CALLING

Transitioning from Unified CM to Unified CM Cloud

Deployment Guide

May 27, 2020

© 2020 Cisco – CTG TME
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>3</td>
</tr>
<tr>
<td>TARGET AUDIENCE</td>
<td>3</td>
</tr>
<tr>
<td>OVERVIEW</td>
<td>3</td>
</tr>
<tr>
<td>CORE COMPONENTS</td>
<td>8</td>
</tr>
<tr>
<td>TRANSITION</td>
<td>10</td>
</tr>
<tr>
<td>PRE-TRANSITION STEPS AND CONSIDERATIONS</td>
<td>10</td>
</tr>
<tr>
<td>1. Develop a Back-Out Option</td>
<td>10</td>
</tr>
<tr>
<td>2. Instruct Users to Prepare for Transition to Unified CM Cloud</td>
<td>11</td>
</tr>
<tr>
<td>3. Inventory Existing Endpoints and Jabber Clients</td>
<td>11</td>
</tr>
<tr>
<td>4. Upgrade All Endpoints to the Latest Enterprise Phone Firmware</td>
<td>11</td>
</tr>
<tr>
<td>5. Audit the Existing Unified CM Deployment</td>
<td>12</td>
</tr>
<tr>
<td>TRANSITION STEPS AND CONSIDERATIONS</td>
<td>13</td>
</tr>
<tr>
<td>1. Certificate Management</td>
<td>14</td>
</tr>
<tr>
<td>2. Cluster Security Mode Configuration</td>
<td>14</td>
</tr>
<tr>
<td>3. TFT Files</td>
<td>14</td>
</tr>
<tr>
<td>4. Replicate Unified CM Configuration on Unified CM Cloud Deployment</td>
<td>14</td>
</tr>
<tr>
<td>5. Emergency Calling Configuration</td>
<td>22</td>
</tr>
<tr>
<td>6. Perform Initial Testing</td>
<td>22</td>
</tr>
<tr>
<td>7. Prepare Phones for Transition by Consolidating TFTP Certificates</td>
<td>22</td>
</tr>
<tr>
<td>8. Configure DNS SRV Records</td>
<td>24</td>
</tr>
<tr>
<td>9. Configure DHCP Options</td>
<td>24</td>
</tr>
<tr>
<td>10. Perform Final Testing</td>
<td>24</td>
</tr>
<tr>
<td>POST-TRANSITION STEPS AND CONSIDERATIONS</td>
<td>25</td>
</tr>
<tr>
<td>1. Handover Document for End Users</td>
<td>25</td>
</tr>
<tr>
<td>2. Decommission the On-Premises Unified CM Cluster</td>
<td>25</td>
</tr>
<tr>
<td>REFERENCES</td>
<td>26</td>
</tr>
<tr>
<td>CISCO UNIFIED CM</td>
<td>26</td>
</tr>
<tr>
<td>CISCO UNIFIED CM CLOUD</td>
<td>27</td>
</tr>
<tr>
<td>COLLABORATION TRANSITIONS</td>
<td>27</td>
</tr>
<tr>
<td>COLLABORATION PREFERRED ARCHITECTURES</td>
<td>27</td>
</tr>
<tr>
<td>APPENDIX: WORKSHEET OF TASKS</td>
<td>28</td>
</tr>
</tbody>
</table>
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 Unified CM Cloud. This document does not address any of the following which are documented on the Unified CM Cloud Help site available at https://ucmcloudhelp.cisco.com/ and the Cisco Unified Communications Manager Cloud SaleConnect site available at https://salesconnect.cisco.com/#/program/PAGE-15188:

- Unified CM Cloud sales cycle
- Unified CM Cloud business agreements
- Unified CM Cloud partner onboarding
- Unified CM Cloud partner operations
- Unified CM Cloud customer onboarding
- Unified CM Cloud analytics

Once the Unified CM 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 Unified CM 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 Unified CM 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 Unified CM Cloud instead of Unified CM.

Related Unified CM Cloud Documents

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

- **Completed Build Document**
  The completed “Unified CM Cloud Build Document” is the documented result of the implemented CQ and is authored by the Cisco team that built the customer’s private Unified CM 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 Unified CM 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 Cisco Unified CM for call control, Cisco 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, Cisco Webex DX and Room) 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**

Table 1 lists the key elements of the on-premises architecture prior to transitioning to Unified CM Cloud.
Table 1. Before: On-Premises Calling Infrastructure Components

<table>
<thead>
<tr>
<th>Product</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified CM</td>
<td>On-premises call control providing device registration and call routing services</td>
</tr>
<tr>
<td>Cisco Expressway-C/E</td>
<td>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]</td>
</tr>
<tr>
<td>Cisco Unity Connection</td>
<td>On-premises voice messaging platform providing voicemail and unified messaging capabilities. [Optional]</td>
</tr>
<tr>
<td>Cisco Instant Messaging and Presence</td>
<td>On-premises messaging, presence, and contacts services. [Optional]</td>
</tr>
<tr>
<td>Cisco Emergency Responder</td>
<td>On-premises emergency enhancement services. [Optional]</td>
</tr>
<tr>
<td>Cisco IP Phones and Cisco Jabber</td>
<td>IP-based devices registered to Unified CM and provides voice and video calling capabilities</td>
</tr>
</tbody>
</table>

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 Unified CM 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.
Once the Unified CM environment is migrated to Unified CM 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 Unified CM Cloud components deployed in Cisco’s cloud as depicted in Figure 3.

Figure 3. After: Cisco Unified CM Cloud Calling

Figure 3 also shows an SFTP server on the customer’s network, accessible to both the on-premises Unified CM and Unified CM 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 Unified CM 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)
Core Components

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 Unified CM 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 2 lists the new elements of the architecture after transitioning to Unified CM Cloud.

**Table 2. After: Unified CM Cloud Calling Infrastructure Components**

<table>
<thead>
<tr>
<th>Product</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified CM Cloud</td>
<td>Unified CM Cloud call control providing device registration and call routing services</td>
</tr>
<tr>
<td>Cisco Expressway–C/E</td>
<td>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]</td>
</tr>
<tr>
<td>Cisco Unity Connection Cloud</td>
<td>Unified CM Cloud voice messaging platform providing voicemail and unified messaging capabilities. [Optional]</td>
</tr>
<tr>
<td>Cisco Instant Messaging and Presence Cloud</td>
<td>Unified CM Cloud messaging, presence, and contacts services. [Optional]</td>
</tr>
<tr>
<td>Cisco Emergency Responder Cloud</td>
<td>Unified CM Cloud on-premises emergency enhancement services. [Optional]</td>
</tr>
<tr>
<td>Cisco IP Phones and Cisco Jabber</td>
<td>IP–based devices registered to Unified CM Cloud and provides voice and video calling capabilities</td>
</tr>
</tbody>
</table>
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 Unified CM 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 Unified CM 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 Unified CM 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 Unified CM Cloud.

1. Develop a Back-Out Option

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


   Once the Unified CM 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 Unified CM Cloud**

   Notify users that they should prepare to lose at least the following:
   - Call history for both phones and Jabber
   - Speed dials for both phones and Jabber
   - Voicemail messages for both phones and Jabber
   - Jabber chat history
   - Jabber contact lists

3. **Inventory Existing Endpoints and Jabber Clients**


   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 Unified CM Cloud so that they do not immediately upgrade on initial registration to Unified CM Cloud. Upgrading before moving to Unified CM Cloud will result in a more efficient transition process for the team performing the transition to Unified CM 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**

![Non-Default Firmware Load Information](image)

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 5 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
Transition

- 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 Unified CM Cloud to replicate their existing Unified CM configuration.

Once you have completed configuring Unified CM 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 Unified CM 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 Unified CM 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 Unified CM 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 Unified CM 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 Unified CM Cloud Deployment**

   The following configuration parameters on the source Unified CM deployment will need to be replicated on the Unified CM 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 Unified CM 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 Unified CM 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 Unified CM 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).
iii. Feature Group Template Configuration

You should define Feature Group Templates for the LDAP sync agreement to apply when synchronizing users on the production Unified CM 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 Unified CM 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 Unified CM 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 Unified CM 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.
Transition

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 back 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 Unified CM Cloud cluster. Perform the following using the Bulk Certificate Management option:

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

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

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

The key is to import the Unified CM Cloud TFTP / ITLRecovery certificates into the Unified CM phone-SAST-trust so that phones can trust and accept the CTL/ITL files of Unified CM Cloud when they migrate to Unified CM Cloud. If the Unified CM Cloud is in mixed mode, Locally Significant Certificates (LSC) are installed on the phones, and phones are configured in encrypted mode, then use Bulk Certificate Management 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 Bulk Certificate Management and select the option “All” in order to exchange all certificates.


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 Unified CM 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 Unified CM Cloud servers instead of the on-premises Unified CM servers. When devices power up or refresh their DNS information, they will learn about the Unified CM Cloud infrastructure and no longer know about the on-premises Unified CM infrastructure.

9. Configure DHCP Options

You must change DHCP Option 150 and any DHCP options the customer’s Unified CM deployment required to direct devices to appropriate Unified CM 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 Unified CM Cloud.

10. Perform Final Testing

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

- Power-cycle a phone and verify that the response it gets from DHCP and DNS cause it to successfully register to the Unified CM Cloud cluster.

- Reset a Jabber client and verify that it successfully registers to the Unified CM 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 Unified CM 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 Unified CM 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 Unified CM 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 Bulk Administration Guide for Release 12.5(1)

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

- Unified CM Disaster Recovery System (DRS)

- Migrate Phones Between Secure Clusters Technote

- Unified CM Deprecated Phone Models

- Unified CM Certificate Regeneration/Renewal Process

- Unified CM Manually Verifying Phone’s ITL with Unified CM Cloud’s ITL
  https://www.cisco.com/c/en/us/support/docs/voice-unified-
Cisco Unified CM Cloud

- Unified CM Cloud Partner Help Desk Portal
  https://ucmcloudhelp.cisco.com/
- Unified CM Cloud SalesConnect Documentation
  https://salesconnect.cisco.com/#/program/PAGE-15188

Collaboration Transitions

- Collaboration Transitions Program Page
  https://www.cisco.com/go/ct

Collaboration Preferred Architectures

- Collaboration Preferred Architectures Page
  https://www.cisco.com/go/pa
Appendix: Worksheet of Tasks

Table 3 below provides a worksheet overview of the tasks listed in this document.

Table 3. Unified CM to Unified CM Cloud Transition Worksheet of Tasks

<table>
<thead>
<tr>
<th>Step / Consideration</th>
<th>Complete?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PRE-TRANSITION STEPS AND CONSIDERATIONS</strong></td>
<td></td>
</tr>
<tr>
<td>Develop a back-out option</td>
<td></td>
</tr>
<tr>
<td>Instruct users to prepare for transition to Unified CM Cloud</td>
<td></td>
</tr>
<tr>
<td>Inventory existing endpoints and Jabber clients</td>
<td></td>
</tr>
<tr>
<td>Upgrade all endpoints to latest enterprise phone firmware</td>
<td></td>
</tr>
<tr>
<td>Audit the existing Unified CM deployment</td>
<td></td>
</tr>
<tr>
<td><strong>TRANSITION STEPS AND CONSIDERATIONS</strong></td>
<td></td>
</tr>
<tr>
<td>Certificate Configuration</td>
<td></td>
</tr>
<tr>
<td>Cluster Security Mode Configuration</td>
<td></td>
</tr>
<tr>
<td>TFTP Files</td>
<td></td>
</tr>
<tr>
<td>UC Service Configuration</td>
<td></td>
</tr>
<tr>
<td>Service Profile Configuration</td>
<td></td>
</tr>
<tr>
<td>Feature Group Template Configuration</td>
<td></td>
</tr>
<tr>
<td>Authentication and Authorization Configuration</td>
<td></td>
</tr>
<tr>
<td>LDAP Synchronization Agreement Configuration</td>
<td></td>
</tr>
<tr>
<td>Unified CM Group Configuration</td>
<td></td>
</tr>
<tr>
<td>Partition Configuration</td>
<td></td>
</tr>
</tbody>
</table>
### Appendix: Worksheet of Tasks

<table>
<thead>
<tr>
<th>Calling Search Space Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Partition Configuration</td>
</tr>
<tr>
<td>Directory Number Configuration</td>
</tr>
<tr>
<td>Translation Pattern Configuration</td>
</tr>
<tr>
<td>Call Park and Call Pickup</td>
</tr>
<tr>
<td>Transformation Pattern Configuration</td>
</tr>
<tr>
<td>Global Dial Pattern Replication</td>
</tr>
<tr>
<td>SIP Route Pattern Configuration</td>
</tr>
<tr>
<td>Route Group and Route List Configuration</td>
</tr>
<tr>
<td>Media Resource Configuration</td>
</tr>
<tr>
<td>Device Pool Configuration</td>
</tr>
<tr>
<td>CTI Route Point Configuration</td>
</tr>
<tr>
<td>Phone and Client Configuration</td>
</tr>
<tr>
<td>Trunk Configuration</td>
</tr>
<tr>
<td>Remote Destination Configuration</td>
</tr>
<tr>
<td>Device Settings Configuration</td>
</tr>
<tr>
<td>Trunk Configuration</td>
</tr>
<tr>
<td>Headset Configuration</td>
</tr>
<tr>
<td>LDAP Synchronization Agreement Configuration</td>
</tr>
<tr>
<td>Emergency Calling Configuration</td>
</tr>
<tr>
<td>Perform Initial Testing</td>
</tr>
</tbody>
</table>
### Appendix: Worksheet of Tasks

<table>
<thead>
<tr>
<th>Preparing Phones for Transition by Consolidating TFTP Certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure DNS SRV Records</td>
</tr>
<tr>
<td>Configure DHCP OPTIONs</td>
</tr>
<tr>
<td>Perform Final Testing</td>
</tr>
</tbody>
</table>

### POST-TRANSITION STEPS AND CONSIDERATIONS

| Handover Document for End Users                               |
| Decommission the On-Premises Unified CM Cluster               |