication Timeout, see the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service guide for details.	Use this procedure if you increased the database replication timeout value before you began the upgrade process. Perform this procedure on Cisco Unified Communications Manager nodes only.
Step 11	Upgrade RTMT, see the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service guide for details.	If you use Cisco Unified Real Time Monitoring Tool (RTMT), upgrade to the new software version.

	Command or Action	Purpose
Step 12	Manage TFTP Server Files, see the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service guide for details.	Optional. Use this procedure to upload phone rings, callback tones, and backgrounds to a TFTP server so that they are available to Cisco Unified Communications Manager nodes.
Step 13	Set Up a Custom Log-On Message, see the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service guide for details.	Optional. Upload a text file that contains a customized log-on message that appears in Cisco Unified Communications Operating System Administration, Cisco Unified CM Administration, Cisco Unified Serviceability, Disaster Recovery System Administration, Cisco Prime License Manager, and the command line interface. Perform this procedure on Cisco Unified Communications Manager nodes only.
Step 14	Configure IPSec Policies, see the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service guide for details.	Use this procedure only if you are performing a PCD migration from Release 6.1(5). Recreate your IPSec policies after the PCD migration is complete, because IPSec policies from Release 6.1(5) are not migrated to the new release.
Step 15	Assign New Manager Assistant Roles, see the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service guide for details.	Perform this procedure only if your previous release was configured to use the Cisco Unified Communications Manager Assistant feature, and you assigned application users to use either the Inter-Cluster Peer-User or the Admin-CUMA roles. The InterCluster Peer-User and Admin-CUMA roles are deprecated and are removed during the upgrade process. Assign new roles for those users. Perform this procedure on Cisco Unified Communications Manager nodes only.
Step 16	Enable High Availability on Presence Redundancy Groups, see the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service guide for details.	This procedure applies to IM and Presence Service nodes only. If you disabled high availability on presence redundancy groups before beginning the upgrade process, use this procedure to enable it now.
Step 17	Restart the IM and Presence Sync Agent, see the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service guide for details.	If you stopped the IM and Presence Sync Agent service before you began the upgrade process, restart it now.
Step 18	(Optional) To upgrade JTAPI application, from Cisco Unified CM Administration, choose **Application** > **Plugins** and download the JTAPI installer. Then, follow the instructions in the Cisco Unified JTAPI Developers Guide: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html	Upgrade your JTAPI application, if necessary.

Restore Cisco Emergency Responder

Procedure

	Command or Action	Purpose
Step 1	Replace the files if CER uses secure JTAPI connection.	If Cisco Emergency Responder uses secure JTAPI connection, the `CTLfile.tlv`, `JtapiClientKeyStore`, and `JtapiServerKeyStore` files can get deleted after the upgrade. Use the following options as a workaround: • Copy the `CTLfile.tlv`, `JtapiClientKeyStore`, and `JtapiServerKeyStore` files from `/partB//usr/local/CER/lib` to `/usr/local/CER/lib` location and restart the Cisco Emergency Responder service. **Note** Access to the root account is required to copy the files. • Regenerate the CAPF profile on Unified CM for the Cisco Emergency Responder application user that is used for controlling route points and CTI ports. See Cisco Unified JTAPI Developers Guide for information: https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html.

Validate UC Application

This section describes the checks for validating the UC applications upgrade.

Validate Unified CM and IM and Presence

Procedure

	Command or Action	Purpose
Step 1	See the Verify the Registered Device Count topic in the Upgrade and Migration Guide for Cisco Unified Communications Manager guide.	Use this procedure to verify your endpoints and resources on Cisco Unified Communications Manager nodes after the upgrade is complete.
Step 2	See the Verify Assigned Users topic in the Upgrade and Migration Guide for Cisco Unified Communications Manager guide.	Use this procedure to verify the number of assigned users on IM and Presence Service nodes after the upgrade is complete.

	Command or Action	Purpose
Step 3	See the Test Functionality topic in the Upgrade and Migration Guide for Cisco Unified Communications Manager guide.	Verify phone functions and features are working correctly after the upgrade.

Validate Unity Connection

Procedure

	Command or Action	Purpose
Step 1	Verify the version of CUC server in CLI using the command: **`show cuc version`**.	Cisco Unity Connection server active and inactive version details.
Step 2	Verify the CUC upgrade status in CLI using the command: **`utils system upgrade status`**.	Cisco Unity Connection upgrade status details.

Upgrade Toolkit Overview

The Upgrade Checks for UC applications using HCM-F 11.5(4) SU1 and later enables partners to perform a quick and hassle free:

- Checks before and after upgrade.
- Use the results obtained from upgrade checks (before and after) to validate upgrade.
- Understand the deprecated phones in the network.

HCM-F has information of the UC applications and various other devices in partner network. This information is used along with the information available from compatibility matrices to build a rich source of data useful for partners.

For information about API, see *Cisco Hosted Collaboration Mediation Fulfillment Developer Guide*.

Limitations

There are limitations for the following scenarios:

Scenario	Tasks or Error Message
Upgrading Cisco Unified IM and Presence from Release 11.5(x) to 12.5(x)	While upgrading from 11.5(x), keep the Cisco Unified Communications Manager IM and P and Cisco Unified Communications Manager clusters separate until the **Upgrade Comparison** is complete. After completing and verifying the comparison results, delete the Unified CM I and P cluster and add it to Cisco Unified Communications Manager.
Upgrade Check - Cluster Version Information	When Cisco Unified Communications Manager IM and P is a separate cluster in Release 11.5(x)/12.5(x), node count fails with node count as 0.

Scenario	Tasks or Error Message
Upgrade Check - Phone Count and CTI Device Count	Phone count does not appear for phones with status **None**.

Upgrade Toolkit Prerequisites

The following prerequisites are required to perform upgrade checks, upgrade comparison and phone compatibility check:

Note Ensure to upgrade HCM-F version to 11.5(4)SU1 or later to use the upgrade checks.

S.No	Checks	Path/Reference
1	Activate the following services to perform upgrade checks and comparison post upgrade: To verify if the services are started, do any one of the following: • In HCM-F, select **Infrastructure Manager** > **Service Provider Toolkit**. • Enter the following command in CLI: **utils service list**	
	UC Monitor	**utils service activate Cisco HCS UC Monitor Service**
	Cisco HCS CAA CUCM Service	**utils service activate Cisco HCS CAA CUCM Service**
	Cisco HCS CAA IMP Service	**utils service activate Cisco HCS CAA IMP Service**
	Data Access Manager (DAM) **Note** This service is active by default.	**utils service activate Cisco HCS Data Access Manager Service**
	Cisco HCS CAA UCXN Service	**utils service activate Cisco HCS CAA UCXN Service**
	Cisco HCS CAA CER Service	**utils service activate Cisco HCS CAA CER Service**
	Cisco HCS UCSM Sync Service	**utils service activate Cisco HCS UCSMSync Service**
	Cisco HCS VCenter Sync	**utils service activate Cisco HCS VCenterSync Service**
2	Certificate scheduling and email notification must be configured or collect the certificates on-demand.	For configuration, see Certificate Configuration in *Cisco Hosted Collaboration Solution Upgrade and Migration Guide*.

S.No	Checks	Path/Reference
3	Check if all customers and their clusters for the UC applications are added. Supported UC applications: Cisco Unified CM, Cisco Unity Connection and Cisco UCM IM and P.	To test the cluster connection, see Test Cluster Connection procedure in *Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide* .
4	While adding new clusters for the UC applications, ensure to select the **Access Type** as **Platform** and **Admin**	Path: **Infrastructure Management** > **Application Management** > **Cluster Application** > **Add New** > **Credentials**
5	Check if vCenter is configured for each vCenter server deployed in the Data Center and VCenter sync is enabled.	Path: **Infrastructure Management** > **Data Center Management** > **Data Center** > **vCenter**. For configuration information, see Add vCenter procedure in *Cisco Hosted Collaboration Mediation Fulfillment Install and Configure Guide* .

Upgrade Toolkit Workflow

Complete the following tasks to perform the upgrade.

Before you begin

Upgrade Toolkit Prerequisites, on page 23

Step 1 Perform Upgrade Checks, on page 25

Perform upgrade checks on the UC application clusters before the upgrade. Ensure all checks pass.

Step 2 Verify the job status in the HCM-F interface.

Check the **Status** column for the **Job Entity**, **UC Monitor** in the path: **Infrastructure Manager** > **Administration** > **Jobs**.

Note If the job fails, go to **Upgrade Checks** and check the **Status** column for failures and Recommended Action.

Step 3 Click **Save for Compare** to save the check result after executing all the checks before upgrade.

Step 4 Perform the Phone Compatibility Check to understand the deprecated phone models.

Step 5 Remove the deprecated phone models.

To remove the deprecated phone models, see Delete Phones procedure in *Cisco Hosted Collaboration Solution End-User Provisioning Guide*.

Step 6 Perform the steps mentioned in Prepare-Pre Upgrade Actions, Upgrade UC Applications, and Restore-Post Upgrade Actions procdures to upgrade the UC Applications.

To understand end-to-end UC upgrade workflow, see *Cisco Hosted Collaboration Solution Upgrade and Migration Guide*.

Step 7 Perform Upgrade Checks, on page 25

Perform upgrade check on the UC application clusters after the upgrade.

Step 8 Click **Submit** after executing the checks post upgrade.

Step 9 Post Upgrade Comparison, on page 43

Compares and displays the check results obtained before and after upgrade.

Perform Upgrade Checks

Perform upgrade checks on the UC application clusters and vCenter.

Before you begin

Upgrade Toolkit Prerequisites, on page 23

Step 1 From the side menu, choose **Service Provider Toolkit** > **Upgrade Toolkit** > **Upgrade Checks**.

Step 2 From **Select a Customer** drop down, select the customer name for performing the checks.

Step 3 From **Select a Cluster** drop down, select the UC application cluster. On selecting a shared cluster, it displays the name of customers associated with the selected shared cluster.

Note If upgrade checks are performed for the first time, **Not Executed** appears in the **Status** column. If a check is already performed, then the status of the check appears (tick or cross-mark).

Step 4 By default, all the checks are selected. To perform a particular check, uncheck the check box from the table header and select the individual checks using the check box.

Note Ensure to perform all the checks.

Step 5 Click **Submit** to perform the selected checks.

Step 6 (Optional) Check the job status.

Select **Infrastructure Manager** > **Administration** > **Jobs**. Check for Job Entity, UC Monitor Checks.

Note You can run the upgrade check on different clusters for the same customer at the same time. But, if another upgrade check for the same cluster associated with the same customer is initiated, then the initiation fails. Also, a message appears that the job is in progress.

Step 7 In the **Status** column, the tick-mark appears if the check is successful and cross-mark appears if the check fails. Click the cross-mark in the **Status** column to understand the recommended action for the entire check as well as the individual check result:

- **Status**: Indicates the check failed.
- **Last Execution Date/Time**: Indicates the time when the check was last executed.
- **Recommended Action**: Indicates the recommended action for the check failure.

To understand the details of the check, click the arrow button to expand the check in the **Check** column. The tick-mark appears if the collection is successful. Cross-mark appears if the HCM-F is unable to collect the details from all the clusters during the check. It can be due to any of the following reasons:

- Node not reachable
- Check was not complete.

Note On the table header, click **Checks** to sort the table alphabetically or click **Status** to sort the table based on the execution status.

Manually perform and verify the skipped checks.

Step 8 Complete these steps to save the check result and use it for comparison depending on when the Upgrade Check is performed:

a. **Before Upgrade**: Click **Save for Compare**.

b. **After Upgrade**: Click **Submit**.

Note Use **Save for Compare** only to save the *Check Result* before upgrade. If it is selected after upgrade, the check result saved before the upgrade is overwritten.

Perform this step only after performing all the checks before upgrade.

a) (Optional) Click **Download** to download (present) check results.

The *Check Result* are saved to `UpgradeChecksReport_<clustername>_<timestamp in yyyymmdd_hhmmss>.csv`.

b) (Optional) Click **Download Saved Reports** to download the last saved results.

The *Check Result* are saved to `UpgradeSavedChecksReport_<clustername>_<timestamp in yyyymmdd_hhmmss>.csv`.

c) (Optional) Select **Open File** to view the spreadsheet without saving or select **Save File** to save it to a location and click **OK**.

Upgrade Checks

The following checks involve checking all or some nodes (Subscriber and Publisher) in the UC application cluster for the selected customer.

Even if one node fails while executing a check, the entire check fails and cross-mark appears in the **Status** column. See the **Recommended Action** and perform the recommended action if there is a failure and execute the check again.

Table 4: Upgrade Checks

Upgrade Checks	Is Upgrade Check Supported on UC Application?				Nodes of the Cluster Supported by Check
	Unified CM	Unity Connection	IM and Presence	Emergency Responder	
Available Common Partition Space, on page 28	Y	N	Y	Y	Publisher and Subscriber
CLI Diagnostics, on page 28	Y	Y	Y	N	Publisher and Subscriber
CTI Device Count, on page 29	Y	N	N	N	Publisher
CTI Route Point Status, on page 30	Y	N	N	N	Publisher
Certificate Status Information, on page 30	Y	Y	Y	Y	Publisher and Subscriber
Check Cluster Status, on page 31	N	Y	N	N	Publisher
Cluster Version Information, on page 31	Y	Y	Y	Y	Publisher and Subscriber
DB Consistency State	N	Y	N	N	All nodes
Disaster Recovery System Backup, on page 33	Y	N	Y	Y	Publisher and Subscriber
Enterprise Service Parameters, on page 34	Y	N	Y	N	Publisher
Health of Network Within the Cluster, on page 34	Y	N	Y	N	Publisher and Subscriber
Installed COP Files, on page 35	Y	Y	Y	Y	Publisher and Subscriber
LDAP Details, on page 35	Y	N	N	N	Publisher and Subscriber
List of Services, on page 36	Y	N	Y	Y	Publisher and Subscriber
Network Connectivity (DNS, SMTP, and NTP), on page 37	Y	Y	Y	Y	Publisher and Subscriber
Phone Count, on page 37	Y	N	N	N	Publisher
Port Information, on page 38	N	Y	N	N	All nodes
Run Pre-Upgrade Test, on page 39	N	Y	N	N	Publisher and Subscriber

Upgrade Checks	Is Upgrade Check Supported on UC Application?				Nodes of the Cluster Supported by Check
	Unified CM	Unity Connection	IM and Presence	Emergency Responder	
State of Database Replication, on page 39	Y	N	Y	N	Publisher and Subscriber
SIP Trunk Information	Y	N	N	N	Publisher
Syslog Information	Y	N	N	N	Publisher
VCenter and ESXi and UCS Details, on page 42	Y	Y	Y	Y	Publisher and Subscriber
VM Configurations	Y	Y	Y	Y	Publisher and Subscriber

Available Common Partition Space

Checks for the availability of minimum 25 GB of common partition space.

Check	Displays the available space in the cluster.

Check Result	These are the results for the check:
	• Application Name: Specifies the node name.
	• Available Space: Specifies the available space in the common partition.
	• Used Space: Specifies the used space in the common partition.
	• Status:
	  • Pass: Indicates that the available common partition space is atleast 25 GB.
	  • Fail: Indicates that the available common partition space is less than 25 GB.

Status and Recommended Action	If the check fails, clear the space so that the minimum available partition space is 25 GB. Run the **show diskusage common** command to check the amount of used space.

CLI Diagnostics

Runs multiple tests to verify the disk status, Tomcat process status, and NTP status and so on. Log into HCM-F interface and run the **utils diagnose test** command on all nodes within the cluster with the admin credentials.

Check	Displays result of the tests run by the **utils diagnose test** command.

Check Result	The results of the check are:
	• Application Name: Specifies the node name.
	• Test Name: Specifies the test run by **utils diagnose test** command.
	• Result: Indicates if the test passed or failed.
	• Status:
	  • Pass: Indicates that the tests run as part of **utils diagnose test** command passed or skipped in the cluster.
	  • Fail: Indicates that the test executed as part of **utils diagnose test** command failed in the cluster.

Status and Recommended Action	If the check fails, check the node connectivity.

CTI Device Count

Records the total number of CTI devices, which includes CTI ports and Route Points.

Use this information for comparison post upgrade.

Check	Displays the CTI device count.

Check Result	The results of the check are:
	• Application Name: Specifies the node name.
	• CTI Device Status: Collects CTI device count for the following status:
	  • Registered
	  • Partially Registered
	  • Unregistered
	  • Rejected
	• CTI Device Count: Specifies the CTI device count for the preceding status.
	• Status:
	  • Pass: Indicates that the collection of CTI device count was successful.
	  • Fail: Indicates one of the following:
	  • HCM-F is unable to fetch the device count data from Cisco Unified Communications Manager.
	  • Using Invalid network configurations for the nodes.
	  • Using Invalid credentials in HCM-F.

Status and Recommended Action	If the status fails, check cluster reachability and the credentials using the Cisco Unified CM user interface.

CTI Route Point Status

Displays the CTI route point status and the IP address of the third-party application to which the route point is registered.

Use this information for comparison post upgrade.

Check	Displays the CTI Route point name, Route point status and IP address of the application to which the route point is registered.

Check Result	The results of the check are:
	• Application Name: Specifies the route point name.
	• CTI Route Status: Displays the CTI route point status:
	  • Pass: Indicates that the collection of CTI route point status was successful.
	  • Fail: Indicates that the collection of CTI route point status was unsuccessful.
	• IP Address: Specifies the IP address of the third-party application that is registered.

Status and Recommended Action	If the status fails, check cluster reachability and the credentials using the Cisco Unified CM user interface.

Certificate Status Information

Displays the Certificate information that is collected from the Certificate Monitor, and verifies the certificate status information. Certificates are sorted based on the number of days to expire.

Check	Displays the certificate status.

Check Result	• Certificate Name: Specifies the certificate name.
	• Expiry Date: Specifies the certificate expiry date. The table is sorted based on the certificate expiry date.
	• Status:
	  • Pass: Indicates that all the certificates are valid.
	  • Fail: Indicates that one or more certificates on any of the cluster's node is not valid.

Status and Recommended Action	If the certificates that are collected by certificate monitor is older than seven days, then the overall status fails. Check the certificate validity and **Recommended Actions**. • Run the **show cert list own** command to get the list of all the certificates on all nodes. • Run the **show cert own <cert_name>** command to check the status of a certificate.

Check Cluster Status

Checks if the publisher server has Primary status and subscriber server has Secondary status. This check is applicable only for Cisco Unity Connection.

Check	Displays the publisher and subscriber server name and status.

Result	Following are the result details:
	• Application Name: Specifies the node name. It is applicable only for publisher.
	• Server Name: Specifies the publisher and subscriber server name.
	• Server State: Specifies that one server node has publisher (Primary status) and the other has subscriber (Secondary status).
	• Internal State: Specifies if the server is active or inactive.
	• Status:
	  • Pass: Indicates that one node of the cluster is in Primary role and the other node is in secondary role. Also, both the nodes are online.
	  • Fail: Indicates failure for the following server states:
	  • Both nodes are in Primary.
	  • Both nodes are in Secondary.

Status and Recommended Action	Check the Recommended Action for failure. Run the **show cuc cluster status** command, to view the cluster status.

Cluster Version Information

Checks if all the applications for the selected cluster are available.

Check	Displays the application version and cluster node count.

Check Result	Following are the result details:
	• Application Name: Specifies the node name.
	• Application Version: Specifies the UC application version installed on the node.
	• Cluster Nodes Count: Specifies the number of nodes in the cluster. This entry is available only for publisher node.
	• Status:
	  • Pass: Indicates that these conditions passed:
	  • All the nodes of the cluster are reachable.
	  • All nodes of the cluster have same software version (including the build number) installed.
	  • Configuration in HCM-F aligns with the cluster configuration.
	  • Fail: Indicates that one or all of these conditions failed:
	  • Cannot retrieve version data due to invalid network configuration or credentials.
	  • Versions installed on all the nodes of the cluster do not match.
	  • Version configured in the HCM-F for the cluster does not match the actual active versions available on the cluster nodes.
	  • The number of nodes configured in the HCM-F does not match with the actual number of cluster nodes.

Status and Recommended Action	If the check fails, check node connectivity and credentials. Add the missing applications for the cluster. Run the **show version active** command, to view the version information and run the **show network cluster** command to get details of the cluster.

DB Consistency State

Checks the consistency of tables and validates indexes for the unitydirdb, unitydyndb, unitymbxdb1, and unityrptdb database in Unity Connection. This check runs on all nodes in the cluster.

Use this information from the check for comparison post upgrade.

Check	Checks the consistency of tables and validates indexes for the database in Unity Connection. Run the **show cuc dbconsistency <dbname>** command on each database using the HCM-F admin credentials.

Check Result	These are result for the check:
	• Database name: Specifies the names of the Unity Connection database.
	• Result:
	  • Checks for the table consistency.
	  • Index validation.

Status and Recommended Action	If the check fails, check the table for inconsistencies, disabled indexes or invalid index entries. Run these commands to check for inconsistencies: • **show cuc dbconsistency unitydirdb** • **show cuc dbconsistency unitydyndb** • **show cuc dbconsistency unityrptdb** • **show cuc dbconsistency unitymbxdb1**

Disaster Recovery System Backup

Checks if Disaster Recovery System (DRS) is configured and backup is complete.

Check	Displays the feature considered for backup with their status.

Check Result	These are the results for the check:
	• Application name: Specifies the node name.
	• Backup Filename: Specifies the backup filename with file extension as .tar.
	• Features: Lists the backup features separated by comma.
	• Backup Status: Specifies backup status with the percentage completed. Displays the percentage of backup completed, if the backup is in progress.
	• Status:
	  • Pass: Indicates that the backup is complete.
	  • Fail: Indicates one of these reasons for failure:
	  • The last backup has failed.
	  • Backup is still in progress.
	  • Cancelled the last backup.
	  • No backup status is available.

Status and Recommended Action	If the status fails, check if DRS is configured and run the scheduled or manual backup on all features. Run the **utils disaster_recovery status backup** command to check the backup status.

Enterprise Service Parameters

Displays all the enterprise service parameters for Unified Communications Manager and IM and P.

Check	Collects the service parameter values.

Check Result	These are the results for the check:
	• Application Name: Specifies the node name.
	• Service Parameter: Specifies the service parameter name and the service name separated by PIPE (|||). Format of the output is `<Service Parameter Name>||| <Service Name>`.
	• Value: Specifies present value of the service parameter.
	• Status:
	  • Pass: Indicates that the service parameter collection was successful from all nodes in the cluster.
	  • Fail: Indicates one of these reasons:
	  • The service parameter collection was unsuccessful
	  • Invalid network configurations are used for the nodes.
	  • Invalid credentials are used in HCM-F.

Status and Recommended Action	If the status fails, then check if the nodes in the selected cluster are reachable from HCM-F. Run the **show tech params enterprise** command, to view the service parameters that are configured for each of the services.

Health of Network Within the Cluster

Checks the network reachability among nodes in the selected cluster.

Check	Displays the node name and its reachability status.

Check Result	These are the results for the check:
	• Application Name: Specifies the node name.
	• Network Connectivity: Specifies if all the nodes are reachable or not.
	• Status:
	  • Pass: Indicates that all the cluster nodes are reachable to each other.
	  • Fail: Indicates that some or all the nodes are not reachable.

Status and Recommended Action	If the check fails, check the node connectivity and credentials. Log into each cluster node and run the **utils network ping <node-host-name>** command to check the network connectivity with the other nodes.

Installed COP Files

Checks if the required COP files are available for the upgrade.

The required COP file while upgrading from Cisco Unity Connection Release 10(x)/11(x) to 12.5(x) is `ciscocm.cuc_upgrade_12_0_v1.2.k3.cop`.

Check	Displays the COP files available in the cluster.

Check Result	These are the results for the check:
	• Application Name: Specifies the node name.
	• Installed COP Files: Specifies the list of COP files installed.
	• Status:
	  • Pass: Indicates the required COP files are available for the upgrade.
	  • Fail: Indicates the required COP files are not available for the upgrade.

Status and Recommended Action	If the check fails, install the required COP files for upgrading Cisco Unified Communications Manager. Run the **show version active** command to check the version of the COP file.

LDAP Details

Checks the last sync status of all LDAPs and their network connectivity.

Check	Displays LDAPs network connectivity and last sync status.

Check Result	These are the results for the check: • Application Name: Specifies the node name. • LDAP Server: Specifies the LDAP server name. • LDAP Status: Specifies the sync status and connectivity of all the LDAPs. • Status: • Pass: Indicates that the LDAP sync and connectivity are available. **Note** The status appears as Pass even if LDAP is not configured. • Fail: Indicates that the LDAP is not synchronized or the LDAP server is not reachable.
Status and Recommended Action	If LDAP sync fails, update the LDAP credentials and rerun the sync. If LDAP is not in network, add LDAP to the network. Log into Cisco Unified CM Admin page and check the LDAP configuration and its network connectivity.

List of Services

Checks and displays the status all the services.

Check	Displays the status all the services.
Check Result	These are the results for the check: • Application Name: Specifies the node name. • Service Name: Lists the services available in the cluster. • Service Status: Specifies if the service is started or if it is stopped. • Status: • Pass: Indicates the cluster was reachable for the collection. • Fail: Indicates one of these reasons: • Clusters were not reachable for the collection. • Invalid network configuration for the nodes. • Invalid credentials are used in HCMF.
Status and Recommended Action	If the check fails, check the cluster credentials and its reachability. For Cisco Emergency Responder, check if the SNMP master Agent is running else the check fails. Run the **utils service list** command to display the status of all the services present on cluster nodes.

Network Connectivity (DNS, SMTP, and NTP)

Checks if SMTP and DNS (Primary and Secondary) are configured and reachable. The DNS reachability and SMTP reachability fields display the server address along with the reachability status. The NTP status shows whether the UC application is synchronized with the configured NTP servers.

Note The check ignores the status, if DNS, SMTP or NTP protocols are not configured.

Check	Displays the DNS (Primary and Secondary), SMTP reachability status along with the NTP synchronization status.

Check Result	Following are the result details for the check:
	• Application Name: Specifies the node name.
	• DNS Reachability: Specifies the DNS configuration and reachability status. Only if DNS is configured, Primary and Secondary DNS reachability status are displayed.
	• SMTP Reachability: Specifies the SMTP configuration and reachability status.
	• NTP Status: Specifies the UC application synchronization with the NTP server.
	• Status:
	  • Pass: DNS or SMTP configured on the nodes are reachable and UC application is synchronized with the NTP server.
	  • Fail: Indicates one of these reasons
	  • DNS, NTP or SMTP configured on the nodes are not reachable
	  • UC application is not synchronized with the NTP server.

Status and Recommended Action	If the check fails, check the network connectivity with the configured DNS and SMTP. Diagnose NTP server configuration using the diagnostic modules. • Run the **show network eth0** command to view details on the configured DNS server and run the **utils network host <node-host-name>** command to check the connectivity with the DNS. • Run the **show smtp** command to view details of the configured SMTP server. • Run the **utils ntp status** command to view details of the configured NTP server.

Phone Count

Displays the phone count with status.

Use this information for comparison post upgrade.

Check	Displays the phone count with status.

Check Result	Following are the result details for the check:
	• Application Name: Specifies the node name.
	• Phone Status: Collects phone count for the following phone status:
	  • Registered
	  • Partially Registered
	  • Rejected
	  • UnRegistered
	• Phone Count: Specifies the phone count for the preceding status.
	• Status
	  • Pass: Indicates that clusters were reachable for collecting the phone count.
	  • Fail: Indicates one of the following:
	  • Clusters are not reachable for collecting the phone count.
	  • Invalid network configuration is used for the nodes.
	  • Invalid credentials are used in HCM-F.

Status and Recommended Action	If the status fails, check if the node is reachable from HCM-F and run the check again.

Port Information

Displays the active ports and the total ports that are configured on the nodes. This check runs on all nodes in the cluster and is applicable only to Cisco Unity Connection.

Use this information for comparison post upgrade.

Check	Displays the active ports and the total ports that are configured on the nodes.

Check Result	Following are the result details for the check:
	• Total Ports: Displays the total ports configured for the node.
	• Ports in Service: Specifies the number of ports in service.
	• Status
	  • Pass: Indicates that the number of ports in service are less than the total number of ports configured.
	  • Fail: Indicates that the number of ports in service are more than the total number of ports configured.

Status and Recommended Action	If the check fails, check the connectivity to Cisco Unity Connection, administrator credentials, node version, and test the multiple network address.

Run Pre-Upgrade Test

Performs the pre-upgrade checks and displays the result. This check is applicable only for Cisco Unity Connection.

Check	Performs the pre-upgrade checks and displays the result.

Result	• Application Name: Specifies the node name.
	• Test name: Lists the executed tests:
	  • Locales Installation Test
	  • Connection DB Test
	  • DRS Backup History Test
	  • Cluster State Test
	  • Critical Services Test
	  • COP File Installation Test
	• Result: Specifies the status of the tests that is listed in the Test Name.
	• Status:
	  • Pass: Indicates that all the tests passed.
	  • Fail: Indicates that one or more pre-upgrade test has failed.

Status and Recommended Action	Check the Recommended Actions to understand the failure reason. Run the **run cuc preupgrade test** command to execute the pre-upgrade check.

State of Database Replication

Checks the status of the database replication between publisher and subscriber nodes for Cisco Unified Communications Manager and IM and Presence.

Check	Displays the status of the database replication between publisher and subscriber nodes for Cisco Unified Communications Manager and IM and P.

Check Result	These are the details of the check:
	• Application Name: Specifies the node name.
	• Database Replication Status: Specifies the node replication status.
	• Status:
	  • Pass: Indicates that cluster nodes are reachable and data replication values are collected successfully.
	  • Fail: Indicates that the cluster nodes are not reachable or the data replication failed for the cluster nodes.

Status and Recommended Action	If the status fails, check the connectivity between publisher and subscriber nodes in the cluster. Also, check the reachability of cluster from HCM-F. • To trigger the database replication, run the **utils dbreplication status** command. • To check the status of the triggered database replication, run the **utils dbreplication runtimestate** command. Ensure that the output displays "(2) Setup Completed" status for all the cluster nodes.

SIP Trunk Information

Checks if the configured SIP Trunks are in service, and the destination is reachable.

Use this information for comparison post upgrade.

Check	Records the total number of SIP trunks that are configured in the network.

Check Result	These are the result of the check: • Trunk Name: Specifies the trunk name. • Destination Detail: Specifies the IPV6/IPV4 address of the destination, if it is configured. **Note** The Destination Detail displays the SIP Trunk Service type name for these trunk types: Call Control Discovery, Extension Mobility Cross Cluster, and Cisco Intercompany Media Engine instead of the destination address. • Trunk Status: • Pass: Indicates one of these reasons for success: • OPTIONS ping enabled SIP Trunks are in Full Service. • Destination address is reachable. • Fail: Indicates one of these reasons for failure: • Trunk is out of service. • Destination is not reachable.
Status and Recommended Action	If the check fails, see the Verify & Troubleshoot section in these guides: • Verifying and Troubleshooting SIP Features document in CUCM • Calls through Session Initiation Protocol (SIP) Trunk Failure • Configure Options Ping Between CUCM and CUBE

Note The report contains SIP Security Profile Properties, SIP Profile Properties, and Recording enabled information along with the SIP Trunk Name, Status, and Destination details.

Syslog Information

Checks if the Syslog Configuration parameters are configured, and the remote servers are reachable.

Use this information for comparison post upgrade.

Check	Displays the Syslog parameters that are configured in the Cisco Unified CM Administrator user interface for message logging.

Check Result	The results of the check are:
	• Application Name: Specifies the publisher name of the Cisco Unified CM application.
	• Syslog Configuration: Specifies these parameter configurations:
	  • Servers: Specifies the IP address of the configured servers.
	  • Severity Level: You can limit messages that are displayed for the selected device by specifying the severity level of the message.
	  • Unreachable Servers: Displays the IP address of the servers that could not be reached.
	  • Status: Specifies if the check passed or failed.
	  • Service Status: Specifies the status for the Cisco Syslog Agent service for the Cisco Unified CM.

Status and Recommended Action	If the status fails, run these commands from the Cisco Unified CM CLI interface: • **utlis service list** command to check if syslog service is started • **utils network ping <server address>** command to check if the servers are reachable.

VCenter and ESXi and UCS Details

Collects the information about ESXi (host configuration) for understanding the supported and unsupported versions of vCenter, ESXi and VM hardware.

Check	Use this information to understand the supported and unsupported versions.

Check Result	Following are the result details:
	• Application Name: Specifies the node name.
	• ESXi/Host Configuration: Displays the following information:
	  • VCenter version
	  • ESXi version
	  • VM hardware version
	  • Blade model
	  • VM Tools running
	• Pass: Indicates that the node was reachable for collection.
	• Fail: Indicates that the node was not reachable for collection.

Status and Recommended Action	If the check fails, check the node connectivity and credentials.

VM Configurations

Checks the VM configuration and verifies if the OVA is compatible with the target upgrade version for each of the UC applications.

Check	Use this information to understand if the VM configuration meets the target upgrade requirements.

Check Result	Following are the result details:
	• Application Name: Specifies the node name.
	• VM Configuration: Displays the following information:
	  • Users—Displays the number of licensed users and the maximum number of supported users for the VM configurations when the publisher node is Unified CM. For all other nodes, it displays the maximum number of supported users related to the VM configuration.
	  • Actual—Displays the current VM configuration information such as Number of CPU, Memory in GB, Hard Disk Size in GB.
	  • Required—Displays the required VM configuration information such as Number of CPU, Memory in GB, Hard Disk Size in GB.
	• Pass: Indicates that the node meets the requirements.
	• Fail: Indicates that the node does not meet the requirement and must be re-configured before you trigger an upgrade.
	Note The OVA check compares the current ova type (small,medium,large) in the HCS environment with the corresponding ova type in the targeted upgrade version.

Status and Recommended Action	If the check fails, check the VM requirement for each UC application using these links: • Cisco Unified CM • Cisco Unity Connection • Cisco IM and Presence • Cisco Emergency Responder

Post Upgrade Comparison

Perform upgrade comparison to validate the results obtained before and after upgrade.

Before you begin

Ensure to do the following:

- See Upgrade Toolkit Prerequisites, on page 23

- Ensure to perform Perform Upgrade Checks, on page 25 on the UC application clusters before and after upgrade.

Step 1 From the side menu, choose **Service Provider Toolkit** > **Upgrade Toolkit** > **Upgrade Comparison**.

Step 2 From **Select a Customer** drop down, select the same customer name on which you performed Upgrade Checks before and after upgrade.

Step 3 From **Select a Cluster** drop down, select the the same UC application cluster on which you performed Upgrade Checks before and after upgrade..

The comparison check results (tick or cross-mark) for the selected UC application cluster appear in the Status column.

Step 4 Click the tick or cross-mark in the **Status** column to understand the result details.

Upgrade Comparison

The checks in **Upgrade Comparison** use the results obtained from the **Upgrade Checks** before and after upgrade for comparison. The following table lists the checks that are supported on different UC applications.

Table 5: Upgrade Comparison

Upgrade Comparison	Is Upgrade Comparison Supported on UC Application?		
	Unified CM	Unity Connection	IM and P
Installed COP Files	Y	N	Y
LDAP Details	Y	N	N
CTI Device Count	Y	N	N
List of Services	Y	N	Y
Phone Count	Y	N	N
CLI Diagnostics	Y	N	Y
Enterprise Service Parameters	Y	N	Y
Cluster Version Information	Y	Y	Y
Check Cluster Status	N	Y	N

Phone Compatibility Check

Perform this check to know the phone details with the list of supported and unsupported phones along with the Jabber devices.

Before you begin

Upgrade Toolkit Prerequisites, on page 23

Note Before performing the compatibility check, ensure Cisco HCS CAA CUCM Service, Cisco HCS CAA IMP Service, and Cisco HCS UC Monitor Service are active by using **utils service activate Cisco HCS CAA CUCM Service**, **utils service activate Cisco HCS CAA IMP Service** and **utils service activate Cisco HCS UC Monitor Service** commands respectively.

Step 1 From the side menu, choose **Service Provider Toolkit** > **Upgrade Toolkit** > **Phone Compatibility Check**.

Step 2 From **Select a Customer** drop-down, select the customer name for performing the checks.

Step 3 From **Select a Cluster** drop-down choose a UC application cluster, or choose **All** to perform the compatibility check on all clusters of a customer.

Date and time when the last phone compatibility check for the cluster was performed appears, if the compatibility check for the same customer and the same UC application cluster is initiated. The compatibility check result is downloaded using **Download**.

Step 4 From **Target Version** drop-down choose a UC application version.

Step 5 Select the option **Include Jabber Devices** to include the Jabber device details in the report.

Step 6 Click **Submit** to perform the compatibility check.

The job initiation status appears.

Step 7 Check the job status.

Select **Infrastructure Manager** > **Administration** > **Jobs**. Check for Job Entity, UC Monitor Checks.

Note You can run the check on different clusters for the same customer at the same time. But, if a check for a customer cluster is in progress and if another check is initiated for the same cluster, the initiation fails.

Step 8 Click **Download** to download the .csv file.

The .csv file contains Customer Name, Cluster Name, User Name, Phone Model, Device Name, Directory number, Phone IP address, Hardware Support Status, and Version. The report specifies the following:

- Supported or unsupported status for the phone models in the Hardware Support Status column.
- Displays the associated software version for the Jabber endpoints and the Phone firmware version for phones in the Version column.

Note Jabber—The Version column for Jabber users does not display information, if the soft-phone is not registered since the last restart of the Cisco Unified CM application. The Jabber versions of all the soft phones are displayed in the version column irrespective of whether the version is supported or not supported in the targeted upgrade version.

Hard phones—The Hardware Support Status column applies only for the hard phones. The firmware version of all the hard phones are displayed in the version column irrespective of whether the phone model is supported or not supported in the targeted upgrade version.

Upgrade Requirements for Push Notifications

Use the following table to determine whether you need to upgrade your system in order to deploy Push Notifications.

Table 6: Upgrade Requirements to Support Push Notifications

If your Apple mobile deployment includes...	Upgrade to these minimum releases...
No Jabber clients on iOS	No upgrade required
Phone only (with iOS)	See the Cisco Hosted Collaboration Solution Compatibility Matrix for details on minimum supported versions of Cisco Jabber, Unified CM, and Expressway MRA for implementing Apple Push Notification Service for IM and presence.
Instant Messaging only (with iOS)	See the Cisco Hosted Collaboration Solution Compatibility Matrix for details on minimum supported versions of Cisco Jabber, Unified CM and IM and Presense Service, and Expressway MRA for implementing Apple Push Notification Service for IM and presence.
Full Unified Communications (calling and instant messaging)	See the Cisco Hosted Collaboration Solution Compatibility Matrix for details on minimum supported versions of Cisco Jabber, Unified CM and IM and Presense Service, and Expressway MRA for implementing Apple Push Notification Service for IM and presence.
Full Unified Communications (calling and WebEx Messenger)	See the Cisco Hosted Collaboration Solution Compatibility Matrix for details on minimum supported versions of Cisco Jabber, Unified CM for implementing Apple Push Notification Service for IM and presence.

Upgrades from 11.5(1)SU2 with Push Notifications Enabled

If you are upgrading from the 11.5(1)SU2 release and you had Push Notifications enabled in the old release, you must disable Push Notifications in the current release and then follow the onboarding process to enable Push Notifications once again. This is required due to API changes in this release that were not a part of the 11.5(1)SU2 release. Your upgraded system will not be able to send troubleshooting logs to the Cisco Cloud unless you disable Push Notifications and then follow the onboarding process for this release.

After you upgrade your system, do the following:

Step 1 Disable Push Notifications

Follow these steps:

a. From Cisco Unified CM Administration, choose **Advanced Features** > **Cisco Cloud Onboarding**

b. Uncheck the following check boxes:

- **Enable Push Notifications**
- **Send Troubleshooting information to the Cisco Cloud**

- **Send encrypted PII to the Cisco Cloud for troubleshooting**

c. Click **Save**.

Step 2 Enable Push Notifications for this release.

For the full onboarding process, see the "Push Notifications Configuration Task Flow" in the *Deploying Push Notifications for Cisco Jabber on iPhone and iPad* document at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/pushNotifications/11_5_1_su2/cucm_b_push-notification-deployment-iPhone-iPad.html.