

Call Control

Revised: February 19, 2019

This chapter describes the call control function for the Cisco Preferred Architecture (PA) for Enterprise Collaboration.

Certain requirements might put your deployment outside the PA design guidelines and recommendations, in which case you might have to use other documentation such as the *Cisco Collaboration SRND* and related product documentation.

The first part of this chapter provides an architectural overview and introduces some fundamental design concepts, while the second part explains more detailed deployment considerations. The Architecture section discusses topics such as redundancy concepts, high availability, Computer Telephony Integration (CTI), and IM and presence architecture, and it introduces a hypothetical customer topology used in the examples throughout this document. The focus of this chapter is the Deployment Overview section. The deployment examples in that section will help you to understand the background of certain design decisions more clearly than an abstract discussion of concepts can. Topics covered in the Deployment Overview section include DNS requirements, cluster provisioning, certificate management, dial plan configuration, user provisioning using LDAP, media resources, SIP trunking considerations, endpoint provisioning, and multi-cluster considerations. The order of the topics in the Deployment Overview section follows the recommended configuration order.

What's New in This Chapter

Table 2-1 lists the topics that are new in this chapter or that have changed significantly from previous releases of this document.

Table 2-1 New or Changed Information Since the Previous Release of This Document

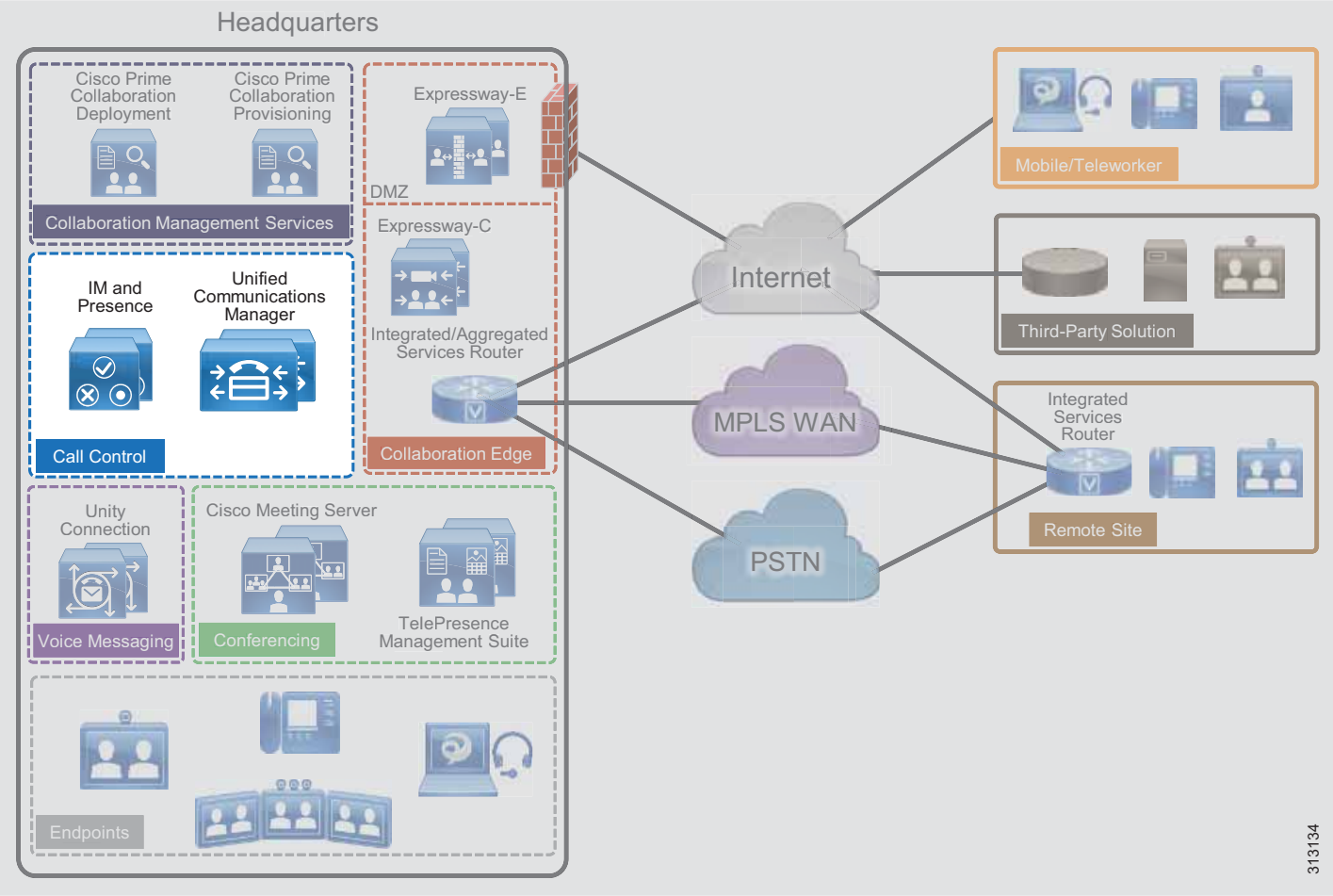
New or Revised Topic	Described in:	Revision Date
Added information on Apple Push Notification service (APNs)	Integration with Apple Push Notification Service (APNs), page 2-9 Onboarding for Push Notifications via Apple Push Notification Service (APNs), page 2-24 Other IM and Presence Settings, page 2-25	August 30, 2017
OAuth with Refresh Login Flow	Other IM and Presence Settings, page 2-25 Table 2-2	August 30, 2017

Core Components

The core architecture contains these key elements (Figure 2-1):

- Cisco Unified Communications Manager
- Cisco Unified Communications Manager IM and Presence Service
- Cisco Integrated Services Router (ISR)

Figure 2-1 Preferred Architecture Overview



Key Benefits

- Call control is centralized at a single location that serves multiple remote sites.
- Management and administration are centralized.
- Common telephony features are available across voice and video endpoints.
- Single call control and a unified dial plan are provided for voice and video endpoints.
- Critical business applications are highly available and redundant.

Architecture

The handling and processing of voice and video calls is a critical function provided by enterprise communications systems. This functionality is handled by some type of call processing entity or agent. Given the critical nature of call processing operations, it is important to design unified communications deployments to ensure that call processing systems are scalable enough to handle the required number of users and devices and are resilient enough to handle various network and application outages or failures.

This chapter provides guidance for designing scalable and resilient call processing systems with Cisco Unified Communications Manager (Unified CM) and Survivable Remote Site Telephony (SRST). A centralized Unified CM cluster implements call processing services for all customer sites. Unified CM IM and Presences Service as part of the centralized Unified CM cluster implements instant messaging and presence services for the enterprise. Cisco Survivable Remote Site Telephony (SRST) is used to implement backup services for remotes sites when the corporate WAN reliability does not match the voice services availability requirements.

Cisco Unified CM provides call processing services for small to very large single-site deployments, multi-site centralized call processing deployments, and/or multi-site distributed call processing deployments. Unified CM is at the core of a Cisco Collaboration solution, and it serves as a foundation to deliver voice, video, IM and presence, messaging, mobility, web conferencing, and security.

Access to the enterprise collaboration network and to Unified CM from the Internet to enable remote access and business-to-business secure video communications, is also available through various collaboration edge solutions such as VPN and Cisco Expressway.

Role of Unified CM

Cisco Unified CM is the central call control component in any Cisco collaboration deployment. Unified CM provides foundation services including call control, endpoint registration, endpoint configuration, call admission control, codec negotiation, trunk protocol translation, and CTI. Unified CM is the central point of administration and provisioning. All SIP trunks to other components – including conferencing media resources, gateways, and other components – are terminated on Unified CM so that Unified CM can orchestrate access to all of those components. Call routing is controlled by the dial plan configuration applied to Unified CM.

Role of IM and Presence Service

The Cisco Unified CM IM and Presence Service provides on-premises instant messaging and presence. It uses standards-based XMPP and also supports SIP for interoperability with SIP IM providers. Cisco Unified CM IM and Presence Service is an on-premises solution. The other Cisco instant messaging and presence service, Cisco WebEx Messenger, is a cloud-based service and is not covered in this document.

Role of SRST

When deploying Cisco desk phones in branch locations separated from a centralized call processing platform by a low-speed or unreliable WAN link, it is important to consider local call processing redundancy. By leveraging Survivable Remote Site Telephony (SRST) on a Cisco IOS router in each branch location, basic IP telephony services can be maintained for the desk phones if connectivity to the centralized call processing platform is lost. However, the set of available user-facing features is much smaller when a device is registered to SRST than when the phone is registered to Unified CM.

Unified CM Redundancy with Survivable Remote Site Telephony (SRST)

Cisco IOS SRST provides highly available call processing services for endpoints in locations remote from the Unified CM cluster. Unified CM clustering redundancy schemes provide a high level of redundancy for call processing and other application services within a LAN or MAN environment. However, for remote locations separated from the central Unified CM cluster by a WAN or other low-speed links, SRST can be used as a redundancy method to provide basic call processing services to these remote locations in the event of loss of network connectivity between the remote and central sites. We recommend deploying SRST-capable Cisco IOS routers at each remote site where call processing services are considered critical and need to be maintained in the event that connectivity to the Unified CM cluster is lost. Endpoints at these remote locations must be configured with an appropriate SRST reference within Unified CM so that the endpoint knows what address to use to connect to the SRST router for call processing services when connectivity to Unified CM subscribers is unavailable.

Unified CM and IM and Presence Service Clustering

Unified CM supports the concept of clustering. The Unified CM architecture enables a group of server nodes to work together as a single call processing entity. This grouping of server nodes is known as a cluster.

There are two types of Cisco Unified CM nodes: publisher and subscriber.

- Unified CM publisher

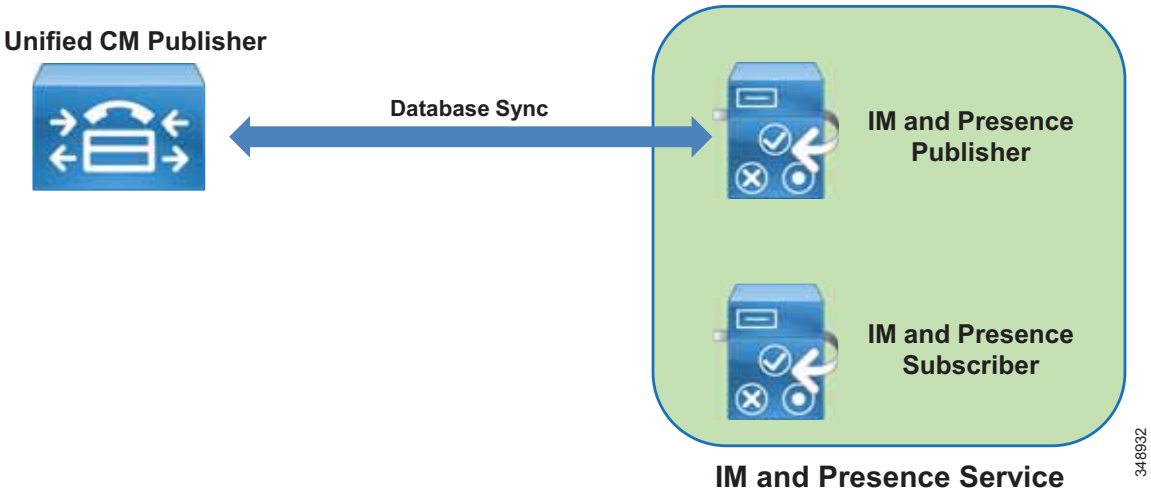
  The publisher is a required server node in all clusters. There can be only one publisher per cluster. This server node contains the cluster configuration, and it provides the database services to all other subscribers in the cluster. In this design, the Unified CM publisher is a dedicated node; it does not handle TFTP requests, endpoint registration, or call processing.

- Unified CM subscriber

  Subscriber nodes subscribe to the publisher to obtain a copy of the database information. Subscriber nodes include, for example, the Unified CM TFTP nodes and the Unified CM call processing subscriber nodes.

Cisco IM and Presence nodes have the same clustering concept. The first IM and Presence node is the IM and Presence publisher. The other IM and Presence nodes are the IM and Presence subscribers, and they obtain a copy of their database from the IM and Presence publisher. The IM and Presence publisher communicates with the Unified CM publisher and most of the IM and Presence configuration is actually done through the Unified CM publisher (for instance, the Unified CM users, the UC services available to presence users, and the service activation). Hence, all IM and Presence nodes, including the IM and Presence publisher, are considered subscribers of the larger Unified CM and IM and Presence Service cluster. Figure 2-2 shows the relationship between the Unified CM publisher and a two-node IM and Presence cluster.

Figure 2-2 Relationship Between Unified CM and a Two-Node IM and Presence Cluster



High Availability

Unified CM and IM and Presence nodes should be deployed in a highly available infrastructure. For example, the use of dual power supplies combined with the use of uninterruptible power supply (UPS) sources will provide maximum power availability. From a network perspective, the platform servers should be connected to multiple upstream switches.

Unified CM and IM and Presence systems also handle high availability at the application level.

With Unified CM in this design, two TFTP servers should be deployed for redundancy. The call processing nodes should be deployed with one-to-one (1:1) redundancy, where for every primary call processing subscriber there is a backup call processing subscriber. This 100%:0% redundancy design compared to a 50%:50% redundancy design has a number of advantages, including the reduction of Unified CM groups and device pools and simplified configuration and distribution of devices with fewer redundancy options.

Cisco IOS Survivable Remote Site Telephony (SRST) provides highly available call processing services for endpoints in locations remote from the Unified CM cluster when the WAN links are down.

Individual Cisco IM and Presence nodes are grouped in subclusters. A subcluster can have one or two nodes. Adding the second node in a subcluster provides high availability. High availability is recommended, and therefore in this design each subcluster consists of two nodes. A two-node subcluster allows for users associated with one server of the subcluster to use the other server in the subcluster automatically if a failover event occurs. We recommend balancing the user assignment between the two nodes in each pair. The IM and Presence publisher handles IM and Presence information from presence clients just like any other IM and Presence subscriber does, and it is deployed as one of the two nodes in an IM and Presence subcluster.

Computer Telephony Integration (CTI)

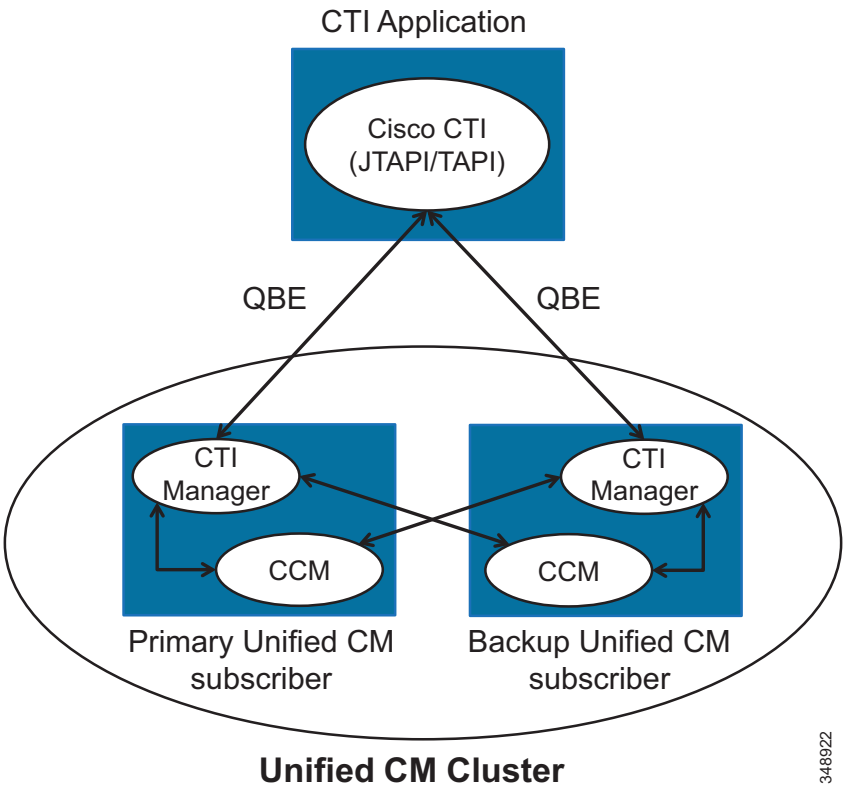
Cisco Computer Telephony Integration (CTI) extends the rich feature set available on Cisco Unified CM to third-party applications.

CTI Architecture

Cisco CTI consists of the following components (Figure 2-3), which interact to enable applications to take advantage of the telephony feature set available in Cisco Unified CM:

- CTI application — Cisco or third-party application written to provide specific telephony features and/or functionality. It can use a JTAPI or TAPI interface. The protocol between the CTI application and Unified CM is Quick Buffer Encoding (QBE).
- Unified CM subscriber with the following services:
  - CCM — The Cisco CallManager Service, the telephony processing engine.
  - CTI Manager (CTIM) — A service that runs on one or more Unified CM subscribers operating in primary/secondary mode and that authenticates and authorizes telephony applications to control and/or monitor Cisco IP devices.

Figure 2-3 CTI Architecture



High Availability for CTI

High availability for CTI Manager relies on the CTI application being able to connect to the backup CTI Manager Service in case the primary CTI Manager fails. In case both the CTI Manager and CCM services on the primary Unified CM subscriber fail (for example, if the entire primary Unified CM subscriber fails), then both CCM and CTI Manager services running on the backup Unified CM subscriber will become active, and the CTI Manager service will monitor and control the devices that are registered to the CCM service located on the same backup Unified CM subscriber. If the primary CTI Manager Service fails but the primary CCM Service is still running (assuming you have 1:1 redundancy with a distribution of 100%/0% on the primary/backup Unified CM subscribers), then all the devices will stay registered to the CCM Service running on the primary Unified CM subscriber, and the CTI Manager running on the backup Unified CM subscriber will become active and will monitor and control the CTI devices even though they are registered to a CCM service running on a different node (the primary Unified CM subscriber in this case).

Capacity Planning for CTI

Ensure the capacity limits are not exceeded for the three types of CTI resources:

- The maximum number of CTI applications connecting to a given CTI Manager instance (Unified CM node running the CTI Manager service). This number is typically low with CTI server-based application, but with CTI client-based applications such as Jabber clients in deskphone mode where each Jabber client is considered a CTI application, it is important to ensure the limit is not exceeded when deploying a large number of Jabber clients.
- The maximum number of CTI-enabled endpoints registered to a given Unified CM call processing subscriber.
- The maximum number of CTI-enabled endpoints monitored and controlled by a CTI Manager instance. Ideally, the CTI Manager service running on a Unified CM node monitors only the endpoints registered to that Unified CM node. But it is possible that a CTI Manager service also monitors endpoints registered to other Unified CM nodes.

The CTI limits are the same for all three CTI resources described above. The CTI capacity limits vary with the type of OVA template. If the CTI limit is reached, deploy another pair of Unified CM call processing nodes running the CTI Manager service.

IM and Presence Architecture

The Cisco Unified CM IM and Presence Service provides on-premises instant messaging and presence. The main presence component of the solution is the IM and Presence Service, which incorporates the Extensible Communications Platform (XCP) and supports SIP/SIMPLE and Extensible Messaging and Presence Protocol (XMPP) for collecting information regarding a user's availability status and communications capabilities. The user's availability status indicates whether or not the user is actively using a particular communications device such as a phone.

Applications (either Cisco or third-party) can integrate presence and provide services that improve the end user experience and efficiency. In addition, Cisco Jabber is a supported client of the IM and Presence Service that also integrates instant messaging and presence status.

The IM and Presence Service uses the same underlying appliance model and hardware used by Unified CM on the Cisco Unified Computing System (UCS) platform.

The IM and Presence Service is deployed as an IM and Presence cluster. The IM and Presence cluster consists of up to six nodes, including one designated as a publisher and up to five subscriber nodes. As discussed in the sections on Unified CM and IM and Presence Service Clustering and High Availability, the IM and Presence nodes are grouped in subclusters and each subcluster consists of two nodes for high availability. As discussed in the sizing section, a single subcluster can be deployed in order to support up to 15,000 users. The IM and Presence publisher handles IM and presence requests, just like the IM and Presence subscribers do, so the first subcluster consists of the IM and Presence publisher and one IM and Presence subscriber.

As discussed in the section on Unified CM and IM and Presence Service Clustering, the IM and Presence nodes are considered part of the larger Unified CM and IM and Presence Service cluster.

Deployment of the Unified CM and IM and Presence Service Cluster

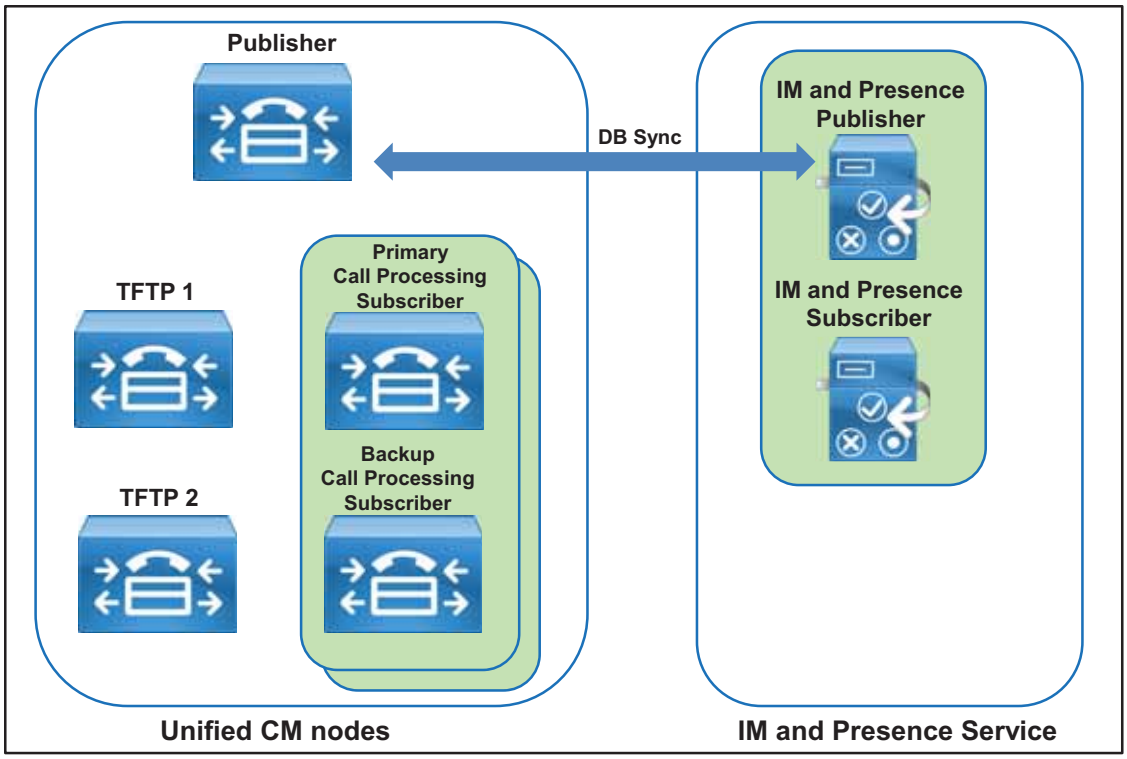
The Cisco Unified CM and IM and Presence Service cluster consists of the following nodes:

- 1x Cisco Unified CM publisher
- 2x (1 pair) Cisco Unified CM TFTP server subscribers
- 2x (1 pair) Cisco Unified CM call processing subscribers (Add additional pairs to scale.)
- 2x (1 pair) Cisco Unified IM and Presence nodes (Add additional pairs, or subclusters, to scale.)

The number of Unified CM call processing pairs and of IM and Presence pairs to add in order to scale is discussed in the chapter on Sizing.

Figure 2-4 shows an example of a Unified CM and IM and Presence Service cluster deployment with up to 10,000 devices and 10,000 users. For more sizing information, refer to the Sizing chapter.

Figure 2-4 Unified CM and IM and Presence Service Cluster Deployment



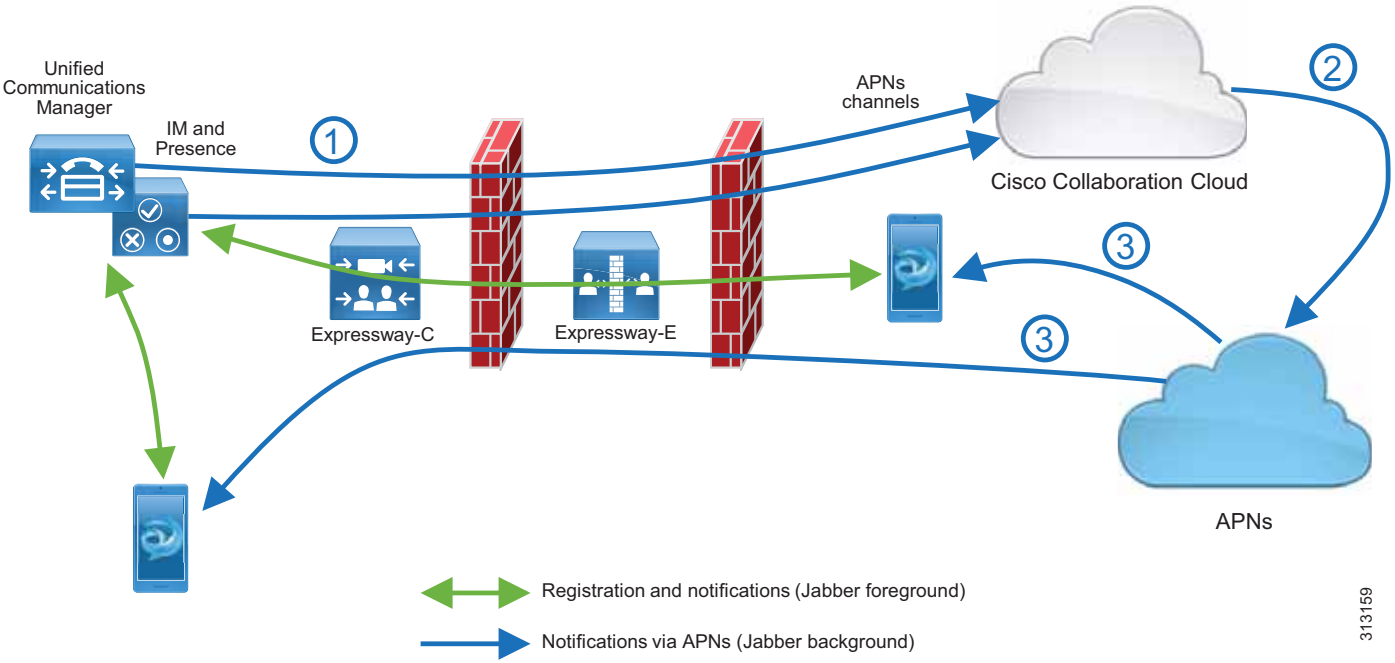
Unified CM with IM and Presence Service

Integration with Apple Push Notification Service (APNs)

When integrating a deployment of Unified CM and Unified CM IM and Presence Service with Apple Push Notification service (APNs), you can use Apple's cloud-bases Push Notification service to push notifications for voice and video calls and instant messages to Cisco Jabber for iPad and iPhone clients that are running in the background. Cisco Jabber clients on start-up register with Unified CM either directly when on the corporate network or through Cisco Expressway using mobile and remote access (MRA) when connecting from outside the corporate network. As long as the Cisco Jabber client is running in foreground mode, call and IM notifications are received directly from Unified CM or Unified CM IM and Presence Service. As soon as the Cisco Jabber client transitions to suspended mode (background), this direct method of receiving notifications transitions to Apple Push Notifications. Cisco Jabber clients in the background are activated as soon as an Apple Push Notification is received by Apple iOS. Cisco Jabber then re-activates direct communication with Unified CM and Unified CM IM and Presence Service. With this mechanism Cisco Jabber does not need to constantly poll for events such as incoming IM messages or call events. This leads to better battery lifetime and improved user experience.

Figure 2-5 shows the overall architecture of the integration with APNs. Each application running on an Apple iOS platform registers with APNs to be able to receive notifications via APNs and receives a device and application specific device token. Notification providers intending to send notifications via APNs register with APNs; and when they send a notification to a device, they need to present the device token uniquely identifying the target device and application.

Figure 2-5 Architecture for Integration with APNs



In the architecture shown in Figure 2-5, a single APNs provider is used for all integrations, and this APNs provider (Push REST service) is hosted in the Cisco Collaboration Cloud. To enable APNs integration for a given Unified CM and IM and Presence Service cluster, the cluster first needs to be onboarded into the cloud-based Push REST service. During this onboarding process a machine account is created for the specific cluster in the Cisco Collaboration Cloud, and an OAuth refresh token is issued for the cluster. With this information, all IM and Presence nodes and call processing nodes of the cluster can then create connections to the Push REST service to issue notification requests targeted for specific Jabber clients (step 1). These requests are authenticated using OAuth access tokens generated using the OAuth refresh token obtained during the onboarding process.

The Jabber clients obtain a device token from APNs during registration with APNs. This device token is reported back to the Unified CM cluster and is then used by the IM and Presence and call processing nodes in outbound notification requests to the Push REST service.

The Push REST service relays all notification requests coming in from the IM and Presence and call processing nodes to APNs (step 2), which then in turn forwards the notifications to the individual devices over the persistent connection between the Apple iOS devices and APNs (step 3).

When an Apple Push Notification is received, Apple iOS dispatches the notification to the target application. This wakes up Cisco Jabber, which transitions into foreground mode and resumes normal calling and IM interaction with Unified CM and with Unified CM IM and Presence Service.

Jabber clients running on Apple iOS need to be able to connect to APNs in the Apple cloud on port 443/TCP from within the enterprise to be able to create the connection with APNs and receive notifications from APNs.

Endpoints

Jabber

Cisco Jabber clients provides core collaboration capabilities for voice, video, and instant messaging to users. Cisco Jabber is available on a wide variety of platforms including Windows, Mac, and mobile devices such as smartphones and tablets.

Cisco Jabber can be deployed in either of two modes:

- Full UC and Cisco Jabber for Everyone (IM only) Mode

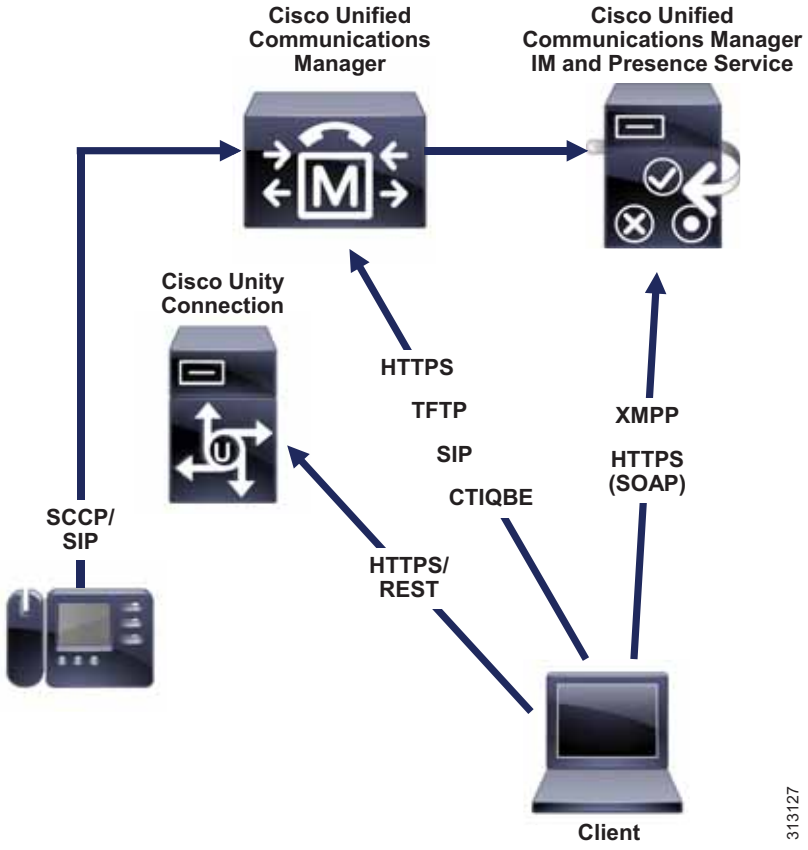
  This is the default mode. The user's primary authentication is to an IM and Presence server. This is the mode used in this Preferred Architecture design and cover in this document.

- Phone Mode

  In phone mode, the IM and Presence Service is not required.

Figure 2-6 illustrates the architecture of an on-premises deployment that includes Cisco Unified Communications Manager IM and Presence.

Figure 2-6 Cisco Unified Communications with IM and Presence Architecture



To connect to services, Cisco Jabber requires the following information:

- Source of authentication that enables users to sign in to the client

  In full UC or IM-only modes, the source of authentication is the IM and Presence service. In phone-only mode, it is Unified CM.

- Location of services

  The services include IM and Presence, directory, CTI, voicemail, and conferencing.

To provide this information to the client, we recommend using the Service Discovery method over the Manual Connection method. With the Service Discovery method, the client automatically locates and connects to services.

In this design, the client automatically discovers services and configuration with the SRV record _cisco-uds that is retrieved when the user first enters his or her email address in the Jabber client.

The Jabber Contact Sources can be an LDAP contact source with Cisco Directory Integration (CDI). Another source for the contacts can be the Unified CM User Data Service (UDS), but CDI is the recommended contact source for on-premises deployments.

Multi-Cluster Considerations

In a multi-cluster deployment, interconnect all the individual Unified CM clusters through SIP trunks. To avoid session traversal through individual clusters, deploy a full mesh of SIP trunks. With four or more clusters, deploy Cisco Unified CM Session Management Edition (SME) to centralize the dial plan and trunking and to avoid the complexity of a full-mesh SIP trunk topology. Cisco Unified CM SME is not covered in this document. For more information about SME, refer to the *Cisco Collaboration SRND*.

In multi-cluster deployments, use Global Dial Plan Replication (GDPR) to replicate dial plan information between clusters. GDPR can advertise a +E.164 number, one Enterprise Significant Number (ESN), and up to five alpha-numeric URIs per directory number. An ESN is the abbreviated inter-site dialing equivalent of a directory number. The information advertised and learned through GDPR enables deterministic intercluster routing for these dialing habits:

- +E.164 dialing based on the advertised +E.164 numbers
- Enterprise abbreviated inter-site dialing based on the advertised ESNs
- Alpha-numeric URI dialing based on the advertised URIs

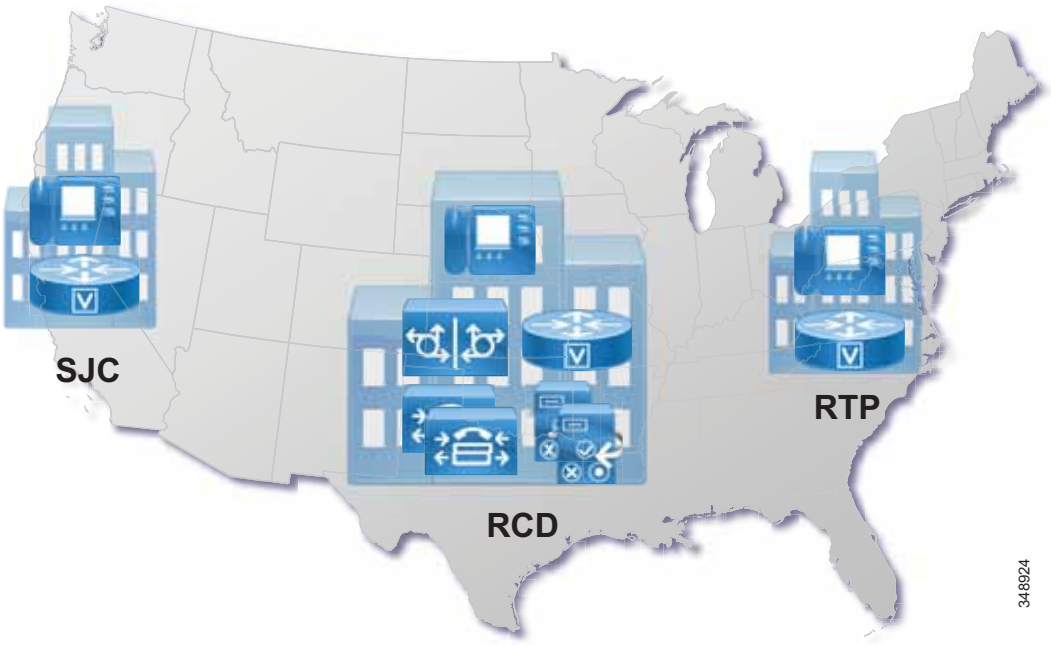
GDPR uses Intercluster Lookup Service (ILS) as the transport medium, therefore setting up ILS between all Unified CM clusters is required for multi-cluster deployments. In addition to GDPR, UDS-based service discovery used by Jabber also relies on the ILS exchange to detect the existence of UDS nodes on remote clusters to which /cucm-uds/homeCluster requests of non-local users can be forwarded to determine the home cluster of a user trying to log in to Jabber.

IM and Presence functionality is limited by having communications within a single cluster. To extend presence and instant messaging capability and functionality, these standalone clusters can be configured for peer relationships for communication between clusters within the same domain. This functionality provides the ability for users in one cluster to communicate and subscribe to the presence of users in a different cluster within the same domain. To create a fully meshed presence topology, each Cisco IM and Presence cluster requires a separate peer relationship for each of the other Cisco IM and Presence clusters within the same domain. The intercluster peer is configured as the IP address of the remote Unified CM cluster IM and Presence publisher node.

Topology Example

For the purpose of this document, we assume a centralized call processing deployment serving three sites in the US: SJC, RCD, and RTP. The Unified CM and IM and Presence Service servers are centrally located in RCD. Central PSTN access is in RCD as well. SJC and RTP are assumed to be small sites, with Survivable Remote Site Telephony (SRST) configured locally, with local PSTN access when the WAN connectivity to the RCD site is down. Figure 2-7 illustrates this topology example.

Figure 2-7 Example Topology



The topology example used in this document for multi-cluster considerations is a two-cluster deployment: the cluster in the United States as shown in Figure 2-7, and a second cluster to cover Europe, the Middle East, and Africa (EMEA).

Certificate Considerations

For certificate considerations – general concepts, deployment recommendations, and so forth – refer to the Security chapter.

DNS Considerations

As explained in the previous section, the identity of server certificates presented during connection setup is validated. This implies that clients need to initiate connections based on fully qualified domain names (FQDNs) so that the subject in the presented certificate really can be checked against the identity to which the client intends to connect. The use of FQDNs for connection initiation implies that DNS is a fundamental requirement. The enterprise DNS needs to be set up so that name resolution is reliably

available for all clients and servers in the network. In addition to providing reliable FQDN-to-IP-address (and reverse) resolution, DNS also is required for the automatic service discovery process used by Jabber clients.

During startup, Jabber clients locate the UDS service required for UDS-based service discovery by trying to resolve the _cisco-uds._tcp SRV using DNS. For best redundancy and load balancing, we recommend provisioning DNS SRV records with equal priority and weight for the Unified CM publisher and TFTP nodes.

Endpoint Addressing

All directory numbers on endpoints with DID address are provisioned as +E.164 numbers. The benefits of this approach include the following:

- +E.164 directory numbers are unique by definition.
- +E.164 directory numbers enable one dialing habit (+E.164) directly without requiring any further dial plan configuration.
- +E.164 directory numbers simplify the implementation of forced on-net routing.
- Configuration of Automated Alternate Routing (AAR) is greatly simplified. There is no need to provision multiple AAR groups and AAR PSTN prefixes because the target on-net destination can be used directly as an alternate PSTN address; it is a +E.164 number.
- Correct caller ID is automatically achieved for all call flows (direct, forwarded, on-net, and off-net).

Unique addresses are also required for endpoints without an associated DID (for example, lobby phones) and enterprise services (for example, call pickup, call park, and so forth). Since no +E.164 number exists for them, we recommend the use of an alternate enterprise specific numbering (ESN) schema to address them. The recommended format for the ESN schema is an access code chosen so that no overlap between ESN dialing and other dialing habits is created, followed by a site code and the intra-site extension. The length of the site code and extension is a trade-off between providing a large enough number space and keeping the ESN dialing as short as possible.

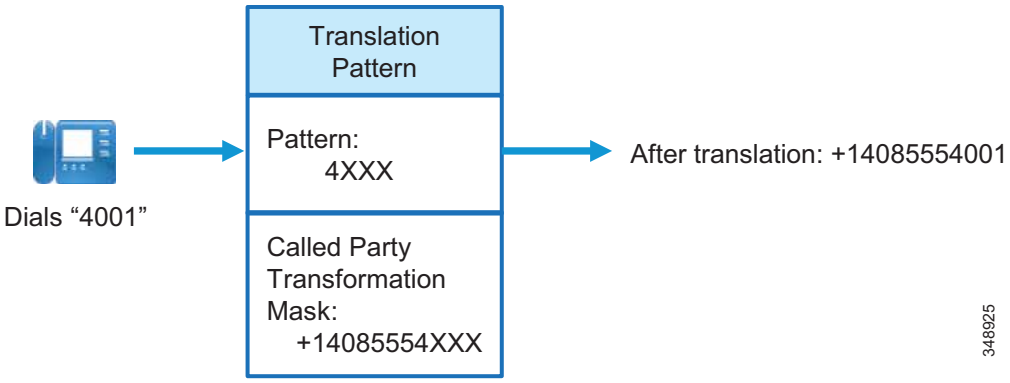
+E.164 Routing and Dialing Normalization

To achieve the intended forced on-net routing (calls to any on-net destination dialed using any of the supported numeric dialing habits has to be routed on-net), the recommended dial plan design uses a two-step routing approach. In the first step, the dialed digit string is normalized to +E.164, if possible (calls to non-DIDs obviously cannot be normalized to +E.164), and then in the second step the resulting +E.164 digit string is matched against a +E.164 numeric plan that includes directory numbers and route patterns.

The dialing normalization is achieved by provisioning translation patterns matching on the non+E.164 dial strings, and then the dialed string is transformed to +E.164 through the called party transformations on the translation patterns.

Figure 2-8 shows an example of a dialing normalization translation pattern that can be used to normalize abbreviated intra-site dialing in SJC to the full +E.164 number of the dialed destination. If a user in site SJC dials 4001, this dialed string is matched by a translation pattern 4XXX; and the called party transformation mask configured on the translation pattern, when applied to 4001, creates the resulting digit string +14085554001, which then can be routed in a +E.164 routing schema.

Figure 2-8 Example Dialing Normalization Translation Pattern



After applying the called party transformations defined on a translation pattern, Unified CM then executes a secondary lookup of the resulting digit string using the calling search space (CSS) defined on the translation pattern. Unified CM enables definition of translation patterns that use the originator's CSS for this secondary lookup. This allows definition of dialing normalization translation patterns that can be reused in multiple context, because after applying the dialing normalization, the secondary lookup of the normalized digit string is executed, not based on a single fixed CSS, but based on the CSS in effect when the translation pattern was engaged.

Tip On dialing normalization translation patterns, set the option **Use Originator's Calling Search Space** so that the CSS used for the secondary lookup is identical to the CSS used for the primary lookup.

Tip On dialing normalization translation patterns that are fixed length (they do not end with a variable length wildcard), also set the option **Do Not Wait For Interdigit Timeout On Subsequent Hops** so that even if the secondary lookup matches on a variable length route pattern, the call is still routed without inter-digit timeout.

Classes of Service and Calling Search Spaces (CSSs)

Partitions and CSSs are the fundamental components in Unified CM used to build classes of service. Dialable patterns are grouped into equivalence classes by putting patterns belonging to the same class into the same partition. Each CSS then is a list of partitions that defines which partitions and, thus, which patterns a calling entity using the CSS can access. A CSS effectively enforces class of service by determining which destinations can be reached from a device using this CSS.

The number of classes of service defined is the major factor driving dial plan complexity, and thus the number of required classes of service should be as small as possible. In a well designed enterprise dial plan, re-use of patterns and partitions for multiple classes of service helps to simplify the dial plan deployment.

Outbound Gateway Selection Using Local Route Group

Following the maxim to avoid and eliminate redundancies in the dial plan as much as possible, the concept of Local Route Groups (LRGs) is used to define the egress gateway selection.

Route patterns using a local route group offer a unique characteristic: they allow for dynamic selection of the egress gateway based on the device originating the call. By contrast, calls routed by route patterns using static route groups will route the call to the same gateway, no matter which device originated the call. Route patterns configured to refer to a route list that makes use of LRGs will resolve to the actual route group configured as the LRG in the calling party's device pool.

This allows for re-use of route patterns that are not specific to each site, instead of requiring you to provision site-specific route patterns that are directly associated with the egress gateway of the respective site.

Outbound Calls: Called and Calling Number Localization

The dial plan design presented in this document uses local route groups for egress gateway selection based on the calling device. Hence, calling and called party transformations required to adapt to service provider requirements cannot be done on the route pattern or route list level. These transformations would be shared among all gateways. Instead, these service provider specific transformations to localize calling and called party information are configured either on the gateway using Cisco IOS voice translation rules or on Unified CM using calling and called party transformation patterns addressed by calling and called party transformation CSSs configured on the gateway or on the gateway's device pool.

Inbound Calls: Called and Calling Number Globalization

Because all call routing on Unified CM is based on +E.164 numbers for all incoming calls arriving at Unified CM, we need to make sure that called party information is globalized to +E.164 from the format received on the link from the provider. This is achieved through a combination of Cisco IOS translations on the SIP gateways (required to avoid loss of number type information received from the ISDN network when sending the request to Unified CM over SIP) and prefixes and possibly calling and called number transforms configured on Unified CM.

User Provisioning with LDAP Synchronization

Synchronization of Unified CM with a corporate LDAP directory allows the administrator to provision users easily by mapping Unified CM data fields to directory attributes. Critical user data maintained in the LDAP store is copied into the appropriate corresponding fields in the Unified CM database on a scheduled basis. The corporate LDAP directory retains its status as the central repository. Unified CM has an integrated database for storing user data and a web interface within Unified CM Administration for creating and managing user accounts and data. When LDAP synchronization is enabled, the local Unified CM database is still used, and additional local end-user accounts can be created. Management of end-user accounts is then accomplished through the interface of the LDAP directory and Unified CM Administration.

User Authentication with LDAP

The LDAP authentication feature enables Unified CM to authenticate LDAP synchronized users against the corporate LDAP directory. Locally configured users are always authenticated against the local database. Also, PINs of all end users are always checked against the local database only.

To enable authentication, a single authentication agreement is defined for the entire cluster.

The following statements describe Unified CM's behavior when authentication is enabled:

- End user passwords of users imported from LDAP are authenticated against the corporate directory by a simple bind operation.
- End user passwords for local users are authenticated against the Unified CM database.
- Application user passwords are authenticated against the Unified CM database.
- End user PINs are authenticated against the Unified CM database.

In environments that employ a distributed Active Directory topology with multiple domain controllers geographically distributed, authentication speed might be unacceptable. When the Domain Controller for the authentication agreement does not contain a user account, a search must occur for that user across other domain controllers. If this configuration applies to your deployment, and login speed is unacceptable, it is possible to set the authentication configuration to use a Global Catalog Server.

An important restriction exists, however. A Global Catalog does not carry the employeeNumber attribute by default. In that case either use Domain Controllers for authentication (beware of the limitations listed above) or update the Global Catalog to include the employeeNumber attribute. Refer to Microsoft Active Directory documentation for details.

To enable queries against the Global Catalog, configure the LDAP Server Information in the LDAP Authentication page to point to the IP address or host name of a Domain Controller that has the Global Catalog role enabled, and configure the LDAP port as 3268.

Deployment Overview

Deployment begins with provisioning of the centralized Cisco Unified CM cluster followed by further configuration and provisioning tasks. The following sections describe how to set up and configure the call control according to the Preferred Architecture design in this document:

- DNS Requirements
- Provision the Cisco Unified CM and IM and Presence Service Cluster
- Cisco Unified CM and IM and Presence Service Certificate Management
- Initial Cisco Unified CM Configuration
- Other IM and Presence Settings
- Dial Plan Configuration
- LDAP System Configuration
- Cisco Unified CM Group Configuration
- Phone NTP References
- Date and Time Groups
- Media Resources
- Device Pools
- SIP Trunks
- Endpoint Provisioning
- ILS Configuration for Multi-Cluster Deployments
- GDPR Configuration (Multi-Cluster Only)
- Survivable Remote Site Telephony (SRST) Deployment
- Extension Mobility
- Busy Line Field (BLF) Presence
- Deploying Computer Telephony Integration (CTI)

DNS Requirements

Before deploying the solution, make sure DNS resolution is available for all servers to be deployed. Both forward (from DNS name to IP address) and reverse (from IP address to DNS name) lookups have to be configured in the enterprise DNS.

Also, the DNS resolver configured in Unified CM IM and Presence Service and in Unified CM call processing nodes must allow resolution of externally routable addresses. This is required for Push notifications via APNs.

In addition to enabling UDS-based service discovery for Jabber clients, provision DNS SRV records for all Unified CM publisher and TFTP subscriber nodes, defining these as service locations for _cisco-uds. Example 2-1 shows an example of DNS SRV records defining a number of Unified CM nodes as _cisco-uds service locations.

Example 2-1 DNS SRV Record for UDS-Based Service Discovery

```
_cisco-uds._tcp.ent-pa.com     SRV service location:
          priority       = 10
          weight         = 10
          port           = 8443
          srv hostname   = us-cm-pub.ent-pa.com
_cisco-uds._tcp.ent-pa.com     SRV service location:
          priority       = 10
          weight         = 10
          port           = 8443
          srv hostname   = us-cm-tftp1.ent-pa.com
_cisco-uds._tcp.ent-pa.com     SRV service location:
          priority       = 10
          weight         = 10
          port           = 8443
          srv hostname   = us-cm-tftp2.ent-pa.com
```

In Example 2-1, three Unified CM nodes (publisher and two TFTP subscriber nodes) are defined as service locations for UDS service discovery to make sure that the load of the initial UDS requests from Jabber clients making use of UDS service discovery are evenly distributed among all active Unified CM nodes.

As part of the UDS service discovery process, after locating the home cluster using the /cucm uds/clusterUser resource, Jabber clients will use the /cucm-uds/servers resource to get a list of all UDS nodes in the user's home cluster, so that the actual UDS requests during the registration process are load balanced between all UDS nodes of the cluster even if the SRV records defined only the publishers as service locations.

Provision the Cisco Unified CM and IM and Presence Service Cluster

To deploy the Unified CM and IM and Presence Service cluster, perform the following tasks:

1. Determine the number of required call processing subscriber pairs based on the target number of users and devices.
2. Determine the number of required IM and Presence nodes based on the target number of users.
3. Determine the network parameters (DNS names, IP addresses, and so forth) for all required cluster members. Make sure to consider the TFTP servers also.
4. Deploy the required number of virtual machines on your compute infrastructure using the appropriate Cisco provided OVA template files. For information on how to obtain these OVA files, refer to the documentation at

   https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-sizing.html
5. In Cisco Prime Collaboration Deployment, define the Unified CM cluster with all its members, and map the nodes to the virtual machines created in task 4.
6. Deploy all nodes using Cisco Prime Collaboration Deployment.

For more information on how to provision a cluster using Cisco Prime Collaboration Deployment, refer to the latest version of the *Cisco Prime Collaboration Deployment Administration Guide*, available at

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

Cisco Unified CM and IM and Presence Service Certificate Management

Follow the steps outlined in the section on Server Certificate Generation and Management in the Security chapter. Even if you are not planning to configure encryption on the endpoints, we recommend having an external CA sign the Tomcat certificates of Cisco Unified CM and IM and Presence Service and Cisco Unity Connection.

It is important to make sure that certificates issued by the CA have the required key usage and extended key usage. A typical problem is that the CA issuing the certificate based on the provided CSR does not simply issue a certificate with the key usage and extended key usage copied from the CSR, but instead sets the key usage and extended key usage of the issued certificate based on settings in a template selected for issuing the certificate. A certificate issued based on a typical Web Server template, for example, will not have the TLS Web Client Authentication extended key usage include. This creates problems with inter-server communications – for example, Intercluster Lookup Service (ILS) and User Data Store (UDS) – where the Tomcat certificate on the initiating side of the TLS connection is also used as a client certificate, and thus TLS connection setup fails due to the incorrect key usage (see the section Consider UDS Certificate Requirements).

Initial Cisco Unified CM Configuration

Immediately after installing the Unified CM cluster, perform the following basic configuration tasks:

- Node Name Configuration
- Enterprise Parameter Settings
- Service Activation
- Service Parameter Settings

Node Name Configuration

To allow for correct certificate validation and to ensure that references to Unified CM cluster members can always be resolved correctly, set the node names under System/Server in the Unified CM administration GUI to fully qualified domain names (FQDNs) for all cluster members. To achieve this, navigate to System/Server in the Cisco Unified CM administration GUI and verify that all servers show up in the first column as FQDNs. Change the entries of servers showing up as only a hostname without a DNS domain, to FQDNs.

Enterprise Parameter Settings

Check and update the Enterprise Parameters listed in Table 2-2.

Table 2-2 Enterprise Parameters

Enterprise Parameter	Description	Value
Cluster ID	Used to uniquely identify the Unified CM cluster in a number of intercluster features, including Intercluster Lookup Service (ILS) and intercluster call admission control	Example: USCluster
Auto Registration Phone Protocol	Signaling protocol provisioned for auto-registering phones	SIP

Table 2-2 Enterprise Parameters (continued)

Enterprise Parameter	Description	Value
BLF For Call Lists	Specifies whether call lists in phones supporting this feature should show presence	Enabled
URI Lookup Policy	According to RFC 3261, when determining SIP URI equivalence, the check on the left-hand side (user portion) of the URI has to be case-sensitive. The default behavior of Unified CM is to adhere to this standard, but to avoid potential issues with URIs using mixed capitalization, it is typically better to change the default.	Case Insensitive
Enable Dependency Records	Dependency records simplify the administration of Unified CM.	True
Auto select DN on any Partition	Simplifies administration. If enabled, the directory number configuration page automatically gets populated with the data of the first matching directory number.	True
CDR File Time Interval	Determines the time interval for call detail record (CDR) file updates	10
URL Authentication URL Directories URL Information URL Services Secured Authentication URL Secured Directory URL Secured Information URL Secured Services URL	URLs used by endpoints for various purposes	Make sure these URLs refer to the FQDN of the Unified CM publisher node
Organization Top Level Domain		Example: ent-pa.com
Cluster Fully Qualified Domain Name	When routing numeric SIP URIs, Unified CM considers SIP URIs with the right-hand side (host portion) of the URI matching the configured Cluster Fully Qualified Domain Name (CFQDN) as destinations to be routed according to the configured local numeric dial plan. If no match is found for the numeric left-hand side of the URI in the configured numeric dial plan, then Unified CM rejects the call. For more details, refer to the section on *Routing of SIP Requests in Unified CM* in the *Dial Plan* chapter of the latest version of the *Cisco Collaboration System SRND*.	Space-separated list of all Unified CM call processing nodes in the cluster. Example: us-cm-sub1.ent-pa.com us-cm-sub2.ent-pa.com
OAuth with Refresh Login Flow	This enables OAuth grant flow authentication. This is highly recommended for deployments using push notifications via APNs. OAuth grant flow authentication makes sure that a Jabber client receiving an incoming call APN can be brought to the foreground and re-authenticate quickly enough for the user to answer the incoming call in a timely manner. It is also required to enable encrypted media and signaling with Jabber, if no Locally Significant Certificate (LSC) is installed on Jabber.	Enabled

Service Activation

Table 2-3 summarizes the services to be activated on the Unified CM publisher node, the dedicated Unified CM TFTP server subscriber nodes, and the Unified CM call processing subscriber nodes.

Table 2-3 Unified CM Node Service Activation

Service	Publisher	Dedicated TFTP Subscriber	Call Processing Subscriber
CM Services			
Cisco CallManager			Yes
Cisco IP Voice Media Streaming App			Yes
Cisco CTIManager			Yes
Cisco Intercluster Lookup Service	Yes		
Cisco Location Bandwidth Manager			Yes
Cisco Dialed Number Analyzer Server	Yes		
Cisco Dialed Number Analyzer	Yes		
Cisco Tftp		Yes	
CTI Services			
Cisco WebDialer Web Service			Yes
Database and Admin Services			
Cisco Bulk Provisioning Service	Yes		
Cisco AXL Web Service	Yes		
Performance and Monitoring Services			
Cisco Serviceability Reporter	Yes		
Cisco CallManager SNMP Service	Yes	Yes	Yes
Security Services			
Cisco CTL Provider	Yes	Yes	Yes
Cisco Certificate Authority Proxy Function	Yes		
Directory Services			
Cisco DirSync	Yes		

Table 2-4 lists the services to be activated on Cisco Unified CM IM and Presence publisher and subscriber nodes.

Table 2-4 Unified CM IM and Presence Node Service Activation

Service	Publisher	Subscriber
Cisco AXL Web Service	Yes	Yes
Cisco Bulk Provisioning Service	Yes	
Cisco Serviceability Reporter	Yes	
Cisco SIP Proxy	Yes	Yes
Cisco Presence Engine	Yes	Yes
Cisco XCP Connection Manager	Yes	Yes
Cisco XCP Authentication Service	Yes	Yes

Service Parameter Settings

Some service parameters of the Cisco CallManager service are global in nature and need to be set only once in Unified CM Administration. The global service parameter settings for Cisco CallManager service are listed in Table 2-5.

Note Only non-default Service Parameter and other configuration field values are specified in this document. If a field configuration value is not mentioned, then the default value should be assumed.

Note Some of the service parameters listed are advanced service parameters.

Table 2-5 Global Service Parameters

Service Parameter	Value	Description
Call Diagnostics Enabled	Enable Only When CDR Enabled Flag is True	This parameter determines whether call management records (CMR), also called diagnostic records, are generated.
T302 Timer	5000	Whenever a destination is dialed digit-by-digit and based on the numeric dial plan provisioned in Unified CM, no immediate deterministic decision can be made about which provisioned pattern has to be considered for the dialed destination. Because a potential longer match (could be variable length) exists, the T302 inter-digit timeout has to expire before Unified CM selects the best route and routes the call. The default of 15,000 milliseconds (ms) typically is too long.
Apply Transformations On Remote Number	True	Makes sure that calling party transformations are also applied mid-call; for example, if a call is transferred from one party to another.
Max Forward UnRegistered Hops to DN	2	Limit CFUR loops from occurring, for example, if a phone is unregistered but the site's gateway still is registered with Unified CM.
Stop Routing on Q.931 Disconnect Cause Code	3 21 27 28 38 42 63	Allows Unified CM to stop hunting down the configured hunt list when receiving specific Q.850 cause codes.

Table 2-5 Global Service Parameters (continued)

Service Parameter	Value	Description
G.722 Codec Enabled	Enabled for All Devices Except Recording-Enabled Devices	G.722 disabled on recording-enabled devices to avoid problems with G.722 not being supported by the recorder.
Automated Alternate Routing Enable	True	This service parameter globally enables automated alternate routing (AAR).

Other service parameters of the Cisco CallManager service must be set explicitly as shown in Table 2-6 for each Unified CM call processing node.

Table 2-6 Per-Node Service Parameters

Service Parameter	Value	Description
CDR Enabled Flag	True	This parameter enables the generation of call detail records (CDR).
CDR Log Calls with Zero Duration Flag	True	This parameter enables or disables the logging of call detail records (CDRs) for calls that never connected or that lasted less than 1 second.
Digit Analysis Complexity	TranslationAndAlternatePatternAnalysis	This parameter specifies the amount of digit analysis information that CCM trace files will provide.

Onboarding for Push Notifications via Apple Push Notification Service (APNs)

Follow the *Push Notifications Configuration Task Flow* described in the latest version of the document on *Push Notifications Deployment for Cisco Jabber on iPhone and iPad with Cisco Unified Communications Manager*, available at

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

In summary the following steps are required for the onboarding:

- Smart License Registration
  - Register the Unified CM cluster on the license management page
- Voucher generation
  - In **Advanced Features** > **Cisco Cloud Onboarding** click **Generate Voucher**
- Onboarding
  - In **Advanced Features** > **Cisco Cloud Onboarding**

    Select **Enable Push Notifications**.

    Select **Send Troubleshooting information to the Cisco Cloud**.

    Select **I want Cisco to manage the Cisco Cloud Service CA Certificates required for this trust**.

    Select **Enable HTTP Proxy** and enter Proxy details if the connectivity requirements in Table 2-7 require the use of a forward proxy.

    Click **Save**.

- Restart the **XCP Router Service** on Unified CM IM and Presence nodes
  - After successfully onboarding the cluster, you must restart the XCP Router Service on all Unified CM IM and Presence nodes in the cluster. We recommend restarting the service during a maintenance window.

Table 2-7 summarizes the connectivity requirements for the various Unified CM nodes. If direct access is not possible due to existing networking policies, then access to the destinations in Table 2-7 must be enabled through a forward proxy.

Table 2-7 Cloud Connectivity Requirements for Push Notifications via APNs

From	To	Port	Usage
Unified CM Publisher	Cisco cloud	443/TCP	The Unified CM publisher during the onboarding process needs access to the onboarding service hosted at **fos-a.wbx2.com**.
Unified CM IM and Presence and call processing	Cisco cloud	443/TCP	All call processing subscribers and IM and Presence nodes need access to the Common Identity service at **idbroker.webex.com** to obtain OAuth access tokens. Also, they need to be able to access the Push REST service at **push.webexconnect.com**.

Other IM and Presence Settings

Previous sections discussed the IM and Presence service activation, certificates management, and the IM and Presence SIP trunk configuration. In addition to that, configure settings on IM and Presence servers:

- Configure a Unified CM domain in the **IM&P Cisco SIP Proxy** Service Parameter.
- In **Cisco Unified CM IM and Presence Administration** > **Presence** > **Settings** > **Standard Configuration**:
  - Configure a Cluster ID value.
  - Enable availability sharing. If not enabled, users can view only their own availability status.
  - Check **Enable ad-hoc presence subscriptions** to turn on ad-hoc presence subscriptions for Cisco Jabber users.
- In **Cisco Unified CM IM and Presence Administration** > **Presence** > **Routing** > **Settings**:
  - Configure **Proxy Server Settings**: **Enable Method/Event Routing Status**
- In **Cisco Unified CM IM and Presence Administration** > **Messaging** > **Settings**:
  - Enable instant messaging.
- Enable OAuth grant flow authentication.
  - Set the Enterprise parameter **OAuth with Refresh Login Flow** to **Enabled**.
- Enable Multi Device Messaging.
  - In Cisco Unified CM IM and Presence Administration, choose **System** > **Service Parameters**.
  - From the **Server** drop-down list, choose the IM and Presence Service Publisher node.
  - From the **Service** drop-down list, choose **Cisco XCP Router (Active)**.
  - From the **Enable Multi-Device Messaging** drop-down list, choose **Enabled**.
  - Click **Save**.

- Enable Push Notifications High Availability.
  - In Cisco Unified CM IM and Presence Administration, choose **System** > **Service Parameters**.
  - From the **Server** drop-down list, choose the IM and Presence Service Publisher node.
  - From the **Service** drop-down list, choose **Cisco XCP Router (Active)**.
  - From the **Push Notifications High Availability** drop-down list, choose **Enabled**.
  - Click **Save**.
- Restart the XCP Router Service.
  - Changing the two service parameters to enable Multi Device Messaging and Push Notifications High Availability requires you to restart the **Cisco XCP Router** service on all Unified CM IM and Presence nodes during a maintenance window.

Also configure UC services for Jabber clients, as described in the section on Jabber Provisioning.

Dial Plan Configuration

A structured, well-designed dial plan is essential to successful deployment of any call control system. The design of an enterprise dial plan needs to cover these main areas:

- Endpoint addressing
- General numbering plan
- Dialing habits
- Routing
- Classes of service

The recommended dial plan design follows the design approach documented in the *Dial Plan* chapter of the latest version of the *Cisco Collaboration System SRND*.

Example Topology

For the purpose of this document, we assume a centralized call processing deployment serving three sites in the US: SJC, RCD, and RTP. Table 2-8 provides the DID (direct inward dial) ranges for these sites.

Table 2-8 DID Ranges for Example Sites

Site	DID range
SJC	+1 408 555 4XXX
RCD	+1 972 555 5XXX
RTP	+1 919 555 1XXX

Endpoint Addressing

For endpoints with DID addresses, directory numbers are provisioned as full +E.164 numbers, where +E.164 represents a leading "+" followed by the full global E.164 phone number. To provision a +E.164 directory number in Unified CM, the leading "+" has to be escaped; for example, extension 4001 in SJC would have to be provisioned as \+14085554001.

Some endpoints will not have DIDs because not enough DIDs are available from the provider or because the associated devices do not need to be reachable from the PSTN (for example, lobby phones). For these endpoints no DIDs (E.164 numbers) exist, and thus an address format other than +E.164 is required for these endpoints. This address format is discussed in the section on General Numbering Plan.

Addressing Enterprise Services for External Access

Some services have assigned PSTN numbers. An example of this might be a voicemail pilot number that has to be reachable from the outside to enable users to call into voicemail from the PSTN. PSTN E.164 numbers for these services have to be reserved from the DID ranges assigned by the PSTN providers.

General Numbering Plan

In addition to endpoints with associated DIDs for which +E.164 addresses can be used, a number of additional destinations exist for which no DIDs exist:

- Lobby phones
- Regular endpoints for which no DIDs could be assigned by the provider
- Services (call pickup numbers, call park numbers, conferences, and so forth)

In this document we refer to these types of destinations as *non-DIDs*.

Addresses for these non-DIDs, similar to +E.164 addresses, must be unique system-wide to avoid site-specific partitions for non-DIDs. The recommended solution is to introduce an enterprise specific numbering (ESN) schema for all non-DIDs. This ESN schema follows the structure of typical abbreviated inter-site dialing:

- Access-code

  A single-digit access code for abbreviated inter-site dialing. In the design phase, choose the access code so that there is no overlap with any other enterprise dialing habit (see below).

- Site-code

  A digit sequence uniquely identifying a site in the network. In the design phase, choose the length of the site code so that it not only covers all existing sites, but also allows for growth.

- Extension

  A digit sequence uniquely identifying the respective entity within the site.

In this document we use 8 as the access-code for abbreviated inter-site dialing, and thus all ESNs start with 8 and use a three-digit site code and a four-digit extension. Table 2-9 indicates an ESN range for the DID and non-DID numbers for each site in our example.

Table 2-9 ESN Ranges for DIDs and Non-DIDs

Site	+E.164 Range	Site Code	ESN Range for DIDs	ESN Range for Non-DIDs
SJC	+1 408 555 4XXX	140	8-140-4XXX	8-140-5XXX
RCD	+1 972 555 5XXX	197	8-197-5XXX	8-197-6XXX
RTP	+1 919 555 1XXX	191	8-191-1XXX	8-191-2XXX

The plan is to use the same site code for DIDs and non-DIDs, but the first digit of the extension for non-DIDs is different from the first digit of the DID extensions. This also allows for abbreviated four-digit intra-site dialing to non-DIDs and DIDs.

While the ESN ranges in Table 2-9 leave room in the ESN plan for site-specific numbers, there is also a requirement to assign number ranges for non-site-specific services such as, for example, scheduled conferences. Table 2-10 shows an example of how this requirement can be addressed by reserving a dedicated site code (in this case 099).

Table 2-10 ESN Ranges for Conferences

ESN Range	Usage
8099[12]XXX	Scheduled conferences

Dialing Habits

Dialing habits describe what end users must dial to reach various types of destinations. Dialing habits can first be classified as numeric dialing (for example, 914085550123) or alphanumeric dialing (for example, bob@ent-pa.com).

In this design, in addition to alpha URI dialing, the numeric dialing habits shown in Table 2-11 are supported.

Table 2-11 Supported Numeric Dialing Habits

Dialed Pattern	Example (site SJC)	Type of Destination
XXXX	4001 (DID) 5001 (non-DID)	Abbreviated intra-site dialing to reach a destination at the same site. The called destination can be a DID, a non-DID, or a service number.
+E.164	+14085554001 (on-net, SJC) +19195551001 (on-net, RTP) +1212551001 (off-net)	Full +E.164 dialing for example from directories. The dialed destination can be on-net or off-net. The implemented dial plan makes sure that calls to on-net destinations dialed as +E.164 are routed on-net. Non-DIDs obviously cannot be called as +E.164.
Access code–site code–extension	8-140-4001 (DID, SJC) 8-140-5001 (non-DID, SJC) 8-191-1001 (DID, RTP) 8-191-2001 (non-DID, RTP)	Abbreviated inter-site dialing to reach a destination at the same site or a different site. The called destination can be a DID, a non-DID, or a service number. The access code (8 in the example) has to be selected so that it does not overlap with any other dialing habit; for example any abbreviated intra-site dialing: access code 8 for inter-site dialing prohibits four digit intra-site dialing starting with 8.
*E.164	*12125551567	Dialing of a video call through dedicated video ISDN gateways. The * is used to create a specific dialing habit with no overlap to any other numeric(!) dialing habit. To avoid the use of * also a number area starting with the abbreviated inter-site access code 8 can be used: for example 8000-<E.164>.

Table 2-11 Supported Numeric Dialing Habits (continued)

Dialed Pattern	Example (site SJC)	Type of Destination
91-<10 digits>	914085554001 (on-net, SJC) 919195551001 (on-net, RTP) 912125551001 (off-net)	US specific habitual PSTN dialing of national destinations. The implemented dial plan ensures that if the dialed destination is on-net then the call is routed on-net. The leading 9 here is the PSTN access code typically used in the US.
9011-<E.164 number>	90114961007739764	US specific habitual PSTN dialing of international destinations. The implemented dial plan makes sure that if the dialed destination is on-net then the call is routed on-net.

In general, using fewer supported dialing habits simplifies the design. Starting the design process with an overview of all dialing habits makes sure that overlaps between any two dialing habits leading to inter-digit timeouts are detected and can be resolved before starting the dial plan deployment. Avoiding overlaps with any other (typically on-net) dialing habit is the key reason for using a PSTN access code (typically 9 in the US, as shown above).

Partitions

When defining the partitions and CSSs provisioned to build an enterprise dial plan, one goal is to avoid replication of duplicate configuration as much as possible. Following this maxim, Table 2-12 shows the global (that is, not site or country specific) partitions required.

Table 2-12 Global Partitions

Partition	Description
DN	Holds all +E.164 directory numbers and other local on-net +E.164 destinations (for example, pilot numbers reachable from the PSTN). All +E.164 patterns are provisioned as urgent patterns.
ESN	Holds all Enterprise Specific Numbers (ESNs). This includes ESN directory numbers (for example, for non-DID phones) as well as dialing normalization translation patterns transforming from abbreviated inter-site dialing of DIDs to +E.164.
PSTNInternational	Holds +E.164 route patterns required to provide PSTN access to international destinations.
URI	Holds manually provisioned URIs.
onNetRemote	Holds all patterns of remote on-net destinations. In environments with multiple Unified CM clusters, this includes all remote number ranges learned via Global Dial Plan Replication (GDPR).
B2B_URI	Holds SIP route patterns required for business-to-business (B2B) URI dialing through the Internet.
Directory URI	System Partition where all auto-generated URIs are put. This partition does not need to be created. It is listed here for reference to introduce the partition, which is used again later in this document.

All of the partitions Table 2-12 except the Directory URI partition must be created. In addition to the pattern classes represented by these global partitions, several site, country, or class-of-service specific pattern classes are required, as show in Table 2-13.

Table 2-13 Country or Site Specific Partitions

Partition	Description
USPSTNNational	Holds +E.164 route patterns required to provide PSTN access to national destinations in the US. To support other countries, and thus other country-specific dialing habits, a country appropriate xxPSTNNational partition (where xx represents the country; for example, DEPSTNNational, UKPSTNNational, ITPSTNNational) also needs to be provisioned, which then holds the +E.164 route patterns required to provide PSTN access to national destinations of that country. The reason we differentiate between international PSTN access (see Table 2-12) and national PSTN access is that we need to be able to build differentiated classes of service allowing calls to reach national only, or national and international destinations.
USToE164	Holds dialing normalization translation patterns to transform US specific habitual PSTN dialing (for example, 91-<*10 digits*>) to +E.164. To support other countries, and thus other country-specific dialing habits, a country appropriate xxToE164 partition (where xx represents the country; for example, DEToE164, UKToE164, ITToE164) also needs to be provisioned, which then holds the dialing normalization translation patterns required to transform the country specific habitual PSTN dialing to +E.164.
USEmergency	Holds route patterns required to provide access to emergency calls using the US specific emergency dialing habits.
USPhLocalize	Holds calling party transformation patterns to localize +E.164 calling party numbers for abbreviated display on phones in the US.
<site>Intra	Site-specific intra-site dialing. For example: SJCIntra. Holds dialing normalization patterns to transform site-specific abbreviated intra-site dialing to DIDs, or non-DIDs to +E164 or ESN, respectively.
<site>PhLocalize	Site-specific. For example: SJCPhLocalize. Holds calling party transformation patterns to localize +E.164 calling party numbers for abbreviated display on phones in a given site.

As emergency calls are placed using country specific dialing habits, partition USEmergency with the route patterns enabling the US dialing habit for emergency calls also is country specific. To also support other dialing domains (countries), the equivalent partitions for these other dialing domains (for example, DEEmergency, ITEmergency, DEPhLocalize, ITPHLocalize, for Germany and Italy respectively) would need to be created.

Dialing Normalization Translation Patterns

Table 2-14 summarizes which dialing normalization translation patterns need to be provisioned using the partitions from the previous section. All dialing normalization translation patterns are provisioned as urgent patterns and have **Use Originator's Calling Search Space** set as described in section on Partitions so that, after applying the called party transformation defined in the dialing normalization translation pattern, the original CSS is used to find the final match for the dialed destination.

Table 2-14 Summary of Dialing Normalization Translation Patterns

Partition	Pattern	Called Party Transformation Mask	Note
ESN	81404XXX	+14085554XXX	Abbreviated inter-site dialing to site SJC
ESN	81975XXX	+19725555XXX	Abbreviated inter-site dialing to site RCD
ESN	81911XXX	+19195551XXX	Abbreviated inter-site dialing to site RTP
SJCIntra	4XXX	+14085554XXX	Abbreviated intra-site dialing in site SJC to DID in SJC
SJCIntra	5XXX	81405XXX	Abbreviated intra-site dialing in site SJC to non-DID in SJC
RCDIntra	5XXX	+19725554XXX	Abbreviated intra-site dialing in site RCD to DID in RCD
RCDIntra	6XXX	81976XXX	Abbreviated intra-site dialing in site RCD to non-DID in RCD
RTPIntra	1XXX	+19195551XXX	Abbreviated intra-site dialing in site RTP to DID in RTP
RTPIntra	2XXX	81912XXX	Abbreviated intra-site dialing in site RTP to non-DID in RTP
UStoE164	9.1[2-9]XX[2-9]XXXXXX	No Mask, strip pre-dot, prefix +	US specific habitual PSTN dialing to national destinations in the US
UStoE164	9011.!#	No Mask, strip pre-dot, prefix +	US specific habitual PSTN dialing to national destinations in the US.
UStoE164	9011.!	No Mask, strip pre-dot, prefix +	US specific habitual PSTN dialing to national destinations in the US **Note** This is the only pattern for which **Do Not Wait For Interdigit Timeout On Subsequent Hops** is not set.

For dialing domains other than the US, other country specific dialing normalization translation patterns must be defined if the installation has to support those country specific dialing habits. Table 2-15 shows the required dialing normalization for Germany (DE) and Italy (IT) as examples.

Table 2-15 Dialing Normalization for Germany and Italy

Partition	Pattern	Called Party Transformation	Note
DEtoE164	000.!	strip pre-dot, prefix +	Germany: international call (000-E.164). **Note** **Do Not Wait For Interdigit Timeout On Subsequent Hops** is not set.
DEtoE164	000.!#	strip pre-dot trailing #, prefix +	Germany: international call (000-E.164).
DEtoE164	00.[^0]!	strip pre-dot, prefix +49	Germany: national call (00-national significant number). **Note** The numbering plan in Germany is variable length and this pattern needs to cover this. **Note** **Do Not Wait For Interdigit Timeout On Subsequent Hops** is not set.
DEtoE164	00.[^0]!#	strip pre-dot trailing #, prefix +49	Germany: national call (00-national significant number).
ITtoE164	000.!	strip pre-dot, prefix +	Italy: international call (000-E.164). **Note** **Do Not Wait For Interdigit Timeout On Subsequent Hops** is not set.
ITtoE164	000.!#	strip pre-dot trailing #, prefix +	Italy: international call (000-E.164)
ITtoE164	0.0[^0]!	strip pre-dot, prefix +39	Italy: national call (0-national significant number (NSN) where NSN starts with 0). **Note** The numbering plan in Italy is variable length and this pattern needs to cover this. **Note** **Do Not Wait For Interdigit Timeout On Subsequent Hops** is not set.
ITtoE164	0.0[^0]!#	strip pre-dot trailing #, prefix +39	Italy: national call (0-NSN where NSN starts with 0).
ITtoE164	0.[^0]!	strip pre-dot, prefix +39	Italy: national call (0-NSN where NSN does not start with 0). **Note** The numbering plan in Italy is variable length and this pattern needs to cover this. **Note** **Do Not Wait For Interdigit Timeout On Subsequent Hops** is not set.
ITtoE164	0.[^0]!#	strip pre-dot trailing #, prefix +39	Italy: national call (0-NSN where NSN does not start with 0).

The example in Table 2-15 shows that in Italy and Germany the ITU recommended 0 is used to access a trunk from inside the enterprise, and then 0 and 00 are used for national and international access. Since 1998, geographic numbers in Italy start with 0, and digits 1 to 9 as the first digit of a national significant number indicate different types of numbers. Hence, dial strings starting with exactly two 0s (00) need to be treated differently in Italy than in Germany. In Italy the second zero has to be considered part of the NSN and hence has to be kept in the resulting +E.164 digit string, while a second zero in Germany would need to be removed because geographic numbers in Germany do not start with a zero.

The example of the dialing normalization required for these two countries shows how country specific dialing habits can be modeled in the design approach presented.

For more information on international numbering plans, see the *International Numbering Resources* page of the ITU-T at https://www.itu.int/en/ITU-T/inr/Pages/default.aspx. There you can find links to various resources, including E.164 country codes and national numbering plans. An overview of dialing procedures used in various countries can be found in *Operational Bulletin No.994 (15.XII.2011) and Annexed List: Dialling procedures (international prefix, national (trunk) prefix and national (significant) number) (in accordance with ITU-T Recommendation E.164 (11/2010)) (Position on 15 December 2011)*, available at https://www.itu.int/pub/T-SP-OB.994-2011. The actual list of dialing procedures starts at page 25 of that document and is also available for download at https://www.itu.int/dms_pub/itu-t/opb/sp/T-SP-E.164C-2011-PDF-E.pdf.

Classes of Service and Calling Search Spaces (CSSs)

As mentioned before, a CSS is a list of partitions that defines which partitions, and thus patterns, a calling entity using the CSS can access. In this document we use a dial plan approach that uses only the line CSS to define class of service.

Table 2-16 lists the classes of service considered in this design. The classes of service chosen for this design are only examples. If further classes of services are required, then these can be defined equivalently.

Tip The number of classes of service is one of the key parameters driving the complexity of enterprise dial plan designs. Therefore, it is good practice to define as few classes of service as possible for the dial plan.

The recommended design makes use of only the CSS provisioned on the line and does not use the device CSS to define class of service. The device CSS can be used to implement general dialing habits that need to be available for everyone. An example for this is emergency calling; see the section on Emergency Call Considerations in Multi-National Environments for more details on when to use the device CSS to implement emergency calls.

Table 2-16 Classes of Service

Class of Service	Access to
International	All on-net destinations
	National PSTN destinations
	International PSTN destinations
	Business-to-business URI dialing
	Emergency calls
National	All on-net destinations
	National PSTN destinations
	Emergency calls
Internal	All on-net destinations
	Emergency calls

Adding business-to-business URI dialing to only the International class of service is an example based on the assumption that business-to-business (B2B) calls consume limited edge resources. Also we are trying to avoid increasing the number of classes of service by a factor of two by introducing classes of service International, InternationalB2B, National, NationalB2B, Internal, and InternalB2B.

Because only the line CSS is used to define both class of service and the set of dialing habits available to a given caller, a CSS needs to be provisioned per site and class of service.

Table 2-17 shows how class of service International for a user in site SJC would be defined based on the partition set previously defined (see Table 2-12 and Table 2-13).

Table 2-17 Class of Service International for SJC User

CSS Name	Partitions
SJCInternational	DN Directory URI URI ESN onNetRemote SJCIntra UStoE164 USPSTNNational PSTNInternational B2B_URI USEmergency

As depicted in Table 2-18, the remaining classes of service are created equivalently by selectively removing access to B2B URI dialing, international, and national PSTN destinations.

Table 2-18 Classes of Service National and Internal for SJC User

CSS Name	Partitions
SJCNational	DN Directory URI URI ESN onNetRemote SJCIntra UStoE164 USPSTNNational USEmergency

CSS Name	Partitions
SJCInternal	DN Directory URI URI ESN onNetRemote SJCIntra UStoE164 USEmergency

CSSs for classes of services for users in other sites are created equivalent to the above CSSs, with the only difference being a different partition used with the site-specific dialing normalization patterns. Table 2-19 shows an example of the RTP site National and Internal classes of service.

Table 2-19 Classes of Service National and Internal for RTP User

CSS Name	Partitions
RTPNational	DN Directory URI URI ESN onNetRemote RTPIntra UStoE164 USPSTNNational USEmergency

CSS Name	Partitions
RTPInternal	DN Directory URI URI ESN onNetRemote RTPIntra UStoE164 USEmergency

These examples clearly show that the chosen partition scheme allows for optimal reuse of patterns and partitions when creating CSSs to implement classes of service for multiple sites.

For sites in other dialing domains (countries), the same CSS and partition schema as shown above can be used, with the only difference being that the dialing normalization partition for the specific dialing domain and the partition with the country specific route to national PSTN destinations would be used instead of the US partitions used above. For example, Table 2-20 shows the CSS for class of service International for a site FRA in Germany (DE).

Table 2-20 Class of Service International for Users in site FRA in Germany (DE)

CSS Name	Partitions
FRAInternational	DN Directory URI URI ESN onNetRemote FRAIntra DEtoE164 DEPSTNNational PSTNInternational B2B_URI DEEmergency

Special CSSs

In addition to classes of service for users, calling search spaces (CSSs) also are used to define classes of service for applications connected through trunks, such as Cisco Unity Connection, for example. Assuming that Unity Connection should have access only to on-net destinations and that, in addition to ESN and +E.164 dialing, also US dialing habits should be supported from Unity Connection, Table 2-21 shows the CSS to implement this class of service.

Table 2-21 Class of Service for Voicemail

CSS Name	Partitions
VoiceMail	DN ESN URI onNetRemote Directory URI UStoE164

In scenarios where Cisco Unity Connection needs to serve multiple countries, then implementing the country specific dialing normalization as defined in partition UStoE164 in the above example is not an option. The only dialing habits that can be supported in that case are the globally significant dialing habits ESN and +E.164.

To use Unified CM presence, a subscribe CSS has to be provisioned, among other things, to allow access to all presentities that a presence user subscribes to. To allow for a very simple provisioning of Unified CM presence without further differentiation of presence access, a single CSS needs to be provisioned that allows access to all possible on-net destinations. Table 2-22 shows the settings for this default subscribe CSS.

Table 2-22 Default Subscribe CSS

CSS Name	Partitions
DefaultSubscribe	DN ESN URI onNetRemote Directory URI

This subscribe CSS ensures access to all types of on-net destinations.

Table 2-23 shows the (trivial) CSS "DN" to be used as the incoming CSS on PSTN trunks. To avoid loops, a PSTN trunk can address only +E.164 directory numbers. A PSTN trunk would not need access to ESN patterns, dialing normalization patterns, or URIs because only a single number format is supported by the PSTN, and this is normalized to +E.164 on ingress.

Table 2-23 Inbound CSS for PSTN Gateways

CSS Name	Partitions
DN	DN

Table 2-24 shows the CSS ICTInbound to be used as an incoming CSS on trunks to other Unified CM clusters. To avoid loops, the incoming CSS on these intercluster trunks should not provide access to remote on-net destinations (partition onNetRemote), but the trunks (inbound CSS) need to support all valid on-net addressing modes (+E.164, ESN, and URIs). Dialing normalization is not part of this CSS because dialing habits other than +E.164 and ESN would already have been normalized to +E.164 or ESN on the remote Unified CM cluster prior to landing on the incoming intercluster trunk.

Table 2-24 Inbound CSS for Trunks to Other Unified CM Clusters

CSS Name	Partitions
ICTInbound	DN ESN URI Directory URI

Local Route Groups for Call Type Specific Outbound Gateway Selection

To allow for flexible egress gateway selection based on the calling device, we recommend using local route groups (LRGs). Using LRGs for egress gateway selection avoids the need for site-specific route patterns.

To allow for differentiated LRG selection for different call types, set up multiple LRG names as shown in Table 2-25.

Table 2-25 Local Route Group Names

Local Route Group Name	Description
LRG_PSTN_1	Local route group referring to primary PSTN resources to be used for PSTN calls
LRG_PSTN_2	Local route group referring to secondary PSTN resources to be used for PSTN calls
LRG_VIDEO_1	Local route group referring to primary PSTN resources to be used for video PSTN calls
LRG_VIDEO_2	Local route group referring to secondary PSTN resources to be used for video PSTN calls
LRG_Emergency_1	Local route group referring to primary PSTN resources to be used for emergency calls
LRG_Emergency_2	Local route group referring to secondary PSTN resources to be used for emergency calls

With these LRG definitions, dedicated route lists can be created for both "normal" PSTN calls and emergency calls so that different PSTN resources (gateways) are used for emergency calls than for normal PSTN calls. This makes sense in scenarios where centralized PSTN resources are provisioned for normal PSTN calls, but emergency calls should still use dedicated small gateways local to the site to allow for local emergency call routing to the correct Public Safety Answering Point (PSAP).

The video LRGs are provisioned for video-enabled ISDN gateways and treat them as separate resources.

Route Lists Using Local Route Groups

Using the LRGs as defined in the previous section, route lists should be created as depicted in Table 2-26.

Table 2-26 Route List Definitions

Route List	Members	Description
RL_PSTN	LRG_PSTN_1 LRG_PSTN_1 Standard Local Route Group	Normal PSTN calls should make use of the primary and secondary site-specific PSTN resources defined for normal PSTN calls. The last member, Standard Local Route Group, allows for fallback to PSTN resources not specific to a call type.
RL_Emergency	LRG_Emergency_1 LRG_Emergency_2 LRG_PSTN_1 LRG_PSTN_1 Standard Local Route Group	For emergency calls, the first call-specific resources for emergency calls should be used, then the second, then the PSTN resources defined for normal PSTN calls, and lastly the non-specific PSTN resources.
RL_VIDEO	LRG_VIDEO_1 LRG_VIDEO_2 LRG_PSTN_1 LRG_PSTN_2 Standard Local Route Group	For video calls, first the video-specific gateway resources are used, then the regular PSTN resources are considered as a fallback (audio only), and lastly the Standard Local Route Group is used if the others fail.

With the above LRG and route list definition on each device pool, up to seven route groups can be selected for the defined LRGs to allow for very specific outbound gateway selection. The actual PSTN resources to be used for certain call types are defined during device pool provisioning. If selecting different outbound PSTN resources based on call type is not required for a given set of devices, and only a single PSTN resource is needed for all call types, then it is sufficient to define only an actual route group for the Standard Local Route Group on the respective device pool and leave all other LRGs in that device pool set to **<None>**. Having **Standard Local Route Group** as the last entry in all route lists is a good way to achieve this.

Route Patterns for PSTN Access and Emergency Calls

PSTN access is achieved through PSTN route patterns. As described in the section about Classes of Service and Calling Search Spaces (CSSs), the route to international destinations needs to be provisioned in the PSTNInternational partition, while national PSTN routes are provisioned in the dialing domain specific partitions xxPSTNNational (where xx represents dialing domain USPSTNNational, for example). Table 2-27 shows the configured PSTN route patterns.

Table 2-27 PSTN Route Patterns

Pattern	Partition	Gateway or Route List	Description
\+!	PSTNInternational	RL_PSTN	Variable length to allow for dialing of arbitrary international destinations.
\+!#	PSTNInternational	RL_PSTN	Alternative pattern for international destinations to allow terminating variable length dialing with #. Discard Digits set to **Trailing-#**
\+1[2-9]XX[2-9]XXXXXX	USPSTNNational	RL_PSTN	Explicit pattern for national destinations in the US. **Urgent Priority** checked to avoid overlap with variable length PSTN route pattern \+! defined for international destinations.
911	USEmergency	RL_Emergency	US emergency calling **Urgent Priority** checked
9911	USEmergency	RL_Emergency	US emergency calling **Urgent Priority** checked

Apart from the route pattern settings explicitly shown in Table 2-27, all other settings are left with default values as shown in Table 2-28. This especially includes the calling, connected, and called party transformations, which are left empty (apart from stripping a trailing # as mentioned above) because the calling and called party transformations required to match the PSTN requirements are configured as explicit calling and called party transformations. This is described in the sections on Outbound Calls: Called and Calling Number Transformations on ISDN Gateways and Outbound Calls: Called and Calling Number Transformations on SIP Trunks.

Table 2-28 Route Pattern Default Settings

Setting	Value
Pattern Definition	
Numbering Plan	-- Not Selected --
Route Filter	<None>
MLPP Precedence	Default
Apply Call Blocking Percentage	Unchecked
Resource Priority Namespace Network Domain	<None>
Route Class	Default
Route Option	Route this pattern
Call Classification	OffNet
External Call Control Profile	<None>
Allow Device Override	Unchecked
Provide Outside Dial Tone	Checked
Allow Overlap Sending	Unchecked

Table 2-28 Route Pattern Default Settings (continued)

Setting	Value
Require Forced Authorization Code	Unchecked
Authorization Level	0
Require Client Matter Code	Unchecked
Calling Party Transformations	
Use Calling Party's External Phone Number Mask	Unchecked
Calling Party Transform Mask	Leave empty; do not enter any value
Prefix Digits (Outgoing Calls)	Leave empty; do not enter any value
Calling Line ID Presentation	Default
Calling Name Presentation	Default
Calling Party Number Type	Cisco CallManager
Calling Party Numbering Plan	Cisco CallManager
Connected Party Transformations	
Connected Line ID Presentation	Default
Connected Name Presentation	Default
Called Party Transformations	
Discard Digits	<None>
Called Party Transform Mask	Leave empty; do not enter any value
Prefix Digits (Outgoing Calls)	Leave empty; do not enter any value
Called Party Number Type	Cisco CallManager
Called Party Numbering Plan	Cisco CallManager
ISDN Network-Specific Facilities Information Element	
Network Service Protocol	-- Not Selected --
Carrier Identification Code	Leave empty; do not enter any value
Network Service	-- Not Selected --

While the international PSTN route patterns in partition PSTNInternational are not dialing domain (country) specific, the route patterns in partitions USPSTNNational and USEmergency are country specific. If the dial plan needs to support other countries, then the route patterns for these countries need to be created as shown in Table 2-29.

Table 2-29 Non-US Route Patterns for National Destinations

Pattern	Partition	Gateway or Route List	Description
\+49!	DEPSTNNational	RL_PSTN	Variable length because the German numbering plan with country code 49 is variable length.
\+49!#	DEPSTNNational	RL_PSTN	Alternative pattern for national destinations to allow terminating variable length dialing with #. Discard Digits set to **Trailing-#**
\+33XXXXXXXXX	FRPSTNNational	RL_PSTN	Explicit pattern for national destinations in France. **Urgent Priority** checked to avoid overlap with variable length PSTN route pattern \+! defined for international destinations.
112	DEEmergency	RL_Emergency	German emergency calling **Urgent Priority** checked
0112	DEEmergency	RL_Emergency	German emergency calling **Urgent Priority** checked
112	FREmergency	RL_Emergency	French emergency calling **Urgent Priority** checked
0112	FREmergency	RL_Emergency	French emergency calling **Urgent Priority** checked

Table 2-29 shows the difference between fixed and variable length numbering plans. The national numbering plan in Germany is variable length and thus the route pattern to match on national destinations in Germany has to match on variable length digit strings, and we also need to provision an alternate route pattern ending on # to enable users to explicitly terminate dial strings with # to avoid inter-digit timeouts when dialing national destinations. In contrast to this, the national numbering plan in France is fixed length (as in the US), and thus a single urgent fixed-length route pattern is enough to cover all national numbers in France.

Because Germany and France use the same emergency dialing habit, the emergency routing can be simplified by combining both emergency partitions DEEmergency and FREmergency into a single partition 112Emergency and by using that partition instead in the CSS definitions.

Emergency Call Considerations in Multi-National Environments

Independent from individual classes of service, access to emergency numbers is required from all endpoints at all times. As shown previously, this is easily achieved by adding the partition with the emergency calling route patterns to all CSSs. This approach is problematic if multiple countries need to be supported, those countries require different emergency dialing habits, and mobility features such as extension mobility and device mobility are used.

In this case, if a user roams between countries with different emergency dialing habits, then the device this user is using inherits the emergency dialing habits specific to the visiting user. For example, if a user from Germany logs into a phone in the US, then the line CSS as defined on the German user's extension

mobility profile gets assigned to the visited phone in the US, so that on this phone emergency calls now need to be placed using the German emergency calling dialing 112, and the US emergency call dialing habit 911 is not supported any longer.

To make sure that phones in a given country always support the national emergency call dialing habit independent of whether a foreign user logged into the phone, a different approach for emergency calls can be implemented. Instead of adding the USEmergency to all CSSs, create a dedicated USEmergency CSS and assign that CSS as the device CSS on all devices in the US. Then if a foreign user logs into a phone in the US, the visiting user's "home" dialing habits as defined by the line CSS will be combined with the visited countries emergency dialing habit. In the above case of a German user logging into a US phone, that user's German PSTN dialing habits will be supported together with the US specific emergency dialing habit 911. Keep in mind that this combination of dialing habits between different countries might create overlaps between the visited sites' emergency dialing and the visiting user's regular dialing habits. For example, if a site in Germany has four-digit extensions starting with 9 (such as +E.164 range +49 6100 773 9XXX), then the abbreviated four-digit intra-site dialing defined for that site through a 9XXX dialing normalization translation pattern creates an overlap with the US emergency dialing 911 if a user from that German site logs into a phone in the US. As long as the emergency dialing habit is more specific, then creating the emergency calling route pattern as urgent pattern makes sure that no delay is experienced when placing an emergency call. On the other hand, the 911 US emergency pattern would "block" all four-digit dialing starting with 911, affecting four-digit intra-site dialing to directory numbers +49 6100 773 911X, for example.

Moving the emergency dialing from the line to the device CSS also avoids the problem that visiting users' emergency dialing habits (112 in case of a user from Germany) need to be transformed to the visited countries emergency dialing habit (911 in the US).

Route Patterns for Video PSTN (ISDN) Calls

Video ISDN gateways require special treatment from the dial plan perspective because it is unfeasible from the cost perspective to use ISDN video gateways for regular voice calls. In this design the selection of video ISDN gateways is explicitly tied to a special video PSTN dialing habit (see Table 2-11). Table 2-30 shows the required route patterns to enable this dialing habit.

Table 2-30 Route Patterns for Video PSTN (ISDN) Calls

Pattern	Partition	Gateway or Route List	Description
*!	PSTNInternational	RL_VIDEO	Variable length because we need to support E.164 behind the *
*!#	PSTNInternational	RL_VIDEO	Alternative pattern to allow termination of variable length dialing with #. Discard Digits set to **Trailing-#**
*1XXXXXXXXXX	PSTNInternational	RL_VIDEO	Supplementary route pattern to allow dialing to US destinations (fixed length) without inter-digit timeout. **Urgent Priority** checked.

Putting the video ISDN route patterns into partition PSTNInternational effectively adds video dialing capabilities to class of service International.

Outbound Calls: Called and Calling Number Transformations on ISDN Gateways

On ISDN trunks, calling and called party number information is sent and received in calling and called party information elements. These information elements are a triplet consisting of numbering plan, number type, and number. How these fields need to be set depends on the trunk service definition of the provider. As an example, for a call to E.164 destination 4961007739764 on a trunk in Germany in the same area code 6100, the called party number in the outgoing ISDN SETUP message could be sent as (plan/type/number) ISDN/national/61007739764, ISDN/subscriber/7739764, or unknown/unknown/061007739764.

If gateways terminating ISDN trunks are connected to Unified CM using SIP, then number types cannot be sent from Unified CM to the gateway because SIP does not know the concept of number types. Whether different ISDN number types need to be supported for different call types depends on the provider's SIP trunk service definition. On ISDN trunks, some providers always allow called and calling party numbers independent of called destination to be sent using the same ISDN plan and type indication.

Table 2-31 shows an example of alternate called party number formats that an ISDN provider in the US might accept.

Table 2-31 Alternate ISDN Number Format for Calls on US ISDN Trunk

Type of Call	Destination	Called Party Plan/Type/Number to Be Sent to PSTN	Digit String Sent to Gateway
National	+12125551234	unknown/unknown/12125551234	*12125551234
International	+4961007739764	unknown/unknown/0114961007739764	*0114961007739764

The digit string sent to the gateway is prefixed with a "*" to simplify the dial peer definition on the gateway. Prefixing called party numbers sent to the gateway with a "*" enables easy non-colliding destination-pattern based outbound dial-peer selection on the gateway for inbound and outbound calls because called party numbers received from the PSTN never start with a "*". The leading "*" prefixed by Unified CM needs to be removed on the gateway before sending the call to the PSTN. The leading "*" on all called party numbers sent from Unified CM to the gateway allows the use of "destination-pattern *" on the POTS dial peers on the gateway. The default digit stripping behavior of Cisco IOS will then automatically strip the leading "*".

The transformation from the called +E.164 destination to the digit string to be sent to the PSTN can be achieved on Unified CM, and on the gateway the ISDN plan and type can be enforced easily using Cisco IOS voice translation rules as shown in Example 2-2.

Example 2-2 Cisco IOS Voice Translations to Force Single ISDN Plan and Type

```
voice translation-rule 1
    rule 1 /^\*/ // type any unknown plan any unknown
    rule 2 // // type any unknown plan any unknown
voice translation-profile ISDNunknown
    translate called 1
    translate calling 1
dial-peer voice 1 pots
    translation-profile outgoing ISDNunknown
```

The Cisco IOS configuration piece shown in Example 2-2 demonstrates how to force a single ISDN plan and type for calling and called party information to be sent to the PSTN through a given POTS dial-peer. Rule 1 of voice-translation-rule 1 matches all numbers starting with "*" and simply removes this leading "*". Rule 2 of voice translation-rule 1 matches on all numbers with any plan and type, and it forces both

plan and type to unknown while not changing the actual digit string of the number. With this Cisco IOS voice translation-rule applied to the POTS dial peer pointing to the ISDN, all called and calling party numbers sent from Unified CM to the gateway will be forwarded to the PSTN unchanged, with plan and type forced to unknown.

With this translation logic in place on the gateway, the piece that still needs to be provisioned on Unified CM is the transformation of the +E.164 called party information to the digit string to be sent to the PSTN according to Table 2-31. Table 24 depicts the required called party transformation patterns for localizing +E.164 for ISDN dialing.

Table 2-32 Called Party Transformation Patterns to Localize +E.164 for ISDN via SIP

Pattern	Partition	Transformation	Description
\+.1!	USGWLocalizeCd	Strip pre-dot, prefix *	+12125551234 –> *12125551234
\+.!	USGWLocalizeCd	Strip pre-dot, prefix *011	+4961007739764 –> *0114961007739764

To apply the called party transformations defined by the called party transformation patterns shown in Table 2-32 to a gateway, a CSS USGWLocalizeCd with only partition USGWLocalizeCd in it needs to be defined, and this CSS is then set as **Called Party Transformation CSS** in the **Device Mobility Related Information** section on the gateway's device pool. Configuring these transformations on the device pool enables sharing the same settings with multiple gateways in the same site sharing the same called party transformation requirements. To achieve this, the **Use Device Pool Called Party Transformation CSS** option needs to be checked in the **Outbound Calls** section on the gateway configuration page.

Also, we need to provision the transformation required to force the calling party number from +E.164 to whatever needs to be sent to the service provider. Here we need to consider how to treat calling party information for a call originating from a non-DID or a call originating from a DN that is not part of the DID range associated with the given gateway. The most common option is to set the caller ID to a site-specific main extension. This site specificity requires creation of site-specific calling party transformations as illustrated by Table 2-33.

Table 2-33 Calling Party Transformation Patterns to Localize +E.164 for ISDN via SIP

Pattern	Partition	Transformation	Description
\+.19195551XXX	RTPGWLocalizeCn	Strip pre-dot	+19195551001 –> 19195551001 Forward caller ID from the DID range associated with the gateway, but strip the leading plus (+), assuming that the calling party number can be sent to the provider as 1 plus 10 digits
\+!	RTPGWLocalizeCn	Mask 19195551888	Force everything to 19195551888
!	RTPGWLocalizeCn	Mask 19195551888	Force everything to 19195551888

The calling party transformation patterns in Table 2-33 perform the required transformations that make sure any calling party number, whether in the form of a +E.164 number or an enterprise specific number not matching the trunks DN range, is forced to a main number (19195551888).

To enable these transformations equivalent to the above method to apply outbound called party transformations, a CSS RTPGWLocalizeCn needs to be created using only partition RTPGWLocalizeCn, and this CSS needs to be applied as the calling party transformation CSS in the **Outbound Calls** section on the gateway configuration page or in the **Device Mobility Related Information** section on the gateway's device pool.

If a specific called or calling party transformation is needed per gateway, then using the device pool level settings for the called party transformations is overly complicated. In that case uncheck the **Use Device Pool Called/Calling Party Transformation CSS** options in the **Outbound Calls** section on the gateway configuration page, and set the called or calling party transformation CSS there.

Outbound Calls: Called and Calling Number Transformations on SIP Trunks

As mentioned earlier, SIP does not have the concept of "typed" numbers. Usually on SIP trunks all called and calling party numbers need to be sent in a single format independent of the type of called destination. The most common options are +E.164 or E.164. To enable easier dial-peer configuration with non-overlapping destination patterns for inbound and outbound calls, again we want to prefix all E.164 called party information with "*" when sent to the Cisco Unified Border Element terminating the SIP trunk.

If E.164 needs to be sent (without the +), then the above approach using called party transformation patterns can be reused. The single called party transformation shown in Table 2-34 is enough to make sure that the leading + of all +E.164 numbers gets stripped. Again we also need to create a CSS (for example, GWNoPlus) that addresses only partition GWNoPlus, and then apply this called party transformation pattern as **Called Party Transformation CSS** on either the gateway or the gateway's device pool.

Table 2-34 Called Party Transformation Pattern to Localize +E.164 to *E.164 for SIP

Pattern	Partition	Transformation	Description
\+.!	GWNoPlus	Strip pre-dot, prefix *	+4961007739764 –> *4961007739764 +12125551234 –> *12125551234

Even if no format transformation is required for calling party information sent on a SIP trunk, some filtering still needs to be applied to the calling party information to make sure that only valid numbers are sent to the provider. The same calling party transformations as described before in section on Outbound Calls: Called and Calling Number Transformations on ISDN Gateways and summarized in Table 2-33 can be used. Cisco IOS voice translations on Cisco Unified Border Element then make sure that the calling party information is sent to the provider according to the format requirements of the provider. Example 2-3 shows Cisco IOS voice translations to be applied on the VoIP dial-peer on the Cisco Unified Border Element (CUBE) pointing to the provider. These translations transform called party information from *E.164 to +E.164 and the calling party information from E.164 to +E.164.

Example 2-3 Cisco IOS Voice Translations to Force +E.164 Calling and Called Party Number on CUBE

```
voice translation-rule 2
    rule 1 /^\*/ /+/
    rule 2 // /+/
voice translation-profile SIPtoE164
    translate called 2
    translate calling 2
dial-peer voice 2 voip
    translation-profile outgoing SIPtoE164
```

Rule 1 in Example 2-3 replaces a leading "*" with a leading "+" while rule 2 just prefixes a "+" to all numbers.

Inbound Calls: Called and Calling Number Transformations on ISDN Gateways

Because all call routing on Unified CM is based on +E.164 for all incoming calls arriving at Unified CM, we need to make sure that called party information is transformed to +E.164 from the format received on the link from the provider. As mentioned earlier in the section on Outbound Calls: Called and Calling Number Transformations on ISDN Gateways, calling and called party information sent and received on ISDN trunks is a triplet consisting of numbering plan, number type, and number. Because SIP does not support number types, the semantics of the number type as received from the provider is lost if only the actual number is forwarded by the gateway over the SIP trunk to Unified CM. To avoid this, Cisco IOS voice translation needs to be deployed on the gateway to create a +E.164 digit string to be sent to Unified CM based on the received number plan, type, and number. Example 2-4 shows the Cisco IOS voice translation configuration to achieve this.

Example 2-4 Cisco IOS Voice Translations to Map from ISDN to +E.164

```
voice translation-rule 3
    rule 1 /^\(.+\)$/ /+1\1/ type national unknown plan any unknown
    rule 2 /^\(.+\)$/ /+\1/ type international unknown plan any unknown
voice translation-profile ISDNtoE164
    translate called 3
    translate calling 3
dial-peer voice 1 pots
    translation-profile incoming ISDNtoE164
```

The Cisco IOS translation shown in Example 2-4 assumes that we received called party information as type national and that the number in this case has only 10 digits. Rule 1 matches on any number (/^\(.+\)$/) with type international and simply prefixes +1 (/+\1/) while forcing plan and type to unknown because both are irrelevant when forwarded on the SIP trunk to Unified CM. The same translation rule is applied to both calling and called party information in translation profile ISDNtoE164, so that the calling party information as a 10-digit number with type national will be transformed correctly to +E.164 by rule 1. Rule 2 does not really apply to received called party information because the provider will typically send called party information using only a single format. Hence, rule 2 is relevant only for calls received from international destinations for which we expect to receive calling party information as type international with the number set to the full E.164 number of the calling party.

Different number formats might be used, depending on the provider, and this will require use of different transformations on the gateway or on Unified CM. For a detailed explanation of voice translation rules, see the document on *Number Translation using Voice Translation Profiles*, available at

https://www.cisco.com/c/en/us/support/docs/voice/call-routing-dial-plans/64020-number-voice-translation-profiles.html

If for some reason the same rules cannot be used for calling and called party information transformation, then separate voice translation rules need to be provisioned for calling and called party information and associated with translation of calling and called party information in one translation profile.

Using inbound Cisco IOS voice translation rules is required only if different number types are sent by the provider. If the number type for calling or called party information is always unknown, for example, then the digit transformation to globalized +E.164 can happen on Unified CM either by using the inbound prefixes for calling and called party information or by using calling and called party transformation CSSs. Both prefixes and calling and called party transformations can be defined either

on the trunk level or on the device pool level. Keep in mind that, because SIP does not support different number types, inbound calling and called prefixes or CSSs need to be set for number type **unknown** if set on the device pool level.

Inbound Calls: Called and Calling Number Transformations on SIP Trunks

Inbound call number information treatment on PSTN SIP trunks is generally simpler than the number handling in the ISDN case described before. The main reason is that number information on SIP trunks is not typed, and thus transformations are less complex and need to consider only the received digit string. Typically both calling and called party information on a SIP trunk is already in +E.164 format, and thus no transformations are needed.

If calling and called parties are received in E.164 format, then the easiest way to transform to +E.164 is to simply configure a prefix "+" on the SIP trunk in Unified CM or on the trunk's device pool. This prefix can be configured in the Incoming Calling Party Settings or Incoming Called Party Settings on the trunk or the trunk's device pool. Remember that for SIP trunks the setting for number type **Unknown Number** is relevant on the device pool level.

Calling Party Information Display on Phones

Because all directory numbers are provisioned as +E.164 numbers for calls originating from these +E.164 directory numbers, calling party information is in +E.164 format automatically. To simplify and provide consistent calling party presentation for all possible call flows, all calling party information received from outside networks such as the PSTN is normalized to +E.164 as discussed earlier. When a call is presented to a phone or to an outside network, the calling party information presented for that call sometimes needs to be transformed to the format expected by the network in case of the call being sent to a gateway or the format expected by the user in case of the call being sent to a phone.

Of special consideration are calls originating from phones with non-DIDs. In this case the only available calling party information is identical to the provisioned non-DID in the format of an enterprise specific number (ESN). Table 2-9 summarizes the ESN ranges used in the example topology.

On phones, sometimes +E.164 is not the preferred calling party display information, although keeping this information as +E.164 simplifies the deployment and is preferred. In that case the desired format typically depends on both the calling and called entities. Table 2-35 shows an example of the expected calling party display on a phone in site SJC for calls from various sources.

Table 2-35 Expected Calling Party Display on SJC Phone

Calling Entity "Native" Calling Party Information	Expected Display	Comment
+12125551234	912125551234	Call from US; display follows PSTN dialing habit.
+14085554001	4001	Call from +E.164 DN in the SJC DID range; display follows abbreviated intra-site dialing habit.

Table 2-35 Expected Calling Party Display on SJC Phone (continued)

Calling Entity "Native" Calling Party Information	Expected Display	Comment
81405001	5001	Call from non-DID in the SJC ESN range (see Table 2-9); display follows abbreviated four-digit intra-site dialing to non-DIDs in site SJC.
+4961007739764	90114961007739764	Call from international PSTN destination; display follows US PSTN dialing habit for international destinations.

To achieve the display format depicted in Table 2-35, calling party transformation patterns need to be provisioned in adequate partitions, and calling party transformation CSSs based on these partitions have to be configured on the phones, to enable the transformations.

Table 28 summarizes all calling party transformation patterns that must be provisioned to achieve the abbreviated calling party number display shown in Table 2-35 for all US sites based on the number ranges shown in Table 2-9.

Table 2-36 Phone Localization Calling Party Transformation Patterns

Pattern	Partition	Transformation	Description
\+.1!	USPhLocalize	Strip pre-dot, prefix 9	Any US destination: +12125551234 –> 912125551234
\+.!	USPhLocalize	Strip pre-dot, prefix 9011	Any international destination: +4961007739764 –> 90114961007739764
\+14085554XXX	SJCPhLocalize	Mask 4XXX	Call from local DN range: +14085554001 –> 4001
81405XXX	SJCPhLocalize	Mask 5XXX	Call from local non-DID range: 81405001 –> 5001
\+19725555XXX	RCDPhLocalize	Mask 5XXX	Call from local DN range: +19725555001 –> 5001
81976XXX	RCDPhLocalize	Mask 6XXX	Call from local non-DID range: 81976001 –> 6001
\+19195551XXX	RTPPhLocalize	Mask 1XXX	Call from local DN range: +19195551001 –> 1001
81912XXX	RTPPhLocalize	Mask 2XXX	Call from local non-DID range: 81912001 –> 2001

Table 2-37 shows the calling party transformation CSSs to enable calling party localization for phones in all US sites. The schema allows the reuse of dialing domain (country) specific calling party localization transformation patterns for all sites in that dialing domain (country). The country specific calling party localization patterns basically map national and international numbers to the country specific national and international dialing habit.

Table 2-37 Phone Localization Calling Party Transformation CSSs for US Sites

CSS	Partitions
SJCPhLocalize	SJCPhLocalize USPhLocalize
RCDPhLocalize	RCDPhLocalize USPhLocalize
RTPPhLocalize	RTPPhLocalize USPhLocalize

Table 2-38 shows an example of the country specific phone localization calling party transformation patterns that would need to be provisioned for Italy and Germany.

Table 2-38 Phone Localization Calling Party Transformation Patterns for Italy and Germany

Pattern	Partition	Transformation	Description
\+49.!	DEPhLocalize	Strip pre-dot, prefix 00	Any German destination: +4941001234 –> 0041001234
\+.!	DEPhLocalize	Strip pre-dot, prefix 000	Any international destination: +14085551234 –> 00014085551234
\+39.!	ITPhLocalize	Strip pre-dot, prefix 0	Any Italian destination: +390730123456 –> 00730123456 +393012345678 –> 03012345678
\+.!	ITPhLocalize	Strip pre-dot, prefix 000	Any international destination: +14085551234 –> 00014085551234

Automated Alternate Routing

Automated alternate routing (AAR) is a mechanism that reroutes calls to registered endpoints via an alternate route through the PSTN in case sufficient bandwidth is not available (call admission control does not allow the call) between the originating endpoint, gateway, or trunk and the called endpoint. AAR applies only to calls to endpoints. Insufficient bandwidth for calls to other destinations such as gateways and trunks does not trigger AAR. For those cases, the alternate routing mechanism is based on route lists and route groups. The following steps are required to activate AAR:

- Set the Automated Alternate Routing Enable service parameter (see the section on Service Parameter Settings).
- Configure a single AAR group **Default** without any Dial Prefix (default).
- Define a CSS PSTNReroute with access only to +E.164 PSTN route patterns. Based on the examples in this design, this CSS would need to include only partition PSTNInternational.
- On all endpoints, trunks, and other devices initiating calls that potentially might be subject to AAR:
  - Set the AAR Calling Search Space to PSTNReroute.
  - Set AAR Group to **Default**.
- On all device pools, set the AAR Calling Search Space to PSTNReroute.
- On all device pools, set AAR Group to **Default**

- On +E.164 directory numbers, configure the AAR masks so that the resulting number is the +E.164 number of the directory number. In a country with a fixed length numbering plan, the mask can be set to some identical value on all directory numbers (such as +1XXXXXXXXXX in the US). If variable length directory numbers need to be covered, more specific masks covering a single site or, as a worst case scenario, a fully qualified +E.164 AAR mask identical to the respective directory number have to be provisioned. For non-DIDs the AAR mask is left empty. This effectively disables AAR if a non-DID is called. This makes sense because a non-DID does not have an equivalent E.164 address and thus cannot be reached via the PSTN.

The above list shows one of the advantages of a dial plan using +E.164 directory numbers. In this case the called +E.164 address can be reused directly for alternate dialing over the PSTN without applying any other modifications.

Alternate Routing for Unregistered Endpoints

In case of a WAN failure in a multi-site deployment with centralized call processing, endpoints in the affected lose connectivity with the centralized Unified CM and register with a local SRST gateway instead (see the section on Survivable Remote Site Telephony (SRST) Deployment). This allows the affected phones to still place and received calls to and from phones in the same site and the PSTN. Calls from phones registered with the central Unified CM will fail, though, because from the central Unified CM's perspective the called device is unregistered and thus unreachable. To enable automatic rerouting of calls to unregistered endpoints over the PSTN, perform the following tasks on each directory number that requires automatic rerouting:

- Set the Forward Unregistered Internal and Forward Unregistered External destination to the same value as the phone's +E.164 directory number.
- Set the Forward Unregistered Internal and Forward Unregistered External CSS to PSTNReroute. This is the same CSS as defined in the section on Automated Alternate Routing, and it allows access to PSTN route patterns.
- Set the **Max Forward UnRegistered Hops to DN** service parameter to a value other than zero to make sure to limit the impact of routing loops that can occur if a phone is unregistered (for example, because it is not plugged in) while the site's gateway still is connected to Unified CM.

Alternate routing over the PSTN for unregistered endpoints makes sense only for endpoints with +E.164 directory numbers. For endpoints without a DID (endpoints with an ESN as directory number), the only meaningful rerouting for unregistered endpoints is to forward incoming calls to voicemail. To forward calls to unregistered endpoints to voicemail, perform these tasks:

- Select the Voicemail options for Forward Unregistered Internal and Forward Unregistered External.
- Set the Forward Unregistered Internal and Forward Unregistered External CSS to a CSS implementing class of service Internal (for example, SJCInternal). Effectively this CSS has to provide access to only the voicemail pilot number.

LDAP System Configuration

Before defining the actual synchronization agreements, the LDAP system has to be enabled. In the LDAP System Configuration menu, do the following:

- Select (check) the **Enable Synchronizing from LDAP Server** option
- Select the correct LDAP Server Type for your deployment.
- Select the correct LDAP Attribute for User ID for your deployment.

In an environment where users are synchronized from Microsoft Active Directory, use the settings shown in Table 2-39.

Table 2-39 LDAP System Settings for Microsoft Active Directory

Setting	Value
LDAP Server Type	Microsoft Active Directory
LDAP Attribute for User ID	sAMAccountName

LDAP Custom Filter

If a Unified CM based directory search is used on phones, then it does make sense to synchronized the full corporate LDAP directory to Unified CM. In that case we need to be able to differentiate between users who actually use UC services of the local cluster and users who are synchronized only to reflect the complete corporate LDAP directory on Unified CM.

To achieve this goal, custom LDAP filters can be used to define two groups of users: local and remote. Remote here means that these users do not use any UC services on the local Unified CM cluster. Table 2-40 shows two custom LDAP filters, assuming that our deployment has users in the US and Europe and that only the US users are considered as local users.

Table 2-40 Custom LDAP Filter Settings

LDAP Filter Name	Filter
Local	(& (objectclass=user) (!(objectclass=Computer)) (!(UserAccountControl:1.2.840.113556.1.4.803:=2)) (telephoneNumber=+1*))
Remote	(& (objectclass=user) (!(objectclass=Computer)) (!(UserAccountControl:1.2.840.113556.1.4.803:=2)) (| (telephoneNumber=+3*) (telephoneNumber=+4*)))

For better readability, the LDAP filter strings in Table 2-40 are separated into multiple lines, with the indentation levels reflecting the structure of the LDAP filter strings. To provision these LDAP filters in Unified CM, you have to concatenate all lines of a given filter into a single line.

Both LDAP filters are extensions of the default LDAP filter for Microsoft Active Directory. Default LDAP filters for other directory types can be found in the chapter on *Directory Integration and Identity Management* in the latest version of the *Cisco Collaboration System SRND* and in the Unified CM online help for the LDAP directory settings.

The LDAP filters in Table 2-40 use the beginning of the phone numbers as criteria to determine whether the individual user is a local or a remote user.

When using multiple LDAP synchronization agreements, you have to make sure that the LDAP filters used by these synchronization agreements are disjunct so that no single user is matched by both filters.

Feature Group Templates

Capabilities of users synchronized from LDAP are defined in a feature group template (FGT). Table 2-41 summarizes the settings for the FGT defining the capabilities of users with active devices on the Unified CM cluster.

Table 2-41 Feature Group Template for Local Users

Setting	Value	Comment
Name	FGTlocal	Name should indicate that this is an FGT used for local users.
Description	FGT for local users	
Home Cluster	Checked	Make sure that UDS-based service discovery for this user resolves to the local Unified CM cluster.
Enable User for Unified CM IM and Presence	Checked	Enable the user for IM and Presence
BLF Presence Group	Standard Presence Group	Single BLF presence group for all users, to simplify the deployment.
SUBSCRIBE Calling Search	DefaultSubscribe	Use the default subscribe CSS described in the section on Special CSSs.

All other settings can be left as default values.

Because remote users are also synchronized from LDAP (see the section on LDAP Custom Filter), an FGT for remote users must also be provisioned. The key difference is that in that FGT the **Home Cluster** and **Enable User for Unified CM IM and Presence** options are not checked. Table 2-42 summarizes these settings.

Table 2-42 Feature Group Template for Remote Users

Setting	Value	Comment
Name	FGTremote	Name should indicate that this is an FGT used for remote users.
Description	FGT for remote users	

Table 2-42 Feature Group Template for Remote Users (continued)

Setting	Value	Comment
Home Cluster	Not checked	Make sure that UDS-based service discovery for this user does not resolve to the local Unified CM cluster.
Enable User for Unified CM IM and Presence	Not checked	Do not enable the user for IM and Presence.

All other settings can be left as default values.

LDAP Synchronization Agreements

To synchronize all local users to Unified CM, an LDAP synchronization agreement needs to be configured. Table 2-43 shows the required settings to be configured under **System/LDAP/LDAP Directory**.

Table 2-43 LDAP Synchronization Agreement for Local Users

Setting	Value	Comment
LDAP Configuration Name	Local	Indicates that this LDAP synchronization agreement synchronizes local users.
LDAP Manager Distinguished Name	Name of admin users	Can be in the form of ldapaccess@ent-pa.com or cn=ldapaccess,cn=users,dc=ent-pa,dc=com
LDAP Password	Password of the LDAP admin	
LDAP User Search Base	LDAP Search base	Example: dc=ent-pa,dc=com
LDAP Custom Filter	Local	Refers to the custom LDAP filter described in the section on LDAP Custom Filter.
Perform Sync Just Once	Unchecked	LDAP synchronization is executed periodically.
Perform a Re-sync Every	Reasonable interval	Make sure to set the interval small enough to pick up corporate directory changes in a reasonable time, but keep in mind that executing the LDAP synchronization creates significant load on the Unified CM publisher. Synchronizing once every 24 hours probably is a good default.
Directory URI	mail	Typically directory URIs of users are identical to their email addresses.
Access Control Groups	Standard CCM End Users Standard CTI Enabled	Add or remove other access control groups as needed, but keep in mind that without Standard CCM End Users, the users will not be able to log into the self-service portal.
Feature Group Template	Local	Refers to the FGT described in the section on Feature Group Templates.
LDAP Server Information	References to corporate LDAP servers to be uses as source	Make sure to provision redundant servers, if possible.

The LDAP synchronization agreement in Table 2-43 ties together the FGT and custom LDAP filter defined before. This makes sure that, for all users in the corporate directory matching the custom LDAP filter, a user on Unified CM is created with the capabilities defined in the FGT.

A dedicated LDAP synchronization agreement is also required to synchronize the remote users who do not use UC services on the local Unified CM cluster. Table 2-44 summarizes the settings for this LDAP synchronization agreement.

Table 2-44 LDAP Sync Agreement for Remote Users

Setting	Value	Comment
LDAP Configuration Name	Remote	Indicates that this LDAP synchronization agreement synchronizes remote users.
LDAP Manager Distinguished Name	Name of admin users	Can be in the form of ldapaccess@ent-pa.com or cn=ldapaccess,cn=users,dc=ent-pa,dc=com
LDAP Password	Password of the LDAP admin	
LDAP User Search Base	LDAP Search base	Example: dc=ent-pa,dc=com
LDAP Custom Filter	Remote	Refers to the custom LDAP filter described in the section on LDAP Custom Filter.
Perform Sync Just Once	Unchecked	LDAP synchronization is executed periodically.
Perform a Re-sync Every	Reasonable interval	Make sure to set the interval small enough to pick up corporate directory changes in a reasonable time, but keep in mind that executing the LDAP synchronization creates significant load on the Unified CM publisher. Synchronizing once every 24 hours probably is a good default.
Directory URI	mail	Typically directory URIs of users are identical to their email addresses.
Access Control Groups	No access control groups selected	Remote users are not members of any access control group.
Feature Group Template	Remote	Refers to the FGT described in the section on Feature Group Templates.
LDAP Server Information	References to corporate LDAP servers to be uses as source	Make sure to provision redundant servers, if possible.

Using the above LDAP synchronization agreements, all users can be identified from the corporate directory, and the FGTs associated with the LDAP synchronization agreements make sure that capabilities are configured correctly for all users.

User Authentication with LDAP

Table 2-45 shows an example of LDAP authentication settings.

Table 2-45 LDAP Authentication Settings

Setting	Example	Comment
LDAP Authentication for End Users		
Use LDAP Authentication for End Users	Checked	Enables LDAP authentication for the Unified CM cluster.
LDAP Manager Distinguished Name	cn=ldapmanager,dc=ent pa,dc=com	Distinguished name of an AD account with read access rights to all user objects in the desired user search base.
LDAP Password	Some password	
Confirm Password	Same as above	
LDAP User Search Base	ou=enterprise,dc=ent-pa,dc=com	
LDAP Server Information		
Host Name or IP Address for Server	ent-dc1.ent-pa.com	Server with global catalog role
LDAP Port	3268	Port to access global catalog (recommended)

Cisco Unified CM Group Configuration

Cisco Unified CM groups allow you to define groups of Unified CM instances in the cluster that determine which Unified CM instances should be used by devices to register to the Unified CM cluster. If only a single Unified CM call processing pair is deployed (see the section on Provision the Cisco Unified CM and IM and Presence Service Cluster for more information), then a single Unified CM group named Default also needs to be deployed, and both Unified CM instances running on the single pair of Unified CM call processing subscribers in the cluster have to be members of this single Unified CM group.

If more than one pair of Unified CM call processing subscribers exists, then additional Unified CM groups need to be provisioned (one for each pair of Unified CM call processing subscribers), and in each Unified CM group the two Unified CM instances running on that specific pair are added to the group.

For a Unified CM cluster with two pairs of Unified CM call processing subscribers named ucm1a.ent-pa.com and ucm1b.ent-pa.com in the first pair and ucm2a.ent-pa.com and ucm2b.ent-pa.com in the second pair, with ucm1a and ucm2a being the primary Unified CM call processing subscribers in each pair, Table 2-46 lists the Unified CM groups to be provisioned.

Table 2-46 Example Unified CM Group Definition

Unified CM Group	Unified CM Group Members
CM_1	CM_ucm1a.ent-pa.com CM_ucm1b.ent-pa.com
CM_2	CM_ucm2a.ent-pa.com CM_ucm2b.ent-pa.com

All registrations have to be equally balanced between Unified CM groups. This is achieved by assigning devices to Unified CM groups via device pool configuration as discussed in the section on Device Pools.

Phone NTP References

If you want to do so, you can configure phone Network Time Protocol (NTP) references in Cisco Unified Communications Manager Administration to ensure that a phone running SIP gets its date and time from the NTP server. If all NTP servers do not respond, the phone that is running SIP uses the date header in the 200 OK response to the REGISTER message for the date and time.

After you add the phone NTP reference to Cisco Unified CM Administration, you must add it to a date/time group.

To define phone NTP references, get the IP addresses of the NTP servers you plan to use, and configure the settings according to Table 2-47.

Table 2-47 Phone NTP Reference Settings

Setting	Example	Comment
IP Address	66.228.35.252	IP address of NTP server to be used
Description	0.pool.ntp.org	Should refer to the hostname of the IP address being entered
Mode	Unicast	Unicast limits devices to using only NTP response from listed servers

Make sure to provision multiple phone NTP references for redundancy.

Date and Time Groups

Date and time groups allow you to define the time zone and the date and time format to be used for sets of devices registering with Unified CM. The date/time group configuration is specified in the device pool, and the device pool is specified on the phone page. For more information on device pools, see the section on Device Pools.

If you want SIP phones to get their date and time from NTP servers, then in the date/time group you prioritize the phone NTP references, starting with the first server that you want the phone to contact.

Create one named Date/Time Group for each of the time zones in which you will deploy endpoints, as illustrated in Table 2-48.

Table 2-48 Example Date/Time Group Definitions

Date and Time Group	Time Zone
RCD_Time	America/North_Dakota/New_Salem
RTP_Time	America/New_York
SJC_Time	America/Los_Angeles

Media Resources

A media resource is a software-based or hardware-based entity that performs media processing functions on the data streams to which it is connected. Media processing functions include mixing multiple streams to create one output stream (conferencing), passing the stream from one connection to another (media termination point), converting the data stream from one compression type to another (transcoding), streaming music to callers on hold (music on hold), echo cancellation, signaling, voice termination from a TDM circuit (coding/decoding), packetization of a stream, streaming audio (annunciation), and so forth. The software-based resources are provided by the Cisco Unified CM IP Voice Media Streaming Application.

Media Resource Manager

The Media Resource Manager (MRM), a software component in the Unified CM, determines whether a media resource needs to be allocated and inserted in the media path. When the MRM decides and identifies the type of the media resource, it searches through the available resources according to the configuration settings of the media resource group list (MRGL) and media resource groups (MRGs) associated with the devices in question. MRGLs and MRGs are constructs that hold related groups of media resources together for allocation purposes

Media Resource Selection and Avoiding the Default MRG

Media resource groups (MRGs) and media resource group lists (MRGLs) provide a method to control how resources are allocated, which could include rights to resources, location of resources, or resource type for specific applications. MRGs are used to group together media resources of similar characteristics, and MRGLs define a set of MRGs to be considered when selecting a required media resource for a session. If the Media Resource Manager does not find a required resource by searching through a configured MRGL, considering all media resources being members of MRGs of that list, then the Media Resource Manager checks a default media resource group for media resources. All media resources by default are members of this default MRG unless they are explicitly configured to be members of any specific MRG.

In this design we will not use the default MRG because it makes troubleshooting of media resource selection more complicated. To make sure that the default MRG is empty, you have to assign all media resources to at least one MRG.

Cisco IP Voice Media Streaming Application

The Cisco IP Voice Media Streaming Application provides the following software-based media resources:

- Conference bridge
- Music on Hold (MoH)
- Annunciator
- Media termination point (MTP)

When the IP Voice Media Streaming Application is activated on a node in the Unified CM cluster, one of each of the above resources is automatically configured. For service activation recommendations, see Table 2-3.

In this design only unicast MoH is used, with media being streamed from the Cisco IP Voice Media Streaming Application running on the Unified CM cluster subscriber nodes.

An annunciator is a software function of the Cisco IP Voice Media Streaming Application that provides the ability to stream spoken messages or various call progress tones from the system to a user.

All MOH and annunciator media resources created by the Cisco IP Voice Media Streaming Application running on Unified CM are combined in a single MRG by performing the following tasks:

- Create an MRG named Software.
- Assign all annunciator resources created by the Cisco IP Voice Media Streaming Application to MRG Software.
- Assign all MoH resources created by the Cisco IP Voice Media Streaming Application to MRG Software.

The software-based conferencing and media termination points created by the Cisco IP Voice Media Streaming Application are not used in this design. To disable them, perform the following tasks:

- Create an MRG named Unused.
- Assign all software-based conference bridges created by the Cisco IP Voice Media Streaming Application to MRG Unused.
- Assign all software-based media termination points created by the Cisco IP Voice Media Streaming Application to MRG Unused.

This makes sure that these resources are not part of the default MRG any longer and are never considered in the Media Resource Manager media resource selection process.

MRG and MRGL Definitions

Its good practice to keep the number of provisioned MRGLs to a minimum. Factors contributing to the number of required MRGLs include:

- Site specificity

  If site-specific media resources exist, then site-specific MRGs for those resources need to be configured, and typically also site-specific MRGLs are required to allow for site-specific selection of (typically local) media resources.

- Different types of media resources of the same class

  Unified CM does not differentiate between audio-only and audio/video conferencing resources. If both audio and audio/video conferencing media resources are provisioned, then an MRG (and MRGL) is required per type of media resource to allow configuration of differential access policies to these resources. See the Conferencing chapter for more details on conferencing resources.

If no site-specific media resources and no differentiation of media resource types is required, then at least a single MRGL named Standard needs to be configured.

For each required MRGL based on site specificity and media resource type provision, create an MRGL by performing the following tasks:

- Set the MRGL name so that it reflects the site specificity and media resource type of the MRGL.
- Select the desired MRGs for the MRGL. Make sure to always include the Software MRG so that access to MoH and Annunciator is ensured.

Table 2-49 shows example MRGL definitions that provide differentiated treatment of audio and video conferencing. MRGL Audio would need to be assigned to devices requiring access to audio conferencing media resources only, while MRGL Video would allow access to video conferencing resources.

Table 2-49 Example MRGL Definition with Audio and Video Conferencing

MRGL Name	MRGs	Comment
Audio	Audio Software	MRGL with access to audio conferencing media resources in MRG Audio. MRG Software added to provide access to MoH and annunciator.
Video	Video Software	MRGL with access to video conferencing media resources in MRG Video. MRG Software added to provide access to MoH and annunciator.

Device Pools

Device pools define sets of common characteristics for devices. Characteristics defined on the device pool include the settings shown in Table 2-50.

Table 2-50 Device Pool Settings

Setting	Description
Cisco Unified Communications Manager Group	Unified CM groups are needed to distribute registrations equally among Unified CM call processing subscriber pairs (see the section on Cisco Unified CM Group Configuration). The Unified CM Group provisioned on the device pool determines the Unified CM call processing subscribers to which devices associated with the given device pool will try to register.
Local Route Groups	As described in the section on Local Route Groups for Call Type Specific Outbound Gateway Selection, multiple LRGs are defined to allow for call type specific egress gateway selection based on LRGs. For each defined LRG name, the route group selected for that LRG name defines which devices will be considered for a call of the selected type (defined by the route pattern matching on the called number and pointing to a route list referring to specific LRGs). It is important to set route groups for all defined LRG names to avoid call failures due to route lists not containing any valid PSTN resources.
Roaming Sensitive Settings	
Date/Time Group	Defines date and time format and phone NTP references. See the section on Phone NTP References.
Media Resource Group List	MRGL defining the media resources available for a group of devices. See the section on MRG and MRGL Definitions.
Device Mobility Related Information	
AAR Calling Search Space	The CSS used to route calls to an alternate PSTN destination. The dial plan design in this document allows use of the same AAR CSS (PSTNReroute) in all cases (see the section on Automated Alternate Routing).
AAR Group	To enable AAR, an AAR group has to be defined. Using +E.164 directory numbers allows you to deploy AAR using a single AAR group, Default (see the section on Automated Alternate Routing).
Calling Party Transformation CSS	This CSS defines the calling party transformations applied to calling party information sent in the direction of the affected device. For gateways this CSS is tied to the calling party transformation CSS defined in the Outbound Calls section on the gateway configuration page. For phones this CSS is tied to the calling party transformation CSS defined in the Remote Number section on the phone configuration page.
Called Party Transformation CSS	This CSS defines the called party transformations applied to called party information sent in the direction of the affected device. For gateways this CSS is tied to the called party transformation CSS defined in the Outbound Calls section on the gateway configuration page. For phones this CSS has no equivalent on the phone configuration page and does not have any effect when configured on a device pool used for phones.
Call Routing Information	This setting allows you to define incoming calling and called party transformations per numbering type to be applied to incoming calls on gateways. The same settings also can be configured in the gateway configuration page if individual gateway-specific settings are required.

All other device pool level settings are not used in this design.

Whenever the same settings for the configuration options listed in Table 2-50 need to be applied to a group of devices, we recommend creating a device pool with these settings and then assigning all devices to this device pool. If one of the settings needs to be changed for all of the devices, the device pool level configuration allows you to change the setting for all devices at one point.

To minimize the number of device pools, create a device pool only if multiple devices share the same characteristics. An example of this is phones in the same site. Table 2-51 shows an example of device pool settings for phones with video conferencing capabilities in site RTP.

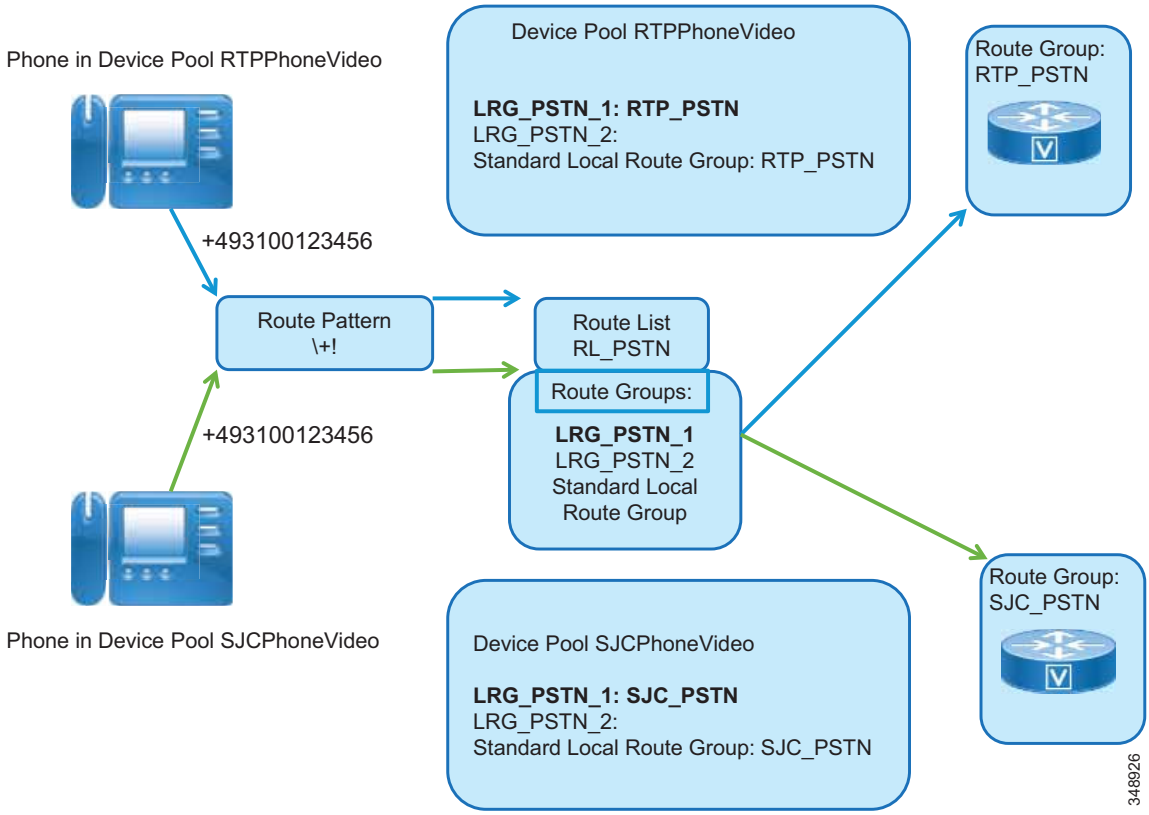
Table 2-51 Device Pool Settings for Phones with Video Conferencing Capabilities in Site RTP

Setting	Value	Comment
Device Pool Name	RTPPhoneVideo	Name should uniquely identify the devices (type and further classification) this device pool is used for. In this case we use this device pool for phones in site RTP with video conferencing capabilities
Cisco Unified Communications Manager Group	CM_1	
Local Route Group Settings		
Standard Local Route Group	RTP_PSTN	All route lists use Standard Local Route Group as last option. Always set Standard Local Route Group to the local PSTN gateways' route group.
LRG_PSTN_1	RTP_PSTN	First option for PSTN calls is to use local RTP gateways.
LRG_PSTN_2	SJC_PSTN	Use HQ gateways as fallback.
LRG_VIDEO_1	SJC_VIDEO	No site-specific video gateways exist. We use the video gateway in site SJC.
LRG_VIDEO_2	<None>	
LRG_EMERGENCY_1	<None>	No setting; fallback to Standard Local Route Group.
LRG_EMERGENCY_2	<None>	No setting; fallback to Standard Local Route Group.
Roaming Sensitive Settings		
Date/Time Group	RTP_Time	See the section on Date and Time Groups.
Media Resource Group List	Video	Provide access to video conferencing media resources (see Table 2-49).
Device Mobility Related Information		
AAR Calling Search Space	PSTNReroute	Same for all devices and device pools.
AAR Group	Default	Same for all devices and device pools.
Calling Party Transformation CSS	RTPPhLocalize	Site-specific calling party transformations (see Table 2-36 and Table 2-37).
Called Party Transformation CSS	<None>	Does not apply to phones.

Table 2-51 shows how the actual site-specific PSTN gateways are assigned to the LRG names to achieve the site-specific egress gateway selection for phones in different sites.

Figure 2-9 shows how different LRG selections for the same LRG name LRG_PSTN_1 on the device pools for phones in site RTP and SJC make sure that PSTN calls from phones in site RTP and SJC egress to the PSTN through different gateways although the same route pattern and route list are used for calls from both sites.

Figure 2-9 Site-Specific Egress Gateway Selection



From the example in Table 2-51 we can see that, following the same schema, we would need to provision two device pools per site to be able to differentiate between devices with and without video conferencing capabilities. If video conferencing capabilities were the exception, we could decide to use only one device pool per site with MRGL set to Audio and then on the few video-enabled devices set the MRGL to Video in the device configuration.

Table 2-52 summarizes the device pool settings of the device pool used for gateways in a specific site. Site RTP is used as an example here.

Table 2-52 Device Pool Settings for PSTN Gateways in Site RTP

Setting	Value	Comment
Device Pool Name	RTP_PSTN	Name should uniquely identify the devices (type and further classification) this device pool is used for. In this case we use this device pool for PSTN gateways in site RTP.
Cisco Unified Communications Manager Group	CM_1	
Local Route Group Settings		
Standard Local Route Group	RTP_PSTN	There actually is no call flow for which a PSTN trunk would need a PSTN resource. Also see the note on configuration order in the section on Route Groups. When you create the device pool, the required route group does not exist yet. Hence, initially you need to configure the device pool and leave the LRG mapping set to <None>. After configuring the SIP trunks and route groups, you can come back and set the LRG mapping.
LRG_PSTN_1	<None>	
LRG_PSTN_2	<None>	
LRG_VIDEO_1	<None>	
LRG_VIDEO_2	<None>	
LRG_EMERGENCY_1	<None>	
LRG_EMERGENCY_2	<None>	
Roaming Sensitive Settings		
Date/Time Group	RTP_Time	See the section on Date and Time Groups.
Media Resource Group List	Audio	Calls coming in from the PSTN would not require access to video conferencing resources.
Device Mobility Related Information		
AAR Calling Search Space	PSTNReroute	Same for all devices and device pools, although not really required for a PSTN trunk.
AAR Group	Default	Same for all devices and device pools, although not really required for a PSTN trunk.
Calling Party Transformation CSS	RTPGWLocalizeCn	Site-specific calling party transformations to make sure that only valid calling party information is sent (all numbers not belonging to the RTP DID range are masked). Also, the digit string is set to a format suitable for the ISDN gateway (see Table 2-33).
Called Party Transformation CSS	USGWLocalizeCd	See Table 2-32. This transformation makes sure that called party numbers are transformed from +E.164 to the format that can be sent as plan **unknown** and type **unknown**.
Call Routing Information		
Incoming Calling Party Settings	Nothing is configured here. We assume that the transformation from ISDN number format to +E.164 is achieved using Cisco IOS voice translation rules on the gateway (see the section on Inbound Calls: Called and Calling Number Transformations on ISDN Gateways).	
Incoming Called Party Settings		

Table 2-53 summarizes the device pool settings for a SIP trunks to other Unified CM clusters and application servers. SIP trunks to other Unified CM clusters do not require any transformations on calling and called part information because the called party number already is globalized to +E.164 by the dialing normalization translation patterns provisioned in the dial plan, and calling party information internal to Unified CM based on the provisioned dial plan is either +E.164 or an ESN and both formats make sense in the context of on-net intercluster calls.

Table 2-53 Device Pool Settings for Central Trunks and Applications

Setting	Value	Comment
Device Pool Name	Trunks_and_Apps	Name should uniquely identify the devices (type and further classification) this device pool is used for.
Cisco Unified Communications Manager Group	CM_1	
Local Route Group Settings		
Standard Local Route Group	RTP_PSTN	Trunks actually do not need PSTN access, but applications might require PSTN access. So PSTN resources of one site are selected via the Standard Local Route Group configuration. Other site's PSTN resources can be used as failover.
LRG_PSTN_1	RTP_PSTN	
LRG_PSTN_2	SJC_PSTN	
LRG_VIDEO_1	<None>	
LRG_VIDEO_2	<None>	
LRG_EMERGENCY_1	<None>	
LRG_EMERGENCY_2	<None>	
Roaming Sensitive Settings		
Date/Time Group	RTP_Time	See the section on Date and Time Groups.
Media Resource Group List	Video	Intercluster calls could potentially require video media resources.
Device Mobility Related Information		
AAR Calling Search Space	PSTNReroute	Same for all devices and device pools.
AAR Group	Default	Same for all devices and device pools.
Calling Party Transformation CSS	<None>	No transformations on intercluster trunks and trunks to application servers.
Called Party Transformation CSS	USGWLocalizeCd	No transformations on intercluster trunks and trunks to application servers.
Call Routing Information		
Incoming Calling Party Settings	Nothing configured. We assume that inbound calling and called party numbers already are normalized.	
Incoming Called Party Settings		

SIP Trunks

All connections to other entities, including call controls, applications, and conferencing resources, use SIP trunks.

SIP Profiles

A SIP profile comprises the set of SIP attributes that are associated with SIP trunks and SIP endpoints. To keep the number of SIP profiles to a minimum, follow these rules:

- Consider the default profiles first.
- Then consider already defined non-default profiles.
- Create a new SIP profile only if none of the default profiles match.
- Avoid defining profiles per trunk.

Table 2-54 shows the settings for a SIP profile to be used for all SIP IP phones and SIP trunks to other Unified CM clusters or SIP gateways.

Table 2-54 SIP Profile for SIP Phones and Standard Trunks

Setting	Value	Comment
Copy of Standard SIP Profile		
Name	FQDN	
Use Fully Qualified Domain Name in SIP Requests	Checked	Prevents IP address of Unified CM server from showing up in SIP calling party information sent by Unified CM.
Early Offer support for voice and video calls	Best Effort (no MTP inserted)	This is the recommended configuration for all Unified CM trunks. Best Effort Early Offer trunks never use MTPs to create an Early Offer and, depending on the calling device, can initiate an outbound SIP trunk call using either Early Offer or Delayed Offer. In the context of this design, outbound calls always use Early Offer.
Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"	Checked	Allows monitoring of the reachability of SIP trunk peers; applies to SIP trunks only.
Ping Interval for In-service and Partially In-service Trunks (seconds)	10	One ping every 10 seconds, combined with a retry count of 6, makes sure that SIP trunk unavailability is detected within a minute.
Ping Interval for Out-of-service Trunks (seconds)	60	If a trunk is out of service, then we do not have to try to reach the peer as often.
Ping Retry Timer (milliseconds)	500	
Ping Retry Count	6	

SIP Trunk Security Profiles

Cisco CallManager Administration groups SIP trunk security-related settings – for example, device security mode, digest authentication, and incoming/outgoing transport type settings – so you can apply all configured settings to a SIP trunk when you choose the profile in the SIP Trunk Configuration window.

Table 2-55 shows the default settings on the system generated SIP trunk security profile Non Secure SIP Trunk Profile. This SIP trunk security profile is used for the SIP trunks to ISDN PSTN gateways, for example.

Table 2-55 Non Secure SIP Trunk Profile SIP Trunk Security Profile Settings

Setting	Value
Name	Non Secure SIP Trunk Profile
Device Security Mode	Non Secure
Incoming Transport Type	TCP+UDP
Outgoing Transport Type	TCP
Enable Digest Authentication	Not Checked
Incoming Port	5060
Enable Application level authorization	Not Checked
Accept presence subscription	Not Checked
Accept out-of-dialog refer	Not Checked
Accept unsolicited notification	Not Checked
Accept replaces header	Not Checked
Transmit security status	Not Checked
Allow charging header	Not Checked
SIP V.150 Outbound SDP Offer Filtering	Use Default Filter

Table 2-56 shows the settings for a SIP Trunk Security Profile used for a SIP trunk to the IM and Presence nodes, differing from the default settings in Table 2-55.

Table 2-56 SIP Trunk Security Profile for IM and Presence Trunk

Setting	Value	Comment
Name	IM and Presence	Meaningful name describing the use of the SIP Trunk Security Profile.
Accept Presence Subscription	Checked	
Accept Out-of-Dialog REFER	Checked	
Accept Unsolicited Notification	Checked	
Accept Replaces Header	Checked	

Table 2-57 shows the settings on the SIP trunk security profile to be used for intercluster trunks to other Unified CM clusters. On these trunks we want to accept presence subscriptions to enable intercluster Busy Lamp Field (BLF) presence.

Table 2-57 SIP Trunk Security Profile for Intercluster Trunks

Setting	Value	Comment
Name	ICT	Name describing the use of the SIP Trunk Security Profile.
Accept Presence Subscription	Checked	
Transmit Security Status	Checked	

SIP Trunk Connections

SIP trunks are the preferred way to set up connectivity between Unified CM clusters and between Unified CM and other systems such as gateways, applications, and media resources. Depending on the type of connected system, the parameters configured on each SIP trunk differ slightly. Table 2-58 summarizes the settings for a SIP trunk to a PSTN gateway in site RTP.

Table 2-58 SIP Trunk Settings for Trunk to ISDN Gateway in Site RTP

Setting	Value	Comment
Name	ST_RTP_PSTN_1	Prefix ST_ to avoid name collisions with other devices stored in the same table internally. The remainder of the name identifies the location of the gateway and allows numbers for multiple gateways.
Description		Some meaningful description
Device Pool	RTP_PSTN	Common device pool for all RTP PSTN gateways. Allows sharing of site-specific settings between all RTP gateways.
Media Resource Group List	<None>	Use the MRGL defined on the device pool.
AAR Group	Default	Same everywhere
PSTN Access	Checked	
Run On All Active Unified CM Nodes	Checked	This settings is recommended on all SIP trunks. This makes sure that outbound calls to SIP do not require intra-cluster control signaling between Unified CM call processing subscribers.
Inbound Calls		
Calling Search Space	DN	Inbound calls have +E.164 called party numbers, and only local destinations can be called from the PSTN. Hence, no access is required to ESN numbers and intercluster destinations.
AAR Calling Search Space	PSTNReroute	
Outbound Calls		
Use Device Pool Called Party Transformation CSS	Checked	

Table 2-58 SIP Trunk Settings for Trunk to ISDN Gateway in Site RTP (continued)

Setting	Value	Comment
Use Device Pool Calling Party Transformation CSS	Checked	
SIP Information		
Destination	X.X.X.X	IP address of ISDN gateway
SIP Trunk Security Profile	Non Secure SIP Trunk Profile	Default SIP trunk security profile
SIP Profile	FQDN	

The key here is that the inbound CSS provides access to local +E.164 destinations only. These include voicemail pilots or other services that need to be reachable from the PSTN, but no access is required to PSTN route patterns, dialing normalization translation patterns, ESNs, URIs, and intercluster destinations.

Settings for SIP trunks to other Unified CM clusters differ somewhat from the settings on SIP trunks to ISDN gateways. Table 2-59 summarizes these settings.

Table 2-59 SIP Trunk Settings for Intercluster Trunk to Other Unified CM Cluster

Setting	Value	Comment
Name	ST_UCM_EMEA	Prefix ST_ to avoid name collisions with other devices stored in the same table internally. The remainder of the name identifies the trunk's purpose.
Description		Some meaningful description
Device Pool	Trunks_and_Apps	Common device pool for central trunks (see Table 2-53)
Media Resource Group List	<None>	Use the MRGL defined on the device pool.
AAR Group	Default	Same everywhere
PSTN Access	Not checked	
Run On All Active Unified CM Nodes	Checked	This settings is recommended on all SIP trunks. This makes sure that outbound calls to SIP do not require intra-cluster control signaling between Unified CM call processing subscribers.
Inbound Calls		
Calling Search Space	ICTInbound	Incoming calls on trunks need to support +E.164, ESN, and URI dialing. This special CSS supports all three dialing habits but does not provide access to PSTN or remote on-net destinations (see Table 2-24 in the section on Special CSSs). For applications requiring PSTN access, another special class of service (CSS) is required to also provide access to the partitions with PSTN access route patterns (see Table 2-27 in the section on Route Patterns for PSTN Access and Emergency Calls).
AAR Calling Search Space	PSTNReroute	Same CSS everywhere

Table 2-59 SIP Trunk Settings for Intercluster Trunk to Other Unified CM Cluster (continued)

Setting	Value	Comment
Outbound Calls		
Use Device Pool Called Party Transformation CSS	Checked	
Use Device Pool Calling Party Transformation CSS	Checked	
Calling and Connected Party Info Format	Deliver URI and DN in connected party, if available	On intercluster trunks to other Unified CM clusters, blended identity with both numeric and URI information should be delivered to the remote cluster. If both types of identity exist, then based on the capabilities of the called endpoint, the cluster terminating the call can decide which piece of the identity information can be displayed on the final called party.
SIP Information		
Destination	X.X.X.X	List IP addresses of all Unified CM call processing subscribers of remote Unified CM cluster. The order of the IP addresses is not relevant because outbound calls are randomly distributed among the defined destinations.
SIP Trunk Security Profile	ICT	See Table 2-57
SUBSCRIBE Calling Search Space	ICTInbound	Subscriptions on +E.164, ESN, and URIs should be accepted. For the definition of the CSS, see the section on Special CSSs.
SIP Profile	FQDN	See Table 2-54

In contrast to the SIP trunk to a PSTN ISDN gateway, inbound calls from other Unified CM clusters in addition to +E.164 numbers also need access to ESNs and URIs. However, to avoid routing loops and transit-routing, intercluster trunks do not have access to intercluster destinations (partition onNetRemote, see Table 2-12).

For the SIP trunk to the IM and Presence nodes, configure a SIP trunk between Unified CM and IM and Presence. For this SIP trunk, configure the destination IP addresses of all IM and Presence nodes. Select the SIP Trunk Security Profile that you just created for the IM and Presence Service. Also select the Standard SIP Profile.

Route Groups

All SIP trunks are assigned to route groups. Route groups combine trunks with common characteristics. Table 2-60 shows the route group definition for the PSTN gateways in site RTP.

Table 2-60 Route Group for RTP PSTN Gateways

Setting	Value	Comment
Route Group Name	RTP_PSTN	Meaningful name
Distribution Algorithm	Circular	We want to make sure to balance the load over all gateways.
Route Group Members	ST_RTP_PSTN_1 ST_RTP_PSTN_2 ST_RTP_PSTN_3	Add all SIP trunks to all SIP gateways in site RRP.

Note Route groups can be configured only after the SIP trunks have been created, and these can be added only after the respective device pool have been configured. This means that at the time of creating the device pool for PSTN gateways, route groups do not yet exist. Thus the configuration order is:

1. Configure the device pool for the PSTN gateway without defining the LRG mapping in the device pool.
2. Configure SIP trunks.
3. Create the route group.
4. Go back to the device pool and add LRG mapping (if required).

For intercluster trunks to other Unified CM clusters, a route group per trunks also needs to be defined. Table 2-61 shows an example of a route group for an intercluster trunks to a remote Unified CM cluster.

Table 2-61 Route Group for Intercluster Trunk to Other Unified CM Cluster

Setting	Value	Comment
Route Group Name	UCM_EMEA	Meaningful name; in this case, for the route group holding only the intercluster trunk to the EMEA Unified CM cluster.
Distribution Algorithm	Circular	Irrelevant as long as only one route group member exists.
Route Group Members	ST_UCM_EMEA	SIP trunk to remote Unified CM cluster.

Similar trivial route groups must be created for each non-PSTN SIP trunk provisioned on Unified CM.

Specific Non-LRG Route Lists

The section on Route Lists Using Local Route Groups introduces route lists for PSTN access using local route groups only. For non-PSTN trunks, specific route lists need to be created using the route groups referring to these non-PSTN trunks. The reason for defining trivial route groups with only a single member and trivial route lists with only a single non-LRG route group as member, is that route patterns in Unified CM should never point to a trunk directly, because whenever a route pattern is changed in Unified CM, then the device the route pattern is pointing to is reset, and pointing route patterns to a route list instead of trunks makes sure that editing the route patterns will not reset the trunk itself but rather the route list. Examples for such trunks include trunks to other Unified CM clusters and applications.

Table 2-62 shows the trivial route list for an intercluster trunk to another Unified CM cluster.

Table 2-62 Route List for Intercluster Trunk to Another Unified CM Cluster

Route List	Members	Description
RL_UCM_EMEA	UCM_EMEA	Only a single member: the actual trunk to the remote Unified CM cluster. The leading RL makes sure to avoid naming collisions with trunks. Internally route lists are treated as devices, and the names of route lists cannot be identical to names of SIP trunks, for example.

Similar trivial route lists have to be created for each non-PSTN SIP trunk provisioned on Unified CM.

Endpoint Provisioning

When provisioning a new endpoint, these minimum tasks are required:

- Configure the Device
- Configure the Line
- Add the Device to Devices Controlled by the User
- Configure the Line Association for Presence

Configure the Device

When adding a new endpoint to Unified CM, the design described in this document requires the settings summarized in Table 2-63. Settings not mentioned here are either left as default or have to be configured according to device-specific requirements:

Table 2-63 Endpoint Device Settings

Setting	Value	Description
Device Information		
Device Pool	RTPPhoneVideo	Site-specific device pool for endpoints (see Table 2-51). In this case this is the device pool for endpoints in site RTP with access to video conferencing media resources.
Calling Search Space	USEmergency	Access to emergency routing in multi-national environments is implemented on the device level (see the section on Emergency Call Considerations in Multi-National Environments). If only one country (dialing domain) such as the US needs to be supported, then this CSS can be left as <None>.
AAR Calling Search Space	PSTNReroute	Same everywhere (see the section on Automated Alternate Routing).
Media Resource Group List	<None>	Use device pool level settings.
AAR_Group	Default	Same everywhere (see the section on Automated Alternate Routing).
Owner	Select "User"	If the device is a phones without user association (for example a lobby phone), then select "Anonymous (Public/Shared Space)" and do not set the "Owner User ID"
Owner User ID	Select the user ID of the owner of this phone.	
Allow Control of Device from CTI	Checked	
Number Presentation Transformation		
Caller ID For Calls From This Phone	"Use Device Pool Calling Party Transformation CSS (Caller ID For Calls From This Phone)" checked	
Remote Number	"Use Device Pool Calling Party Transformation CSS (Device Mobility Related Information)" checked	
Protocol Specific Information		
SIP Profile	FQDN	See Table 2-54

Configure the Line

On each endpoint, at least the first line needs to be provisioned. Table 2-64 summarizes the line settings specific to the design described in this document.

Table 2-64 Line Settings

Setting	Value	Description
Directory Number Information		
Directory Number	\+14085554146	Full +E.164 directory number matching the phone number of the user this DN is provisioned for. The leading + has to be escaped with \. If a non-DID is provisioned, then the directory number is set to the ESN (for example, 81405001).
Route Partition	DN	If a non-DID is provisioned, then the partition is ESN.
Alerting Name	Aristotle Boyle	Full name of the user associated with the number. If the number is not associated with a user, then provision a meaningful name (for example, Bldg. 31 Lobby).
Allow Control of Device from CTI	Checked	
Directory Number Settings		
Calling Search Space	SJCInternational	CSS defining the effective class of service for calls from this line. The CSS is specific to site and class of service (see the section on Classes of Service and Calling Search Spaces (CSSs) for other CSSs).
BLF Presence Group	Standard Presence Group	Same for all lines
+E.164 Alternate Number		
Number Mask	Leave mask empty	An empty mask creates the +E.164 alternate number identical to the directory number configured above. If a non-DID is provisioned, no +E.164 alternate number is added because no PSTN address exists for non-DIDs, by definition.
Add to Local Route Partition	Not checked	The +E.164 alternate number is not added to a local route partition because the directory number itself already is a +E.164 number
Advertise Globally via ILS	Not checked	The +E.164 alternate number is not advertised via ILS. Instead, summary routes for each DID range are advertised (see Table 2-68). The only reason to create the +E.164 alternate number is to be able to advertise this +E.164 alternate number as the GDPR PSTN failover number for URIs associated with this directory number.
PSTN Failover for Enterprise Alternate Number, +E.164 Alternate Number, and URI Dialing		
Advertised Failover Number	+E.164 Number	The +E.164 number is advertised as GDPR PSTN. If a non-DID is provisioned, then set to <None>.

Table 2-64 Line Settings (continued)

Setting	Value	Description
AAR Settings		
Voice Mail	Not checked	If a non-DID is provisioned, then check this option.
AAR Destination Mask	+14085554XXX	This DID range mask makes sure that the alternate PSTN destination for AAR is equal to the directory number. If a non-DID is provisioned, then leave this mask empty.
AAR Group	Default	Same everywhere
Call Forward and Call Pickup Settings		
Calling Search Space Activation Policy	Use System Default	
Forward All	"Voicemail" not checked Calling Search Space: SJCInternational	CSS might be set to a more restricted CSS
All other Forward settings other than "Forward Unregistered Internal" and "Forward Unregistered External"	"Voicemail" checked Calling Search Space: SJCInternational	CSS might be set to a more restricted CSS
"Forward Unregistered Internal" and "Forward Unregistered External"	Destination: +14085554146 Calling Search Space: PSTNReroute	Forward Unregistered implements an alternate route through the PSTN in case the endpoint is unregistered. This makes sense only for endpoints in remote sites with local PSTN access for which an alternate route through the PSTN can be established. If a non-DID is provisioned or a DN for which PSTN reroute does not make sense, then check "Voicemail" and set the CSS to SJCInternational or some other CSS that can reach the voicemail pilot.
Line 1 on Device		
Display (Caller ID)	Aristotle Boyle	Full name of the user associated with the number. If the number is not associated with a user then, provision a meaningful name (for example, Bldg. 31 Lobby).
Line Text Label	4146	Makes sure that the last four digits of the directory number are displayed next to the line button on the phone. This setting exists only for lines on devices supporting line text labels.
External Phone Number Mask	+14085554XXX	The external phone number mask is not referenced anywhere in the provisioned dial plan and can be set to anything. For phones on which the external phone number mask determines the text in the first line on the phone display, the mask can be set to something that creates a meaningful label.

Add the Device to Devices Controlled by the User

For devices associated with users, after provisioning the device in the End User Configuration of the respective user in the Device Information section in Unified CM Administration, make sure that the device is associated with the user. The recommended way to achieve this is to select **Device Association** and search for devices where the directory number matches the phone number of the user.

Configure the Line Association for Presence

To determine the presence state of a user, only the line appearances (per DN and device) explicitly associated for presence are considered. To make sure that all line appearances of a user's directory numbers are considered for presence, in the End User Configuration of the respective user in the section on Device Information in Unified CM Administration, select **Line Appearance Association for Presence** and associate all line appearances.

Verify the User's Primary Extension

To make sure that the user's directory URI synchronized from LDAP propagates to the directory number, select the Primary Extension in the Directory Number Associations section in the End User Configuration of the respective user in Unified CM Administration.

Jabber Provisioning

Service Discovery enables Jabber to establish configuration automatically. The Jabber client gets its configuration through Unified CM User Discovery Service (UDS). It is the recommended configuration and is preferred over the older manual configuration.

The services are configured through UC services. A Service profile specifies which UC services to use. Each user is associated with a service profile.

Table 2-65 shows the UC services that can be made available to Jabber clients. Those services are configured in **User Management** > **User Settings** > **UC service**.

Table 2-65 UC Services

UC Service Type	Comment
IM and Presence	Create an IM and Presence service for each IM and Presence node.
Directory	Create a Directory service for each active directory server. Do not select "Use UDS for Contact Resolution" when integrating with LDAP directly. The recommended contact source for on-premises deployments is CDI.
CTI	Create a CTI service for each Unified CM running the CTI Manager service. This is used for desk phone control mode. Load balance the CTI load across all Unified CM call processing nodes.
Voicemail	Create a Voicemail service for each Unity Connection node.

Associate the UC services to a Service Profile. A Service Profile is then associated to each user. For deployments with more than two Unified CM call processing subscribers, spread the CTI load equally across all Unified CM call processing subscribers and ensure that the CTI scalability limit is not

exceeded on any single Unified CM call processing subscriber running the CTI Manager service. To associate Jabber clients with another Unified CM call processing subscriber running the CTI Manager service, configure another Service Profile with the relevant CTI UC service settings.

For users connected to the internal enterprise network (not using Cisco Collaboration Edge), directory search Contact Sources can be provided through UDS or through LDAP. With LDAP, Cisco Directory Integration (CDI) is available. The Contact Source or directory can be configured through the jabber-config.xml file or through the directory UC service which takes precedence. The recommendation is to configure a jabber-config.xml file that is uploaded onto the Unified CM TFTP server. The jabber-config.xml file is also used to enable URI dialing for Jabber clients. Example 2-5 shows a jabber-config.xml file to enable URI dialing for Jabber clients. This is the recommended minimum. Additional configuration options can be added.

Example 2-5 jabber-config.xml File to Enable URI Dialing

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
    <Policies>
        <EnableSIPURIDialling>true</EnableSIPURIDialling>
    </Policies>
</config>
```

For more details, refer to the latest version of the following documents:

- *Configuration and Administration of IM and Presence on Cisco Unified Communications Manager*

  https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html
- Cisco Jabber Install and Upgrade Guides

  https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html

ILS Configuration for Multi-Cluster Deployments

When the Intercluster Lookup Service (ILS) is configured on multiple clusters, ILS updates Unified CM with the current status of remote clusters in the ILS network.

The ILS cluster discovery service allows Unified CM to learn about remote clusters without the need for an administrator to manually configure connections between each cluster.

The ILS cluster discovery service enables UDS-based service discovery for Jabber clients in multi-cluster environments. In addition, ILS is the foundation for global dial plan replication (GDPR), which allows the exchange of reachability information for both alphanumeric URIs and numeric destinations between Unified CM clusters to enable deterministic intercluster routing for those destinations.

To create an ILS network of multiple Unified CM clusters, perform the following tasks:

- Assign Unique Cluster IDs for Each Unified CM Cluster in the Network
- Activate ILS on the First ILS Hub Cluster in the Network
- Activate ILS on the Remaining ILS Clusters in the Network
- Consider UDS Certificate Requirements

Assign Unique Cluster IDs for Each Unified CM Cluster in the Network

The cluster IDs defined in the Unified CM cluster enterprise parameters have to be unique. See Table 2-2 for details.

Activate ILS on the First ILS Hub Cluster in the Network

Forming an ILS network starts with activating ILS on the first Unified CM cluster. This done by changing the role from Standalone Cluster to Hub Cluster in the ILS Configuration menu in Unified CM Administration.

Table 2-66 shows the settings to be applied when activating ILS on the first Unified CM cluster.

Table 2-66 ILS Activation on First Unified CM Cluster

Setting	Value	Comment
Role	Hub Cluster	ILS is activated by changing the role from Standalone Cluster to Hub Cluster.
Exchange Global Dial Plan Replication Data with Remote Clusters	Checked	Makes sure that URI and numeric reachability information is exchanged with remote clusters.
Advertised Route String	us.route	The advertised route string is the location attribute tied to all URI and numeric reachability information advertised by this Unified CM cluster. Remote clusters trying to reach any of the destinations advertised by this cluster will establish the route to this destination by matching the learned SIP route string against SIP route patterns provisioned on the remote cluster.
Synchronize Clusters Every	2	Setting the synchronization interval to a reasonably small interval makes sure that changes are picked up by remote clusters after a short period of time. The overhead of a short synchronization interval is limited because GDPR uses an incremental update algorithm that exchanges only delta information if any changes occurred since the last update.
ILS Authentication		
Use TLS Certificates	Checked	Certificate-based authentication of ILS TLS connections.
Use Password	Checked	Password-based authorization.
Password	<some password>	Choose a secure password. This password is shared among all Unified CM clusters participating in the ILS network.

When you activate ILS by changing the role from Standalone Cluster to Hub Cluster in Unified CM Administration, an ILS Cluster Registration pop-up appears and asks you to input a Registration Server. When you activate ILS on the first Unified CM cluster, no registration server information is available, so the input in that pop-up should be left empty.

If you activate both **Use TLS Certificates** and **Use Password** at the same time, then at TLS connection setup the TLS certificate presented by the remote end has to pass only the regular TLS certificate validity checks (identity, validity, and trust), and the decision whether the remote peer is a trusted peer for ILS communication is based on checking the shared secret (password). Without using the shared secret

(password) authorization, all Tomcat certificates of all clusters involved in the ILS exchange would need to be exchanged between all clusters. Using shared secret (password) authorization greatly simplifies the deployment of ILS with CA-signed certificates.

Activate ILS on the Remaining ILS Clusters in the Network

Adding more Unified CM clusters to the ILS network requires the same process as activating ILS on the first Unified CM cluster: changing the role from Standalone Cluster to Hub Cluster in the ILS Configuration menu in Unified CM Administration.

Table 2-67 shows the settings to apply when activating ILS on the remaining Unified CM clusters.

Table 2-67 ILS Activation on Additional Unified CM Clusters

Setting	Value	Comment
Role	Hub Cluster	ILS is activated by changing the role from Standalone Cluster to Hub Cluster.
Exchange Global Dial Plan Replication Data with Remote Clusters	Checked	Makes sure that URI and numeric reachability information is exchanged with remote clusters.
Advertised Route String	emea.route	Make sure that the SIP route string for each cluster is unique to allow for deterministic routing based on these route strings. The example here indicated that this is a Unified CM cluster serving EMEA destinations.
Synchronize Clusters Every	2	Make sure to use the same synchronization interval on all clusters for consistency.
ILS Authentication		
Use TLS Certificates	Checked	Certificate-based authentication of ILS TLS connections.
Use Password	Checked	Password-based authorization is selected.
Password	<some password>	Choose a secure password. This password is shared among all Unified CM clusters participating in the ILS network.

Consider UDS Certificate Requirements

To enable UDS-based service discovery, the UDS process on each Unified CM cluster tries to establish connectivity with the UDS processes running on remote Unified CM clusters to learn about the remote clusters' UDS nodes. For this server-to-server communication, TLS connections between the Unified CM clusters' nodes are established and the remote peers' certificates are validated during TLS connection setup. To prevent this validation from failing, the Tomcat certificates of the Unified CM publisher and call processing subscriber nodes must be signed by a trusted CA.

Also, this server-to-server communication is one of the reasons why **TLS Web Client Authentication** has to be in the X.509 extended key usage when issuing Tomcat certificates on an external CA.

GDPR Configuration (Multi-Cluster Only)

When Global Dial Plan Replication (GDPR) is enabled across an ILS network, remote clusters in an ILS network share global dial plan data, including the following:

- Directory URIs
- +E.164 and ESN patterns
- PSTN failover numbers

GDPR allows you to create a global dial plan, including intercluster dialing of directory URIs and alternate numbers, that spans across an ILS network. GDPR allows you to quickly configure the global dial plan across the ILS network without the need to configure each dial plan component on each cluster separately.

Configuring GDPR requires the following steps in addition to activating ILS as described in the previous section:

- Advertise URIs
- Configure Advertised Patterns
- Configure Partitions for Learned Numbers and Patterns
- Configure Intercluster Trunks
- Configure SIP Route Patterns

Advertise URIs

In this document we assume that URIs for users are automatically provisioned based on the directory URI synchronized for each user from the email attribute of the corporate directory (see Table 2-43) and the primary extension configure for the user. By default the **Advertise Globally via ILS** option is set for these URIs automatically created in partition Directory URI. Also make sure to set the **Advertise Globally via ILS** option on all URIs you have provisioned in addition to the ones created automatically.

Configure Advertised Patterns

To keep the route plan small on remote clusters, in this design only summary patterns are advertised for each +E.164 and ESN range hosted on each cluster. For the example cluster hosting the sites RTP, RCD, and SJC, the patterns shown in Table 2-68 need to be configured as GDPR advertised patterns. For information on the DID ranges and ESN ranges used in the example, refer to Table 2-9 and Table 2-10.

Table 2-68 Patterns Advertised via GDPR

Pattern	Pattern Type	PSTN Failover Setting	Comment
+14085554XXX	+E.164 Number	Use Pattern as PSTN Failover Number	Site SJC DID range
81404XXX	Enterprise Number	Apply Strip Digits and Prepend Digits to Pattern and Use for PSTN Failover PSTN Failover Strip Digits: 4 PSTN Failover Prepend Digits: +1408555	ESN range of SJC DIDs. Strip digits and prefix to transform from ESN to PSTN failover number.
81405XXX	Enterprise Number	Don't use PSTN Failover	ESN range of SJC non-DIDs. No PSTN failover possible.

Table 2-68 Patterns Advertised via GDPR (continued)

Pattern	Pattern Type	PSTN Failover Setting	Comment
+19195551XXX	+E.164 Number	Use Pattern as PSTN Failover Number	Site RTP DID range
81911XXX	Enterprise Number	Apply Strip Digits and Prepend Digits to Pattern and Use for PSTN Failover PSTN Failover Strip Digits: 4 PSTN Failover Prepend Digits: +1919555	ESN range of RTP DIDs. Strip digits and prefix to transform from ESN to PSTN failover number.
81912XXX	Enterprise Number	Don't use PSTN Failover	ESN range of SJC non-DIDs. No PSTN failover possible.
+19725555XXX	+E.164 Number	Use Pattern as PSTN Failover Number	Site RCD DID range
81975XXX	Enterprise Number	Apply Strip Digits and Prepend Digits to Pattern and Use for PSTN Failover PSTN Failover Strip Digits: 4 PSTN Failover Prepend Digits: +1972555	ESN range of RCD DIDs. Strip digits and prefix to transform from ESN to PSTN failover number.
81976XXX	Enterprise Number	Don't use PSTN Failover	ESN range of RCD non-DIDs. No PSTN failover possible.
8099XXXX	Enterprise Number	Don't use PSTN Failover	ESN ranges for conferences on this cluster (see Table 2-10).

Advertising both the +E.164 range and the ESN range for each site makes sure that both formats can be used as the intercluster dialing habit on the remote clusters learning this information.

Configure Partitions for Learned Numbers and Patterns

Numeric patterns (+E.164 and ESN) learned from remote clusters are added to the local route plan into predefined partitions. The **Partitions for Learned Numbers and Patterns** menu in Unified CM Administration allows you to define differentiated partitions for each type of learned information. In this design we do not need this differentiation and simply configure GDPR to learn all remote numeric patterns in a single partition, onNetRemote (see Table 2-12).

Table 2-69 summarizes the settings for the GDPR partitions.

Table 2-69 GDPR Partition Settings

Setting	Value	Comment
Partition for Enterprise Alternate Numbers	onNetRemote "Mark Learned Numbers as Urgent" checked	
Partition for +E.164 Alternate Numbers	onNetRemote "Mark Learned Numbers as Urgent" checked	Marked urgent to avoid inter-digit timeout on +E.164 on-net intercluster calls.

Table 2-69 GDPR Partition Settings (continued)

Setting	Value	Comment
Partition for Enterprise Patterns	onNetRemote "Mark Fixed Length Patterns as Urgent" checked "Mark Variable Length Patterns as Urgent" unchecked	
Partition for +E.164 Patterns	onNetRemote "Mark Fixed Length Patterns as Urgent" checked "Mark Variable Length Patterns as Urgent" unchecked	Marked urgent to avoid inter-digit timeout on +E.164 on-net intercluster calls.

Configure Intercluster Trunks

The GDPR exchange only makes sure that all URI and numeric reachability information is exchanged between Unified CM clusters and associated with a SIP route string as the location attribute. Sessions between clusters need SIP trunks to be established. In this design we assume full-mesh SIP trunks between all Unified CM clusters, with a maximum of three Unified CM clusters. The maximum of three Unified CM clusters makes sure that the topology of the full mesh of SIP trunks is manageable. If more than three Unified CM clusters are required, then adding Unified CM Session Management Edition (SME) is recommended to simplify the topology to a hub-and-spoke topology with SME as the hub and all other Unified CM clusters as spokes or leaf clusters.

Regular SIP intercluster trunks are used for GDPR routing. SIP trunk ST_UCM_EMEA, as with the settings shown in Table 2-59, is an example of an intercluster trunk provisioned for GDPR routing.

Configure SIP Route Patterns

SIP route patterns tie together the SIP route strings learned via GDPR and the SIP trunk topology. Think of it as if a GDPR route strings tells us "where" a learned URI or numeric pattern is located, and we need route patterns matching on these route strings to tell how to get to this destination.

To achieve full GDPR reachability, we need to make sure that each SIP route string advertised via GDPR can be routed according to the provisioned SIP route patterns. Table 2-70 summarizes the trunks, route groups, route lists, and SIP route patterns that need to be provisioned to enable full intercluster GDPR routing between two Unified CM clusters.

Table 2-70 GDPR Routing with Two Unified CM Clusters

Component	US Cluster	EMEA Cluster	Comment
SIP Trunk	ST_UCM_EMEA	ST_UCM_US	SIP trunk on each cluster to the other Unified CM cluster (see Table 2-59)
Route Group with above SIP trunk as member	UCM_EMEA	UCM_US	Dedicated route group for the intercluster trunk (see Table 2-61)
Route List with above route group as member	RL_UCM_EMEA	RL_UCM_US	Dedicated non-LRG route list for the intercluster trunk (see Table 2-62)

Table 2-70 GDPR Routing with Two Unified CM Clusters (continued)

Component	US Cluster	EMEA Cluster	Comment
SIP Route String	us.route	emea.route	SIP route string advertised by the Unified CM cluster
SIP Route Pattern pointing to above route list	emea.route in partition onNetRemote	us.route in partition onNetRemote	Provisioned SIP route pattern matches on the SIP route string advertised by the other Unified CM cluster

Example GDPR Call Flow

With the above configuration, this section describes how a call would be routed if +14085554001 is dialed on an endpoint with class of service "international" registered to the EMEA cluster in the above example.

1. The dialed digits (+14085554001) are matched against the dial plan on the EMEA cluster, using the calling device's CSS XXXInternational, where XXX represents a site code of a site provisioned on the EMEA cluster. The actual site-specific dialing normalization is irrelevant here.

   The important point is that CSS XXXInternational contains at least the following partitions (see Table 2-17; again XXX represents a site code while XX represents some dialing domain identifier):

   - DN
   - Directory URI
   - URI
   - ESN
   - onNetRemote
   - XXXIntra
   - XXtoE164
   - XXPSTNNational
   - PSTNInternational
   - B2B_URI
   - USEmergency

   The dialed digits (+14085554001) in these partitions have three matches:

   - +14085554XXX in partition onNetRemote learned from the US cluster with SIP route string us.route (see Table 2-68)
   - \+! in partition PSTNInternational (see Table 2-27)
   - \+!# in partition PSTNInternational (see Table 2-27)

2. Because +14085554XXX in partition onNetRemote is inserted into the route plan as urgent pattern (see Table 2-69) and this pattern at this point is the best match, digit collection is stopped immediately and the call is routed based on this best match.

3. +14085554XXX in partition onNetRemote is a GDPR learned pattern and is associated with SIP route string us.route. Hence, us.route is matched against the configured SIP route patterns on the EMEA cluster, again using the calling device's CSS XXXInternational.

   The only match is SIP route pattern us.route in partition onNetRemote.

4. The call on the EMEA cluster is extended to SIP trunk ST_UCM_EMEA, dereferencing the route list RL_UCM_EMEA the matched SIP route pattern us.route points to and route group RG_UCM_EMEA (see Table 2-70)
5. On the US cluster, the inbound CSS ICTInbound of SIP trunk ST_UCM_EMEA (see Table 2-59) is used to route the inbound call to destination +14085554001.
6. CSS ICTInbound has these partitions:
   - DN
   - ESN
   - URI
   - Directory URI

   In these partitions the only (potential) match is on a +E.164 directory number \+14085554001 (marked urgent) in partition DN. If this directory number exists, then the call is extended to all associated devices.

Routing of remotely dialed ESN destinations follows the exact same flow, with the only exception being that the final lookup on the US cluster using CSS ICTInbound in that case would find a match on an ESN in partition ESN.

IM and Presence Intercluster

To create a fully meshed presence topology, each Cisco IM and Presence cluster requires a separate peer relationship for each of the other Cisco IM and Presence clusters within the same domain. The address configured in this intercluster peer is the IP address of the remote Unified CM cluster IM and Presence publisher node.

The interface between each Cisco IM and Presence cluster is two-fold: an AXL/SOAP interface and a signaling protocol interface (SIP or XMPP). The AXL/SOAP interface, between publisher-only servers of an IM and Presence cluster, handles the synchronization of user information for home cluster association, but it is not a full user synchronization. The signaling protocol interface (SIP or XMPP) is a full mesh encompassing all servers within the deployment. It handles the subscription and notification traffic, and it rewrites the host portion of the URI before forwarding if the user is detected to be on a remote Cisco IM and Presence cluster within the same domain.

When Cisco IM and Presence is deployed in an intercluster environment, a presence user profile should be determined. The presence user profile helps determine the scale and performance of an intercluster presence deployment and the number of users that can be supported. The presence user profile helps establish the number of contacts (or buddies) a typical user has, as well as whether those contacts are mostly local cluster users or users of remote clusters.

Survivable Remote Site Telephony (SRST) Deployment

Configure SRST at each remote site in order to provide call processing survivability in case the WAN to the remote site fails. With SRST, if the WAN fails, phone calls can still be made within the remote site or out to the PSTN.

Deployment

Deploy one Cisco Integrated Services Router (ISR) for each remote sites that you want to enable for SRST.

Provisioning

To configure SRST, you must perform the configuration on both Unified CM and the SRST router.

On Unified CM:

- Configure an SRST Reference for each remote site, and associate this SRST Reference in the device pool of the remote phones.
- Configure Call Forwarding Unregistered (CFUR) on the DNs of the remote phones to use the phone's +E.164 number and the AAR CSS. In case the WAN fails and the phone unregisters, Unified CM uses this information to route incoming calls destined for the unregistered phone to the site's gateway via the PSTN.
- Set the **Max Forward UnRegistered Hops to DN** service parameter to a value other than zero to make sure to limit the impact of routing loops that can occur if a phone is unregistered (for example, because it is not plugged in) while the site's gateway still is connected to Unified CM.

On the SRST router:

- Configure SRST on each remote branch router. Since our recommendation is to use SIP phones, use the **voice register global** and **voice register pool** commands. Use the **voice service voip/sip** command to bind the IP addresses of the source interface and enable the registrar capability. Configure DHCP for the phones in the remote branch. The DHCP server may be configured on the SRST router or on other network service resources.
- If the WAN fails, the SIP phones will register with their +E.164 extensions. In order to allow users to call other local users by their four-digit extensions, configure a voice translation profile that is referenced as an incoming profile in the voice register pool configuration. This voice translation profile transforms the called number from four digits to the complete +E.164 number.
- Configure POTS dial-peers to allow local access to the PSTN in case the WAN is down. Configure translation voice profiles in order to comply with the service provider's PSTN dialing requirements. For more details on dial-peer configuration, refer to the section that describes how to Deploy Cisco Unified Border Element.

The SRST configuration in Example 2-6 is just a partial configuration to illustrate some of the concepts discussed in the previous paragraphs. It does not cover the full SRST configuration. For instance, configuration to reach the Cisco Unity Connection server in the main site is covered in the chapter on Voice Messaging.

Example 2-6 SRST Partial Configuration

```
voice service voip
 allow-connections sip to sip
sip
  bind control source-interface GigabitEthernet0/0.241
  bind media source-interface GigabitEthernet0/0.241
  registrar server
!
voice register global
 mode srst
 max-dn 100
 max-pool 100
!
voice register pool  1
 translation-profile incoming 4-digit-rtp
 id network 10.0.94.0 mask 255.255.255.0
!
voice translation-rule 1
 rule 1 /\(^1...\)$/ /+1919555\1/
!
voice translation-profile 4-digit-rtp
 translate called 1
!
```

For more details on configuring SRST, refer to the *Cisco Unified SCCP and SIP SRST System Administrator Guide*, available at

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cusrst/admin/sccp_sip_srst/configuration/guide/SCCP_and_SIP_SRST_Admin_Guide.html

Extension Mobility

Cisco Extension Mobility allows users to temporarily access their Cisco Unified IP Phone configuration – such as line appearances, services, and speed dials – from other Cisco Unified IP Phones.

One or two Unified CM call processing nodes can actively handle Extension Mobility requests. The benefits of adding a second Unified CM call processing node for Extension Mobility are resiliency and increased capacity. In this scenario, a load balancer is required to send the requests to both Unified CM nodes. Cisco IOS Server Load Balancing can be used, for example.

Extension Mobility Cross Cluster (EMCC) provides the ability to perform Extension Mobility logins between clusters within an enterprise. This feature is not covered in this guide. For more details on EMCC, refer to the latest version of the *Cisco Collaboration System SRND* and the EMCC product documentation.

Deploying Extension Mobility

To deploy Extension Mobility, perform the following tasks:

- Ensure that the Cisco Extension Mobility service is activated on one or two Unified CM call processing servers.
- Add an IP Phone Service for Extension Mobility. A secure IP Phone Services URL using HTTPS in addition to a non-secure URL can be configured. The non-secure URL is

  http://<*IPAddress*>:8080/emapp/ EMAppServlet?device=#DEVICENAME#

  You can either make this service available to all phones in the cluster by selecting Enterprise Subscription or make it available to selected phones by subscribing those phones to this service.
- For each user that will use Extension Mobility, create at least one Device Profile. Since a Device Profile is tied to a specific user, the Device Profile is usually referred to as a User Device Profile. If a Device Profile is not created for a user, that user will not be able to log in with extension mobility.
- Associate the device profile to a user for extension mobility. If CTI is needed, also associate the profile to be a CTI controlled device profile.
- For each phone that can be used for users to log in, enable Extension Mobility.
- On the DN configuration, configure the association of the appropriate user to the line. This allows the DN to send presence information for that user if the line of that phone is in use. For example:

  User B is using Jabber and is monitoring user A. User A logs into a phone with Extension Mobility and has a User Device Profile with the DN associated to himself/herself. When user A goes off-hook, this presence information will be reported on the Jabber client of user B.

For more details on Extension Mobility, refer to the latest version of the *Feature Configuration Guide for Cisco Unified Communications Manager*, available at

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

Busy Line Field (BLF) Presence

The BLF Presence feature allows a user (watcher) to monitor the real-time status of another user at a directory number or SIP URI from the device of the watcher. A watcher can monitor the status of the user by using the following options:

- BLF/SpeedDial buttons
- Missed call, placed call, or received call lists in the directories window
- Shared directories, such as the corporate directory

BLF Presence is not based in Cisco Unified IM and Presence.

Deploying BLF Presence

- Enable the **BLF for Call List** enterprise parameter (see Table 2-2).
- Configure the cluster-wide service parameters for BLF presence.
- To use BLF presence group authorization, configure BLF presence groups and permissions.
- Apply a BLF presence group to the directory number, SIP trunk, phone that is running SIP, phone that is running SCCP, end user, and application user (for application users that are sending BLF presence requests over the SIP trunk) in Cisco Unified Communications Manager Administration.

- To allow BLF presence requests from a SIP trunk, select the **Accept Presence Subscription** option in the SIP Trunk Security Profile Configuration window (see Table 2-57).
- Configure the SUBSCRIBE calling search space and apply the calling search space to the phone, trunk, or end user, if required.
- For BLF/SpeedDial buttons on the phones, customize phone button templates for the BLF/SpeedDial buttons or add them directly to the phones.

Deploying Computer Telephony Integration (CTI)

- Activate the CTI Manager service on the Unified CM call processing nodes that need the CTI Manager service.
- For redundancy, through the CTI application administration, select a primary and backup Unified CM node running the CTI Manager service,
- Download the TAPI client software for applications using TAPI.
- If possible, for a given CTI-enabled endpoint, configure the same Unified CM call processing node for CCM registration and for CTI Manager monitoring and control.
- Ensure the CTI load is spread across all Unified CM nodes running the CTI Manager and that the CTI capacity limits are not exceeded. For example, with Jabber clients, if two Unified CM call processing pairs are required, spread the registration across the two pairs; also, if the Jabber clients are configured with the ability to be in deskphone mode, spread the CTI Manager connectivity across the two pairs. This can be achieved with multiple Service Profiles with different CTI profiles associated. Ensure the number of Jabber clients in deskphone mode monitored and controlled by each Unified CM running the CTI Manager service does not exceed the CTI capacity limit.