Cisco Hosted Collaboration Solution
Shared Architecture
Recommended Deployment

White Paper
# Contents

Introduction ................................................................................................................................................................ 4
Cisco HCS Shared Architecture........................................................................................................................................ 5
Assumptions .................................................................................................................................................................. 5
Endpoints Support ............................................................................................................................................................ 5
Prerequisites .................................................................................................................................................................. 5
Caveats ......................................................................................................................................................................... 6
Software Matrix from Lab ............................................................................................................................................. 6
Infrastructure Setup ........................................................................................................................................................ 6
VM and Cluster Setup ..................................................................................................................................................... 6
UC App OVA Specifications ......................................................................................................................................... 6
Expressway OVA Specifications .................................................................................................................................... 7
Recommended Virtual Machine Sizing ............................................................................................................................ 7
Install and Configure Cisco Unified Communications Manager .................................................................................. 8
Install and Configure IM&P ........................................................................................................................................... 8
Install and Configure CUC ............................................................................................................................................ 8
Install Expressway on VM ............................................................................................................................................... 8
Configure HCM-F ........................................................................................................................................................... 8
Cisco Unified CDM Setup – Cluster Configuration ......................................................................................................... 9
Add HCM-F to CUCDM .................................................................................................................................................... 9
Add Provider to CUCDM .................................................................................................................................................... 9
Assign a Cluster to a License Manager in HCM-F ............................................................................................................ 9
Configure UC Cluster in CUCDM .................................................................................................................................... 10
Single Sign On ............................................................................................................................................................... 12
Configure Single Sign-On for Cisco Unified Communications Domain Manager .......................................................... 13
Set up Circle of Trust (Co-T) ........................................................................................................................................... 16
Configuring the Expressway-C for Unified Communications .......................................................................................... 17
Configuring DNS and NTP settings .................................................................................................................................. 17
Enabling Mobile and Remote Access ................................................................................................................................ 17
Configuring the Domains to Route to Unified CM ................................................................................................................ 17
Configure SIP .................................................................................................................................................................. 18
Configuring Unified CM Servers ....................................................................................................................................... 18
Configure a Unified Communications Traversal Zone to Expressway-E ........................................................................... 19
Configure the Expressway-E for MRA ............................................................................................................................... 19
Configuring DNS, NTP, and IP Settings ............................................................................................................................. 20
Configure Mobile and Remote Access .................................................................................................................................. 20
Configure SIP .................................................................................................................................................................. 21
Create the DNS Zone .......................................................................................................................................................... 21
Configure a Unified Communications Traversal Zone to Expressway-C ........................................................................... 22
Cisco Unified CM Setup – Call Routing .............................................................................................................................. 23
Setting up the Hierarchy ...................................................................................................................................................... 25
Configure Entitlement ........................................................................................................................................................ 25
Configure a Network Device List ....................................................................................................................................... 26
CUCM Group Configuration .............................................................................................................................................. 26
Create a Customer Dial Plan .............................................................................................................................................. 27
Add a Country Dial Plan to a Dial Plan Before Deploying to a Customer ............................................................................. 28
Add a Site ........................................................................................................................................................................ 29
Add First Site Dial Plan ...................................................................................................................................................... 31
Cisco Unified CDM Number Management .......................................................................................................................... 33
Add Directory Number Inventory .......................................................................................................................................... 33
Configure Directory Number Routing .................................................................................................................................. 35
Associate a Range of E.164 Numbers to a Range of Directory Numbers ........................................................................... 35
Add Central Breakout SIP Trunk .......................................................................................................................................... 36
Cisco UCDM SIP Trunk Settings ........................................................................................................................................ 36
SBC ................................................................................................................................................................................. 38
Create Customer and Users in AD ....................................................................................................................................... 38
LDAP Integration in Cisco Unified CDM ............................................................................................................................. 39
Set up an LDAP Server ...................................................................................................................................................... 39
Set up LDAP for User Synchronization ............................................................................................................................... 40
Auto Move Users to Site .................................................................................................................................................... 42
Synchronize Users from LDAP .............................................................................................................................................. 42
Move Users to Site (optional if not automatically done from above) .................................................................................. 43
Fill in the CUCM LDAP Directory Name field in the LDAP Server on CUCDM ........................................................................... 47
Introduction

HCS Shared Architecture (SA) enables our partner to provide a true UCaaS service for customers with the best collaboration solution and a more affordable price. Shared Architecture also provides HCS partners with the ability to deploy the Unified Communications solution via Over the Top (OTT) for customers.

HCS SA not only allows partner to save capex investment at Data Center (DC) by sharing the Unified Communications (UC) cluster with multiple tenants, it also paves the way to automate the customer/user onboarding process for partner to save even more on Operation Expenses (Opex). By introducing OTT access for all end-points, essentially, end user shall be able to follow a simple instruction to register their phone and/or jabber via auto-registration process.

Although HCS SA is designed to provide UCaaS service for customers with less than 100 users, nothing exists to prevent HCS SA from providing service for a larger customer. Indeed, HCS SA is a perfect solution for a large customer with a lot of small sites.

Shared Architecture is Partner Cloud Collaboration Service for 100 users or less. It has Full suites of collaboration offers from dial tone, video, mobility to team collaboration.

Here is a list of customer profiles for HCS SA:

- Government Agencies
- Large Retailers
- Franchise Stores
- Small to Medium Business
- Public Schools
- Any business/organization which has distributed office/store locations and requires mobility

This whitepaper provides configuration steps for Shared Architecture. These steps have been validated in Cisco labs to help partners deploy the solution quickly and easily.

It is recommended partners reference the Cisco HCS Solution Reference Network Design (SRND) for further details.
Cisco HCS Shared Architecture

Assumptions

- SAN has been deployed and configured
- VMware licenses purchased and installed
- The management applications have been installed i.e.
  - Cisco Unified Communications Domian Manager(CUCDM) 10.6.3
  - Cisco Hosted Collaboration Mediation Fulfillment(HCM-F)
  - Prime License Manager(PLM)
  - Prime Collaboration Assurance(PCA)(used for moitoring the UC cluster only and not for shared customers)
- Using partner provided IT domain example, ciscolabs.com for collaboration. Partner managed domain will be shared by other customers.

Endpoints Support

The Cisco HCS shared Instance architecture supports the following endpoints:

- Cisco Jabber Desktop – Windows, MacOS
- Cisco Jabber Mobile - iPhone, Android, and iPad
- Cisco IP Phones 8800 and 7800 series Cisco DX series, Cisco SX series

Prerequisites

- Software Downloads
- Licenses
Caveats

Users’ passwords managed within Partner AD.

Software Matrix from Lab

Table 1: Software matrix from lab

<table>
<thead>
<tr>
<th>Component</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified CDM</td>
<td>10.6.3 SU1a</td>
</tr>
<tr>
<td>CUCM</td>
<td>10.5.2</td>
</tr>
<tr>
<td>IM&amp;P</td>
<td>10.5.2</td>
</tr>
<tr>
<td>CUC</td>
<td>10.5.2</td>
</tr>
<tr>
<td>Expressway-C</td>
<td>X8.7, X8.8, X8.9</td>
</tr>
<tr>
<td>Expressway-E</td>
<td>X8.7, X8.8, X8.9</td>
</tr>
<tr>
<td>Imagicle Application Suite for</td>
<td>Winter Release</td>
</tr>
<tr>
<td>Cisco UC</td>
<td></td>
</tr>
</tbody>
</table>

Infrastructure Setup

- Management components to be implemented in existing Management Virtual Route Forwarding (VRF) table using available IP addresses in this space.
- UC Applications to be implemented in new shared VRF just like any other customer UC apps in a dedicated instance.
- Session Border Controller (SBC) interface for shared cluster to be in shared VRF with UC apps.
- Shared VRF will need to be extended from DC PE to Core Nexus 7000 and Aggregation Nexus 7000 - Just like any other Tenant (in case of MPLS).
- Create a context for shared VRF in the Firewall just like any other tenant.
- Per customer VRF to be terminated on Data Center Provider Edge (in case of MPLS).
- Partners may use 'Cisco HCS DC Flexibility Guide' to innovate their own DC based on legacy VMDC 3.0 architecture or Application Centric Infrastructure.

VM and Cluster Setup

UC App OVA Specifications

Table 2: OVA for UC Apps

<table>
<thead>
<tr>
<th>Application</th>
<th>CPU</th>
<th>RAM (GB)</th>
<th>HD(GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Communications Manager – 2,500 Users</td>
<td>2x800 MHz*</td>
<td>4</td>
<td>80</td>
</tr>
<tr>
<td>Unified Communications Manager – 7,500 Users</td>
<td>2 Cores</td>
<td>6</td>
<td>110</td>
</tr>
<tr>
<td>Unified Communications Manager – 10,000 Users</td>
<td>4 Cores</td>
<td>6</td>
<td>110</td>
</tr>
</tbody>
</table>
## Expressway OVA Specifications

### Table 3: Required Minimum Specifications for Expressway by Deployment Size

<table>
<thead>
<tr>
<th>Deployment size</th>
<th>vCPU</th>
<th>Reserved CPU Resource</th>
<th>Reserved RAM</th>
<th>Disk space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small (for Business Edition 6000 platform)</td>
<td>2 core</td>
<td>3600 MHz (2x1.8GHz)</td>
<td>4GB</td>
<td>132GB</td>
</tr>
<tr>
<td>Medium (typical installation)</td>
<td>2 core</td>
<td>4800MHz (2x2.4GHz)</td>
<td>6GB</td>
<td>132GB</td>
</tr>
<tr>
<td>Large (extra performance and scalability capabilities)</td>
<td>8 core</td>
<td>25600MHz (8x3.2GHz)</td>
<td>8GB</td>
<td>132GB</td>
</tr>
</tbody>
</table>

## Recommended Virtual Machine Sizing

### Table 4: VM Sizing for different users

<table>
<thead>
<tr>
<th>Server</th>
<th>4000 users</th>
<th>7.5K OVA Customer Limit-340</th>
<th>Hardware-3xB200 M4</th>
</tr>
</thead>
<tbody>
<tr>
<td>UC manager</td>
<td>1 Pub/TFTP,2 Sub</td>
<td>5K Ova</td>
<td>6 Cores</td>
</tr>
<tr>
<td>Unified Presence</td>
<td>2 Nodes</td>
<td>5K Ova Customer Limit-40</td>
<td>4 Cores</td>
</tr>
<tr>
<td>Unity Connection</td>
<td>1Pub,1 Sub Active-Active</td>
<td>Medium OVA 10,000 registrations,800 active calls</td>
<td>4 Cores</td>
</tr>
<tr>
<td>Expressway Cluster(C&amp;E)</td>
<td>6 Exp C,6 Exp E</td>
<td>24 Cores</td>
<td>24 Cores</td>
</tr>
<tr>
<td>Imagicle UC App suite</td>
<td>2 Nodes</td>
<td>8 Cores (Co resident with AD/DNS)</td>
<td>8 Cores</td>
</tr>
<tr>
<td>AD</td>
<td>1 Node</td>
<td>1 or 2 Nodes-Primary/Secondary</td>
<td>1 or 2 Nodes-Primary/Secondary</td>
</tr>
<tr>
<td>DNS</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Server Sizing

<table>
<thead>
<tr>
<th>User Type</th>
<th>OVA Size 1</th>
<th>OVA Size 2</th>
<th>OVA Size 3</th>
<th>OVA Size 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>12 Exp C, 12 Exp E (2 Clusters)</td>
<td>10K OVA</td>
<td>2x5K OVA</td>
<td>10K OVA</td>
<td>2 Medium OVA clusters, 10,000, 1,600 active calls</td>
</tr>
<tr>
<td>8000 users</td>
<td>1 Pub, 1 TFTP, 3 Sub</td>
<td>4 Nodes</td>
<td>1 Pub, 2 Sub</td>
<td>1 or 2 Nodes - Primary/Secondary</td>
</tr>
</tbody>
</table>

### Hardware

<table>
<thead>
<tr>
<th>Hardware Type</th>
<th>Cores 1</th>
<th>Cores 2</th>
<th>Cores 3</th>
<th>Cores 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>7x B200M4</td>
<td>16 Cores</td>
<td>8 Cores</td>
<td>12 Cores</td>
<td>48 Cores</td>
</tr>
</tbody>
</table>

### Procedure

**Step 1** Review the installation requirements and record the configuration settings for each server that you plan to install.

**Step 2** For every node in your cluster, create virtual machines using the Virtual Server Template (OVA file) recommended for your current release.

Different OVA files are available; choose the correct OVA file based on the environment in which you are deploying.

**Step 3** OVA Templates can be downloaded from the following locations:

- [Cisco Unified Communications Manager](https://cisco.com)
- [IM&P](https://cisco.com)
- [CUC](https://cisco.com)
- [Expressway](https://cisco.com)

#### Install and Configure Cisco Unified Communications Manager

Refer to the *Installation guide for Cisco Unified Communications Manager* on [cisco.com](https://cisco.com) for details of installation.

#### Install and Configure IM&P

Refer to the *Installation guide for Cisco Unified IM and Presence* on [cisco.com](https://cisco.com) for details of installation.

#### Install and Configure CUC

Refer to the *Installation guide for Cisco Unity Connection* on [cisco.com](https://cisco.com) for details of installation.

#### Install Expressway on VM

For installation instructions, please review the *installation* guide on [cisco.com](https://cisco.com).

#### Configure HCM-F

For customers on Cisco Unified Communications Domain Manager 10.6(x), the information will be pushed from the Cisco Unified Communications Domain Manager server to the Cisco HCM-F server and does not require configuration.
Cisco Unified CDM Setup – Cluster Configuration

Add HCM-F to CUCDM

Procedure

Step 1  Login as hcsadmin.
Step 2  Go to Device Management > HCMF.
Step 3  Click Add and fill in the hostname, admin credentials, and version.
Step 4  Click Save.

Add Provider to CUCDM

Procedure

Step 1  Login as hcsadmin.
Step 2  Go to Provider Management > Providers
Step 3  Click Add and fill in the name, domain name, and admin credentials
Step 4  Click Save.

Add a License Manager to HCM-F
A separate PLM (standalone) is recommended for Shared Architecture customers. If a partner plans to implement a reseller program, a separate PLM (standalone) is suggested for each reseller to manage the license properly. A partner can also use existing PLM.

Procedure

Step 1  From the side menu, select License Management > License Manager Summary.
Step 2  Click Add New.
Step 3  Enter the licensing details.
Step 4  Click Save.

Assign a Cluster to a License Manager in HCM-F

Procedure

Step 1  From the Infrastructure Manager interface, select License Management > License Manager Summary.
Step 2  Select the License Manager to which you want to assign a cluster.
Step 3  Expand the Clusters Managed by section.
Step 4  Click Assign.
Step 5  Select the cluster you want to assign and click Assign.
Configure UC Cluster in CUCDM

Procedure

Step 1  Log in as the appropriate hierarchy administrator.
  Only a provider administrator can create a shared instance.

Step 2  Set the hierarchy path to the top level. Create a shared instance node at the provider level. Optionally, partners can create a reseller node.
  The UC cluster server should be placed either at shared instance provider node or the reseller node (exclusive Shared instance cluster for the reseller).

Step 3  Click Device Management > CUCM > Servers.

Step 4  Click Add.

Step 5  Enter the Unified CM server name in the CUCM Server Name field.
  A Unified CM server that has been configured in HCM-F and synced into Cisco Unified Communications Domain Manager may exist at the sys.hcs hierarchy. If the server name you enter matches this server, the Migrate from HCM-F to Unified CDM check box is displayed. Click Save to migrate this server to the current hierarchy level. The fields are populated with the values that were configured in HCM-F. If you do not want to migrate the server, enter a different server name.

Step 6  Select Voice/Video in the Server Type field.

Step 7  To configure a publisher node, check Publisher.
  On the Publisher tab, you can specify the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prime Collaboration</td>
<td>Select the Prime Collaboration management application monitoring this cluster. To unassociate Prime Collaboration for this cluster, select None.</td>
</tr>
<tr>
<td>Call Processing ID</td>
<td>The Call Processing ID of this cluster.</td>
</tr>
<tr>
<td>Cluster ID</td>
<td>The Cluster ID of this cluster.</td>
</tr>
<tr>
<td>Multi-Tenant</td>
<td>Read-only field. If creating at provider level, this field is set to Shared. If creating at customer level, this field is set to Dedicated.</td>
</tr>
<tr>
<td>Version</td>
<td>Select the version of the Unified CM Servers in this cluster. The available versions depend on the version of the HCM-F device that has been configured.</td>
</tr>
<tr>
<td>Port</td>
<td>The port on the Unified CM server to connect to. Default is 8443.</td>
</tr>
<tr>
<td>User Move Mode</td>
<td>Set to Automatic to automatically move synced in users to sites, based on the filters and filter order defined in User Management &gt; Manage Filters.</td>
</tr>
</tbody>
</table>
Step 8  For a Unified CM Publisher node, fill in the Cluster Name field with the name you want for this cluster. A new cluster is created with this name. This field is required. For Unified CM Subscribers, select the Unified CM cluster from the Cluster Name pull-down menu.

Step 9  Expand Network Addresses.
   a. Select the SERVICE_PROVIDER_SPACE address space.
   b. The Hostname field is automatically populated with the Unified CM Server Name. Edit it if necessary.
   c. Enter the IP address of the Cisco Unified Communications Manager Server in the IPv4 Address field.

      Either the hostname or the IP address as required. Ensure that the hostname or IP address does not contain a trailing blank space. Unified CDM cannot validate an entry that contains a blank space at the end of the hostname or IP address.

   d. Fill in the domain of the Unified CM application.
   e. Provide an optional description for the network address.

If NAT is used, configure an APPLICATION_SPACE network address.

Step 10  Expand Credentials.
   a. Add credentials for PLATFORM, ADMIN, HTTP, and SNMP_Vx credential types. Click + to add more credentials.
   b. Fill in the user ID and password that you configured when you installed the Unified CM.
   c. Select RO (Read-only) or RW (Read or Write) for the Access Type. The default is RO.
   d. Provide an optional description for the credential.

ADMIN, HTTP, PLATFORM, and SNMP are required for PCA to manage Unified CM. PLATFORM and ADMIN are also required for Service Inventory to generate reports for UC applications.

Expiration of the ADMIN account results in failed data syncs between Unified CM and Unified CDM.

Step 11  On the Field Mappings tab, complete field mappings as desired. Hard-coded mappings appear in grey and cannot be modified.
Step 12  Click Save. A Unified CM network device is created in Unified CDM. A cluster and Unified CM are created in the SDR.

Step 13  Test the connection between Unified CM and Unified CDM.
   a. Select Device Management > Advanced > CUCM Network Device.
   b. Click the Unified CM you just added.
   c. Select Action > Test Connection.

If the test fails, and you used a hostname, make sure Unified CDM has the correct DNS and Domain set.
   a. Log in to the platform CLI.
   b. Query the current DNS setting: network dns
   c. Set the DNS if needed: network dns <dns_server_ip_address>
   d. Query the current domain setting: network domain
   e. Set the domain if needed: network domain <domain>

Note Use the CUCM Network Device page only for testing the connection. Do not edit Unified CM from this page. To change any configuration of the Unified CM, edit it from the Device Management > CUCM > Servers page in Unified CDM.

Partitioned Unity Connection
To help the Cisco HCS solution scale more customers on the same hardware, you can partition a single Cisco Unity Connection instance to support multiple customer domains.

Cisco Unity Connection exposes the configuration and provisioning to support multiple customers by means of REST APIs. The Cisco HCS service fulfillment layer uses the partitioned Unity Connection REST APIs to allow Cisco HCS service providers to configure and provision customers into the partitioned Unity Connection.

Cisco HCS continues to support the dedicated Cisco Unity Connection in addition to the new partitioned instance. Partitioned Unity Connection is not a new product with a new SKU. The HCS administrator and domain managers must decide the role of Unity Connection as either regular or partitioned.

Single Sign On

SSO Certificate Management
Use this procedure to create a self-signed or third-party-signed system certificate to use when setting up Single Sign-On (SSO) on the web proxy node on Cisco Unified Communications Domain Manager 10.6(x).

Note This is customer specific during customer onboarding.

Procedure

Step 1  Login as hcsadmin.

Step 2  Select Single Sign On > Certificate Management.

Step 3  Click Add.
Step 4  On the Base tab, enter a Name and Description for the certificate.
  - For a self-signed certificate, leave Generate Certificate Signing Request unchecked.
  - For a third-party-signed certificate, check Generate Certificate Signing Request.

Step 5  For a self-signed certificate, control when the certificate is valid by changing the Valid From and Valid To fields. These are measured in seconds and default to 0 (now) and 315360000 (10 years), respectively.

Step 6  (Optional) Change the Key Length from the default of 1024.

Step 7  Click the Certificate Information tab.

Step 8  Complete the required fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name</td>
<td>Enter the FQDN for your server.</td>
</tr>
<tr>
<td>Country Code</td>
<td>A two-digit country code</td>
</tr>
<tr>
<td>State</td>
<td>An appropriate country subdivision</td>
</tr>
<tr>
<td>City</td>
<td>Your city</td>
</tr>
<tr>
<td>Organization</td>
<td>Your organization</td>
</tr>
<tr>
<td>Organization Unit</td>
<td>Your organization subunit</td>
</tr>
</tbody>
</table>

Step 9  Click Save.

Step 10  If you created a self-signed certificate you are done. If you requested a third-party-signed certificate, continue to the next step.

Step 11  Click the certificate you just created.

Step 12  Select Action > Export Certificate Request.

Step 13  Follow your organization's procedures to obtain the third-party signature for the certificate.

Step 14  Click the certificate.

Step 15  Select Action > Upload Signed Certificate.

Step 16  Browse to the signed certificate and click OK.

**Configure Single Sign-On for Cisco Unified Communications Domain Manager**

Follow these steps to configure self-service Single Sign-On (SSO) for Cisco Unified Communications Domain Manager (Unified CDM). The configuration applies to the customers and customer administrators associated with the IdP.
SSO support for administrative users is defined as follows:

- SSO is not supported for administrative users under User Management > Local Admins because their passwords are stored locally (and so are not available for SSO).
- SSO is supported for administrative users under User Management > Users, except for users with the Role set to Self-service.

Before You Begin

Create a self-signed or third-party-signed system certificate before you configure self-service SSO. For more information, see SSO Certificate Management.

The Unified CDM server and the IdP (identify provider) server must be configured so that their clocks are synchronized.

Procedure

Step 1 Log in to Unified CDM as hcsadmin.

Step 2 Select Single Sign On > SSO SP Settings.

Step 3 Click Add.

Note: Configure only one instance of SSO SP Settings.

Step 4 On the Base tab, select the System Certificate to use. To allow the SSO SP Setting to expire, enter a number of hours in the Validity field.

Note: Specifying an unsigned third-party-signed certificate will result in an error.

Step 5 On the SAML SP Settings Tab, enter the FQDN of the Unified CDM server. Check Sign Authn Requests and Want Assertions Signed as required by your security environment.

Step 6 Click Save.

Step 7 To view the location of the Unified CDM SP metadata that you will upload to the IdP, select Single Sign On > SSO SP Metadata. Point your browser to the URL shown here, and then save a copy of the SP metadata.

Step 8 Upload the SP metadata to the IdP. Refer to your IdP documentation for details on configuring SSO on your IdP.

Note: The IdP must release the UID and map it to an appropriate attribute. For example, an IdP that authenticates with Active Directory can map the uid SAML attribute to sAMAccountName in the Active Directory server.

Step 9 Download the IdP metadata from the IdP server.

Refer to your IdP documentation for details on downloading IdP metadata.
Step 10  Log in as Provider, Reseller, or Customer Admin, depending on your IdP configuration level.

Step 11  Select Administration Tools > File Management and upload the IdP metadata.

Step 12  Select Single Sign On > SSO Identity Provider.

Step 13  Click Add to add the SSO Identity Provider configuration.

Note Only one instance of an SSO Identity Provider can be configured for a hierarchy node.

Step 14  Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity Id</td>
<td>Entity ID of the IdP. This can be extracted from the IdP metadata file. This field is mandatory.</td>
</tr>
<tr>
<td>Login URI</td>
<td>Login URI for the IdP. This is the URI that will be imbedded in SSO Login URL. It can contain only alphanumeric characters and forward slashes. This field is mandatory.</td>
</tr>
<tr>
<td>Local Metadata File</td>
<td>Choose the IdP metadata file. This field is mandatory and must be unique across the system.</td>
</tr>
<tr>
<td>SSO Enabled</td>
<td>Check to enable SSO for users synched in or created at the current hierarchy level. Unchecking this node will disable SSO for the users associated with the defined IdP.</td>
</tr>
<tr>
<td>Note</td>
<td>Reminder to upload the IdP metadata file</td>
</tr>
<tr>
<td>SSO Login URL</td>
<td>Read-only field displays the SSO Login URL to use.</td>
</tr>
</tbody>
</table>

Step 15  Click Save to save the SSO Identity Provider Configuration and enable SSO if selected.

Step 16  Select Single Sign On > SSO User to display enabled SSO users.

Use this URL for your SSO login: https://<cucdm hostname>/sso/<login_URI>/login

**Configure Single Sign-On for Cisco Hosted Collaboration Mediation Fulfilment**

Configure self-service single sign-on (SSO) with SAML 2.0, for Cisco Hosted Collaboration Mediation Fulfilment. The configuration applies to service providers and service provider administrators associated with the identity provider for SSO.

Note Single logout is not implemented.

Before configuring SSO, ensure that you:
• Install and configure the required identity provider (IdP). For more information, see the IdP product documentation.
• Set up AD/LDAP configuration for user management.
• Add a Service Provider Administrator user in the active directory.
• Set up Circle of Trust (Co-T). For more information, see Set Up Circle of Trust (Co-T).

Procedure

Step 1  Log in to the CLI as an administrator on the Cisco HCM-F platform.

Step 2  Enter set sso enable command to enable SSO.

Step 3  Enter show sso status command to verify SSO status.

Step 4  Enter utils service restart Cisco Tomcat command to stop and restart Tomcat service.

Set up Circle of Trust (Co-T)

Circle of Trust consists of the various service providers that share and authenticate against one IdP. SAML single sign-on (SSO) establishes a Co-T by exchanging metadata and certificates as part of the provisioning process between the IdP and the service provider. The service provider verifies the Identity Provider (IdP) user information and provides access to various services or applications.

To enable SAML SSO, the administrator must establish a Co-T between the service provider and the IdP. The following steps provide a high-level overview of the procedure.

------------

Note For more information, see the IdP product documentation.

------------

Procedure

Step 1  Log in to the IdP using administrator credentials.

Step 2  Enter the show sso sp-metadata command on the HCM-F App node to generate SSO Service Provider metadata.

Step 3  Transfer the metadata from the HCM-F App node directly to the IdP or to an intermediate server and then to the IdP, using SFTP.

Step 4  Modify the relying party.xml on the IdP to add the HCM-F App node service provider metadata to the IdP.

Step 5  Restart Tomcat on IdP.

Step 6  Enter the set sso idp-url https://<IDP-FQDN>/<IdP path> command to download IdP metadata on the HCM-F App node.
**Note:** IDP-FQDN is the fully qualified domain name of the IdP host.

Examples for commands:

- set sso idp-url https://<IDP-FQDN>/idp/shibboleth
- set sso idp-url https://<IDP-FQDN>/FederationMetadata/2007-06/FederationMetadata.xml
- set sso idp-url http://<IdP-FQDN>:8080/openam/saml2/jsp/exportmetadata.jsp

### Configuring the Expressway-C for Unified Communications

#### Configuring DNS and NTP settings

Check and configure the basic system settings on Expressway:

**Procedure**

1. Ensure that System host name and Domain name are specified (System > DNS).
2. Ensure that local DNS servers are specified (System > DNS).
3. Ensure that all Expressway systems are synchronized to a reliable NTP service (System > Time). Use an Authentication method in accordance with your local policy.

### Enabling Mobile and Remote Access

To enable mobile and remote access functionality:

**Procedure**

1. Go to Configuration > Unified Communications > Configuration.
2. Set Mobile and remote access to On.
3. Click Save.

### Configuring the Domains to Route to Unified CM

You must configure the domains for which registration, call control, provisioning, messaging and presence services are to be routed to Unified CM.

**Procedure**

1. On Expressway-C, go to Configuration > Domains.
2. Select the domains (or create a new domain, if not already configured) for which services are to be routed to Unified CM.
3. For each domain, turn On the services for that domain that Expressway is to support.
Figure 1: Domains

Configure SIP

Procedure

Step 1  Navigate to Configuration > Protocol > SIP.

Step 2  Configure the SIP settings as follows –

Figure 2: SIP configuration

Configuring Unified CM Servers

To configure the Unified CM servers used for remote access:

Procedure

Step 1  On Expressway-C, go to Configuration > Unified Communications > Unified CM servers. The resulting page displays any existing servers that have been configured.
Step 2  Add the details of a Unified CM publisher:
   a. Click New.
   b. Enter the Unified CM publisher address and the Username and Password credentials of an application user account that can access the server. The address can be specified as an FQDN or as an IP address. The Unified CM user must have the Standard AXL API Access role.
   c. TLS Verify Mode is set to OFF.
   d. The system then attempts to contact the publisher and retrieve details of its associated nodes.
   e. Repeat for every Unified CM, IM and Presence, and Unity Connection nodes.

Configure a Unified Communications Traversal Zone to Expressway-E

Procedure

Step 1  On the Zones page create a Unified Communications Traversal Zone to VSCE.
   a. Configure the SIP settings and authentication as per the screenshot below.
   b. Ensure the Peer 1 address reflects the FQDN of Expressway-E and it resolves to the externally reachable IP.
   c. Once added, ensure the Status of the Zone is Active.

Step 2  Navigate to Configuration > Dial Plan > Search rules and click New.
Create Search rules to route traffic from Expressway-E to Unified CM and from Unified CM to Expressway-E.

For more information on creating Secure Traversal Zones, please refer to the Expressway 8.9 Administration Guide at:

Cisco Expressway Administration Guide (X8.9) (PDF)
Configure the Expressway-E for MRA

Ensure that Expressway-E is publicly accessible and can be reached via a browser by using the domain address [example: vcse.collabedge-XXX.dc-YY.com]

Configuring DNS, NTP, and IP Settings

Check and configure the basic system settings on Expressway:

Procedure

Step 1  Ensure that System host name and Domain name are specified (System > DNS).

Step 2  Ensure that public DNS servers are specified (System > DNS).

Step 3  Ensure that all Expressway systems are synchronized to a reliable NTP service (System > Time). Use an Authentication method in accordance with your local policy.

Step 4  Ensure the LAN settings (System > Network interfaces > IP) are in IPv4 mode, dual network interfaces are configured properly if needed, the IPv4 address/gateway/subnet mask are correct, IPv4 static NAT mode is on for the external LAN, and the IPv4 static NAT address is the correct public IP.

Enabling Mobile and Remote Access

To enable mobile and remote access functionality:

Procedure

Step 1  Go to Configuration > Unified Communications > Configuration.
Step 2  Set Mobile and remote access to On.

Step 3  Click Save.

**Configure SIP**

**Procedure**

Step 1  Navigate to Configuration > Protocol > SIP.

Step 2  Configure the SIP settings as follows:

**Figure 4: Configure SIP settings**

![SIP Configuration](image)

**Create the DNS Zone**

Next, you will need to create a new DNS Zone that allows your Expressway-E to identify and route OTT calls.
Procedure

Step 1  On the Expressway-E, navigate back to Configuration > Zones > Zones and click New.

Step 2  Configure zone of type DNS, TLS Verify Mode set to OFF.

Step 3  Click Create Zone.

Configure a Unified Communications Traversal Zone to Expressway-C

Procedure

Step 1  On the Zones page create a Unified Communications Traversal Zone to Expressway-C.

Step 2  Configure the SIP settings and authentication as per the screenshot below.

Step 3  The connection credentials on the expressway pair should match.

Step 4  Ensure the TLS verify subject name address reflects the FQDN of Expressway-C and it is reachable.

Step 5  Once added, ensure the Status of the Zone is Active.

Step 6  Navigate to Configuration > Dial Plan > Search rules and click New.

Step 7  Create Search rules to route traffic from Expressway-E to Unified CM and from Unified CM to Expressway-E.

For more information on creating Secure Traversal Zones, please refer to the Expressway 8.9 Admin Guide at Cisco Expressway Administration Guide (X8.9) (PDF)
Configure Unified CM for Call Routing

This section details how to configure Cisco Unified Communications Manager to receive calls directly from Expressway-E through Expressway-C and assist with Mobile Remote Access (MRA).

Procedure

Step 1 Login to the Shared Architecture Unified CM.

Step 2 Navigate to System > Enterprise Parameters.

Step 3 Search (CTRL+F) for fully which will bring you to the setting Cluster Fully Qualified Domain Name.

Step 4 Enter the public domain name created for MRA followed by the FQDN of the Shared architecture CUCM.

[Example: collabedge-161.dc-01.com cucm-shared.dcloud.cisco.com]

Step 5 Click Save.

Step 6 Create a SIP Profile by going to Device > Device Settings > SIP Profile.

Step 7 Toward the bottom of the page, for the Early Offer support for voice and video calls setting in the Trunk Specific Configuration section choose the option Best Effort (no MTP inserted).
Step 8  Create a Non Secure SIP Trunk Profile by going to Device > Trunk.

Step 9  Add New SIP trunk. Set the following parameters –

- Calling and Connected Party Info Format (Outbound Calls section) to Deliver URI and DN in connected party, if available.
- Destination Address (SIP Information section) to IP Address of Expressway-C used for B2B/MRA.

Step 10  Choose the newly created SIP Trunk Security Profile and SIP Profile.

Step 11  Add New SIP route pattern that matches the cloud URI IPv4 pattern to be sent out through the new SIP trunk to the Expressway-C.
Cisco Unified CDM Setup – Customer Configuration

Setting up the Hierarchy

Sign in to the server as the provider or reseller administrator, depending on which organization manages the customer.

Procedure

Step 1  Create a Customer.
   a.  Go to Customer Management and Customers.
   b.  Click Add.
   c.  Fill in the Customer Name and Admin Password plus any other optional details.
   d.  Click Shared UC Applications.
   e.  Click Save.

Step 2  Create an Intermediate Node.
   a.  Go to Hierarchy Management and Hierarchy.
   b.  Select the new customer in the top dropdown menu.
   c.  Click Add.
   d.  Fill in the Name and optional Description.
   e.  Click Save.

Step 3  Review the Hierarchy.

Step 4  Manage Local Administrators (Optional).

Configure Entitlement

Entitlement represents the set of services and devices (and their number) available for particular subscribers.

Example:
1.  Customer A specifies a user has voice service, an IP device, an analog set, and nothing else.
2.  Customer B specifies users have both voice and voicemail services on ten devices, and nothing else.

Procedure

Step 1  (Optional) Define additional device types.

Step 2  Create device groups to define sets of device types that users may be entitled to.

Step 3  Create entitlement catalogs to define limits on devices and services that entitlement profiles may entitle users to.

Step 4  Create entitlement profiles to define the devices and services users are entitled to.

Step 5  Identify the entitlement profile for users synced from Cisco Unified Communications Manager.

Step 6  Identify the entitlement profile for users synced from LDAP.
Step 7  Assign entitlement profiles to existing users in Cisco Unified Communications Domain Manager 10.6(x).

**Configure a Network Device List**

**Procedure**

Step 1  Sign in to Unified CDM as a provider administrator or reseller administrator.

Step 2  Click Customer Management > Network Device Lists. Select a customer on the hierarchy tree where the NDL is to be created.

Step 3  Click Add.

Step 4  Enter a name for the NDL and optionally a description.

Step 5  Click the + next to Cisco Unified CM.

Step 6  Select the Cisco Unified Communications Manager instance from the dropdown menu.

Step 7  Click the + next to the Cisco Unity Connection.

Step 8  Select the Cisco Unity Connection instance from the dropdown menu.

Step 9  (Optional) Add Cisco Unity Connection and Cisco WebEx instances to the NDL.

Step 10  Click Save.

**CUCM Group Configuration**

**Procedure**

Step 1  Log in as the Provider, Reseller, or Customer Administrator.

Step 2  If you are adding a new instance, ensure the hierarchy path is set to the target node for the new instance.

Step 3  Log in as the Provider or Reseller Administrator, select Device Management > CUCM > Unified CM Groups.

Step 4  Perform any one of the following:

- To add a new Cisco Unified Communications Manager group, click Add, then go to step 5.
- To edit an existing Cisco Unified Communications Manager group, click on the line item in the list of existing instances. Go to step 5.

Step 5  Modify the following fields as required.
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name (Mandatory)</td>
<td>Enter the name of the new group.</td>
</tr>
<tr>
<td>Auto-registration Cisco Unified Communications Manager Group</td>
<td>Check the Auto-registration Cisco Unified Communications Manager Group check box if you want this Cisco Unified Communications Manager group to be the default Cisco Unified Communications Manager when auto-registration is enabled. Leave this check box unchecked if you do not want devices to auto-register with this Cisco Unified Communications Manager group. Each Cisco Unified Communications Manager cluster can have only one default auto-registration group. If you choose a different Cisco Unified Communications Manager group as the default auto-registration group, that is, you check the Auto-registration Cisco Unified Communications Manager Group check box for a different Cisco Unified Communications Manager group, the previously chosen auto-registration group no longer serves as the default for the cluster; the Auto-registration Cisco Unified Communications Manager Group check box displays for the previously chosen group (the original default), and the check box gets disabled for the group that now serves as the default.</td>
</tr>
<tr>
<td>Unified CM Group Items (Mandatory)</td>
<td>Click the Add (+) button to select a Cisco Unified Communications Manager to add to the group. Repeat as necessary to add multiple Cisco Unified Communications Managers to the group. Click the Remove (-) button to remove a Cisco Unified Communications Manager from the group. Click the up and down arrow buttons to change the order of the Cisco Unified Communications Managers in the group.</td>
</tr>
<tr>
<td>Priority (Mandatory)</td>
<td>Enter the priority number for this Cisco Unified Communications Manager in the group. The smaller the integer, the higher the priority.</td>
</tr>
<tr>
<td>Selected Cisco Unified Communications Managers</td>
<td>This field displays the Cisco Unified Communications Managers that are in the Cisco Unified Communications Manager group.</td>
</tr>
</tbody>
</table>

**Step 6**  Click Save.

The group appears in the Call Manager Groups list. When you click on the name of the Cisco Unified Communications Manager group in the list, the group's characteristics are displayed.

- To modify any of these characteristics, make your changes and click Save.
- To delete a group, check the box to the left of the Name column in the group list, and click Delete.

### Create a Customer Dial Plan

**Type 4 dial plan will be configured**

**Procedure:**

**Step 1**  Log in as the Customer Administrator or the Provider Administrator.

**Step 2**  Select Dial Plan Management > Customer > Dial Plan.
Step 3  Click Add to add a Customer Dial Plan.

Step 4  A Site Location Code is NOT required for this customer, do not click the Site-Location Code (SLC) based dial plan box

Step 5  Check Enable CSS filtering to filter the calling search spaces available when configuring a Subscriber, Phone, or Line, to site level Class of Service calling search spaces. Filtering is disabled by default, which results in all available Cisco Unified Communications Manager calling search spaces being available when configuring a Subscriber, Phone, or Line.

Step 6  Click Save to add the Customer Dial Plan you defined.

Note

The Customer ID is a unique, auto-generated, read-only number allocated to the customer. The Customer ID is particularly useful in shared deployments (where a cluster may be shared across multiple customers) to correlate specific elements to a customer. It appears in the Cisco Unified Communications Manager as a prefix to elements (for example Cu2Si7 identifies Customer 2, Site 7).

Add a Country Dial Plan to a Dial Plan Before Deploying to a Customer

These instructions are only needed if a custom dial plan is required.

Procedure

Step 1  Login as hcsadmin or provider admin.

Step 2  Select Dial Plan Management > Advanced Configuration > Dial Plan Schema Group.

Step 3  Choose an existing dial plan schema group to clone, or create a new dial plan schema group. If you choose an existing dial plan schema group, select Action > Clone. Update the Dial Plan Schema group Name on the General tab. For example, clone Cisco Type 4 Schema Group and give it the name "Cisco Type 4 Schema Group with France."

Step 4  Click the Country Schemas tab.

Step 5  Add the two schemas associated with the country dial plan to the dial plan schema group.

- HcsGenericCustomer<Country>DP-V<version>-SCH: The schema template used to deploy the customer-level country dial plan elements for the target country.
- HcsGenericSite<Country>DP-V<version>-SCH: The schema template used to deploy the site-level country dial plan elements for the target country.

Provide the following mandatory information for the two schemas:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dial Plan Schema Usage</td>
<td>Select Add Site for both schemas.</td>
</tr>
<tr>
<td>Country Name</td>
<td>Select the target country.</td>
</tr>
<tr>
<td>Dial Plan Schema Scope</td>
<td>Select Customer for the customer schema. Select Site for the site schema.</td>
</tr>
</tbody>
</table>
Dial Plan Schema Name

Select HcsGenericSite<Country>DP-V<version>-SCH for the site schema.

Note: Add additional country dial plan schemas as needed by the customer.

Step 6  Click Save.

Step 7  Deploy the customized schema group to the customer.
   b. Set the hierarchy path to the customer hierarchy node.
   c. Click Add.
   d. From the Dial Plan Schema Group pull down, select the customized dial plan schema group with your added country or countries.
   e. Click Save.

Add a Site

Procedure

Step 1  Log in to server as a Provider, Reseller, or Customer administrator.

Step 2  Make sure that the hierarchy is set to the customer for whom you are creating the site.

Step 3  Click Site Management > Sites.

Step 4  Click Add.

Step 5  Complete the following fields:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Name</td>
<td>The name of the site. This field is mandatory. Any spaces in the site name are converted to underscores in the site local administrator name and email, if Create Local Admin is checked. A customer location that has been configured in HCM-F and synced into Cisco Unified Communications Domain Manager may exist at the sys.hcs hierarchy. If the Site Name you enter matches this customer location, the Migrate from HCM-F to Unified CDM check box is displayed. Click Save to migrate this customer location to a site at the current hierarchy level. The fields are</td>
</tr>
</tbody>
</table>
populated with the values that were configured in HCM-F. If you do not want to migrate the customer location, enter a different Site Name.

You cannot migrate a customer location to a site if the customer for the site is different than the customer associated with the customer location.

When migrating a customer location to a site, an NDL is not selected for the site. You can set the NDL for the site later.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A description for the site.</td>
</tr>
<tr>
<td>Extended Name</td>
<td>External clients can use the Extended Name of the site if needed. This field is not used by other components within Cisco HCS.</td>
</tr>
<tr>
<td></td>
<td>This field exists in the Customer Location record in SDR. When the customer is managed by Cisco Unified Communications Domain Manager 8.1(x), the Extended Name is synced from Cisco Unified Communications Domain Manager 8.1(x) to the Customer Location record in SDR. When the customer is managed by Cisco Unified Communications Manager 10.x, the Extended Name is synced from Cisco Unified Communications Manager 10.x to the Customer Location record in SDR.</td>
</tr>
<tr>
<td>External ID</td>
<td>External clients can use the External ID of the site if needed. This field is not used by other components within Cisco HCS.</td>
</tr>
<tr>
<td>Create Local Admin</td>
<td>Controls whether a default local administrator is created for the site.</td>
</tr>
<tr>
<td>Cloned Admin Role</td>
<td>The customer role used to create a new role prefixed with the site name. The created site role, shown in Default Admin Role field, is assigned to the default local administrator user. This field appears only if Create Local Admin is checked.</td>
</tr>
<tr>
<td>Default Admin Role</td>
<td>The created site role that is assigned to the default local administrator. This field is read only and appears only if Create Local Admin is checked.</td>
</tr>
<tr>
<td>Default Admin Password</td>
<td>The password to assign to the default local administrator. This field appears only if Create Local Admin is checked.</td>
</tr>
<tr>
<td>Repeat Default Admin Password</td>
<td>Confirm the default local administrator password. This field appears only if Create Local Admin is checked.</td>
</tr>
<tr>
<td>Country</td>
<td>The country is used to determine which dial plan to download to the site when the dial plan is configured on the site. This field is mandatory.</td>
</tr>
<tr>
<td>Network Device List</td>
<td>Choose the NDL containing the UC applications and WebEx to be used by the site. Once an NDL has been set for the site, it</td>
</tr>
</tbody>
</table>
 cannot be removed from the site, nor can the NDL be changed to another NDL.

<table>
<thead>
<tr>
<th>Auto Push Users to CUCM</th>
<th>If enabled, users are automatically pushed to the Cisco Unified Communications Manager that is associated with the NDL. The default is disabled. You can edit the site later, and enable this check box for one of the following reasons:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• To automatically push users at the site to the Cisco Unified Communications Manager</td>
</tr>
<tr>
<td></td>
<td>• To perform an Auto User Push when an NDL is added to the site</td>
</tr>
<tr>
<td></td>
<td>• To perform an Auto User Push when a Cisco Unified Communications Manager is associated with an NDL</td>
</tr>
</tbody>
</table>

**Step 6** Click Save.

Once saved, the following occurs:

- A Site hierarchy node is created.
- A Location is created.
- A Customer Location in the SDR is created.
- Optionally, a default site administrator is created.
- If the Auto Push Users to CUCM box is checked, all users associated with the NDL are pushed to the Cisco Unified Communications Manager associated with the NDL.

### Add First Site Dial Plan

**Procedure**

**Step 1** Log in as the Customer Administrator or Provider Administrator.

**Step 2** Set the hierarchy path to the site for which you want to create a site dial plan. If the hierarchy path is not set to a site, you are prompted to select a site.

**Step 3** Select Dial Plan Management > Site > Dial Plan.

**Step 4** Click Add to add a Site Dial Plan.

**Step 5** Modify the External Breakout Number, if desired. The External Breakout Number is the PSTN prefix that is used when deploying a country dial plan. For Cisco HCS Type 1 to 4 dial plan schemas, you deploy country dial plans at the customer level. The country dial plan is not pushed to Unified CM until the first site associated with a given country is deployed. For example, if a site is associated with the United States, and it is the first site dial plan being created for the USA, the US country dial plan is deployed as part of creating the site’s dial plan. Default is 9. The External Breakout Number is one digit in length.

**Note** We support only one External Breakout Number for each country. For example, all sites within USA have the same External break out as the first site within USA.

**Step 6** Enter the Extension Length. Values can be 1 to 30. Default is 4; for example, 2000.
When adding DNs for a site, extension length is not currently enforced. Therefore, the administrator must be conscious of extension length when adding DNs for a particular site; otherwise DNs may not be dialable.

**Note**

Step 7 Perform one of the following for sites without Inter-Site Prefixes (ISPs):

**Note**

This field appears if your Customer Dial Plan does not use ISPs; for example, HCS Type 3 dial plans (SLC, no ISP, DN=SLC+EXT)

- Check Use extension prefix? If your customer dial plan has an extension prefix defined and you want this site to use the extension prefix.
- If an Extension prefix is not defined in the customer dial plan for this site, go to the next step.

Step 8 Enter the Area Code. Enter zero or more valid local area codes for the site. Specify the length of the subscriber part of the PSTN number for each area code. The Area Code is used to generate the PSTN local route patterns for the site. For example, in the USA, if area codes are added for Dallas, Texas, the area codes could be specified for local dialing as 214, 469, and 972 with a subscriber length of 7.

Step 9 Enter the Local Number Length. Local Number Length is the length for the subscriber section of the entire E.164 number.

Step 10 Check Area Code used for Local Dialing if the area code is needed for local dialing from this site. In the US this setting determines whether you use 7-digit or 10-digit local dialing.

Step 11 Select the Published number from the drop-down of available E.164 inventory numbers, or enter a custom number. The site published number is the default E.164 mask when a line is associated to a phone at a particular site.

Step 12 Select the Emergency Call Back Number for the site from the drop-down of available E.164 inventory numbers, or enter a custom number. The site emergency call-back number is the calling number when initiating an outgoing emergency call. It can be used when you use Extension Mobility and make an emergency call from a site other than your own. It can be used when the emergency call goes out to the PSTN network, when the system includes the site emergency number so that the origin of the call is known. The system adds this calling party transformation to the DN2DDI4Emer-PT partition.

**Note**

The Emergency Number is not the number to dial for an emergency. Instead, it is the number used to identify the calling party for emergency calls originating from a particular site.

**Note**

Under the Emergency Number field, there is the Site ID read-only field. The Site ID is a unique, auto generated, read-only number for each customer site which is prefixed to elements as an identifier (for example, Cu4Si2 indicates Customer 4, Site 2).

Step 13 Click Save to add the Site Dial Plan you defined. The site information is loaded on the Unified CM, and is identifiable by its Customer ID, Site ID prefix.
Cisco Unified CDM Number Management

Add E.164 Inventory

Use this procedure to define an inventory of E.164 numbers available to users.

Important: Each addition to the E.164 Inventory must contain a unique set of numbers. That is, you cannot assign the same number more than once (globally).

Procedure

Step 1  Log in as a provider, reseller, or customer administrator.

Step 2  Set the hierarchy path to point to the customer for whom you are adding the E.164 inventory.

Step 3  Select Dial Plan Management > Number Management > Add E164 Inventory.

Step 4  Provide the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site</td>
<td>For a site-specific E.164 inventory, select the customer site. For a customer-wide E.164 inventory, leave this field unset.</td>
</tr>
<tr>
<td>Country</td>
<td>Select the country associated with the E.164 inventory. If a site was specified, this field is automatically populated with the country associated with the site. This field is mandatory.</td>
</tr>
<tr>
<td>Country Code</td>
<td>The country code for the selected country. Refer to this read-only field when specifying the Starting Number and Ending Number fields which must contain a valid country code.</td>
</tr>
<tr>
<td>Starting Number</td>
<td>Enter the starting number of the range of E.164 numbers. The field is populated with + followed by the country code for the selected country. Append the rest of the starting number after the country code. This field is mandatory.</td>
</tr>
<tr>
<td>Ending Number</td>
<td>Enter the ending number of the range of E.164 numbers. The format is the same as the Starting Number. This field is optional. If not provided, the single E.164 Number specified in the Starting Number is added. If provided, the range of E.164 Numbers is added: Starting Number – Ending Number, inclusive. A maximum of 1000 numbers can be added at a time.</td>
</tr>
</tbody>
</table>

Step 5  Click Save.

Add Directory Number Inventory

Use this procedure to add a single directory number (DN) or range of DNs for your customer. The DNs (extensions) you specify are validated against the Dial Plan type (Type 1 to 4). The extension length assigned to the site is enforced for site location code (SLC)-based dial plans. The maximum number of directory numbers you can add at a time is 1,000.

If you are a customer with multiple sites using a Type 4 dial plan, ensure that the directory numbers you specify are unique across sites.
This procedure only creates the DN inventory in Cisco Unified Communications Domain Manager 10.6(x). The numbers are not passed on to Cisco Unified Communications Manager.

Directory numbers can only be added or deleted. You cannot edit the directory numbers once they are added. The usage and availability property for each DN is associated with a line or taken into use by a service.

Step 1 Log in as the Provider, Reseller, or Customer Administrator.

Step 2 Select an available Customer from the hierarchy node breadcrumb at the top of the interface.

Step 3 Select Dial Plan Management > Number Management > Add Directory Number Inventory.

Step 4 From the Site dropdown menu, select the site for which you are adding directory numbers. Leave this field empty to add customer level directory numbers.

Customer level directory numbers can only be created for dial plans that do not use site location codes (flat dial plans). Attempting to create customer level directory numbers for site location code-based dial plans result in an error instructing you to specify a site when adding new DN inventory.

Note For a Type 4 dial plan (no SLCs), the Starting and Ending Extension fields must contain no more than 16 digits each, including the + sign before the DN number, if used. For Types 1 to 3 dial plans, the Starting and Ending Extension fields must be less than or equal to the site Extension Length. If the Starting or Ending Extension field length is less than the site Extension Length, the DN number is padded with zeroes until its length equals that of the site Extension Length.

For a Type 4 dial plan (no SLCs), the Starting and Ending Extension fields may contain a * prefix (asterisk) before the 15-digit directory number. The * prefix denotes DNs that are used with hunt groups, assistant lines, Contact Center lines, and so on. This type of directory number cannot be reached from an outside line and cannot be associated with E.164 numbers. Typically, a DN with the * prefix is not called from another line (user), but is tied to a service feature such as call pickup, hunt groups, or contact center.

Example: If the Extension Length field shows four digits for a Type 3 Dial Plan, ensure that you enter a number containing four digits or less in the Starting Extension field. For example, DN 1234. If you enter DN 123, the extension number is created as DN 0123.

Step 5 Using the Extension Length, Site Location Code, and ISP read-only fields as a guide for the site, enter the first number for the DN range in the Starting Extension field.

Step 6 (Optional). Using the Extension Length, Site Location Code, and ISP read-only fields as a guide for the site, enter the last number for the DN range in the Ending Extension field. If you are adding a single DN, the ending number is the same as the starting number.

The maximum number of directory numbers you can add is 1,000 at a time. If you need more than 1,000 directory numbers, repeat this procedure as required to add ranges.

Step 7 Click Save to save the single DN or DN range.
Configure Directory Number Routing

Use this procedure to define Directory Number Routing. Directory Number Routing is a translation pattern that is put into the PreISR and ISR partitions to route intrasite and intersite calls to extensions (directory numbers). This is similar to the way site location codes (SLCs) are used as short codes for Type 1, 2, and 3 customer dial plans.

Typically, Directory Number Routing is used for Type 4 (flat dial plans) so that from a customer and site perspective, you can see which patterns are directory numbers because there are no SLCs available.

Procedure

Step 1  Log in as the Provider, Reseller, Customer, or Site Administrator.

When adding Directory Number Routing, ensure that you select a valid site under your customer in the hierarchy node breadcrumb at the top of the view. If you attempt to add Directory Number Routing at any other node in the hierarchy, you will receive an error indicating that you must be at a site.

Step 2  Select Dial Plan Management > Site > Directory Number Routing.

Step 3  Click Add to add Directory Number Routing.

Step 4  Enter a prefix in the Directory Number Routing Prefix field using up to 30 characters.

Example: Enter 234

Step 5  Enter a DN mask length in the Directory Number Mask Length field.

Example: Enter 4. For this example, the Directory Number Routing would be 234XXXX, where XXXX is the mask.

Step 6  Click Save to add the Directory Number Routing that you defined. The new Directory Number Routing appears in the table and it can be edited or deleted as required.

Associate a Range of E.164 Numbers to a Range of Directory Numbers

Use this procedure to associate a range of E.164 numbers with a range of directory numbers (DN) at a customer or site. These associations create Direct Dial Inward (DDI) associations so that incoming PSTN numbers are routed to directory numbers.

If you create the association at a site, you can mix customer-level DNs and E.164 numbers with site-level DNs and E.164 numbers.

Procedure

Step 1  Sign in as provider, reseller, customer, or site administrator.

Step 2  Set the hierarchy path to point to the customer or site where you want to associate E.164 numbers with directory numbers.

Step 3  Select Dial Plan Management > Number Management > E164 Associations (N to N DN).

Step 4  Click Add.

Step 5  Provide the following information:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range</td>
<td>Select one of the following ranges:</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The range values you select map to the mask value when the association translation pattern is created. For example, when 10 is selected, all E.164 numbers and directory numbers that end in 0 are listed. The mask affects all digits 0 to 9, so you can't start the mask on a nonzero number. Likewise, when 100 is selected, the E.164 number and DN end in two zeros. This pattern results in a mask of XX.</td>
</tr>
<tr>
<td></td>
<td>• 1—To list all E.164 numbers and DNs</td>
</tr>
<tr>
<td></td>
<td>• 10—To list all E.164 numbers and DNs that end in one zero (0)</td>
</tr>
<tr>
<td></td>
<td>• 100—To list all E.164 numbers and DNs that end in two zeros (00)</td>
</tr>
<tr>
<td></td>
<td>• 1000—To list all E.164 numbers and DNs that end in three zeros (000)</td>
</tr>
<tr>
<td>E164 Number</td>
<td>Select the starting number of the range of E.164 numbers from the drop-down menu. For a customer-level association, only customer-level E.164 numbers are available. For a site-level configuration, both customer-level and site-level E.164 numbers are available. This field is mandatory.</td>
</tr>
<tr>
<td>DN Number</td>
<td>Select the starting extension number from the drop-down menu. This field is mandatory.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You cannot associate extension numbers that begin with the prefix * (asterisk).</td>
</tr>
</tbody>
</table>

Step 6 Click Save.

**Add Central Breakout SIP Trunk**

From the current onboarding guide,

For Shared Architecture, the customer references in these steps mean the single (representative) customer that represents all of the customers in the Shared Architecture cluster.

Need to look at a design where each customer is separated.

**Cisco UCDM SIP Trunk Settings**

**Procedure**

Step 1 Log in as the Provider, Reseller, or Customer Administrator.

Step 2 Make sure the hierarchy path is set to the node where the Cisco Unified Communications Manager is configured.

Step 3 Perform any one of the following:

• If you logged in as the Provider or Reseller Administrator, select Device Management > CUCM > SIP Trunks.
• If you logged in as the Customer Administrator, select Device Management > Advanced > SIP Trunks.

Step 4 Perform any one of the following:

• To add a new SIP trunk, click Add, then go to Step 4.
• To edit an existing SIP trunk, choose the SIP trunk to be updated by clicking on its box in the leftmost column, then click Modify to edit the selected SIP trunk. Go to Step 5.

Step 5 From the CUCM pulldown menu, select the hostname, domain name, or IP address of the Unified CM to which you want to add the SIP trunk.

Note The CUCM pulldown menu only appears when a SIP trunk is added; it does not appear when you edit a SIP trunk.

Important: The CUCM pulldown menu shows, in addition to the Unified CM located at the node, ALL the Unified CM nodes in the hierarchies above the node you are adding the SIP trunk. To provision a Unified CM server, refer to the “Installation Tasks” section of Installing Cisco Unified Communications Manager.

Step 6 Enter a unique name for the new SIP trunk in the Device Name field, or modify the existing Device Name if desired.

Step 7 Complete the fields on each tab as appropriate. The following fields on each tab are required:

• Device Information tab
  o Device Name
  o Trunk Service Type
  o Call Classification
  o Location
  o Use Trusted Relay Point

• Call Routing General tab
  o SIP Privacy

• Call Routing Inbound tab
  o Significant Digits
  o Connected Line ID Presentation
  o Connected Name Presentation

• Call Routing Outbound tab
  o Calling Party Selection
  o Calling Line ID Selection
  o Calling Name Presentation
  o Calling and Connected Party Info Format

• SP Info tab
  o Destination - Destination IPv4
- Destination - Destination IPv6 (if Destination - Destination IPv4 field is not completed)
- Destination - Destination Port
- Sort Order
- MTP Preferred Originating Codec
- BLF Presence Group
- SIP Trunk Security Profile
- SIP Profile
- DTMF Signalling Method

GeoLocation tab: no mandatory fields

For details on each tab's fields, see SIP Trunks Field Descriptions.

Step 8  To save a new SIP trunk, click Save. To save an updated SIP trunk, click Update.

The SIP trunk appears in the SIP trunk list. You can view the SIP trunk and its characteristics by logging in to the Unified CM where the SIP trunk was added, selecting Device > Trunk, and performing the Find operation. When you click on the name of the SIP trunk in the list, the trunk characteristics are displayed.

The SIP trunk is automatically reset on the Unified CM as soon as it is added. To reset the SIP trunk at any other time, perform Reset SIP Trunks. For more details on configuring SIP trunk, refer Installing and Configuring Cisco HCS for Contact Center 10.6(1) guide.

SBC

With the Open Architecture partners are free to choose alternative options to Cisco SBC offering. This option has been open to Partners since HCS 10.0.1.

Depending on your planned deployment, you could configure using either:

Cisco Unified Border Element (SP Edition)

Or

Perimeta SBC.

For details please refer to the Data Center Provisioning and Aggregation chapter in the Cisco Hosted Collaboration Solution, Release 10.6(1) Customer Onboarding Guide.

Create Customer and Users in AD

The following steps show one way to add a customer and users into a Microsoft AD if not already done. User management can also be done with Imagicle which provides LDAP services to integrate with CUCDM and CUCM. The Imagicle team can help install and configure the Imagicle app for user management services in HCS-SA if an alternative to Microsoft's AD is desired.

Procedure

Step 1  Open the AD.

Step 2  Create a new OU under the main domain.

Step 3  Create a new user in the new OU.

  a. Fill in the First name, Last name, and User logon name fields then click Next.
  b. Fill in the Password and any other optional check boxes then click Next.
c. Click Finish.

Step 4 After creating the user then double click the user to open the properties.
   a. In the General tab fill in the Telephone number and E-mail.
   b. In the Telephones tab fill in the IP phone number.

Step 5 Fill in any other optional data as needed.

LDAP Integration in Cisco Unified CDM

Set up an LDAP Server

Use this procedure to set up an LDAP server for integration with Cisco Unified CDM.

Procedure

Step 1 Log in as a provider, reseller, or customer administrator.

Step 2 Set the hierarchy node to the desired node where you want the users synchronized (recommend the intermediate node).

Step 3 Navigate to LDAP Management > LDAP Server.

Step 4 Click Add.

Step 5 Complete the fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Defaults to the current hierarchy level.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Hostname or IP address of the LDAP server. This field is required.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number for LDAP traffic. Defaults to 389.</td>
</tr>
</tbody>
</table>
| User DN     | The User Distinguished Name of an administrative user who has access rights to the Base DN on the LDAP server. This field is required. Examples:  
  - Administrator@stb.com  
  - OU=LDAP0,DC=stb,DC=com  
  - uid=admin,ou=system |
| Admin Password | Admin password associated with the user. This field is required. |
| Search Base DN | Base Distinguished Name for LDAP search. This should be a container or directory on the LDAP server where the LDAP users exist, such as an Organization Unit or OU.  
As an example, to search within an Organizational Unit called CUS01 under a domain called GCLAB.COM, the Search Base DN would be OU=CUS01,DC=GCLAB,DC=COM.  
For Shared Architecture the OU will be unique for each customer.  
The domain will be the same for all customers. |
Set up LDAP for User Synchronization

Follow these steps to set up an LDAP for user synchronization. This process synchronizes users from the configured LDAP directory into Cisco Unified CDM. The users then appear at the hierarchy node at which the LDAP User Sync object exists. You can manage the users through User Management menu options (for example, move users to other hierarchies, or push to Cisco Unified Communications Manager).

Procedure

Step 1  Log in as a provider, reseller, or customer administrator.

Step 2  Set the hierarchy path to the node of the LDAP server you want to synchronize users from.

Step 3  Select LDAP Management > LDAP User Sync.

Step 4  Click Add.

Step 5  On the Base tab, provide the following information:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Server</td>
<td>This read-only field displays the LDAP Server you are synchronizing users from.</td>
</tr>
<tr>
<td>LDAP Authentication Only</td>
<td><strong>Important</strong> Leave unchecked to synchronize users from LDAP. Default is unchecked. When unchecked, users are synchronized from the configured LDAP directory and their passwords are authenticated against the configured LDAP directory. When checked, users are not synchronized from the configured LDAP directory, but their passwords are authenticated against the LDAP directory. When checked, you can manually add users from the GUI or API, bulk load them, or synchronize them from Cisco Unified CM.</td>
</tr>
<tr>
<td>User Model Type</td>
<td>The User Model Type identifies which LDAP object, defined in the configured LDAP server, is used to import and authenticate users. If the LDAP server is Active Directory, the default is device/ldap/user. If the LDAP server is OpenLDAP, the default is device/ldap/inetOrgPerson. To identify a non-default User Model Type to use, contact the LDAP administrator for the LDAP server from which you are synchronizing users.</td>
</tr>
<tr>
<td>User Entitlement Profile</td>
<td>Select the User Entitlement Profile that specifies the devices and services to which users synchronized from the LDAP server are entitled. The selected entitlement profile is assigned to each synchronized user. It is checked during user provisioning to ensure the user's configuration does not exceed the allowed services and devices specified in the entitlement profile.</td>
</tr>
<tr>
<td>User Role</td>
<td>Select the User Role to be assigned to all synchronized users. This value can be changed manually for individual users after synchronization. This field is mandatory.</td>
</tr>
<tr>
<td>User Move Mode</td>
<td>Indicates whether users are automatically moved to sites based on the filters and filter order defined in User Management &gt; Manage Filters.</td>
</tr>
<tr>
<td>User Delete Mode</td>
<td>Indicates whether users are automatically deleted from Cisco Unified CDM if they are deleted from the LDAP directory. If set to automatic, all subscriber resources associated with the user, such as a phone, are also deleted.</td>
</tr>
<tr>
<td>User Purge Mode</td>
<td>Indicates whether users are automatically deleted from Cisco Unified CDM if they are purged from the LDAP device model. An administrator can remove the LDAP user from the device layer even if the user has not been removed from the LDAP directory.</td>
</tr>
</tbody>
</table>

Step 6  Click the Field Mappings tab and enter the following required mappings:

- *LDAP Username* (for example, sAMAccountName)
- *Surname*

Step 7  (Optional) Complete other field mappings as needed, for other operations such as pushing users to Cisco Unified Communications Manager or creating move filters.
Step 8  Click Save.

**Auto Move Users to Site**

**Procedure**

Step 1  Select the customer intermediate node in the hierarchy.

Step 2  Go to User Management -> Manage Filters -> Define Filters

Step 3  Fill in name, desired hierarchy, and role (recommend self service)

Step 4  Decide what is the condition to determine site

**Synchronize Users from LDAP**

For Cisco Unified Communications Domain Manager 10.6(x) and later, you can synchronize users from LDAP by activating a scheduled synchronization, or by performing a manual synchronization.

**Procedure**

Step 1  To activate a scheduled LDAP synchronization:
   
   a. Navigate to LDAP Management > LDAP Schedule.
   
   b. Click an LDAP Schedule.
   
   c. Check the Active check box.
   
   d. Click Save.

Step 2  To perform a manual LDAP synchronization:
   
   a. Set the hierarchy path to the hierarchy node where the LDAP server is.
   
   b. Click User Management > Sync & Purge > LDAP Users.
   
   c. Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove Log Messages</td>
<td>Select if you want to remove user management logs before synchronizing or purging.</td>
</tr>
<tr>
<td>Remove Log Direction</td>
<td>Select Local to remove logs at the hierarchy of the LDAP server. Select Down to remove logs at and below the hierarchy of the LDAP server. This field appears only if Remove Log Messages is checked.</td>
</tr>
<tr>
<td>Action</td>
<td>Select synchronize or purge. This field is mandatory.</td>
</tr>
</tbody>
</table>

   d. Click Save to start the action you selected.

Cisco Unified CDM attempts to synchronize users from the LDAP server. It may take a few minutes for the users to show up in Cisco Unified CDM.
Move Users to Site (optional if not automatically done from above)

Procedure

Step 1  Sign in as a provider, reseller, or customer administrator to Unified CDM.

Step 2  Go to User Management and Move Users.

Step 3  Select Move user by username Action.

Step 4  Select User.

Step 5  Select correct site for Move To Hierarchy option.

Step 6  Select SiteSelfService for Move To Role option.

Step 7  Click Save.

Enable LDAP Authentication in Unified CM for Users Synced from LDAP to Unified CDM

Use this procedure to enable LDAP Authentication on Cisco Unified CM in the following situation, sometimes referred to as "top-down" deployment:

- You plan to sync users from LDAP to Cisco Unified CDM.
- You do not plan to sync those users from LDAP to Cisco Unified CM.
- You plan to push those users from Cisco Unified CDM to Cisco Unified CM.
- You want to use LDAP to authenticate those users' access to Cisco Unified CM.

Procedure

Step 1  On Cisco Unified CM, disable dirsync.

  a. Log in as an administrator.
  b. In the Navigation menu, select Cisco Unified Serviceability and click Go.
  c. Select Tools > Service Activation.
  d. Scroll down to Directory Services and uncheck Cisco DirSync.
  e. Click Save.

Step 2  On Cisco Unified CM, enable LDAP.

  a. In the Navigation menu, select Cisco Unified CM Administration and click Go.
  b. Select System > LDAP > LDAP System.
  c. Check Enable Synchronizing from LDAP Server.
  d. Select the LDAP Server Type. Important:
     This value must match the LDAP Server Type you choose in Cisco Unified CDM.
  e. Select the LDAP Attribute for User ID. Important:
     This value must match the LDAP attribute you choose in Cisco Unified CDM.
  f. Click Save.
Step 3  In Cisco Unified CM, configure LDAP Directory.

a. In the Navigation menu, select Cisco Unified CM Administration and click Go.

b. Select System > LDAP > LDAP Directory.

c. Configure fields in the LDAP Directory Information section.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Configuration Name</td>
<td>Enter a unique name (up to 40 characters) for the LDAP directory. Important: You use the LDAP Configuration Name when you configure the LDAP Server in Cisco Unified CDM.</td>
</tr>
<tr>
<td>LDAP Manager Distinguished Name</td>
<td>Enter the user ID (up to 128 characters) of the LDAP Manager who is an administrative user that has access rights to the LDAP directory.</td>
</tr>
<tr>
<td>LDAP Password</td>
<td>Enter a password (up to 128 characters) for the LDAP Manager.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Re-enter the password that you provided in the LDAP Password field.</td>
</tr>
<tr>
<td>LDAP User Search Base</td>
<td>Enter the location (up to 256 characters) where all LDAP users exist. This location acts as a container or a directory. This information varies depending on your customer setup.</td>
</tr>
<tr>
<td>LDAP Custom Filter</td>
<td>Select an LDAP custom filter to filter the results of LDAP searches. LDAP users that match the filter are imported into the Unified CM database. LDAP users that do not match the filter do not get imported. The default value is &lt;None&gt;. This value applies a default LDAP filter that is specific to the LDAP server type. The available default LDAP filters are:</td>
</tr>
<tr>
<td></td>
<td>o Microsoft Active Directory (AD):(&amp;(objectclass=user)(!(objectclass=Computer))(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))</td>
</tr>
<tr>
<td></td>
<td>o iPlanet or Sun One LDAP Server:(&amp;(objectclass/inetOrgPerson)</td>
</tr>
<tr>
<td></td>
<td>o OpenLDAP:(&amp;(objectclass=inetOrgPerson)</td>
</tr>
<tr>
<td></td>
<td>o Microsoft Active Directory Application Mode (ADAM):(&amp;(objectclass=computer)(!(msDS-UserAccountDisabled=TRUE)))</td>
</tr>
</tbody>
</table>

d. Configure fields in the LDAP Server Information section.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname or IP Address for Server</td>
<td>Enter the hostname or IP address of the server where the data for this LDAP directory resides.</td>
</tr>
</tbody>
</table>
### LDAP Port

Enter the port number on which the corporate directory receives the LDAP requests. You can access this field only if LDAP authentication for users is enabled.

The default LDAP port for Microsoft Active Directory and for Netscape Directory specifies 389. The default LDAP port for Secured Sockets Layer (SSL) specifies 636.

How your corporate directory is configured determines which port number to enter in this field. For example, before you configure the LDAP Port field, determine whether your LDAP server acts as a Global Catalog server and whether your configuration requires LDAP over SSL. Consider entering one of the following port numbers:

**LDAP Port when the LDAP server is not a Global Catalog server:**

- 389 – When SSL is not required. (This port number specifies the default that displays in the LDAP Port field.)
- 636 – When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.)

**LDAP Port when the LDAP server Is a Global Catalog server:**

- 3268 – When SSL is not required.
- 3269 – When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.)

**Tip**

Your configuration may require that you enter a different port number than the options that are listed in the preceding bullets. Before you configure the LDAP Port field, contact the administrator of your directory server to determine the correct port number to enter.

### Use SSL

Check this check box to use Secured Sockets Layer (SSL) encryption for security purposes.

If LDAP over SSL is required, the corporate directory SSL certificate must be loaded into Cisco Unified CM. The *Cisco Unified Communications Operating System Administration Guide* documents the certificate upload procedure in the Security chapter.

### Add Another Redundant LDAP Server

Click this button to add another row to provide information about another LDAP server.

e. **Click Save.**

**Step 4**

On Cisco Unified CM, configure LDAP Authentication.

a. In the Navigation menu, select Cisco Unified CM Administration and click Go.

b. Select System > LDAP > LDAP Authentication.

c. Check Use LDAP Authentication for End Users.
d. Enter the LDAP Manager Distinguished Name who is an administrative user that has access rights to the LDAP directory.

e. Enter the LDAP Password for the user ID in previous step.

f. Enter the LDAP User Search Base. Important:
   This value must match the LDAP User Search Base you configured for the LDAP Directory in Unified CM. It must also match the LDAP Server you configure in Unified CDM.

g. Enter the hostname or IP of the LDAP server. Important:
   This value must match the LDAP server hostname you configured for the LDAP Directory in Unified CM. It must also match the LDAP Server hostname you configure in Unified CDM.

h. Click Save.

Step 5 On Cisco Unified CDM, sync Cisco Unified CM data to Cisco Unified CDM.

   a. Log in as a customer administrator.
   b. Select Device Management > Advanced > Perform Publisher Actions.
   c. Select Action > Import
   d. Select the App Type, CUCM Device.
   e. Select an Available CUCM device to be synced.
   f. Click Save.

Step 6 On Cisco Unified CDM, configure the LDAP Server. Important:
Be sure to set CUCM LDAP Directory Name to the LDAP Configuration Name you used to configure LDAP Directory on Cisco Unified CM.
For a detailed procedure, see Cisco Unified Communications Domain Manager, Release 10.6(3) Maintain and Operate Guide.

Step 7 On Cisco Unified CDM, set up LDAP for user synchronization.
For a detailed procedure, see Cisco Unified Communications Domain Manager, Release 10.6(3) Maintain and Operate Guide.

Step 8 On Cisco Unified CDM, sync users from LDAP to Cisco Unified CDM.
For a detailed procedure, see "Sync and Purge LDAP Users" in Cisco Unified Communications Domain Manager, Release 10.6(3) Maintain and Operate Guide.

Step 9 On Cisco Unified CDM, push users to Cisco Unified CM, either by Manage Users or by Subscriber Management.
For more information, see Cisco Unified Communications Domain Manager, Release 10.6(3) Maintain and Operate Guide.

When users are pushed to Cisco Unified CM, the ldapDirectoryName field in the device/cucm/User is populated with the CUCM LDAP Directory Name. Cisco Unified CM treats the users as LDAP integrated, instead of local. The users appear as LDAP Active Users and use LDAP bind for authentication. From now on, the users are authenticated in Cisco Unified CM against the LDAP directory.
Fill in the CUCM LDAP Directory Name field in the LDAP Server on CUCDM

Procedure

Step 1  Go to LDAP Management -> LDAP Server

Step 2  Select the appropriate server

Step 3  Fill in the CUCM LDAP Directory Name with the LDAP Directory name from CUCM (found in CUCM System -> LDAP -> LDAP Directory) and click save.

Step 4  Add/update users in CUCM

Step 5  Select site in hierarchy and User Management > Manage users.

Step 6  Select Add or update users to CUCM for the Action.

Step 7  Select the Network Device List and select all users and Click Save.

Step 8  Repeat for other sites.

Endpoint Registration for Desk Phones and Jabber

Self-Provisioning

The Cisco Unified Communications Domain Manager Self-Provisioning feature allows an end user or administrator to add an un-provisioned phone to a Cisco Unified Communications Manager system with minimal administrative effort. A phone can be added by plugging it into the network and following a few prompts to identify the user.

The following process is used to self-provision a phone:

Procedure

Step 1  The user or admin connects the phone to the network.

Step 2  The user or admin enters the Server Domain for the Expressway (ex. collabedge-161.dc-01.com) and user credentials.

Step 3  The phone connects to the Expressway and auto-registers.

Step 4  The user or admin dials the IVR application and satisfies the prompts (selfservice ID and PIN provided by admin).

Step 5  The IVR application deletes the auto-registered phone and adds it back using templates associated with the user via their User Profile.

Required Configuration in Cisco Unified Communications Domain Manager

The following configuration in Unified CDM must be already configured before proceeding:

Procedure

Step 1  The Hierarchy Management (ex. Provider > Customer > IntermediateNode > Site).
Step 2  Site dial plan: Dial Plan Management > Site > Dial Plan.

Step 3  Site Defaults: Site Management > Defaults.

Step 4  Directory Number Inventory: Dial Plan Management > Number Management > Add Directory Number Inventory to add if not already done.

Step 5  Make sure the dial plans match the user's numbers in the AD.

Add a Self-Provisioning User Profile

Procedure

Step 1  Sign in as a provider, reseller, or customer administrator to Unified CDM.

Step 2  Set the hierarchy path to the site node where you want to configure self-provisioning.

Step 3  Select User Management > Self-Provisioning > User Profile.

Step 4  Click Add.

Step 5  Click the Device Template Desk Phone tab.
  a. Click the plus sign to add a new template.
  c. Check the Allow Control Of Device From Cti.
  d. Under Calling Search Space select the appropriate option (ex. Cu2Si4-InternalOnly-CSS).

Step 6  Click the Line Template tab.
  a. Click the plus sign to add a new template.
  b. Under Partition select the appropriate option (example. Cu2-DirNum-PT).
  c. Under Calling Search Space select the appropriate option (example. Cu2Si4-InternalOnly-CSS).
  d. Under Voice Mail Profile select the appropriate option or Default.

Step 7  Click Save.

Step 8  Enter other optional settings, if applicable.

Set a Default User Profile for a Site

Set a default user profile for a site, to be used when no user profile is specified when adding a subscriber.

Procedure

Step 1  Log in as provider, reseller, or customer admin to Unified CDM.
Step 2 Select Site Management > Defaults.

Step 3 Click the Defaults to edit.

Step 4 In the Default User Profile (for User Self Provisioning) field, enter the default user profile for the site.

Step 5 Click Save.

Add Self-Provisioning Line Mask

Procedure

Step 1 Log in as provider, reseller, or customer admin to Unified CDM.

Step 2 Set the hierarchy path to the site node where you want to configure self-provisioning.

Step 3 Select User Management > Self-Provisioning > Line Mask.

Step 4 Click Add.

Step 5 Provide the following information:
   a. Description.
   b. Mask (ex XXXX).

Step 6 Click Save.

Cisco Unified Communications Manager Configuration for Self-Provisioning

To use self-provisioning, the following one-time configuration tasks must be done on Cisco Unified Communications Manager:

Procedure

Step 1 Ensure that the Cisco CallManager, Cisco CTIManager, and Self-Provisioning IVR services are activated and running.

Step 2 Configure Auto Registration.
   a. System > Cisco Unified CM.
   b. Select the desired CUCM.
   c. Set starting and ending directory number range.
   d. Select the created Universal Device Template and Universal Line Template.
   e. Uncheck Auto-registration Disabled.

Step 3 Create a partition and calling search space for self-provisioning
   a. Call Routing > Class of Control > Partition and add New.
   b. Call Routing > Class of Control > Calling Search Space and add New.
c. Select the previously created partition to be assigned with the new CSS.

Step 4 Configure a CTI Route Point (this provides the number that users dial to connect to the IVR).
   a. Device > CTI Route Point.
   b. Add New.
   c. Fill in name, device pool, CSS, and any options desired.
   d. Add a new DN in the proper partition (this is the IVR number end user dials).

Step 5 Configure an Application User and credentials so the system can connect to the IVR self-provisioning service.
   a. User Management > Application User.
   b. Add New.
   c. Fill in User ID and password.
   e. Add CTI Route Point device to list of controlled devices.

Step 6 Configure Self-Provisioning (NOTE: May not work in Google Chrome browser).
   b. Add the previously created CTI Route Point.
   c. Select the Application User.
   d. Click Save.

**Verification for Self-Provisioning**

**Procedure**

Step 1 Sync users from LDAP to Unified CDM or create users in Unified CDM.

Step 2 Make sure subscribers have a Primary Extension and Self Service configured in Subscriber Management > Subscribers.
   a. If they do not, then go to Subscriber Management > Quick Add Subscriber.
   b. Select the proper Username.
   c. Enter a PIN.
   d. Click Set Self Service Id at the bottom of the page.
   e. Add the proper Lines info for the subscriber.
   f. Add Jabber Device details if applicable.
   g. Click Save.

Step 3 Sync users from Unified CDM to CUCM if not setup to auto sync.
   a. In Unified CDM o to User Management > Manage Users.
   b. Select Add or update users to CUCM.
c. Select the appropriate Network Device List.

d. Select the desired users.

e. Click Save.

Step 4 Verify end users in CUCM have Primary Extension and Self-Service User ID auto generated.

Step 5 Info Provider Gives to End User to Register Endpoints:

a. Collabedge address

b. User ID

c. User password

d. User self-service ID (only for desk phones)

e. User PIN (only for desk phones)

Step 6 Users are now ready to self-provision their desk phones or Jabber accounts! The users will need their User ID, password, their self-service ID, and PIN. Then, users can execute the following steps for desk phones:

a. Plug their phone into the network.

b. Enter the Expressway address for the Server Domain.

c. Enter the User ID and password.

d. Wait for phone to auto register.

e. Dial the IVR number.

f. Enter the user self-service ID.

g. Enter the user PIN.

Wait for the phone to reboot and register with their extension.

Step 7 Users can get the Jabber install from either the provider or can download the file from cisco.com

Step 8 The following steps can be followed for Jabber accounts:

a. Open Jabber.

b. Enter the User ID with the collabedge domain (example. user1@collabedge-161.dc-01.com).

Enter the User’s password and click sign in.

Tip: End user needs to restart Jabber (2-3 times) for directory search to work in case it doesn’t work first time.

Add Imagicle for Directory Search in Jabber

The following steps will make directory searches in Jabber only show the users in their own customer base instead of all the users in the AD.

Procedure

Step 1 Create XML File.

Change the UdsServer to the appropriate customer domain from the below template and save it as jabber-config-customer-name.
Step 2 Upload XML File to CUCM TFTP.
   a. Login to CUCM.
   b. Go to Cisco Unified OS Administration.
   c. Go to Software Upgrades and TFTP File Management.
   d. Click the Upload File.
   e. Click Choose File and find the XML file.
   f. Click the Upload File.

Step 3 Restart TFTP Service.
   a. Go to Cisco Unified Serviceability.
   b. Go to Tools and Control Center – Feature Services.
   c. Select the CUCM Server.
   d. Select Cisco TFTP.
   e. Click the Restart button.

Step 4 Add Customer Entry into DNS Host/Alias.
   a. First customer
      i. Go to the Forward Lookup Zone for the AD.
      ii. Create a new domain under the SP domain (ex dcloud.cisco.com).
      iii. The domain will start with imagicle (ex imagicle.dcloud.cisco.com).
      iv. Create a new host in the imagicle domain with the customer name (ex c1.imagicle.dcloud.cisco.com) and the address is the IP of the Imagicle server.
   b. Additional customers
      i. Create a new Alias in the imagicle domain.
      ii. The alias name is the customer name (ex c2 with FQDN as c2.imagicle.dcloud.cisco.com).
      iii. The FQDN for the target host is the original host (ex c1.imagicle.dcloud.cisco.com).

Step 5 Add Customer Entry into Exp-C Allow List.
   a. Login to Expressway-C with admin user.
   b. Go to Configuration and Unified Communications and Configuration.
   c. Click the Configure HTTP server allow list.
   d. Click New.
Enter the customer domain with imagicle in the name (ex c2.imagicle.dcloud.cisco.com).

Click Create entry.

Step 6 Fill in the Cisco Support Field with XML Config.

a. Login to CUCM.

b. Find the desired device configuration page for the associated Jabber device.

c. Fill in the Cisco Support Field with configurationfile=jabber-config-c2.xml and replace the xml file name with the appropriate file name.

d. If you do not see the Cisco Support Field for mobile devices, then please install the following Cisco Options Packages for your release of CUCM – cmterm-android-install-XXX.cop.sgn, cmterm-jabbertablet-install-XXX.cop.sgn, and cmterm-iphone-install-XXX.cop.sgn.

Add Imagicle for Directory Search in Desk Phones

The following steps will make directory searches in Desk Phones only.

Procedure

Step 1 Login to CUCM.

Step 2 Go to Device > Device Settings > Phone Services.

Step 3 Search for Corporate Directory and select.

Step 4 In the Service URL field, enter http://1.1.1.1/fw/Apps/Speedy/xml/directories/default.aspx?name=#DEVICENAME# with the IP of the Imagicle server replacing 1.1.1.1

Step 5 Click Save.

Step 6 Reboot any phones already registered.

Another option is to modify the “Alternate phone book server address” in the device page with “https://customer-name.imagicle.domain.com:8443/cucm-uds/users”. Make sure to replace customer-name with the DNS name for the customer and domain.com with the HCS-SA domain.

Imagicle add-on applications for Shared Architecture

Beyond the customer separation through Speedy Directory services, the Imagicle AppSuite can offer multiple services to multiple customers with a single instance (one or multiple vm):

Fax Server

MRA does not allow managing fax transactions using analog fax machines on ATA. In order to provide fax functionality, it is possible to use Imagicle StoneFax, a completely software-based IP Fax Server that virtualizes fax management. StoneFax allows users to send/receive faxes directly through e-mail, web, multifunction printers, Cisco Jabber desktop and on mobile smartphones and tablets.

ACD and IVR auto attendant

Native CUCM call queueing and hunt groups are not supported through MRA. In order to provide this functionality, it is possible to adopt Imagicle QueueManager, a complete inbound ACD solution that allows creating unlimited queues and answering groups, with related time tables and voice prompts. Imagicle QueueManager includes auto-
attendant features with the optional IVR module, together with advanced historical reports for IVR, queues and agents. QueueManager and IVR module are both configurable through an easy and intuitive web portal.

**Attendant Console**

An IP-phone connected through MRA can’t be controlled by jabber desktop client because desk-phone CTI control mode is not supported. In order to allow control of your desk phone in MRA mode and gain advanced features, it is possible to use Imagicle Blue’s Attendant PC client, allowing to monitor and control telephony functionalities, display BLF and rich presence status of colleagues, access to internal/external company and personal Speedy contacts (separated per customer). Imagicle Blue’s Attendant Console is fully integrated with Imagicle QueueManager, being able to see the calls waiting in queue, login/logout to queues and real-time statistics, to provide an advanced ACD-IVR and attendant console solution.

For more information, refer to the following link for Imagicle Administration Guides.
Appendix A-High Level Onboarding steps

Customer on boarding steps

Perform the following steps -.

Procedure

Step 1  Create Customer and Users in AD.

Step 2  Unified CDM Setup - Customer Configuration

a. Setting up the Hierarchy.
b. Configure Entitlement.
c. Configure a Network Device List.
d. CUCM Group Configuration.
e. Create a Customer Dial Plan.
g. Add a Site.
h. Add First Site Dial Plan.
i. Cisco Unified CDM Number Management.
j. Add Directory Number Management.
k. Configure Directory Number Routing.
l. Associate a Range of E.164 Number to a Range of Directory Numbers.

Step 3  LDAP Integration in Unified CDM

a. Set up an LDAP Server.
b. Set up LDAP for User Synchronization.
c. Synchronize Users from LDAP.

Step 4  Move Users to Site.

Step 5  Enable LDAP Authentication in Unified CM for Users Synced from LDAP to Unified CDM.

Step 6  Endpoint Registration for Desk Phones and Jabber.

a. Add a Self-Provisioning User Profile.
b. Set a Default User Profile for a Site.
c. Add Self-Provisioning Line Mask.
d. CUCM Configuration for Self-Provisioning.
e. Verification for Self-Provisioning.

Step 7  Add Imagicle for Directory Search in Jabber.
New user on boarding steps

Perform the following steps –

Procedure

Step 1  Create Customer and Users in AD (only need to add users).

Step 2  Synchronize Users from LDAP.

Step 3  Move Users to Site.

Step 4  Verification for Self-Provisioning.
References

Cisco Hosted Collaboration Solution, Release 10.6(1) Solution Reference Network Design Guide

Cisco Hosted Collaboration Solution, Release 10.6(1) Customer Onboarding Guide

Cisco Hosted Collaboration Solution, Release 10.6(1) Installation Guide

Cisco Expressway on Virtual Machine Installation Guide

Installing Cisco Unified Communications Manager and IM and Presence Service, Release 10.0(1)

Install, Upgrade, and Maintenance Guide for Cisco Unity Connection Release 10.x

Cisco Expressway on Virtual Machine Installation Guide