CALLING

Transitioning from Unified CM to UCM Cloud

Deployment Guide

August 5, 2021

Contents

What's New in This Guide

Table 1 lists updates and new topics added to this guide since previous releases of this document.

Table 1. *Updated or New Topics Since the Previous Release of this Guide*

Updated or New Topic Location(s)	Updated or New Topic Details	Date
Initial Release	Initial publication of this guide.	May 26, 2020
Step 2 of Pre-Transitions Steps and Considerations References	Added information about saving/exporting the following user specific historical data prior to transition: Voicemail messages – backed up using COBRAS. Jabber contact lists – exported using Unified CM IM&P BAT.	August 10, 2020
Title page, document footer, and locations throughout document.	Changed naming references from "Unified CM Cloud" to "UCM Cloud"	August 26, 2020
Locations throughout document	▪ Product reference name changes including "Cisco Webex DX and Room" to "Webex Desk and Room Series ▪ Branding Updates and Format Corrections	August 5, 2021

Introduction

Target Audience

This transition deployment guide is intended to be used by teams or individuals with expert experience configuring and administering Cisco Unified Communications Manager (Unified CM) and Cisco endpoints including IP desk phones, video devices, and Jabber soft clients. There are links to product and support documentation throughout this document to assist.

Note: Read this document in its entirety before taking any action. Do not proceed if you are unclear about any task or possible repercussions.

Overview

This document is technical in nature and discusses transitioning from on-premises Unified CM to UCM Cloud. This document does not address any of the following which are documented on the UCM Cloud Help site available at https://ucmcloudhelp.cisco.com/ and the Cisco Unified Communications Manager Cloud SalesConnect site available at https://salesconnect.cisco.com/#/program/PAGE-15188:

- UCM Cloud sales cycle
- UCM Cloud business agreements
- UCM Cloud partner onboarding
- UCM Cloud partner operations
- UCM Cloud customer onboarding
- UCM Cloud analytics

Once the UCM Cloud cluster is deployed by Cisco, it is ready for configuration by you, the partner's administration team. The cluster is in a just-built state as described in the completed *Build-Handover* document based on the initial *Customer Questionnaire* document. The UCM Cloud cluster has test configuration parameters configured for initial post-build cluster testing by Cisco. Test configuration parameters are prefaced with "x-" and can safely be replaced with actual configuration parameters. This document takes you from this point and is intended to help you with this configuration process.

As the administrator, your role is to configure the UCM Cloud cluster to replicate the Unified CM source cluster. Specifically, you must focus on preventing the end-user

experience from changing in any way, and if done carefully, the end-user should not know nor care that their devices are now registering to UCM Cloud instead of Unified CM.

Related UCM Cloud Documents

- **Customer Questionnaire (CQ)**

  The completed “Customer Questionnaire for UCM Cloud” (CQ) spreadsheet describes the necessary network infrastructure and sizing-related data required for Cisco to deploy sufficient UCM Cloud cluster resources. The CQ responses do not provide sufficient detail to configure the UCM Cloud system.

- **Build Document**

  The “Build Document” is the documented result of the completed CQ. The document describes details the build team needs to build the customer’s UCM Cloud environment.

- **Completed Build Document**

  The completed “UCM Cloud Build Document” is the documented result of the implemented CQ and is authored by the Cisco team that built the customer’s private UCM Cloud instance. The document describes network infrastructure, UC applications, edge components, and server names.

- **Customer Handover**

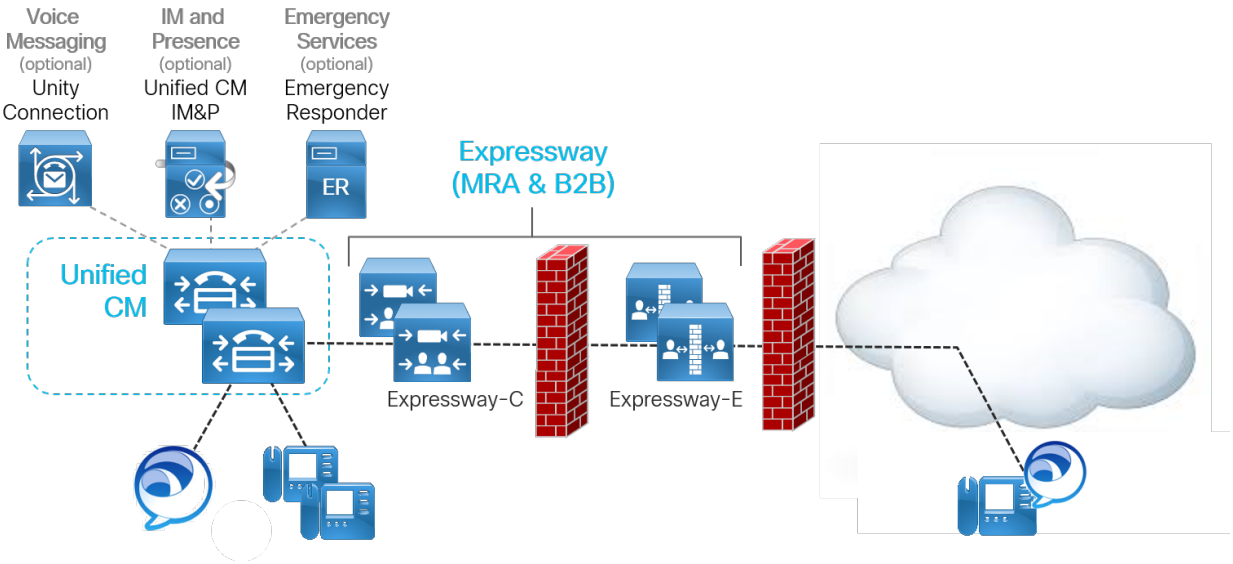
  The completed “Customer Handover” workbook is intended for you, the partner. It includes spreadsheets for UC applications, edge applications, and domain information. Access to this document must be carefully restricted because it has log in credentials for administrative access as configured by Cisco’s build team.

- **End-user Document**

  This document should be authored by you, the partner for the customer’s end-users. It should explain that the system has undergone maintenance, that their phone has been restarted, and they should log out of their Jabber client and log back in. The document should provide hotline contact information for the morning after cutover to the UCM Cloud should they need any assistance.

As shown in Figure 1, a typical deployment includes different collaboration infrastructure components on the network, a call control platform, an edge platform, hardware and software endpoints, and in some cases additional applications. In the Cisco architecture this would include Unified CM for call control, Unified CM IM&P for instant messaging and presence, Cisco Expressway for remote access and business-to-business (B2B) edge services, Cisco Unity Connection for voice messaging, Cisco Emergency Responder for emergency service call routing, and user-facing hardware (Cisco IP Phones, Webex Desk and Room Series) and software (Cisco Jabber) IP-based endpoints. These components may vary slightly in some environments, but this is the starting point for the transition described in the rest of this document.

Figure 1. *On-Premises Collaboration Architecture: Call Control and Remote Access*



Note: The simplified architecture shown in Figure 1 is based on the Preferred Architecture (PA) for Cisco Collaboration Enterprise On-Premises Deployments. For more information on the Enterprise On-Premises PA, refer to the https://www.cisco.com/go/pa site.

Table 2 lists the key elements of the on-premises architecture prior to transitioning to UCM Cloud.

Table 2. *Before: On-Premises Calling Infrastructure Components*

Product	Description
Cisco Unified CM	On-premises call control providing device registration and call routing services

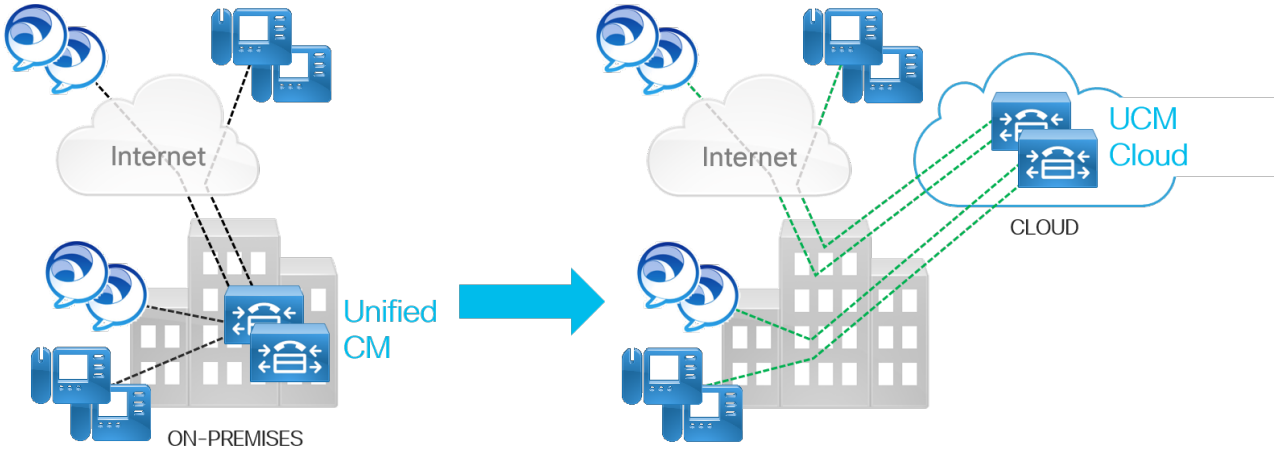
Cisco Expressway-C/E	Edge infrastructure providing Mobile and Remote Access (MRA) (business-to-business (B2B)) functionality enabling remote endpoints to connect securely from outside the organization. Expressway is deployed in pairs to provide firewall traversal for external endpoints. [Optional]
Cisco Unity Connection	On-premises voice messaging platform providing voicemail and unified messaging capabilities. [Optional]
Cisco Instant Messaging and Presence	On-premises messaging, presence, and contacts services. [Optional]
Cisco Emergency Responder	On-premises emergency enhancement services. [Optional]
Cisco IP Phones and Cisco Jabber	IP-based devices registered to Unified CM and provides voice and video calling capabilities

As shown in **Figure 2**, this transition document addresses customers who have on-premises call control with Unified CM as well as IP phones and clients that have decided to transition the architecture toward a UCM Cloud calling architecture.

The decision needs to be made based on customer's functionality requirements. Customers that have the following requirements should consider carefully before making this decision and may ultimately decide to keep call control on-premises:

- Restrictive, limited, or unreliable Internet access.
- Strict no cloud policy or other restrictions related to off-premises components and services.

Figure 2. *On-Premises to Cloud Calling Transition Decision*



Once the Unified CM environment is migrated to UCM Cloud, no Unified CM servers need remain on the customer's premises as depicted in **Figure 2**. The end-user's experience, dialing habits, and feature set should not change in any way from the way they worked when registered to Unified CM. While end-user dialing habits and user behavior will be protected and remain the same, be aware that historical user data such as call history, speed dials, voicemail, Jabber chat history, and Jabber contact lists cannot be efficiently transitioned to new equipment.

Core Components

The target architecture for this transition includes new, dedicated UCM Cloud components deployed in Cisco's cloud as depicted in **Figure 3**.

Figure 3. *After: Cisco UCM Cloud Calling*

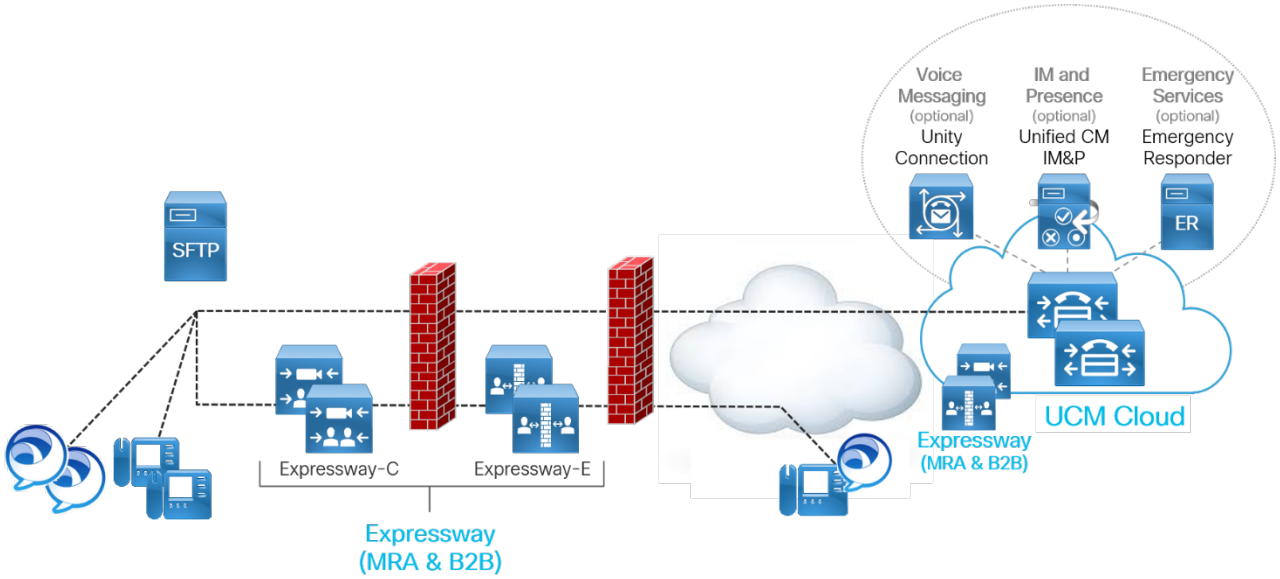


Figure 3 also shows an SFTP server on the customer's network, accessible to both the on-premises Unified CM and UCM Cloud clusters. This SFTP server can be used to transition data such as Jabber configuration files from Unified CM TFTP servers and phone ITL (initial trust list) files. The customer's dedicated UCM Cloud servers replace their on-premises Unified CM servers and leverage other assets as follows:

- Unified CM publisher and subscribers

  The on-premises Unified CM publisher and subscribers will be removed from service in the final steps of this document.

- Unified CM TFTP server(s)

  The Unified CM TFTP server(s) will be removed from service in the final steps of this document.

- DHCP server(s)

The on-premises DHCP server will remain in service and OPTIONS such as 150 must be modified to point to the appropriate TFTP server(s).

- DNS server(s)

  The on-premises DNS server(s) will remain in service and SRV records such as _cisco-uds must be modified to point to the new UCM Cloud server as appropriate.

- Active Directory or LDAP server(s)

  The existing AD/LDAP server will remain in service and should not require modification.

Table 3lists the new elements of the architecture after transitioning to UCM Cloud.

Table 3. *After: UCM Cloud Calling Infrastructure Components*

Product	Description
Cisco UCM Cloud	Unified CM Cloud call control providing device registration and call routing services
Cisco Expressway-C/E	Edge infrastructure providing Mobile and Remote Access (MRA) (business-to-business (B2B)) functionality enabling remote endpoints to connect securely from outside the organization. Expressway is deployed in pairs to provide firewall traversal for external endpoints. Expressway cluster nodes may be deployed on-premises or they can be deployed in the cloud by the partner provider or Cisco. [Optional]
Cisco Unity Connection	Voice messaging platform providing voicemail and unified messaging capabilities. [Optional]
Cisco Unified CM Instant Messaging and Presence (IM&P)	Messaging, presence, and contacts services. [Optional]
Cisco Emergency Responder	On-premises emergency enhancement services. [Optional]

Cisco IP Phones and Cisco Jabber	IP-based devices registered to UCM Cloud and provides voice and video calling capabilities

Transition

This section covers the pre-transition preparation steps, the transition implementation steps, and the post-transition steps to be considered for this workflow transition.

This document initially discusses transitioning from a Unified CM voice-only deployment to a full UCM Cloud deployment as a flash cut-over. While not realistic for a real-world production environment, this approach makes it easier to quantify important concepts and basic task-flow.

Migrating from Unified CM to UCM Cloud is no different from migrating from one Unified CM cluster to another Unified CM cluster. This document suggests an order in which to complete tasks so that you can test along the way to reduce any potential for wasting time.

Because user phones and devices do not physically move when migrating from Unified CM to UCM Cloud, no major DHCP nor DNS changes are needed and the existing DHCP and DNS servers can continue to be used.

Pre-Transition Steps and Considerations

The following steps provide an overview of migration steps followed by more detail on migrating Unified CM configuration to UCM Cloud.

1. Develop a Back-Out Option

Before proceeding you should back up all collaboration and infrastructure systems if anything goes wrong at any time during the transition, and you must back out or abandon the transition.

Back up the existing Unified CM configuration at the cluster-level using the Disaster Recovery System (DRS). For information on DRS refer to the *Back Up the System* chapter of the Administration Guide for Cisco Unified Communications Manager and IM and Presence Service available at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Once the UCM Cloud environment is fully deployed and operational, the DRS archive is no longer needed and can be discarded.

2. Instruct Users to Prepare for Transition to UCM Cloud

Notify users that they may lose the following:

- Call history for both phones and Jabber.
- Speed dials for both phones and Jabber.
- Voicemail messages for both phones and Jabber.

Note: Administrators can back up voicemail messages prior to transition by leveraging Cisco Unified Backup and Restore Application Suite (COBRAS) available at http://www.ciscounitytools.com/Applications/General/COBRAS/COBRAS.html.

- Jabber chat history.
- Jabber contact lists.

Note: Administrators can back up Jabber contact lists prior to the transition by leveraging the Export Contact List option with the Bulk Administration Tool (BAT) on Unified CM IM and Presence. For more information refer to the information in the Configuration and Administration of the IM and Presence Service guide available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/configAdminGuide/12_5_1/cup0_b_config-and-admin-guide-1251/cup0_b_config-and-admin-guide-1251_chapter_0100011.html?dtid=osscdc000283#task_0F2C26E2BC3929146D9AF931141F1691.

3. Inventory Existing Endpoints and Jabber Clients

You must inventory your customer's hardware and software endpoints. You will use the inventory of phone models to identify endpoints not supported by UCM Cloud. Unsupported models must be replaced prior to the transition. Refer to the Unified CM Deprecated Phone Models documentation available at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-device-support-tables-list.html.

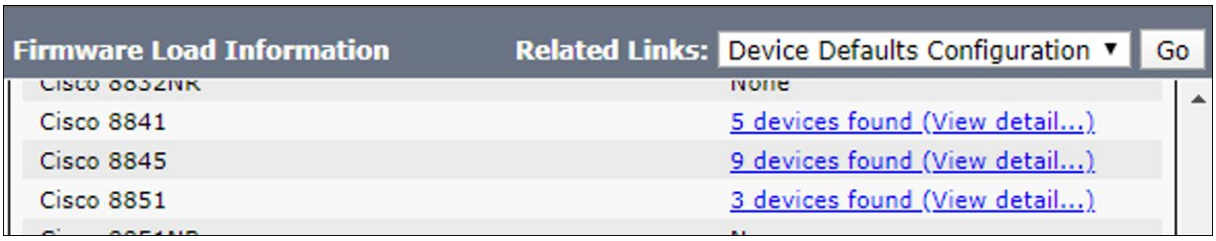
Document the deployment mode(s) implemented for Jabber (IM-only, phone-only, and/or full UC modes) and document any other on-premises services (Unified CM IM&P, Unity Connection, Cisco Meeting Server, and so on) consumed by Jabber.

4. Upgrade All Endpoints to the Latest Enterprise Phone Firmware

You should upgrade all phones before moving them to UCM Cloud so that they do not immediately upgrade on initial registration to UCM Cloud. Upgrading before moving to UCM Cloud will result in a more efficient transition process for the team performing the transition to UCM Cloud.

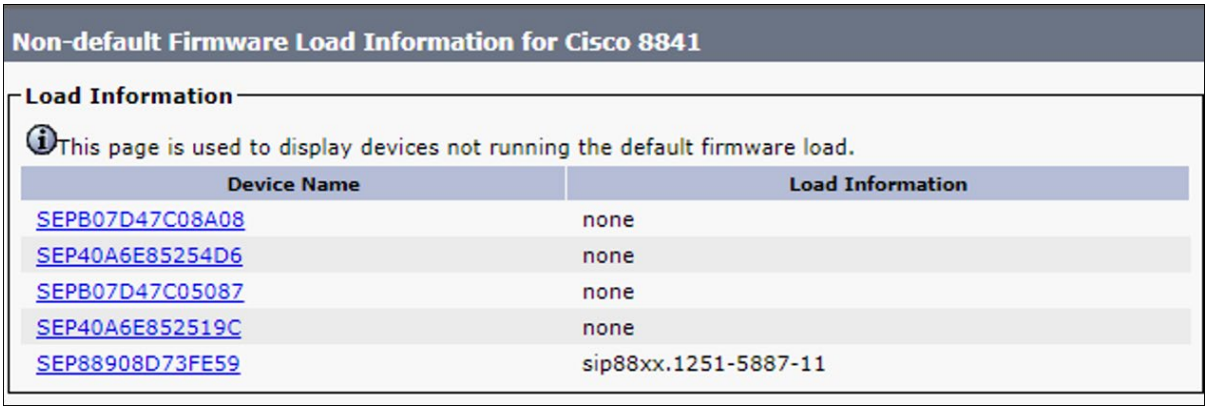
Verify that all phones are running the default firmware load by navigating to **Device > Device Settings > Firmware Load Information** as shown in **Figure 4**.

Figure 4. *Firmware Load Information for Existing Devices*



Selecting one of the hyperlinks on the **Firmware Load Information** page will show you which phones may not be running the current default load. Examples of phones not using the default firmware will have a name in the 'Load Information' field as shown in **Figure 5**.

Figure 5. *Non-Default Firmware Load Information*



Clicking the linked device name provides direct access to change to the default firmware version.

5. Audit the Existing Unified CM deployment

Select a representative sample of about five user types and carefully document their phone-related and Jabber client workflows. You will use this sampling during and after transition as an early form of acceptance testing to verify that their dialing habits and workflows remain identical after transition.

Before performing any configuration, you must perform a comprehensive audit of the existing Unified CM deployment that includes at least the following:

- Certificates
- Unified CM devices and related configuration
- Users and their associated devices
- Network
- Firewall
  - Ingress Ports
  - Egress Ports
- DNS SRV records: _cisco_uds._tcp.<domain>
- DHCP scope and advertised DHCP OPTIONS
- AD / LDAP
- Dial Plan
  - Hunt Groups
  - Hunt Pilots
  - Hunt Lists
- PSTN
- SRST
- User Provisioning methods
- TFTP files

Note: Jabber 11.8 and later versions do **NOT** support SRST

Transition Steps and Considerations

This section assumes you have performed all previous pre-transition steps relevant to your customer's current Unified CM deployment.

Users can continue to use their phones and Jabber clients on their existing Unified CM environment while you configure UCM Cloud to replicate their existing Unified CM configuration.

Once you have completed configuring UCM Cloud, you must perform testing on a representative set of phones and Jabber clients. When test results confirm that the full Unified CM configuration is properly replicated in the UCM Cloud cluster, initiate a maintenance window where DNS and DHCP services will be modified. This maintenance window is required because changes to DNS and DHCP will directly impact users trying to work when their phones and Jabber clients attempt to register to UCM Cloud.

There are multiple ways to transition an existing Unified CM cluster's configuration to another cluster. This section provides an overview of this transition task using the Unified CM administration web interface. Advanced administrators may choose to use AXL, Bulk Administration Tool (BAT), 3rd-party migration tools, or some combination of these options.

The following steps include basic Unified CM administration web interface navigation information for the primary Unified CM configuration parameters:

1. Certificate Management

   You are responsible for generating Certificate Signing Requests (CSR) and submitting them to the appropriate Certificate Authority (CA). You are also responsible for installing the signed certificates as described in Cisco documentation.

   To manage Unified CM system certificates, navigate to **System > Security > Certificates**.

2. Cluster Security Mode Configuration

   You must configure UCM Cloud to run in the security mode specified by your customer's security policy. This will already be correctly configured by Cisco's build team based on the response to the "Secure Calls Required" question in the *Customer Questionnaire*.

   To determine the cluster security mode, navigate to **System > Enterprise Parameters** and scroll to Security Parameters section to find the **Cluster Security Mode** setting. A setting of '0' indicates the cluster is in non-secure mode. A setting of '1' indicates the cluster is in mixed mode (secure). To change the Unified CM

security mode, you must use the **utils ctl set-cluster** command at the system Command Line Interface (CLI) through an SSH session.

If moving from a secure mode cluster, you must perform additional steps when transitioning Cisco IP phones from Unified CM to UCM Cloud to avoid loss of trust which would require having to physically touch every phone to manually clear the trust list.

3. TFTP Files

You should copy any needed TFTP files from your customer's Unified CM environment to the temporary SFTP server shown in Figure 3.

4. Replicate Unified CM Configuration on UCM Cloud Deployment

The following configuration parameters on the source Unified CM deployment will need to be replicated on the UCM Cloud deployment:

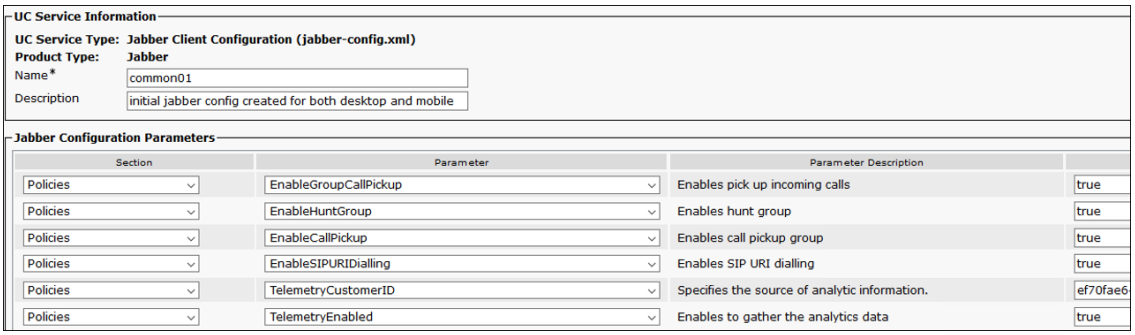
i. UC Service Configuration

You must define any UC Services (for example, voicemail, conferencing, directory, and so on) that will be required for the production UCM Cloud system.

To ensure Jabber service discovery and automatic configuration works properly, navigate to **User Management > User Settings > UC Service** to define any UC Services that will be required for the production UCM Cloud system.

You must also define at least one Jabber Client Configuration (jabber-config.xml) UC Service Type where all Jabber configuration parameters from your customer's Unified CM's jabber-config.xml file are included (see **Figure 6**).

Figure 6. *UC Service Definition Example for Jabber*



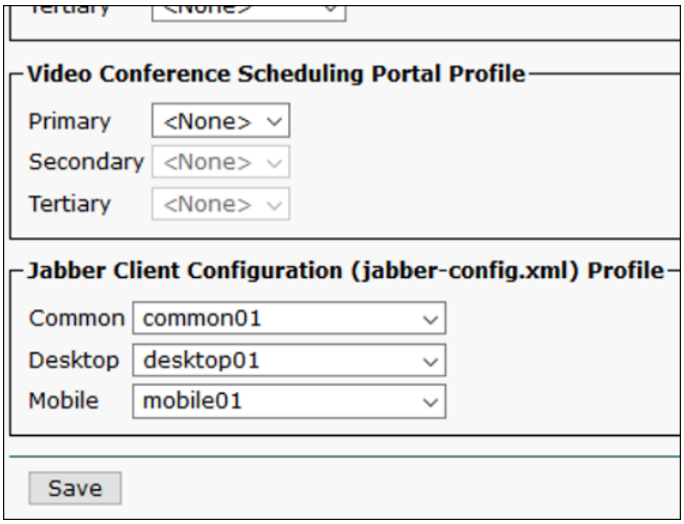
This service type is referenced later when defining service profile(s).

ii. Service Profile Configuration

You must define any Service Profiles required for the production UCM Cloud system. To configure service profiles with Jabber client configuration and other UC services, navigate to **User Management > User Settings > Service Profile**.

Ensure you have defined Jabber Client Configuration (jabber-config.xml) Profiles for "Common", "Desktop", and/or "Mobile" to populate the jabber-config.xml file for Jabber clients on the new system (see **Figure 7** for an example).

Figure 7. *Service Profile: Jabber Client Configuration*



iii. Feature Group Template Configuration

You should define Feature Group Templates for the LDAP sync agreement to apply when synchronizing users on the production UCM Cloud system from Active Directory (AD).

To configure Feature Group Templates, navigate to **User Management > User/Phone Add > Feature Group Template**.

iv. Authentication and Authorization Configuration

You must configure authentication and authorization based on your security model. SAML SSO and OAuth with Refresh Tokens are Cisco recommended best practices.

To configure OAuth with Refresh Tokens and other authorization settings, navigate to **System > Enterprise Parameters > SSO and OAuth Configuration**. You should configure authorization based on your security model.

To configure single sign-on (SSO), navigate to **System > SAML Single Sign-On**.

To configure LDAP authentication, navigate to **System > LDAP > LDAP Authentication**. Specify the LDAP server(s) for end user authentication.

v. **LDAP Synchronization Agreement Configuration**

You should configure LDAP to synchronize users from the Active Directory (AD) LDAP system. Provided the UC Services, Service Profiles, and Feature Group Templates exist and are appropriately defined, users will enjoy full services as soon as they are synchronized from AD to your UCM Cloud cluster.

To configure LDAP synchronization with AD, navigate to **System > LDAP > LDAP System / LDAP Directory**.

vi. **Unified CM Group Configuration**

You must configure at least one Unified CM Group if the source Unified CM included Device Pool configuration.

Unified CM nodes may be grouped in order to assign endpoints to a set of nodes for registration and call routing registration.

To control the Unified CM node grouping, navigate to **System > Cisco Unified CM Group**.

vii. **Partition Configuration**

You must configure partitions required for calling search space definitions.

A partition contains a list of route patterns (directory number (DN) and route patterns). Partitions facilitate call routing by dividing the route plan into logical subsets that are based on organization, location, and call type.

To configure class of service call routing partitions, navigate to **Call Routing > Class of Control > Partition**.

viii. **Calling Search Space Configuration**

You must configure Calling Search Space (CSSs) to replicate the source Unified CM configuration.

A CSS is comprised of an ordered list of route partitions that are typically assigned to devices. CSSs determine the partitions that calling devices search when they are attempting to complete a call.

To configure CSSs, navigate to **Call Routing > Class of Control > Calling Search Space**.

ix. **Route Pattern Configuration**

You must configure route patterns to replicate the source Unified CM configuration in part to carry forward end user dialing habits.

To configure calling route patterns, navigate to **Call Routing > Route/Hunt > Route Patterns**.

x. **Directory Number Configuration**

You should define and assign directory numbers to either replicate what was configured on the source Unified CM cluster or define new directory numbers for the UCM Cloud deployment.

Directory numbers are assigned to specific endpoints and serve as an identifiable address for the device.

To configure directory numbers, navigate to **Call Routing > Directory Number**.

xi. **Translation Pattern Configuration**

You must define translation patterns on the UCM Cloud deployment to mimic the dialing habits to which the Unified CM users are accustomed. This is the most important part of the migration and if done properly, will mean that users experience no changes in their workflows and thus will not need any training or behavior modification.

To configure translation patterns for manipulating called numbers, navigate to **Call Routing > Translation Pattern**.

xii. **Call Park and Call Pickup Configuration**

If applicable to the deployment, you must configure call park and call pickup groups to replicate what was configured on Unified CM previously.

The call pickup feature allows users to pick up incoming calls which are routed to pre-defined group of users and available for whichever user is available.

To configure call park and call pickup features on the new system, navigate to **Call Routing > Call Park / Directed Call Park / Call Pickup Group**.

The call park feature allows users to place a call on hold, so it can be retrieved from another phone by dialing the number the call is parked on.

xiii. **Transformation Pattern Configuration**

If applicable to the deployment, you must configure transformation patterns for both calling party and called party to replicate what was configured on Unified CM previously.

To configure transformation patterns for manipulating called and/or calling numbers, navigate to **Call Routing > Transformation > Transformation Pattern**.

xiv. **Global Dial Plan Replication Configuration**

If Global Dial Plan Replication (GDPR) is applicable to the deployment, you must configure and create alternate number patterns that the Intercluster Lookup Service (ILS) advertises to remote clusters in the ILS network. To configure GDPR and create alternate number patterns, navigate to **Call Routing > Global Dial Plan Replication > Advertised Patterns**.

If GDPR is applicable to the deployment, you must first configure ILS by navigating to **Advanced Features > ILS Configuration**.

xv. SIP Route Pattern Configuration

You should configure SIP route patterns to replicate what was configured on the source Unified CM cluster.

To configure route patterns for SIP-based IP address or domain call routing, navigate to **Call Routing > SIP Route Pattern**.

xvi. Route Group and Route List Configuration

You should configure route groups and route lists to replicate what was previously configured on the source Unified CM cluster.

Route groups allow you to designate the order in which gateways and trunks are selected for call routing. They allow prioritization of a list of gateways and ports for outgoing trunk selection. Route groups are configured as members of route lists which associate a set of route groups and as such should be configured prior to route lists. Route lists associate a set of route groups in a specified priority order and are the target for call routing by route patterns.

To configure route groups and route lists, navigate to **Call Routing > Route/Hunt > Route Group / Route List**.

xvii. Media Resource Configuration

If applicable to the deployment, you should configure media resources to replicate the source Unified CM cluster configuration.

To configure and manage media resources like music on hold, transcoders, and conference bridges for the new system, navigate to **Media Resources** and select appropriate resources, groups / lists, and so on.

xviii. Device Pool Configuration

If applicable to the deployment, you must configure device pools to replicate the source Unified CM configuration.

Device pools define sets of common characteristics for devices including system, device, and location-related information.

To configure device pools on the system for groups of devices, navigate to **System > Device Pool**.

xix. **CTI Route Point Configuration**

If applicable to the deployment, you must configure CTI Route Point to replicate the source Unified CM configuration.

A CTI route point designates a virtual device that can receive multiple, simultaneous calls for application-controlled redirection.

To configure Computer Telephony Integration (CTI) route points, navigate to **Device > CTI Route Point**.

xx. **Phone and Client Configuration**

To add and configure phones, clients, and other endpoints on the system, navigate to **Device > Phone**.

Add phones and clients manually to replicate the devices users have in the source Unified CM configuration. Alternatively, you can use the Bulk Administration Tool (BAT) to add phones and clients to the system in bulk.

xxi. **Trunk Configuration**

You must define trunks to replicate the source Unified CM configuration.

To add and configure trunks for routing calls to other cluster, applications, or the PSTN, navigate to **Device > Trunk**.

xxii. **Device Settings Configuration**

You must configure device defaults, templates, and profiles to replicate what was configured on Unified CM previously.

To configure and manage device related settings, navigate to **Device > Device Settings** and select appropriate defaults, profiles, and templates including phone button and softkey templates, phone services, remote destination

profiles, and so on.

xxiii. Remote Destination Configuration

You must define remote destinations (and remote destination profiles) to replicate the source Unified CM configuration.

To configure remote destination numbers for single number reach and other Unified Mobility functionality, navigate to **Device > Remote Destination**. Remote destinations are assigned to remote destination profiles.

Note: Before configuring remote destinations for Unified Mobility features, you must first configure remote destination profiles. To configure remote destination profiles, navigate to **Device > Device Settings > Remote Destination Profile** (see previous step).

xiv. Headset Configuration

If applicable to the deployment, you must configure headset templates to replicate the source Unified CM configuration.

To configure and manage headsets on the system, navigate to **Device > Headset > Headset Template**. Headset templates as well as headset inventory (**Device > Headset > Headset Inventory**) provide ability to control headset configuration, firmware, inventory, troubleshooting, and diagnostics.

5. Emergency Calling Configuration

You must define and configure all emergency calling definitions and settings to exactly match what was configured on the previous Unified CM deployment.

6. Perform Initial Testing

Manually register and test a representative sample of devices. Verify that dialing habits are the same as the Unified CM environment before proceeding to the next step.

7. Prepare Phones for Transition by Consolidating TFTP Certificates

This step will directly impact users so must be performed during a maintenance window that is large enough to allow for backing out and reverting to the on-premises system if anything goes wrong.

If phone transition steps are not performed in proper order, you will have to manually delete each phone's Initial Trust List (ITL) / Certificate Trust List (CTL) files and then reset the phone. This is because Cisco IP phones authenticate downloaded TFTP files against the certificates in their ITL file.

If you need to manually delete the ITL file on each phone, perform the following:

- 78XX/88XX Series: **Settings > Administrator Settings > Reset Settings > Security Settings**.
- 89XX/99XX Series: **Settings > Administrator Settings > Reset Settings > Security Settings**.
- 79XX Series: **Settings > Security > Trust List > ITL File > **# (to unlock the settings) > Erase**.

You can circumvent the CTL/ITL issues by exchanging certificates between the Unified CM cluster and UCM Cloud cluster. Perform the following using the Bulk Certificate Management (BCM) option:

i. If Unified CM is running release 11.5 or earlier, export TFTP certificates from both the UCM Cloud and source Unified CM clusters to the same directory on temporary SFTP server shown in Figure 2.

   If Unified CM is running release 12.0 or later, export ITLRecovery certificates from both the UCM Cloud and from Unified CM clusters to the same directory on temporary SFTP server shown in Figure 2.

ii. Use Consolidate on both the UCM Cloud and source Unified CM clusters to create a PKCS12 file which contains certificates for both Unified CM and UCM Cloud.

iii. On both the UCM Cloud and source Unified CM clusters, use BCM to import the TFTP / ITLRecovery certificates from the SFTP server.

The key is to import the UCM Cloud TFTP / ITLRecovery certificates into the Unified CM phone-SAST-trust so that phones can trust and accept the CTL/ITL files of UCM Cloud when they migrate to UCM Cloud. If the UCM Cloud is in mixed mode, Locally Significant Certificates (LSC) are installed on the phones, and phones are configured in encrypted mode, then use BCM in order to also exchange the Certificate Authority Proxy Function (CAPF) certificates between the clusters. In general, a simpler option that works with any Unified CM release, whether mixed mode is enabled or not, or whether LSC certificates are installed or not, is to use BCM and select the option "All" in order to exchange all certificates.

For additional details refer to the **Procedure for Bulk Certificate Management Between Unified CM Clusters for Phone Migration** technote available at https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/215539-procedure-for-bulk-certificate-managemen.html.

Refer to the *Phone Verifies ITL and Configuration File* section of the **Unified CM Security By Default and ITL Operation and Troubleshooting** technote available at https://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-callmanager/116232-technote-sbd-00.html for details on how phones will verify the CTL/ITL during migration.

8. Configure DNS SRV Records

Because the steps from this point on directly impact users and transition their devices to UCM Cloud, the following steps must be performed during a maintenance window that is large enough to allow for backing out and returning to the on-premises deployment if anything goes wrong.

You must change the _cisco-uds._tcp.<domain> DNS SRV record to point to the UCM Cloud servers instead of the on-premises Unified CM servers. When devices power up or refresh their DNS information, they will learn about the UCM Cloud infrastructure and no longer know about the on-premises Unified CM infrastructure.

9. Configure DHCP Options

You must change DHCP Option150 and any DHCP options the customer's Unified CM deployment required to direct devices to appropriate UCM Cloud resources and away from the on-premises Unified CM server(s).

Use BAT or similar method to restart all phones and verify that when they come back up, they successfully register to UCM Cloud.

10. Perform Final Testing

Preform the following final tasks to verify that all devices and features have been successfully transitioned to UCM Cloud:

- Power-cycle a phone and verify that the response it gets from DHCP and DNS cause it to successfully register to the UCM Cloud cluster.
- Reset a Jabber client and verify that it successfully registers to the UCM Cloud cluster.
- Refer to the user workflow and dialing habits of representative users that you documented pre-migration and verify that each user's device is registered to the UCM Cloud and their dialing habits continue to work in the expected manner. Be sure to include emergency calling tests.
- Verify that Music on Hold works as expected
- Working with the customer's administration staff, verify that:
  - User MACD operations can be performed in the same manner as before migration
  - Adding a new device can be performed in the same manner as before migration
  - Registering a previously unregistered phone works as expected

Post-Transition Steps and Considerations

Once the transition from Unified CM to UCM Cloud is complete, there are a few additional steps that should be considered:

1. Handover Document for End Users

Provide the customer an end-user document explaining that:

- The system has undergone maintenance.
- There should be no changes in phone behavior.
- Their call history will have been cleared.
- They should reset Jabber.

Provide hotline contact information for the morning after cutover to the UCM Cloud so users can easily receive any needed assistance.

2. Decommission the On-Premises Unified CM Cluster

Delete or remove all on-premises Unified CM cluster node virtual machines and/or servers. Repurpose compute resources and hardware as needed. These resources are no longer needed for call control. You may also remove any other on-premises collaboration application nodes and or servers which have been replicated in the cloud.

References

Cisco Unified CM

- Unified CM Command Line Interface Reference Guide for Release 12.5(1)

  https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/cli_ref/12_5_1/cucm_b_cli-reference-guide-1251.pdf

- Unified CM Bulk Administration Guide for Release 12.5(1)

  https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/bat/12_5_1/cucm_b_bulk-administration-guide-1251.html

- AXL Developer Guide

  https://developer.cisco.com/docs/axl/#!axl-developer-guide

- Unified CM Disaster Recovery System (DRS)

  https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/11_5_1/Admin/cucm_b_administration-guide-1151/cucm_b_administration-guide-1151_chapter_01010.html

- Migrate Phones Between Secure Clusters Technote

  https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/213407-migrate-phones-between-secure-clusters.html

- Unified CM Deprecated Phone Models

  https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-device-support-tables-list.html

- Unified CM Certificate Regeneration/Renewal Process

  https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/200199-CUnified CM-Certificate-Regeneration-Renewal-Pr.html

- Unified CM Manually Verifying Phone's ITL with UCM Cloud's ITL

  https://www.cisco.com/c/en/us/support/docs/voice-unified-

communications/unified-communications-manager-callmanager/116232-technote-sbd-00.html#anc9

Cisco UCM Cloud

- UCM Cloud Partner Help Desk Portal

  https://ucmcloudhelp.cisco.com/

- UCM Cloud SalesConnect Documentation

  https://salesconnect.cisco.com/#/program/PAGE-15188

Unified CM IM & Presence

- Unified CM IM & Presence Export Contact Lists

  https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/configAdminGuide/12_5_1/cup0_b_config-and-admin-guide-1251/cup0_b_config-and-admin-guide-1251_chapter_0100011.html?dtid=osscdc000283#task_0F2C26E2BC3929146D9AF931141F1691

Cisco Unified Communications Tools

- Unity Connection Tools

  https://ciscunitytools.com

Collaboration Preferred Architectures

- Collaboration Preferred Architectures Page

  https://www.cisco.com/go/pa

Collaboration Transitions

- Collaboration Transitions Program Page

  https://www.cisco.com/go/ct

- Transition Map for Transitioning from Unified CM to UCM Cloud

  https://www.cisco.com/c/dam/en/us/td/docs/solutions/PA/mcp/TDM_CALLING_UnifiedCM_to_UCM_Cloud.pdf

Appendix: Worksheet of Tasks

Table 4 below provides a worksheet overview of the tasks listed in this document.

Table 4. *Unified CM to UCM Cloud Transition Worksheet of Tasks*

Step / Consideration	Complete?
PRE-TRANSITION STEPS AND CONSIDERATIONS	
Develop a back-out option	
Instruct users to prepare for transition to UCM Cloud	
Inventory existing endpoints and Jabber clients	
Upgrade all endpoints to latest enterprise phone firmware	
Audit the existing Unified CM deployment	
TRANSITION STEPS AND CONSIDERATIONS	
Certificate Configuration	
Cluster Security Mode Configuration	
TFTP Files	
UC Service Configuration	
Service Profile Configuration	
Feature Group Template Configuration	
Authentication and Authorization Configuration	
LDAP Synchronization Agreement Configuration	
Unified CM Group Configuration	
Partition Configuration	

Calling Search Space Configuration	
Route Partition Configuration	
Directory Number Configuration	
Translation Pattern Configuration	
Call Park and Call Pickup	
Transformation Pattern Configuration	
Global Dial Pattern Replication	
SIP Route Pattern Configuration	
Route Group and Route List Configuration	
Media Resource Configuration	
Device Pool Configuration	
CTI Route Point Configuration	
Phone and Client Configuration	
Trunk Configuration	
Remote Destination Configuration	
Device Settings Configuration	
Trunk Configuration	
Headset Configuration	
LDAP Synchronization Agreement Configuration	
Emergency Calling Configuration	
Perform Initial Testing	

Preparing Phones for Transition by Consolidating TFTP Certificates	
Configure DNS SRV Records	
Configure DHCP OPTIONs	
Perform Final Testing	
POST-TRANSITION STEPS AND CONSIDERATIONS	
Handover Document for End Users	
Decommission the On-Premises Unified CM Cluster	

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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